45 P0T3NC14l1D4D35

D3 4T1V1D4D35

P3D4GÓG1C4S

3NV0LV3ND0

PR0BL3M45

C R1PT0GR4F1C05

N4 3XPL0R4ÇÃ0

D45 1D3145

4550C14D45

4 FUNÇ40 4FIM

UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
INSTITUTO DE GEOCIÊNCIAS E CIÊNCIAS EXATAS

Beatriz Fernanda Litoldo

As potencialidades de atividades pedagógicas envolvendo problemas criptográficos na exploração das ideias associadas à função afim.

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Educação Matemática do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", campus de Rio Claro, como parte dos requisitos para obtenção do título de Mestre em Educação Matemática.

Orientadora: Dra. Arlete de Jesus Brito

Rio Claro
2016

510.07 Litoldo, Beatriz Fernanda
L776p As potencialidades de atividades pedagógicas envolvendo problemas criptográficos na exploração das ideias associadas à função afim / Beatriz Fernanda Litoldo. - Rio Claro, 2016
198 f. : il., figs., quadros

Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas
Orientadora: Arlete de Jesus Brito

1. Matemática - Estudo e ensino. 2. Ensino Médio. 3. Criptografia. 4. Cifras. 5. Criptoanálise. I. Título.

Ficha Catalográfica elaborada pela STATI - Biblioteca da UNESP
Campus de Rio Claro/SP

Beatriz Fernanda Litoldo

As potencialidades de atividades pedagógicas envolvendo problemas criptográficos na exploração das ideias associadas à função afim

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Educação Matemática do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", campus de Rio Claro, como parte dos requisitos para obtenção do título de Mestre em Educação Matemática.

Comissão Examinadora

Profª. Drª. Arlete de Jesus Brito – Orientadora
IB/UNESP/Rio Claro (SP)

Profª. Drª. Cármen Lúcia Brancaglion Passos
CECH/UFSCAR/São Carlos (SP)

Prof. Dr. Eugenio Maria de França Ramos
IB/ UNESP/ Rio Claro (SP)

Rio Claro, SP 06 de junho de 2016

DEDICATÓRIA

Dedico essa dissertação a minha mãe Helena, pela força e coragem que me ofereceu durante toda esta longa caminhada. Mãe, você foi e sempre será meu exemplo de vida. Obrigada por ser a mulher que é e por fazer de mim a filha que sou.

AGRADECIMENTOS

Gostaria de agradecer, em primeiro lugar, a minha família, começando por minha mãe Helena Caritá, um exemplo de vida e minha heroína, obrigada por todo o seu apoio e incentivo nas horas difíceis, de desânimo e cansaço. Sua garra em enfrentar a vida e buscar o seu melhor sempre só me fez acreditar no quanto a senhora é especial, felizes são aqueles que te conhecem e podem conviver ao seu lado. Aos meus tios, agradeço por todos os momentos que passamos juntos e aos meus primos Marcelo Corroqué e Nádia Corroqué por sempre estarem ao meu lado e por serem meus primeiros espelhos. A minha avó Maria Caritá, que com seus gatinhos sempre nos recebe de braços abertos, ao meu falecido avô Davi Caritá, que sempre fazia de tudo por seus netos e nunca se deixava abater pelos obstáculos da vida e ao meu também falecido avô Pedro Litoldo, o qual eu nunca esqueci, mesmo a vida nos tenha levado a caminhos diferentes.

Agradeço também, com o coração cheio de alegria e amor, a todo carinho, companheirismo e amor que recebo continuamente de meu namorado Éverton dos Santos. Seu amor e apoio se tornaram fundamentais para minha vida. Muito obrigada por me deixar fazer parte de sua vida e por dividir momentos especiais dela comigo. Juntamente, agradeço a sua família, D. Alzira dos Santos, minha sogra e Emerson dos Santos e Evelyn dos Santos, meus cunhados. Vocês me receberam de braços abertos e há muito tempo já me considero parte da família Carvalho. As minhas duas princesinhas Maria Eduarda dos Santos e Maria Fernanda dos Santos e ao meu principezinho Leo Corroqué. Com vocês não há dias ruins e poder fazer parte de suas vidas é a coisa mais gostosa que existe.

Não poderia deixar de registrar o meu agradecimento ao Prof. Dr. Henrique Lazari, o qual apoiou esta pesquisa desde seus primeiros passos e a orientou por um bom tempo. Por situações da vida, a pesquisa mudou de orientador e tive a graça de poder contar com a Prof.ª Dra. Arlete de Jesus Brito. Minha já conhecida professora de graduação, e um espelho para mim no meio acadêmico, tive a honra de poder ser orientada por essa mulher incrível e admirável. Suas discussões, observações e orientações tiveram papel fundamental na finalização desse trabalho. Agradeço de coração pela paciência e por se permitir aventurar pela minha pesquisa, ela só teve a ganhar com a sua participação.

Registro também meus agradecimentos a uma grande amiga por ter me dado todo o apoio que precisei durante essa etapa. Ronilce Lopes, realizar essa pesquisa e enfrentar seus obstáculos podendo contar com você só a fez ficar mais leve. Sua paciência em me ouvir e ler tudo o que escrevia fizeram muita diferença no resultado deste trabalho. Ele tem muito de

você e das nossas discussões. Sinto-me muito agradecida pelo destino ter colocado você no meu caminho e pela amizade linda que construímos.

Não poderia deixar de expressar minha gratidão aos membros da banca Prof.ª Dra. Cármen Passos, Prof. Dr. Eugenio Ramos e Prof.ª Dra. Arlete de Jesus Brito. Seus comentários e observações só ampliaram o espectro de minhas reflexões perante a este trabalho. Com análises e encaminhamentos persistentes esta pesquisa só veio a crescer com vocês. Saibam que todos contribuíram, não somente para esta dissertação, mas também para o meu próprio crescimento profissional.

Reservo um espaço para agradecer ao programa de Pós- Graduação da Educação Matemática (PGEM), em especial ao coordenador da PGEM Prof. Marcus Maltempi, por toda a atenção dedicada aos alunos e pela competência na coordenação e a secretária da PGEM Inajara Moraes, por todo auxílio dado aos alunos, e por nos socorrer sempre que precisamos de informações. Seu trabalho faz diferença nesse programa. Aos professores, meus agradecimentos. A qualidade com que vocês ministram suas disciplinas e trabalham em seus grupos de pesquisa, juntamente com o respeito que tem com seus alunos, só me faz acreditar mais ainda na competência fantástica que esse programa tem. Tenho muito a agradecer à vocês, pois muito do que sou hoje é reflexo do aprendizado proporcionado por vocês. Não posso deixar de agradecer, em especial, aos grupos de pesquisa GTERP (Grupo de Trabalho e Estudos em Resolução de Problemas) e GPIMEM (Grupo de Pesquisa em Informática, outras Mídias e Educação Matemática), que me adotaram durante essa caminhada proporcionando constantemente, aprendizados, ajudas e momentos de discussões e de descontração. Agradeço à todos os integrantes dos grupos. Vocês foram grandes apoios para mim, obrigada pela oportunidade da minha inserção aos grupos e por me receberem de braços abertos.

Gostaria de destacar alguns nomes de mestres que foram muito importantes para minha formação até aqui. Aos grandes professores amigos deixo meus agradecimentos a Marta Gadotti, Renata Zotin, Suzinei Marconato, João Peres, Miriam Penteado, Roger Miarka e Heloisa da Silva. Em especial ao professor Marcelo Borba, do qual o auxilio dado a mim é imensurável. Muito do que aprendi como pesquisadora vem de nossas caminhadas e happy hours. Faltam-me palavras para demonstrar o quanto seus conselhos me guiaram nessa jornada. Para encerrar os agradecimentos aos mestres, nada me deixa mais contente do que agradecer a uma grande professora e amiga Eliris Rizziolli. Com você Eliris aprendi a ser mais doce com a vida, a ter mais seriedade nas decisões, a refletir melhor sobre meus atos e a acreditar no potencial dos meus alunos. Você não é somente um espelho acadêmico, mas sim, um espelho pra vida. Muito obrigada pela sua amizade.

Dedico um singelo agradecimento a todos os funcionários da UNESP, sendo eles porteiros, jardineiros, equipes de limpeza, todo o pessoal da administração (graduação e pós-graduação) e aos atenciosos servidores do R.U. Vocês fazem parte dessa família chamada UNESP, sem vocês essa engrenagem não conseguiria manter-se funcionando. Com muito carinho, agradeço à todos os funcionários da biblioteca e dos departamentos de Educação Matemática e Matemática. Vocês nos recebem com muito apreço e oferecem, sempre que solicitados, muita atenção e ajuda. Nossa caminhada por essa instituição se torna muito mais leve quando deparamos com pessoas dedicadas e competentes como vocês.

Também agradeço à CAPES, por todo o financiamento desta pesquisa. Sem ele minha dedicação integral ao mestrado seria impossível e com isso, realizar esse trabalho teria sido uma tarefa muito mais árdua. Juntamente, gostaria de agradecer a escola e aos alunos que aceitaram fazer parte dessa pesquisa. Sem vocês esse trabalho não teria sido realizado.

Por fim, para encerrar a seção de agradecimentos com chave de ouro, quero agradecer todos os amigos que, de algum modo, nos momentos serenos ou apreensivos, fizeram ou fazem parte da minha vida; por isso primeiramente começo agradecendo a minha professora de inglês Eliana Ventura, a qual, com sua enorme paciência e irreverencia tem batalhado ao meu lado na difícil tarefa de me ensinar inglês. Em segundo lugar, teço agradecimentos para minhas professoras da academia Glaucia Peruzzi e Fernanda Guzzo. Vocês duas são grandes responsáveis por minha saúde corporal e mental. No embalo fitness agradeço aos meus companheiros de sofrimento Carla Gomes, Maraci Soares, Tatiane Alvez, Mauricio Alvez, Paulo Campacci, Daniel Pilla, Fernanda Hebling, Cristina dos Santos, Mateus Arena, Renato Favaro e entre outros amigos que fazem cada dia de academia ser mais alegre. Malhar com vocês é um privilégio, e dividir o sofrimento acalma a alma e o corpo.

Aos meus amigos de graduação e pós-graduação agradeço à todos de coração. Lucas Mazzi, Patrick Ferrari, Leandro Sannomiya (Japa), Marcia da Silva, Hannah Lacerda, Patricia Peralta, Luana Oliveira, Rose Batistela, Ingrid Firme, Helber Almeida, Douglas da Silva, Carla Vital entre outros tantos. Vocês estiveram ao meu lado tanto nos momentos difíceis quanto nos momentos alegres. A realização desse trabalho tem um pouco de cada um, de cada discussão, de cada conselho e de cada comemoração que fizemos. Trilhar o mestrado teria sido muito mais difícil sem vocês comigo. Muito obrigada por me dar suporte, seus ombros, seus sorrisos e seus abraços. Vocês foram essenciais para sustentar o emocional dessa caminhada.

Finalizo os agradecimentos aos amigos lembrando dos que já faziam parte da minha vida e daqueles que ganhei nesses últimos anos fora da matemática. Minha gratidão aos amigos de

longa data Natália Bernardi, Paulo Vedovello (Paulão), Fernando de Almeida (Zoio) e Paola Bello e aos amigos mais novos, mas tão importante quanto, Amanda Oliveira, Thays Guedes, Rivania Teixeira, Carlos Awano, Raphael Malagoli (Araça) e Douglas Morais entre outros. Vocês presenciaram muito de perto toda a jornada desse trabalho, as alegrias e os sofrimentos. Meus agradecimentos por sempre estarem dispostos a me ouvir, me ajudar e me alegrar. Minha vida fora da UNESP tem muito de vocês. Enfim, deixo registrado que minha gratidão se entende a todas as outras pessoas, que de alguma forma ou de outra estiveram presentes em minha vida durante esses anos de mestrado.

“Nunca deixe que lhe digam que não vale a pena
Acreditar no sonho que se tem
Ou que seus planos nunca vão dar certo
Ou que você nunca vai ser alguém
Tem gente que machuca os outros
Tem gente que não sabe amar
Mas eu sei que um dia a gente aprende
Se você quiser alguém em quem confiar
Confie em si mesmo
Quem acredita sempre alcança!
(Mais uma vez - RENATO RUSSO).

ELEMENTAR, MEU CARO WATSON!

(Conan Doyle)

R3SUM0

Esta pesquisa tem por objetivo compreender em que atividades envolvendo problemas de Criptografia podem auxiliar os alunos na exploração das ideias associadas à função afim. As atividades propostas aos estudantes foram estruturadas na forma de enigmas envolvendo contos baseados no personagem Sherlock Holmes, de Sir Arthur Conan Doyle. As atividades foram desenvolvidas com um grupo de alunos do primeiro ano do Ensino Médio da escola pública E. E. Prof. Mycroft, localizada na cidade de Rio Claro/SP. Este trabalho está fundamentado na Metodologia de Pesquisa Intervenção com enfoque Qualitativo. A metodologia de análise dos dados se aproxima de estudos sócio-culturais conjuntamente com estudos cognitivos permeados por meio da resolução de problemas e investigações matemáticas. Como aporte teórico, a dissertação apresenta uma discussão e reflexão acerca do envolvimento da matemática em relação aos campos de poderes (social, politico, econômico, territorial, entre outros) sempre elencando esse entrelaçamento com a constante evolução da criptografia e sua busca constante de cifras seguras e poderosas. Os dados da pesquisa foram produzidos a partir de observações e anotações em um diário de campo, realizadas pela pesquisadora, filmagens e gravações de áudio dos encontros, entrevistas semiestruturadas e fichas de perguntas das atividades. Como conclusões, observou-se que os alunos desenvolveram atitudes autônomas durante seus processos de aprendizagem, fomentando posturas investigativas. Tais atitudes contribuíram na criação e experimentação de diferentes estratégias de resolução o que refletiu nas explorações e investigações realizadas por eles a respeito das ideias associadas ao conceito de função afim.

Palavras-chave: Educação Matemática. Ensino Médio. Criptografia. Cifras. Criptoanálise.

ABSTRACT

This research aims to understand how activities involving encryption problems can assist students to explore the ideias associated with affine functions. The activities proposed to the students were structured in the form of enigmas involving tales based on the character Sherlock Holmes, by Sir Arthur Conan Doyle. The activities were developed with a group of students in the first year of high school of the public school E. E. Prof. Mycroft, located in Rio Claro/SP. This work is based on Intervention Research Methodology with Qualitative approach. .Data analysis methodology approaches socio-cultural studies in conjunction with cognitive studies influenced by problem solving and mathematical investigations. As a theoretical framework, the dissertation presents a discussion and reflection about the involvement of mathematics in relation to the powers of fields (social, political, economic, territorial, etc.) always listing this entanglement with the constant evolution of cryptography and its constant search of safe and powerful figures. The research data were produced through observation and by notes in a field diary, carried out by the researcher, in addition to semi-structures interviews and questions cards activities. In conclusion, it was observed that the students developed autonomous attitudes during their learning processes, encouraging investigative positions. Such attitudes have contributed in the creation and experimentation of different resolution strategies, which have reflected on the explorations and investigations that they did about the ideas associated with the concept of affine function.

Keywords: Mathematics Education. High school. Encryption. Cipher. Cryptanalysis.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE TABELAS

SÚMARIO

“- Ainda não temos dados – ele respondeu. – É um erro capital teorizar antes de conhecer todas as evidências. Distorce o raciocínio”.

(Sherlock Holmes)

1 CONHECENDO O CASO

Este capítulo inicial relata o caminho percorrido até a elaboração desta pesquisa de mestrado. Desse modo, discorro acerca da minha formação acadêmica e de como surgiu o interesse pelo fenômeno em estudo, destacando o processo de amadurecimento da pergunta diretriz. Em seguida será apresentado o objetivo da pesquisa, juntamente com sua relevância, e, por fim, a estrutura da dissertação. Assim, o leitor terá uma visão geral do que foi constituído, bem como o modo como isso ocorreu.

1.1 A p3squisadora e a P3rgunta D1retr1z

No ano de 2012, finalizei o curso de Licenciatura em Matemática na Universidade Estadual Paulista (UNESP) "Júlio de Mesquita Filho", *Campus* Rio Claro. Durante minha graduação, entre os anos de 2010 e 2012, fui bolsista do Programa de Educação Tutorial (PET). O vínculo com o PET proporcionou o desenvolvimento de iniciações científicas (IC), já que estas faziam parte das obrigações estabelecidas pelo programa, além da participação em projetos de ensino, pesquisa e extensão, visando à melhoria do ensino e formação acadêmica dos alunos da graduação.

Tendo em vista os mais variados caminhos que se apresentam a um aluno de graduação, procurei diversificar ao máximo minha formação, a fim de conhecer algumas áreas de atuação de um estudante de Matemática. Desse modo, a cada ano, durante a IC, abordei uma área diferente da Matemática.

Em meu primeiro projeto de IC (2010), intitulado *Estudo de Modelos Matemáticos através de Equações Diferenciais Ordinárias*, fui inserida no meio científico, tendo a oportunidade de experimentar um estudo na área de Equações Diferenciais Ordinárias (EDO). No ano seguinte, desenvolvi o projeto intitulado *Estatística Aplicada a Dados da Área da Saúde*. Foi nesse mesmo período, cursando as disciplinas de Didática, Filosofia da Educação: Questões da Educação Matemática e Prática de Ensino e Estágio Supervisionado I, que entrei em contato com textos pertinentes à Educação e à Educação Matemática, e o encantamento por essa área surgiu.

Em meu terceiro projeto de IC e último ano de graduação, resolvi estudar detalhadamente um livro de "causos" matemáticos do autor Ian Stewart (2008), cujo nome é *Jogos, Conjuntos e Matemática*. Para realizar tal estudo, entrei em contato com o Professor Dr. Henrique Lazari, meu docente na graduação, e apresentei a ideia de estudar o livro e aprofundar a

Matemática encontrada em cada "causo". O mesmo deu seu aval e, por estar familiarizado com a obra de Stewart, me orientou nas teorias matemáticas apresentadas pelo autor.

Esse livro contém várias histórias que se desenrolam em torno de algum conceito matemático, mas havia uma em especial: a história do "Pôquer por telefone", a qual utilizava a ideia de cifrar as cartas do baralho, que despertou meu interesse por criptografia. Meu fascínio foi observado pelo professor Henrique, que sugeriu um livro chamado *O livro dos Códigos*, do autor Simon Singh (2008). Após desfrutar a leitura da obra e conhecendo um pouco mais sobre o desenvolvimento da criptografia, é que o docente direcionou a minha IC para os estudos da criptografia RSA[1]. Para entender melhor a Matemática envolvida por trás dessa criptografia, me foi indicado um estudo detalhado do artigo *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* (1978), dos autores R. L. Rivest, A. Shamir e L. Adleman.

O crescente interesse durante a IC em relação à criptografia ocorria simultaneamente com o interesse em relação à Educação Matemática, resultado da disciplina Prática de Ensino e Estagio Supervisionado II. Essa área se mostrava cada vez mais atrativa e condizente com minhas características e anseios pessoais. Com o estágio obrigatório da disciplina, o convívio na escola e o desenvolvimento de atividades elaboradas na disciplina com os alunos me fizeram perceber que estudar nessa área me realizava, assim como a criptografia.

A vontade de começar a pesquisar ambas me fez querer associá-las e, neste contexto, surgiu a aspiração de trabalhar a criptografia dentro da Educação Matemática. A possibilidade de uni-las gerou grandes reflexões sobre como o processo evoluiria. Para o amadurecimento da ideia a ponto de desenvolver um projeto de mestrado, em 2013, participei como aluna especial do Programa de Pós-Graduação em Educação Matemática (PPGEM), oferecido pela UNESP, *Campus* de Rio Claro.

Para dar início a esse estudo, uma busca na Internet sobre o tema foi realizada. No que diz respeito à criptografia, encontram-se disponíveis na literatura diversos textos sobre sua história, a formulação matemática, bem como suas aplicações, como em transferências bancárias, aplicações eletrônicas, compras e vendas *on-line*, entre outras. No entanto, em uma primeira pesquisa vinculando os temas Criptografia e Educação Matemática, notou-se que não há muitos trabalhos publicados acerca desse entrelaçamento.

Em uma pesquisa realizada na Internet, em 2013, utilizando-se algumas palavras-chave, como "Criptografia e Ensino", "Códigos e Ensino", "Criptografia e Educação Matemática",

[1] As siglas R,S e A significam a inicial dos nomes de seus criadores, a saber, Rivest, Shamir e Adleman.

entre outras, foram encontrados 25 trabalhos que relacionavam esses dois temas. Dentre tais trabalhos, destacam-se os artigos "Codificando e Decifrando Mensagens" (TAMAROZZI, 2001), "Currículo de Matemática no Ensino Médio: atividades didáticas com o tema Criptografia" (GROENWALD; OLGIN, 2011b), "Códigos e senhas no Ensino Básico" (GROENWALD; FRANKE; OLGIN, 2009) e "Criptografia e o Currículo de Matemática no Ensino Médio" (GROENWALD; OLGIN, 2011a), um trabalho de conclusão de curso intitulado "Criptografia como agente motivador na aprendizagem da Matemática em sala de aula" (FINCATTI, 2010) e uma dissertação intitulada "Currículo no Ensino Médio: uma experiência com o tema Criptografia" (OLGIN, 2011).

Tais trabalhos destacam-se por apresentar um material didático em que a criptografia é vinculada a alguns conteúdos matemáticos, como função afim, função quadrática, função exponencial, matrizes, entre outros. Eles argumentam que esse material didático pode contribuir para exercitar, fixar, aprofundar e revisar alguns conteúdos matemáticos, além de permitir o desenvolvimento de estratégias de resolução de problemas e trabalhos em grupo. Eles também levantam considerações sobre o quanto entrelaçar a criptografia a alguns conteúdos matemáticos pode ser interessante dentro da sala de aula, no sentido de que problemas envolvendo a criptografia podem motivar e instigar os alunos a estudar Matemática. De modo geral, esses trabalhos concluem que esse tema ajuda a complementar e reforçar alguns conceitos matemáticos e que podem e devem ser inseridos no currículo de Matemática do Ensino Médio. No capítulo 2, o leitor encontrará mais detalhes sobre essas obras e outras que foram desenvolvidas durante os anos de 2013 e 2014.

A leitura e análise desses trabalhos permitiu uma reflexão acerca da importância desse tema no currículo de Matemática e do material didático apresentado por seus autores. Ponderando sobre o material já existente, surgiram as seguintes questões: Será que é possível explorar um conteúdo matemático com os alunos por meio de problemas criptográficos? De que maneira podemos apresentar uma sequência pedagógica de atividades criptográficas de forma a estimular, motivar os alunos e prender sua atenção para resolver os problemas propostos e consequentemente trabalhar o conteúdo matemático escolhido?

Pensando nesses questionamentos iniciais e nos trabalhos já produzidos é que surge então a primeira versão da pergunta diretriz, a saber: *"Quais as potencialidades[2] da Criptografia na aprendizagem de conceitos matemáticos por meio de resolução de problemas?"*. Com esta pergunta, surge o questionamento sobre qual conceito matemático esta pesquisa iria abordar.

[2] Potencialidades esta sendo entendido nesse trabalho como um termo que nos permite refletir sobre as potências das atividades, assim como suas possíveis limitações.

Para tanto, considerou-se trabalhar com funções. A ideia era abordar os conceitos de Domínio, Contradomínio e Imagem das funções, podendo estas ser polinomiais de primeiro e segundo grau, exponenciais ou logarítmicas. Assim sendo, houve uma reformulação da pergunta diretriz, a qual ganhou o seguinte corpo: *"Como os alunos relacionam conceitos matemáticos sobre funções por meio de atividades de caráter criptográfico?"*.

Essa nova pergunta gerou grandes inquietações. O fato de que as atividades poderiam abordar diferentes tipos de funções e a dificuldade em criar tais atividades que se relacionassem provocaram um grande incômodo. Havia a necessidade de restringir ainda mais o conceito que eu trabalharia nas atividades. Ademais, depois de algumas discussões e reflexões, foi observado que tal pergunta não contemplava os meus questionamentos iniciais. Portanto, retornei aos trabalhos de Groenwald e Olgin (2011a), Olgin (2011) e Fincatti (2010), sendo feito um novo processo de reflexão acerca de qual conteúdo seria escolhido para ser trabalhado nesta pesquisa. Após longas discussões com o Prof. Henrique Lazari[3], decidiu-se, naquele momento, que restringiríamos o conceito de função para a função afim, a qual permitiria uma maior flexibilidade para criar atividades criptográficas. Esta flexibilidade é designada pelo fato de que a função afim tem como característica ser bijetora, o que para a criptografia é de extrema importância. Deste modo, não abordaríamos os problemas de restrições do domínio da função, podendo manipular a função afim de maneira segura e coerente no campo da criptografia e por ser a função mais primitiva do campo das funções.

Com essas novas decisões, e levando em consideração os questionamentos iniciais, a pergunta diretriz sofreu mais uma modificação e foi reformulada para: *"Quais as potencialidades de uma sequência didática de atividades envolvendo problemas criptográficos na construção do conteúdo de função afim?"*.

Esse questionamento acompanhou-me até o início de 2015. A sequência de atividades foi criada com base no mesmo, e uma análise inicial dos dados também foi desenvolvida na tentativa de respondê-la. Entretanto, no mês de abril de 2015, realizei a apresentação obrigatória da pesquisa para os alunos e professores do Programa no qual estou inserida e, com isso, surgiram algumas contribuições referentes à atual pergunta diretriz. Após as discussões e reflexões acerca das sugestões feitas durante a apresentação e procurando sempre melhorias para a pesquisa, a questão diretriz sofre mais uma modificação, tomando um novo corpo, a saber: *"Quais as potencialidades de atividades pedagógicas envolvendo problemas criptográficos na exploração das ideias associadas à função afim?"*. Desde então, tal

[3] Nesse momento do trabalho o Prof. Henrique Lazari era o orientador da pesquisadora. O processo de mudança de orientador ocorreu por volta de setembro de 2015.

indagação vem me acompanhando durante todo o processo de categorização, análise dos dados, bem como na elaboração da dissertação.

1.2 0bjetiv0

Esta pesquisa tem como objetivo compreender em que atividades pedagógicas envolvendo problemas de criptografia pode auxiliar os alunos na exploração das ideias associadas à função afim.

1.3 R3levânc1a

A busca de alternativas metodológicas diversificadas para o ensino da Matemática, de acordo com os Parâmetros Curriculares Nacionais para o Ensino Médio (PCNEM) (BRASIL, 2000), é o grande desafio do professor. Segundo os PCNEM (BRASIL, 2000), o professor é:

> Quem seleciona conteúdos instrucionais compatíveis com os objetivos definidos no projeto pedagógico; problematiza tais conteúdos, promove e media o diálogo educativo; favorece o surgimento de condições para que os alunos assumam o centro da atividade educativa, tornando-se agentes do aprendizado; articula abstrato e concreto, assim como teoria e prática; cuida da contínua adequação da linguagem, com a crescente capacidade do aluno, evitando a fala e os símbolos incompreensíveis, assim como as repetições desnecessárias e desmotivantes (BRASIL, 2000, p. 51).

Além de ter como desafio levar em conta os conhecimentos prévios dos alunos no processo pedagógico (BRASIL, 2000).

Com relação a esses conhecimentos prévios, a Base Nacional Comum Curricular[4] (BNCC) (BRASIL, 2015) ressalta a importância de se valorizar o conhecimento trazido pelo aluno adquirido de suas ações sociais do dia a dia. De acordo com a BNCC, (BRASIL, 2015) não se pode assumir que os estudantes cheguem à escola vazios de qualquer conhecimento. Adverso a isso, a BNCC (BRASIL, 2015) argumenta que:

> Todo/a estudante carrega consigo uma diversidade de conhecimentos matemáticos que podem e devem servir de ponto de partida para novas aprendizagens. É muito importante, em sala de aula, provocar o/a estudante para que ele/ela explicite esses conhecimentos, os quais devem ser, permanentemente, associados aos conhecimentos escolares trabalhado (BRASIL, 2015, p. 116–117).

[4] A BNCC é um documento, em versão inicial, que foi apresentado à sociedade em escala nacional, no ano de 2015, para que esta possa intervir debatendo, ampliando e modificando tal documento antes deste ser oficializado como Base Nacional Comum Curricular.

Além de se dar a devida importância aos conhecimentos prévios dos alunos, os PCNEM (BRASIL, 2000) ainda afirmam que existe a necessidade de se adotarem métodos de aprendizagem ativos e interativos e que o processo pelo qual os alunos alcançam o aprendizado é complexo, no qual o professor e a escola exercem um papel fundamental.

> O professor e a escola contribuem permitindo ao aluno se comunicar, situar-se em seu grupo, debater sua compreensão, aprender a respeitar e a fazer-se respeitar; dando ao aluno oportunidade de construir modelos explicativos, linhas de argumentação e instrumentos de verificação de contradições; criando situações em que o aluno é instigado ou desafiado a participar e questionar; valorizando as atividades coletivas que propiciem a discussão e a elaboração conjunta de ideias e de práticas; desenvolvendo atividades lúdicas, nos quais o aluno deve se sentir desafiado pelo jogo do conhecimento e não somente pelos outros participantes (BRASIL, 2000, p. 52).

Além de corroborar os PCNEM (BRASIL, 2000), a BNCC (BRASIL, 2015) ainda alega que a escola necessita "propor situações em que o/a estudante perceba a necessidade e a importância de estabelecer relações entre conteúdos, de elaborar e de comprovar hipóteses, de fazer generalizações e de lidar com a ideia de incerteza, características do pensamento científico" (BRASIL, 2015, p. 141).

Assim, como argumentado pelos PCNEM (BRASIL, 2000) e pela BNCC (BRASIL, 2015), a contribuição do professor e da escola no processo de formação matemática dos alunos pode ser dada, por exemplo, a partir do uso de atividades estimulantes e desafiadoras, além da criação de situações envolventes, nas quais os alunos se sintam motivados a realizá-las. Aulas que promovam o desenvolvimento da curiosidade, da imaginação, do processo de investigação, contextualizados, sempre que possível, de acordo com a BNCC (BRASIL, 2015), contribuem para a formação das visões da matemática, da sociedade e do mundo. Além disso, de acordo com esse documento,

> para que o/a estudante tenha sucesso em Matemática, é preciso que ele/a atribua sentido para os conceitos aprendidos na escola. Esse processo demanda, muitas vezes, o recurso à contextualização dos problemas apresentados a ele/a [...] É preciso que sua situação apresentada demande que o/a estudante elabore hipótese de resolução, teste a validade dessas hipóteses, modifique-as, se for o caso, e assim por diante. Trata-se, portanto, de desenvolver um tipo de raciocínio próprio da atividade matemática, permitindo compreender como os conceitos se relacionam entre si (BRASIL, 2015, p. 117).

Desse modo, um ambiente com as características acima depende, em parte, do professor, e é nesse contexto que buscamos a criptografia como tema um aliado para a criação de tal ambiente. Um espaço constituído por alunos, professor e escola, onde estes estejam desenvolvendo atividades envolvendo problemas de criptografia relacionados à Matemática, será chamado de ambiente criptográfico, que, *a priori*, definimos como sendo o conjunto dos meios materiais e intelectuais que permitam a atividade de cifração e decifração de mensagens, com objetivos de exploração dos conceitos matemáticos abordados.

Um ambiente criptográfico pode ser criado por meio de atividades com cenários enigmáticos e criptografados para despertar a curiosidade dos alunos, podendo motivá-los e desafiá-los. Atividades contextualizadas dentro de tal ambiente podem, por exemplo, contribuir para desenvolver e aprimorar a capacidade de concentração e a persistência dos alunos, estimulando seu gosto pela Matemática e colaborando para o desenvolvimento da habilidade de pensar em estratégias para a resolução das atividades (FIARRESGA, 2010). Desse modo, a combinação de atividades envolvendo alguns conteúdos matemáticos com a criptografia pode vir a se constituir em um "material útil para exercícios, como também para atividade e jogos de codificação. [Podendo] o professor dispor deles para a fixação de conteúdos matemáticos" (TAMAROZZI, 2001, p. 41).

Ao abordar o tema Criptografia em sala de aula, se torna oportuno apresentar, discutir e questionar sobre a presença desse assunto no mundo (transações bancárias, compras e vendas *on-line*, senhas de *e-mail*, *facebook*, entre outros procedimentos). Por fazer parte do cotidiano da sociedade e de permitir a exploração de vários assuntos incluindo conteúdos relacionados à Matemática, a criptografia pode ser uma ferramenta que possibilita ao professor desenvolver atividades mais instigantes e desafiadoras, sem perder o foco no conteúdo que deseja abordar, além de poder levar em consideração os conhecimentos prévios dos alunos e propiciar a autonomia dos mesmos no próprio processo de aprendizagem.

Assim, pode-se observar que atividades envolvendo problemas de criptografia e as construções de um ambiente criptográfico enquadram-se nas características citadas pelos PCNEM (BRASIL, 2000) e pela BNCC (BRASIL, 2015) sobre o ambiente desenvolvido pelo professor.

Dessa forma, tendo como diferencial de outras pesquisas, este trabalho tem como objetivo compreender em que atividades pedagógicas envolvendo problemas de criptografia pode auxiliar os alunos na exploração das ideias associadas à função afim.

Outro fator relevante para esta pesquisa é a falta de trabalhos que ligam a Criptografia e a Educação Matemática, além da escassez de atividades prontas envolvendo essas duas áreas.

Como já citado na seção 1.1, existe uma carência de trabalhos na literatura que aborda essas duas áreas de conhecimento. Assim, ao vincular a criptografia e a Educação Matemática, espera-se propiciar atividades instigantes envolvendo o conteúdo matemático de função afim do Ensino Médio e ainda contribuir não apenas para uma bibliografia que discorra sobre estes temas, mas também para a ampliação dessas duas áreas, a partir de seu entrelaçamento.

1.4 E5trutur4 da Disserta4ção

Este trabalho está dividido em cinco capítulos. Este primeiro apresenta um breve resumo sobre minha trajetória acadêmica, bem como os caminhos trilhados para se chegar a tal pesquisa. A pergunta diretriz e todo o seu movimento de aperfeiçoamento também são apresentados, assim como o objetivo e a relevância de tal pesquisa.

O segundo capítulo objetiva apresentar uma discussão acerca do empoderamento da matemática. Trazendo autores que abordam esse assunto, pretendeu-se levantar reflexões sobre o entrelaçamento entre o poder e a matemática, além de trazer para essa discussão as ideias desse vínculo no campo da criptografa e sua repercussão na história e nos dias de hoje.

O terceiro capítulo é constituído pelo referencial teórico metodológico adotado neste trabalho, assim como suas características. Em seguida são apresentadas considerações a respeito do aprendizado do aluno na concepção construtivista e sobre a resolução de problemas e suas investigações. Dando continuidade ao capítulo, uma revisão de literatura elencando trabalhos que envolvam a criptografia e a Educação Matemática é realizada. Inicialmente, discorro brevemente sobre os trabalhos apresentados, trazendo um panorama geral das produções realizadas acerca dessas duas temáticas. Em seguida, trago algumas atividades encontradas nesses trabalhos que abordam o conceito de função afim. Posteriormente, apresento os participantes da pesquisa e sua escola. Logo após, apresento uma descrição detalhada do processo de criação das atividades, assim como os procedimentos metodológicos adotados nesta pesquisa e, finalmente, concluo o capítulo apresentando uma exposição sobre como se deu a organização dos dados.

O quarto capítulo apresenta alguns episódios que foram considerados relevantes na busca de possíveis respostas para a pergunta diretriz. O capítulo está dividido em três itens. Cada um deles representa uma categoria. Os itens elencados são: atitudes investigativas, procedimentos e, por fim, conceitos. Juntamente com a apresentação desses episódios separados em cada categoria, uma análise é realizada com base em todo o referencial teórico apresentado no capítulo 2 e em minha visão de pesquisadora.

O quinto e último capítulo aborda uma síntese da pesquisa e apresenta reflexões sobre os resultados obtidos da mesma. Na sequência, discorro sobre o envolvimento que ocorreu entre a pesquisadora, a escola e os alunos e seus professores. Em seguida, elenco algumas dificuldades que emergiram durante o trabalho de campo. Finalizando o capítulo, e concluindo a pesquisa, aponto alguns questionamentos para futuras investigações.

“Você sabe que um mágico perde o encanto se explica seus truques. E, se eu lhe revelar muita coisa do meu método, você acabará pensando que o que eu faço não tem nada de mais.

- Nunca vou pensar isso – respondi. Você elevou a investigação ao nível de ciência exata, de uma forma insuperável”.

(Sherlock Holmes)

2 CONTRUÍNDO INFORMAÇÕES

2.1 P0der, matemática e cr1ptografia

A história da escrita secreta teve início há muito tempo atrás, quando a necessidade de comunicações eficientes e sigilosas se tornaram essenciais na administração de países e de exércitos. Garantir que mensagens transitassem de forma segura e eficiente era uma das mais importantes preocupações. O receio de que mensagens fossem interceptadas e seu conteúdo revelado motivou o desenvolvimento de métodos e processos para ocultar uma mensagem, de modo que somente o destinatário pudesse ler seu conteúdo. É nesse cenário que surgem os códigos e as cifras[5].

O interesse em manter a confidencialidade de mensagens levou nações a criarem departamentos para a produção de códigos e cifras cada vez mais fortes. Em contrapartida, surgiram os quebradores de códigos, conhecidos como decifradores, que se empenhavam em desvendar os segredos ocultados. De acordo com Singh (2008, p. 11), "A história dos códigos e de suas chaves é a história de uma batalha secular entre os criadores de códigos e os decifradores, uma corrida armamentista intelectual que teve um forte impacto no curso da história humana".

As notáveis descobertas científicas acerca da arte da comunicação secreta, também conhecida como criptografia, deram-se na contínua batalha entre os criadores e os decifradores de códigos. Os cifradores, em busca de cifras cada vez mais seguras, e os decifradores, em constante trabalho de quebra, marcaram a história, sendo eles personagens importantes na narrativa de guerras e nos resultados de batalha.

Singh (2008) afirma que, atualmente, os matemáticos são os responsáveis por essa batalha. Segundo esse autor,

> Já se falou que a Primeira Guerra Mundial foi a guerra dos químicos, devido ao emprego, pela primeira vez, do gás de mostarda e do cloro, e que a Segunda Guerra Mundial foi a guerra dos físicos devida à bomba atômica. De modo semelhante se fala que uma Terceira Guerra Mundial seria a guerra dos matemáticos, porque os matemáticos terão o controle sobre a próxima grande arma de guerra, a informação. Os matemáticos têm sido responsáveis pelo desenvolvimento dos códigos usados atualmente para a proteção das informações militares. E não nos surpreende que os matemáticos estejam também na linha de frente da batalha para tentar decifrar esses códigos (SINGH, 2008, p. 13).

[5] Um *código* é definido como uma substituição de palavras ou frases, enquanto que a *cifra* é definida como uma substituição de letras.

Assim, ao estudar a evolução da criptografia e compreender como seu desenvolvimento esteve atrelado à história, é possível perceber como o poder (social, político, econômico, cientifico, etc.) e a matemática se entrelaçam.

No entanto, mesmo percebendo toda a relação entre a matemática e as relações de poder, Portanova (2006, p. 437) diz que "a matemática era vista como uma ciência neutra, sem influências 'externas' e como uma progressão de ideias, buscando cada vez mais a abstração". Em relação a essa imparcialidade, Upinsky (1989) chama a atenção ao quanto a neutralidade da matemática pode ser enganadora. Segundo ele, ela está implicitamente presente em vários setores da sociedade, mascarada nos mais diversos ramos. O autor classifica a matemática como uma entidade perversa, malvada e despótica que, muitas vezes, se apresenta disfarçadamente de maneira respeitável e neutra.

> É um travesti quando se tem Razão na filosofia, Igualdade na justiça, Democracia na política, Moeda na economia, Massa na propaganda e na guerra, Cálculo no amor, com don Juan, Razão de Estado no governo, com Maquiavel... (UPINSKY, 1989, p. 4).

Nesse sentido, observa-se que a matemática se esconde nas mais diversas ramificações da sociedade e sua manipulação, a princípio, sempre é regida pelo interesse de poucos. Napoleão (1981, *apud* UPINSKY, 1989, p. 30) argumenta que "'os pretextos jamais faltam para os que têm o poder de fazer o que lhes agrada' e 'tomando como pretexto o suposto princípio de utilidade geral, chega-se até onde se quer'".

Destarte, percebe-se como os números têm o poder de reger o mundo, tendo na matemática os algarismos que "dançam" no sistema do poder (UPINSKY, 1989). Mas, afinal, se os números regem o mundo, como queria Galileu, qualquer coisa que existe, por sua vez, deve ter um número. Nessa direção, Upinsky (1989) menciona que, como resultado desse princípio – os números governam o mundo –, "não somente todas as coisas possuem número, como ainda, diziam [os pitagóricos], 'todas as coisas são números'" (UPINSKY, 1989, p. 73). Com esse mesmo pensamento, o autor traz Roger Bacon (1214-1294), para argumentar a respeito da soberania da matemática sobre todas as coisas. De acordo com ele,

> Roger Bacon, [repetia] sempre que: 'todas as causas dos fenômenos naturais podem ser representados por linhas, ângulos e figuras' [onde proclamou que] 'a matemática tem experiências universais que se aplicam a todas as ciências e nenhuma ciência pode ser compreendida sem a matemática' (UPINSKY, 1989, p. 121).

Com essa postura, entende-se como a matemática, sendo olhada na perspectiva de poder, passa a ser o maestro das ciências, assumindo grande importância em várias atividades cotidianas do homem. Associando esse poder à criptografia observa – se que sua evolução é marcada pela busca de cifras poderosas, em que a matemática entra em sua história trazendo as funções e a teoria dos números como sendo excelentes ferramentas de cifrações seguras. Dispor da matemática para desenvolver cifras protegidas é dispor de um poder de sigilo, o que em muitos casos, como por exemplo, das Guerras Mundiais, é dominar situações e até mesmo influenciar o curso da história (SINGH, 2008).

Nessa acepção, considerando o poder dos números sobre os homens, Upinsky (1989, p. 111) traduz uma das "máximas preferidas de Napoleão: 'Os homens são como algarismos, só tem valor pela sua posição'". Como exemplo, baseando-se em uma análise aritmética de posição, suponha-se o número um. Sozinho tal número vale apenas um, porém, de acordo com o nosso sistema decimal (uma aritmética de posição), colocando-o à esquerda de um zero, que tem seu valor nulo, este passa a valer dez vezes mais do que inicialmente. Colocando o mesmo número um à esquerda de dois zeros, ele agora passará a valer cem vezes mais que no início, e assim sucessivamente. Desse modo observa-se que, dependendo de sua posição, um algarismo qualquer pode assumir valores relativamente grandes. Neste pensar, Upinsky (1989) contextualiza essa ideia para o poder de batalha, dizendo que:

> O general que é "1" à frente de sua tropa terá seu valor decuplicado. Assim, o homem assentado em sua poltrona não terá o mesmo peso se ele se instalar numa poltrona de ministro. 'Tornar-se o homem de seu uniforme' (Napoleão). A posição ou o bom lugar é tudo! (UPINSKY, 1989, p. 111–112).

Frente a tudo isso, é fato que o pensamento matemático e principalmente a sua manipulação vêm intervindo no curso da história. A partir disso, a supremacia consiste em entender a lógica do sistema e compreender suas regras a ponto de interpretá-las e utilizá-las a seu favor, como, por exemplo, inventar um tipo de flecha para atingir um inimigo que só é perigoso de perto (UPINSKY, 1989).

Assimilar essa lógica é ter consciência de que quem vence é aquele que ascende mais rápido e é também entender que esse confronto apenas gera um aumento maior na organização do poder. Por exemplo, os resultados das guerras nada mais são do que o reflexo do constante reforço de armamentos e técnicas de combate, incluindo o poder de sigilo das informações (UPINSKY, 1989; SINGH, 2008). É a partir dessa ideia que a criptografia e a criptoanálise se chocam e evoluem constantemente, pois da mesma maneira é preciso reforçar

e criar novas técnicas de cifragem e de decifragem. Assim, a partir dessa concepção, o confronto altera o equilíbrio do poder, gerando seu aumento.

O elo entre a ‘arte da guerra’ e a matemática é antigo. Desde muito tempo, a matemática começou a figurar como sendo um elemento importante e útil para as mecânicas da guerra, um conhecimento prático exigido no ramo da arte militar. É na necessidade prática (o das construções militares e da artilharia) que a matemática alterou totalmente os significados das defesas e dos ataques nas guerras (VALENTE, 1999). Como afirma Valente (1999), no século XIV surgem as primeiras armas de fogo que foram utilizadas nas guerras. Tais armas entraram em rápida evolução e aperfeiçoamento e isso influenciou, consideravelmente, os poderes de defesa e ataque. Por exemplo, após a transformação significativa dos canhões de uso, as novas questões e problemas sobre as defesas surgiram. De acordo com o autor,

> Os muros das fortalezas medievais já não mais resistem às investidas das bolas dos canhões. Mais do que nunca, a “arte de bem fortificar” torna-se um negócio de estado. Multiplicam-se os livros sobre fortificação, os engenheiros transformam-se em grandes personagens e figuras fundamentais de poder (VALENTE, 1999, p. 41–42).

Nesse contexto, então, tem-se que áreas da matemática, como aritmética e geometria, acabaram virando garantias de segurança, as quais são “utilizadas como instrumental de persuasão pela sua inefabilidade e pelas novas luzes e fecundidade que a demonstração possibilita” (VÉRIN, 1993 *apud* VALENTE, 1999, p. 42). Nesse sentido, é considerando o saber da geometria que a prática dos engenheiros é elevada e acaba configurando-se em papéis fundamentais para os combatentes. Portanto, coube à geometria tornar-se a sustentação dos tratados e escritos militares (VALENTE, 1999). Assim, pode-se observar que o engenheiro, inicialmente, era voltado às engenharias militares, sendo este um oficial e um “matemático” (VÉRIN, 1993 *apud* VALENTE, 1999, p. 41).

Deste modo, com as alterações e aperfeiçoamentos das ferramentas de guerra, é que se deu a necessidade de criação de novas arquiteturas de fortificações. De acordo com Magalhães (1948 *apud* VALENTE, 1999, p. 40), “ambos: a evolução da artilharia e o consequente nascimento de novas formas construtivas, criam a necessidade da existência de uma mão-de-obra especializada. É assim que nascem, por toda a parte, as *Aulas de Artilharia e Fortificação*”.

Para compreender essa “expansão” da matemática como instrumento de guerra, olhemos, por exemplo, para o seu surgimento e desenvolvimento no Brasil. Enquanto colônia, inicialmente, o país tinha preocupações com sua própria formação, alargamento e

estabilização com a produção da riqueza demográfica e material. Os homens que na época eram chamados de matemáticos vieram para o Brasil em missões e trabalhos de cartografia, astronomia e engenharia (LEITE, 1945 *apud* VALENTE, 1999, p. 34). Quanto à matemática escolar, suas origens encontram-se enraizadas no final do século XVII, quando, por meio da *Aula da Esfera*[6] do Colégio de Santo Antão, os alunos aprendiam introdução de conteúdos de geometria e aritmética. Posteriormente, atendendo a uma determinação real de D. João IV, o colégio iniciou na *Aula* uma espécie de preparatório para os alunos, cujo destino era cursar as *Aulas de Artilharia e Fortificação*, nas quais a geometria prática, a dos engenheiros, era tida como matéria fundamental (VALENTE, 1999).

Fundada em 1647, em Portugal, por D. João IV, a *Aula de Fortificação e Arquitetura Militar* tinha como importante tarefa reorganizar sua força militar. Naquela época, "era urgente tomar ciência dos avanços realizados na *arte da guerra*. O expediente era contratar *experts* internacionais sobre o assunto. Tal prática era comum entre os países cujo intento era o aperfeiçoamento de seus exércitos" (VALENTE, 1999, p. 43). Assim, depois de Portugal, em 1648, foi realizada a "contratação pela Corte Portuguesa de estrangeiros, especialistas em cursos militares, para virem ao Brasil ensinar e formar pessoal capacitado para trabalhos com fortificações militares"(LYRA TAVARES, 1965, *apud* VALENTE, 1999, p. 43) .

A partir do século XVIII, o Brasil se encontrava na grande corrida pelo ouro, a qual acabou movimentando uma exploração inicial desordenada, influenciando a Coroa a tomar "sucessivas providências para arrecadar sempre o máximo possível, [assim] fiscos e militares assumiam o comando da organização, fundação de vilas e construção da vida civil em regiões surgidas pela mineração" (VALENTE, 1999, p. 43). Nesse contexto, com o aumento das riquezas exploradas, as ameaças ao território também aumentavam, o que, por sua vez, ampliava a necessidade de se defender. Isso foi determinante na criação da escola de *Fortificação e Arquitetura Militar*, que, mais tarde, cindiu em dois ramos, a saber, o ensino militar e o ensino familiar (VALENTE, 1999).

De acordo com Valente (1999), a Aula do Terço de Artilharia do Rio de Janeiro representou o momento inicial da formação de uma classe importante na sociedade colonial. Por meio de um curso, que se tornou a base da escolaridade militar, os filhos de militares e dos nobres já podiam buscar a carreira bélica na *Aula de Artilharia e Fortificações do Rio de Janeiro*. Segundo esse autor, o ensino nesse tipo de academia era:

[6] A Aula da Esfera era inicialmente direcionada ao ensino da marinharia (cartografia, construção de instrumentos náuticos e formação de pilotos do mar). Conforme as transformações ocorridas, ao longo do tempo, tal aula configurou-se em ensinamentos para traçados e construções de fortificação (conhecimentos de geometria envolvendo proporções, cálculos de distância, alturas, escala, entre outros). Para mais informações a esse respeito, ver: Valente (1999, p. 26-29).

> baseado na filosofia racionalista de Descartes, (...) formar engenheiros militares, cartógrafos e matemáticos, capazes de levar a cabo o levantamento de mapas com latitudes determinadas pelos novos métodos empregados na Inglaterra e na França, e habilitar engenheiros a construir fortificações para a defesa dos domínios ultramarinos (VALENTE, 1999, p. 46).

Por essa citação, percebe-se como as escolas militares estavam relacionadas à matemática, não somente pelos seus conhecimentos teóricos, mas também, fortemente, pelos seus conhecimentos práticos, como os da geometria, da matemática dos engenheiros, dentre outros. A partir dessas concepções é que ocorre uma difusão das escolas militares no Brasil, a qual acaba propiciando a disseminação de vários cursos de matemática durante o século XVIII. É neste cenário, no núcleo dos cursos técnico-militares, que se figurou e se constituiu o repertório de conteúdos da matemática escolar secundária presentes nos colégios do século XIX (VALENTE, 1999).

Com esse breve exemplo a respeito da constituição da matemática no Brasil, pode-se perceber como esta esteve atrelada, nos momentos iniciais, às ideias da arte da guerra e da conquista dos poderes (políticos, territoriais, econômicos, entre outros). Assim, perante tudo aqui exposto, pode-se realmente concluir que a matemática e sua evolução teórica estão intrinsicamente ligadas à guerra? Vale relembrar, neste momento, a questão que nos movimenta a pensar sobre tal discussão, sendo esta a corrida armamentista intelectual em que os cifradores e os decifradores atuaram e atuam na busca pelo poder do sigilo (SINGH, 2008). Esta corrida deve-se à matemática e ao poder que ela exerce nos algoritmos de cifração e de decifração. Deste modo, a pergunta realizada acima se torna ainda mais complexa no sentido de que, nos dias de hoje, a informação e seu sigilo são uma das caracterizações mais influentes do poder, seja ele social, político, econômico, cientifico, etc.

Frente a toda essa discussão, percebe-se que a matemática e seus conflitos geradores estão intimamente entrelaçados, sendo tênue a linha que os separa. Sobre isso, D'Ambrosio (2011) argumenta que:

> Passamos o ano 2000 com grandes festividades, fomos ameaçados pelo *bug* do milênio, produto de poderosos vírus construídos com sofisticada matemática computacional, escapamos desse *bug* graças a poderosos antivírus desenvolvidos graças à mesma matemática, passamos pelo ano 2001, que terminou sob o impacto dos ataques terroristas nos Estados Unidos e dos ataques de retaliação no Afeganistão. Todos realizados com precisão matemática. E agora, em 2011, testemunhamos guerra civis locais e envolvimentos internacionais com conseqüências imprevisíveis. Tudo

> baseado na utilização de alta tecnologia, desenvolvida graças ao extraordinário avanço das ciências (D'AMBROSIO, 2011, p. 68).

Como conclusão dessa citação, o autor apresenta a seguinte contradição, a saber, "esses atos abomináveis só podem ser idealizados e executados graças a um elaborado instrumental científico e os que idealizam, planejam e executam esses atos são internacionalmente reconhecidos como cientistas competentes" (D'AMBROSIO, 2011, p. 68). É nesse cenário que D'Ambrosio (2011) levanta questões acerca da possível irresponsabilidade dos cientistas ou de uma passiva ingenuidade e, ainda, lança a pergunta sobre em qual momento a matemática deixa de se relacionar com a guerra e passa a se relacionar com a paz.

Nesse sentido, Upinsky (1989) também argumenta sobre a utilização das tecnologias voltadas para o bem ou para o mal. No entanto, o autor afirma que a tecnologia por si só é neutra e alerta que sustentar a ilusão de que tais tecnologias necessariamente incubem-se à construção de um estado totalitário seria errôneo. Tomemos como exemplo dessas tecnologias na criptografia a máquina Enigma e a máquina chamada *bomba*[7]. Durante a Segunda Guerra Mundial, a máquina Enigma foi considerada, de acordo com Singh (2008) com sendo o sistema de cifragem mais temível da história. Sendo utilizada pelos alemães a máquina garantia a transmissão de mensagens entre os nazistas de forma segura e sigilosa. Entretanto, foi outra máquina, a chamada bomba, desenvolvida por Alan Turing, que conseguiu decifrar de maneira poderosa a Enigma, fragilizando assim, a comunicação entre os alemães. Nesse ponto, percebe-se a neutralidade das tecnologias, sendo a sua utilização o que as caracteriza como sendo para o bem ou para o mal.

Upinsky (1989) ainda ressalta as ideias de transformação da informação. De acordo com ele, essa topologia "distorce, deforma e recompõe constantemente a estrutura e o espaço financeiro, econômico, social, politico e cultural". Dentro desse pensamento, Upinsky (1989) faz a observação de que, com essas modificações do espaço, logo as pessoas estarão cada vez mais ligadas às outras pessoas, outros ambientes, por meios de algarismos, fórmulas, meios de comunicação cada vez mais complexos, interativos e interligados. De acordo com ele,

> Seus recursos, sua posição social, sua felicidade estarão ininterruptamente e desvantajosamente ligados a este fio. É a nova religião: necessidade de uma fé comum, de um calor partilhado, tudo com o caráter quantitativo. Quando os nossos ancestrais mal podiam conceber a coabitação, sob a mesma autoridade, de pessoas que não partilham da mesma fé, nós recorremos ao "sistema de informação" para manter a coerência de tudo...(UPINSKY, 1989, p. 175 - 176).

[7] Para mais informações ver Singh (2008, p. 143 – 211).

Com as ideias apresentadas por D'Ambrosio (2011) acerca da irresponsabilidade ou ingenuidade dos cientistas e com as relações de mutação e ligação do espaço e das pessoas trazidas por Upinsky (1989) é que caminha uma reflexão cuidadosa a respeito dos avanços tecnológicos. De acordo com Hobsbawn (1995), a tecnologia, embasada em avançadas teorias e pesquisas cientificas, dominou o estouro econômico por volta da segunda metade do século XX. Segundo ele,

> o problema dessas tecnologias é que se baseavam em descobertas e teorias tão distantes do mundo cidadão comum, mesmo nos países desenvolvidos mais sofisticados, que só algumas dezenas ou, no máximo, algumas centenas de pessoas no mundo podiam capitar inicialmente que elas tinham implicações básicas (HOBSBAWM, 1995, p. 507).

Em relação a isso, para contextualizar seu pensamento, Hobsbawn (1995) argumenta que a física e a matemática já no século XVII governavam os engenhos e as descobertas químicas e elétricas no fim do século XVIII e início do século XIX já se tornavam essenciais às indústrias e às comunicações. Nesse caminhar, percebe-se o quanto as explorações dos pesquisadores científicos eram importantes e reconhecidas como o *start* imprescindível para o avanço tecnológico. Como conclusão dessa observação, o autor argumenta que "a tecnologia com base na ciência já se achava no âmago do mundo burguês do século XIX, embora as pessoas práticas não soubessem exatamente o que fazer com os triunfos da teoria científica, a não ser, nos casos adequados, transformá-las em ideologias" (HOBSBAWM, 1995, p. 507). Olhando para a história da criptografia, as tecnologias surgem por volta do século XV, com o disco de cifras, inventada por Leon Alberti, mas, somente em 1918é que a mecanização das cifras ganha força com a invenção de Scherbius, a máquina Enigma (SINGH, 2008).

Para exemplificar como esses avanços ocorriam, Hobsbawn (1995) cita duas figuras importantes para a história da humanidade: Otto Hahn e Alan Turing. O primeiro, físico alemão, descobriu a fissão nuclear no início de 1939 e:

> Mesmo alguns cientistas mais ativos no campo, como o grande Niels Bohr (1885-1962), duvidavam que tivesse alguma aplicação prática na paz ou na guerra, pelo menos no futuro previsível. E se os físicos que entendiam seu potencial não tivessem falado a seus generais e políticos, estes sem dúvida teriam continuado na ignorância, a menos que fossem eles próprios físicos com pós-graduação, o que era muito improvável (HOBSBAWM, 1995, p. 507–508).

Já o segundo forneceu um importante trabalho para a história da computação. Turing, que inicialmente trabalhou com a exploração especulativa para lógicas matemáticas, acabou desenvolvendo a base da moderna teoria computacional (HOBSBAWM, 1995; SINGH, 2008). No entanto, como afirma Hobsbawn (1995, p. 508), "a guerra lhe deu, e a outros, a oportunidade de traduzir a teoria nos primórdios de uma prática para a decifração de códigos, mas quando foi publicado ninguém, com exceção de uns poucos matemáticos, sequer leu, quanto mais tomou conhecimentos de seu trabalho".

É nesse limiar que as ciências eram incentivadas, apoiadas e por fim utilizadas. Os investimentos por parte dos governos eram feitos sob a luz de seus próprios interesses, em que o resultado final, na maioria das vezes, eram tecnologias para fins bélicos ou sua utilização para prestígios nacionais (HOBSBAWM, 1995). Com relação a isso, Hobsbawn (1995) assegura que:

> Os governos não estão interessados na verdade última (a não ser da ideologia ou religião), mas na verdade instrumental. No máximo, podiam promover a pesquisa "pura" (isto é, no momento inútil) porque ela poderia um dia produzir alguma coisa útil, ou por motivos de prestigio nacional, em que a busca de prêmios Nobel vinha antes de medalhas olímpicas e ainda continua mais altamente valorizada (HOBSBAWM, 1995, p. 536).

Com base nisso, apesar de esse tipo de investimento cientifico ter resultado em catástrofes, como o ataque a Hiroshima, o século XX ficou marcado como sendo o século do crescimento humano. Isso mostra a maneira pela qual as estruturas de pesquisa e de teoria científica se levantaram (HOBSBAWM, 1995). Assim, com a propagação das tecnologias e das técnicas de comunicação, pode-se observar o desenvolvimento dos aparelhos elétricos. Tais artefatos, como o telégrafo (1842), o telefone (1880), o alto-falante (1902), a telegrafia sem fio (1909), a radiotelefonia, a radiotelegrafia e a radiodifusão (1935), a televisão (1945), o telex e o computador (1950), entre outros, mostraram as grandes descobertas de comunicação nas quais se utilizavam os avanços da ciência para se constituir e se aperfeiçoar durante os tempos.

Nesse sentido, Upinsky (1989) descreve uma citação de Albert Speer (1905-1981), o qual argumenta sobre as relações entre as técnicas de comunicação e a iniciativa do totalitarismo durante a Segunda Guerra Mundial. De acordo com Speer,

> Graças aos meios técnicos como os do rádio e dos alto-falantes, oitenta milhões de homens se tornaram escravos da vontade de um só individuo; [e concluindo que] o telefone, o telex e o rádio permitiram às mais altas

> instâncias transmitirem, imediatamente, suas ordens aos mais baixos escalões que aplicavam, sem discutir, as razões da alta autoridade de que provinham... Estes meios possibilitaram uma extrema vigilância ramificada dos cidadãos, ao mesmo tempo a possibilidade de que ações criminosas permanecessem secretas (...) (SPEER, 1971, *apud* UPINSKY, 1989, p. 171).

Ao recorrer à história da evolução da criptografia, fica claro entender como o desenvolvimento e a utilização desses meios de comunicação durante a Segunda Guerra Mundial tomaram corpo e influenciaram nas situações de batalhas e de transmissões de informação (SINGH, 2008) . Neste momento, há de se perceber quão delicado é lidar com os desenvolvimentos tecnológicos e o quanto suas aplicações práticas podem resultar em situações ou catastróficas ou, por que não, salvadoras.

Ao adentrar essas questões do avanço tecnológico, percebe-se que o sistema binário (0 ou 1) toma o lugar da aritmética de posição e se torna a mais recente demonstração do entrelaçamento entre a arte da guerra e sua administração (UPINSKY, 1989). Tais mudanças tecnológicas vêm atreladas aos fortes interesses políticos e financeiros, como já mencionado, assim, pode-se levantar a questão de que o futuro das próximas guerras emergirá na internet, e, de acordo com Tamdjian e Mendes (2010), muitos países já estão atentos e se preparando para enfrentar esses tipos de problemas.

Segundo esses autores,

> Essa situação de disputas digitais está mostrando que os conflitos podem ocorrer entre países ou grupos de países, bloqueando ou sabotando as redes de computadores rivais como uma forma de tornar o oponente vulnerável, causando a sua paralisia e levando-o ao caos, uma vez que aumentada dia a dia a utilização dos computadores no mundo todo, e suas relações com as economias são cada vez mais profundas (TAMDJIAN; MENDES, 2010, p. 44).

Com os avanços na área da informática, é possível observar situações que possibilitam às pessoas trabalharem praticamente a partir de qualquer lugar. Com a transmissão progressivamente ilimitada de dados, a expansão da conectividade vem alterando "sensivelmente a sociedade e as grandes corporações empresariais" (TAMDJIAN; MENDES, 2010, p. 36). Nesse cenário, é possível observar como a internet está atrelada a essas inovações tecnológicas. Um exemplo simples que as associa é a difusão do comércio on-line (Figura 1). Segundo Tamdjian e Mendes (2010, p. 36), "a compra de bens de consumo e serviços utilizando o computador, o chamado comércio eletrônico, é uma nova ferramenta cujos desdobramentos ainda estão sendo estudados em nossos dias".

De acordo com Tamdjian e Mendes (2010), tudo se iniciou nos anos de 1989 e 1990, com a popularização dos computadores pessoais e da internet. Fazendo uso das tecnologias chamadas 3G/4G, Wi-Fi e Bluetooth, encontradas nos aparelhos móveis (celulares, *tablets*, *smartphones*, entre outros), é possível observar a migração dos aparelhos ditos hoje como tradicionais (telefone fixo, telégrafo, rádio) para as novas tecnologias móveis. Assim, vendo esse setor conquistando um crescimento exponencial, percebe-se que a utilização da internet não se restringe mais às pessoas e aos serviços oferecidos por ela, mas também envolve negócios entre empresas e em escala internacional.

Segundo dados de Tamdjian e Mendes (2010),

> Hoje, esse nicho de mercado já conta com quase 30% das transações comerciais internacionais feitas pela internet [...] [e] acredita-se que em pouco tempo, no mesmo ritmo do avanço da velocidade da internet, fazer comércio eletrônico vai se tornar uma ação rotineira para a maioria dos consumidores (TAMDJIAN; MENDES, 2010, p. 37–38).

Figura 1 – Sistema de compras on-line.

Fonte: Tamdjian e Mendes (2010, p. 37).

Contudo, caminhando paralelamente a esse crescimento ocorrem também os desenvolvimentos da segurança de dados. Garantir aos consumidores, às empresas e aos governos trocas de dados sigilosos é tão importante quanto a própria eficiência da internet. São nestes aspectos que se retomam as ideias iniciais na discussão proposta deste capítulo. A

importância de cifras seguras para garantir a transferência de dados segue em constante evolução, visto que os decifradores continuam em busca de suas quebras, obtendo assim os segredos. Desse modo, de acordo com Tamdjian e Mendes (2010, p. 37), "ainda há muita resistência a esse processo em função da segurança da internet quanto ao uso de dados pessoais, como números de cartão de crédito e documentos".

Diante de tudo aqui discorrido, percebe-se como a matemática, a necessidade de segurança, a informação, os avanços tecnológicos estão entrelaçados às disputas de poder e, por consequência, aos poderes por estas constituídos.

Nessa corrida entre o sigilo e sua quebra, já se registram grandes impasses internacionais relacionados com a internet, as redes de comunicação e os crimes digitais. Envolvendo os conceitos de cifração e decifração, os crimes digitais podem se configurar como sendo aquela tal corrida armamentista intelectual entre os *hackers* e os sistemas de segurança (TAMDJIAN; MENDES, 2010). Os chamados *hackers* nada mais são que entusiastas de computadores, com amplo conhecimento em informática, que podem utilizar tal conhecimento em atividades lícitas (melhorias em segurança eletrônica, criação de novos sistemas, entre outras) ou ilícitas (invasão de sistemas, quebra de senhas, transferências ilegais, entre outras).

Os tipos de crimes ocorridos no ciberespaço[8] têm chamado a atenção de grandes países, com isso gerando grandes investimentos em novas tecnologias. Para exemplificar essa situação, Tamdjian e Mendes (2010) apresenta um momento de preocupação das autoridades dos EUA,

> A situação é tão preocupante que o governo dos EUA criou um Comando Militar Digital para proteger de invasões a rede de computadores governamentais e das Forças Armadas. Assuntos que hoje parecem ficção cientifica em breve serão realidade. Um exemplo é a notícia de que espiões digitais instalaram programas nas redes de computadores dos Estados Unidos que podem interromper o funcionamento de milhões de computadores, levando à paralisia da economia e de muitas atividades e, consequentemente, gerando prejuízos incalculáveis (TAMDJIAN; MENDES, 2010, p. 43).

Corroborando essas preocupações, Upinsky (1989) reflete sobre a grande quantidade de informações que o ciberespaço contempla e como seus manuseios podem afetar a sociedade. De acordo com o autor,

[8] Nome dado ao espaço que contempla um conjunto de equipamentos eletrônicos (computadores, provedores, redes de comunicação e programas de processamentos de dados) ligados à internet.

> O volume fantástico de informações bancárias, econômicas, políticas e sociais que atravessam o espaço por meio dos satélites, rádios, cabos, etc., [é] de causar vertigem; um simples lançamento bancário (apenas alguns "dígitos") atravessa o espaço e em consequência uma fábrica se fecha e famílias são lançadas na miséria. O dólar baixa na bolsa de Nova Iorque e imediatamente se segue uma infinidade de acontecimentos afetando diretamente a vida de milhões de pessoas (UPINSKY, 1989, p. 175).

Entretanto, há de se ter cuidado ao levantar essas questões referentes à importância do sigilo e do quanto isso influencia as nações. Concordamos que as brigas entre cifradores e decifradores existem e que elas estão cada vez mais baseadas nas teorias matemáticas. Contudo, destaca-se aqui que as ações de cifrar e decifrar não assumem características fixas, sendo do "bem" ou do "mal". Quebrar cifras, como foi o caso da quebra do sigilo da máquina Enigma durante a Segunda Guerra Mundial, foi um fato importante para contribuir na opressão da expansão dos nazistas. No entanto, quebrar o sigilo de dados bancários de pessoas é uma violação e, portanto, um crime digital.

É nessa reflexão, sobre os atos de se manter ou não o sigilo de uma informação, que se apresenta um caso importante e que está em circulação atualmente. A possível guerra na internet destacada por Tamdjian e Mendes (2010) pode ter começado no ano de 2010, quando um site chamado Wikileaks começou a divulgar arquivos secretos dos Estados Unidos da América, sobre a Guerra do Afeganistão e a Guerra do Iraque, contendo muitas denuncias graves a respeito das violações aos direitos humanos. O Wikileaks é uma organização transnacional, sem fins lucrativos, que publica em seu *site* dados de fontes anônimas, revelando documentos, fotos e informações confidenciais, vazadas de governos ou empresas. Seu editor e porta-voz, o jornalista e ciberativista Julian Assenge, encontra-se desde 2012 em asilo político na embaixada do Equador em Londres. Com as ameaças de ser detido assim que deixar a embaixada, pelos governos da Suécia e do Reino Unido, e ainda de ser mandado para julgamento nos EUA, Assenge continua travando uma briga junto à ONU para ter direito a liberdade e a indenização.

Enquanto que para alguns países o vazamento de informações gerou grandes conflitos, para outros a iniciativa de revelar verdades escondidas se caracterizou em uma das mais importantes portas de transparência e liberdade de expressão. Com isso, abriu-se um precedente para a divulgação de informações sobre corrupção, violação dos direitos humanos e crimes de guerra. Em decorrência, o *site* inclusive foi indicado pelo parlamento norueguês, em 2011, para concorrer ao prêmio Nobel da Paz.

É com essa situação e com tudo o que se discorreu neste capítulo que se observa e se reflete sobre como a criptografia e a criptoanálise vêm, há muito tempo, ganhando espaço na história da humanidade e se configurando como elementos de poder. Atreladas às guerras em suas constantes corridas armamentistas intelectuais, e à matemática com seus avanços teóricos-tecnológicos, é possível perceber a complexidade desse assunto e ressaltar a importância de se iniciar discussões a respeito dos poderes da informação e do sigilo, na escola básica.

> “Depois que Holmes saiu para ir ao concerto, deitei-me no sofá, com a intenção de dormir algumas horas. Foi inútil. Minha cabeça estava tão agitada por tudo o que ocorrera e foi invadida por fantasias e suposições das mais estranhas”.

> “Senti que, enquanto essas perguntas não fossem respondidas, nem eu e nem Holmes conseguiríamos dormir com facilidade. Contudo, sua atitude autoconfiante e tranquila convenceu-me de que ele já formulara alguma teoria que explica todos os fatos, embora eu não conseguisse sequer imaginá-la”.

> “Deixei Holmes sentado em frente à lareira e, até altas horas, ouvi os lamentos baixos e melancólicos de seu violino, que me faziam saber que ele refletia sobre o estranho problema que se dispôs a resolver”.

(Sherlock Holmes)

3 PESQU1SANDO, PLANEJANDO E COLETANTO DADOS

3.1 P3squisa Int3rvençã0 com enfoque qualitat1vo

A opção pela pesquisa intervenção com enfoque qualitativo se deu a partir de reflexões sobre de que maneira o objetivo deste trabalho poderia ser alcançado. Tendo como pergunta diretriz ***"Quais as potencialidades de atividades pedagógicas envolvendo problemas criptográficos na exploração das ideias associadas à função afim?"***, concluiu-se que, para tentar respondê-la, haveria a necessidade de analisar o processo de investigação que os alunos desenvolveram para chegar à resolução das atividades propostas. Esta necessidade de observar e compreender o processo discutido e vivenciado pelas pessoas em determinados contextos bem estabelecidos pode ser preenchida pela pesquisa qualitativa. Segundo Goldenberg (2011, p. 53), "os dados qualitativos consistem em descrições detalhadas de situações com o objetivo de compreender os indivíduos em seus próprios termos". Além disso, a análise desse tipo de dados possibilita a revelação de situações interessantes para o objeto de estudo, além de poder levar em consideração não só seus sujeitos da pesquisa, como também suas influências externas, como ambiente, outros sujeitos, pesquisador etc. Assim, os dados desta pesquisa podem ser classificados como de natureza qualitativa, pois são constituídos de descrições detalhadas sobre o processo desenvolvido pelos alunos durante a resolução das atividades.

Entende-se que a pesquisa qualitativa é o método de pesquisa mais adequado para compreender o modo de agir e de pensar dos sujeitos da pesquisa durante o processo de desenvolvimento das situações propostas. Borba e Araújo (2012) argumentam que este tipo de abordagem favorece informações mais detalhadas, que priorizam e evidenciam as ações dos indivíduos. Neste sentido, Goldenberg (2011) afirma que:

> Na pesquisa qualitativa a preocupação do pesquisador não é com a representatividade numérica do grupo pesquisado, mas com o aprofundamento da compreensão de um grupo social, de uma organização, de uma instituição, de uma trajetória etc (GOLDENBERG, 2011, p. 14).

D'Ambrósio (1996) alega que a pesquisa qualitativa tem como foco o indivíduo e com ele toda a sua complexidade e interação com o ambiente sociocultural e natural no qual ele está inserido. Corroborando esta ideia, Goldenberg (2011, p. 63) ressalta que esse tipo de abordagem permite ao pesquisador "observar, diretamente, como cada indivíduo, grupo ou

instituição experimenta, concretamente, a realidade pesquisada". Sobre a mesma temática, Rogoff (1998), fundamentada nas ideias de Vygotsky, argumenta exatamente sobre os papéis interdependentes do indivíduo e de seu mundo social. De acordo com essa autora, o indivíduo e o ambiente estão conectados por estruturas temporais, e tentar analisar um determinado acontecimento separando esses elementos é acordar que eles não mais funcionam como um conjunto todo (ROGOFF, 1998).

Ainda nesse sentido, Rogoff (1998) afirma que:

> O uso da "atividade" ou do "acontecimento" como a unidade de análise [...] possibilita uma reformulação da relação entre o indivíduo e os ambientes sociais e culturais nos quais cada um está inerentemente envolvido na definição de outros. Nenhum existe separadamente (ROGOFF, 1998, p. 124).

Nessa linha de pensamento, a autora põe em discussão três conceitos inseparáveis, a saber, o aprendizado, a participação guiada e a apropriação participatória, que refletem planos diferentes na análise da atividade sociocultural. Tais planos são entendidos como tendo abordagens diferentes de enfoque e não separados ou hierárquicos a determinados acontecimentos. O entendimento de um plano depende exatamente de compreender os outros e o papel que esses outros acarretam no plano de enfoque.

A pesquisa de intervenção com perspectiva qualitativa aqui proposta se aproxima das ideias apresentadas acima sobre os planos de aprendizagem, participação guiada e apropriação participatória. Dentro desse contexto, Rogoff (1998) discute que no aprendizado existe uma troca de habilidades e entendimentos entre pessoas mais experientes e outras menos experientes, e ainda ressalta que somente por meio de uma atividade culturalmente organizada é que tal troca é possível, ressaltando que a ideia de aprendizado de conceitos "vai além da dualidade experiente-inexperiente; enfoca um sistema de envolvimentos pessoais e combinações nos quais pessoas se engajam na atividade culturalmente organizada na qual aprendizes se tornam participantes mais responsáveis" (ROGOFF, 1998, p. 126).

No plano da participação guiada, Rogoff (1998) articula a ideia dos processos e sistemas de envolvimento entre as pessoas à medida que elas se relacionam, comunicam e coordenam esforços para participar de atividades culturais. A proposta é olhar essas interações como participações em conjunto e não isoladas de cada indivíduo. No campo da apropriação participatória, a autora se refere às mudanças ocorridas entre os indivíduos por meio de seu envolvimento nas atividades. Segundo ela:

> A apropriação participatória é o processo pessoal pelo qual, através do compromisso em uma atividade, os indivíduos mudam e controlam uma situação posterior de maneiras preparadas pela própria participação na situação prévia. Esse é um processo de apropriação, e não de aquisição (ROGOFF, 1998, p. 126).

Olhando para esses três planos, observa-se que o pesquisador, ao analisar dados qualitativos em uma pesquisa de intervenção, deve perceber as sutilezas que o enfoque em cada acontecimento pode conter. Os indivíduos se modificam a cada acontecimento, interagem, cooperam, participam e trocam experiências que implicam em novas posturas diante de acontecimentos subsequentes. O próprio pesquisador é sujeito da pesquisa, visto que este se relaciona, orienta, participa de todo o processo de intervenção. Nesse sentindo, ressalte-se que conduzir uma pesquisa que envolva indivíduos, enfocando em como eles participam das atividades e de como suas posturas se modificam em relação a essas participações, contribui para clarear mais os processos de aprendizagem e de desenvolvimento que o objeto de estudo se propõe a abordar.

No que concerne ao pesquisador e seu ato de pesquisar, Ponte corrobora as ideias de Rogoff, (1998) ao destacar que o pesquisador também faz parte da pesquisa, atuando lado a lado com seus participantes na construção e transformação da prática educativa. No entanto, esse envolvimento pode interferir nos resultados da pesquisa. A personalidade e os valores do pesquisador podem contaminar as respostas dos sujeitos da pesquisa (GOLDENBERG, 2011). Nesse sentido, Goldenberg (2011, p. 17) destaca que este "não pode fazer julgamentos nem permitir que seus preconceitos e crenças contaminem a pesquisa". Quanto a isso, ela ainda argumenta que "a melhor maneira de controlar esta interferência é tendo consciência de como sua presença afeta o grupo e até que ponto este fato pode ser minimizado ou, inclusive, analisado como dado da pesquisa" (GOLDENBERG, 2011, p. 55).

Ao olhar a pesquisa como um todo, num plano em que ela se encontra finalizada, sua apresentação é dada de forma linear, tecendo a cada capítulo um pedaço a mais de todo o processo no qual a pesquisa esteve inserida. Essa estrutura contínua pode ser observada na fala de D'Ambrósio (1996), quando ele argumenta sobre a organização da pesquisa qualitativa em etapas, a saber:

> 1) Formulação das questões a serem investigadas com base no referencial teórico do pesquisador; 2) Seleção de locais, sujeitos e objetos que constituirão o foco da investigação; 3) Investigação das relações entre esses elementos; 4) Definição de estratégias de coleção e análise dos dados; 5) Coleção de dados sobre os elementos selecionados no item 2 e sobre as relações identificadas no item 3; 6) Análise desses dados e refinamento das questões formuladas no item 1 e da seleção proposta no item 2; 7)

> Redefinição de estratégias definidas no item 4; 8) Coleta e análise dos dados (D'AMBROSIO, 1996, p. 103).

As etapas apresentadas por D'Ambrósio (1996) dão uma linearidade na organização da pesquisa qualitativa. Deslauriers e Kèrisit (2012) consideram essas etapas como sendo o delineamento da pesquisa, e em relação a isso afirmam que:

> A lógica de apresentação não é a da ação; neste caso, e por necessidade de causa, a apresentação dos diferentes elementos da pesquisa qualitativa seguirá uma ordem linear que nem sempre é a encontrada na própria prática da pesquisa (DESLAURIERS; KÉRISIT, 2012, p. 128).

Nesse sentido, o pesquisador tem a liberdade de transitar entre estas etapas durante a sua pesquisa, sendo ele livre para decidir quais etapas seguir para buscar os objetivos propostos.

Tendo, então, como foco de pesquisa analisar o processo de investigação e resolução utilizados pelos alunos para resolver as atividades envolvendo problemas criptografados e função afim, é que o perfil desta pesquisa pode ser considerado qualitativo. Assim sendo, levando em consideração a importância do pesquisador nas escolhas de sua pesquisa e no quanto sua figura interfere no trabalho de campo é que apresento, nas próximas seções, a elaboração e produção de algumas das etapas da pesquisa citada por D'Ambrósio (1996).

3.2 C0ncepção c0nstrutiv1sta – apr3nder conc3itos, pr0cedim3ntos e at1tud3s

A aprendizagem na concepção construtivista é um elemento que contribui para o desenvolvimento do aluno na medida em que este é capaz de produzir uma representação pessoal sobre o objeto (real) ou conteúdo a ser aprendido (SOLÉ; COLL, 2009). Em relação às representações construídas pelos próprios alunos, Ponte e Serrazina (2000) argumentam que elas são importantes para o desenvolvimento dos alunos acerca de suas compreensões relacionadas às ideias matemáticas. De acordo com esses autores, mesmo que as representações sejam, na maioria das vezes, pouco precisas e bem particulares, elas podem derivar situações valiosas uma vez que "apoiam a compreensão e solução de problemas, fornecem formas significativas de registro de um método ou de uma solução e fornecem um ponto de partida do qual os alunos podem desenvolver uma apreciação de outras representações" (PONTE; SERRAZINA, 2000, p. 43). Nessa direção, esses autores concluem que, ao observar as representações desenvolvidas pelos alunos em relação às situações propostas, o professor tem a oportunidade de observar o modo de pensar dos mesmos

podendo utilizar essas informações para estabelecer envolvimentos entre as representações particulares desenvolvidas por eles com as representações usuais utilizadas na matemática.

Nesse pensar, Solé e Coll (2009) argumentam que as elaborações das representações se aproximam do objeto ou conteúdo a partir das experiências, disposições e conhecimentos prévios, que, presumidamente, dão suporte às novas informações. Nesse sentido, os autores acima argumentam que, perante uma situação nova, os significados já interiorizados ora se mantêm, servindo apenas para a interpretação do que se parece novo, ora se modificam, pois o novo é visto como um desafio e, desse modo, exige alterações para a construção de novos significados. Nesse segundo processo, de acordo com eles, "não só modificamos o que já possuímos, mas também interpretamos o novo de forma peculiar, para poder integrá-lo e torná-lo nosso" (SOLÉ; COLL, 2009, p. 20).

Assim, os autores acima definem que o aluno *aprende significativamente* quando este se apropria e se desenvolve no segundo processo, construindo, assim, significados próprios e pessoais para os objetos de conhecimento. Os autores ainda ressaltam que este processo não "conduz à acumulação de novos conhecimentos, mas à integração, modificação, estabelecimento que já possuíamos, dotados de uma certa estrutura e organização que varia, em vínculos e relações, a cada aprendizagem que realizamos" (SOLÉ; COLL, 2009, p. 20). Dessa maneira, pode-se concluir que a aprendizagem é significativa, uma vez que as condições da nova informação estejam bem determinadas, podendo essas ser abertas a modificações e aperfeiçoamentos.

Na concepção construtivista, o ensino e a aprendizagem são regidos por processos conjuntos e compartilhados, nos quais os alunos, por meio da mediação do professor, desenvolvem aspectos de competência e autonomia na resolução de atividades, na utilização dos conceitos, na ação de determinadas práticas, entre outros. Desse modo, os alunos constroem aprendizagens mais ou menos significativas, resultantes não apenas de seus conhecimentos prévios e nem pela natureza do conteúdo, mas sim de toda ajuda oferecida pelo professor acerca da mediação desses conhecimentos prévios com a estimulação e apropriação progressiva desse novo aprendizado (SOLÉ; COLL, 2009). Nesse sentido, Solé e Coll (2009, p. 23) afirmam que "essa ajuda, a orientação que ela oferece e a autonomia que permite, é o que possibilita a construção de significado por parte do aluno".

Acerca do amadurecimento do aluno sobre sua aprendizagem, Solé (2009) tece considerações a respeito de a elaboração do conhecimento necessitar de tempo, esforço e compreensão pessoal. Exigir que o aluno compreenda o conteúdo, o relacione com seus conhecimentos prévios, extraia conclusões e que aprenda significativamente, sem dar-lhe

tempo e condição para tal, é presumir a ocorrência do fracasso escolar, resultante, assim, de um estudo superficial. Além disso, a autora ainda argumenta sobre a contribuição do professor em relação ao seu incentivo e afeto. De acordo com ela, esses dois elementos podem contribuir, de certo modo, para o processo de aprendizado. Partir dos saberes pessoais dos alunos, potencializá-los e expressá-los positivamente estabelece uma relação de respeito com o aluno acerca da importância de suas contribuições, refletindo, por fim, em sua autoestima. Nesse sentido, Solé (2009) infere algumas reflexões quanto à postura do professor no contexto da aprendizagem do aluno.

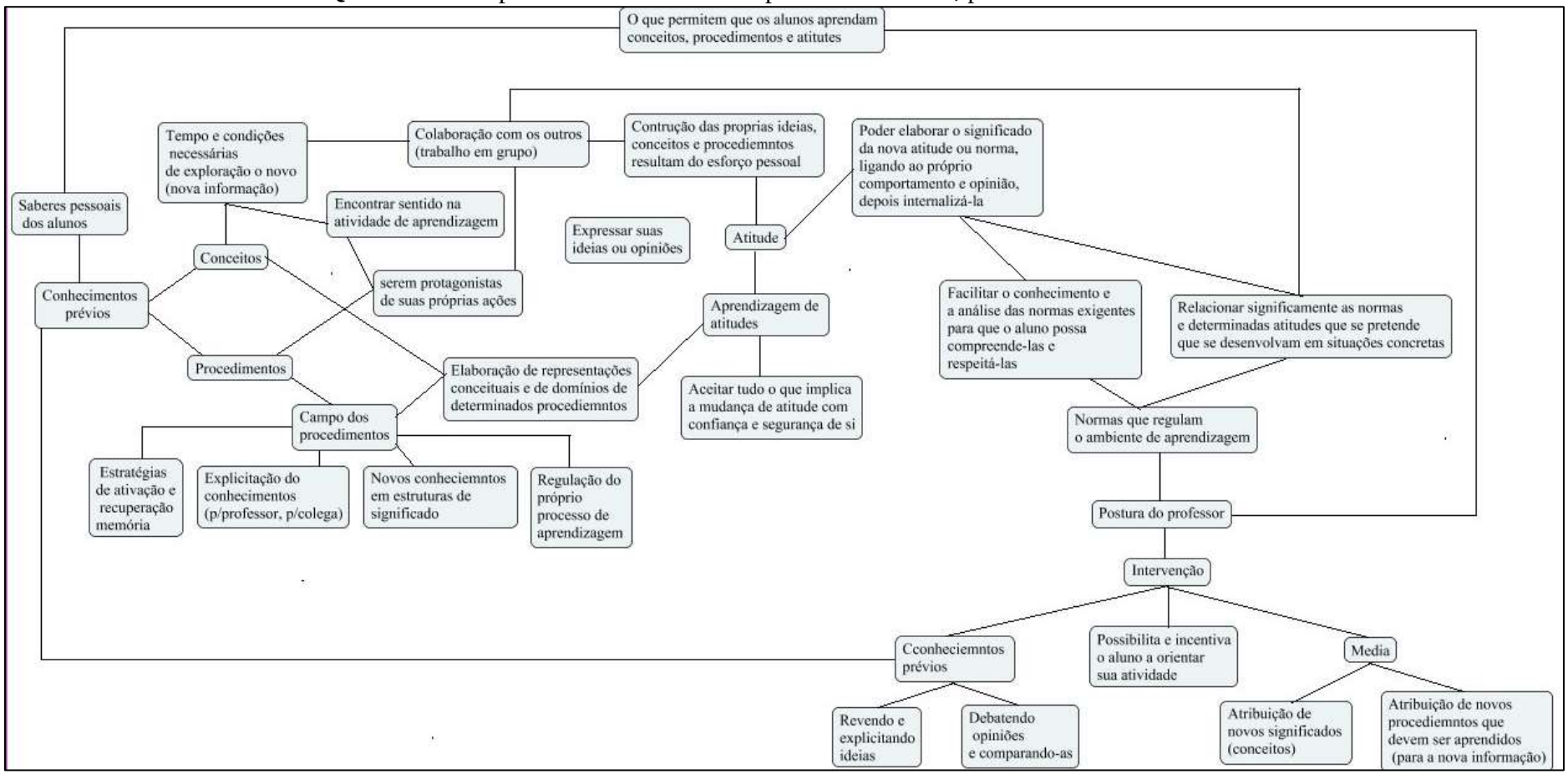
> 1) Colocar os desafios ao seu alcance, observar uma distância ótima entre o que traz e o que lhe é colocado incentivam seu interesse e lhe permite confiar em suas próprias possibilidades; proporcionar-lhes as ajudas necessárias possibilita forjar uma imagem positiva e ajustada. 2) Interpretar a situação de ensino como um contexto compartilhado contribui para que o aluno se sinta, ao mesmo tempo, como um interlocutor interessante e com a segurança que dá saber que outro mais especializado está ali para ajudar, para ensinar a chegar onde ainda é impossível chegar sozinho. 3) Garantir que o aluno possa mostrar-se progressivamente autônomo no estabelecimento de objetivos, no planejamento das ações que o conduzirá a eles, em sua realização e controle e, enfim, naquilo que pressupõe autodireção e autorregulação do processo de aprendizagem traduz confiança em sua possibilidade e educa na autonomia e na responsabilidade. 4) Valorizar seus resultados em relação às suas capacidades e ao esforço realizado [...], incentivando a autoestima e a motivação para continuar aprendendo (SOLÉ, 2009, p. 53).

Dessa maneira, a construção de significados na aprendizagem se relaciona com a aquisição de sentimentos de competência, autoestima e de respeito a si próprio e aos outros, além também de estar intimamente ligada com o desenvolvimento e a exploração do domínio de procedimentos, a criação e aceitação de atitudes e da compreensão de determinados conceitos.

É sobre esses três últimos elementos, procedimentos, atitudes e conceitos que Mauri (2009) dedica a articular com a aprendizagem significativa, de modo a discutir a teia de conexões que se estabelecem no ato de aprendê-los. A autora articula sobre o que propicia o ato de aprender dos alunos e o divide em dois pontos: 1) em relação aos alunos – dispor de uma série de conhecimentos e 2) em relação ao professor – sua atuação considerando o aluno como o centro de sua intervenção.

O Quadro 1 apresenta um esquema, resumindo consideravelmente as conexões existentes entre os três elementos e o aprendizado do aluno, partindo dos dois pontos do aprender destacados por Mauri (2009), dentro da perspectiva construtivista de aprendizado.

Quadro 1 - Mapa de conexões sobre o aprender conceitos, procedimentos e atitudes.



Fonte: Construído pela pesquisadora (2016).

Em relação aos saberes prévios dos alunos, Mauri (2009) destaca que eles se encontram tanto na área dos conceitos quanto na área dos procedimentos. Em relação aos primeiros, a autora destaca que "ter conhecimentos conceituais prévios organizados, pertinentes e relevantes" (MAURI, 2009, p. 105) contribui para se concatenar com as novas informações (objeto de aprendizagem). Em relação aos segundos, ela considera que as técnicas, os métodos, as regras, as normas, os algoritmos, as habilidades motoras e cognitivas e as estratégias são conhecimentos prévios que devem proporcionar ao aluno a capacidade de "realizar ou executar, em algum grau, as operações de procedimentos necessárias para lograr a meta proposta e, também, possuir uma representação ou ideia do procedimento em si mesmo" (MAURI, 2009, p. 111). Em relação a isso, Echeverría e Pozo (1998) destacam que esse tipo de procedimento é utilizado para se solucionar um problema. De acordo com eles, esses procedimentos "se constituem em conhecimentos adquiridos que permitem transformar a informação de uma maneira fixa, eficaz e concreta, embora possam ser utilizados num grande número de situações" (ECHEVERRÍA; POZO, 1998, p. 24).

Entretanto, eles destacam e distinguem esse tipo de procedimentos entre os procedimentos estratégicos ou heurísticos, os quais são definidos como sendo os planos, metas e submetas que os alunos estabelecem em sua busca durante o desenvolvimento da solução do problema (ECHEVERRÍA; POZO, 1998). Corroborando a distinção que Echeverría e Pozo (1998) ressaltam, Mauri (2009) ainda argumenta sobre a importância dos procedimentos estratégicos ou heurísticos, destacando que esses tipos de procedimentos surgem nos momentos de busca dos métodos de ativação da memória e de suas recuperações, na explicitação desses conhecimentos para outros (professor, aluno), na construção dos novos conhecimentos em estruturas de significado e em relação à autonomia do próprio processo de aprendizagem.

Ainda dentro desse espectro, Mauri (2009) argumenta sobre o sentido encontrado na atividade de aprendizagem por parte dos alunos. De acordo com ela, esse sentido decorre tanto do tempo e das condições dispostas a eles durante a exploração de seus conceitos quanto da liberdade de investigação de seus procedimentos, o que favorece a atuação protagonista de suas ações. Esse momento se reflete na independência do aluno e ocasiona um possível trabalho em grupo, pois, além de oportunizar um momento de expressar suas opiniões e ideias, contribui para a construção e organização de outras. Isso tudo incide no desenvolvimento da atitude. Segundo Mauri (2009),

> A aprendizagem de atitudes se apoia, como demonstramos, na elaboração de representações conceituais e no domínio de determinados procedimentos (estratégias de memória, estratégias de relação com os outros etc.). Por sua vez, atitudes estão na base do desenvolvimento pessoal de estratégias de direção, orientação e manutenção da própria atividade de aprendizagem (MAURI, 2009, p. 120).

Com relação a essa aprendizagem, fica compreensível a postura do professor, o qual tem o dever de explicitar as normas que regulam o ambiente de aprendizagem e de facilitar, para os alunos, o conhecimento dessas normas, para que estes possam compreendê-las, respeitá-las e interiorizá-las, a fim de elaborarem seus significados e ligá-las a seus próprios comportamentos e opiniões (MAURI, 2009).

Nesse ponto é que se pode compor o plano do professor. Sua atuação, considerando o aluno como sendo o centro de sua ação, o põe em uma situação na qual ele assume uma postura de orientador que intervém no processo de aprendizagem do aluno levantando questionamentos, debatendo discussões e, revendo e explicitando ideias sobre os conhecimentos prévios trazidos por eles. Além disso, o professor deve possibilitar e incentivar o aluno a tomar a frente de sua atividade e, com todo esse ambiente, ele deve mediar a atribuição de significados da nova informação (conceitual) e dos novos procedimentos a serem aprendidos (relacionados com a nova informação) (MAURI, 2009).

Portanto, é dentro desse cenário, levando em considerações os saberes dos alunos e a postura do professor, que Mauri (2009) traz discussões a respeito do aprendizado de conceitos, procedimentos e atitudes em uma perspectiva construtivista. E, como conclusão dessa rede de conexões, pode-se observar que, na aprendizagem de conceitos, é necessário que procedimentos e atitudes sejam trabalhados, não em planos separados, mas sim em atividades que explorem e construam significados para cada um desses elementos.

3.3 R3soluçã0 de Probl3mas e suas Inv3stigaçõ3s

De acordo com os PCNEM (BRASIL, 2000), a metodologia resolução de problemas é uma importante estratégia de ensino na disciplina de Matemática. De acordo com ele:

> Os alunos, confrontados com situações-problema, novas mas compatíveis com os instrumentos que já possuem ou que possam adquirir no processo, aprendem a desenvolver estratégia de enfrentamento, planejando etapas, estabelecendo relações, verificando regularidades, fazendo uso dos próprios erros cometidos para buscar novas alternativas; adquirem espírito de pesquisa, aprendendo a consultar, a experimentar, a organizar dados, a

> sistematizar resultados, a validar soluções; desenvolvem sua capacidade de raciocínio, adquirem auto-confiança e sentido de responsabilidade; e, finalmente, ampliam sua autonomia e capacidade de comunicação e de argumentação (BRASIL, 2000, p. 52).

A resolução de problemas pode proporcionar aos alunos aulas diferenciadas, nas quais o ensino de Matemática ocorre em um ambiente caracterizado pela exploração de problemas. Dante (2000, p. 9) afirma que "um problema é qualquer situação que exija o pensar do indivíduo para solucioná-la" e um problema matemático é "qualquer situação que exija a maneira matemática de se pensar e conhecimentos matemáticos para solucioná-la" (DANTE, 2000, p. 10). Sobre a definição de problema, Ponte e Serrazina (2000, p. 52) argumentam que "uma questão é um problema, para dado aluno, se ele não tiver nenhum meio para encontrar uma solução num único passo". Com uma definição muito parecida, Echeverría e Pozo (1998) detalham que:

> Uma situação somente pode ser concebida como um problema na medida em que exista um reconhecimento dela como tal, e na medida em que não dispomos de procedimentos automáticos que nos permitam solucioná-la de forma mais ou menos imediata, sem exigir, de alguma forma, um processo de reflexão ou uma tomada de decisões sobre a sequência de passos a serem seguidos (ECHEVERRÍA; POZO, 1998, p. 16).

Nesse sentido, os autores acima afirmam que guiar um currículo para a solução de problemas significa "procurar e planejar situações suficientemente abertas para introduzir nos alunos uma busca e apropriação de estratégias adequadas não somente para darem resposta a perguntas escolares como também às da realidade cotidiana" (ECHEVERRÍA; POZO, 1998, p. 14). Assim, ensinar a resolver problemas não se baseia apenas em prover os alunos de habilidades e estratégias eficientes, mas também de oportunizar aos alunos o desenvolvimento de praxes e atitudes de afrontar a própria aprendizagem (ECHEVERRÍA; POZO, 1998; PONTE; SERRAZINA, 2000). Em outras palavras, "o verdadeiro objetivo final da aprendizagem da solução de problemas é fazer com que o aluno adquira o hábito de propor-se problemas e de resolvê-los como forma de aprender" (ECHEVERRÍA; POZO, 1998, p. 15). Corroborando essa ideia Ponte e Serrazina (2000) afirmam que,

> A resolução de problemas ajuda a desenvolver a compreensão das ideias matemáticas e a consolidar as capacidades já aprendidas e, por outro lado, constitui um importante meio de desenvolver novas ideias matemáticas. Por outras palavras, a resolução de problemas pode construir o ponto de partida e o ponto de chegada do ensino-aprendizagem da Matemática (PONTE; SERRAZINA, 2000, p. 55–56).

Desse modo, observa-se que, o problema deve, então, ser caracterizado por situações mais abertas ou novas, o que coloca os alunos em uma posição que eles desconheçam, uma forma ou um caminho direto para a sua resolução e, assim, busquem, em seus conhecimentos prévios, os procedimentos (técnicos ou heurísticos), os conhecimentos conceituais e as atitudes que lhes possibilitem explorar os dados do problema e investigar as estratégias de resolução. No entanto, também é importante que, no momento inicial da resolução de problemas, os alunos se sintam instigados e motivados a realizar a atividade proposta, sendo que os problemas constituam um verdadeiro desafio para os mesmos. Isso contribui para aguçar a motivação para resolver os problemas e dar sentido à realização da atividade (ECHEVERRÍA; POZO, 1998).

Segundo Ponte, Brocado e Oliveira (2009) a realização de investigações tem estreita associação com a resolução de problemas. O ato de investigar consiste em trabalhar com questões abertas que exigem dos alunos o ato de inquirir e explorar os dados do problema, a ponto de organizá-los e de desenvolver as estratégias de resolução (PONTE; BROCADO; OLIVEIRA, 2009). De acordo com esses autores, as investigações matemáticas, além de envolver os conceitos, os procedimentos e as representações matemáticas, se caracterizam fortemente pelo caráter conjectura-teste-refutação ou confirmação da hipótese. Assim, eles definem que atividades de ensino-aprendizagem envolvendo investigações matemáticas ajudam a:

> Trazer para a sala de aula o espírito da atividade matemática genuína, constituindo, por isso, uma poderosa metáfora educativa. O aluno é chamado a agir com um matemático, não só na formulação de questões e conjecturas e na realização de provas e refutações, mas também na apresentação de resultados e na discussão e argumentação com seus colegas e o professor (PONTE; BROCADO; OLIVEIRA, 2009, p. 23).

As situações de investigação e estratégias feitas pelos alunos durante as resoluções dos problemas podem contribuir para o desenvolvimento cognitivo, afetivo e coletivo dos mesmos. Durante o trabalho de resolução, o aluno tem o controle para investigar, questionar e modificar seus métodos de resolução. Isso propicia aos alunos uma autonomia nos processos de resolução, juntamente com o desenvolvimento de uma visão crítica dos procedimentos, a fim de empreender a construção e formalização dos conceitos – além de favorecer o envolvimento ativo do aluno em sua aprendizagem (PONTE; BROCADO; OLIVEIRA, 2009).

Ponte, Brocado e Oliveira (2009) argumentam sobre as possíveis fases da investigação de um problema que podem surgir em um ambiente investigativo. De acordo com esses autores, existem algumas etapas gerais, como por exemplo, a introdução da tarefa feita pelo professor e a discussão de suas resoluções com todos os alunos, e as subetapas, que abrangem todo o processo dos alunos realizado durante o desenvolvimento das investigações. Essas subetapas contemplam o reconhecimento da situação, exploração preliminar e formulação de questões, as formulações de hipóteses com suas verificações e seus refinamentos e a argumentação, demonstração e avaliação do trabalho realizado (entre os alunos). Echeverría e Pozo (1998) também tecem considerações a respeito dos passos dos alunos durante a resolução de problemas. De acordo com eles, "a solução de um problema exige uma compreensão da tarefa, a concepção de um plano que nos conduza à meta, a execução desse plano e, finalmente, uma análise que nos leve a determinar se alcançamos ou não a meta" (ECHEVERRÍA; POZO, 1998, p. 22). Destaca-se sobre essas fases da investigação que não há uma linearidade entre esses procedimentos heurísticos. Os alunos permeiam entre as fases conforme suas necessidades e todo esse conjunto de passos faz parte do processo de investigação e resolução dos problemas propostos.

Dentro dessa esfera de fases apresentada acima, Ponte, Brocado e Oliveira (2009) reforçam que o ambiente de aprendizagem que se cria dentro da sala de aula é de extrema importância. Corroborando as concepções de Mauri (2009), esses autores destacam que:

> É fundamental que o aluno se sinta à vontade e lhe seja dado tempo para colocar questões, pensar, explorar as suas ideias e exprimi-las, tanto ao professor como aos seus colegas. O aluno deve sentir que as suas ideias são valorizadas e que se espera que as discuta com os colegas, não sendo necessária a validação constante por parte do professor. Portanto, na fase inicial de uma investigação, o professor deve procurar criar esse tipo de ambiente e informar os alunos do papel que se propõe desempenhar. Esses devem saber que podem contar com o apoio do professor, mas que a atividade depende, essencialmente, da sua própria iniciativa (PONTE; BROCADO; OLIVEIRA, 2009, p. 28).

Desse modo, observa-se que o trabalho investigativo também favorece a situação de trabalho em grupo, o qual potencia o levantamento de alternativas de exploração, de debates e afrontamentos de ideias, contribuindo para explorações de procedimentos e afirmações de atitudes. Também nota-se a postura atribuída ao professor, o qual está presente a todo o momento na situação de investigação, sendo ele um orientador desse processo de aprendizado. Esses autores ainda afirmam que o professor está a todo o momento buscando o equilíbrio entre "a autonomia [dos alunos] que é necessária para não comprometer a sua

autoria da investigação, e por outro lado, garantir que o trabalho dos alunos vá fluindo e seja significativo do ponto de vista da disciplina de Matemática" (PONTE; BROCADO; OLIVEIRA, 2009, p. 47).

Assim sendo, para se chegar a uma aprendizagem significativa, é necessário que os alunos se deparem com diálogos e problemas estimulantes, para que estes desenvolvam situações de investigação, a qual propicia o desenvolvimento dos saberes prévios de procedimentos técnicos ou heurísticos, que explorem seus próprios conhecimentos conceituais e que adquiram atitudes ativas e interativas com o problema e o ambiente exposto. Deste modo, observa-se que a investigação surge como um possível meio de construção do conhecimento, o qual leva em consideração toda a esfera do ambiente de aprendizagem que foi apresentada e discutida nesta seção.

Dessa forma, com as considerações apresentadas no item 3.2 sobre a concepção construtivista, partindo de um olhar sobre como se aprender atitudes, procedimentos e conceitos e levando em conta as ponderações sobre o que é ser um problema e de como um ambiente em sala de aula pode se constituir baseados nas resoluções de problemas discutidas na seção 3.3 é que o referencial teórico dessa pesquisa foi constituído a fim de dar suporte posteriormente para a analise dos dados.

3.4 Cr1ptograf1a e Educ4ção Mat3mática

Nesta seção, serão apresentadas algumas pesquisas que entrelaçam as áreas da Criptografia e da Educação Matemática. Moura e Ferreira (2005) afirmam que a revisão de literatura é um processo interessante, entretanto nada mecânico. A busca de trabalhos de interesse exige do pesquisador conhecimento prévio sobre a área pesquisada, curiosidade e certa capacidade de investigação (MOURA; FERREIRA, 2005). Esses autores ainda argumentam que,

> De todo modo, a revisão da literatura é uma busca sistemática, a fim de mapear o que se tem pesquisado na área. Não é uma fase discreta, independente da pesquisa. A investigação do material levantado deve permitir uma análise do que se tem denominado "o estado da questão" sobre um determinado tema ou problema de pesquisa, revelando lacunas que justificam o estudo que se pretende realizar (MOURA; FERREIRA, 2005, p. 36).

Borba e Araújo (2012) reforçam que a revisão de literatura é um processo primordial da pesquisa, a qual situa o trabalho do pesquisador perante a produção do conhecimento da sociedade cientifica. Assim, espera-se trazer, nesta seção, uma visão panorâmica dos trabalhos encontrados[9] sobre o entrelaçamento da Criptografia com a Educação Matemática.

Os trabalhos serão expostos de forma cronológica a partir das publicações. A ideia de seguir essa ordem é a de mostrar ao leitor como esse assunto veio sendo abordado e a pesquisa sobre ele veio crescendo ao longo do tempo. Durante as pesquisas realizadas, em busca do entrelaçamento dessas duas áreas, foram encontrados um total de trinta e sete trabalhos, sendo eles minicursos, artigos e trabalhos acadêmicos. Por questão de interesse de pesquisa, apenas alguns artigos e os trabalhos acadêmicos serão abordados[10].

O primeiro trabalho encontrado é o artigo de Tamarozzi (2001) intitulado "Codificando e Decifrando Mensagens". Nele, o autor apresenta brevemente algumas ideias da criptografia e expõe dois exemplos básicos para o processo de cifragem, um utilizando uma função afim e o outro, uma matriz. O autor deixa claro que acredita que essas atividades podem ser utilizadas em sala de aula. Segundo ele, esse material pode ser "útil para exercícios, como também para atividades e jogos de codificação. O professor pode dispor deles para a fixação de conteúdos matemáticos associados" (TAMAROZZI, 2001, p. 41).

Explorando as sugestões de Tamarozzi, o trabalho de Groenwald, Franke e Olgin (2009) traz argumentos para a inserção desse tema no Ensino Básico, além de apresentar outras possibilidades de uso da criptografia em sala de aula. De acordo com as autoras,

> O ponto de referência do processo de ensino e aprendizagem da Matemática deve ser a abordagem de assuntos de interesse do aluno, que estimulem a curiosidade e que desencadeiem um processo que permita a construção de novos conhecimentos. A Matemática torna-se interessante e motivadora para a aprendizagem quando desenvolvida de forma integrada e relacionada a outros conhecimentos, trazendo o desafio de desenvolver competências e habilidades formadoras do pensamento matemático (GROENWALD; FRANKE; OLGIN, 2009, p. 41-42).

Em relação a isso, elas apresentam o tema criptografia como sendo o agente motivador e gerador das situações descritas acima. Segundo elas, as situações didáticas envolvendo a criptografia podem permitir o "aprofundamento da compreensão dos conceitos matemáticos, possibilitando ao aluno perceber a utilização do conhecimento matemático em situações

[9] Busca realizada na Biblioteca Digital de Teses e Dissertações – BDTD e no Google em Junho de 2015, por meio das palavras chaves: Criptografia e Educação Matemática, Criptografia e Ensino, Códigos e Ensino, Cifras e Ensino, entre outras.
[10] Tais trabalhos foram escolhidos, pois, na visão da pesquisadora, são os que trazem mais informações quanto ao entrelaçamento entre o tema Criptografia e o Currículo de Matemática.

práticas" (GROENWALD; FRANKE; OLGIN, 2009, p. 42). O artigo de Groenwald, Franke e Olgin (2009) mostra atividades envolvendo as cifras que surgiram durante a evolução da criptografia, como, por exemplo, os códigos ISBN[11], a cifra de César, a cifra de Vigenère, a cifra do Chiqueiro[12], Anagramas e, também, códigos envolvendo conceitos vistos no Ensino Básico, como funções exponenciais, logarítmicas e análise combinatória.

O TCC de Fincatti (2010) aborda as definições e operações da função afim, das matrizes e da função exponencial, trazendo para cada um desses conceitos uma orientação para o professor sobre como as atividades criptográficas poderiam envolver esses temas e a criptografia. Já o trabalho de Fiarresga (2010) foi a única pesquisa estrangeira encontrada que traz alguma reflexão sobre a inserção da criptografia em sala de aula. Sua pesquisa se concentra em detalhar a Matemática por trás da criptografia, abordando conteúdos como grupos, anéis e corpo, congruências, teorema de Euler, resíduos quadráticos, curvas elípticas, entre outros, fazendo um detalhamento dos tipos de cifras simétricas e assimétricas e, por último, abordando a definição e os esquemas das assinaturas digitais. Embora este autor realize um trabalho mais matemático e não apresente atividades envolvendo esses conceitos, em sua conclusão ele tece algumas considerações sobre uma atividade realizada com alunos do sétimo ano de escolaridade. De acordo com ele, adaptações acerca da linguagem Matemática foram realizadas e um algoritmo para se calcular o dia da semana a partir de uma data qualquer foi ensinado aos alunos e a uma professora de francês. Utilizando apenas a ajuda de uma calculadora científica, Fiarresga (2010) ressalta que este teria sido um exemplo de que alunos do Ensino Básico seriam capazes de desenvolver e perceberem a Matemática, entusiasmando-se com ela. Em suas considerações finais, ele ressalta que a criptografia e a criptoanálise podem auxiliar os alunos no desenvolvimento da concentração e da persistência dos mesmos, quando estes se deparam com problemas matemáticos.

No artigo de Olgin e Groenwald (2011), as autoras abordam sobre quais os temas que aparecem no Currículo de Matemática do Ensino Médio poderiam ser aliados a temas de interesse dos alunos. Uma sugestão de tema apresentado que poderia ser trabalhado seria a criptografia. De acordo com elas,

> A Criptografia é um exemplo de tema que pode ser abordado no Currículo do Ensino Médio, pois permite: desenvolver atividades didáticas utilizando

[11] International Standard Book Number.
[12] Para mais informações a respeito das cifras de cifra de César, a cifra de Vigenère, a cifra do Chiqueiro ver SINGH, S. *O livro dos códigos: A ciência do sigilo - do antigo Egito à criptografia quântica*. 7. ed. Rio de Janeiro: Record, 2008.

> padrões e regras de codificação e decodificação; trabalhar os conteúdos matemáticos, já desenvolvidos em sala de aula pelos professores, dentro de um contexto que envolve segurança de dados; possibilita recontextualizar um conteúdo dentro de outro tema, produzindo novos significados e relações enriquecedoras (OLGIN; GROENWALD, 2011, p. 75).

Assim, olhando para os conteúdos matemáticos do currículo do Ensino Médio e para as cifras utilizadas na criptografia, as autoras elaboraram uma tabela (Figura 2) que apresenta sugestões de atividades didáticas com esse tema.

Figura 2 - Tema criptografia aliado a conteúdos do Ensino Médio.

ATIVIDADES DIDÁTICAS COM O TEMA CRIPTOGRAFIA	
Atividades	**Conteúdos Matemáticos**
Criptogramas	Aritmética
Código ISBN	Aritmética modular.
Código com Função Linear	Função Linear, cálculo da imagem da função, cálculo de função inversa.
Código com Função Quadrática	Função Quadrática, cálculo da imagem da função, cálculo de função inversa.
Código com Função Exponencial e Logarítmica	Propriedades da potenciação, equações exponenciais, cálculo da imagem de uma função e logaritmo mudança de base.
Código com Matrizes	Matrizes, multiplicação de matrizes, operações com matrizes, matriz transposta e cálculo de matriz inversa.

Fonte: Olgin e Groenwald (2011, p. 75).

Essas autoras ainda publicaram outros artigos a respeito da inserção da criptografia na sala de aula, entretanto é na dissertação de Olgin (2011) que aparecem maiores resultados com relação a isso. Sua pesquisa traz as possíveis relações que a criptografia poderia ter com os conteúdos matemáticos do Ensino Médio e apresenta um levantamento sobre as atividades didáticas existentes que envolvem as situações desejadas. Com o objetivo de investigar quais as possibilidades de se implementar uma Engenharia Didática[13] no desenvolvimento de atividades criptográficas relacionadas aos temas do Ensino Médio, Olgin (2011) propõe a aplicação das atividades selecionadas a alunos de uma escola estadual do terceiro ano do Ensino Médio.

[13] Engenharia Didática é uma metodologia de investigação, composta por um esquema experimental que se caracteriza por aplicações planejadas de atividades didáticas em sala de aula. Para mais informação ver em OLGIN, C. DE A. *Currículo no Ensino Médio: uma experiência com o tema criptografia*. 2011. 136 f. Mestrado – Universidade Luterana do Brasil, Canoas, 2011.

As atividades, além de abordarem os conteúdos já estudados pelos alunos, como função linear, função quadrática, função exponencial, função logarítmica e matrizes, trouxeram outros conhecimentos (diferentes tipos de cifras) para os mesmos. Os alunos tiveram, com essas atividades, a oportunidade de revisar, explorar, aprofundar e fixar os conteúdos já aprendidos e, também, de conhecer, na prática, as cifras de César, do Chiqueiro e de Playfair. Olgin (2011) ainda destaca que foi possível perceber que os alunos trabalharam em equipe durante a resolução das atividades. Ela ainda ressalta que esse tema abriu discussões acerca da utilização das calculadoras em sala de aula. Nas atividades em que se trabalharam as funções exponenciais e logarítmicas, essa ferramenta foi fortemente utilizada pelos alunos para auxiliá-los na resolução das operações. De acordo com ela, a calculadora "serviu de facilitador para cálculos longos. Esse item também foi uma ampliação aos conhecimentos dos alunos, pois já utilizavam a calculadora, mas não sabiam utilizar as teclas de potência, parênteses, cursores e não a utilizavam para resolver expressões" (OLGIN, 2011, p. 119–120).

Como resultados de sua pesquisa, Olgin (2011, p. 31) afirma que explorar a criptografia aliada aos conteúdos do Ensino Médio permite que "o estudante desenvolva habilidades que podem ser utilizadas no ambiente de trabalho e no convívio em sociedade". Além do trabalho em grupo e de oportunizar aos alunos reforçar os conteúdos já estudados, essas atividades permitiram que os mesmos "explorassem os diversos recursos da calculadora científica, facilitando-lhes os cálculos longos e a compreensão de conceitos matemáticos" (OLGIN, 2011, p. 121).

Corroborando Olgin (2011), os artigos de Oliveira e Kripka (2011) e Silva e Sousa (2013) também abordam a relevância da inserção da criptografia dentro da sala de aula. Oliveira e Kripka (2011) trazem atividades envolvendo as cifras de César e Vigenère e também a utilização das matrizes na cifração de mensagens por meio de transformações lineares, exemplo de atividade voltada ao Ensino Superior. De acordo com elas, o uso da criptografia dentro da sala de aula pode "ajudar aos educadores matemáticos na árdua tarefa de incentivarem seus educandos, uma vez que os conceitos de criptografia possibilitam inserir atividades lúdicas e diferenciadas em sala de aula" (OLIVEIRA; KRIPKA, 2011, p. 11).

Já o trabalho de Silva e Sousa (2013) apresenta o resultado de uma intervenção realizada pelo PIBID[14] em uma escola na qual exploraram os conceitos de funções e matrizes com os alunos por meio de atividades criptográficas. De acordo com eles, a "turma reagiu de maneira

[14] Programa Institucional de Bolsas de Iniciação à Docência.

satisfatória e todos os alunos dedicaram-se ao máximo à atividade que estava sendo proposta, demonstrando interesse e entusiasmo pela oficina" (SILVA; SOUSA, 2013, p. 6).

Seguindo a cronologia, no ano de 2013, ainda têm-se as pesquisas de Oliveira (2013), Santos (2013), Schürmann (2013), Marques (2013) e Rodrigues (2013). Os quatro primeiros autores abordam em seus trabalhos atividades envolvendo a criptografia aliadas aos conteúdos do Ensino Médio, além de darem uma atenção especial às orientações para os professores na forma como tais atividades podem ser desenvolvidas com os alunos. O último autor volta a sua pesquisa para o Ensino Fundamental e traz algumas aplicações das atividades propostas em seu trabalho. Oliveira (2013) narra o desâmino encontrado em seus alunos durante seus anos de atuação profissional. De acordo com ele, existia uma busca particular para modificar o cenário da sua sala de aula. Assim, quando teve a oportunidade de conhecer o tema criptografia, logo pensou em como poderia utilizar essa temática nas suas aulas do Ensino Médio. Então, ao desenvolver as atividades criptográficas com os alunos, a fim de trabalhar os conceitos de matrizes, Oliveira (2013) chegou às seguintes conclusões:

> Verificou-se também que em determinado grupo de alunos que estavam desanimados e cansados e já haviam abandonado a rotina escolar, ou seja, estavam na escola com outros objetivos diferentes do aprender nas aulas, desenvolveram de forma prazerosa e dinâmica as atividades em sala [...] Em relação aos alunos que se esforçam e tem objetivos direcionados para o pós ensino médio, ou seja, querem entrar em uma universidade, foram além e tentaram dificultar a encriptação de mensagem, oferecendo o desafio aos demais. (OLIVEIRA, 2013, p. 53).

A pesquisa de Oliveira (2013) mostra, claramente, as angústias de um professor quando este não consegue mais ter a atenção e o interesse dos alunos em suas aulas. Narrando suas próprias experiências e agonias, fazendo em sua conclusão um apelo aos seus leitores, a saber:

> Precisamos inovar. Urgentemente. Os alunos da escola pública estão esperando por isso. A aplicação dessa aula foi uma pequena experiência que demonstrou o quanto eles estão prontos para interagir e absorver os conteúdos propostos. A maneira pela qual conduzimos tal aprendizado faz a diferença no resultado final (OLIVEIRA, 2013, p. 55).

O trabalho de Santos (2013) apresenta uma seção mais densa sobre a teoria da criptografia, abordando conceitos mais complexos do Ensino Superior. Contudo, ele apresenta uma série de atividades envolvendo o ensino de funções, análise combinatória e matrizes. Para cada um desses conceitos, Santos (2013) desenvolve uma sequência de atividades que se interligam e exploram os conteúdos abordados, sempre aumentando a complexidade da

atividade. Já na pesquisa de Schürmann (2013), suas atividades, que envolvem somente o estudo de matrizes, são todas fundamentadas em uma releitura simplificada do drama shakespeariano *Romeu e Julieta*. O autor conseguiu dividir o drama em diversas partes e montou as atividades de cifração e decifração, envolvendo matrizes, de acordo com os trechos em que Romeu e Julieta trocavam mensagens. Tendo como objetivo central "apresentar aos professores de Matemática e demais interessados uma estratégia de ensino diferenciada para se ensinar Matemática de forma significativa" (SCHÜRMANN, 2013, p. 61), o autor argumenta que esse tipo de atividades pode auxiliar o ensino de matrizes para os alunos do segundo ano do Ensino Médio.

Marques (2013) explora em seu trabalho as relações binárias e os algoritmos discretos trazendo um estudo sobre as relações de equivalência e suas classes, sobre funções, grupos, grupos cíclicos, raízes primitivas e logaritmos discretos. Este autor ainda aborda sobre a criptografia Diffie-Hellman destacando o problema da distribuição de chaves, o uso das funções para solucionar esse problema e por fim o protocolo das trocas de chave de Diffie-Hellman. Como propostas de trabalhos com a criptografia em sala de aula, Marques (2013) apresenta três atividades, a primeira envolve a Cifra de César com uma função definida por várias sentenças, a segunda sobre matrizes e suas propriedades e por último a criptografia de Diffie-Hellman.

Os últimos trabalhos encontrados são de Arinos (2014), Souza Neto (2014) e França (2014), além do artigo de Litoldo e Lazari (2014). Arinos (2014) traz várias atividades em sua pesquisa, tanto para o Ensino Médio como para o Ensino Fundamental, e, também, reforça a utilização das mesmas para o ensino e aprendizagem dos alunos acerca dos conteúdos matemáticos. Corroborando Olgin (2011) em termos de tecnologia, Arinos (2014) afirma que:

> A forma atual em que a criptografia está inserida, induz a utilização de recursos tecnológicos, como a calculadora e o computador, proporcionando aos estudantes as competências e habilidades necessárias para a sua formação como cidadão de uma sociedade comprometida com o futuro (ARINOS, 2014, p. 84).

O trabalho de Souza Neto (2014), embora esteja voltado para o Ensino Básico, apresenta uma densa seção teórica sobre Aritmética Modular e Criptografia, e no final apresenta atividades mais adequadas a serem desenvolvidas no Ensino Superior. Já a pesquisa de França (2014), além de mostrar atividades para o professor envolvendo os conteúdos de função afim, função quadrática, função exponencial e logarítmica, matrizes e braile, dá uma atenção especial às criptografias digitais, trazendo um conteúdo resumido, mas interessante, sobre as

cifras simétricas DES, AES (Advanced Encription Standard) e IDEA (International Data Encryption Algorithm) e sobre as assimétricas RSA, ELGmal e Curvas Elípticas.

O artigo de Litoldo e Lazari (2014) apresenta uma análise desenvolvida nos livros didáticos que foram aprovados pelo PNLD – 2012. Em busca de alguma atividade que envolvesse o tema criptografia, foram analisadas três das cinco coleções aprovadas. Dentre as coleções examinadas, encontraram-se três situações em que se aborda o tema criptografia. Nas seções *Saiba Mais* e *Contexto*, os livros apresentaram um resumo sobre o que é a criptografia e trazem exemplos de atividades envolvendo o conceito da inversa da função afim e as operações de soma e multiplicação das matrizes. Como conclusão dessa análise, os autores ressaltaram que, embora o tema tenha aparecido nos livros didáticos, ele foi apresentado no final dos capítulos sem conexão com o livro como um todo.

Após esse mapeamento sobre as pesquisas já desenvolvidas, observa-se que a cada ano o desenvolvimento desse assunto vem crescendo. A prova disso é a quantidade maior de trabalhos encontrados nos dois últimos anos. Isso pode ser reflexo da proliferação dos cursos Nacionais[15] que abordam em seu currículo o tema criptografia e também do fato de que este tema, de uns tempos para cá, está se tornando mais presente na mídia, não só nas produções da teledramaturgia, mas também nos noticiários, em suas reportagens sobre espionagens nacionais e internacionais. Ainda, observa-se que as atividades criptográficas aliadas aos conteúdos do Ensino Básico começaram a ser mais bem desenvolvidas, sendo essas elaboradas em contextos mais interessantes, como é o exemplo apresentado no trabalho de Schürmann (2013).

A seguir, serão apresentados alguns trabalhos que abordam atividades envolvendo a criptografia com os conceitos e os pensamentos algébricos de função afim, conteúdo matemático do Ensino Médio escolhido para ser trabalhado nesta pesquisa.

3.4.1 Criptografia e função afim – o que já existe

Nesta seção, serão apresentados quais os conteúdos que os onze trabalhos acadêmicos abordaram em suas pesquisas, dando ênfase ao tema de funções e realizando uma descrição de algumas atividades que trabalham a função afim em um contexto criptográfico.

Alguns trabalhos, como é o caso de Souza Neto (2014), Oliveira (2013) e Schürmann (2013), focam suas pesquisas em apenas um conteúdo: matrizes. Já o restante dos trabalhos,

[15] Profmat – Mestrado Profissional em Matemática.

além de trazer atividades sobre matrizes, abordam também outros conteúdos, a saber, função afim, função quadrática, função exponencial, função logarítmica e função modular.

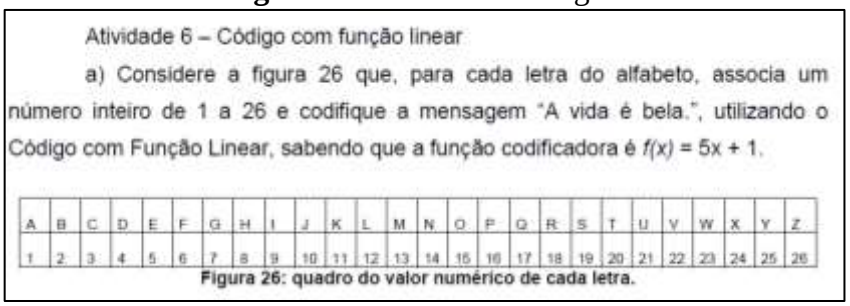
Atentando-se apenas para o conteúdo de função afim, observou-se que tal conteúdo foi abordado pelos oito trabalhos restantes. Dentre esses oito trabalhos, o conteúdo de função afim varia entre atividades que se referem apenas a utilização da expressão $f(x) = a \times x + b$ para se cifrar e decifrar as mensagens e atividades que sugerem algumas discussões acerca dos coeficientes *a* e *b* da função. Nota-se que em nenhum trabalho se explorou a parte gráfica da função afim, nem se abordaram as particularidades (função linear, função constante e função identidade), preterindo, também, as possíveis discussões sobre o crescimento e decrescimento dessa função. Acredita-se que o fato de tais trabalhos não explorarem a parte gráfica da função, suas particularidades e as faixas de crescimento e decrescimento da mesma se dá em virtude de que eles somente apresentam tais atividades como meios de revisão, fixação e exploração dos conteúdos já estudados. Abaixo serão apresentadas algumas dessas atividades e as orientações que os autores fazem para o professor, visando à aplicação das mesmas.

No trabalho de Fincatti (2010), antes de apresentar uma aplicação da criptografia com o conteúdo de função afim, a autora traz uma orientação para o professor, explicando quais seriam os pré-requisitos para essa atividade. De acordo com ela, "para ensinar função do primeiro grau, o aluno deve ter conhecimento da definição de funções, diagrama de flechas, domínio e contradomínio, gráficos, noções básicas do plano cartesiano, construção de gráficos e análise de gráficos" (FINCATTI, 2010, p. 52). Em seguida, a autora traz a definição de função afim, juntamente com a sua parte gráfica, relacionando o crescimento e decrescimento da função e as nomenclaturas dos coeficientes *a* e *b*. No entanto, ao apresentar a atividade de criptografia, ela orienta o professor a realizar uma demonstração de como decifrar uma mensagem e afirma que, fazendo isso, "o professor terá aguçado a curiosidade" (FINCATTI, 2010, p. 61) dos alunos. Continuando com as indicações, ela sugere que o professor distribua uma tabela relacionando o alfabeto a números e que ele explique como utilizar a função afim para cifrar uma mensagem. A partir de então, introduza a explicação do conteúdo de função afim. Depois, juntamente com os alunos, cifram e decifram uma mensagem utilizando tal função. Mesmo ela abordando os conceitos gráficos da função, na atividade apresentada, a construção do gráfico ou as discussões sobre o mesmo não ocorreram.

Olgin (2011) apresenta a atividade da Figura 3 em seu trabalho e, com a tabela apresentada, solicita que os alunos cifrem e decifrem algumas mensagens. A autora ainda

sugere outras funções afins, para que os alunos, utilizando a mesma tabela, façam os processos de cifração e decifração.

Figura 3 - Atividade de Olgin.



Atividade 6 – Código com função linear

a) Considere a figura 26 que, para cada letra do alfabeto, associa um número inteiro de 1 a 26 e codifique a mensagem "A vida é bela.", utilizando o Código com Função Linear, sabendo que a função codificadora é $f(x) = 5x + 1$.

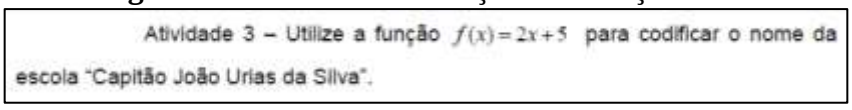
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Figura 26: quadro do valor numérico de cada letra.

Fonte: Olgin (2011).

O trabalho de Rodrigues (2013) apresenta uma atividade, solicitando que os alunos cifrem uma frase, como mostra a Figura 4. A autora argumenta que o assunto de função afim não foi aprofundado com os alunos, porque estes eram do nono ano, e que caberia ao primeiro ano do Ensino Médio abordar as questões de injetividade, sobrejetividade e bijeção da função. Ela ainda traz outras atividades (Figuras 5 e 6), uma solicitando que os grupos troquem mensagens cifradas entre si e outra que o aluno decifre a mensagem apresentada com uma nova função afim.

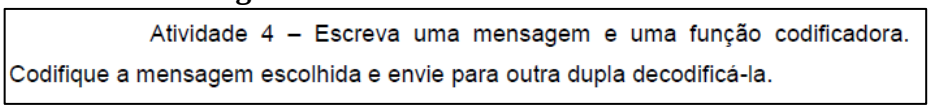
Figura 4 - Atividade de cifração com função afim.



Atividade 3 – Utilize a função $f(x) = 2x + 5$ para codificar o nome da escola "Capitão João Urias da Silva".

Fonte: Rodrigues (2013, p. 24).

Figura 5 - Atividade de trocas de cifras.



Atividade 4 – Escreva uma mensagem e uma função codificadora. Codifique a mensagem escolhida e envie para outra dupla decodificá-la.

Fonte: Rodrigues (2013, p. 28).

Figura 6 - Atividade de decifração com função afim.

Atividade 5: Decodifique a mensagem a seguir sabendo que a função codificadora usada foi $f(x) = 5x + 3$:

1305643 – 556078 – 1214998 – 1307613 – 599628 – 1509618 – 599558 – 1561058.

Fonte: Rodrigues (2013, p. 30).

Como conclusão de seu trabalho, Rodrigues (2013) afirma que a criptografia é:

> Capaz levar o aluno a atribuir significado ao conceito de função na etapa final do Ensino Fundamental. Além de possibilitar ao professor opções para desenvolver atividades diferenciadas e divertidas que auxiliem a fixação, revisão e aprofundamento do conceito de função e relações algébricas, (...) [além se ser também] uma ótima ferramenta para ajudar os alunos na construção empírica do conhecimento sobre funções inversas (RODRIGUES, 2013, p. 32).

Na pesquisa de Marques (2013), a função afim é trabalhada em um sistema de várias sentenças. O autor define a função que será utilizada na atividade (Figura 7) e, depois de realizar um exemplo de cifração, solicita que a frase "**eu amo criptografia"** seja cifrada. Ele também pede a representação dessa função por meio de diagramas utilizando o esquema de flechas (esse esquema foi apresentado por ele no decorrer de sua pesquisa) e questiona se existem letras que não terão representação no texto cifrado. Marques (2013) argumenta que os objetivos específicos dessa atividade seriam: a) o reconhecimento de uma função definida por várias sentenças; b) o cálculo dessa função para as letras do alfabeto; c) a retomada da ideia de diagramas representados por esquemas de flechas; e d) a relação entre uma função definida por várias sentenças e o processo de cifração e decifração de mensagens.

Figura 7 - Função definida em duas sentenças.

Atividade

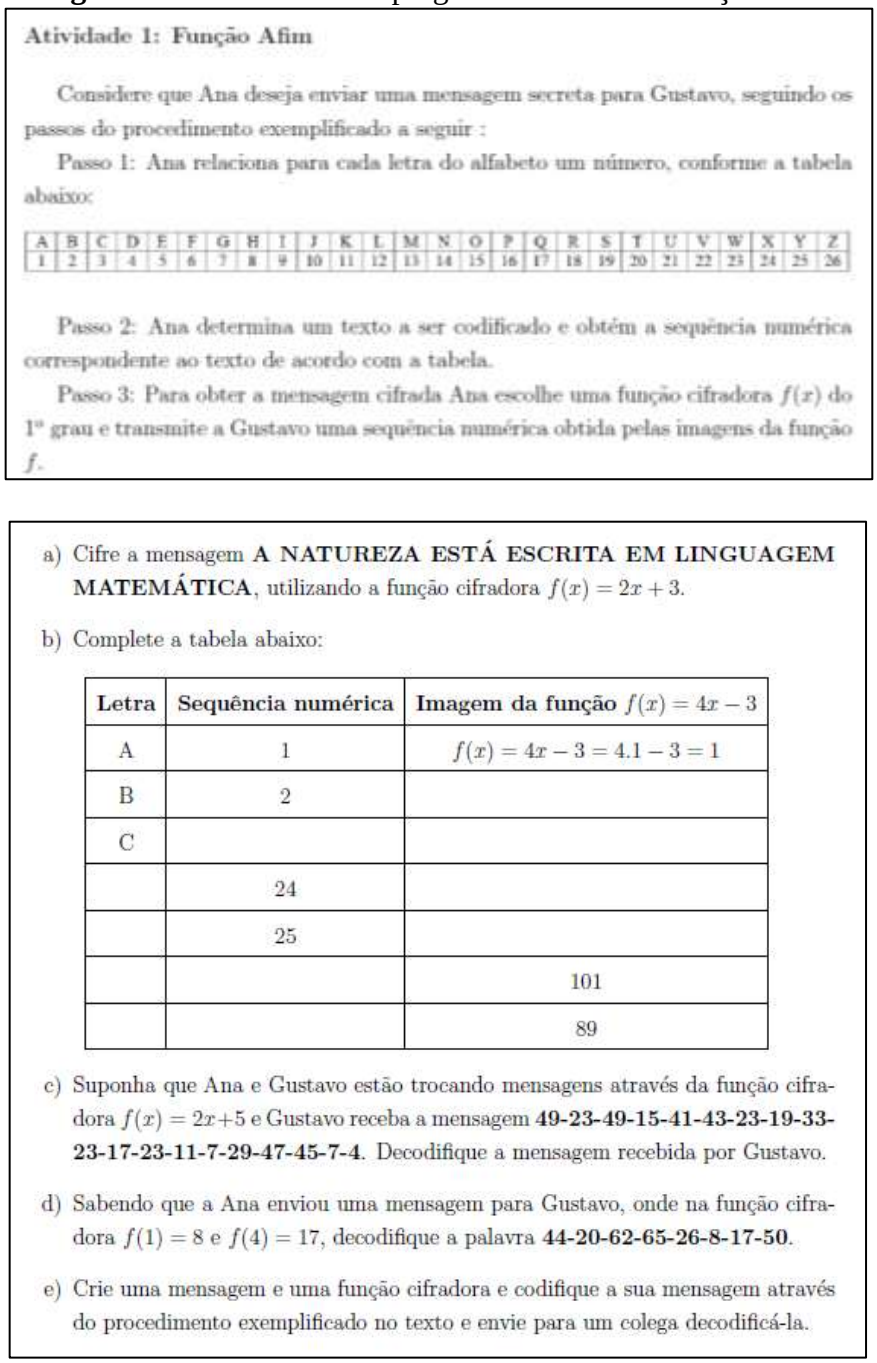
A função $f : \mathbb{N}^* \to \mathbb{N}^*$, definida por $f(x) = \begin{cases} 2x+1, \text{ se } x \leq 12 \\ x, \text{ se } x > 12 \end{cases}$, será responsável pela codificação de mensagens cujas letras estarão associadas com os números da tabela a seguir:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Fonte: Marques (2013, p. 52-53).

Já os trabalhos de França (2014), Santos (2013) e Arinos (2014) trazem atividades que aprofundaram o conceito. Por exemplo, França (2014) propõe, em seu objetivo geral, que tal atividade explore "o conceito de função polinomial do 1º grau na criptografia, visando uma aprendizagem contextualizada e significativa" (FRANÇA, 2014, p. 39). Para tanto, a atividade (Figura 8) trabalha o cálculo e a determinação da imagem da função, a resolução de sistemas lineares, a obtenção da função afim por meio de dois pontos e a resolução de problemas que envolvam o conceito de função.

Figura 8 - Atividade de criptografia utilizando a função afim.



Atividade 1: Função Afim

Considere que Ana deseja enviar uma mensagem secreta para Gustavo, seguindo os passos do procedimento exemplificado a seguir :

Passo 1: Ana relaciona para cada letra do alfabeto um número, conforme a tabela abaixo:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Passo 2: Ana determina um texto a ser codificado e obtém a sequência numérica correspondente ao texto de acordo com a tabela.

Passo 3: Para obter a mensagem cifrada Ana escolhe uma função cifradora $f(x)$ do 1º grau e transmite a Gustavo uma sequência numérica obtida pelas imagens da função f.

a) Cifre a mensagem **A NATUREZA ESTÁ ESCRITA EM LINGUAGEM MATEMÁTICA**, utilizando a função cifradora $f(x) = 2x + 3$.

b) Complete a tabela abaixo:

Letra	**Sequência numérica**	**Imagem da função** $f(x) = 4x - 3$
A	1	$f(x) = 4x - 3 = 4.1 - 3 = 1$
B	2	
C		
	24	
	25	
		101
		89

c) Suponha que Ana e Gustavo estão trocando mensagens através da função cifradora $f(x) = 2x+5$ e Gustavo receba a mensagem **49-23-49-15-41-43-23-19-33-23-17-23-11-7-29-47-45-7-4**. Decodifique a mensagem recebida por Gustavo.

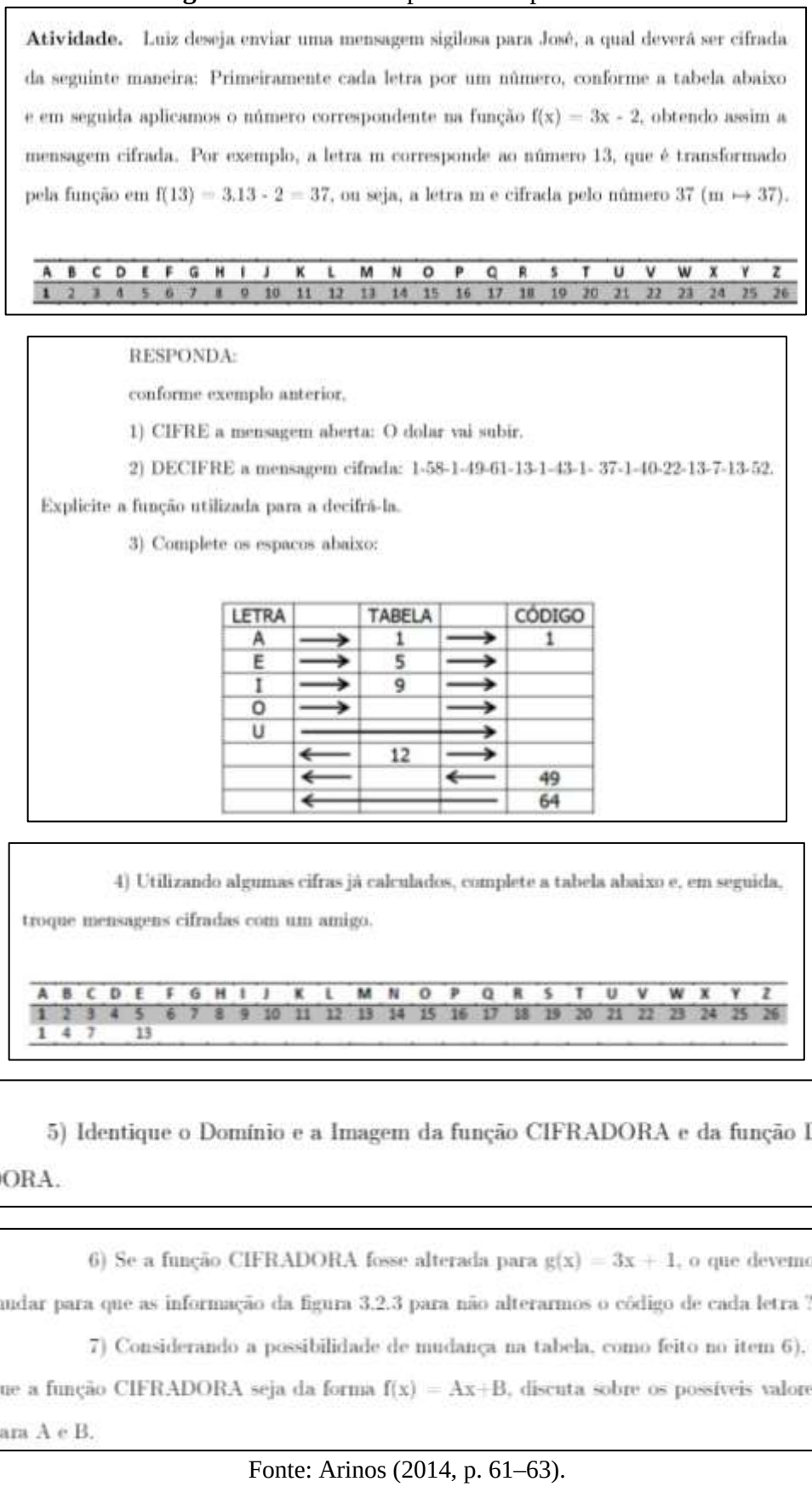
d) Sabendo que a Ana enviou uma mensagem para Gustavo, onde na função cifradora $f(1) = 8$ e $f(4) = 17$, decodifique a palavra **44-20-62-65-26-8-17-50**.

e) Crie uma mensagem e uma função cifradora e codifique a sua mensagem através do procedimento exemplificado no texto e envie para um colega decodificá-la.

Fonte: França (2014, p. 40-42).

De modo parecido com a atividade apresentada acima, Arinos (2014) também propõe a cifração e a decifração de uma mensagem e o preenchimento de uma tabela. No entanto, ele traz questões sobre o domínio e imagem da função cifradora, como mostra a Figura 9. O autor argumenta que essa atividade tem como objetivo "introduzir a criptografia em sala de aula como fator motivacional para verificar a aprendizagem dos alunos com respeito a funções inversas" (ARINOS, 2014, p. 60).

Figura 9 - Atividade apresentada por Arinos.



Atividade. Luiz deseja enviar uma mensagem sigilosa para José, a qual deverá ser cifrada da seguinte maneira: Primeiramente cada letra por um número, conforme a tabela abaixo e em seguida aplicamos o número correspondente na função $f(x) = 3x - 2$, obtendo assim a mensagem cifrada. Por exemplo, a letra m corresponde ao número 13, que é transformado pela função em $f(13) = 3.13 - 2 = 37$, ou seja, a letra m e cifrada pelo número 37 ($m \mapsto 37$).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

RESPONDA:

conforme exemplo anterior,

1) CIFRE a mensagem aberta: O dolar vai subir.

2) DECIFRE a mensagem cifrada: 1-58-1-49-61-13-1-43-1- 37-1-40-22-13-7-13-52. Explicite a função utilizada para a decifrá-la.

3) Complete os espacos abaixo:

LETRA		TABELA		CÓDIGO
A	→	1	→	1
E	→	5	→	
I	→	9	→	
O	→		→	
U	→		→	
	←	12	→	
	←		←	49
	←			64

4) Utilizando algumas cifras já calculados, complete a tabela abaixo e, em seguida, troque mensagens cifradas com um amigo.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	4	7		13																					

5) Identique o Domínio e a Imagem da função CIFRADORA e da função DECIFRADORA.

6) Se a função CIFRADORA fosse alterada para $g(x) = 3x + 1$, o que devemos mudar para que as informação da figura 3.2.3 para não alterarmos o código de cada letra ?

7) Considerando a possibilidade de mudança na tabela, como feito no item 6), e que a função CIFRADORA seja da forma $f(x) = Ax+B$, discuta sobre os possíveis valores para A e B.

Fonte: Arinos (2014, p. 61–63).

Santos (2013) descreve com mais detalhes as orientações para o professor a respeito da aplicação da atividade. Chamando de *Ações Didáticas*, ele sugere que o trabalho com os alunos seja desenvolvido em grupos e que cada aluno tenha uma função nesse grupo: líder, executor, relator e verificador. De acordo com ele, cada uma dessas funções seria um modo de organizar e incentivar o trabalho em grupo. Ele também orienta sobre a utilização de uma calculadora para facilitar os cálculos e sobre o tempo mínimo de duração da atividade. Como objetivo, Santos (2013, p. 51) afirma que tal atividade (Figura 10) servirá para explorar "o conceito básico de função no sentido de transformação, o cálculo da imagem de um elemento do domínio da função, a determinação da inversa de uma função bijetora e o cálculo da pré-imagem de um elemento da imagem".

Com as descrições dos trabalhos encontrados e com o detalhe das atividades apresentadas, espera-se ter dado condições para que o leitor tenha compreendido o desenvolvimento do entrelaçamento da Criptografia e da Educação Matemática, propiciando uma visão panorâmica dos trabalhos já desenvolvidos e que, com isso, ele possa compreender o diferencial da atual pesquisa. O atual trabalho não se restringe em apresentar atividades envolvendo a criptografia com o conteúdo de função afim, tendo como objetivo explorar, fixar ou revisar esse conteúdo, e nem de oferecer orientações aos professores sobre as atividades e suas aplicações, mas sim, tentar compreender em que atividades pedagógicas envolvendo problemas de criptografia pode auxiliar os alunos na exploração das ideias associadas à função afim.

Figura 10 - Atividade apresentada por Santos.

Atividade:

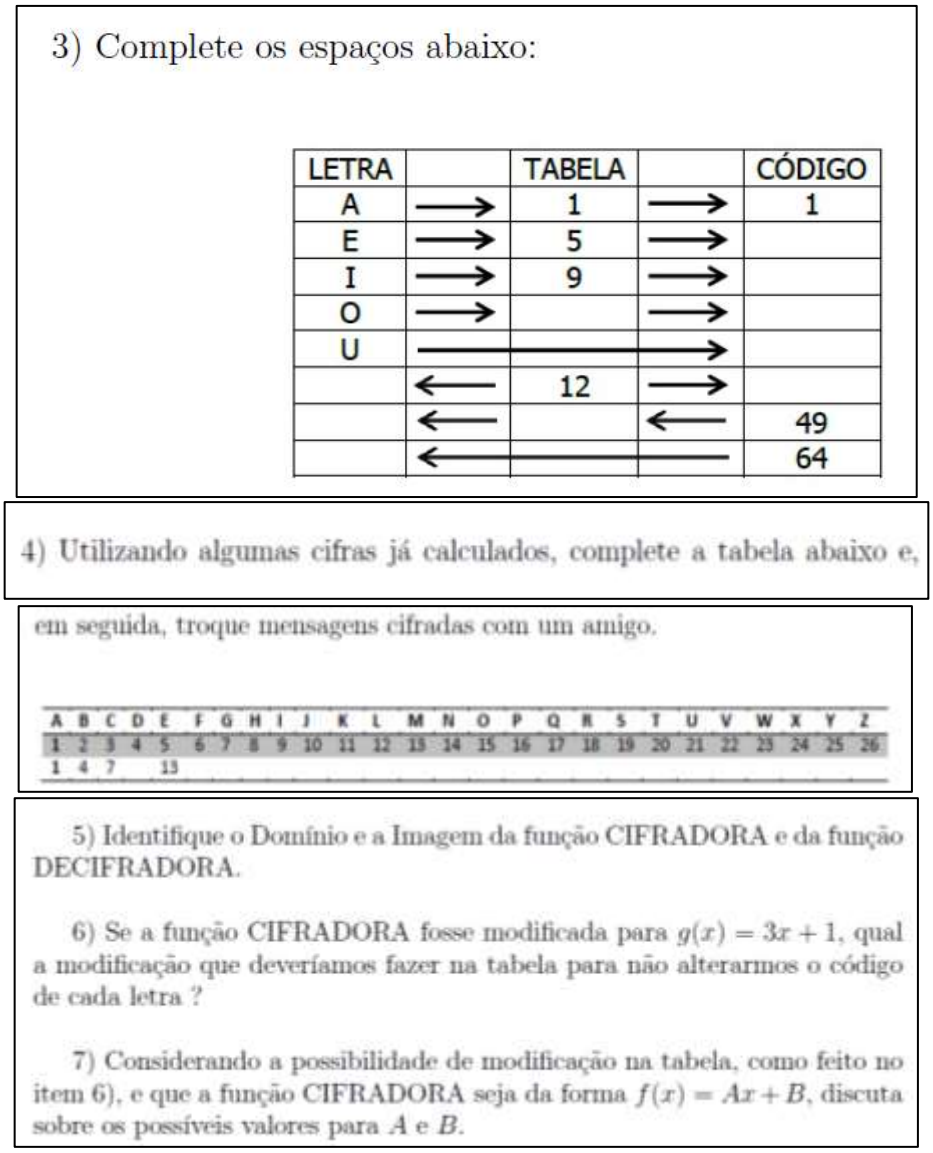
Luiz deseja enviar uma mensagem sigilosa para José, a qual deverá ser cifrada substituindo-se cada letra por um número, conforme a tabela abaixo, aplicando o número correspondente na função $f(x) = 3x - 2$, obtendo a mensagem cifrada. Por exemplo, a letra m corresponde ao número 13, que é transformado pela função em $f(13) = 3 \times 13 - 2 = 37$, ou seja, a letra m é cifrada pelo número 37 ($m \mapsto 37$).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

RESPONDA:

1) CIFRE a mensagem aberta: *O dólar vai subir.*

2) DECIFRE a mensagem cifrada: $1-58-1-49-61-13-1-43-1-37-1-40-22-13-7-13-52$. Explicite a função utilizada para a decifração.



3) Complete os espaços abaixo:

LETRA		TABELA		CÓDIGO
A	→	1	→	1
E	→	5	→	
I	→	9	→	
O	→		→	
U	→		→	
	←	12	→	
	←		←	49
	←			64

4) Utilizando algumas cifras já calculados, complete a tabela abaixo e, em seguida, troque mensagens cifradas com um amigo.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	4	7		13																					

5) Identifique o Domínio e a Imagem da função CIFRADORA e da função DECIFRADORA.

6) Se a função CIFRADORA fosse modificada para $g(x) = 3x + 1$, qual a modificação que deveríamos fazer na tabela para não alterarmos o código de cada letra ?

7) Considerando a possibilidade de modificação na tabela, como feito no item 6), e que a função CIFRADORA seja da forma $f(x) = Ax + B$, discuta sobre os possíveis valores para A e B.

Fonte: Santos (2013, p. 52–53).

3.4.2 Criptografia e função afim – o que foi criado

A sequência pedagógica de atividades criadas, que podem ser vistas em sua totalidade no Apêndice B, levou em consideração toda a esfera de definições sobre o que é um problema e de como ele pode ser proposto os alunos, bem como o ambiente proporcionado pelo pesquisador para o desenvolvimento das atividades. A seguir, a Tabela 1 é apresentada, contendo o nome da atividade, sua descrição, seu objetivo, a quantidade de encontros, e de alunos, as datas dos encontros e os destaques ocorridos durante o desenvolvimento das atividades. A apresentação dos sujeitos da pesquisa, a maneira como foi realizada a escolha dos alunos, bem como se deu os encontros serão dissertados em seguida na seção os participantes da pesquisa.

Tabela 1 - Atividades

NOME DA ATIVIDADE	DESCRIÇÃO DA ATIVIDADE	OBJETIVO DA ATIVIDADE	DURAÇÃO DAS ATIVIDADES (ENCONTROS)	DATA DOS ENCONTROS	ALUNOS PRESENTES
SI-LÁ-BOX	Desenvolvida com um alfabeto em símbolos, a atividade consistia em um pergunta principal. Para responder a essa pergunta, a atividade trazia uma série de dicas. Cada dica tinha que ser respondida em sílabas e, no final, algumas sílabas em destaque formavam uma frase que respondia à pergunta principal. Cada letra correspondia a um símbolo e símbolos iguais representavam letras iguais.	O objetivo da atividade era de apresentar aos alunos a criptografia.	1 (um)	05/05/2014	7 (sete)
DESTAQUES OCORRIDOS: Para apresentar a criptografia aos alunos, foi preparado uma apresentação, em Power Point, com um breve relato sobre o que é a criptografia e sobre sua evolução com o passar dos tempos[16]. Realizar essa apresentação para os alunos foi importante, pois, esse momento oportunizou a eles conhecerem um pouco sobre sua história e para exemplificar algumas cifras as quais poderiam, futuramente, auxiliá-los na resolução das atividades. Para complementar tal apresentação, um vídeo intitulado "Criptografia, Chave privada e Chave pública" da série *Matemática Multimídia* foi passado aos alunos com o intuito de mostrar a eles como a criptografia está presente no cotidiano da sociedade. O vídeo apresentava uma série de conceitos sobre as ideias de chave simétrica, assimétrica e sobre a operação módulo. Após toda essa apresentação, um aluno se manifestou dizendo que seria interessante se eles aprendessem as operações que apareceram no vídeo. Ao observar que os restantes dos alunos também gostariam de rever os cálculos do vídeo, um material foi elaborado posteriormente para ser aplicado no próximo encontro, abordando a operação módulo e seu significado dentro das ideias associadas à chave simétrica e assimétrica.					

[16] Para realizar essa apresentação a pesquisadora baseou-se no resumo da evolução da criptografia, o qual pode ser lido no Apêndice C.

UM CASO DE SEQUESTRO	Um conto fictício sobre o sequestro do professor de um professor de matemática foi apresentado aos alunos e, com ele, uma carta criptografada que, segundo o conto, continha o paradeiro do professor, quem o havia sequestrado e o motivo do sequestro. O conto solicitava a ajuda dos alunos para decifrar a carta criptografada e resolver o enigma. No final da atividade, uma ficha de perguntas foi entregue aos alunos, a qual contemplava perguntas sobre o enigma da carta e pedia que eles identificassem a relação utilizada para se criptografar a carta e de que maneira eles poderiam representar essa cifração por meio de um esquema.	Essa atividade tinha como objetivo introduzir para os alunos a ideia de conjunto, variável e de expressão matemática, por meio da cifração das letras do alfabeto.	2 (dois)	08/05/2014	6 (seis)
DESTAQUES OCORRIDOS: Os alunos iniciaram a atividade com posturas mais investigativas. Começaram levantando hipóteses de enumeração do alfabeto para tentar decifrar a carta criptografada. Observando que suas conjecturas acerca do alfabeto cifrado não estavam fazendo sentido na decifração da carta, os alunos relembraram da atividade anterior, na qual lhes foi apresentado a Cifra de César. Recordado que essa cifra desloca o alfabeto quatro casas a esquerda, os alunos conseguiram decifrar a carta criptografada. A expressão "alfabeto normal" foi assumida por um dos grupos para designar o alfabeto enumerado do n.º 1 ao n.º 26. Esse termo acabou sendo assumido por todos os alunos até o final dos encontros. Durante as discussões sobre a atividade, os alunos ajudaram a pesquisadora a escrever o deslocamento do alfabeto por meio de uma expressão matemática e durante tal discussão, pode-se observar que os alunos haviam compreendido a ideia de se representar a mudança das letras por uma letra x e que na sua expressão matemática a letra x representava a variável dessa expressão. No final dessa atividade, os alunos mostraram indícios de que haviam assimilado a ideia do que seria um conjunto, de como associar a mudança das letras do alfabeto a uma variável *x*, e de como representar a cifração dessas letras por meio de uma expressão matemática entre dois conjuntos.				

O DETETIVE WATSON	Essa atividade se constituía em um conto que convidava os alunos a decifrar cinco pistas que, juntas, desvendavam o mistério do conto. As pistas foram cifradas utilizando-se a enumeração do alfabeto a partir do número um, mas, para cada pista, foi utilizada uma função afim diferente. Essas pistas foram apresentadas aos alunos como um quebra-cabeça e, ao montar o quebra-cabeça, os alunos percebiam certa ordem da decifração de cada uma. Essa ordem foi estabelecida para que os alunos fossem percebendo que as decifrações das pistas iam se tornando mais complexas. Após essas decifrações, uma ficha de perguntas sobre elas foi entregue aos alunos. Nessa ficha, havia tanto perguntas que abordavam o mistério desvendado no conto quanto perguntas sobre os modos de cifração. Em relação às perguntas sobre os modos de cifração, foi pedido aos alunos, primeiramente, que identificassem e escrevessem o modo que foi utilizado para se criptografar cada pista, em seguida, que eles observassem as semelhanças e diferenças entre esses modos. Na questão seguinte, pedia-se que os alunos	O objetivo inicial dessa atividade era fazer com que os alunos identificassem os diferentes modos utilizados na cifração das pistas e, com isso, saber expressar esses modos em forma de expressões matemáticas. Com a identificação dessas expressões, esperava-se que os alunos fizessem uma análise sobre elas e conseguissem chegar à generalização da expressão da função afim.	4 (quatro)	22/05/2014	7 (sete)

	escrevessem, em forma de expressões matemáticas, os modos identificados e que justificassem essas expressões. Antes da pergunta que pedia aos alunos a generalização da expressão matemática que estava sendo utilizada para cifrar as pistas, havia algumas perguntas convidando os alunos a pensar e escolher uma nova expressão matemática com base nas expressões encontradas, e que, com ela, cifrassem um de seus nomes.				
DESTAQUES OCORRIDOS: Os alunos identificaram logo no início que as pistas faziam parte de um quebra-cabeça e após realizar sua montagem, começaram a decifrá-las. A exploração das expressões matemáticas utilizadas na cifração das pistas ocorreu durante a resolução da atividade, bem como, durante sua discussão com todos os alunos. Os alunos também perceberam e evidenciaram para a pesquisadora as várias estratégias de resolução encontradas por eles para decifrar as pistas. A grande discussão que movimentou essa atividade girou em torno de que maneira se poderiam representar as mudanças ocorridas no alfabeto normal, por meio de uma expressão matemática. Conforme os alunos iam decifrando as pistas, eles exploravam mais as ideias de se encontrar uma expressão para auxiliá-los na decifração das pistas. A dúvida sobre o que era "escrever de modo geral", questão da ficha de perguntas acerca da generalização da expressão da função afim, gerou discussões. Para alguns alunos, um exemplo de expressão já representava seu modo geral, já para outros, o "escrever de modo geral" tinha que representar as mesmas características das expressões das pistas, mas sem ser propriamente um exemplo. Essas discussões sobre a generalização da expressão da função afim conduziram para a introdução dos termos: coeficientes *a* e *b* da função e em conjunto com os alunos houve a construção de uma expressão que pudesse representar sua generalização.					
O POEMA	Essa atividade solicitava que os alunos sorteassem dois números entre 1 e 9. Com esses números, os alunos teriam que designar qual seria o coeficiente *a* e qual seria o coeficiente *b*. Feito isso,	Essa atividade tinha como objetivo resgatar as discussões feitas no encontro anterior sobre a definição de função	1 (um)	05/06/2014	2 (dois)

	cada aluno construiria sua função afim e, a partir dela, cifraria uma frase. A junção de todas as sete frases (uma para cada aluno) se constituiria no poema Soneto da Fidelidade, de Vinicius de Morais. Ao terminar a cifração, os alunos trocariam entre si as frases e teriam, como meta, descobrir a frase cifrada e quais foram as funções afins criadas pelos seus colegas para cifrá-la.	afim e sobre seus coeficientes *a* e *b*. Ela também marcou o encerramento dos encontros do primeiro semestre exigindo dos alunos criatividade, organização nas estratégias de cifração e a retomada das ideias discutidas anteriormente sobre função afim.			
DESTAQUES OCORRIDOS: Após entender o que a atividade solicitava, foram sorteados, para os alunos, os números para a formação de sua função afim. Em seguida, os alunos criaram suas funções e iniciaram a cifração de uma frase do poema. Cada aluno organizou a sua função e a sua frase de um modo, resultando em diferentes estratégias de cifração. Um aspecto interessante foi o depoimento dos alunos dizendo que a decifração havia sido uma tarefa mais fácil do que a cifração, já que para cifrar as letras era necessário ter muito cuidado e atenção, para que erros de cifração não ocorressem. De acordo com eles, a chance de erras na cifração das letras era muito grande e essa atenção redobrada dificultava o processo de cifração.					
CRIPTOGRAMA	Essa atividade apresentava aos alunos um conto fictício e, com ele, um criptograma a ser decifrado. O conto narrava aos alunos uma conversa entre Sherlock Holmes e o Dr. Watson a respeito da criptografia e da Criptoanálise, retomando, em seu texto, a representação do esquema criptográfico, por meio de conjuntos. O conto solicitava que os alunos	Essa atividade tinha como objetivo introduzir a parte gráfica da função afim e trazer uma discussão sobre a diferença entre conjuntos discretos e conjuntos contínuos e de como esses conjuntos interferem na	1 (um)	21/07/2014	4 (quatro)

	decifrassem o criptograma para descobrir qual o conceito matemático que Holmes havia utilizado para cifrar tal criptograma. No final da atividade, uma ficha de perguntas foi entregue aos alunos. A ficha de perguntas contemplava questões sobre qual o conceito matemático que havia surgido nas casas em destaque do criptograma, qual a função afim que havia sido utilizada para cifrá-lo e, por último, pedia que os alunos representassem o esquema criptográfico por meio de um plano cartesiano.	representação gráfica das funções em geral.			
DESTAQUES OCORRIDOS: Os alunos iniciaram as resoluções das atividades com estratégias bem próximas das utilizadas nas atividades anteriores, contudo, depois de um tempo, alguns alunos se recordaram das discussões feitas anteriormente sobre as expressões matemáticas que representam uma função afim, assim, esses alunos iniciaram uma busca pelos valores dos coeficientes *a* e *b* que satisfizessem a cifração utilizada na atividade. A construção dos gráficos solicitou que os alunos relembrassem do plano cartesiano e explorassem seus eixos de acordo com os alfabetos (cifrados e decifrados). Uma conversa acerca da diferença entre conjuntos discretos e contínuos foi realizada, no entanto, essas questões não geraram grandes discussões com os alunos.					
	Um conto fictício foi apresentado aos alunos e, com ele, uma figura contendo seis gráficos de função afim. A narrativa apresentava aos alunos uma situação em que Sherlock Holmes era posto à prova e em que, nesse jogo, sua derrota representaria a morte de uma celebridade. De acordo com o conto,	Essa atividade tinha como objetivo trabalhar com os alunos a parte gráfica da função afim, de modo a abordar essa função por meio de seus gráficos e discutir as análises que podem ser			

O JOGO	Holmes teria recebido durante um mês seis mensagens cifradas e, nelas, havia o nome da celebridade que estava correndo perigo de morte; no entanto, Holmes não havia conseguido decifrar as pistas, mas havia montado um esquema de gráficos, em que cada gráfico correspondia a uma função de cada pista. A tarefa dos alunos era ajudar Holmes a relacionar cada gráfico com cada mensagem, por meio de sua função. No final da atividade, uma ficha de perguntas foi entregue aos alunos. A ficha de perguntas contemplava questões sobre: o processo de identificação de cada função; para que valores de *x* cada função atingia o zero; a partir de que valor cada função se tornava maior ou menor que zero; a mensagem formada pelas mensagens cifradas; uma análise sobre os coeficientes *a* e *b* de cada função, de acordo com suas semelhanças e diferenças; a classificação das funções em crescentes ou decrescentes e a generalização de quando uma função afim é crescente ou decrescente.	feitas sobre ele, de acordo com cada função afim.	6 (seis)	31/07/2014	5 (cinco)
DESTAQUES OCORRIDOS: Recordando dos encontros anteriores, alguns alunos iniciaram a resolução da atividade já buscando encontrar os valores dos coeficientes *a* e *b* que satisfizessem cada gráfico. Intuitivamente, os alunos analisavam os gráficos e denominavam os valores para alguns pontos, conseguindo assim, montar algumas expressões. Com as discussões de como se poderiam encontrar as funções dos gráficos sem ter que ficar “chutando” os valores de *a* e *b* foi explicado aos alunos sobre o significado de pontos no plano cartesiano e de					

como, por meio de dois pontos, se poderiam encontrar a função do gráfico que passa por eles. Ao longo dessa atividade os alunos demonstraram uma maior organização dos cálculos referentes ao alfabeto cifrado e um pensamento mais estruturado que se refletiu em suas falas, as quais já eram mais articuladas. Durante essa atividade, surgiu o interesse dos alunos em levar as atividades para a casa, situação que se propagou para as outras atividades até o final dos encontros.					
O POETA ASSASSINO	A atividade apresentava aos alunos um poema cifrado e, junto com cada linha do poema, sua função afim cifradora. A atividade trazia um conto sobre um poeta assassino. A cada crime que o poeta cometia, ele deixava com a vítima um poema que continha pistas sobre seu próximo crime. No entanto, esse poema era todo cifrado. Assim, os alunos foram convidados a decifrarem o poema para tentar descobrir quais eram as pistas deixadas pelo poeta sobre a sua próxima vítima, o local onde o crime ocorreria e seu motivo.	Essa atividade tinha como objetivo trabalhar com os alunos as ideias de função inversa e, mais especificamente, levá-los a construir as funções afins inversas de cada uma apresentada.	2 (dois)	05/09/2014	5 (cinco)
DESTAQUES OCORRIDOS: A discussão dessa atividade girou em torno de como os alunos haviam decifrado as frases do poema. Inicialmente, os alunos argumentaram que a estratégia que eles estavam utilizando estava sendo muito demorada e cansativa, de modo que eles sentiram necessidade de buscar um mecanismo mais rápido para decifrarem as frases. Assim, durante a resolução da atividade, a pesquisadora introduziu a discussão de como se poderia desenvolver uma estratégia que lhes desse uma decifração mais rápida dos números. Com a utilização de alguns exemplos, a pesquisadora introduziu a ideia de função inversa, sem designar essa operação por esse nome. Somente depois de realizar tal operação com a função genérica, é que a pesquisadora trouxe a nomenclatura para os alunos. Entretanto, não houve uma formalização do conceito de função inversa. No final da atividade, os alunos escreverem na ficha de perguntas como eles haviam descoberto a maneira mais fácil, prática e rápida de encontrar as letras cifradas.					
	A atividade se constituía em histórias criadas pelos próprios alunos. A solicitação	O objetivo dessa atividade é colocar os alunos numa			

CIFRANDO SUA HISTÓRIA	da criação dessas histórias foi realizada pela pesquisadora em alguns encontros anteriores. Os alunos criaram seus enigmas, entregaram para a pesquisadora, e esta apenas digitou as histórias, separando as partes misteriosas que os próprios criadores cifrariam. Assim, os alunos receberam suas próprias histórias e criaram suas funções cifradoras, cifrando, assim, as partes enigmáticas de suas produções.	situação em que eles fossem os cifradores das mensagens, já que a maioria das atividades havia exigido apenas posturas de decifradores. Na posição de cifrador, o aluno tem a oportunidade e a autonomia de escolher a transformação cifradora das mensagens. No entanto, a única exigência feita para os alunos era que eles escolhessem uma função afim como sendo a transformação cifradora. A atividade também marcou o encerramento dos encontros e, consequentemente, o encerramento do projeto com os alunos na escola.	1 (um)	23/09/2014	3 (três)
DESTAQUES OCORRIDOS: Nessa atividade os alunos utilizaram muito a criatividade, montando suas histórias. Houve uma concentração e organização muito grande por parte dos alunos para a cifração dos mistérios de suas próprias histórias. A troca dos enigmas e a tentativa de descobrir o mistério que o amigo criou junto com a função utilizada para cifrar as partes misteriosas da história fez com que os alunos ficassem muito concentrados na atividade. Durante as discussões para tentar descobrir os mistérios da história, observou-se que os alunos tentavam explorar as ideias discutidas sobre função afim junto com a investigação das partes cifrados da história.					

Fonte: Construído pela pesquisadora (2016).

3.5 Os p4rticip4ntes da p3squ1sa

Nesta seção, serão apresentados, de maneira geral, os sujeitos da pesquisa, bem como o ambiente em que o trabalho de campo ocorreu.

3.5.1 Os estudantes

A decisão de trabalhar com alunos do primeiro ano do Ensino Médio se apoiou no Currículo do Estado de São Paulo (SÃO PAULO, 2011), que traz em documento um quadro de conteúdos que insere a consolidação do tema função afim nessa série. Em decorrência, os alunos iniciaram os encontros com a pesquisadora antes de terem, em suas aulas regulares, o contato com o conceito de função afim.

Essa opção se deu em virtude do objetivo proposto pela pesquisa: compreender em que atividades pedagógicas envolvendo problemas de criptografia pode auxiliar os alunos na exploração das ideias associadas à função afim. Nesse sentido, as potencialidades de tais atividades melhor seriam investigadas se os sujeitos da pesquisa ainda não tivessem estudado tal assunto nas aulas regulares. Os alunos do segundo e terceiro anos não se enquadram nos objetivos de pesquisa, visto que tais alunos já teriam tido contato com esse tema com mais detalhes e, teoricamente, já teriam o conceito de função afim bem estabelecido.

Esta pesquisa poderia até ter sido desenvolvida com alunos do nono ano, no entanto essa opção foi desconsiderada por alguns motivos. Inicialmente, existia um interesse preliminar da pesquisadora em trabalhar com alunos do Ensino Médio, em virtude de sua afinidade com o público que o constitui e, em segundo lugar, ao escolher o tema função afim, desejava-se construir atividades envolvendo problemas criptográficos que abordassem alguns tópicos que constituem esse tema, a saber, as relações ou associações entre grandezas; correspondência entre elementos de dois conjuntos; “regra” ou “lei de formação” envolvendo as grandezas; compreensão da construção gráfica de funções afins; caracterização de crescimento e decrescimento das funções afins, entre outros.

Ao recorrer ao Currículo do Estado de São Paulo (SÃO PAULO, 2011) e verificar em qual ano os tópicos citados acima se enquadravam, observou-se que, segundo o currículo, no nono ano o tema função afim é abordado introduzindo-se as noções básicas sobre função, a ideia de variação e a construção de tabelas e gráficos para a sua representação. Já no primeiro ano do Ensino Médio, a orientação é a construção dos conhecimentos mais abrangentes a respeito de função afim. Deste modo, é nesse ano que é proposta a aprendizagem da relação

entre grandezas, a qual engloba todos os tópicos requeridos primeiramente para o desenvolvimento destas atividades. Assim, diante de tal situação, ficou decido que os sujeitos da pesquisa seriam alunos do primeiro ano do Ensino Médio.

Os encontros entre a pesquisadora e os alunos para o desenvolvimento das atividades ocorreram na própria escola deles, uma escola da rede pública de ensino da cidade de Rio Claro/SP. Cabe aqui ressaltar que a pesquisadora, até o momento da pesquisa, nunca havia tido contato com a escola, nem enquanto aluna, visto que a pesquisadora é natural da cidade, nem como professora da rede estadual. Deste modo, o primeiro contato com a escola foi no momento da apresentação e exposição da pesquisa para os diretores.

Após esclarecimentos sobre como o trabalho com os alunos ocorreria, o diretor autorizou que tal pesquisa fosse desenvolvida em sua escola e ainda fez um breve relato sobre algumas questões problemáticas que a escola estava enfrentando naquele momento. Uma delas era o fato de que duas turmas do primeiro ano do Ensino Médio estavam, a partir daquele dia, sem professor de Matemática, e que eles ainda não tinham previsão de quando um novo professor iria assumir as aulas. Diante dessa situação, a pesquisadora foi convidada pelo diretor a começar a desenvolver as atividades com os alunos interessados nos próprios horários das aulas de Matemática, já que esses alunos estavam com esse horário livre. A princípio, a pesquisadora havia estipulado que os encontros entre ela e os alunos iriam ocorrer nos horários extraclasse, entretanto, o diretor advertiu que isso poderia ser um problema, visto que a maioria dos alunos já possuía obrigações nos períodos contrários às aulas regulares. Diante, então, do convite e ponderando sobre as informações dadas pelo diretor da escola sobre a dificuldade de encontros contraturno[17] à pesquisadora, após verificar que estes alunos não haviam trabalhado ainda o conceito de função afim, decidiu-se, então, dar início ao trabalho de campo.

Assim sendo, em meados de abril de 2014, foi realizado o convite aos alunos de duas turmas para participar da pesquisa. Foi explicado a eles sobre do que se tratava a pesquisa e o que seria feito nos encontros entre eles e a pesquisadora. Ao perguntar quais alunos estariam interessados em participar da pesquisa em horários contraturno, verificou-se que, realmente, nenhum aluno se disponibilizou, mas, ao fazer o convite para que os encontros fossem nos horários das aulas de Matemática, nove alunos, dentre as duas turmas, mostraram-se interessados. Para esses alunos, foi entregue um termo de esclarecimento sobre a pesquisa e sobre os meios em que esta iria ocorrer. Assim, foi pedido aos alunos que trouxessem esse

[17] Horário oposto ao período escolar, destinado a atividades complementares.

termo assinado por eles e por um responsável na próxima aula de Matemática, já que esta seria o primeiro encontro.

Ao dar início aos encontros, apenas sete, dos nove alunos, trouxeram o termo assinado. Deste modo, os alunos se encontraram com a pesquisadora entre os meses de maio e setembro de 2014, ocorrendo um ou dois encontros por semana e tendo como duração duas horas cada encontro. Vale salientar que o período de coleta dos dados acabou se estendendo além do planejado, visto que o ano de 2014 teve um cronograma escolar[18] atípico. O fato de os encontros ocorrerem em aulas regulares também contribuiu para um período mais longo de coleta de dados, pois houve momentos em que os encontros foram cancelados em virtude de excursões, casa aberta, início de férias, entre outros eventos.

Os encontros ocorreram, então, no mesmo horário das aulas regulares de Matemática, no entanto, os alunos eram retirados de suas turmas e designados a algum outro lugar da escola. Na maioria das vezes, esse lugar era a sala de vídeo, e em outros casos uma sala de aula disponível. Sem conhecimento algum sobre os alunos, no primeiro encontro, foi solicitado a eles que se dividissem em duas duplas e em um trio. A opção de colocar os alunos para trabalhar juntos se deu porque a interação entre dois ou três estudantes pode proporcionar mais discussões e estratégias de resolução do que quando estes trabalham individualmente (BENEDETTI, 2003). Sendo assim, os alunos se dividiram do seguinte modo: Gustavo e Fernando, Janaína e Jaciara, e Kall, Igor e Leandro[19].

Após o primeiro encontro, algumas reflexões sobre a postura dos alunos diante de suas interações foram realizadas. Foi observado que os alunos se agruparam por afinidades. Gustavo e Fernando eram da mesma turma (e mais tarde, nas entrevistas, foi descoberto que eles eram primos) e não tinham muita proximidade com o restante dos alunos. Embora Janaína, Jaciara, Kall, Igor e Leandro fossem da mesma sala, as meninas eram muito amigas, o que ocasionou a dupla Janaína e Jaciara. Os alunos Kall, Igor e Leandro não tiveram opção e constituíram o trio. Com essa formação, pôde-se observar algumas características dos alunos.

Gustavo mostrava-se um aluno muito ativo, entretanto, era visível que este, por ter muita pressa em resolver a atividade, não desenvolvia muitas discussões com seu parceiro. Fernando já era um menino muito quieto e tímido, o que acarretava ainda mais na pouca interação entre ambos.

[18] O ano de 2014 foi o ano em que ocorreu a Copa do Mundo no Brasil, o que gerou mudanças no calendário escolar.
[19] Os nomes dados aos alunos dão fictícios, resguardando, assim, a identidade de cada um.

Jaciara e Janaína demonstraram ter muitas dificuldades em desenvolver discussões e estratégias de resoluções. Uma sempre esperava a outra dar alguma sugestão. A passividade das meninas em resolver a primeira atividade proposta alertou a pesquisadora quanto à composição desta dupla.

Kall, Igor e Leandro tomaram a postura de verdadeiros detetives. Os três alunos se mostraram muito ativos e comunicativos. Cada um conseguia levantar questionamentos e, com eles, gerar discussões muito interessantes em termos de estratégias de resolução do problema.

Com estas primeiras características observadas e levando em consideração o comportamento dos alunos acerca da atividade proposta, ficou decidido que as duplas seriam, a cada atividade, reformuladas. Estas novas composições de duplas e trio também ficaram dependentes da presença dos alunos no dia dos encontros e de alguns outros problemas resultantes.

Durante o período de maio a junho, os sete alunos participaram dos encontros, mas foi no segundo semestre que os problemas emergentes ocorreram. Ao dar início aos encontros em julho, foi esclarecido pela direção que os alunos Kall e Leandro não estavam mais matriculados na escola. Kall havia se mudado para outro estado e Leandro para uma escola mais perto de sua casa. Assim, os encontros, a partir do segundo semestre, contavam apenas com cinco alunos.

Mas os problemas não cessaram por aí: a participação de Fernando decaiu muito durante todo o segundo semestre. Ele e Gustavo tiveram alguns desentendimentos durante o décimo terceiro encontro, mas foi no décimo quarto encontro que os conflitos se tornaram mais graves. Diante dessas discussões e da falta de interesse de Fernando em participar das atividades, foi posto, como opção para ele, retirar-se da pesquisa. Essa opção foi aceita pelo aluno, o qual deixou a pesquisa no décimo sétimo encontro. O leitor encontrará, no capítulo 5, o qual está destinado às considerações finais, mais detalhes sobre os problemas emergentes e a maneira como se lidou com eles.

De modo geral, a relação entre a pesquisadora e os alunos foi amigável, e isso constituiu um ambiente confortável para ambos. Durante os encontros, os alunos foram adquirindo mais confiança e autonomia para expor suas opiniões e discutir as questões referentes às atividades. Tirando os conflitos específicos entre Gustavo e Fernando no final dos encontros, não houve identificação de problemas de relacionamento entre os outros alunos.

Em relação às filmagens, em nenhum momento os alunos demonstraram constrangimentos em fazer ou falar alguma coisa devido à presença das câmeras. Como já

mencionado, o ambiente nos encontros era agradável e o ato de filmá-los não interferiu na maneira como eles foram conduzidos.

3.5.2 A escola[20]

O leitor encontrará nesta seção um resumo sobre a formação da escola, em termos históricos, e uma descrição detalhada dos aspectos físicos que a constituem. Essa exposição minuciosa foi considerada importante, visto que ela oferece ao leitor um panorama geral da escola, para que ele possa compreender melhor o ambiente no qual o trabalho de campo foi desenvolvido.

A Escola Estadual Prof. Mycroft foi fundada em 01 de agosto de 1979, pelo Governo do Estado de São Paulo. A escola foi construída em decorrência da urbanização do bairro, visando atender ao grande número de migrantes de vários estados brasileiros. Desde o início de sua atuação, a escola funciona em prédio próprio, sendo composta por duas alas unidas por meio de um galpão coberto: a ala administrativa (sala dos professores, sala da direção, secretaria, banheiros e sala da coordenação) e a ala das salas de aula, que em 1983 era composta por seis salas. A partir de 1984, a escola passou a funcionar com doze salas de aula, uma ampliação iniciada em 1982, devido à grande demanda de alunos.

Ela atende atualmente a comunidade de seu bairro e de bairros próximos. De acordo com o Plano de Gestão da escola, muitos de seus alunos "convivem em lares cujo ambiente às vezes é conturbado, tendo a mãe ou a avô como únicos responsáveis" e são "carentes tanto de material como de afetividade" (DIRETORIA DE ENSINO - REGIÃO DE LIMEIRA, 2012, p. 06). Segundo a Vice-Diretora, Prof.ª Irene, a classe socioeconômica dos alunos é de média para baixa. De acordo com ela, existem mais alunos de classe baixa do que alunos de classe média. A Prof.ª Irene também argumenta que o principal problema social dos alunos na escola é a violência. Segundo ela:

> [...] o grupo social no qual a escola está inserida, certos... os bairros, que estão aqui ao redor, você tem o contexto de violência familiar, violência no bairro, violência entre eles, que já vem praticamente do berço [...] então você tem um... um lidar com eles, você tem um grupo muito tranquilo, um grupo que é todo tranquilo, que você não tem problema, tem problema nenhum, você tem a minoria, na verdade é a minoria, mas essa minoria, ela vem como uma agressividade interior tão grande que ela acaba contaminando aquele ambiente que eles estão (Transcrição da entrevista).

[20] O nome dessa escola e, de qualquer outra, apresentado nessa pesquisa são fictícios, preservando, assim, a identidade de cada uma.

A média de estudantes na escola é de 700 alunos na faixa de 11 a 18 anos, distribuídos nos períodos da manhã e tarde, entre o Ensino Fundamental II e o Ensino Médio. A média de alunos em sala de aula varia entre 30 e 35 alunos no Ensino Fundamental II e de 35 a 40 alunos no Ensino Médio. Os alunos são todos uniformizados, para cada turma há uma pasta de documentos, identificando a série ou ano[21] e contendo o nome de todos os alunos pertencentes a ela.

No ano de 2014, a escola se tornou uma escola prioritária para o CGEB[22], pois não alcançou os índices do IDESP[23] no ano de 2013. Assim, para este ano, foi designada para a escola uma coordenadora pedagógica do PCGAP[24] para auxiliar as ações pedagógicas da escola. Deste modo, no presente momento, a escola é composta por três coordenadoras pedagógicas (uma para o Ensino Fundamental II, uma para o Ensino Médio e uma do PCGAP), um diretor, duas vice-diretoras, sendo que uma é voltada para a escola da família, seis agentes de organização da escola (três na secretaria e três no pátio), um gerente administrativo e 35 professores efetivos. Até o ano de 2013, a escola apresentava um professor mediador[25], mas, para este ano, embora a escola apresente a necessidade de um professor mediador, ela não tem mais em seu quadro de funcionários algum professor preenchendo esse cargo.

A escola comporta doze salas de aula, uma sala de Educação Física, uma sala de informática contendo quatorze computadores com acesso à internet, uma sala de vídeo com quadro branco, uma biblioteca (sala de leitura), uma sala dos professores contendo um computador para pesquisa, uma impressora, uma estante com várias revistas e armários individuais, uma quadra poliesportivas descoberta, um refeitório, que comporta em média 100 alunos, e uma mesa de ping-pong, que fica instalada no pátio. Ela também tem recursos físicos e pedagógicos, como materiais pedagógicos, *data show*, tela de projeção, *notebook*, televisão, vídeo, DVD, rádios, caixas de som e microfone. Em média, as salas de aula têm quarenta carteiras e cadeiras, uma mesa do professor, uma lousa e um ventilador.

---

[21] A escola ainda se encontra na fase de transição de todas as séries para ano do Ciclo Fundamental.

[22] CGEB – Coordenadoria de Gestão da Educação Básica. Para mais informações acessar: <http://www.derita.com.br/noticias_pdf/plano_acao_escolas_prioritarias.pdf>.

[23] IDESP – Índice de Desenvolvimento da Educação de São Paulo. Para mais informações acessar: <http://idesp.edunet.sp.gov.br/Arquivos2013/041661.pdf>.

[24] PCAGP – Professor Coordenador de Apoio à Gestão Pedagógica. Para mais informações acessar: <http://www.derita.com.br/noticias_pdf/pcagp.pdf>.

[25] De acordo com a Prof.ª Irene, o professor mediador tem como função descobrir os problemas (agressividade, disciplina, problemas de interesse, entre outros) que os alunos apresentam dentro da escola. Ele tenta mediar as questões de melhoria do comportamento do aproveitamento do aluno.

O pátio onde os alunos ficam durante o intervalo é o galpão que une a ala administrativa à ala das salas de aula. Esse galpão é separado das alas por portões com grades. No intervalo, os alunos se locomovem até esse galpão, que é pequeno, mas arejado, e permanecem nele apenas durante o intervalo. O espaço de circulação dos alunos acaba sendo muito pequeno, visto que ele é dividido com as mesas do refeitório e com a mesa de ping-pong. O pátio da escola também oferece um bebedouro com cinco torneiras com água gelada e banheiros em bom estado, que aparentemente são suficientes para a quantidade de alunos presentes na escola.

Embora nesta escola haja alunos com algum tipo de necessidades especiais, não existe, ainda, algum programa que auxilia esses alunos e seus professores. Em termos de estrutura física, a escola não se mostra estar preparada para receber algum aluno com deficiência física[26], pois seu acesso à ala das salas de aulas é por meio de escadas. Atualmente na escola há oito alunos com algum tipo de deficiência, a saber, um com baixa visão, um com TDAH[27], um copista[28], um esquizofrênico e quatro com limitações cognitivas. Segundo a Prof.ª Irene, os alunos que apresentaram algum tipo de deficiência já foram levados para a APAE[29] para serem "laudados"[30]. De acordo com ela, alguns alunos já apresentam um laudo e outros ainda estão em processo de "laudação". A Prof.ª Irene ainda ressalta que o único auxílio que a escola tem, em termos de materiais pedagógicos para esses alunos, são alguns materiais adaptados disponibilizados para a escola, muitas vezes via e-mail, enviados pela Diretoria de Ensino.

Em paralelo com as aulas, a escola organiza três projetos de extensão. São eles: "Roda da leitura", que visa ampliar a visão do aluno em relação ao mundo, incentivando o gosto por diversos gêneros literários e formando leitores críticos e atualizados; "Prevenção também se ensina", que trabalha com o objetivo de discutir com os alunos sobre as mudanças corporais, e o "Projeto JPME (Juntos pelas mudanças da escola)", que tem como objetivo levar os alunos a gostar mais da escola e diminuir a indisciplina nas aulas pós-intervalo. O último projeto é organizado em conjunto com o Grêmio Estudantil da escola. Este, segundo a Prof.ª Irene, é um grêmio ativo que organiza atividades, como a gincana entre os alunos e o monitoramento do intervalo juntamente com os agentes. A escola também desenvolve o projeto chamado "Escola da família", mas ainda não existem oficinas sendo desenvolvidas neste projeto.

---

[26] Deficiência física é o nome dado à característica dos problemas que ocorrem no cérebro ou no sistema locomotor, e leva a um mau funcionamento ou paralisia dos membros inferiores e/ou superiores.

[27] TDAH – Transtorno do Déficit de Atenção com Hiperatividade. Para mais informações acessar: <http://www.tdah.org.br/sobre-tdah/o-que-e-o-tdah.html>.

[28] Termo designado pela Prof.ª Irene referente ao aluno que somente copia as lições.

[29] APAE – Associação de Pais e Amigos dos Excepcionais.

[30] Para esta pesquisa, o termo "laudados" se refere aos alunos encaminhados para a APAE para serem consultados e receberam um laudo médico. Já o termo "laudação" se refere aos alunos que estão no processo médico de receber um laudo.

No geral, a escola é limpa, mas em suas salas de aula as carteiras e cadeiras são sempre sujas e até mesmo quebradas. A rede elétrica das salas de aula está sempre desativada, entretanto, quando ligada, muitas tomadas não funcionam. Em cada sala de aula há apenas um ventilador funcionando e aparentemente ele é suficiente para arejar e refrescar o ambiente, embora ressalte que a estrutura da escola contribui para a circulação do ar e que tal pesquisa não ocorreu na estação de verão. Do mais, a escola tenta dar boas condições de trabalho para os professores e alunos, oferecendo, assim, um ensino de qualidade para a sua comunidade.

A escolha dessa escola se deu por um motivo particular da pesquisadora. Fazer o trabalho de campo em uma escola longe da Universidade Estadual de São Paulo – UNESP – *Campus* de Rio Claro, era um desejo especial. A pesquisadora sentia a necessidade de permitir a entrada da Universidade em outras escolas, sem serem aquelas aos seus arredores. Um levantamento das escolas distantes foi feito e com isso foi investigada a possibilidade de desenvolvimento da pesquisa. A primeira opção foi a escola E. E. Prof. Moriarty, distante da UNESP aproximadamente 3,5 Km, no entanto, tal escola não aceitou os termos da pesquisa. Como segunda opção, a escola E. E. Prof. Mycroft, distante da UNESP aproximadamente 6,6 Km, foi contactada e, depois de se fazer toda a apresentação da investigação, a mesma concordou com os termos da pesquisa, aceitando, assim, abrir suas portas para a presente pesquisadora.

3.6 Os pr0cediment0s metodológ1cos da p3squi5a

Este tópico apresentará todo o processo de criação e elaboração das atividades utilizadas nesta pesquisa, bem como os recursos utilizados para coletar seus dados.

3.6.1 Atividade protótipo

Fã de carteirinha do famoso personagem de ficção Sherlock Holmes, do escritor inglês Sir Arthur Conan Doyle, a pesquisadora tinha como primeira intenção criar um conto que envolvesse um mistério, cujo segredo fosse revelado apenas por meio da decifração de uma mensagem criptografada. A ideia era fazer com que os alunos se envolvessem em uma narrativa e se sentissem motivados a descobrir a mensagem cifrada. A possível motivação gerada para descobrir a mensagem cifrada faria o aluno buscar, por si próprio, mecanismos de decifração, e é neste momento que a Matemática entraria em ação.

Com o conceito matemático já definido, a saber, função afim, e inspirada em um passatempo chamado “criptograma e palavras cruzadas em branco”, a pesquisadora criou o primeiro protótipo da atividade. Chamada de “O caso do sequestro do matemático”[31], a atividade era composta, então, por um conto totalmente fictício, criado pela pesquisadora, por uma carta criptografada que continha dados sobre os mistérios do conto e por uma ficha de perguntas que abordavam questões como: descreva detalhadamente o processo de decifração da carta; qual foi a expressão matemática utilizada para cifrar a mensagem da carta, entre outras.

Após a conclusão dessa atividade, surgiu uma oportunidade de colocá-la em prática. Um amigo que lecionava na rede pública da cidade de Rio Claro/SP convidou a pesquisadora para desenvolver a atividade com seus alunos. O convite foi, então, aceito, e a atividade protótipo posta em prática.

3.6.2 O primeiro teste

As condições deste primeiro teste foram muito favoráveis à pesquisadora. O fato de os alunos fazerem parte de uma escola pública da cidade e de estarem no primeiro ano do Ensino Médio encaixava-se nas características estipuladas para os sujeitos da pesquisa. O ambiente se tornava muito próximo das condições previstas para o trabalho de campo e se diferenciava apenas pelo fato de que esses alunos já haviam abordado o conceito de função afim. No entanto, esse fato acabou contribuindo para observar melhor como os alunos lidavam com a atividade, mesmo estes já tendo visto o conceito previamente.

Assim sendo, em um determinado dia, a pesquisadora e o Prof. Henrique Lazari foram até a escola e aplicaram a atividade para duas turmas de primeiro ano. O principal objetivo deste teste era observar como os alunos reagiriam à atividade e como ela poderia ser aprimorada e desenvolvida com os sujeitos da pesquisa, de acordo com o objetivo proposto. Sendo assim, várias observações foram feitas e apontamentos levantados em relação à atividade.

O conto foi bem aceito pelos alunos. No momento em que receberam a atividade, eles demonstraram estar muito empolgados, e certa agitação tomou conta da sala de aula. De acordo com eles, todos conheciam o personagem, e começaram a contar sobre os filmes de Sherlock Holmes e como o personagem se comportava diante dos mistérios apresentados a ele. Esse entusiasmo gerado nos alunos contribuiu para que eles se sentissem curiosos em

[31] Apêndice C.

desvendar a carta criptografada. Deste modo, os alunos iniciaram rapidamente discussões e tentativas de decifração da mensagem.

A ficha de perguntas foi introduzida como sendo um "relatório" que eles tinham que fazer para prestar contas sobre o mistério do conto. A observação sobre a maneira como os alunos interpretavam as questões da ficha e desenvolviam suas respostas mostrou para a pesquisadora que algumas questões escritas não estavam muito claras. Além disso, elas influenciaram, em algum sentido, as respostas. Por exemplo, o fato de se apresentar o alfabeto fixado em uma das questões induziu os alunos a montar uma regra de cifração de deslocamento cíclica, o que não era o caso, e isso dificultou os alunos a pensar em outras situações de cifração.

Assim, após varias discussões entre a pesquisadora e o Prof. Henrique Lazari sobre os acontecimentos desse teste e sobre essas observações destacadas pela pesquisadora, algumas decisões foram tomadas. Ficou decidido que a atividade seguiria a estrutura de conter um conto envolvendo o personagem Sherlock Holmes, uma mensagem criptografada que desvendasse o mistério do conto e uma ficha de perguntas. Entretanto, essa ficha deveria ser reformulada para conter questões mais claras e objetivas, sem influenciar as respostas dos alunos.

A ideia de se trabalhar em duplas ou trios foi reforçada, visto que neste teste pôde-se observar claramente como os alunos, em conjunto, construíram mais verbalizações do que quando estes trabalharam sozinhos.

A questão sobre a quantidade dos sujeitos da pesquisa também entrou em discussão. Ficou claro que o trabalho de campo não poderia ser realizado em uma sala de aula regular composta por quarenta alunos. A quantidade de alunos seria um problema, visto que a pesquisadora, não daria conta de observar e colher os dados confiáveis para a pesquisa. Assim, ficou decidido que o trabalho de campo ocorreria com uma quantidade pequena de alunos.

3.6.3 Elaboração das atividades e sua sequência pedagógica

Tentando aperfeiçoar a atividade, a pesquisadora pensou na criação de várias atividades. Com o intuito de que elas englobassem as relações entre grandezas, a correspondência entre elementos de dois conjuntos, sua "regra" ou "lei de formação", a compreensão de sua construção gráfica e suas caracterizações em termos de crescimento e decrescimento, é que surgiu a ideia de se elaborar uma sequência pedagógica de atividades.

O termo sequência pedagógica está sendo assumido, nesta pesquisa, como sendo um conjunto de atividades interligadas, que tem como finalidade promover, por etapas, uma aprendizagem específica e definida, cuja organização é decorrente do objetivo proposto pelo pesquisador. A quantidade de aulas deve ser planejada, e estas devem ser analisadas previamente, com a finalidade de se observar situações de exploração, na qual se envolvem os conceitos determinados na pesquisa.

Assim sendo, inspirada por jogos de criptogramas e palavras cruzadas, e tendo em mente o conceito de função afim, é que foram criadas oito[32] atividades envolvendo problemas criptográficos. Cada uma das oito atividades foi constituída por um conto com o personagem Sherlock Holmes, por uma mensagem criptografada e por uma ficha de perguntas. As oito atividades se relacionam entre si e oferecem desafios com grau de complexidade crescente, para que os alunos possam exercitar suas habilidades, superando-as e atingindo novos níveis de exploração.

As atividades foram construídas da seguinte maneira: a primeira foi produzida com o objetivo de apresentar aos alunos à criptografia. A segunda, terceira e quarta atividades tinham como objetivo abordar a definição de função afim e suas particularidades, como função linear, função identidade e função constante. A quinta e sexta atividades foram destinadas a trabalhar o conceito gráfico dessa função. A sétima abordava a definição de função inversa e, finalmente, a oitava era uma atividade de encerramento que envolvia uma síntese do trabalho desenvolvido com os alunos.

No capítulo 4, onde os dados estão descritos, o leitor encontrará com mais detalhes os objetivos de cada atividade e a maneira como elas se interligam.

3.6.4 Segundo protótipo e as atividades definitivas

O segundo protótipo foi desenvolvido com três alunos da graduação do curso de Matemática da UNESP – *Campus* de Rio Claro/SP. A intenção desse segundo teste era a de observar se a sequência pedagógica estava proporcionando uma exploração gradual do conceito de função afim, bem como se seus contos, suas mensagens cifradas e a ficha de perguntas estavam coerentes e corretos. Nesse teste, os graduandos tomaram uma posição mais crítica, dando à pesquisadora sugestões de como abordar os possíveis questionamentos, por parte dos alunos, sobre as atividades, e de como determinar o tempo de cada uma.

[32] Apêndice D.

As atividades não sofreram grandes modificações; correções de português e de cifrações foram sugeridas e realizadas. Os graduandos também contribuíram para o aperfeiçoamento da apresentação em *Power Point*. Essa apresentação foi realizada no primeiro encontro e trazia um pouco sobre a história da criptografia e de como se deu sua evolução durante os tempos.

3.6.5 Instrumentos de coleta de dado

Os procedimentos metodológicos escolhidos pela pesquisadora, a fim de produzir os dados durante os encontros, foram: as observações e anotações feitas pela pesquisadora no caderno de campo, as gravações em vídeo e áudio referentes às discussões de cada grupo durante os encontros, e as respostas dadas pelos alunos nas fichas de perguntas de cada atividade. Posteriormente à conclusão do trabalho de campo, foram realizadas entrevistas com os alunos participantes do projeto, a fim de produzir mais informações sobre as atividades e consequentemente ouvir os alunos acerca da produção feita por eles durante os encontros.

Em relação às anotações reflexivas da pesquisadora, Bogdan e Biklen (1994, p. 211) afirmam que "os comentários do observador consistem em seções das notas de campo destinadas ao registro do que o investigador vai pensando e sentindo, à medida que faz as suas observações". Sendo assim, a observação da pesquisadora aparece como sendo um meio de recolher as informações sobre as ações dos alunos, como os alunos resgatam os conceitos matemáticos formais e informais, a forma como as discussões caminham, as dificuldades encontradas pelos alunos durante a resolução das atividades, como essas atividades são resolvidas, além de como eles desenvolvem os problemas propostos e qual raciocínio é utilizado para resolvê-los.

Para ajudar a complementar as observações da pesquisadora, visto que ela não consegue observar todos os alunos ao mesmo tempo, bem como todas as suas produções, e pelo fato de o momento de observação ser único, o recurso de filmagens foi utilizado em todos os encontros. Segundo Powell, Francisco e Maher (2004, p. 13), filmagens "são atraentes e auxiliam não apenas as comunicações escritas como também as orais", permitindo, assim, que esses dados possam ser vistos novamente com mais atenção, "não somente por múltiplas visões, mas também por múltiplos pontos de vista" (POWELL; FRANCISCO; MAHER, 2004, p. 10). Da mesma forma, Benedetti (2003, p. 71) aponta duas vantagens do acesso às gravações de vídeo. Ele argumenta, primeiro, que as gravações possibilitam a uma mesma pessoa assistir várias vezes a uma mesma cena, por meio de observações teóricas distintas; segundo, que essas filmagens podem ser assistidas por diferentes pessoas, permitindo uma

visão e análise de diferentes perspectivas. A posição das câmeras era ajustada a cada encontro, o que dependia do lugar em que os encontros ocorriam e da disposições dos alunos e carteiras. Junto com as filmagens, foram utilizados em alguns encontros gravadores de áudio, para que se pudesse gravar com mais detalhes as discussões desenvolvidas entre os alunos e entre a pesquisadora e os alunos. A opção por também gravar em áudio se deu em virtude do excesso de barulho externo à sala de aula e porque muitas vezes os alunos falavam baixo, o que dificultava o entendimento do áudio nas filmagens.

Como outra forma de produção de dados, as fichas de perguntas de cada atividade respondidas pelos alunos (e suas folhas de rascunho) puderam ajudar no entendimento da pesquisadora sobre como o processo de resolução aconteceu em cada grupo, visto que, nas respostas a essas perguntas, os alunos descreveram com mais detalhes o caminho pensado e discutido por eles durante a resolução das atividades.

Após o término das atividades e com uma pré-análise já realizada sobre as observações, as filmagens e as fichas de perguntas respondidas, uma entrevista semiestruturada foi formulada e realizada com os alunos, para tentar preencher as lacunas deixadas durante as outras produções de dados. Esse tipo de entrevista é caracterizado como sendo uma entrevista elaborada com "perguntas abertas e fechadas, onde o informante tem a possibilidade de discorrer sobre o tema proposto [...], também têm como vantagem a sua elasticidade quanto à duração, permitindo uma cobertura mais profunda sobre determinados assuntos" (BONI; QUARESMA, 2005, p. 75).

De acordo com Goldenberg (2011), as entrevistas também contribuem para procurar respostas que outros instrumentos não puderam fornecer. A autora ainda pontua algumas vantagens em se fazer uma entrevista, como, por exemplo, a flexibilidade de conduzir as perguntas buscando as respostas desejadas, uma observação mais ampla sobre as respostas dos entrevistados, bem como a verificação de possíveis contradições, entre outras. Segundo Poupart (2012), essas entrevistas também permitem uma análise do processo a partir da visão dos próprios sujeitos da pesquisa. Assim, as entrevistas se constituíram em um momento em que os alunos puderam expor suas opiniões acerca dos encontros e de todas as atividades desenvolvidas. Todas as entrevistas foram gravadas em áudio e posteriormente transcritas. O uso do gravador durante a entrevista possibilita um registro mais completo do diálogo desenvolvido entre aluno e pesquisador (MOREIRA; CALEFFE, 2008).

Assim, os vários meios de produção de dados aqui apresentados configuram-se como uma grande vantagem, pois podem conduzir o pesquisador, a partir de diferentes ângulos, à resposta de sua pergunta diretriz. Essa perspectiva pode ser definida como triangulação de

dados, que, segundo Araújo e Borba (2012), é a utilização de diferentes processos de coleta de dados sobre uma mesma situação, para que se possa ter uma visão mais aprofundada e detalhada sobre os acontecimentos da investigação da pesquisa, além de aumentar a credibilidade da mesma, quando esta adota uma abordagem qualitativa.

Goldenberg (2011, p. 63) afirma que a triangulação "tem como objetivo abranger a máxima amplitude da descrição, explicação e compreensão do objeto de estudo". Assim, a utilização da triangulação contribui para a análise dos dados, no sentido de, a partir do confronto dos mesmos, oferecer várias informações sobre a mesma situação, possibilitando ao pesquisador chegar a conclusões mais consistentes.

3.7 Organ1zaçã0 dos dad0s

Os dados que compõem esta pesquisa estão no caderno de campo da pesquisadora, nas gravações de vídeo e áudio realizadas durante os encontros, nas fichas de perguntas de cada atividade respondidas pelos alunos e, por último, as entrevistas realizadas com os mesmos, posteriormente ao encerramento dos encontros.

De acordo com Lüdke e André (1986), ao analisar os dados, o pesquisador

> "Trabalha" todo o material obtido durante a pesquisa, ou seja, os relatos de observação, as transcrições das entrevistas, as análises de documentos e as demais informações disponíveis. A tarefa de análise implica num primeiro momento, a organização de todo o material, dividindo-o em partes, relacionando essas partes e procurando identificar nele tendências e padrões relevantes. Num segundo momento essas tendências e padrões são reavaliados, buscando-se relações e inferências num nível de abstração mais elevado (LÜDKE; ANDRÉ, 1986, p. 45).

Segundo essas autoras, a análise dos dados não ocorre somente quando se termina de coletá-los, mas, sim, durante todo o processo de investigação da pesquisa. Entretanto, é na fase posterior da coleta de dados que a análise se torna mais metódica e formal. Esse movimento da análise citado por Lüdke e André (1986) ocorreu durante o trabalho de campo, culminando muitas vezes nas decisões e delineamentos dos encontros, de acordo com o objetivo da pesquisa.

Bogdan e Biklen (1994) também argumentam que a análise dos dados é o momento no qual o pesquisador caracteriza e organiza sistematicamente os dados coletados, contribuindo com seu próprio entendimento em relação a esses materiais e permitindo a apresentação de suas conclusões a outros. De acordo com eles, a categorização de situações que se repetem ou

se destacam, como frases, palavras, padrões de comportamento, formas de os sujeitos pensarem, são atividades que ilustram o desenvolvimento de um sistema chamado, por eles, de categorias de codificação. Essas categorias, segundo esses autores, "constituem um meio de classificar os dados descritivos que recolheu [...], de forma que o material contido num determinado tópico possa ser fisicamente apartado dos outros dados" (BOGDAN; BIKLEN, 1994, p. 221).

Corroborando as ideias de Lüdke e André (1986) e Bogdan e Biklen (1994) em termos da importância da criação e organização das categorias para que se possa analisar o conjunto de dados produzidos, foi necessário o desenvolvimento de algumas etapas para, finalmente, se chegar ao processo de categorização e articulação com a teoria. A seguir, serão apresentadas ao leitor as etapas desenvolvidas citadas acima.

- *Organização dos dados:* A organização dos dados foi sendo realizada de acordo com cada encontro. Após a pesquisadora se encontrar com os alunos, ela transcrevia para o seu *notebook* as anotações realizadas por ela em seu caderno de campo. Juntamente com isso, o vídeo e o áudio também eram transferidos para o seu *notebook*, sendo eles organizados por data e número do encontro. Com os encontros finalizados, a pesquisadora imprimiu todas as anotações do caderno de campo e as juntou, constituindo, assim, o seu caderno de campo impresso (CCI).

  Com esse material em mãos, a pesquisadora realizou uma leitura cuidadosa do CCI e, de acordo com a leitura, uma primeira categorização foi realizada, a fim de conhecer todos os dados e organizá-los de acordo com as situações que se assemelharam durante os encontros.

- *Descrição dos dados:* Essa etapa foi realizada em dois momentos. Primeiramente, o capítulo "Descrição dos dados" foi sendo constituído apenas com o CCI e com o material produzido pelos alunos (as fichas de perguntas respondidas por eles e as folhas de rascunho). As folhas de rascunho acabaram tornando-se fontes muito importantes de informação. Nelas, os alunos escreviam com mais detalhes os cálculos que estavam sendo realizados. Deste modo, uma primeira triangulação foi realizada, buscando nos materiais produzidos pelos alunos as situações destacadas pela pesquisadora durante as suas observações. Em seguida, já tendo uma primeira descrição do que ocorreu durante os encontros, foi a vez de se triangular os vídeos e os áudios. Esse momento foi importante, uma vez que se buscavam os diálogos

realizados pelos alunos durante as atividades e a verificação dos acontecimentos destacados pela pesquisadora durante as suas observações.

Após essa primeira organização, o capítulo que se intitula “Descrição dos dados” foi constituído.

* *Transcrição das entrevistas:* O ato de transcrever as entrevistas foi importante para perceber algumas sutilezas nas falas dos alunos que não foram percebidas no ato da entrevista. As entrevistas contribuíram para entender melhor algumas situações ocorridas durante os encontros e para conhecer a visão dos alunos sobre as atividades e os encontros.

* *Destacar e organizar os dados relevantes:* Tendo pronta a descrição detalhada dos dados e as entrevistas transcritas, foi a vez de se realizar uma leitura minuciosa em busca de episódios que mostrassem indícios de respostas para a pergunta diretriz da pesquisa. Com esse material impresso e seus episódios destacados, um processo de recorte do material foi realizado, e a criação das categorias foi surgindo de acordo com esses eventos.

* *Tracejando as categorias:* No final do processo citado acima, a pesquisadora havia obtivo vários episódios que convergiam para suas sete categorias criadas. No entanto, com essa visão panorâmica, observou-se que algumas categorias poderiam ser juntadas, visto que existia uma dependência entre elas, ou seja, uma categoria só ocorria se a outra ocorresse. Sendo assim, uma nova reflexão sobre elas foi realizada e, no final desse processo, três categorias emergiram, a saber: **Atitudes Investigativas; Procedimentos e Conceitos.**

* *Articulação das categorias com a literatura:* Uma vez estabelecidas as categorias, foi a vez de se debruçar na literatura e iniciar um diálogo entre os dados empíricos e a teoria.

No capítulo seguinte, serão apresentadas as análises das aplicações da sequência pedagógica das atividades desenvolvidas para esta pesquisa, bem como todo o material produzido pelos alunos durante a resolução das atividades.

"– Não há nada como evidências em primeira mão – disse Holmes. – Na verdade, minha opinião sobre o caso já está formada. Mas, ainda sim, é bom recolhermos todas as evidências existentes".

(Sherlock Holmes)

4 ANALISANDO VESTÍGIOS, EVIDÊNCIAS E INDÍCIOS

Este capítulo apresenta as análises dos dados sob o olhar da pesquisadora à luz da literatura acerca das categorias Atitudes Investigativas; Procedimentos e Conceitos estabelecidas e apresentadas no capítulo 3. Deste modo, o objetivo deste capítulo é, então, apresentar indícios que sejam capazes de responder à pergunta diretriz desta pesquisa, a saber:

Quais as potencialidades de atividades pedagógicas envolvendo problemas criptográficos na exploração das ideias associadas à função afim?

Para responder a tal pergunta, as análises de cada categoria foram realizadas de acordo com as ideias apresentadas por Mauri (2009), Echeverría e Pozo (1998) entre outros autores citados no referencial teórico a respeito das atitudes e procedimentos vindos dos alunos com o propósito de se trabalhar o conceito.

4.1 At1tudes Inv3stigativas

As atitudes dos alunos foram se caracterizando durante os encontros, visto que o modo de agir e reagir dos mesmos foram sendo determinados pelas disposições internas[33]. Tais disposições tiveram como partida as próprias atitudes vindas dos alunos e as atitudes da pesquisadora. A postura da pesquisadora durante a resolução das atividades influenciou, de certa forma, a maneira como os alunos se comportaram durante os encontros, contribuindo para que alguns paradigmas de comportamento dos mesmos fossem modificados ao longo das atividades.

Quando se refere à posição da pesquisadora (que durante os encontros assumiu o papel de professora), Freire (2011, p. 2) argumenta que esta deve ter em mente que "*ensinar não é transferir conhecimento, mas criar as possibilidades para a sua própria produção ou a sua construção*". Neste sentido, o professor tem que ser acessível às indagações, às curiosidades dos alunos, às suas inibições e auxiliá-los nos mais variados momentos do processo de aprendizagem (FREIRE, 2011). Em termos desse auxílio ao estudante, Ponte, Brocado e Oliveira (2009) afirmam que este é um dever importante do professor. De acordo com esses autores, o professor precisa estar atento a todo processo de investigação dos alunos durante a resolução dos problemas, cabendo a ele valorizar as ideias trazidas pelos alunos e incentivar as discussões e as investigações de tais ideias. Solé e Coll (2009) também argumentam sobre

[33] Entendem-se aqui como disposições internas as ações vindas dos alunos e da pesquisadora ocorridos dentro da sala de vídeo (ou da sala de aula) durante a realização dos encontros.

a postura do professor, destacando que sua orientação deve favorecer a autonomia do aluno e a estimulação crescente dos novos aprendizados.

As posturas destacadas por Ponte, Brocado e Oliveira (2009) e Solé e Coll (2009) podem ser reconhecidas nas atitudes realizadas pela pesquisadora durante seu trabalho de campo. O episódio abaixo descreve parte do diálogo que ocorreu entre ela e os alunos (Jaciara, Janaína e Fernando) na atividade *Um caso de sequestro*, a partir de uma ideia que Fernando teve para decifrar a mensagem proposta.

Pesquisadora: E aí? Olha só... ele escreveu o alfabeto... mas ele pensou na cifra de César... você lembra que ela desloca 4 casas?

Jaciara: Ahã.

Pesquisadora: Se o A era 1 e eu desloco 4, ele vira o quê? Que número ele vira?

Janaína: D? D? Ah... não, número?

Pesquisadora: Isso.

Janaína: Ah, tá.

Pesquisadora: A gente está olhando número aí, né?... Então, qual que ele vira?

Jaciara: O 19? Não...

Pesquisadora: Do 1...

Jaciara: Pula 4 casas...

Pesquisadora: Anda 4... então, ele vira o número...?

Jaciara: 4.

Pesquisadora: Quase.

Jaciara: 5.

Pesquisadora: 5...

Jaciara: Ah...

Pesquisadora: Então, se B era 2 e andou 4, então vira?... Será que esse aí dá certo?

Fonte: Gravações de vídeo e áudio (2015).

Nesse trecho, observa-se que a discussão partiu de uma ideia de Fernando e que a pesquisadora tentou, por meio de questionamentos, auxiliar a continuação da estratégia de resolução que ele havia pensado. Essa postura da pesquisadora também corrobora os argumentos de Mauri (2009), que afirma que o professor, diante de seus alunos, deve confiar em seus esforços, discutindo com eles as dúvidas emergentes das atividades, levando sempre

em consideração o ponto pessoal de partida para a resolução dos problemas e motivando, por meio dos diálogos, a exposição de suas estratégias e ideias. Solé (2009) argumenta sobre isso que, iniciar a atividade partindo das ideias dos alunos e movimentá-los por meio de discussões e reflexões, contribui para estabelecer as relações de respeito com os alunos gerando autoestimas e autonomias durante o processo de resolução.

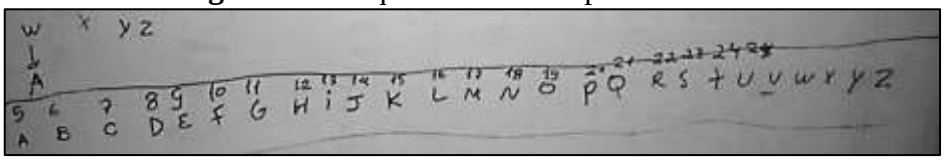
Na continuação do episódio descrito acima, após a intervenção pedagógica da pesquisadora, os alunos conseguiram escrever o alfabeto cifrado, no entanto, outras dúvidas quanto a ele surgiram. Novamente, a pesquisadora argumentou com os alunos sobre suas novas indagações, tentando, cautelosamente, fazer com que os alunos chegassem as respostas para aqueles novos questionamentos.

Pesquisadora: Deu certo?... Não?

Janaína: A gente está vendo aqui como fazer.

Fernando: Se termina, começa do A... [fala se referindo à Figura 11].

Figura 11 - Esquema montado por Fernando.



Fonte: Dados da pesquisa (2015).

Pesquisadora: Será? Olha só, quanto que vale o W?... Será que o alfabeto volta? Quando a gente desloca ele, uma letra, a gente acaba deslocando...?

Janaína e Jaciara: Tudo.

Pesquisadora: Será que ele volta daí no A?

Janaína: Acho que deve voltar...

Fernando: Tem que voltar...

Janaína: Porque, senão, não dá pra fazer...

Fernando: Senão vai ficar sem o A.

Pesquisadora: Hum... então, mas a gente, ali, não está em número?

Fernando: Ahã.

Pesquisadora: Então, a gente tem que pensar em número. Certo? Se o meu A valia 1, ele passou a valer?

Janaína: 5.

Pesquisadora: Você já falou 5, então ele vale um número, se o B era 2 e passou a valer...

Janaína: 6.

Pesquisadora: 6. Se o W vale um número, ele passou a valer?... esse número mais 4... então ele não pode ser o A... porque o A vale 5... vocês concordam?

Fernando: Ah!... Entendi alguma coisa!

Fonte: Gravações de vídeo e áudio e ficha de perguntas (2015).

A intenção da pesquisadora em todos os diálogos foi de sempre tentar ajudar os alunos, partindo da ideia inicial de estratégia de resolução que eles mesmos haviam desenvolvido. Em relação às essas intervenções, Mauri (2009) destaca que elas são importantes, visto que é neste momento, que o professor atua como o mediador, levantando questionamentos, debatendo discussões e revendo e explicitando as ideias prévias trazidas pelos alunos. Ela ainda expressa que o professor deve, por meio dos diálogos, entusiasmar e incentivar os alunos para que eles, mesmo com obstáculos, tenham o interesse em resolver o problema, e que, ao mesmo tempo em que os auxilie, saiba conceder algum tempo aos alunos, para que estes posam se dedicar à tarefa e refletir sobre o problema. A autora argumenta que é necessário que os alunos se sintam a vontade e que seja concedido algum tempo para que eles reflitam e desenvolvam as resoluções. Em relação a esse tempo, Solé (2009) argumenta que ele é necessário para o amadurecimento dos alunos em relação às aprendizagens propostas na atividade, e que é por meio dele que os esforços dos alunos e suas compreensões pessoais se manifestam e se desenvolvem. Entretanto, em nem todos os momentos de dúvidas e dificuldades dos alunos, mesmo com o tempo concedido, este foi suficiente para que eles desenvolvessem suas ideias sozinhos. Em algumas situações, como o episódio descrito abaixo, ocorrido durante a atividade *O detetive Watson*, a pesquisadora precisou interferir um pouco mais, apresentando nos diálogos algumas ideias para se resolver o problema em questão.

Pesquisadora: Aqui a gente viu o quê? O que vocês acham? Tem número positivo?

Igor: Positivo não.

Pesquisadora: Então, aconteceu alguma coisa com o nosso alfabeto que só deu negativo, certo?

Igor: Negativo.

Pesquisadora: Muito bem... ah... olhem para elas com carinho, tem alguma coisa que dá pra gente chutar? Alguma dica, sem ser os números?

Igor: Ah... tem umas letras já.

Pesquisadora: Tem umas letras, né?

Igor: Já, sem número.

Pesquisadora: Tem alguma palavra que tem a letra e que a gente poderia chutar?

Igor e Janaína: Sim, tem U, H, Y, X... e G.

Pesquisadora: E G.

Igor: E U também.

Pesquisadora: E U... esse que tem... tem algum... seleciona essas palavras que têm a letra.

Igor: Vamos ver... cadê o restante?... Alguma palavra que tem H... segunda letra...

Pesquisadora: Essa que tem H é uma palavra grande, né? (chantageada)

Igor: É bem grande.

Pesquisadora: Vocês acham que dá pra chutar alguma?

Igor: Nossa, assim grande eu acho que não...

Pesquisadora: Não, né... tem alguma pequena que dá pra gente chutar?

Igor: Pequena... nossa... essa aqui também é bem grande (aproximar)... parece que as palavras aqui são todas grandes.

Pesquisadora: Não tem nenhuma pequena?

Igor: Só aqui... (um)

Janaína: Aqui, oh [apontando para #U -27#].

Igor: Não, a maioria é tudo grande... olha onde ela começa aqui... ah, não, tá certo, é aqui.

Pesquisadora: Tem duas letras... então, oh. Que palavra tem duas letras e que começa com a letra *u*?

Igor: UM.

Pesquisadora: Muito bem.

Igor: -27 seria M.

Pesquisadora: Ajudou já alguma coisa?

Igor: Ajudou bem... bastante...

***Janaína*:** Para quem não estava fazendo nada...

Pesquisadora: Então, olha só... agora vocês já descobriram que M é igual a -27.

Igor: É.

Pesquisadora: Então, tentem lembrar isso aqui, tá bom! [nessa hora, a pesquisadora se dirige até à lousa e aponta para o desenho dos conjuntos que está desenhado nela]. O que a gente trabalhou na aula passada? A gente sai de um conjunto... 1, 2, 3... bonitinho... o que o Kall chamou de normal, acontece alguma coisa... certo? E chega no nosso alfabeto aqui... o M nesse alfabeto vale quanto?

Igor: No normal?

Pesquisadora: No normal.

Igor: Deixa eu ver.

Igor* e *Janaína: 13.

[...]

Pesquisadora: E agora aqui vale quanto?

Igor: -27.

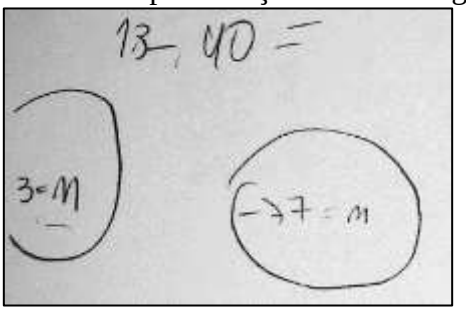
[...]

Após essa interferência, a pesquisadora deixou a dupla refletir um pouco sobre o que eles haviam descoberto (que M valia 13 e agora M passou a valer -27). Depois de um tempo, a pesquisadora perguntou à dupla o que eles haviam concluído e Igor apresentou seus cálculos e a seguinte conclusão:

Janaína: Acho que vai fazendo menos mesmo...

Igor: 13... 13... que eu... subtrai menos o... o 40 do 13... para dar o 27 [apontando para a folha de rascunho (Figura 12)].

Figura 12 - Representação da fala de Igor.



Fonte: Dados da pesquisa (2015).

Pesquisadora: Mas lembra que a gente pensou assim... eu estou retomando as coisas da outra aula, tá?

Igor: Tá certo, professora.

Pesquisadora: Então vamos lá... a gente tem o nosso conjunto bonitinho. Vou usar o M porque a gente já sabe. Porque o M é 13, né?

Igor: Isso.

Pesquisadora: Aí, aconteceu alguma coisa que a gente precisa descobrir e chegou que M vale -27.

Igor: -27.

Pesquisadora: Vocês perceberam que o -27... -27 é o 13 – 40, certo? Tá, a letra *a* vale 1, será que vai dar certo aqui? [apontando para a conta M(normal) = 13 – 40 = -27 = M(novo) na lousa] Vamos ver? Seria o 1 – 40, isso dá o quê?

Igor: 39.

Pesquisadora:-39.

Igor: Isso, -39.

Janaína: Ah!

Pesquisadora: O menor número aí é -39? Que é a letra *a*, né?... Qual é o menor número dessa pista?

Igor: -47, pelo que nós vimos.

Janaína: É -47.

Igor: Pelo que nós vimos, é -47.

Janaína: É -47.

Pesquisadora: E o maior número é quem?

Igor: O maior, se eu não me engano, é 3, -3.

Pesquisadora: -3, então olha só... então, para o M, o que vocês fizeram... mas, para o A falhou, certo?

Igor: Certo.

A pesquisadora observou que os alunos precisavam de mais alguma ajuda para conseguir decifrar esta pista. Assim, ela continuou o diálogo com os alunos, a fim de que eles percebessem o que estava acontecendo com o alfabeto.

Pesquisadora: Então, vamos pensar agora, então, assim... se o meu A é 1, quem é

o primeiro?... O meu primeiro aqui é -3.

Igor: A é -3.

Pesquisadora: A?

Igor: A... não... -3 é o maior.

Pesquisadora: -3 seria o A. Vocês concordam?

Janaína: Eu acho que é.

Igor: É, pode ser que sim.

Pesquisadora: É o maior? Não, né?

Igor: É o maior número... maior número.

Pesquisadora: A gente pode chutar que é o A... pode ser que não dê certo... mas a gente tem que investigar. Então vamos ver. O A valia 1 e foi parar no -3. O M valia 13 e foi parar no -27. O que será que aconteceu? O que eu faço com o A para dar -3? Eu pego o A e faço alguma coisa com esse número. O que será que a gente faz para dar -3?

Igor: Tira 4.

Pesquisadora: Tira 4... tá certo, né?... Vamos ver se para o M dá certo, dá -27?

Igor: Eu acho que não.

Pesquisadora: Dá quanto?

Igor: Eu acho que vai dar -9, não é isso?

Pesquisadora: 9, né?

Igor: É, menos... negativo.

Pesquisadora: 9.

Igor: É, menos.

Pesquisadora: Menos?

Igor: Não... não, verdade, maior.

Pesquisadora: Então não deu -27. Então não é simplesmente o 4.

Igor: É.

Pesquisadora: Vocês percebem que tem que dar certo nos dois, se vocês acharem alguma coisa que dê certo nos dois... manda bala que é por aí.

Igor e Janaína: Nossa...

Igor: Aí fica difícil.

Janaína: Ai, meu Deus...

Igor: Vai... vai dar pra fazer.

Janaína: Então vamos lá.

Pesquisadora: Que outro jeito que dá -3? Vamos pensar, oh! 1 alguma coisa... esse alguma coisa que eu falo pode ser soma ou subtração, como o Igor está tentando, mas pode também ter a multiplicação de um número aqui, tá? É alguma coisa... que vai dar -3. Ele chutou -4 e não deu certo, que outra coisa pode fazer aqui?

Nesse momento, os alunos começaram a falar alguns valores para multiplicar a letra do alfabeto e, em conjunto, os cálculos foram feitos. Foi sugerida a seguinte sentença: $1 \times (-4) + 1 = -3$, mas verificou-se que, para a letra *m*, o resultado dessa conta não batia, pois M daria -51 e não -27, como queríamos. Os alunos também sugeriram as sentenças $1 \times (-4) - 1 = -5$ e $1 \times (-3) - 1 = -4$, mas nenhuma delas estava dando certo. A pesquisadora observou que eles apresentavam muitas dificuldades em encontrar números que dessem certo para esses cálculos. Embora ambos demostrassem entender que o alfabeto criptografado era o resultado de uma multiplicação do alfabeto normal com uma soma (subtração) desse valor, a dupla não encontrava esses valores. Desse modo, a pesquisadora tentou direcionar as ideias dos alunos para a expressão utilizada nessa cifra. Para isso, a pesquisadora sugeriu que os alunos olhassem para a fatoração do número 3.

Pesquisadora: O 3 a gente pode decompor ele com a soma de que números?

Igor: Soma?

Pesquisadora: O mais simples.

Igor: É... 1...

Pesquisadora: A gente pode ter $1 + 1 + 1$. O que mais a gente pode ter?

Igor: É.

Pesquisadora: Que mais que a gente pode ter?

Igor: $2 + 1$.

Pesquisadora: $2 + 1$...

Igor: Acho que é...

Pesquisadora: $1 + 2$.

Igor: Isso também... acho que... só isso.

Pesquisadora: Os primeiros a gente pode usar assim... o que será... o que são esses...?

Igor: Pode ser que seja uma conta aí dentro.

Pesquisadora: Uma conta?

Igor: Não sei, pode...

Pesquisadora: Que número a gente pode pôr aqui? [apontando para o parênteses da expressão $1 \times ( ) - 1 = -3$].

Igor: Um só, você fala?

Pesquisadora: É... um número só. Se aqui for menos e aqui for menos...

Igor: Vai dar mais.

Pesquisadora: A gente teria menos... é esse número menos esse. Quem que vezes 1 com -1 dá -3? [nessa hora, a pesquisadora apontava para a expressão escrita na lousa].

Igor: 1 vezes 1...

Janaína: Olha aqui.

Igor: Acho que...

Pesquisadora: 1 vezes algum número menos 1 dá -3... quem que é esse número aqui?

Igor e Janaína: [depois de discutir um pouco, respondem] Pode ser que seja o próprio 3.

Pesquisadora: O próprio 3? Vamos lá. 1 vezes -3, -3 com -1... -4. Se a gente fixa essa aqui [apontando para o -3] vai cair pra quanto [apontando para o número entre parênteses]?

Igor: Como assim?

Pesquisadora: Oh! A gente tinha feito com (-4) e deu (-5) [apontando para a conta $1 \times (-4) - 1 = -5$, escrita na lousa]. Aí a gente tentou pro (-3) caiu pra (-4) [apontando para a conta $1 \times (-3) - 1 = -4$, escrita na lousa].

Igor: -2.

Janaína: Eu falei isso, professora.

Após esse diálogo, a pesquisadora, com a ajuda dos alunos, realizou os cálculos na lousa e observou com eles que, multiplicando por -2 e subtraindo 1, a letra *a*, que era 1, daria -3, e *m*, que era 13, daria -27. Assim, os alunos concluíram que a expressão matemática utilizada para essa pista era $(-2) \times x - 1$.

Fonte: Gravações de vídeo e áudio, ficha de perguntas e diário de campo (2015).

Mesmo havendo momentos de maior interferência, a pesquisadora percebeu que, nessas horas, os alunos realmente atentavam - se à problemática e que, de alguma forma, eles se envolveram com a proposta. Os alunos se esforçavam em tentar compreender as explicações da pesquisadora e as utilizavam para dar continuidade às resoluções. Mauri (2009) argumenta que é importante que os alunos percebam seus esforços no processo de ensino-aprendizagem e que as expectativas dos alunos em relação à resolução da atividade se acordem às expectativas do professor. Ela ainda evidencia que o professor deve:

> Permitir que o aluno e a aluna apreendam o objetivo da tarefa de aprendizagem, os materiais e as condições de trabalho. Os professores ajudarão os alunos a estabelecer semelhanças entre a nova tarefa de aprendizagem e outras atividades anteriores [...], a elaborar analogias que relacionem essa experiência com outras que estão no repertório dos alunos [...] e a situar a atividade de aprendizagem em relação a outras já realizadas anteriormente (MAURI, 2009, p. 107).

Esse momento de consonância entre as expectativas dos alunos e as da pesquisadora nem sempre ocorreu, no entanto, o fato de a atividade envolver problemas de criptografia dá a ela a característica de se resolver as mensagens cifradas por meio de várias estratégias; contudo, ao chamar a atenção para a transformação cifradora, a pesquisadora tentava guiar os alunos a olhar essa transformação por meio de uma expressão matemática. Assim, como o episódio descrito abaixo, ocorrido durante a atividade *O detetive Watson*, nos momentos em que os alunos se afastavam desse propósito, a pesquisadora tentava resgatá-los para essa ideia e, ao fazer este movimento, os alunos acabavam relembrando situações anteriores que lhes davam subsídios para repensar a situação que estava em discussão.

Igor e Gustavo perceberam que, para essa pista, o menor número que aparecia era o número 1, então eles levantaram a hipótese de que o número 1 poderia ser a letra *a*. Depois eles acharam o segundo menor número, que, neste caso, era o número 9. Para o número 9, eles designaram a letra *b*. Fazendo isso, eles perceberam que de A para B se somou o número 8. Concluindo isso, Gustavo escreveu em sua folha o alfabeto $A = 1, B = 9, C = 17, \dots, Z = 201$, olhando apenas para o padrão mais 8 em cada letra, e, desse modo, eles decifraram a pista.

A pesquisadora percebeu que Igor e Gustavo olharam apenas para o alfabeto cifrado para resolver a 5ª pista. Como o intuito era o de que os alunos associassem o alfabeto cifrado a partir do alfabeto normal, a pesquisadora lançou para os meninos a seguinte pergunta:

Pesquisadora: O que aconteceu daqui para cá?... [apontando para o conjunto do alfabeto "normal" e para o conjunto do alfabeto cifrado desenhados na lousa].

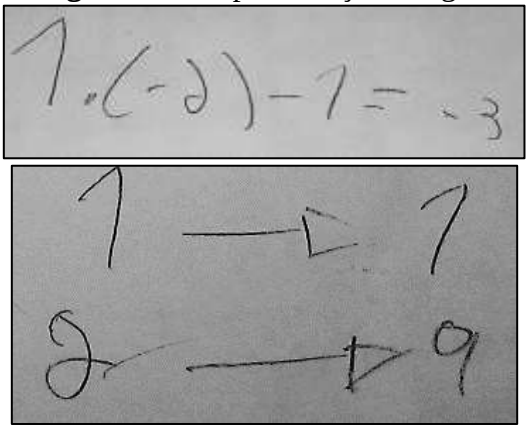
Igor, Fernando e Gustavo demonstraram não entender a pergunta. Então, a pesquisadora falou:

Pesquisadora: Se o A valia 1... ele continuou sendo o 1... mas o B, que valia 2, virou 9, o C, que valia 3, virou 17; o que aconteceu?... O que foi aplicado?

Nesse momento, Igor se pronunciou dizendo que já havia entendido o que a pesquisadora estava falando. Desse modo, a pesquisadora pediu que ele explicasse aos outros meninos. Igor aceitou e, puxando uma folha de rascunho, começou a explicar:

Igor: Tem a ver com o que fizemos na outra cifra, lá fizemos $1 \times (-2) - 1 = -3$. [nessa hora ele escreveu o seguinte esquema na folha (Figura 13)].

Figura 13 - Representação de Igor.



Fonte: Dados da pesquisa (2015).

Com esse esquema escrito, Igor relembrou a expressão $1 \times (-2) - 1 = -3$, utilizada na 3ª pista. Com isso, a pesquisadora argumentou que o número 8 poderia estar em algum lugar daquela expressão e questionou os alunos sobre a posição em que o 8 poderia estar [ao falar isso, a pesquisadora apontou para a posição (-2) e -1 da expressão $1 \times (-2) - 1 = -3$]. Gustavo e Igor responderam sobre a posição apontando para o número -2 e, em seguida, Igor escreveu em sua folha de rascunho as

seguintes expressões: $1 \times (8)$ e $2 \times (8)$.

Igor: 1 vezes 8 dá 8.

Pesquisadora: Dá 8.

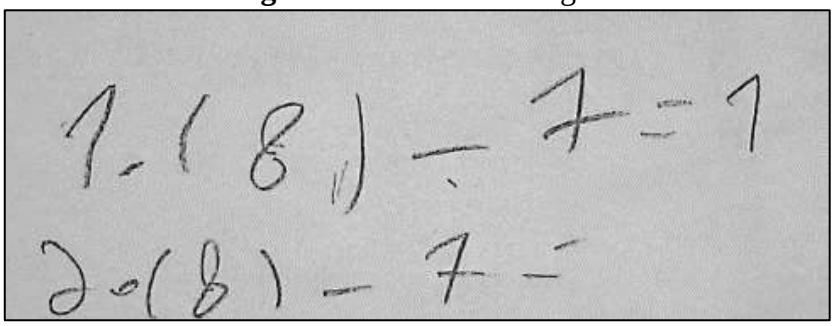
Igor: Dá 8.

Pesquisadora: Mas tem que dar 1... 8 menos o quê dá 1?

Igor: Menos 7 [respondeu já completando a expressão escrita na sua folha (Figura 14)].

Pesquisadora: Muito bem.

Figura 14 - Cálculos de Igor



Fonte: Dados da pesquisa (2015).

Fonte: Gravações de vídeo e áudio, ficha de perguntas e diário de campo (2015).

Com os episódios já apresentados nesta seção, acerca da postura da pesquisadora durante as atividades, já se observa a atitude dos alunos quanto às problemáticas propostas. Com o intuito de que as atividades criadas dessem condições para que os alunos explorassem suas estratégias de resolução, discutissem entre si sobre tais métodos e desenvolvessem um espaço de negociação de significados, no qual os alunos se sentissem como parte daquele aprendizado, é que a pesquisadora foi aos poucos mostrando como esse espaço seria constituído. Nesse sentido, Mauri (2009) argumenta sobre a necessidade da predisposição vinda do professor para facilitar e incentivar a participação e integração dos alunos durante o processo de aprendizagem, debatendo ideias e expondo opiniões.

Essa atitude ativa dos alunos foi sendo construída durante os encontros. De início, eles ainda se mostravam tímidos, e a insegurança sobre como aqueles encontros iriam ocorrer era natural. No entanto, conforme as atividades foram ocorrendo, eles perceberam a dinâmica de

atitude investigativa que estava sendo proposta e cada vez mais ficavam à vontade para expor suas ideias e opiniões. Assim, corroborando Mauri (2009), a pesquisadora tentou:

> Procurar modelos das atitudes que se pretende que os alunos e alunas aprendam na escola e oferecer o apoio e o tempo necessário para que possam ensaiar, testar e imitar. Animar, exigir e apoiar os alunos que tentam mudar, tentando fazer com que eles aceitem o apoio dos demais do grupo e avaliem as críticas que recebem, o trabalho realizado e os sucessos alcançados. (MAURI, 2009, p. 120).

Na entrevista realizada com Jaciara, tempo para a construção dessa postura surgiu quando lhe foi perguntado sobre sua opinião em relação à maneira como as atividades foram desenvolvidas. De acordo com ela, "as atividades foram bem organizadas... cada uma a seu tempo... você não exigiu demais da gente e a gente não exigiu demais de você... foi uma coisa bem regular e completa... a gente aprendeu tudo o que tinha pra aprender" (Jaciara, entrevista, 2015). Por essa fala, percebe-se que a aluna se sentiu confortável com relação ao ambiente desenvolvido durante os encontros. No entanto, houve momentos em que a relação do tempo se tornou delicada. Um contra exemplo a essa questão foi à situação em que a pesquisadora, com medo de que os alunos que faltavam ficassem muito atrasados na atividade em relação aos outros, adiantava algumas explicações para eles sobre os métodos de resolução que os outros alunos já haviam desenvolvido.

Os alunos perceberam esse espaço aberto a discussões e exploravam suas ideias com a ajuda da pesquisadora. Como pode ser observada no excerto a seguir, situação ocorrida durante a atividade *O jogo*, um exemplo desse apoio foi quando Gustavo havia se convencido de que sua estratégia seria mais rápida e eficaz do que a apresentada pela pesquisadora; mesmo a pesquisadora sabendo que tal estratégia, ainda que possível, não seria rápida, apoiou e incentivou Gustavo para que ele explorasse mais suas ideias.

Após várias explicações e exemplos de como se representar um ponto com suas coordenadas, Gustavo concluiu que tentar resolver a atividade olhando para os gráficos seria muito difícil, e que a ideia de se encontrar dois pontos no gráfico para achar sua função e só depois descobrir a mensagem era muito mais complicada. Segundo ele, apenas olhando para as mensagens e usando a lógica do alfabeto e sua frequência de letras, ele conseguiria decifrar as mensagens mais facilmente. A pesquisadora observou que Gustavo estava realmente certo de que sua estratégia seria mais rápida e eficaz, e que tentar direcioná-lo para qualquer outra seria inútil até que ele mesmo pudesse

concluir que seu método não era eficaz em termos de rapidez e talvez de facilidade. Sendo assim, ela ouviu Gustavo e incentivou-o a investigar e explorar suas ideias.

Fonte: Diário de campo (2015).

Observa-se que nesse episódio ouve uma troca de informações em relação às investigações e explorações do problema proposto e com o diálogo pode-se notar um clima de negociação entre a pesquisadora e Gustavo. Esse momento pode explicitar as ideias discutidas por Solé e Coll (2009) em relação às mudanças ou não das ideias interiorizadas pelos alunos, o qual, segundo eles, são justamente os momentos de negociação de significados.

As situações de interação e troca de informações dos alunos entre si e com o professor é destacado por Ponte e Serrazina (2000) por ser um momento vital durante o processo de ensino e de aprendizagem dos alunos. De acordo com esses autores, as interações envolvem relações de diálogos, onde a "comunicação refere-se à produção de mensagens pelos diversos intervenientes na sala de aula, utilizando uma linguagem própria, que é um misto de linguagem corrente e de linguagem matemática" (PONTE; SERRAZINA, 2000, p. 117) e de negociações de significados, onde o espaço de diálogo desenvolvido "respeita ao modo como os alunos e professores expõem uns aos outros o seu modo de encarar os conceitos e processos matemáticos, os aperfeiçoam e ajustam ao conhecimento matemático indicado pelo currículo". (PONTE; SERRAZINA, 2000, p. 117).

Na continuação desse episódio, Gustavo não conseguiu desenvolver suas ideias a ponto de decifrar as mensagens. No momento inicial, ele interpretou a atividade e buscou, em seus conhecimentos, uma estratégia de resolução, no entanto, depois de observar que seu método de resolução não estava ajudando-o a resolver o problema, ele sentiu a necessidade de alterar suas estratégias. Assim, o retrospecto da explicação sobre uma estratégia mais direcionada e rápida foi realizada. Ressalta-se que, essa explicação voltada para a matemática é uma opção da pesquisadora, que ocorre em função do contexto proposto.

Ao iniciar esse encontro, a pesquisadora perguntou a Gustavo se ele havia conseguido resolver ou desenvolver alguma coisa com a estratégia que ele havia pensado antes sobre aquela atividade. Gustavo respondeu que não havia chegado a lugar nenhum. Assim, como ele havia faltado no último encontro e Fernando ainda não havia participado desta atividade em virtude de suas faltas, a pesquisadora, com medo de que essa dupla ficasse muito atrasada em relação à outra, iniciou uma explicação para esses

alunos, tentando mostrar, para eles, o método de resolução que Igor e Jaciara estavam utilizando.

Assim, solicitando a ajuda de ambos, foi pedido que eles escolhessem um gráfico e que dissessem quais eram os pontos pertencentes aos gráficos e ao mesmo tempo pertencentes aos eixos. Gustavo escolheu o gráfico verde e encontrou os pontos (1,0) e (0,-2) pertencentes a ele. Com a ajuda deles, a pesquisadora desenvolveu na lousa o sistema para encontrar a função da reta que passava por esses dois pontos. Após esse diálogo, Gustavo se pronunciou dizendo que já havia entendido e, rapidamente, começou a desenvolver seus cálculos em sua folha de rascunho (Figura 15). Depois de encontrar a função, Gustavo disse que ele não precisava fazer a conta para todas as letras. Ele apenas precisava fazer até encontrar o padrão de uma letra para a outra. Esse raciocínio foi o mesmo pensado por Igor quando apenas estava atentando ao conjunto das imagens da função.

Figura 15 - À esquerda, Gustavo e, à direita, Fernando.

Fonte: Dados da pesquisa (2015).

Fonte: Gravações de vídeo e áudio, ficha de perguntas e diário de campo (2015).

A mudança de postura de Gustavo, ao aceitar a ajuda da pesquisadora, visto que suas ideias não deram certo, vai ao encontro do que Mauri (2009) e Solé e Coll (2009) discutem sobre o discernimento dos alunos sobre suas próprias ações quanto a suas representações e ideias. De acordo com esses autores, o aluno percebe seus limites e se predispõe positivamente a mudá-las. Outro exemplo em que ocorreu essa atitude foi durante a atividade *O poeta assassino*. O trecho abaixo descreve tal situação.

Quando Janaína e Igor terminaram de decifrar as suas segundas frases, ambos argumentaram que decifrar as pistas estava demorando muito, e que essa estratégia de resolução estava se tornando muito cansativa. Jaciara concordou com os argumentos

apresentados por seus colegas.

Observando a necessidade que os alunos apresentaram de encontrar uma estratégia mais rápida para a decifração das frases, a pesquisadora iniciou uma discussão com os alunos para tentar levá-los a observar como se poderiam decifrar as frases do poema sem precisar fazer as contas para todas as letras do alfabeto.

Assim, a pesquisadora perguntou aos alunos se seria possível encontrar o valor de *x* sabendo apenas a função e seu $f(x)$. Os alunos pensaram um pouco sobre essa pergunta, mas não conseguiram articular nenhuma resposta. Para tentar elucidar o que ela estava tentando dizer, a pesquisadora resolveu apresentar um exemplo. Ela escolheu a função $f(x) = 2 \times x + 2$ e pediu que os alunos escolhessem um valor de $f(x)$ que existia na frase cifrada por esta função. Os alunos escolheram o valor 18, assim, tendo $f(x) = 18$ e a função $f(x) = 2 \times x + 2$, a pesquisadora discutiu com os alunos sobre a maneira como eles poderiam encontrar o valor de *x* apenas com esses dois dados. Com a ajuda dos alunos, a resolução da equação $2 \times x + 2 = 18$ foi realizada, obtendo como resposta o valor de $x = 8$, que é representado pela letra *h*.

Nesse momento, os alunos perceberam que não foi preciso achar todo o alfabeto cifrado para descobrir que o valor 18 seria representado pela letra *h*.

[...]

Ao terminar de lhes apresentar a expressão $x = \frac{f(x)-b}{a}, a \neq 0$, observou-se que os alunos ainda tinham algumas dúvidas quanto ao isolamento da variável *x*. No entanto, quando eles tentaram utilizar esse método nas suas frases seguintes, isolar a variável *x* e utilizar a função e suas imagens, pareceu para eles uma ideia mais simples e, segundo Janaína e Jaciara, bem mais rápida do que eles estavam fazendo.

Assim, em suas outras resoluções, os alunos utilizaram a ideia de isolar a variável *x* para descobrir a que letras os valores de $f(x)$ correspondiam. Nesse momento, os alunos fizeram o isolamento da variável *x* para cada $f(x)$, depois eles observaram que poderiam fazer o isolamento da variável *x* com a função e, então, só depois, fazer as substituições de cada $f(x)$ e resolver as contas. Quando os alunos atentaram a esse detalhe, a decifração das frases do poema ocorreu de forma rápida, pois os alunos, em alguns casos, apenas montavam a expressão da função inversa e desenvolviam os cálculos mentalmente.

Fonte: Gravações de vídeo e áudio e diário de campo (2015).

Conforme as atividades iam sendo trabalhadas, os alunos foram criando confiança em suas estratégias e autonomia em direcionar suas ações. As angústias e as inseguranças de errar ou de não encontrar a resposta certa começaram a sair de cena, conforme o espaço das discussões e a liberdade posta a eles se firmavam no ambiente dos encontros. A percepção de suas capacidades e a postura de alunos ativos geraram sentimentos de segurança nas próprias possibilidades de administração das atividades. Nesse sentido, além de levar a situação do ambiente criado, Mauri (2009) explicita que:

> Ter tendência para acreditar que o avanço na construção dos próprios saberes no tocante ao procedimento deve-se ao esforço pessoal. Nesse sentido, os alunos devem estar dispostos a suportar uma execução inicial insegura, pouco organizada ou eficaz, talvez errônea, e interpretar a experiência inicial como um passo necessário para uma aprendizagem significativa e especializada de procedimentos (MAURI, 2009, p. 113).

Freire (2011) também aborda essa mudança de atitude e relaciona a questão da autonomia do aluno com o ambiente de aprendizado desenvolvido em sala de aula. O autor ainda ressalta que a independência dos alunos é construída durante um amadurecimento de todo o dia. De acordo com ele, uma "pedagogia da autonomia tem de estar centrada em experiências estimuladoras da decisão e da responsabilidade, vale dizer, em experiências respeitosas da liberdade" (FREIRE, 2011, p. 105). Em termos dessa responsabilidade, Mauri (2009, p. 118) afirma que o aluno deve "ir elaborando, na medida do possível, critérios pessoais de comportamento ético para poder dar maior relevância a determinadas normas e atitudes em situações concretas e progredir na construção da autonomia pessoal e moral". Dentre todas as ações dos alunos, o interesse em levar as atividades para a casa foi classificado pela pesquisadora como maior evidência dessa atitude de responsabilidade. Como exemplo dessa situação, segue abaixo a descrição da observação da pesquisadora quando o convite foi feito e aceito por alguns alunos, durante a resolução da atividade *O jogo*.

No final desse encontro, a pesquisadora observou que os alunos estavam empolgados em continuar a atividade. Assim, foi perguntado se, por um acaso, eles se interessariam em levar a atividade para casa e tentar dar continuidade a ela. Igor foi o primeiro a se pronunciar, dizendo que ele gostaria de levar a atividade. Gustavo e Jaciara também mostraram interesse em continuar a atividade em suas casas. Janaína argumentou que não gostaria de assumir a responsabilidade de levar para a casa, pois ela sabia que não teria tempo para tentar resolvê-la. Assim, Igor, Gustavo e Jaciara ficaram com a

atividade e se comprometeram a trazê-la para o próximo encontro.

Fonte: Gravações de vídeo e áudio e diário de campo (2015).

Nessa passagem, observa-se que Janaína se preocupou em justificar por que não levaria a atividade. Esse episódio reflete a confiança no grupo que foi sendo estabelecida durante os encontros. O comprometimento dos alunos foi verificado, pois, na continuação deste episódio, e em outros que ocorreu em relação a essa situação, os alunos trouxeram as ideias e estratégias desenvolvidas em suas casas. Em outro momento, por exemplo, antes de iniciar o encontro, o qual daria continuidade com a atividade *O jogo*, a pesquisadora solicitava que os alunos expusessem as ideias pensadas em suas casas, entretanto, essa troca de informação começou a ocorrer sem a pesquisadora pedir – o que evidencia uma autonomia dos alunos ao iniciar suas atividades.

Ao iniciar o encontro, Igor e Jaciara já começaram a trocar entre si o que cada um havia desenvolvido em casa. Jaciara mostrou para Igor todos os cálculos que Janaína havia feito e, nesse momento, Igor retomou com Jaciara a explicação sobre a montagem dos cálculos. Depois de trocarem as informações do que havia sido feito, eles dividiram entre si os gráficos que faltavam e cada um começou a desenvolver a resolução.

Fonte: Gravações de vídeo e áudio e diário de campo (2015).

Nesse trecho, também se podem observar indícios de uma preocupação com o outro, no caso, com a sua dupla. A intenção de situar sua dupla perante o que foi realizado e de trabalhar com ela de uma maneira coletiva se destacou durante os encontros. Em relação ao trabalho em grupo, de acordo com os PCN+[34] (BRASIL, 2002, p. 129) "é um importante recurso para o desenvolvimento das competências". Groenwald e Ruiz (2006) ainda afirmam sobre isso que:

> As pessoas que trabalham em grupo possuem mais idéias, mais energia e mais criatividade para enfrentar obstáculos do que uma pessoa só, além de reforçar as competências individuais. Logo, o resultado de um trabalho em grupo é mais produtivo que a soma das competências individuais (GROENWALD; RUIZ, 2006, p. 21).

[34] PCN+ Ensino Médio: Orientações Educacionais Complementares aos Parâmetros Curriculares Nacionais. Ciências da Natureza, Matemática e suas Tecnologias.

A proposta inicial de trabalho com os alunos foi de reuni-los em duplas ou trios, a fim de poder desenvolver as atividades em um trabalho coletivo. Na primeira atividade, a pesquisadora deixou que os alunos escolhessem suas duplas. A formação destas ocorreu primeiramente pelo fator de amizade e de proximidade. Por exemplo, Janaína e Jaciara, além se serem da mesma sala de Igor, Kall e Luciano, eram muito amigas, o que propiciou que as meninas se juntassem; Gustavo e Fernando eram muito próximos e da mesma sala, o que também ocasionou a formação dessa dupla. Igor, Kall e Luciano acabaram se tornando o trio por exclusão das duas duplas formadas.

Essa afeição pela composição inicial das duplas se enquadra no que Freire (2011) argumenta sobre a formação de grupos. De acordo com ele, "a opção por um determinado grupo (ou querer constituir um), entretanto, é influenciada pela sua identificação com os integrantes do grupo e pela possibilidade de compartilhar problemas, experiências e objetivos comuns" (FREIRE, 2011, p. 60). Após a primeira atividade, em decorrência da fluidez das discussões e da observação da postura dos alunos é que a opção de trocar as duplas foi tomada. Assim, na medida do possível, ou seja, quando todos os alunos estavam presentes, as duplas eram reformuladas.

Essa opção por mudança de duplas foi bem aceita pelos alunos. Isso acarretou uma aproximação com os outros colegas. Mediante este cenário, foi observado que, durante as atividades, os alunos conseguiram trabalhar em grupo. O exemplo que segue abaixo, ocorrido durante a atividade *Um caso de sequestro*, apresenta um episódio em que Leandro, Kall e Igor dividem as tarefas e trabalham conjuntamente na atividade. É possível perceber que os alunos vão aprendendo a mudar as posturas individuais para as coletivas.

Nesse momento, eles começaram a escrever o alfabeto original, já somando a seu valor inicial o número quatro. Leandro tomou a iniciativa e perguntou a Igor qual era a letra que dava no número dezenove. Igor respondeu que era a letra *o*. Leandro falava os números e Igor respondia a que letras eles representavam.

Leandro: 23?
Igor: S.
Leandro: 9?
Igor: E.
Leandro: 21?

Igor: Q.

Leandro foi preenchendo a carta até seu final, mas, no meio da carta, Igor passou sua função, de dizer a Leandro qual era a letra, para Kall, dividindo, assim, a tarefa de ajudar Leandro a preencher a carta. Após Leandro ter terminado de preencher a carta, Kall a pegou e começou a ler, demonstrando muita concentração para entender o que havia sido descoberto na decifração.

Ao entregar a ficha de perguntas para o grupo, Igor leu em voz alta a primeira pergunta e Kall, na mesma hora, deu-lhe a resposta. Ele apontou para a carta e mostrou ao grupo onde estava a resposta para aquela pergunta. Discutindo entre eles, os alunos responderam a todas as perguntas da ficha e ainda montaram, a pedido da pesquisadora, as etapas utilizadas por eles para resolver a atividade. Depois de muita discussão, os alunos chegaram ao consenso de que sua dificuldade fora a de entender como utilizar a cifra de César para decifrar a carta, mas, após encontrar o alfabeto deslocado, eles não tiveram mais nenhuma dificuldade.

Fonte: Gravações de vídeo e áudio, ficha de perguntas e diário de campo (2015).

Outro momento que explicita o trabalho em grupo pode ser observado no trecho a seguir, acontecido na atividade *O poeta assassino*, em que Igor, Janaína e Jaciara dividem as tarefas da atividade.

Olhando para a quantidade de frases que o poema trazia, Igor recomendou uma divisão da tarefa. Ele sugeriu que cada um escolhesse uma função e com ela decifrasse sua frase. Assim, cada um faria a decifração do poema e no final eles juntariam as frases decifradas. As meninas aceitaram sua sugestão e cada um escolheu a frase que desejava decifrar. Desse modo, Jaciara escolheu a primeira frase do poema, a qual era a função $f(x) = x$, Igor a segunda frase, com a função $f(x) = x - 1$, e Janaína a terceira frase, com a função $f(x) = x + 3$.

Fonte: Gravações de vídeo e áudio e diário de campo (2015).

Nesse episódio, observa-se também que é Igor quem sugere a ideia da divisão de tarefas. Dentre outras situações ocorridas durante as atividades do segundo semestre, nota-se que Igor sempre argumentava sobre suas ideias e explicitava sugestões de estratégias e divisão de tarefas. No entanto, durante o primeiro semestre, quem assumia essa atitude era Kall.

Contudo, tanto Kall quanto Igor sempre se preocupavam com suas respectivas duplas. A seguir, dois episódios, ocorridos respectivamente durante a atividade *O jogo* e *O detetive Watson*, exibem a observação da pesquisadora em relação a essa preocupação.

Episódio 1

O grupo de Igor, Jaciara e Janaína não atentou a esse detalhe. Igor tomava a iniciativa e começava a pensar nas funções. Para cada função, Igor montava a equação $a \times x + b = 0$ e a resolvia mentalmente. Após encontrar os valores de *x*, Igor explicou às meninas todo o processo que ele pensou para resolver a equação. Igor sempre se mostrava preocupado em saber se as meninas estavam entendendo tudo o que estava sendo feito, e, por causa dessa preocupação, ele retomava várias vezes as explicações sobre o que ele estava pensando e fazendo (Figura 16).

Figura 16 - Igor explicando para as meninas (Jaciara e Janaína) a primeira questão e o que ele havia pensando e feito a respeito dela.

Fonte: Dados da pesquisa (2015).

Fonte: Gravações de vídeo e áudio, ficha de perguntas e diário de campo (2015).

Episódio 2

Ao terminar de verificar a expressão $13 \times (-2) - 1$, Kall voltou à sua mesa e explicou a Jaciara toda a ideia que o levou a pensar no número (-2) para a expressão $1 \times (?) - 1$. Conforme ele ia lhe explicando, Kall escrevia o alfabeto normal e, ao seu lado, começava a esboçar e a resolver os cálculos com a expressão $x \times (-2) - 1$.

Fonte: Gravações de vídeo e áudio, ficha de perguntas e diário de campo (2015).

A ação investigativa desenvolvida pelos alunos contribuiu para que eles discutissem mais entre si e, assim, desenvolvessem um trabalho coletivo. Ponte e Serrazina (2000)

argumentam que o trabalho em grupo estimula o despontar de novas ideias e conduz a reorganizações das ideias já existentes. Segundo eles,

> O trabalho em pequeno grupo permite que os alunos exponham as suas ideias, ouçam os seus colegas, coloquem questões, discutam estratégias e soluções, argumentem e critiquem outros argumentos. Em pequeno grupo, torna-se mais fácil aos alunos arriscar os seus pontos de vista, avançar com as suas descobertas e exprimir o seu pensamento (PONTE; SERRAZINA, 2000, p. 128).

Da mesma maneira Ponte, Brocado e Oliveira (2009) argumentam sobre o quanto trabalhar em grupo potencializa as investigações e explorações das ideias. No decorrer dos encontros pode-se observar que durante os debates entre os alunos, as discussões das ideias contribuíram para as explorações dos procedimentos de estratégias e consolidação das atitudes investigativas. De acordo com Mauri (2009), esse momento coletivo pode ser decorrente do ambiente de exploração desenvolvido entre eles durante as resoluções das atividades. A liberdade de investigar os problemas e de desenvolver suas próprias estratégias de resolução proporciona uma independência do aluno no sentido de expressar suas opiniões e ideias e debate-las entre os colegas, propiciando, assim, uma construção de novas ideias e opiniões. Em relação a isso, e corroborando Ponte e Serrazina (2000) a autora ainda menciona que o desenvolvimento do trabalho em grupo "permite que os alunos e alunas negociem o significado dos mesmos em situações de atividade conjunta e confrontem suas ideias, podendo resolver dúvidas e usá-las de modo funcional, estudando sua utilidade em diferentes contextos" (MAURI, 2009, p. 116).

O trabalho coletivo também contribuiu para que os alunos desenvolvessem uma melhor organização de suas ideias e estratégias de resolução. O fato de sempre estar se comunicando e de ser comunicado faz com que os alunos melhorassem suas exposições orais e escritas. De acordo com os PCN+ (BRASIL, 2002), o desenvolvimento do trabalho em grupo influencia na comunicação oral dos alunos quando estes, "além de aprenderem uns com os outros, precisam organizar o que sabem para se fazerem entender e, para isso, usam a linguagem que está sendo aprendida" (BRASIL, 2002, p. 129–130). Em relação à comunicação atrelada ao trabalho em grupo Ponte e Serrazina (2000) afirmam que esse momento permite que as ideias se transponham em objetos de reflexão, discussão e refinamento, configurando-se em um momento importante na organização do pensamento das ideias e dos argumentos matemáticos, o qual se torna mais claro quando articulados oralmente ou por escrita. Assim, utilizando os diversos meios de comunicação, os alunos podem "explicar o significado de

conceitos, fazer conjecturas, propor estratégias e soluções para os problemas, devem discutir, testar, aplicar e verificar as suas descobertas. Ao raciocinar em voz alta, desenvolvem em cooperação as ideias e o conhecimento matemático" (PONTE; SERRAZINA, 2000, p. 122).

Essa organização descrita pelos PCN+ (BRASIL, 2002) e por Ponte e Serrazina (2000) pode ser observada nos alunos durante todo o processo de resolução das atividades. Conforme os alunos foram se tornando mais autônomos e ativos, a necessidade de se comunicar ajudou-os a organizarem seus pensamentos tanto nos momentos orais quanto nos escritos. Abaixo seguem alguns episódios observados pela pesquisadora que exemplificam momentos em que essa organização se torna explícita. O primeiro episódio aconteceu durante a atividade *Um caso de sequestro* e os outros dois durante a atividade *O jogo*.

Episódio 1

Durante a exposição das etapas, Kall explicou que seu grupo assumira a expressão "alfabeto normal" para designar o alfabeto enumerado do número um ao número vinte e seis. Destaca-se aqui que a expressão "alfabeto normal", dada por Kall, para se referir ao alfabeto enumerado do um ao vinte e seis, fora assumida por todos os alunos até o final de todos os encontros.

Fonte: Gravações de vídeo e áudio e diário de campo (2015).

Episódio 2

Feito isso, foi solicitado ao grupo que eles, em conjunto, discutissem todos os passos e todos os processos de resolução que eles utilizaram durante essa atividade e que, depois dessa discussão, eles escrevessem esses processos em forma de etapas.

Os três alunos desse grupo iniciaram uma discussão muito interessante. Primeiro eles organizaram todo o material que eles desenvolveram para resolver a atividade. Depois começaram a relembrar quais foram as primeiras ideias que eles tiveram para encontrar as funções. Nesse momento, observou-se que os três alunos estavam muito ativos na discussão e que, embora Igor tenha se destacado em toda a atividade, as meninas Jaciara e Janaína estavam sabendo organizar seus pensamentos e, junto com Igor, construindo os passos que eles utilizaram para decifrar as frases da mensagem. Posteriormente a essa discussão, os três entraram em consenso em relação às etapas e foi solicitado que Jaciara escrevesse os passos em uma folha. Conforme Jaciara escrevia, Igor e Janaína liam e argumentavam se estava faltando algo ou se estava bom

o que Jaciara estava colocando em cada etapa.

Fonte: Gravações de vídeo e áudio e diário de campo (2015).

Episódio 3 Mudando, então, a dinâmica das discussões, antes de começar a responder à ficha de perguntas, foi pedido que os alunos fossem até a lousa e que apresentassem a forma como cada um havia encontrado a função de cada gráfico. Nesse momento, os alunos se auto-organizaram da seguinte forma: O aluno que ia à lousa escolhia o gráfico com o qual ele desejava encontrar a função. Um dos outros dois alunos que estavam sentados na carteira ajudava o que estava na lousa, ditando para ele os cálculos que ele deveria fazer. Após terminar os cálculos e encontrar a função, os papéis dos alunos se alternavam, dando a oportunidade de os três irem à lousa e de os três ditarem as coisas para o outro. Com essa dinâmica, a pesquisadora conseguiu observar individualmente cada aluno sobre a organização dos pensamentos e sobre as estratégias de resolução que eles utilizaram durante toda a atividade.

Fonte: Gravações de vídeo e áudio e diário de campo (2015).

Por meio desses três episódios apresentados acima, podem-se observar a atitude investigativa dos alunos, o trabalho compartilhado ocorrido entre eles e a organização desenvolvida para as apresentações e discussões sobre suas estratégias de resolução. A sequência pedagógica de atividades envolvendo problemas criptográficos foi desenvolvida a fim de oferecer aos alunos problemas com desafios crescentes. A postura dos alunos, em parte, é decorrente da postura da pesquisadora, do ambiente propiciado pelas atividades e da própria característica dos problemas: a particularidade de serem criptografados. Os alunos foram se envolvendo nas explorações de estratégias de resolução, acabando por assumir atitudes investigativas em seus próprios processos de aprendizagem. Na próxima seção, apresentaremos a parte de procedimentos, a qual se mostrou extremamente importante na compreensão das ideias associadas à função afim, a partir das diferentes estratégias de resolução desenvolvidas.

4.2 Pr0cedimentos

Esta seção argumentará sobre os procedimentos produzidos pelos alunos durante as atividades. Entende-se por procedimentos todas as ações organizadas a fim de se chegar à obtenção de uma meta. De acordo com Echeverría e Pozo (1998), a solução de problemas está relacionada à consecução de procedimentos eficazes, e que, sem estes – sendo de habilidades ou estratégias –, o aluno não resolverá o problema. Esses autores ainda argumentam sobre a adaptação dos alunos à estrutura da atividade. Em relação a isso, observa-se que inicialmente cada aluno reagiu de uma maneira diferente em relação à primeira atividade. Os obstáculos encontrados por eles nesse primeiro contato com a criptografia não podem ser totalmente atribuídas às diferenças individuais de capacidades de resolver problemas, mas tem-se que levar em consideração o tipo de atividade apresentada e as diferenças na aprendizagem dos alunos no momento de suas resoluções. Nesse sentido, ocorreram três situações distintas durante a atividade *Si-lá-box* quanto aos obstáculos iniciais de adaptação da atividade.

Janaína e Jaciara

As meninas não conseguiram responder a todas as dicas e, no final da atividade, chutaram as respostas das que não sabiam. Segundo elas, procurar as respostas das dicas foi o mais difícil, e disseram que realmente elas não haviam percebido que poderiam utilizar os símbolos para resolver as dicas.

Fonte: Gravações de vídeo e áudio, ficha de perguntas e diário de campo (2015).

Igor, Luciano e Kall

Para esse grupo, o entrave desta atividade estava em achar o significado dos símbolos, e a facilidade por eles destacada foi o fato de as respostas das dicas estarem separadas em sílabas, o que, segundo eles, facilitou na hora de "chutar" as respostas.

Fonte: Gravações de vídeo e áudio, ficha de perguntas e diário de campo (2015).

Gustavo e Fernando

Este grupo foi o primeiro a acabar a atividade e, segundo eles, não existiu nenhum obstáculo em resolver a atividade. Nas palavras de Gustavo: – tudo foi fácil.

Fonte: Gravações de vídeo e áudio, ficha de perguntas e diário de campo (2015).

Após esse primeiro contato com a atividade envolvendo problemas criptográficos, os alunos começaram a compreender melhor as características desse tipo de problema e as

barreiras inicialmente encontradas foram sendo superadas ao longo das atividades, como por exemplo, o de os alunos não ter conhecimento sobre o que era criptografia. Entender o que essa palavra significava elucidou os alunos quanto à postura que os mesmos deveriam ter perante aquelas atividades. Saber seu significado orientou os alunos a se posicionarem no campo das investigações e das estratégias de resolução.

Echeverría e Pozo (1998) argumentam sobre essa compreensão dos problemas. De acordo com eles, o primeiro passo na resolução de problemas consiste na assimilação dos mesmos, e a atitude de assumir uma disposição para resolvê-los é imprescindível. Os autores ainda complementam que, "para que essa compreensão ocorra, é logicamente necessário que, além dos elementos novos, o problema contenha problemas já conhecidos que nos permitam guiar a nossa busca de solução" (ECHEVERRÍA; POZO, 1998, p. 22). Mauri (2009) argumenta nesse sentido, que no campo dos procedimentos é necessário que os alunos relembrem de fatos isolados e convenientes para a resolução do problema. Esse relembrar é designado por ela como sendo a ativação e recuperação da memória. Este momento, segundo a autora é imprescindível na transição dos pensamentos e ideias às ações de resolução dos problemas. De acordo com ela, a retomada desses fatos isolados e suas combinações adequadas ao problema estão atreladas ao movimento de regulação do próprio processo de aprendizagem e com a construção das novas estruturas de significados.

O fato de as atividades irem aumentando seu grau de complexidade fez com que os alunos sempre se deparassem com novos desafios, e, mesmo muitas vezes utilizando estratégias e recursos já pensados em atividades anteriores, indícios de novas ideias, estratégias e organização sempre surgiam. Por exemplo, no episódio descrito abaixo, ocorrido durante a atividade *Um caso de sequestro*, Igor utiliza a ideia de que as letras do alfabeto foram relacionadas a números. Essa associação havia sido comentada e discutida no encontro anterior, o qual abordou a definição de criptografia. Essa ideia lembrada por Igor guiou-o a iniciar uma estratégia de resolução da carta criptografada, no entanto, sua cifração requeria um pouco mais de reflexão. A ideia de Igor gerou discussões em seu grupo e auxiliou Kall a se lembrar de outra maneira pela qual aquela carta poderia ter sido cifrada.

Os alunos desse grupo analisaram a carta criptografada e perceberam, muito rápido, que o símbolo asterisco (*) estava sendo utilizado para representar os espaços entre as palavras. Os alunos também perceberam que, como a primeira palavra da carta se constituía apenas por uma letra, essa palavra teria que ser uma vogal. O aluno Igor

> “chutou” a vogal *o*, mas, ao associar as letras do alfabeto aos números, ele percebeu que a letra *o* estava associada ao número quinze, e na carta o número que aparecia era o dezenove. Nesse momento, Igor se pronunciou dizendo que os números que apareciam na carta não eram simplesmente a numeração do alfabeto. [...]
> Igor explicitou suas conclusões ao restante de seu grupo. Os meninos também chegaram a pensar em enumerar o alfabeto de trás para frente, mas essa hipótese foi refutada rapidamente após eles verificarem que assim também não daria certo. Após algumas discussões, Kall chamou a pesquisadora e perguntou se era a cifra de César, apresentada no encontro anterior, que fora utilizada para cifrar aquela carta. Para Kall, era essa cifra que havia sido utilizada para cifrar a carta.

Fonte: Gravações de vídeo e áudio e diário de campo (2015).

No trecho acima, pode-se observar que os alunos exerceram uma postura investigativa, pois eles compreenderam o problema, levantaram algumas hipóteses de resolução, executaram essas hipóteses e as analisaram. Essas etapas se assemelham muito às etapas destacadas por Echeverría e Pozo (1998) e Ponte, Brocado e Oliveira (2009). De acordo com esses autores, o primeiro passo para a resolução de um problema deve ser a compreensão do mesmo, em seguida o estabelecimento de um plano que conduza a sua resolução, depois vindo a execução desse plano e, por último, a análise do sucesso ou não da resolução. Junto com essas fases estão os métodos heurísticos, que são desenvolvidos a fim de se buscar uma solução para o problema.

Os procedimentos heurísticos são definidos como sendo os planos, metas e submetas que os alunos desenvolvem durante a busca da solução da atividade. Retomando na memória fatos parecidos, o raciocínio heurístico possibilita os alunos a guiar o caminho da resolução do problema e em toda a ação dos mesmos durante a exploração e investigação da atividade. Essa busca por procedimentos provisórios e plausíveis contribui para o cenário investigativo, no sentido que, tais procedimentos, geram discussões entre professor e alunos e auxiliam na autonomia de aprendizagem dos mesmos (ECHEVERRÍA; POZO, 1998; MAURI, 2009). No episódio abaixo, pode-se observar que Igor e Janaína, após compreenderem a atividade, começam a levantar hipóteses e a raciocinar de maneira heurística. Sem rigor e apenas com certo grau de plausibilidade, os alunos começaram a analisar um dos gráficos apresentados na atividade *O jogo* e, por meio de suas observações superficiais, desenvolveram e executaram um plano de resolução.

A dupla Igor e Janaína não demonstrou ter dificuldades em compreender o que era para ser feito nessa atividade, nem de que maneira eles poderiam resolvê-la. De início, eles associaram os valores positivos do eixo x com os valores do alfabeto $A = 1$, $B = 2 \ldots Z = 26$. Em seguida, começaram a observar o gráfico verde e, com essa observação, levantaram as hipóteses de que $f(B) = 2$ e $f(A) = 0$. Com esses dados, tentaram descobrir os valores dos coeficientes a e b da função $f(x) = a \times x + b$ que representassem o gráfico verde. Eles começaram a pensar e fazer alguns cálculos até chegarem aos valores dos coeficientes $a = 2$ e $b = -2$, criando, assim, a função $f(x) = 2 \times -2$. Ao atribuir outros valores de *x* para essa função, eles concluíram que os valores dos gráficos não estavam se ajustando a essa função e, nesse momento, chamaram a pesquisadora para pedir ajuda.

Fonte: Gravações de vídeo e áudio, ficha de perguntas e diário de campo (2015).

Durante as atividades, os alunos desenvolveram vários procedimentos heurísticos. Depois de compreenderem os problemas, os alunos estabeleciam seus planos e subdividiam a resolução dos problemas. Por exemplo, na atividade *O detetive Watson*, os alunos perceberam que as pistas formavam um quebra-cabeça, assim, eles montaram o quebra-cabeça e repararam que em sua montagem existia uma sequência de setas indicando uma ordem das pistas. Os alunos então decidiram começar a decifrar as pistas conforme as setas lhes eram apresentados. Somente após decifrarem todas as pistas é que os alunos organizaram todas as mensagens cifradas e conseguiram responder ao mistério do conto. Echeverría e Pozo (1998) argumentam sobre as variedades desses procedimentos, destacando alguns, como: "realizar tentativas por meio de ensaio e erro; aplicar a análise meios-fins; dividir o problema em subproblemas; decompor o problema; procurar problemas análogos e ir do conhecido até o desconhecido" (ECHEVERRÍA; POZO, 1998, p. 25). Em relação a isso, pode-se assumir que as investigações desenvolvidas pelos alunos envolvem características de formulação de conjecturas e suas análises quanto a validações ou refutações das mesmas, além de contribuir para a organização na apresentação das ideias, em papel ou oralmente, para o professor e seus colegas (PONTE; BROCADO; OLIVEIRA, 2009; BNCC, 2015).

Nesse sentido, os PCN+ (BRASIL, 2002), discorrem sobre a postura do aluno em analisar o problema e o compreendê-lo por inteiro, a fim de poder tomar decisões sobre suas possíveis estratégias de resolução a partir de seu raciocínio heurístico, além de poder argumentar, expressar e registrar seus métodos de resolução. Com essa atitude, e os diversos procedimentos heurísticos disponíveis, os alunos conseguiram desenvolver e identificar

diferentes estratégias de resolução para um mesmo problema. A seguir, observam-se três episódios (ocorridos respectivamente nas atividades *Um caso de sequestro*, *O detetive Watson* e *Criptograma*) descritos pela pesquisadora que evidenciam a criação, transição e identificação de estratégias diferentes de resolução, por meio do raciocínio heurístico, em uma mesma atividade.

Episódio 1

Fernando começou a decifrar a carta colocando a letra *o* em todos os números dezenove que ele encontrava. Depois, ele fez a mesma coisa com a letra *a* e com a letra *s*, e seguiu essa mesma estratégia de resolução até a decifração de toda a carta. Já as meninas, embora tivessem colocado, de início, todas as letras *o* que apareciam na carta, não seguiram esse mesmo raciocínio para preenchê-la. Elas olhavam qual seria o próximo número da palavra e a preenchiam com sua letra correspondente. Utilizando-se desse processo, Jaciara sugeriu que tentassem formar as palavras antes mesmo de acabar de preenchê-las. Janaína acatou a sugestão e ambas foram decifrando a carta, transitando entre essas duas estratégias de resolução desenvolvidas por elas.

Fonte: Gravações de vídeo e áudio e diário de campo (2015).

Episódio 2

Enquanto Igor terminava de escrever o alfabeto cifrado, Gustavo chamou a pesquisadora para dizer que eles desenvolveram vários jeitos de encontrar o alfabeto cifrado. Foi pedido, então, que eles escrevessem quais seriam esses três métodos de encontrar o alfabeto cifrado. Seguem, abaixo, os três exemplos citados por Gustavo.

1) Você pega a letra do alfabeto e soma a ela o mesmo valor da letra, depois você soma mais um no final. O nº cifrado será o nº negativo dessa soma.

   Ex.: A=1

   $(1 + 1) + 1 = 3$ => -3 A

   B = 2

   $(2 + 2) + 2 = 5$ => -5 B

   C = 3

   $(3 + 3) + 3 = 7$ => -7 C

2) Você pensa em uma expressão que utilize o nº do alfabeto normal para se

chegar ao alfabeto criptografado.
Para a 3ª pista, a expressão é $(-2) \times x - 1$ e se faz a conta para todas as letras do alfabeto.

3) Você encontra a expressão utilizada para cifrar as letras, que, neste caso, é $(-2) \times x - 1$. Realiza os cálculos para as primeiras e observa o padrão que ocorre no resultado das contas. Depois é só completar o alfabeto apenas somando o padrão.
Para a expressão $(-2) \times x - 1$, observou-se que os números aumentavam -2. Assim, a partir de x = 8, era só ir somando (-2) aos resultados.

Ex.: $7 \times (-2) - 1 = -15$

$8 \times (-2) - 1 = -17$ e $(-15) + (-2) = -17$

$9 \times (-2) - 1 = -19$ e $(-17) + (-2) = -19$

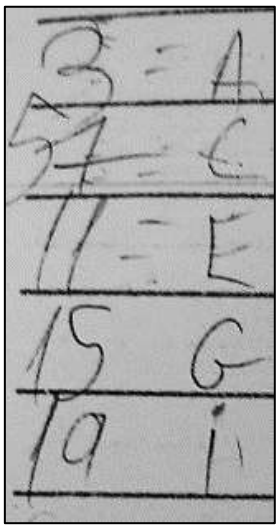
$10 \times (-2) - 1 = -21$ e $(-19) + (-2) = -21$

Fonte: Gravações de vídeo e áudio, ficha de perguntas e diário de campo (2015).

Episódio 3

Essa dupla, após observar o criptograma, começou a responder a todas as dicas que eles sabiam. Quando eles não souberam mais responder, Gustavo começou a escrever em seu rascunho todas as informações que sabia sobre as letras cifradas (Figura 17).

Figura 17 - Informações que Gustavo retirou das dicas respondidas no criptograma.



Fonte: Dados da pesquisa (2015).

Depois de observar o que Gustavo estava anotando, a pesquisadora o questionou sobre

o que ele estava pensando em fazer. Segundo Gustavo, ele apenas estava colocando na folha de rascunho as informações já conhecidas. Com isso, foi perguntado a eles se, com aqueles dados e conhecendo o jeito da função utilizada, seria possível determinar os coeficientes *a* e *b* da função afim. Os meninos pensaram sobre o argumento dado pela pesquisadora, mas Gustavo afirmou que ele conseguiria achar o resto do alfabeto sem ter que encontrar esses coeficientes.

Desse modo, Gustavo observou que os números já conhecidos eram todos números ímpares, começando pelo número 3. De acordo com ele, esse pensamento estava dando certo e, assim, ele escreveu em sua folha de rascunho todo o alfabeto, seguindo a lógica de que os próximos números seriam ímpares. [...] Com todo o alfabeto escrito, Gustavo e Fernando completaram as dicas que faltavam e terminaram rapidamente a atividade.

Fonte: Gravações de vídeo e áudio, ficha de perguntas e diário de campo (2015).

Outro acontecimento relevante, dentre esses procedimentos já citados, foi a utilização da calculadora pelos alunos durante as atividades. Essa ferramenta esteve presente em todos os encontros, e os alunos souberam utilizá-la de duas formas, a saber: para resolver algum cálculo ou para a verificação de algum já feito. Um episódio muito interessante envolvendo a calculadora ocorreu durante a atividade *O detetive Watson*, com a dupla Kall e Jaciara.

Conforme ele ia lhe explicando, Kall escrevia o alfabeto normal e, ao seu lado, começava a esboçar e a resolver os cálculos com a expressão $x \times (-2) - 1$. A resolução dos cálculos estava sendo feita mentalmente, embora ao lado da dupla houvesse uma calculadora. Somente na metade do alfabeto Jaciara começou a utilizar a calculadora para resolver os cálculos, mas o curioso era que Kall não se interessou em utilizar a calculadora e ele continuou atentamente resolvendo as contas mentalmente. Assim, conforme Kall ia colocado as respostas das contas, Jaciara utilizava a calculadora para conferir se a resposta da respectiva conta estava certa. Nesse momento, a pesquisadora observou que Kall conseguiu organizar as contas mentalmente e, com calma e atenção, ele havia feito todos os cálculos corretamente.

Fonte: Gravações de vídeo e áudio e diário de campo (2015).

Nesse episódio, observa-se que, embora Kall pudesse ter utilizado a calculadora, ele preferiu continuar realizando seus cálculos mentalmente. No entanto, Jaciara realizava os cálculos a fim de confirmar os valores que Kall estava encontrando para aquele alfabeto.

A utilização da calculadora para verificação das contas também ocorreu em outro momento. Durante a atividade *Cifrando sua história*, Janaína utilizava essa ferramenta apenas para verificar suas contas, enquanto que Jaciara a utilizava para realizar os cálculos.

Igor criou a função $f(x) = 10 \times x + 2$ e, mesmo montando as contas na tabela, ele resolvia os cálculos um por um mentalmente. Jaciara bolou a função $f(x) = 12 \times x + 8$ e, primeiro, ela montou todos os cálculos para as 26 letras e, somente depois, ela começou a resolvê-los. Janaína inventou a função $f(x) = 10 \times x + 8$ e, para cada letra do alfabeto, montava o cálculo e, logo em seguida, resolvia. Tanto Janaína quanto Jaciara utilizaram a calculadora para ajudar nos cálculos. No entanto, nessa atividade, observou-se que Janaína utilizava a calculadora apenas para verificá-los, já Jaciara a utilizava para resolvê-los.

Fonte: Gravações de vídeo e áudio, ficha de perguntas e diário de campo (2015).

Após todas as atividades, a pesquisadora observou que os alunos utilizaram a calculadora como uma ferramenta de apoio durante o processo de resolução, e que esta era resgatada pelos alunos conforme suas necessidades. Assim, observa-se que essa ferramenta contribuiu com os alunos durante o processo de resolução e que eles a souberam utilizar de diferentes formas e em diferentes momentos. Em relação à utilização dessa ferramenta em sala de aula, Olgin (2011, p. 15) afirma que "as calculadoras possibilitam que o estudante dedique maior concentração às estratégias para resolução de problemas, não desperdiçando tempo com cálculos longos e repetitivos". Bigode (1998) também argumenta sobre a utilização das calculadoras pelos alunos durante o processo de resolução. De acordo com ele,

> A calculadora pode e deve ser usada em sala de aula sempre que o cálculo for um passo do trabalho, e não a atividade principal. Para que seus alunos usem a calculadora com inteligência, o professor precisa selecionar atividades adequadas, que sejam motivadoras e despertem a curiosidade, ajudando a raciocinar (BIGODE, 1998, p. 43).

As atividades apresentadas aos alunos se encaixam exatamente no modelo de atividade citada acima por Bigode (1998). Com a autorização[35] da pesquisadora ao uso da calculadora durante as atividades, observou-se que os alunos atentaram mais aos problemas das atividades do que aos cálculos. Isso vai ao encontro da fala de Bigode (1998, p. 45), quando afirma que "quando liberados do cálculo, os alunos conseguem se concentrar melhor nas relações entre os dados, nas condições e nas variáveis dos problemas. Em outras palavras, canalizam suas energias para o raciocínio".

Assim, dentre todos os episódios apresentados nesta seção, pode-se observar que os alunos levantaram hipóteses, executaram seus planos e tentaram enxergar o problema sob pontos de vista distintos. Encarar as mensagens cifradas sob ângulos diferentes e tentar, de alguma forma, decifrá-las proporcionou que os alunos adquirissem habilidades para selecionar informações do problema, analisar esses dados disponíveis, adequá-los a possíveis outros problemas já resolvidos, desenvolver linguagens e procedimentos matemáticos, e verificar e refutar conjecturas elaboradas por meio de seus raciocínios heurísticos. Todas essas ações transitaram entre os processos de resolução das atividades, nas quais os alunos tiveram autonomia, como já discutido na seção anterior, para trabalharem com suas ideias, seus materiais, suas estratégias e seus questionamentos da melhor maneira que lhes interessasse, para atingir a resolução da atividade. Na seção que segue, serão discutidos os conceitos desenvolvidos e relembrados nas atividades, conforme foram ocorrendo as investigações das estratégias de resolução e seus procedimentos heurísticos.

4.3 C0nceit0s

As ideias associadas ao conceito de função afim foram sendo exploradas pelos alunos a partir da segunda atividade, no entanto, só após as discussões e formalização de sua definição, ocorridos na terceira atividade, é que os alunos foram apresentados formalmente a este conceito. Conforme as atividades foram ocorrendo, observou-se que os alunos amadureciam cada vez mais as ideias relacionadas à função afim. Esse amadurecimento ocorreu em conformidade com a atitude dos alunos e o desenvolvimento de seus procedimentos heurísticos. A liberdade e a autonomia que os alunos tinham em desenvolver suas próprias estratégias de resolução, de discutir e questionar tais processos, e de verificar ou refutar seus planos de execução levaram os alunos a irem explorando cada vez mais o conceito de função

[35] De acordo com os alunos, o uso da calculadora na escola era proibido. No entanto, para os encontros com a pesquisadora seu uso foi concedido pela mesma.

afim, tanto em sua definição como em sua linguagem, por meio de tabelas e gráficos. De acordo com Mauri (2009, p. 110), a aprendizagem de conceitos vem com o trabalho de procedimentos e atitudes. Nesse sentido, ela complementa que se podem diferenciar os procedimentos e a atitude, visto que os primeiros são desenvolvidos por sua potencialidade durante a construção do conhecimento e o segundo refere-se ao aprender a aprender e deter o controle de sua própria atividade de aprendizagem e pensamento (MAURI, 2009).

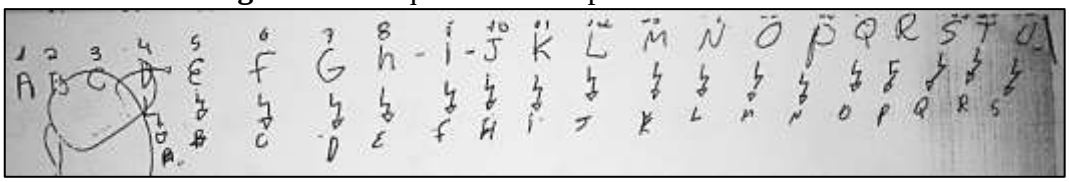
Desse modo, com as atitudes dos alunos sendo consolidadas e as estratégias cada vez mais desenvolvidas, é que o conceito de função afim foi sendo trabalhado. No entanto, não foi somente esse conceito que foi discutido durante as atividades. Os conhecimentos prévios dos alunos proporcionaram aos mesmos utilizar estratégias de resolução durante as atividades, bem com explorar outros conceitos da Matemática. Por exemplo, o episódio abaixo descreve uma situação que ocorreu com alguns alunos em relação à segunda atividade (*Um caso de sequestro*).

Janaína, Jaciara e Fernando

Para iniciar a resolução da atividade, Jaciara e Janaína escreveram em seu rascunho o alfabeto e perceberam que o símbolo asterisco (*), que aparecia na carta, representava o espaço entre as palavras. Logo em seguida, as meninas enumeraram o alfabeto ($A = 1, B = 2, \ldots, Z = 26$) e perceberam que o número dezenove correspondia à letra S, e concluindo que não era essa a numeração que havia sido utilizada na carta. Jaciara sugeriu que elas começassem a numeração de trás para frente ($A = 26, B = 25, \ldots, Z = 1$), mas, com esse novo alfabeto, elas também perceberam que não fazia sentido, pois o número dezenove correspondia à letra *h*.

Enquanto as meninas discutiam outra forma de enumerar o alfabeto, Fernando pensava em decifrar a carta por meio da cifra de César. Ele escreveu, em seu rascunho, o alfabeto original e logo abaixo o mesmo alfabeto, só que deslocado para à direita (Figura 18).

Figura 18 - Esquema escrito pelo aluno Fernando.



Fonte: Dados da pesquisa (2015).

Ao começar a enumerar o alfabeto deslocado, Fernando começou a designar o número um a partir da letra *d*, pois, segundo ele, como o um se iniciava na letra *a* no alfabeto original e agora a letra *a* começava na letra *d*, o número um tinha que começar na letra *d*. Ao fazer, então, toda essa enumeração, Fernando observou que o número dezenove correspondia à letra *v*; então, ele percebeu que algo estava errado, pois não fazia sentido (na língua portuguesa) uma palavra ser constituída apenas pela letra *v*.

Fonte: Gravações de vídeo e áudio, ficha de perguntas e diário de campo (2015).

No episódio acima, observam-se três momentos em que os alunos utilizam seus conhecimentos prévios para iniciar ou desenvolver suas estratégias de resolução. A primeira situação é quando as meninas supõem intuitivamente que o espaço entre as palavras poderia estar sendo representado pelo símbolo asterisco. A segunda e terceira situações ocorrem quando as meninas e Fernando enumeram o alfabeto para tentar resolver a carta. A refutação da hipótese de enumerações do alfabeto, realizada por eles, ocorreu em virtude do primeiro espaço apresentado na carta ser referente ao número dezenove.

Em outros momentos, os conhecimentos trazidos pelos alunos eram referentes a conceitos matemáticos, como, por exemplo, situações que abordaram o conhecimento de números primos, números pares, ímpares e múltiplos de três, conceito de plano cartesiano e de paralelismo de retas. Abaixo são descritos alguns episódios (ocorridos respectivamente os dois primeiros na atividade *O detetive Watson*, o terceiro em *Criptograma* e o quarto em *O jogo*) em que esses conceitos foram abordados pelos alunos durante as atividades.

Episódio 1

Para a 2ª pista, Kall chamou a pesquisadora para apresentar sua ideia.

Kall: Agora, aqui, vai ser um esquema diferente. Aqui eu acho que vai ser números...

Jaciara: Nossa! Igual ao 4...

Kall: Números primos.

Pesquisadora: Números primos?... Hum... mas 12 é um número primo?

Kall: Não!

Pesquisadora: Então uma pista já descartada fora. Uma ideia. Qual a outra ideia?

Jaciara: Aqui não é a cifra de César?

Fonte: Gravações de vídeo e áudio (2015).

Episódio 2

Para ajudar os meninos, a pesquisadora questionou sobre o que eles percebiam ao olhar a 4ª pista. Gustavo argumentou que naquela pista havia números pares e ímpares e Fernando complementou dizendo que aqueles números eram múltiplos de 3. Nesse momento, a pesquisadora chamou a atenção perguntando se, na pista, havia números positivos. Gustavo respondeu dizendo que não, e daí Fernando argumentou que, então, eles eram múltiplos de -3.

Fonte: Gravações de vídeo e áudio e diário de campo (2015).

Episódio 3

Quando eles chegaram à questão que solicitava a representação do esquema criptográfico por meio do plano cartesiano, Igor se pronunciou dizendo que lembrava o que era um plano cartesiano e, para mostrar isso, ele desenhou com o dedo, no espaço, as retas do plano. Ao ser questionado sobre qual era o eixo das abcissas e qual era o das ordenadas, Igor soube responder corretamente. A pesquisadora também perguntou à dupla se eles saberiam dizer qual alfabeto seria representado pelo eixo x e qual pelo eixo y. Jaciara respondeu corretamente e Igor explicou rapidamente com gestos o porquê de a resposta dela estar certa.

Fonte: Gravações de vídeo e áudio e diário de campo (2015).

Episódio 4

Pesquisadora: Vocês conseguem perceber que uma é paralela à outra?... Certo? Olhem para as negativas, olhem para a roxa e olhem para a azul clara, elas também são paralelas. [...] Então, quando os nossos coeficientes *a* são iguais, o que acontecem com os nossos gráficos?

Igor: São paralelos.

Pesquisadora: São paralelos. [...] Se os *a* são diferentes, eles não são paralelos eles se...?

Igor: Se cruzar em algum momento.

Pesquisadora: Eles se cruzam em algum ponto.

Fonte: Gravações de vídeo e áudio e diário de campo (2015).

Em relação ao conhecimento prévio dos alunos, os PCNEM (BRASIL, 2000) afirmam ser muito relevante que tal conhecimento seja levado em consideração durante o aprendizado dos alunos. De acordo com eles,

> Os alunos chegam à escola já trazendo conceitos próprios para as coisas que observam e modelos elaborados autonomamente para explicar sua realidade vivida, inclusive para os fatos de interesse científico. É importante levar em conta tais conhecimentos, no processo pedagógico, porque o efetivo diálogo pedagógico só se verifica quando há uma confrontação verdadeira de visões e opiniões; o aprendizado da ciência é um processo de transição da visão intuitiva, de senso comum ou de auto-elaboração, pela visão de caráter científico construída pelo aluno, como produto do embate de visões (BRASIL, 2002, p. 52).

Nesse sentido, Mauri (2009) também argumenta sobre a importância dos saberes pessoais dos alunos. Segundo ela, os conhecimentos prévios trazidos pelos mesmos, quando organizados, são pertinentes e relevantes, pois contribuem para interligar as novas informações durante a construção de saberes. Essas conexões puderam ser vistas durante todas as atividades, pois a partir ou com os conhecimentos prévios, os alunos desenvolveram suas estratégias e construíram suas ideias associadas ao conceito de função afim. Para Echeverría e Pozo (1998, p. 24), esses conceitos preliminares se "constituem em conhecimentos adquiridos que permitem transformar a informação de uma maneira fixa, eficaz e concreta, embora possam ser utilizadas num grande número de situações". Abaixo, serão apresentados quatro episódios (primeiro e segundo episódio ocorrido na atividade *O detetive Watson*, terceiro episódio em *Criptograma* e quarto episódio em *O jogo*) que mostram como a associação das ideias relacionadas ao conceito de função afim foi sendo explorada e utilizada pelos alunos durante as atividades.

Episódio 1

Kall começou a esboçar a sua ideia [de que aqueles números da carta eram múltiplos de -3] em uma folha de rascunho. Ao mesmo tempo em que falava, ele escrevia:

Kall: $a(-3) = (-3)$ [nesse momento ele pára, corrige seu raciocínio e continua].

Kall: $a(1) = (-3) \times 1$ e $a(2) = (-3) \times 2$.

Pesquisadora: $a(3)$ dá quanto?

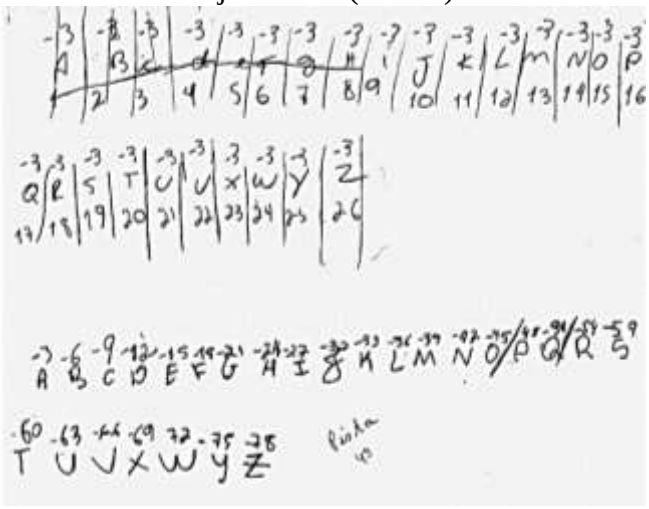
Kall: 9.

Pesquisadora: 9?

Kall: Não, -9.

Ao perceber que esse poderia ser o jeito de decifrar a 4ª pista, Kall escreveu em seu rascunho um esquema e depois reescreveu o alfabeto já cifrado (Figura 19).

Figura 19 - Esquema de Kall para representar os cálculos do alfabeto (acima) e o alfabeto já cifrado (abaixo).



Fonte: Dados da pesquisa (2015).

Fonte: Gravações de vídeo e áudio, ficha de perguntas e diário de campo (2015).

Episódio 2

Para ajudar os alunos a responderem a essa questão e aproveitando para introduzir alguns termos, como os coeficientes *a* e *b*, a pesquisadora iniciou um diálogo com os alunos sobre como seria a representação do modo geral da função que estávamos utilizando.

A pesquisadora, então, foi até à lousa e escreveu algumas expressões das pistas. Ela chamou a atenção dos alunos para os valores que acompanhavam a variável *x*, mostrando-lhes que esses valores estavam mudando de uma expressão para outra. Então, ela perguntou de que maneira eles poderiam olhar a variável *x* e os valores que a acompanham de uma forma generalizada. Depois de mais algumas explicações, Leandro se pronunciou dizendo:

Leandro: *y* ou *x*... sei lá...

Pesquisadora: *y* aonde?

Leandro: *y* no lugar do *x*, eu acho...

Pesquisadora: No lugar do *x*?

Igor: No caso, só está mudando a letra.

Leandro: É... pode ser *x* vezes *y* mais...

Pesquisadora: *x* vezes *y* mais quem?

Leandro: Mais uma letra...

Pesquisadora: Mais... chuta uma letra aí.

Igor: *z*.

Nesse momento, conforme Leandro foi dizendo, a pesquisadora foi escrevendo na lousa as ideias de Leandro e, no final, chegou-se à seguinte expressão: $y \times x + z$, em que *x* representava a variável e *y* e *z* representavam os coeficientes. Leandro discutiu com Igor sobre esse modo generalizado e ambos demostravam entender o que eles haviam acabado de construir.

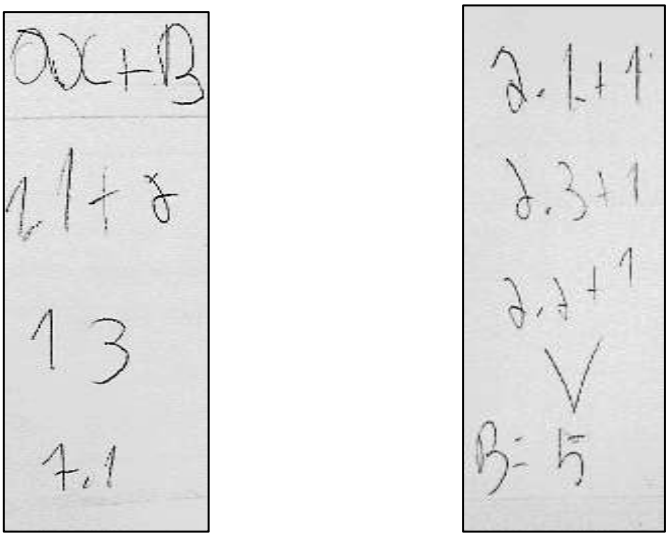
Fonte: Gravações de vídeo e áudio e diário de campo (2015).

Episódio 3

Essa dupla observou o criptograma e, de início, começou a responder às dicas. Após responder às duas primeiras, Igor sugeriu a Jaciara que eles fossem completando os quadrinhos em que havia os números correspondentes às letras que elas já conheciam. Jaciara aceitou a sugestão e começou a colocar, em todos os quadrinhos com o número 3, a letra *a*. Ela continuou fazendo isso para as outras letras conhecidas. Enquanto Jaciara fazia esse processo, Igor pegou uma folha de rascunho e escreveu nela a expressão $a \times x + b$ e começou a pensar nos valores de *a* e *b*. Igor tentou primeiro substituir os valores $a = 1$ e $b = 2$ e resolveu os cálculos para $x = 1$. Embora a expressão $1 \times x + 2$, para $x = 1$, tenha dado 3 (a letra *a*), ele verificou que ela não dava certo para a letra *c*, pois $1 \times x + 2$, para $x = 3$, dava 5 e não 7, como teria que ser (Figura 20). Desse modo, Igor pensou em outros valores para os coeficientes *a* e *b*. Com a intenção de que seus cálculos dessem certo para a letra *c*, Igor pensou nos valores $a = 5$ e $b = 2$. Assim, ele resolveu a expressão $5 \times x + 2$, para $x = 1$, e verificou que o resultado dava 7, mas, nesse momento, Jaciara chamou a atenção de Igor, dizendo que ele havia utilizado $x = 1$ e não $x = 3$, como ele queria (Figura 21). Igor demonstrou entender o que Jaciara estava dizendo. Assim, ambos perceberam que aqueles valores para *a* e *b* ainda não estavam bem definidos. Nesse momento, os dois demonstraram desânimo, pois não haviam ainda acertado os valores para *a* e *b*.

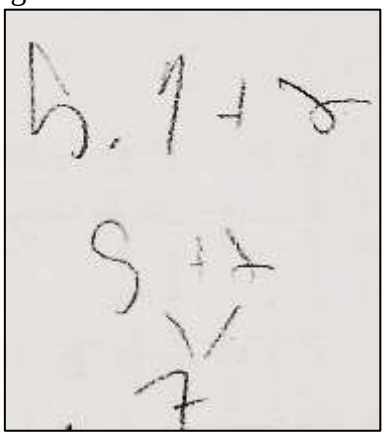
Para que os alunos continuassem com o raciocínio de encontrar os valores dos coeficientes a e b, a pesquisadora interveio, sugerindo que, ao invés de eles utilizarem $a = 1$ e $b = 2$, que tentassem $a = 2$ e $b = 1$. Igor aceitou a sugestão e escreveu em sua folha de rascunho a expressão $2 \times 1 + 1$. Ao resolver a conta, ele verificou que o resultado dava 3, em seguida ele resolveu $2 \times 3 + 1$ e também observou que a resposta era 7. Desse modo, eles perceberam que a expressão $2 \times x + 1$, com x variando nas letras do alfabeto ($A = 1, B = 2, \ldots, Z = 26$), estava correspondendo às letras cifradas do criptograma.

Figura 20 - Igor pensando sobre os coeficientes *a* e *b* e depois testando os coeficientes *a* = 2 e *b* = 1.



Fonte: Dados da pesquisa (2015).

Figura 21 - Igor testando os coeficientes *a* = 5 e *b* = 2.

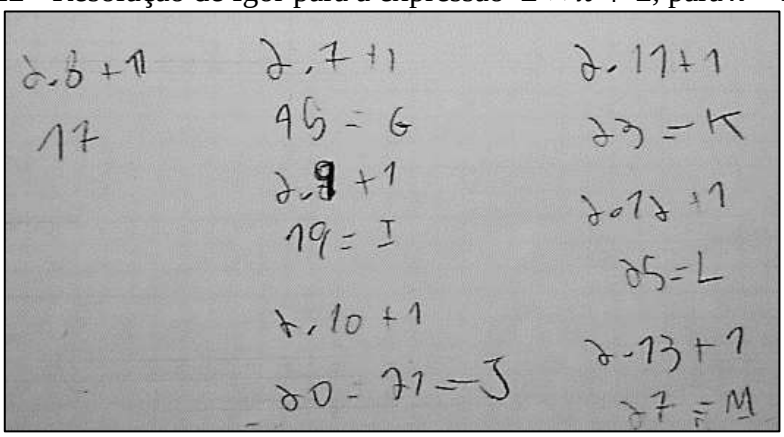


Fonte: Dados da pesquisa (2015).

Com isso, Igor afirmou a Jaciara que, para essa cifra, os valores dos coeficientes eram

$a = 2$ e $b = 1$, e que *x* representava a variável da expressão $2 \times x + 1$. Desse modo, Igor continuou variando *x* de acordo com as letras do alfabeto (Figura 22).

Figura 22 - Resolução de Igor para a expressão $\mathbf{2 \times x + 1}$, para *x* = 1, ..., 26.



Fonte: Dados da pesquisa (2015).

Fonte: Gravações de vídeo e áudio, ficha de perguntas e diário de campo (2015).

Episódio 4

Ao iniciar esse encontro, a pesquisadora perguntou se eles haviam trazido a atividade e o que eles haviam desenvolvido sobre ela em suas casas. Igor respondeu que havia pensado e chegado à decifração de uma mensagem. Sendo assim, a pesquisadora solicitou que Igor explicasse para as meninas tudo o que ele havia pensado e feito em casa.

Igor explicou que havia conseguido encontrar a função $f(x) = 2 \times x - 2$ que representava o gráfico verde. Segundo Igor, ele foi "chutando" os valores para os coeficientes *a* e *b* e mudando o sinal de *b* até dar certo. Fazendo isso, com a função $f(x) = 2 \times x - 2$, ele havia conseguido decifrar a frase que correspondia a essa função [...].

Após essa explicação, todos deram continuidade às resoluções. Igor estava muito preso à ideia de ficar "chutando" os valores para os coeficientes *a* e *b* da função. As meninas demonstraram estar um pouco confusas sobre os cálculos de Igor.

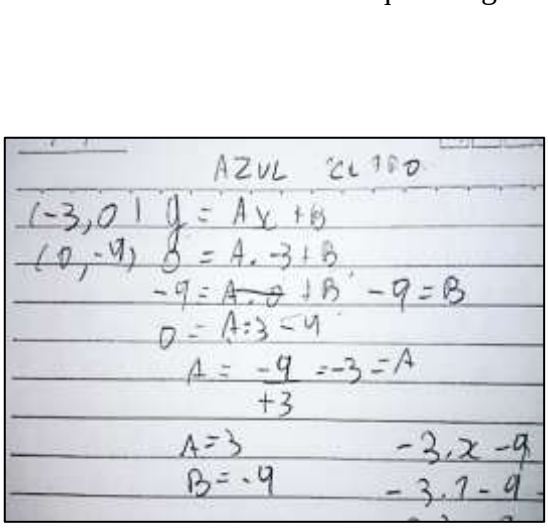
Percebendo que o rendimento das discussões e das resoluções havia baixado, a pesquisadora decidiu interferir, fazendo uma explicação sobre como eles poderiam encontrar as funções sem ter que ficar "chutando" os valores, como Igor estava fazendo. Assim, a pesquisadora retomou a explicação sobre os pontos e suas coordenadas e como, através deles, se poderia encontrar a função do gráfico passando

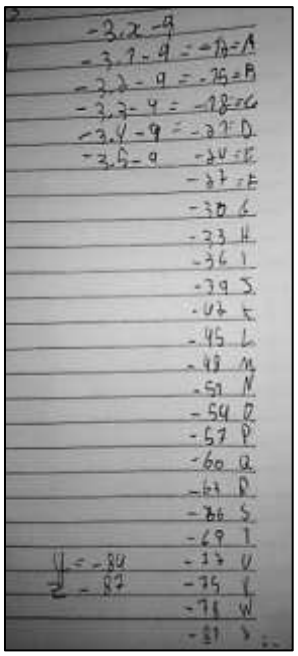
por esses dois pontos.

Conforme a pesquisadora explicava, os alunos começaram a se lembrar um pouco das discussões feitas no encontro anterior. Igor, rapidamente, iniciou seus cálculos em seu rascunho, mas as meninas ainda tiveram algumas dúvidas e dificuldades em iniciar suas resoluções.

Igor escolheu um gráfico e procurou nele os pontos sobre os eixos x e y. Os pontos encontrados por ele foram (-3,0) e (0,-9). Igor desenvolveu os cálculos com esses pontos sem mostrar dificuldades, embora, às vezes, ele cometesse alguns erros na hora de resolver a equações, por exemplo, $-3 \times a - 9 = 0 \Rightarrow a = 3 + 9 \Rightarrow a = 12$. Ao perceber que Igor estava cometendo esse erro, a pesquisadora chamou a atenção dele sobre a maneira como ele estava resolvendo a equação. Após observar o erro, Igor refez os cálculos e conseguiu chegar à função $f(x) = 3 \times x - 9$ e, com isso, descobriu os valores das letras cifradas por essa função (Figura 23).

Figura 23 - À esquerda, a resolução de Igor para os pontos (-3,0) e (0,-9) e, à direita, os cálculos que designam o alfabeto cifrado.





Fonte: Dados da pesquisa (2015).

Fonte: Gravações de vídeo e áudio, ficha de perguntas e diário de campo (2015).

O episódio 1 é muito interessante, visto que, na atividade em que ele ocorreu (terceira atividade), ainda não havia sido discutida formalmente a definição de função afim, embora já se tivesse discutido um pouco sobre essa função e sobre sua notação na atividade anterior.

Notou-se que, nessa situação, Kall relembrou algumas discussões realizadas anteriormente e tentou montar uma expressão matemática que se encaixasse naquela situação. Observa-se que Kall se atentou em diferenciar o número -3 por meio dos parênteses, para discernir esse valor fixo da expressão com os valores que variavam do alfabeto. Assim, após descobrir tal expressão, ele organizou os dados desse alfabeto já com suas letas cifradas.

O episódio 2 mostra a situação em que houve uma discussão a respeito da generalização da expressão que representa uma função afim. Observou-se que, nesse diálogo, os alunos Igor e Leandro conseguiram perceber que os coeficientes a e b das expressões encontradas por eles variavam, no entanto, esses coeficientes não representavam a variação do alfabeto. Com a ajuda desses alunos, a expressão geral que representa a função afim foi criada e várias discussões a respeito dela foram desenvolvidas.

O episódio 3 apresenta Igor tentando resolver a atividade por meio da definição de função afim, discutida nos encontros anteriores. Ele e Jaciara iniciaram a resolução da atividade respondendo às dicas que eles já conheciam; em seguida, Igor relembrou a expressão $a \times x + b$ e começou a buscar valores para a e b que resultassem na expressão utilizada na cifração daquela atividade. Essa ideia de buscar a função para facilitar sua resolução partiu do próprio Igor. Assim, essa ação realizada por ele evidencia como ele associou e explorou as ideias que foram discutidas anteriormente em relação ao conceito de função afim.

Já o episódio 4 complementa essas evidências em relação às ideias e explorações acerca da função afim, visto que, na situação descrita nesse episódio, os alunos tinham como informação os gráficos de funções afins. Nessa atividade, Igor continuou pensando na expressão algébrica $a \times x + b$, buscando os valores de a e b que satisfizessem visivelmente o gráfico escolhido. Assim, inicialmente, Igor descobriu a função que representava o gráfico verde, "chutando" valores para a e b; no entanto, o mesmo processo começou a não dar certo para os outros gráficos. Nesse momento, como se pôde observar no episódio, a pesquisadora interferiu, tentando auxiliar os alunos a encontrar a função por meio dos pontos pertencentes aos eixos. A Figura 24 ilustra, claramente, como Igor pensou e desenvolveu o seu raciocínio depois da ajuda da pesquisadora. Com essa mesma estratégia, Igor e Jaciara descobriram todas as funções referentes aos gráficos e, no final, decifraram as mensagens.

Com esses episódios apresentados nesta seção, pode-se concluir que os alunos desenvolveram e exploraram um domínio sobre o fazer Matemática e um saber pensar Matemática. Esse domínio passou por um processo lento, trabalhoso, o qual foi dependente diretamente da atitude dos alunos e dos procedimentos heurísticos desenvolvidos por eles individualmente e em grupo, durante as atividades. Em relação à construção do conceito

dentro de todo esse processo apresentado, Mauri (2009) tece algumas considerações acerca da consciência do aluno durante esse movimento de aprendizagem. De acordo com ela, o aluno precisa "ter inclinação para acreditar que a construção do conhecimento conceitual não se faz contra os outros, mas com os outros [...]" (MAURI, 2009, p. 106). A autora ainda argumenta que as elaborações e explorações conceituais e os domínios da definição de procedimentos são resultados da aprendizagem de atitudes autônomas e investigativas associadas aos procedimentos heurísticos. Dentro desse cenário, pode-se observar que os alunos exploraram as representações algébricas da função afim buscando o domínio do procedimento algébrico da função para resolver os problemas propostos e, consequentemente, trabalhar a exploração do conceito de função afim.

Por meio das ações desenvolvidas pelos alunos durante as atividades, e de acordo com tudo o que foi apresentado, observa-se que os alunos elaboraram conjecturas, estimularam suas capacidades em busca de informações, desenvolveram estratégias de resolução e melhoraram suas capacidades de argumentação e de organização. Esses elementos, apresentados acima, de acordo com os PCNEM (BRASIL, 2000, p. 41–42), são fundamentais "para o processo de formalização do conhecimento matemático e para o desenvolvimento de habilidades essenciais à leitura e interpretação da realidade e de outras áreas do conhecimento".

A pesquisadora considera que as atividades apresentadas possibilitaram que os alunos, aos poucos, explorassem as ideias associadas à função afim. A postura da mesma durante os encontros e a atitude independente dos alunos contribuíram para que os mesmos desenvolvessem estratégias de resolução. O aspecto desafiador das atividades proporcionou um engajamento dos alunos durante os encontros e a continuidade de seus próprios processos de aprendizagem. Nesse sentido, várias competências dos alunos foram desenvolvidas e trabalhadas, conjuntamente com a aprendizagem dos conceitos relacionados à função afim.

No próximo capítulo, serão apresentadas as considerações finais. Uma síntese da pesquisa é realizada, bem com as reflexões sobre os dados coletados da mesma. Em seguida um relato sobre o envolvimento da pesquisadora com a escola e com os alunos é apresentado, assim como as dificuldades emergentes durante o tralho de campo. Encerrando o capítulo, alguns questionamentos são apesentados. Tais questões são resultantes do trabalho desenvolvido durante a dissertação e podem fazer parte de pesquisas futuras.

“O rosto de Holmes se abriu num sorriso de aprovação.

- Você resumiu muito bem as dificuldades do caso – ele disse. – Muitas coisas ainda permanecem obscuras, embora eu já tenha minha opinião sobre os fatos principais”.

“Sherlock Holmes pulou de sua cadeira, com uma exclamação de alegria.

- O último elo – ele gritou, exultante. – Meu caso está completo”.

“Seus olhos brilhavam enquanto falava. Então, ele colocou a mão sobre o coração e se curvou, como se reverenciasse uma multidão que o aplaudisse”.

(Sherlock Holmes)

5 RELATÓRIO

Neste capítulo de encerramento, faço uma breve síntese da pesquisa, retomando pontos relevantes da mesma e expondo os resultados obtidos. Na sequência, apresento as reflexões acerca dos resultados obtidos. Dando continuidade, apresento as principais dificuldades encontradas durante o trabalho de campo. E, por fim, encerro a dissertação com algumas sugestões para pesquisas futuras. Tais ideias foram questionamentos que surgiram durante este trabalho e que, embora tangentes à pesquisa, não puderam ser discutidos, justamente por não fazerem parte do objetivo principal do mesmo.

5.1 Uma sínt3se da pesqu1sa

Esta pesquisa consistiu em compreender em que atividades pedagógicas envolvendo problemas de criptografia pode auxiliar os alunos na exploração das ideias associadas à função afim. Na busca de pesquisas que envolvessem a Criptografia e a Educação Matemática, foram encontrados trabalhos que abordam as possibilidades da inserção desse tema no Ensino Básico, bem como quais temas do currículo de matemática poderiam ser aliados a essa temática (TAMAROZZI, 2001; GROENWALD; FRANKE; OLGIN, 2009; OLGIN, 2011; OLIVEIRA; KRIPKA, 2011; SILVA; SOUSA, 2013; OLGIN; GROENWALD, 2011). No capítulo dois, é possível encontrar uma apresentação desses trabalhos e de como esses autores abordam a criptografia em atividades matemáticas.

Nessa busca por referências, puderam-se identificar alguns indícios na maneira como a criptografia foi atrelada aos conteúdos do currículo de matemática. Observa-se que, nos trabalhos encontrados, embora alguns autores apresentem um material didático que envolve a criptografia a alguns conteúdos matemáticos, eles não trazem considerações de que esse material pode ser utilizado durante o desenvolvimento e construção dos conteúdos matemáticos e de atitudes. Alguns autores trazem (ou sugerem) aplicações e procedimentos dessas atividades em sala de aula e refletem sobre as possibilidades que o professor tem ao utiliza-las. Como exemplo dessas possibilidades Olgin (2011, p. 121) conclui que “as atividades desenvolvidas e aplicadas [utilizando a criptografia] são exemplos de material didático que pode ser utilizado pelos professores para exercitar, aprofundar, fixar e revisar conteúdos”.

Após uma análise de como esses trabalhos abordaram a criptografia aliada a alguns conteúdos matemáticos, e levando em consideração os questionamentos iniciais da

pesquisadora, é que surgiu o objetivo desta pesquisa. Assim, a fim de alcançar esse objetivo, a pergunta diretriz que guiou este trabalho durante todo o processo foi:

"Quais as potencialidades de atividades pedagógicas envolvendo problemas criptográficos na exploração das ideias associadas à função afim?"

Na tentativa de responder à pergunta diretriz e alcançar o objetivo apresentado, uma sequência pedagógica de atividades envolvendo problemas criptografados foi desenvolvida a fim de abordar a definição de função afim, bem como suas particularidades: função linear, função identidade e função constante, além de trabalhar com a representação gráfica e a definição de inversa. Essa sequência é composta por oito atividades: i) Si-lá-box, ii) Um caso de sequestro, iii) O detetive Watson, iv) Cifrando um poema, v) Criptograma, vi) O jogo, vii) O poeta assassino e viii) Cifrando sua história, sendo que cada uma delas tinha seu objetivo específico e, juntas, o objetivo de abordar o conteúdo de função afim.

As mensagens criptografadas foram caracterizadas como sendo as soluções de enigmas de histórias fictícias. As atividades ii), iii), v), vi) e vii) foram contextualizadas em um gênero investigativo, que tinham como personagens principais o consultor de polícia Sherlock Holmes e seu amigo Dr. Watson. Essas atividades exigiam que os alunos se posicionassem como decifradores, investigando, explorando e desenvolvendo diferentes estratégias de resolução para decifrar as mensagens e resolver os problemas propostos. A atividade i) teve como característica introduzir o conceito de criptografia e as atividades iv) e viii) foram desenvolvidas para serem as atividades de encerramento dos semestres, tendo como principal característica colocar os alunos na postura de cifradores de mensagens.

Então, com as atividades preparadas, é que foi proposta a pesquisa para uma escola pública de Rio Claro/SP. Sendo aceita pelo diretor, os alunos do primeiro ano do Ensino Médio dessa escola foram convidados a participar de encontros entre eles e a pesquisadora, a fim de trabalhar as atividades. Sete alunos aceitaram o convite e demonstraram interesse em participar dos encontros. Toda a coleta de dados ocorreu na própria escola, ora na sala de vídeo, ora em salas de aula. Os encontros foram filmados e os áudios gravados. O material resultante da produção de dados se deu pelas filmagens e gravações do áudio, pelo caderno de campo da pesquisadora, pelas fichas de perguntas (e rascunhos) respondidas pelos alunos sobre cada atividade e pelas entrevistas realizadas posteriormente aos encontros.

Terminada a fase do trabalho de campo é que se iniciou o processo de análise do material coletado, buscando situações convergentes que pudessem apresentar indícios a possíveis

respostas para a pergunta diretriz. A partir da análise dos dados e categorizando as situações convergentes é que emergiram três categorias, a saber: Atitudes Investigativas; Procedimentos e Conceitos.

A primeira categoria apresenta episódios sobre as atitudes dos alunos desenvolvidas durante o processo de resolução das atividades, bem como a postura de mediadora da pesquisadora. A segunda categoria aborda situações de criação e investigação de procedimentos realizados pelos alunos durante as estratégias de resolução, e a última categoria contempla episódios que ilustram situações de exploração do pensamento algébrico e das ideias associadas ao conceito de função afim. A seguir, serão apresentadas algumas reflexões acerca dos resultados desta pesquisa, levando em consideração as três categorias citadas acima.

5.2 Reflexõ3s sobre os resultad0s

Criar situações que desenvolvam um ambiente caracterizado pela exploração de problemas vem ao encontro de situações investigativas proporcionadas por problemas envolvendo a cifração e decifração de mensagens. De acordo com Groenwald e Olgin (2011, p. 77) a "metodologia resolução de problemas é indicada para o desenvolvimento de atividades didáticas com o tema Criptografia", já que, problemas criptografados não apresentam em seus enunciados formas e operações para a sua resolução. Este tipo de atividade se caracteriza pelas várias estratégias de resolução que se podem utilizar para decifrar as mensagens. Sem métodos automáticos de resolução nem aplicações de algoritmos prontos, esse tipo de atividade convida o decifrador a investigar sua criptografia explorando e levantando conjecturas para descobrir a mensagem cifrada.

Assim, problemas com essa característica e relacionados a alguns conteúdos matemáticos, em um espaço constituído por professores e alunos, proporcionam o desenvolvimento de um ambiente criptográfico, no qual os alunos desenvolvem meios materiais e intelectuais que permitem o processo de cifração e decifração de mensagens. Dentro desses cenários enigmáticos e criptografados, observou-se, durante as atividades, que esse ambiente despertou a curiosidade dos alunos, motivando-os e desafiando-os a resolver os enigmas propostos.

Por essa pesquisa ser de intervenção com enfoque qualitativo a interação da pesquisadora com os alunos pode ser continua e intensa. Oportunizando um crescimento profissional, a pesquisadora vivenciou situações dentro da sala de aula em que os encontros e as próprias a

atividades propostas ofereceram algumas reflexões. A princípio a pesquisadora aprendeu a lidar um pouco com as constantes situações da sala de aula e da escola, como a precariedade da sala, das carteiras, da eletricidade entre outras situações estruturais da escola. Em relação aos alunos, e decorrente da postura que a pesquisadora assumiu durante os encontros, houve um aprendizado no sentido de ouvi-los mais e prestar mais atenção nos seus processos de resolução. Ouvir suas ideias, buscar argumentos e questionamentos partindo das próprias estratégias apresentadas pelos alunos, mediar as informações buscando sempre o aprendizado deles entre outras cosias se constituíram num processo de aprender ensinando. Quanto às atividades, houve uma reflexão sobre possíveis modificações de algumas a fim de melhor contribuir para a exploração dos alunos em relação ao conceito proposto a ser trabalhado.

Sobre as reflexões da pesquisadora a respeito das atitudes dos alunos, pode-se observar que a postura dos mesmos foi sendo modificada durante os encontros. A partir do momento em que eles compreenderam que a pesquisadora estava ali para auxiliá-los e orientá-los durante o processo de resolução das atividades, os alunos começaram a se tornar mais ativos, envolvendo-se cada vez mais nas atividades apresentadas e construindo, durante os encontros, ações investigativas e autônomas.

Conforme as atividades iam sendo trabalhadas, a confiança no grupo foi sendo estabelecida e isso se refletiu na atitude dos alunos quanto ao trabalho em grupo. A preocupação com o outro em explicar a atividade ou suas ideias de solução apareceu em vários episódios, e as discussões sobre as estratégias de resolução contribuíram para estabelecer momentos de troca de informações. Como resultado do trabalho em grupo, além de atingir os objetivos de cada atividade, observou-se uma melhoria no diálogo dos alunos quanto às explicações de suas ideias e de suas resoluções. Os alunos demonstravam a cada encontro estar bem mais organizados em seus discursos, tanto para suas explicações orais e escritas quanto em suas dúvidas. Observou-se que os problemas envolvendo a criptografia e a dinâmica dos encontros contribuíram para o estabelecimento do trabalho em grupo e este, por sua vez, fez total diferença no andamento e compreensão das atividades durante todos os encontros.

Em relação aos procedimentos, a pesquisadora inferiu que os alunos compreenderam que problemas envolvendo a criptografia não exigiam uma única estratégia de solução. Eles acabaram desenvolvendo, durante os encontros, várias estratégias de resolução. Fazendo uso de seus conhecimentos prévios e debatendo ideias de seus procedimentos heurísticos, os alunos compreenderam que, para resolver as atividades, eles precisariam criar posturas investigativas. Assim, durante o processo de resolução, os alunos utilizaram seus

conhecimentos prévios para levantar hipóteses, verificavam se suas ideias ajudavam a decifrar as mensagens, quando não, refutavam suas conjecturas e desenvolviam outros métodos de decifração. Todo esse processo ocorreu simultaneamente, ora no campo das conjecturas, ora no momento de validação das mesmas. A pesquisadora também observou que os alunos utilizaram a calculadora como uma ferramenta de apoio durante o processo de resolução das atividades, e que esta era resgatada pelos alunos conforme suas necessidades. Desse modo, pode-se verificar que essa ferramenta contribuiu com os alunos durante o processo de resolução e que estes a souberam utilizar de diferentes formas e em diferentes momentos.

Dessa maneira, analisando os procedimentos desenvolvidos pelos alunos e suas atitudes investigativas, a pesquisadora afirma que é possível observar, por meio das explorações e investigações realizadas pelos alunos, que os mesmos desenvolveram ideias associadas ao conceito de função afim. Uma reflexão a respeito do desempenho dos alunos em relação a sua aprendizagem sobre esse conceito foi realizada, no sentido de tentar entender como essas atividades auxiliaram os alunos a desenvolver ideias e estratégias sobre esse assunto. Como resultado, pôde-se verificar que os alunos exploraram as ideias relacionadas ao conceito de função afim, principalmente no campo do pensamento algébrico, e que eles concatenaram que as letras do alfabeto estavam representando o papel da variável nas situações propostas.

Ressalte-se que essa reflexão leva em consideração todo o plano de ação que foi desenvolvido durante os encontros, bem como as situações ocorridas na escola no decurso do trabalho de campo, como, por exemplo, falta de energia, a falta dos alunos no dia dos encontros, contratempos por parte de funcionários da escola, entre outras. Não se pode deixar de ponderar que os alunos participantes formavam um número reduzido e que os encontros ocorriam em ambientes diferentes do da sala de aula. Nesse aspecto levantam-se reflexões que vai em direção sobre a aplicabilidade dessas atividades em uma sala de aula de quarenta alunos. Mesmo com essas singularidades, a pesquisadora acredita, por sua prática profissional que atividades envolvendo mistérios e textos criptografados podem ser aplicados em uma sala de aula com quarenta alunos. Reflexões que vão nesta direção retomam as discussões a respeito desse alto número de estudantes dentro de uma sala de aula e lembrar que a dificuldade de se trabalhar bem com os alunos não só depende do caráter da atividade, mas também das condições razoáveis que o ambiente em sala de aula proporciona, e a quantidade de alunos é um fator de grande impacto nessa qualidade do ambiente.

Tais atividades podem, além de aguçar a curiosidade dos alunos, permitindo o desenvolvimento de sua criatividade, sua iniciativa e seu espírito explorador, interligar os conteúdos matemáticos, ajudando os alunos a desenvolver habilidades e competências na

resolução de problemas, criando estratégias de resolução, e desenvolvendo atitudes de autonomia e investigação durante o processo de aprendizagem.

Pesquisar sobre as possíveis maneiras de cifração e desenvolver cifras seguras não fazem parte de um novo campo de estudo, contudo atrelar a criptografia a conteúdos do currículo de matemática do Ensino Básico é relativamente novo. A criação e o desenvolvimento de atividades que aliem esse tema a conteúdos de funções, matrizes, progressões, análises combinatórias, entre outros, vêm, cada vez mais, surgindo no meio acadêmico. Isso se mostra interessante, na medida em que essas pesquisas apresentem indícios de que esse tema, entrelaçado a esses conteúdos, possibilita aos alunos ambientes investigativos, em que eles se tornem o centro das ações de seu próprio aprendizado, contribuindo para aulas diferenciadas e instigantes. Assim, a pesquisadora conclui que, a utilização de atividades envolvendo problemas criptográficos durante a construção de algum conteúdo matemático pode indicar melhorias de compreensão e aprendizagem dos conceitos envolvidos, e se elas desenvolvem a autonomia e o espírito investigativo dos alunos, oportunizando aos mesmos explorarem seus conhecimentos e procedimentos heurísticos.

5.3 T0rnando-se pesquisad0ra e aprendendo a sup3rar obstáculos

Durante os encontros, a pesquisadora se deparou com vários problemas extra-atividades. No que concerne aos alunos, eles apresentavam muita dificuldade com a Língua Portuguesa, tanto na escrita das palavras quanto na leitura dos textos. Como sempre, era solicitado que os alunos fizessem a leitura em voz alta das histórias das atividades, e, dado que, em algum momento, todos leram, ficou evidente a dificuldade que todos os alunos têm na leitura dos textos, principalmente em suas pontuações. Os alunos também demonstraram dificuldades com as operações básicas da matemática, principalmente com o algoritmo da divisão, e com a resolução de equações.

O problema da falta dos alunos nos encontros influenciou, o desenvolvimento das atividades. Embora os alunos criassem a atitude de explicar a atividade e retomar as estratégias de resolução para aqueles que haviam faltado, essa situação influenciou no tempo das atividades e até mesmo nas discussões realizadas pelos alunos com a pesquisadora, sobre os conceitos matemáticos abordados. No entanto, o problema mais sério com relação aos alunos surgiu com Fernando. Durante todo o primeiro semestre, ele desenvolveu as atividades e, quando solicitado, trabalhava em conjunto com seus colegas; no entanto, quando os encontros voltaram no segundo semestre, Fernando não demonstrava mais interesse nas

atividades, nem nos encontros. Esse desânimo ficou muito claro quando se iniciou a sexta atividade. Fernando começou a ter muitas faltas e, embora Gustavo também, Fernando não se interessava mais pelas atividades. Ele não contribuía mais com as discussões com seu colega Gustavo, e isso influenciou muito no desenvolvimento das atividades para essa dupla. Sua postura passiva durante o processo de resolução das atividades irritou fortemente Gustavo, a ponto de este pedir para a pesquisadora que mandasse seu colega de volta para a sala. Tendo esta situação, e observando os conflitos entre Fernando e Gustavo, a pesquisadora deu liberdade a Fernando para ele sair dos encontros quando quisesse. Fernando ainda tentou participar passivamente de alguns outros encontros, apenas para não ficar nas aulas regulares, mas ele acabou desistindo de vez e abandonou o grupo. Em explicação sobre suas atitudes no segundo semestre, Fernando explicitou que: "eu estava cansado, estava meio triste, dai eu vinha aqui, como dava pra ver, eu estava com um pouco de sono às vezes, dai eu acabei optando por parar, mas eu sempre gostei de vir, era muito interessante sempre" (Fernando, entrevista, 2015).

No que diz respeito à estrutura da escola, as dificuldades foram grandes. Não existia na escola um lugar em que a pesquisadora pudesse se reunir com os alunos sem ser incomodada. Ou os encontros ocorriam na sala de vídeo da escola, ou na sala do professor que estaria utilizando a sala de vídeo. Em todos os encontros, demorava-se muito para que os alunos e a pesquisadora fossem acomodados em alguma sala, e isso prejudicava sempre o tempo destinado às atividades. Em algumas situações, quando os encontros ocorriam na sala de vídeo, esperavam-se mais de trinta (30) minutos para que os inspetores acendessem a luz da sala e constantemente havia alunos, professores e funcionários que precisavam entrar na sala para pegar algum tipo de material – a sala de vídeo também servia como uma sala para se guardar livros didáticos e apostilas. Era uma sala que sempre estava suja e muito bagunçada. Embora nela houvesse uma lousa branca, era difícil ter canetas e quase nunca havia o apagador. Já na sala de aula, não havia eletricidade nas tomadas, quando muito se tinha tomada. Então, em alguns encontros, foi preciso terminar as atividades mais cedo, pois não havia condição de carregar a bateria da filmadora.

Outra dificuldade extra-atividade que interferiu nos encontros, e respectivamente na pesquisa, foram as decisões e impasses da pesquisadora sobre os mesmos. Por causa das faltas dos alunos, em determinados encontros havia dois ou três alunos e coube à pesquisadora decidir se o encontro ocorreria ou não.

Com as reflexões sobre as dificuldades extra-atividade, a pesquisadora tomava decisões e remontava a dinâmica dos encontros de acordo com o que surgia para ela nesses dias, tanto

com relação à quantidade dos alunos, como no tocante a onde os encontros ocorriam. Sendo assim, condicionada às situações apresentadas à pesquisadora e aos participantes, a coleta aconteceu do jeito que aconteceu devido às escolhas e decisões feitas pela mesma – e ressalte-se que, caso as decisões tivessem sido tomadas de outra maneira, a coleta poderia ter sido diferente.

5.4 P3squisas Futur4s

Nesta última seção serão apresentadas algumas ideias que emergiram durante esta pesquisa. Essas ideias não foram abordadas nesta dissertação, pois não tinham relação direta com o objetivo da pesquisa. Entretanto, elas permearam todo o processo aqui apresentado.

A revisão dos trabalhos que abordam o tema criptografia com conteúdos matemáticos do Ensino Básico, apresentada no capítulo dois, indica uma escassez de pesquisas que envolvam problemas criptográficos no contexto da Educação Matemática. Essa carência de pesquisas entrelaçando essas duas áreas do conhecimento pode estar relacionada com a falta de divulgação sobre o tema criptografia, visto que as discussões e o surgimento na mídia a respeito da segurança de comunicações não são antigos. Aos poucos esse tema vem tomando espaço no meio acadêmico (como exemplo, as disciplinas do Profmat) e em alguns livros didáticos, além de estar sendo notícia nos jornais das TVs e em outros meios de comunicação. Independentemente do motivo pelo qual este assunto não está sendo tratado com frequência no meio acadêmico, esta dissertação é uma contribuição na direção de tentar divulgar e ampliar os entrelaçamentos entre a Criptografia e a Educação Matemática.

Este trabalho tentou compreender em que atividades pedagógicas envolvendo problemas de criptografia pôde auxiliar os alunos na exploração das ideias associadas à função afim. No entanto, durante todo o percurso desta pesquisa algumas ideias e questionamentos surgiram, os quais podem se caracterizar como futuras pesquisas.

Como o tema Criptografia poderia chegar ao professor da sala de aula? Como esse tema poderia ser abordado durante a formação inicial do professor? E para sua formação continuada? Será que a disciplina *Teoria dos Números* seria um bom espaço para apresentar e desenvolver esse tema com os alunos, visto que a teoria matemática que está por trás das criptografias atuais, como a RSA, é fortemente dependente dos conceitos de números primos? Levando em consideração que a evolução da criptografia está ligada às histórias das Guerras Mundiais e aos espaços geográficos, além de ter uma relação com a frequência de letras, seria possível desenvolver projetos interdisciplinares na escola que envolvessem os professores

dessas disciplinas? Será que as ideias de poder ainda estão fortemente ligadas à matemática nos dias de hoje? Será que está sendo estudada atualmente a relação entre matemática e poder? Como a criptografia influencia nos poderes de hoje em dia? Que caminho as novas formas de criptografia estão seguindo? E os computadores quânticos? Quais os papéis deles no meio dessa rede constituída de poder, matemática e criptografia? Como estão sendo exploradas as considerações realizadas por D' Ambrósio (2011) a respeito da matemática pela paz?

Além das ideias citadas acima, questões sobre quais outros conteúdos matemáticos poderiam ser relacionados ao tema, com o intuito de desenvolver atividades pedagógicas que auxiliem os alunos na construção de sua aprendizagem, perpassaram a cabeça da pesquisadora durante todo o estudo desta dissertação. A pesquisadora acredita que pesquisas envolvendo a Criptografia e a Educação Matemática são interessantes na medida em que a articulação dessas duas áreas do conhecimento, pode contribuir para novas maneiras de se ensinar e de se aprender.

Essas são algumas interrogações e inquietações que afloraram durante a caminhada desta pesquisa e que motivam a pesquisadora a continuar refletindo e pesquisando nessa direção. Que este trabalho possa servir de motivação para os pesquisadores a enxergar a criptografia não só dentro do campo da matemática, mas sim dentro do campo da Educação Matemática. Que novos estudos sejam realizados nessa direção e que cada vez mais esse tema seja explorado e debatido nos meios sociais e científicos.

"E agora, cavalheiros – ele continuou, sorrindo satisfeito - , chegamos ao final do nosso mistério. Fiquem à vontade para fazerem suas perguntas, pois irei responder a todos."

(Sherlock Holmes)

Banco de informações

ARINOS, E. J. S. *Criptografia: Aplicações no Ensino Fundamental e Médio*. 2014. 88 f. Dissertação (Programa de Pós-Graduação em Matemática em Rede Nacional) – Universidade Federal De Mato Grosso do Sul, Campo Grande, 2014.

BENEDETTI, F. C. *Funções. Software Gráfico e Coletivos Pensantes*. 2003. 316 f. Dissertação (Mestrado em Educação Matemática) – Universidade Estadual Paulista "Júlio de Mesquita Filho", Rio Claro, 2003.

BIGODE, A. J. L. A calculadora e o raciocínio da criança. *Cadernos da TV Escola: PCN na Escola*, p. 43–47, 1998.

BOGDAN, R.; BIKLEN, S. *Investigação Qualitativa em Educação: uma introdução à teoria e aos métodos*. Porto, Portugal: Porto Editora, 1994.

BONI, V.; QUARESMA, S. J. Aprendendo a entrevistar: com fazer entrevistas em Ciências Sociais. *Revista Eletrônica dos Pós-Graduandos em Sociologia Política da UFSC*, v. 2, n. 1, p. 68–80, 2005.

BORBA, M. C.; ARAÚJO, J. L. (Org.). *Pesquisa Qualitativa em Educação matemática*. 4. ed. Belo Horizonte: Autêntica, 2012.

BRASIL. MEC – Ministério da Educação. *Base Nacional Comum Curricular*. Brasília-DF: Ministério da Educação, 2015. Disponível em: <http://basenacionalcomum.mec.gov.br/#/site/inicio>. Acesso em: 7 jan. 2016.

BRASIL. MEC – Ministério da Educação. *Parâmetros Curriculares Nacionais: Terceiro e Quarto Ciclos de Ensino Médio - Matemática. Brasil*. Brasília-DF: Ministério da Educação / Secretaria de Educação Média e Tecnológica, 2000. Disponível em: <http://portal.mec.gov.br/seb/arquivos/pdf/ciencian.pdf>. Acesso em: 20 fev. 2016.

BRASIL. MEC – Ministério da Educação. PCN + Ensino Médio*: Orientações Educacionais Complementares aos Parâmetros Curriculares Nacionais*. *Ciências da Natureza, Matemática e suas Tecnologias*. Brasília-DF: Ministério da Educação e do Desporto, 2002. v. 1. Disponível em: <http://portal.mec.gov.br/seb/arquivos/pdf/CienciasNatureza.pdf>. Acesso em: 20 fev. 2016.

D'AMBROSIO, U. A busca da paz: responsabilidade de matemáticos, cientistas e engenheiros. *Revista da Universidade Vale do Rio Verde*, v. 9, p. 66–77, 2011.

D'AMBROSIO, U. *Educação Matemática: Da teoria à prática*. Campinas: Papirus, 1996.

DANTE, L. R. *Didática da Resolução de Problemas de Matemática*. 12º. ed. São Paulo - SP: Ática, 2000.

DESLAURIERS, J.-P.; KÉRISIT, M. O delineamento de pesquisa qualitativa. In: POUPART, J. *et al. A pesquisa Qualitativa: enfoques epistemológicos e metodológicos*. Petrópolis: Vozes, 2012. p. 127–153.

DIRETORIA DE ENSINO - REGIÃO DE LIMEIRA. *E. E. "Prof. Mycroft" - Rio Claro : Plano de Gestão. Parecer CCE nº 67/1998.* . [S.l: s.n.]. , Quadriênio: - 2015 2012

ECHEVERRÍA, M. D. P. P.; POZO, J. I. Aprender a Resolver Problemas e a Resolver Problemas para Aprender. In: POZO, J. I. (Org.). . *A Solução de problemas : aprender a resolver, resolver para aprender*. Porto Alegre: ARTMED, 1998. .

FIARRESGA, V. M. C. *Criptografia e Matemática*. 2010. 144 f. Mestrado em Matemática para Professores – Universidade de Lisboa, Portugal, 2010.

FINCATTI, C. A. *Criptografia como agente motivador na aprendizagem da matemática em sala de aula.* 2010. 82 f. Trabalho de conclusão de curso – Universidade Presbiteriana Mackenzie, São Paulo, 2010.

FRANÇA, W. B. A. *A utilização da criptografia para uma aprendizagem contextualizada e significativa*. 2014. 63 f. Dissertação (Mestrado Profissional em Matemática) – Universidade de Brasília, Brasília, 2014.

FREIRE, P. *Pedagogia da Autonomia: Saberes necessários à prática educativa*. 43. ed. São Paulo: Paz e Terra, 2011.

GOLDENBERG, M. *A arte de pesquisar: como fazer pesquisa qualitativa em Ciências Sociais*. Rio de Janeiro: Record, 2011.

GROENWALD, C. L. O.; FRANKE, R. F.; OLGIN, C. DE A. Códigos e Senhas no Ensino Básico. *Educação Matemática em Revista*, v. 2, p. 41–50, 2009.

GROENWALD, C. L. O.; OLGIN, C. DE A. Criptografia e o Currículo de Matemática no Ensino Médio. *Revista de Educação Matemática*, v. 13, p. 71–78, 2011a.

GROENWALD, C. L. O.; OLGIN, C. DE A. Currículo de Matemática no Ensino Médio: atividades didáticas com o tema Criptografia. In: XIII CONFERÊNCIA INTERAMERICANA DE EDUCAÇÃO MATEMÁTICA, 2011b, Recife. *Anais*... Recife: [s.n.], 2011. p. 12.

GROENWALD, C. L. O.; RUIZ, L. M. Formação de professores de Matemática: uma proposta de ensino com novas tecnologias. *Revista de Ciências Exatas e Tecnologia*, v. 8, p. 19–28, 2006.

HOBSBAWM, E. J. Feiticeiros e aprendizes : As ciências naturais. In: HOBSBAWM, E. J. *Era dos extremos: o breve século XX*. Tradução Marcos Santarrita. São Paulo - SP: Companhia das Letras, 1995. p. 504 – 536.

LITOLDO, B. F.; LAZARI, H. Uma análise do uso da criptografia nos livros didáticos de Matemática do Ensino Médio. *REMATEC - Revista de Matemática, Ensino e Cultura*, n. 17, p. 133–152, 2014.

LÜDKE, M.; ANDRÉ, M. E. D. A. *Pesquisa em Educação: Abordagens Qualitativas*. São Paulo: E.P.U., 1986.

MARQUES, T. V. *Criptografia: abordagem histórica, protocolo Diffie-Hellman e aplicações em sala de aula.* 2013. 62 f. Mestrado Profissional – Universidade Federal da Paraíba, Paraíba, 2013.

MAURI, T. O que faz com que o aluno e a aluna aprendam os conteúdos escolares? A natureza ativa e construtiva do conhecimento. In: COLL, C. *et al. O Construtivismo na Sala de Aula*. Tradução Cláudia Schilling. 6º. ed. São Paulo: Ática, 2009. p. 79–122.

MOREIRA, H.; CALEFFE, L. G. *Metodologia da pesquisa para o professor pesquisador*. 2. ed. Rio de Janeiro: Lamparina, 2008.

MOURA, M. L. S.; FERREIRA, M. C. *Projetos de Pesquisa: Elaboração, redação e apresentação*. Rio de Janeiro: Eduerj, 2005.

OLGIN, C. DE A. *Currículo no Ensino Médio: uma experiência com o tema criptografia.* 2011. 136 f. Mestrado em Ensino de Ciências e Matemática – Universidade Luterana do Brasil, Canoas, 2011.

OLGIN, C. DE A.; GROENWALD, C. L. O. Temas de Interesse no Currículo de Matemática do Ensino Médio. *Clame: Comité Latinoamericano de Matemática Educativa*, 2011.

OLIVEIRA, D. DE; KRIPKA, R. M. L. O uso da Criptografia no ensino de Matemática. In: XIII CONFERÊNCIA INTERAMERICANA DE EDUCAÇÃO MATEMÁTICA, 2011, Recife - BR. *Anais*... Recife - BR: [s.n.], 2011.

OLIVEIRA, R. D. *Utilização de mensagens criptografadas no ensino de matrizes*. 2013. 82 f. Dissertação (Programa de Mestrado Profissional em Matemática em Rede Nacional) – Universidade Federal de São Carlos, São Carlos, 2013.

PONTE, J. P.; BROCADO, J.; OLIVEIRA, H. *Investigações matemáticas na sala de aula*. 2º. ed. Belo Horizonte - BH: Autêntica, 2009. (Coleção Tendências em Educação Matemática).

PONTE, J. P.; SERRAZINA, M. DE L. *Didática da Matemática do 1º Ciclo*. 1. ed. Lisboa/Portugal: Artes Gráficas, 2000.

PORTANOVA, R. A Educação Matemática e a Educação para a Paz. *Revista Educação - Pontifícia Universidade Católica do Rio Grande do Sul*, v. XXIX, p. 435–444, 2006.

POUPART, J. A entrevista de tipo qualitativo: considerações epistemológicas, teóricas e metodológicas. In: POUPART, J. *et al. A pesquisa Qualitativa: enfoques epistemológicos e metodológicos*. Petrópolis: Vozes, 2012. p. 215–153.

POWELL, A. B.; FRANCISCO, J. M.; MAHER, C. A. Uma abordagem à Análise de Dados de Vídeo para Investigar o Desenvolvimento das Ideias Matemáticas e do Raciocínio de Estudantes. *Bolema. Boletim de Educação Matemática*, v. 17, n. 21, p. 81–140, 2004.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A Method for Obtaining Digital Signatures and PublicKey Cryptosystems. *Comunicações da ACM*, v. 21, n. 2, p. 120–126, 1978.

RODRIGUES, J. M. *Criptografia e Conteúdos de Matemática no Ensino Fundamental*. 2013. 33 f. Dissertação (Programa de Mestrado Profissional em Matemática em Rede Nacional) – Universidade Federal de São Carlos, São Carlos - SP, 2013.

ROGOFF, B. Observando a atividade sociocultural em três planos: apropriação participatória, participação guiada e aprendizado. In: WERTSCH, J. V.; RÍO, P. D.; ALVARES, A. *Estudos*

socioculturais da mente. Tradução Maria da G. G. Paiva; André R. T. Camargo. Porto Alegre (RS): ArtMed, 1998. p. 123–142.

SANTOS, J. L. *A Arte de Cifrar, Criptografar, Esconder e Salvaguardar como Fontes Motivadoras para Atividades de Matemática Básica*. 2013. 81 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Universidade Federal da Bahia, Salvador - Bahia, 2013.

SÃO PAULO. *Proposta Curricular do Estado de São Paulo: Matemática*. 1º edição ed. São Paulo - SP: [s.n.], 2011.

SCHÜRMANN, H. A. *Criptografia matricial aplicada ao ensino médio*. 2013. 76 f. Dissertação (Programa de Mestrado Profissional em Matemática em Rede Nacional) – Universidade Estadual de Londrina, Londrina, 2013.

SILVA, G. B. DA; SOUSA, J. S. DE. Criptografia como ferramenta para o ensino de matemática. In: XI ENCONTRO NACIONAL DE EDUCAÇÃO MATEMÁTICA, 2013, Curitiba - PR. *Anais*... Curitiba - PR: [s.n.], 2013.

SINGH, S. *O livro dos códigos: A ciência do sigilo - do antigo Egito à criptografia quântica*. 7. ed. Rio de Janeiro: Record, 2008.

SOLÉ, I. Disponibilidade para a aprendizagem e sentido da aprendizagem. In: COLL, C. *et al. O Construtivismo na Sala de Aula*. Tradução Cláudia Schilling. 6º. ed. São Paulo - SP: Ática, 2009. p. 29–55.

SOLÉ, I.; COLL, C. Os professores e a concepção construtivista. In: COLL, C. *et al. O Construtivismo na Sala de Aula*. Tradução Cláudia Schilling. 6º. ed. São Paulo - SP: Ática, 2009. p. 09–28.

SOUSA, A. N. L. *Criptografia de Chave Pública, Criptografia RSA*. 2013. 57 f. Dissertação (Programa de Mestrado Profissional em Matemática em Rede Nacional) – Universidade Estadual Paulista "Júlio de Mesquita Filho", Rio Claro, 2013.

SOUZA NETO, L. A. *Aritmética Modular e Criptografia no Ensino Básico*. 2014. 47 f. Dissertação (Programa de Mestrado Profissional em Matemática em Rede Nacional) – Universidade Federal do Maranhão, São Luís, 2014.

STEWART, I. *Jogos, Conjuntos e Matemática*. 1º. ed. [S.l.]: RBA, 2008.

TAMAROZZI, A. C. Codificando e Decifrando mensagens. *Revista do Professor de Matemática*, v. 45, p. 41–43, 2001.

TAMDJIAN, J. O.; MENDES, I. L. A construção das novas geografias: a internet, o espaço a Antártida. *Geografia : Estudos para a compreensão do espaço*. 1º. ed. São Paulo - SP: FTD, 2010. v. 3. p. 34 – 56.

UPINSKY, A.-A. *A perversão matemática*. Tradução Antônio R. De Oliveira. Rio de Janeiro: Francisco Alves, 1989. (Coleção Ciência).

VALENTE, W. R. *Uma história da matemática escolar no Brasil (1730 - 1930)*. 1º. ed. São Paulo: ANNABLUME, 1999.

APÊNDICE A – PROTÓTIPO DA ATIVIDADE

O caso do sequestro do matemático

Holmes estava na Espanha, entretendo-se com as touradas, quando foi procurado pelo inspetor Charles.

O inspetor trazia para Holmes um caso de sequestro. O professor Sergio Carilho havia sido sequestrado durante sua aula de matemática, na Universidade de Madri.

Na sala de aula, tudo parecia normal, até mesmo algumas contas no quadro negro.

Ao entrar na cena do crime, Holmes analisou o ambiente e na mesma hora sacou o motivo do sequestro. Preocupado, Holmes sabia que a vida do professor estava em suas mãos.

Infelizmente o Dr. Watson estava em uma viagem e assim Holmes se viu sozinho com este caso importante. Desta maneira, ele convocou alguns amigos de investigação para resolver o crime.

Durante a investigação Holmes sentiu um mal estar e foi levado inconsciente para o hospital deixando apenas uma carta criptografada para os seus ajudantes no bolso de seu paletó.

Resta a seus ajudantes descobrir que mensagem estava escrita na carta e torcer para que nela esteja a identidade do(s) sequestrador(es), o motivo do sequestro e o local onde o professor de matemática esta sendo mantido preso, para que a polícia possa agir antes que o criminoso faça algum mal ao professor.

19	*	23	9	21	25	9	23	24	22	5	8	19	22	*	é	*	25	17	*
5	16	25	18	19	*	8	19	*	20	22	19	10	9	23	23	19	22	*	7
12	5	17	5	8	19	*	14	19	23	é	*	20	13	9	22	9	*	8	9
*	19	16	13	26	9	13	22	5	*	19	*	17	19	24	13	26	19	*	8
19	*	23	9	21	25	9	23	24	22	19	*	9	22	5	*	21	u	9	*
19	*	5	16	25	18	19	*	23	9	22	13	5	*	22	9	20	22	19	26
5	8	19	*	18	5	*	8	13	23	7	13	20	16	13	18	5	*	8	9
*	17	5	24	9	17	á	24	13	7	5	*	18	9	23	24	9	*	5	18
19	*	9	*	19	*	20	22	19	10	9	23	23	19	22	*	9	23	24	5
*	23	9	18	8	19	*	17	5	18	24	13	8	19	*	20	22	9	23	19
*	18	5	*	23	5	16	5	*	8	9	*	26	í	8	9	19	*	8	5
*	9	23	7	19	16	5	.												

Pede-se aos alunos:

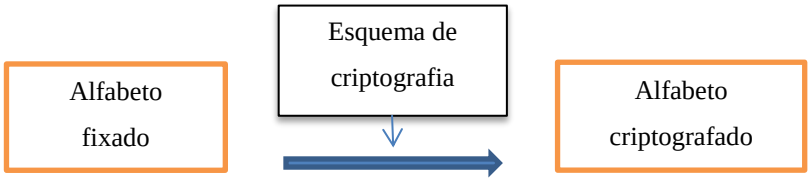
a) Nome do sequestrador:

b) O motivo do sequestro:

c) O local onde o professor esta preso:

d) Descrever detalhadamente qual foi o processo utilizado por vocês para decifrarem a carta de Holmes.

e) Observe o esquema abaixo:



Para se criptografar uma mensagem é preciso ter um alfabeto fixado e aplicar sobre esse alfabeto algum esquema que o criptografe.

Vocês saberiam explicitar através de uma *lei matemática* esse esquema de criptografia, considerando que o alfabeto fixado é o que segue abaixo.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

f) Como vocês pensaram para chegar a essa lei matemática?

g) De que maneira vocês justificariam que essa lei é correta?

h) Após encontrar a lei matemática utilizada para criptografar a mensagem, vocês saberiam esboça-la graficamente?

Se sim, desenhe-o e denomine o que é representado no eixo das abcissas (x) e o que é representado no eixo das ordenadas (y)?

Se não, explique o porquê não se pode esboça-lo.

APÊNDICE B – AS ATIVIDADES

SI - LA – BOX

Procure preencher os quadradinhos, abaixo de cada dica, de acordo com suas sílabas.

EXEMPLO:

Telefone portátil.

C	E

L	U

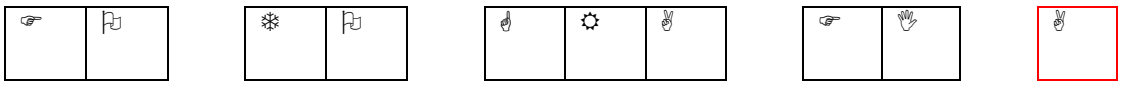
L	A	R

Cada letra corresponde a um símbolo, e símbolos iguais correspondem a letras iguais. As letras Á, Ã, É, Í, Õ e Ç têm símbolos distintos de A, E, I, O e C.

Nos quadradinho em destaque, aparecerá uma data comemorativa importante no Brasil desde o ano 1822.

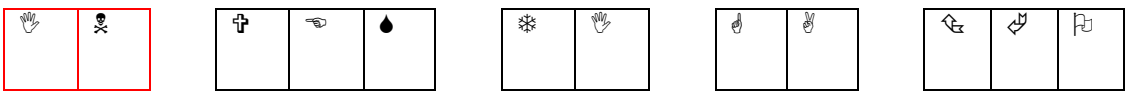
1) Empregada doméstica.

2) Retrato; imagem.

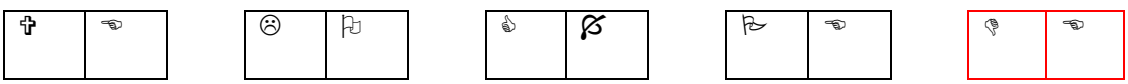


3) Folheto onde são indicados dias, semanas e meses.

4) Ação profissional de um detetive.



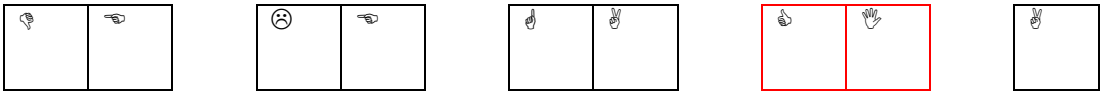
5) Triciclo infantil.



6) Forma de processo mental.

7) Igual; semelhante.

8) Repartição de delegado.



9) Desenho da Disney.

PERGUNTAS

1) Qual foi o dia comemorado desde 1822 que apareceu nos quadradinhos em destaque?

2) Expliquem quais foram às dificuldades sentidas pelo grupo para resolver esta atividade.

3) Expliquem quais foram às facilidades sentidas pelo grupo para resolver esta atividade

4) Descreva detalhadamente o processo de resolução desta atividade.

UM CASO DE SEQUESTRO

Holmes estava na Espanha, entretendo-se com as touradas, quando foi procurado pelo inspetor Lestrade.

O inspetor trazia para Holmes um caso de sequestro. O professor Sergio Carrilho havia sido sequestrado durante sua aula de matemática, na Universidade Complutense de Madri.

Na sala de aula, tudo parecia normal, até mesmo algumas contas no quadro negro.

Ao entrar na cena do crime, Holmes analisou o ambiente e na mesma hora percebeu o motivo do sequestro. Preocupado, Holmes sabia que a vida do professor estava em suas mãos.

Infelizmente o Dr. Watson estava em uma viagem e assim Holmes se viu sozinho com este caso importante. Desta maneira, ele convocou alguns alunos para ajudá-lo a resolver o crime.

Durante as investigações Holmes sentiu um mal estar e foi levado inconsciente para o hospital deixando apenas uma carta criptografada para os seus ajudantes, no bolso de seu paletó.

Assim, resta a seus ajudantes descobrir que mensagem estava escrita na carta e torcer para que nela esteja a identidade do(s) sequestrador(es), o motivo do sequestro e o local onde o professor de matemática está sendo mantido preso, para que a polícia possa agir antes que o criminoso faça algum mal ao professor.

19	*	23	9	21	25	9	23	24	22	5	8	19	22	*	é	*	25	17	*
5	16	25	18	19	*	8	19	*	20	22	19	10	9	23	23	19	22	*	7
12	5	17	5	8	19	*	14	19	23	é	*	20	13	9	22	9	*	8	9
*	19	16	13	26	9	13	22	5	*	19	*	17	19	24	13	26	19	*	8
19	*	23	9	21	25	9	23	24	22	19	*	9	22	5	*	21	u	9	*
19	*	5	16	25	18	19	*	23	9	22	13	5	*	22	9	20	22	19	26
5	8	19	*	18	5	*	8	13	23	7	13	20	16	13	18	5	*	8	9
*	17	5	24	9	17	á	24	13	7	5	*	18	9	23	24	9	*	5	18
19	*	9	*	19	*	20	22	19	10	9	23	23	19	22	*	9	23	24	5
*	23	9	18	8	19	*	17	5	18	24	13	8	19	*	20	22	9	23	19
*	18	5	*	23	5	16	5	*	8	9	*	26	í	8	9	19	*	8	5
*	9	23	7	19	16	5	.												

PERGUNTAS

1) Qual é o nome do sequestrador?

2) Qual o motivo do sequestro?

3) Qual o local onde o professor está sendo mantido preso?

4) Expliquem quais foram às dificuldades sentidas pelo grupo para resolver esta atividade.

5) Expliquem quais foram às facilidades sentidas pelo grupo para resolver esta atividade.

6) Descreva detalhadamente qual foi o processo utilizado pelo grupo para decifrar a carta de Holmes.

7) Qual a relação utilizada para criptografar as letras do alfabeto? Justifique.

8) Monte um esquema que represente a cifração das letras do alfabeto. Justifique seu esquema.

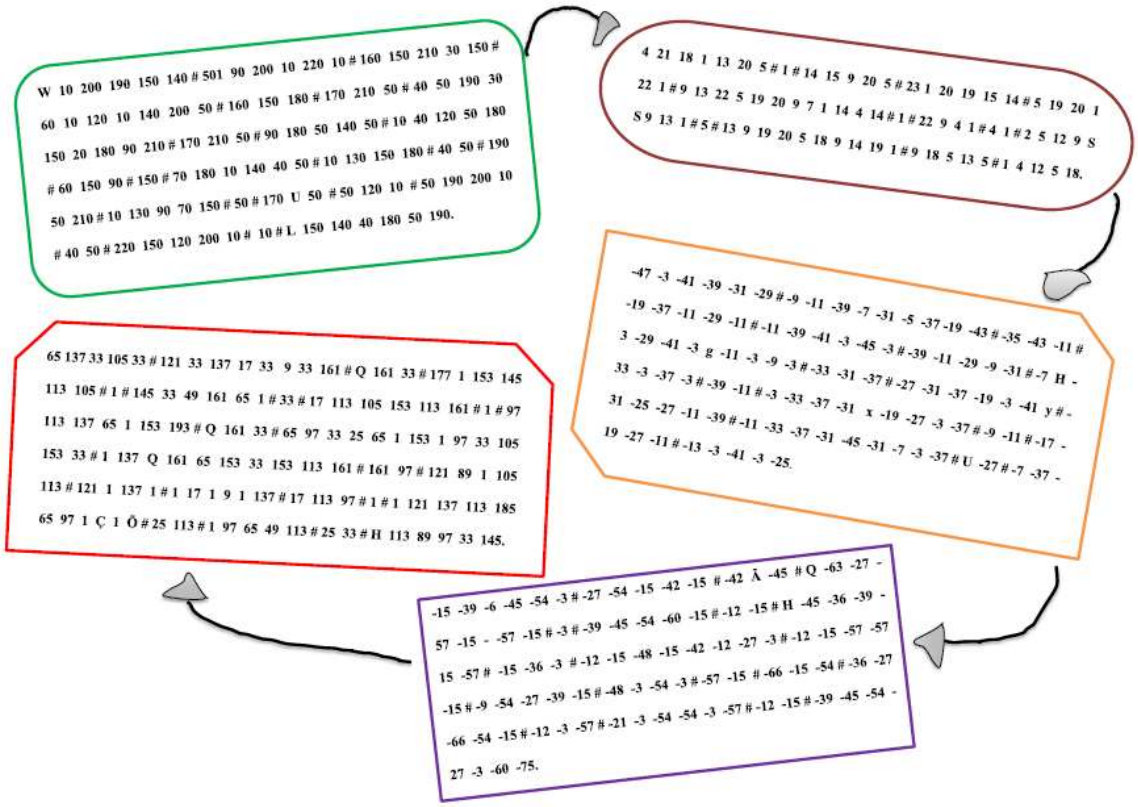
O DETETIVE DR. WATSON

- Watson é um grande amigo e assistente – disse Holmes para o inspetor Lestrade da Scotland Year, mas nos últimos dias ele anda enigmático, pouco falante e mal anda dormindo em casa.

O inspetor, certo de que o Dr. Watson havia se cansado do convívio e da amizade de Holmes, não demostrou interesse em investigar o Dr. Watson e mandou Holmes para casa.

Holmes, como de costume, muito perseverante e confiante em seu instinto decidiu investigar seu amigo por conta própria. Após alguns telefonemas e uma bisbilhotada no quarto de Watson, Holmes encontrou alguns rabiscos criptografados e percebeu que seu amigo estava envolvido em algo misterioso.

Mesmo reunindo todas as pistas, Holmes ainda sentia dificuldade em saber o que estava acontecendo com Watson, sendo assim, ele convocou alguns alunos para ajudá-lo a montar esse quebra cabeça de mistérios que Watson estava envolvido e comprovar para o inspetor Lestrade que algo estava acontecendo.



PERGUNTAS

1) Por que o Dr. Watson estava pouco falante e mal dormia em sua casa?

2) Qual é a teia de mistérios na qual o Dr. Watson estava envolvido?

3) Descreva detalhadamente qual o processo utilizado para decifrarem as pistas.

4) Identifique e escreva abaixo o modo utilizado para se criptografar cada uma das pistas I, II, III, IV e V encontradas por Holmes no quarto de Watson.

5) Existem diferenças e semelhanças entre os modos utilizados para se criptografar cada pista? Caso existam justifique.

6) Discuta com seus colegas se é possível escrever esses modos como uma ***expressão matemática***? Se sim, tente encontrar essas expressões, se não justifique.

7) Pensem em uma nova expressão matemática com base nas expressões matemáticas do item (6) e utilizem-na para criptografar seus nomes.

8) Que expressão matemática vocês escolheram no item (7) para criptografar seus nomes? Justifique essa escolha.

9) Compare a expressão criada por vocês no item (7) com as expressões do item (6). Quais as semelhanças e diferenças entre elas?

10) A partir das respostas dos itens anteriores, tentem escrever de uma maneira geral a expressão matemática que esta sendo utilizada.

O POEMA

Soneto da Fidelidade
Vinicius de Moraes

De tudo ao meu amor serei atento
Antes, e com tal zelo, e sempre, e tanto

Que mesmo em face do maior encanto
Dele se encante mais meu pensamento

Quero vive-lo em cada vão momento
E em seu louvor hei de espalhar meu canto

E rir meu riso e derramar meu pranto
Ao seu pensar ou seu contentamento

E assim quando mais tarde me procure
Quem sabe a morte, angústia de quem vive

Quem sabe a solidão, fim de quem ama
Eu possa me dizer do amor (que tive):

Que não seja imortal, posto que é chama
Mas que seja infinito enquanto dure

ENSINANDO O Dr. WATSON

Em dias ociosos, Holmes deixava de ser detetive e assumia o papel de professor do Dr. Watson.

Hoje era um dia como esse. Nesta manhã, Holmes se levantou disposto a mexer com a cabeça de Watson através da lógica e com isso, aguçar a astúcia de seu amigo.

Logo no café da manhã Holmes anunciou:

- Watson, hoje te apresentarei a arte da Criptografia.

- Criptografia....já ouvi esse termo, mas não sei muito bem o que ela quer dizer – Retrucou Watson para Holmes ainda sonolento.

- Então se sente aqui, e enquanto você toma seu café e desperta para o dia, irei te dar uma pequena aula sobre essa arte magnífica.

- Arte? Mas isso é um quadro por acaso?

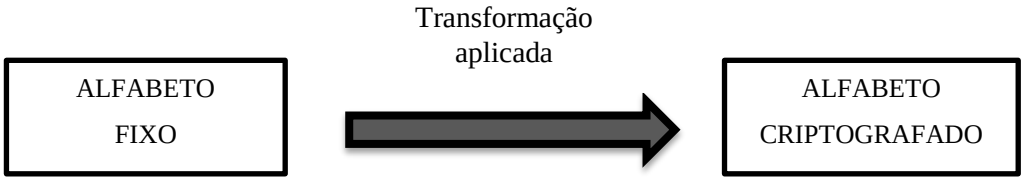
- Ah, meu caro Watson, suas perguntas me fazem rir, mas deixe-me começar a explicar que você já irá entender.

Holmes virou-se então para a lousa, que se encontrava prontamente preparada no meio da sala e começou a falar e rabisca-la a todo o vapor.

Watson acompanhava o raciocínio de Holmes com muita atenção, até que em certo momento ele disse.

- Holmes, podemos então representar a Criptografia através de um esquema criptográfico.

Neste momento Watson levantou-se da mesa e foi até o quadro onde desenhou o seguinte esquema:



Nessa hora Holmes sorriu e disse.

- Isso mesmo Watson, vejo que agora você entendeu exatamente o que é criptografar uma mensagem, mas lembre-se, a transformação utilizada para criptografar pode ser qualquer coisa que cifre as letras do alfabeto, desde símbolos até expressões matemáticas.

- Claro Holmes! Isso já está bem claro para mim, acho que agora já posso dizer que entendo a arte de se criptografar – disse Watson com todo glamour.

Holmes sabia que seu amigo era inteligente e que logo perceberia que a Criptanálise faria parte dessa aula. Contudo resolveu montar um criptograma para Watson com o intuito de que ele percebesse a importância da Criptanálise na Criptografia.

Holmes montou, então, um criptograma tabelado onde, letras iguais são representadas por números iguais. Resolvido este enigma, surgirá, nas casas em destaque um conceito matemático utilizado por Holmes para transformar o alfabeto fixo em um alfabeto criptografado.

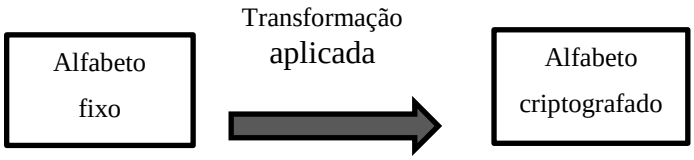
Pessoa cuja profissão costura ternos.	3	25		3	19	3	41	11
Protetor da mata; folclore brasileiro.	7	43	37		33	19	37	3
Ligado (gíria).	3	29	41	11		3	9	31
Arte de tentar esconder uma mensagem.	7	19	13	37	3		55	31
Galpão de preparo de escola de samba.	5	3	37	37	3	7		31
Espanto; terror.	3	39	39	31	27	5	37	
O benefício do testamento.	17	11	37		11	19	37	31
O café rápido feito em máquina.	11	49	33	37		39	39	31
O mais vasto oceano do mundo.		3	7	59	13	19	7	31
Carlos (?) de Andrade, celebre poeta mineiro.	9		43	27	27	31	29	9
Taxa de açúcar no sangue (med.).	15	25		7	11	27	19	3
Parte da reta entre dois pontos (mat.).	39	11	15		11	29	41	31
Razão entre seno e cosseno.	41	3	29	15		29	41	11
Desenho de marca comercial.	25	31	15	31	41		33	31
Estabelecimento que aluga filmes.	25	31	7	3	9	31		3
Bem – (?) : alegre, disposto.	17	43	27	31	37	3	9	
Figura geométrica.	33	31	25	59		31		31
Conjunto (mat.).	19	29	41	11	19		31	39
Colonizou Angola (His.).	33	31	37	41	43	15		25
Instrumento de rodas de capoeira.	5	11	37	19	27	5	3	

PERGUTAS

1. Qual o conceito matemático que surgiu nas casas em destaque?

2. Sendo o alfabeto fixo A=1, B=2, C=3 .... Z=26. Qual a função utilizada para criptografar este alfabeto e montar o criptograma? Justifique.

3. Na história, Watson representou o esquema criptográfico através de dois conjuntos (alfabeto fixo e alfabeto criptografado) e uma flecha.



Agora, utilizando a folha quadriculada, tente representar o esquema criptográfico deste enigma utilizando o plano cartesiano. Lembre-se de denominar o que é representado pelo eixo das abcissas (x) e pelo eixo das ordenadas (y). Justifique seu esquema.

O JOGO

- Alguém está querendo jogar com você – disse Watson para Holmes.

- Mas neste jogo uma pessoa pode estar correndo perigo e a minha derrota pode significar sua morte – retrucou Holmes.

Holmes estava realmente preocupado com este quebra-cabeça. Durante um mês ele recebeu 6 mensagens secretas e um telefonema.

Nesta ligação seu misterioso adversário admitiu que o fracasso de Holmes neste enigma custaria a vida de uma celebridade inglesa e que ele tinha 24 horas para descobrir a mensagem e chegar a tempo de salvar a vida da vítima.

Depois de algumas horas analisando as mensagens enviadas, Holmes percebeu que juntas elas formavam um texto e que quando decifradas revelariam a identidade da celebridade que estava em perigo.

Mais algumas horas estudando o caso, Holmes conseguiu montar um esquema de gráficos (Figura 1) que talvez o ajuda-se a resolver as mensagens secretas.

Cada segmento de reta desenhado no plano cartesiano é um gráfico correspondente a uma função utilizada para cifrar uma mensagem. Os seis gráficos montados por Holmes correspondem a seis funções utilizadas para criptografar as seis mensagens enviadas, mas esta conclusão ainda não resolvia o enigma e a vítima ainda corria perigo.

Com poucas horas para o fim do prazo estipulado pelo seu adversário, Holmes convocou seus ajudantes para lhe auxiliar a desvendar este mistério, salvar a vida da celebridade e ganhar o jogo.

Então vamos ajuda-los!!!!!

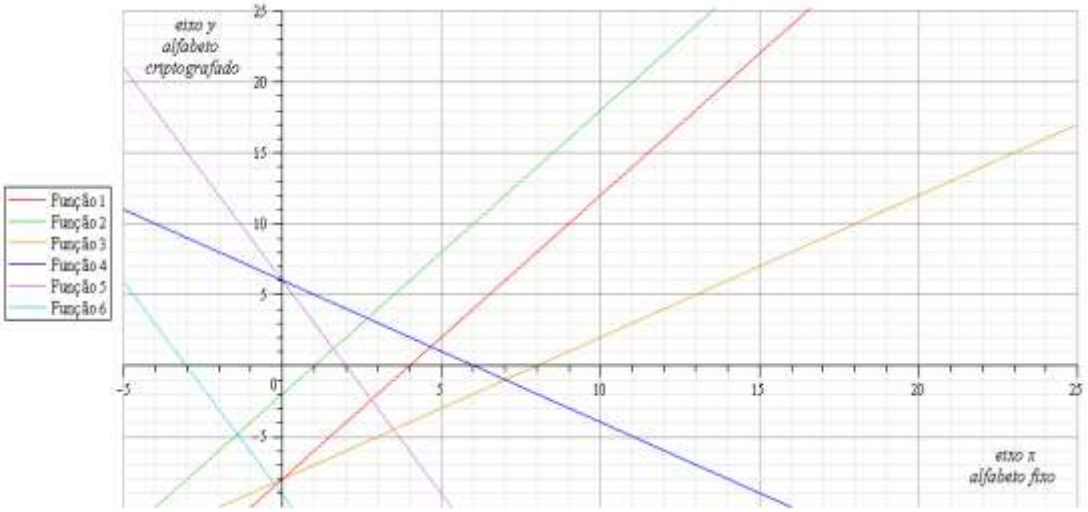


Figura 1

PERGUNTAS

1) Analisando a figura 1 responda:

a) Para que valores de x as funções $F_1(x)$, $F_2(x)$, $F_3(x)$, $F_4(x)$, $F_5(x)$ e $F_6(x)$ são iguais à zero, ou seja, quando $F_i(x)$ for igual a zero seu gráfico cortará o eixo x em que valor?

b) Para quais valores de x as funções $F_1(x)$, $F_2(x)$, $F_3(x)$, $F_4(x)$, $F_5(x)$ e $F_6(x)$ são maiores que zero?

c) Para quais valores de x as funções $F_1(x)$, $F_2(x)$, $F_3(x)$, $F_4(x)$, $F_5(x)$ e $F_6(x)$ são menores que zero?

2) Olhando para a figura 1 e utilizando os resultados do item (1), identifique a função afim de cada função e preencha a tabela. Justifique seu raciocínio.

	Função
Função 1	$F_1(x)$ =
Função 2	$F_2(x)$ =
Função 3	$F_3(x)$ =
Função 4	$F_4(x)$ =
Função 5	$F_5(x)$ =
Função 6	$F_6(x)$ =

3) Qual o texto formado pelas mensagens?

4) Descreva detalhadamente qual o processo utilizado para identificar as funções.

5) Descreva detalhadamente qual o processo utilizado para decifrar as pistas.

6) Analisando a tabela do item (2) descreva todas as semelhanças e todas as diferenças entre os coeficientes ***a*** e ***b*** das funções. Qual o resultado dessas semelhanças e diferenças no gráfico?

7) Compare o comportamento do gráfico das funções baseados nas semelhanças e diferenças entre os coeficientes ***a*** e ***b*** de cada função.

8) Qual é o papel dos coeficientes ***a*** e ***b*** no comportamento de cada função no gráfico?

9) Analisando a figura (1), a tabela do item (2) e as respostas das questões anteriores, classifique as funções $F_1(x)$, $F_2(x)$, $F_3(x)$, $F_4(x)$, $F_5(x)$ e $F_6(x)$ em funções crescentes e decrescentes. Justifique essa classificação.

10) Utilizando os itens (1) e (9) generalize quando uma função é crescente e quando ela é decrescente. Justifique.

O POETA ASSASSINO

A cada crime, o assassino deixava um poema referente ao próximo crime. Neste mês, quatro pessoas foram mortas por esse homem. O inspetor Lestrade, sem saída para este enigma, convidou Holmes e seus ajudantes para tentar decifrar o último poema deixado pelo assassino e com isso, tentar descobrir quem será a próxima vítima, o local do crime e o motivo dessa morte.

Determine a frase original de cada linha do poema, sabendo que para cada linha foi usada uma função de primeiro grau.

Revele o poema deixado pelo assassino e descubra onde será o próximo crime, a vítima e o motivo dessa morte.

f(x) = x	4 9 26 5 13 # 17 21 5 # 20 21 4 15 # 12 1 # 5 # 19 9 14 9 19 20 18 15 # 4 9 6 5 18 5 14 20 5
f(x) = x – 1	0 19 4 # 12 4 18 12 14 # 18 4 20 18 # 12 14 17 0 3 14 17 4 19
f(x) = x + 3	23 18 7 18 # 16 24 17 7 18 # 20 24 8 # 15 4 # 21 8 22 12 7 8 # 8 # 19 4 21 8 17 23 8
f(x) = -x + 40	27 39 21 # 26 39 25 # 21 35 26 20 35 27 # 27 39 31 21 # 39 21 # 36 25 22 35 21
f(x) = 5x	5 # 90 45 85 105 25 130 5 # 25 # 20 25 # 25 95 100 45 65 5 20 75 # 110 5 60 75 90 # 30 45 70 5 70 15 25 45 90 75
f(x) = 4x – 3	13 17 # 57 69 33 25 17 49 # 69 17 49 57 77 1 # 29 57 39 17 54 77 1 # 13 17 # 54 81 1 13 57 # 45 1 5 57 69
f(x) = 2x + 2	12 30 36 44 4 30 42 32 # 8 38 12 40 8 12 # 44 28 # 32 26 18 4 38 # 20 30 42 12 38 12 40 40 12 20 38 32
f(x) = $\frac{6x-2}{2}$	11 14 56 47 14 53 59 2 # 14 38 # 56 14 62 # 56 14 26 44 # 44 11 26 44 # 14 # 53 2 8 44 53
f(x) = -2x + 73	71 # 59 71 45 71 45 67 55 71 # 61 63 21 # 65 63 49 63 # 67 71 41 71 21
f(x) = 3x + 1	13 16 # 16 37 28 40 28 43 4 55 # 52 64 16 40 # 61 28 67 16 58 58 16 # 13 28 43 25 16 28 55 46 # 4 # 13 28 58 49 46 55
f(x) = $\frac{9x-3}{3}$	44 # 26 53 38 2 44 # 11 44 # 38 14 62 # 47 2 26 # 2 50 62 14 35 14 # 53 2 47 2 77
f(x) = 10x - 2	188 48 138 198 88 178 8 # 128 88 138 78 8 # 118 8 128 88 138 8 # 38 88 188 188 88 158 8 178 # 188 48 208 # 28 8 118 148 178

FICHA DE CÁLCULOS

PERGUNTAS

1) Qual o poema deixado pelo assassino?

2) Onde será o próximo crime?

3) Quem será a próxima vítima?

4) Qual o motivo dessa morte?

5) Descreva detalhadamente qual foi o processo utilizado para a decifração do poema.

CIFRANDO SUA HISTÓRIA

O assassinato do Shopping (Igor)

"Notícias chegaram a pouco tempo de um assassinato que ocorreu no shopping de Rio Claro. Não se sabe ainda quem foi o assassino, mas quem foi morto foi o dono de uma loja de roupa que se localizava no shopping. No momento do assassinato estavam o dono do estabelecimento e mais seus funcionários que não sofreram nenhum dano...".

Chegando a cena do crime Jimy, um jovem policial da área, observou a cena do crime, ele observou bem aquela cena. Logo, ele procurou os funcionários do local que ainda estavam lá e começou a interroga-las:

- Olá moças! – disse Jimy.

- Já estou ficando melhor – Falou Jessica.

- Eu ainda preciso de um pouco mais de tempo para me acalmar – disse Sabrina.

- Bom, nos últimos dias teve alguém que ameaçou o seu patrão?

- Não – afirmou Sabrina.

- Espera ai! Teve um homem que entrou na loja ontem, estava muito drogado, ficou bravo por que nós não quisemos atende-lo – disse Jessica.

- Entendo!

Jimy foi até a sala de segurança do shopping. Viu as gravações das lojas e também do estacionamento. Ficou três dias analisando as evidencias, chamou o delegado que estava cuidando do caso, falou com ele e disse:

- Já descobri quem matou o seu João, o dono da loja.

- Quem? – perguntou o delegado.

- Um cara conhecido como Tuto. Ele acabou arrumando confusão na aloja de roupas. Seu João agiu errado ameaçando Tuto. Disse qUe se ele não saísse dali iria mata-lo.

- É – ele agiu errado mesmo.

- Enfim, na noite do crime, Tuto decidiu matar seu João, para ganhar reputação e se vingar dos insultos que seu João fez a ele.

Depois disso, prenderam Tuto que foi condenado a 20 anos de prisão e Tuto voltou a ser o que era.

A escola (Jaciara)

No dia 20 de agosto de 1998, na cidade de Rio Claro, aconteceu um fato surreal, numa escola pública. Dois alunos envolveram em uma briga, que levou a morte de uma dos envolvidas. Eram namorados, tinham muitos amigos e se gostavam muito, mas quando foi um dia, um dia normal, entrou um novato na escola e por coincidência caiu na sala das mesma.

A garota de nome não conhecido, logo o achou interessante, dia a dia, cada vez mais íntimos, ficaram mais amigos, mas isso pareceu não agradar nem um pouquinho ao seu namorado, que cada vez mais ficava com ciúmes.

Bobo, sem perceber, o novato não sabia o que poderia acontecer. Todo dia percebia que cada vez mais ficava mais envolvido com essa garota, não percebia que isso poderia levar a algo maior. O garoto, simples humilde, sempre cabisbaixo, não entendia nada, só sabia que não poderia nem pensar na possibilidade de chegar a ser mais importante e chamar a atenção de quem o odiasse.

O namorado da garota, por sua vez, vendo o que acontecia, não poderia deixar por menos, logo ele chamou todo o grupo e foi tirar satisfação com o novato. Achando que com isso não pagaria de chifrudo, mas algo saiu errado, no meio da briga, com todos discutindo, ouviu-se um tiro, do nada, tudo ficou silencioso, todos assustados sem saber o que aconteceu, perguntavam:

- Quem morreu?

- De onde veio o tiro?

- Quem atirou?

Perguntas sem respostas, de longe ninguém sabia o que havia acontecido. O garoto caído estava morto, mas ninguém sabia quem o montou. Perguntaram:

- Foi o novato?

- Mas será que foi ele? Ninguém sabia, tudo ficou um mistério, mas algum tempo depois uma voz, bem longe escondida disse:

- Fui Eu!

Todos procuraram aquela voz que parecia feminina.

Logo do escuro sai uma garota, todos ficam impressionados, pois a garota era a sua namorada.

Perguntavam:

- Por que você fez isso?

Por algum tempo ficaram sem respostas, mas a garota logo que percebeu o que havia feito começou a chorar e pedir desculpas, pois estava fora de si.

Vendo toda aquela briga, qUe o motivo era ela, nÃo conseguiu ficar quieta, e tomou uma providencia que no caso sem experiência e sem pensar tirou a vida de seu grande amor.O novato não conseguiu acreditar que havia sido ela, pois era tão doce, que nunca pensaria nela como uma assassina.

Todos ali no meio do pátio da escola presenciaram um fato real que deixa marcas profundas, pois a vida é um dilema: Só é boa enquanto dura....

Um lago nem tanto azul (Janaína)

Em um belo dia ensolarado um rapaz estava a passar no parque, esse homem era um cara simples, e de poucas amizades, era um rapaz alto, moreno, de presença, não aparentava nenhuma suspeita.

Mas o que ele não sabia era que naquele dia, algo iria acontecer. Ele havia terminado com a namorada há uma semana, e o que parecia era que ela não estava conformada com a separação e ele nem imaginava que ela também estaria ali naquele mesmo lugar.

Num certo momento, ele resolveu andar pelo centro do lado do parque, quando de repente ele foi surpreendido por uma pessoa encapuzada. Levou-o para dentro de um carro preto.

Esta fazendo um mês que esse rapaz desapareceu, família e amigos espalharam cartazes por toda a vizinhança a procura deste homem, será que há alguma esperança de sobrevivência, ou esta morto?

Esse caso só um detetive conseguiria resolver.

Policiais descontentes com sua investigação resolveram contratar um detetive para resolver esse mistério. Enfim, feita contratação, o nome do contratado era Holmens.

O primeiro passo, de sua investigação: ir ao local do desaparecimento do rapaz. A união das pistas que o gênio Holmens encontrou foi algumas pegadas de tênis do rapaz, mas ele não tinha certeza que era aquele homem.

O segundo passo, era saber mais sobre aquele rapaz e então Holmens foi a procura de amigos e parentes do rapaz e também de familiares de sua ex-namorada. Chegando lá na casa da mãe do rapaz Holmens começou a fazer vários questionamentos para a família.

A família disse que o rapaz era calmo e paciente com sua ex e ela o mesmo com ele, disse também que o casal aparentava muito amor um pelo outro e que não aparentava nenhuma ignorância e desrespeito um com o outro.

Depois dessas informações da família do rapaz, Holmens foi atrás da família da ex namorada e fez as mesmas perguntas a eles. Chegando a casa da ex namorada, Holmens se assustou com a aparência da moça, pálida e de olhos inchados, e como Holmens é muito observador ele viu varias e coisas e começou a perguntar para ela:

- Você tem alguma coisa a ver com esse desaparecimento?

- Não foi por que eu quis.

- Calma, me explique o que esta acontecendo.

- Foi Um dia ensolarado, 08/03/2014, eu fui naquele bendito parque determinada a dar um fim nisso ta basta nesse romance, Mas não fui sozinha, fui acompanhada de meu irmão. Então meu irmão o arrastou até o carro e o levou para uma casa de sitio. Lá nessa casa, eu o matei com um tiro no peito.

Depois da confissão, Holmens fez uma ligação dizendo eu o caso já estava resolvido. Depois de alguns dias o corpo do rapaz foi encontrado e a moça respondia esse crime em liberdade como legitima defesa.

APÊNDICE C – ROTEIRO DAS ENTREVISTAS

Pergunta para os alunos

1- No início do ano quando fui convidar os aluno a participar das atividades envolvendo Criptografia e Matemática, o que levou você a querer participar do trabalho proposto?

2- Durante nossos 18 encontros nós trabalhamos com 8 atividades. Tente lembrar-se desses encontros e conte para mim:

a) Qual foi a atividade que você mais gostou? Por quê?

b) E qual foi a atividade que você menos gostou? Por quê?

c) Qual você sentiu mais dificuldade de desenvolver? Por quê?

3- O que você acha da maneira como as atividades foram desenvolvidas, considerando: a dinâmica em que ocorreram a atividade, o trabalho desenvolvido em grupo, etc.

4- Conte para mim:

a) O que te levou a querer continuar a participar de todas as atividades?

5- Por que você acha que Fernando não continuar participando das atividades / Fernando, no segundo semestre percebi que você não se envolveu tanto com as atividades como no primeiro semestre? Por quê isso ocorreu?

6- Depois de todos os encontros e das atividades desenvolvidas o que você pode dizer sobre

a) Função afim?

b) Criptografia?

c) Em sua opinião quais outros conteúdos que você conhece que poderiam ser desenvolvidos no estilo dos nossos encontros?

Pergunta para a coordenadora pedagógica do Ensino Médio

Considerando o trabalho desenvolvido na escola você, o que você observou nos alunos que participaram do projeto? Houve algo que te chamou atenção?

APÊNDICE D – RESUMO HISTÓRICO

Olhando para a história da criptografia

Este apêndice apresentará um resumo da história da criptografia, relatando algumas passagens interessantes e importantes. Destaca-se que muitos acontecimentos foram deixados de lado, bem como o detalhamento (histórico e matemático) de algumas cifras. Tal resumo se baseou na obra *O livro dos códigos: A ciência do sigilo – do antigo Egito à criptografia quântica*, de Singh (2008) e em pesquisas na internet em relação a alguns nomes, como Babbage, Turing, Rivest, Shamir, Adleman entre outros e a alguns lugares citados por Singh (2008), como, Bletchley Park.

A evolução da escrita secreta

A criptografia é tão antiga quanto a própria escrita. Alguns de seus primeiros relatos datam de Heródoto. Conhecido como "o pai da história", ele escreveu *As histórias*, livro no qual narra os conflitos entre a Grécia e a Pérsia, ocorridos no quinto século antes de Cristo. De acordo com Heródoto, a Grécia só não foi conquistada pelo líder dos persas em virtude de seu exército e de sua comunicação secreta. Outro fato também narrado pelo "pai da história" é sobre Histaeu, que queria encorajar Aristágora de Mileto a se revoltar contra o rei persa. Para enviar a mensagem de forma segura, Histaeu raspou a cabeça de um mensageiro, escreveu a mensagem no couro cabeludo e aguardou que o cabelo crescesse novamente. Podendo viajar tranquilamente, o mensageiro foi enviado e, só depois de chegar ao seu destino, é que sua cabeça foi raspada novamente, revelando ao destinatário a mensagem escondida. Nessa situação, observa-se que a ocultação de uma mensagem foi suficiente para transmitir a mesma em segurança.

A circunstância descrita acima, em que a comunicação secreta é obtida apenas pela ocultação da mensagem, é conhecida como *esteganografia*, que deriva das palavras gregas *steganos*, que significa coberto, e *gráphein*, que significa escrever. Esse tipo de comunicação, embora ofereça certa segurança, sofre uma fraqueza. Se o mensageiro fosse capturado e revistado, a mensagem poderia ser facilmente descoberta e seu conteúdo revelado.

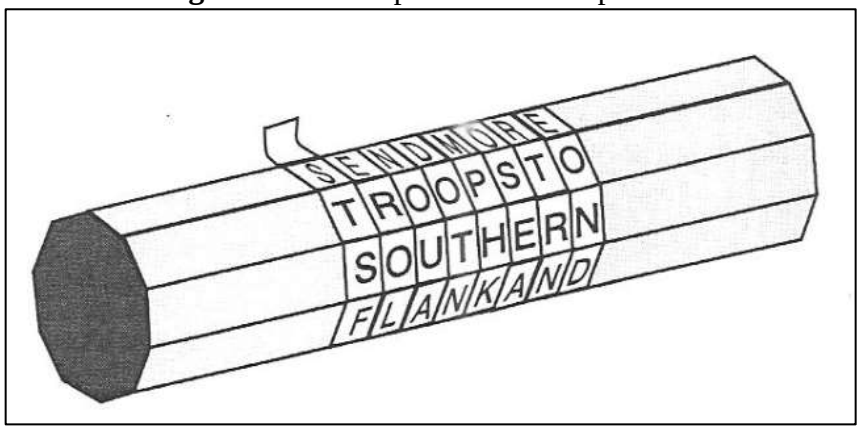
Assim, junto com o desenvolvimento da esteganografia, houve a evolução da *criptografia*, proveniente da palavra grega *kriptós*, que significa oculto. Desse modo, a

criptografia tem como objetivo esconder o significado da mensagem e não somente ocultar a sua existência. Portanto, mesmo se um inimigo interceptasse uma mensagem cifrada, esta seria incompreensível e ele não conseguiria ter acesso ao seu conteúdo. Sem a chave de cifração, o inimigo encontraria grandes dificuldades, ou até mesmo impossibilidades de descobrir a mensagem original.

Ainda que a criptografia e a esteganografia sejam estudos autônomos, elas podem ser usadas em conjunto, a fim de aumentar a segurança das mensagens. Um exemplo dessa combinação é o microponto, utilizado pelos agentes alemães durante a Segunda Guerra Mundial. Os agentes cifravam a mensagem, reduziam-na fotograficamente até transformá-la em um ponto com menos de um milímetro de diâmetro e, por último, este era oculto sobre um ponto final de uma carta supostamente inofensiva. Dentre esses dois ramos da comunicação secreta, a criptografia é considerada a mais poderosa, devido a sua capacidade de proteger as informações, mesmo que estas caiam em mãos inimigas.

A criptografia, por sua vez, pode ser dividida em dois ramos: a *transposição* e a *substituição*. Na transposição, as letras são apenas rearranjadas, produzindo um anagrama. O primeiro aparelho criptográfico militar, conhecido como *citale* espartano, era constituído basicamente pela transposição das letras. Datado do século quinto antes de Cristo, o citale é composto por um bastão de madeira e uma tira de couro ou papiro, a qual era enrolada em forma espiral, como mostra a Figura 24. Já na cifra de substituição, cada letra no texto é substituída por outra letra diferente. Assim, enquanto que na transposição a identidade das letras se mantém, mudando apenas sua posição, na substituição, sua identidade é modificada, mas sua posição é retida.

Figura 24 - Exemplo de Citale Espartano.

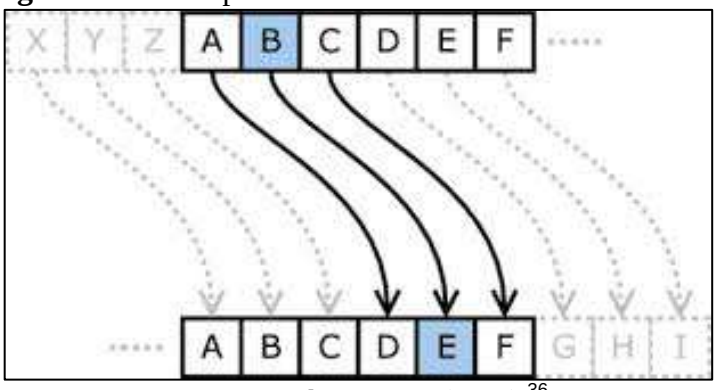


Fonte: Singh (2008, p. 24).

Júlio César, o imperador romano, utilizava muito a escrita de substituição. Em seu documento *Guerras da Gália*, César descreve com detalhes como foi o processo de entrega da

mensagem cifrada. Esse é considerado o primeiro documento que registrou o uso da criptografia para fins militares. César utilizava tão corriqueiramente a cifra de substituição, que uma de suas cifras ficou conhecida como sendo a *Cifra de César*. Essa cifra tinha como característica o deslocamento do alfabeto três casas à frente, ou seja, a letra A de uma mensagem seria cifrada pela letra D, B por E, e, assim por diante (Figura 25). Esse tipo de cifração é considerada uma cifra monoalfabética, pois é dependente de apenas um alfabeto. Uma cifra que depende de mais de um alfabeto é chamada de cifra polialfabética, porque emprega vários alfabetos cifrados por mensagem. Veremos mais adiante o surgimento da cifra polialfabética.

Figura 25 - Exemplo do deslocamento da Cifra de César.



Fonte: Google imagens (2015) [36].

A simplicidade e a força da cifra de substituição dominaram a comunicação secreta durante o primeiro milênio. No entanto, sua quebra foi descoberta no Oriente. De acordo com Singh (2008), os estudiosos árabes foram os responsáveis pela quebra da cifra de substituição, inventando assim um estudo que permite decifrar uma mensagem sem saber sua chave cifradora: a *criptoanálise*. O desenvolvimento da *análise de frequência*, técnica desenvolvida primeiro no mundo árabe e depois na Europa para quebrar a cifra de substituição, colocou a segurança das comunicações em risco. Assim, restava aos criptógrafos criarem uma nova cifra para proteger o sigilo das comunicações secretas.

Um dos progressos das cifras ocorreu somente no final do século XVI, entretanto, suas origens datam do século XV. Em 1440, Leon Battista Alberti propôs o uso de dois ou mais alfabetos cifrados para a cifração de uma mensagem. Alberti tinha a ideia de que, usando esses alfabetos alternadamente, os criptoanalistas seriam confundidos e barrados na decifração dessa nova cifra. Embora esse seja considerado um dos avanços mais significativos da

[36] Disponível em: <http://pt.wikipedia.org/wiki/Cifra_de_C%C3%A9sar>. Acessado em: 11/06/2015.

história, Alberti não conseguiu desenvolver sua ideia no papel, deixando para outras pessoas a tarefa de organizar o sistema completo de cifragem. Na lista de pensadores constam os nomes de Johannes Trithemius, Giovanni Porta e Blaise de Vigenère. No entanto, foi Vigenère, por volta de 1562, que desenvolveu a forma final dessa cifra, ficando conhecida como sendo a *Cifra de Vigenère*. Essa cifra é composta por 26 alfabetos cifrados distintamente (Figura 26), que são utilizados para a cifração de uma mensagem.

Figura 26 - Exemplo da Cifra de Vigenère.

Alfabeto correto	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Fonte: Singh (2008, p. 66).

Esse tipo de cifra, considerada polialfabética, surge na história como sendo uma cifra coerente e muito poderosa, pois, diferentemente da cifra monoalfabética, ela é imune a um ataque simples de análise de frequência. Vigenère publicou seu trabalho em 1586, em um

Tratado sobre a Escrita Secreta, contudo, seu trabalho foi pouco explorado e deixado de lado pelos dois séculos seguintes.

Nos anos de 1700, a criptoanálise já estava fortemente consolidada em vários países. Cada potência europeia tinha um centro chamado *Câmara Negra*, a qual tinha como objetivo decifrar mensagens e reunir informações. As Câmaras Negras tornaram todo o tipo de cifração monoalfabética insegura e, com isso, os criptógrafos foram forçados a aderirem à cifra de Vigenère, que era mais complexa, porém mais segura. O momento histórico também exigia formas mais seguras de cifragem. O desenvolvimento do telégrafo e a necessidade de proteger as mensagens enviadas por eles ajudaram a pressionar os criptógrafos a adotarem oficialmente as cifras polialfabéticas. Apesar de o telégrafo e a revolução das comunicações terem se concretizado no século XIX, seus primeiros passos podem ser encontrados no ano de 1753.

Na Inglaterra, Sir Charles Wheatstone e William Fothergill Cooke construíram um sistema para detectar os sinais elétricos enviados pelos telégrafos. Tal sistema ficou conhecido como *Wheatstone-Cooke* e, por volta de 1839, o sistema funcionava perfeitamente a uma distância de 29 quilômetros entre as estações ferroviárias de West Drayton e Paddington.

Após alguns anos, na América, Samuel Morse se concentrava na construção da primeira linha telegráfica, que cobria uma distância de 60 quilômetros entre Baltimore e Washington. Ele também desenvolveu o *Código Morse*, conhecido até os dias de hoje por transformar as letras do alfabeto em uma série de pontos e traços (Figura 27). A versão de Morse, aos poucos, foi tomando o lugar do sistema Wheatstone-Cooke. Em 1851, o código Morse evoluiu com a inclusão das letras acentuadas. Com o passar dos anos, o código Morse e o telégrafo se tornavam cada vez mais difundidos nas sociedades e exerciam uma influência cada vez maior no mundo. Contudo, ainda existia a preocupação com a proteção das mensagens e o sigilo de seus conteúdos. O código Morse não é uma forma de criptografia, visto que ele não torna a mensagem oculta. Os pontos e traços são apenas representações das letras do alfabeto para as transmissões telegráficas. Assim sendo, o processo de cifração da mensagem ainda era essencial e a cifra polialfabética de Vigenère era claramente a cifra mais forte existente naquela época.

Durante os anos seguintes, a cifra de Vigenère continuou sendo a cifra mais resistente utilizada pelos governantes, entretanto, em 1854, Charles Babbage desenvolveu a quebra dessa cifra, mostrando que ela se tornaria tão fraca quanto qualquer outra – mas Babbage não publicou suas descobertas, ficando essas escondidas até o século XX, quando estudiosos examinaram suas anotações.

Figura 27 - Exemplo do Código Morse.

Símbolo	Código	Símbolo	Código
A	·–	W	·––
B	–···	X	–··–
C	–·–·	Y	–·––
D	–··	Z	––··
E	·	1	·————
F	··–·	2	··———
G	––·	3	···––
H	····	4	····–
I	··	5	·····
J	·–––	6	–····
K	–·–	7	––···
L	·–··	8	–––··
M	––	9	––––·
N	–·	0	–––––
O	–––	ponto final	·–·–·–
P	·––·	vírgula	––··––
Q	––·–	ponto de interrogação	··––··
R	·–·	dois pontos	–––···
S	···	ponto e vírgula	–·–·–·
T	–	hífen	–····–
U	··–	barra	–··–·
V	···–	aspas	·–··–·

Fonte: Singh (2008, p. 80).

As técnicas para decifrar a cifra de Vigenère foram descobertas isoladamente por Friedrich Wilhelm Kasiski. Em 1863, ele publicou seu trabalho e, desde então, essas técnicas ficaram conhecidas como Teste de Kasiski, e as contribuições de Babbage foram ignoradas.

No final do século XIX, a criptografia passava por uma crise. Depois da quebra da cifra de Vigenère, realizada por Babbage e Kasiski, os criptógrafos enfrentavam a pressão de criarem uma cifra mais segura e resistente. A comunicação secreta estava sendo comprometida e cabia a eles restabelecer o sigilo das mensagens novamente. Ademais, o século seguinte seria marcado pelo surgimento do rádio, uma poderosa ferramenta de telecomunicação inventada por Guglielmo Marconi.

Marconi iniciou seus estudos sobre os circuitos elétricos em 1894. Depois de seu projeto passar por aperfeiçoamentos, ele foi capaz de transmitir e receber pulsos de informações a

uma distância de até 2,5 quilômetros. Embora o telégrafo estivesse bem estabelecido, ele requeria o uso de fios para o transporte da mensagem. A invenção de Marconi também transportava uma mensagem, mas, agora, o sistema de telecomunicação não dependia de fios. Em 1896, Marconi patenteou sua ideia e prosseguiu com os experimentos para o progresso de sua invenção. Primeiro, ele aumentou o alcance da comunicação por rádio para uma distância de 15 quilômetros e, depois, para 53 quilômetros. Ao mesmo tempo, ele buscava aplicações comerciais de sua invenção.

Não demoraria muito para os militares se fascinarem com o rádio. As vantagens desse novo meio de comunicação eram claras. Os oficiais poderiam agora se comunicar com suas bases por meio de uma comunicação direta (sem fios) e ainda manteria o contato contínuo com seus batalhões, quando estes estavam nos campos de batalha. Tal invenção causava desejo e medo entre os generais, pois o rádio, ao mesmo tempo em que apresentava a agilidade na comunicação, também apresentava a fraqueza da segurança, já que as ondas de rádio chegavam a qualquer um em qualquer lugar, e uma interceptação poderia ser realizada com grande facilidade.

Frente a essa situação, era essencial a criação de uma cifra confiável. Os criadores de cifras precisavam garantir novamente o sigilo das mensagens durante as suas transmissões. Entre os anos de 1914 e 1918, essa busca foi marcada por vários fracassos. Embora os criptógrafos tenham produzido várias cifras novas, nenhuma delas barrou os ataques dos decifradores. A cifra *ADFGVX*, introduzida no dia 5 de março de 1918, foi uma das cifras mais famosas durante a Primeira Guerra Mundial. Os alemães utilizaram frequentemente essa cifra, acreditando em sua segurança, entretanto, o criptoanalista Georges Painvin, no dia 2 de junho de 1918, realizou a decifração de uma mensagem em ADFGVX.

A quebra dessa cifra foi um exemplo corriqueiro da criptografia durante o período da Primeira Guerra Mundial. Mas, mesmo com o desenvolvimento de novas cifras, todas acabavam sendo variações ou combinações das cifras do século XIX. Além do mais, existia na época uma nova simplicidade para os criptoanalistas: a facilidade da interceptação das mensagens, que eram feitas, então, via rádio.

Nesse momento da história, observam-se claramente as vantagens que os criptoanalistas tinham sobre os criptógrafos. A busca por uma cifra segura continuou durante os anos posteriores à Primeira Guerra Mundial. Não demorou muito para que os criptógrafos fizessem uma descoberta que restabeleceria as comunicações secretas nos campos de batalha. A evolução dessa nova cifra exigiu que os criptógrafos deixassem de lado os lápis e papéis e passassem para a exploração das tecnologias.

A evolução dos equipamentos de cifragem

O surgimento da primeira máquina criptográfica é datado do século XV. O disco de cifras, como ficou conhecido, foi inventado por Leon Alberti. Esta máquina era composta por dois discos de cobre, um maior que o outro. O alfabeto era gravado ao longo da borda de cada disco e ambos eram fixados (o menor em cima do maior) por um pino, que atuava como um eixo (Figura 28). Os dois discos poderiam ser girados de forma independente, assim, suas posições poderiam variar, gerando várias cifras de deslocamento. De acordo com Singh (2008, p. 144), esse disco era "considerado um 'misturador' que pega cada letra do texto original e a transforma em alguma outra coisa".

Esse modo de cifração, embora mecanizado, ainda era relativamente fácil de ser decifrado. Entretanto, Alberti ainda sugeriu que cada letra da mensagem fosse cifrada com uma disposição diferente do disco. Esse rearranjo do alfabeto a cada letra nada mais era do que a cifra polialfabética, uma versão mecanizada da cifra de Vigenère.

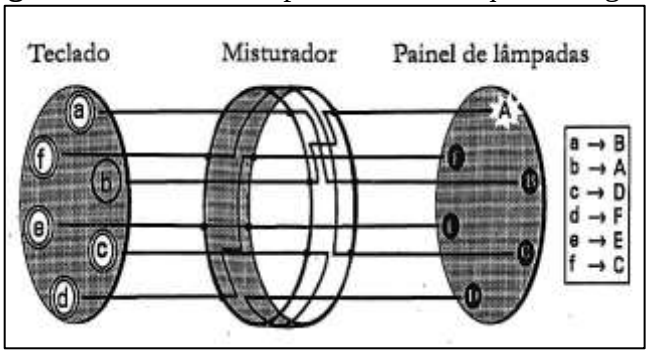
Figura 28 - Exemplo do disco de cifras.

Fonte: Singh (2008, p. 144).

Quinhentos anos depois de Alberti, seu disco de cifras renasceu de forma mais complicada e memorável. No ano de 1918, o inventor Arthur Scherbius e seu amigo Richard Ritter fundaram uma empresa de engenharia chamada Scherbius & Ritter. Com a tarefa de substituir os sistemas criptográficos fracassados anteriormente, Scherbius desenvolveu uma máquina criptográfica. A "Enigma", como era chamada, era considerada uma versão elétrica do disco de cifras de Alberti, entretanto, com o quesito de ser muito mais complexa. Tal invenção, de acordo com Singh (2008, p. 146) "se tornaria o mais terrível sistema de cifragem da história" da criptografia.

A Enigma era formada por basicamente três elementos, a saber: um teclado para a entrada das letras do texto original, um misturador, que servia para cifrar as letras; e um mostrador, que era composto por varias lâmpadas, para identificar as letras cifradas. A Figura 29 é uma ilustração simplificada do esquema que constituía a Enigma.

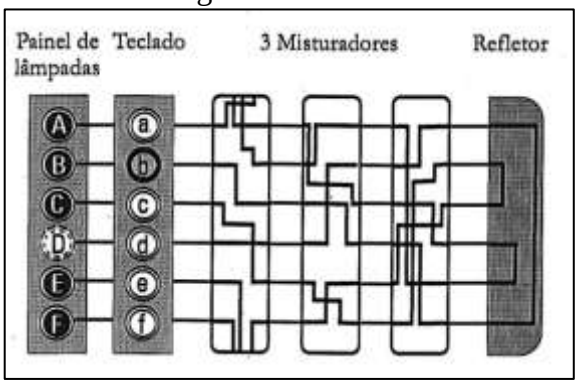
Figura 29 - Versão simplificada da máquina Enigma.



Fonte: Singh (2008, p. 148).

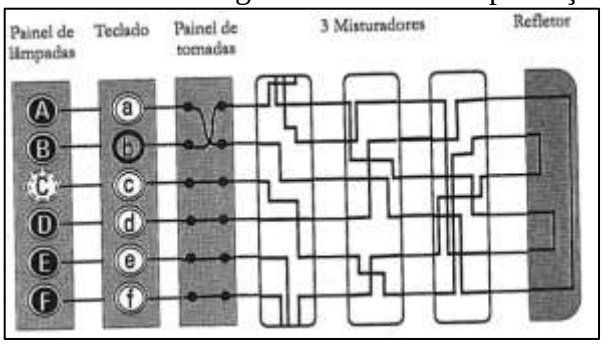
Tentando sempre aperfeiçoar sua invenção, para que cada vez mais a Enigma se tornasse uma máquina extremamente eficaz na segurança do sigilo, sua composição foi cada vez mais elaborada, resultando em máquinas muito mais complexas. A inserção de dois misturadores e de um refletor aumentou consideravelmente o potencial da Enigma (Figura 7). No entanto, os aperfeiçoamentos não pararam por aí, Scherbius ainda acrescentou mais duas características à máquina. Primeiro, ele fez com que os misturadores pudessem ser removidos e trocados de posição. Em segundo lugar, ele introduziu um painel de tomadas entre o teclado e o primeiro misturador. As Figuras 30 e 31, a seguir, representam um esquema da máquina com todas as sofisticações realizadas.

Figura 30 - Versão da Enigma com três misturadores e um refletor.



Fonte: Singh (2008, p. 151).

Figura 31 - Versão da Enigma com todos os aperfeiçoamentos.



Fonte: Singh (2008, p. 154).

Em 1918, a Enigma foi patenteada pelo seu inventor. A máquina de cifragem vinha dentro de uma caixa compacta e, embora não fosse uma máquina muito grande (34x28x15 cm), pesava aproximadamente 12 quilos. A Figura 32 apresenta uma Enigma pronta para uso e a Figura 33, uma Enigma com a tampa interna aberta.

Figura 32 - Uma máquina Enigma pronta para uso.

Fonte: Google Imagens (2015) [37].

[37] Disponível em: <https://pt.wikipedia.org/wiki/Enigma_(m%C3%A1quina)>. Acessado em: 11/06/2015.

Figura 33 - Uma máquina Enigma com sua tampa interna aberta.

Fonte: Google Imagens (2015) [38].

Tentando não repetir os erros cometidos durante a Primeira Guerra Mundial, os alemães viram na Enigma a melhor forma de cifragem. Assim, em 1925, Scherbius iniciou a produção em massa desse equipamento. As máquinas Enigma passaram a ser muito utilizadas pelos militares. Nas duas décadas seguintes, os alemães compraram 30 mil máquinas Enigma, e, segundo Singh (2008, p. 161), "a invenção de Scherbius deu aos alemães o sistema mais seguro de criptografia do mundo". Com essa tecnologia em mãos, os alemães entraram na Segunda Guerra Mundial acreditando que suas comunicações eram altamente seguras. Entretanto, ao mesmo tempo em que a Enigma parecia desenvolver um papel fundamental na vitória nazista, ela acabou sendo uma das personagens principais de sua queda.

Em 1926, a Enigma havia entrado em ação, deixando qualquer criptoanalista desorientado em relação à decifração das mensagens cifradas por ela. Britânicos, americanos e franceses fracassaram na tentativa de quebrar a Enigma. Contudo, o primeiro passo em direção à quebra do segredo da Enigma veio de um alemão. Hans-Thilo Schmidt obteve alguns insucessos em suas vidas social, militar e pessoal. Depois de seu fracasso na carreira militar, Hans-Thilo tentou tornar-se um homem de negócios, mas, em um determinado momento, ele precisou fechar sua fábrica de sabão. Sem mais recursos e vivendo na pobreza, Hans-Thilo se sentiu obrigado a pedir ajuda a seu irmão Rudolph, que era chefe do Estado-maior do Corpo de Sinaleiros. Ele era o responsável por garantir as comunicações seguras e foi ele próprio que oficialmente aprovou o uso da máquina Enigma pelo exército.

[38] Disponível em: <https://pt.wikipedia.org/wiki/Enigma_(m%C3%A1quina)>. Acessado em: 11/06/2015.

Tentando ajudar seu irmão, Rudolph o empregou em Chiffrierstelle, Berlim, um escritório encarregado da administração das comunicações cifradas da Alemanha. Esse escritório era considerado o centro de controle da Enigma e era altamente secreto. Ao assumir o emprego, Hans-Thilo precisou deixar a família e passou a viver isolado em Berlim; em um determinado momento, ele se voltou contra a sua pátria e começou a vender informações sobre o segredo da Enigma para os inimigos.

Com a traição de Hans-Thilo, os aliados poderiam recriar a máquina Enigma utilizada pelos militares alemães. Entretanto, isso não dava a eles o poder de decifrar, visto que era preciso saber sobre o ajuste inicial ao qual a máquina havia sido programada. O serviço secreto francês obteve, então, uma réplica da máquina Enigma, mas ainda era necessário saber sobre as informações da chave utilizada para a cifragem. Os criptoanalistas franceses não conseguiram desenvolver análises consistentes, deixando para os poloneses esse serviço árduo.

O ataque mais fascinante contra a Enigma foi realizado pelo polonês Marian Rejewski. Suas descobertas foram uma das maiores realizações na história da criptoanálise. Rejewski criou uma adaptação da Enigma. As chamadas *bombas* eram máquinas que verificavam cada um dos ajustes da Enigma para uma determinada mensagem. Durante boa parte da década de 1930, Rejewski e seus colegas trabalharam constantemente na descoberta das chaves. No entanto, em 1938 seus esforços foram barrados. Os alemães haviam modificado a Enigma, aumentando a sua segurança com a inserção de mais dois misturadores. Assim, o arranjo dos misturadores poderia, agora, conter quaisquer três dos cinco misturadores disponíveis.

Para dar conta dos novos arranjos, Rejewski precisava construir um número muito grande de novas bombas, o que acabou sendo inviável, em virtude dos custos altíssimos. Sem poder mais dar continuidade às pesquisas, os poloneses apresentaram aos franceses e aos britânicos todo o trabalho de Rejewski, e o desafio de prosseguir o trabalho de decifração da Enigma foi entregue a eles.

Depois de ter conhecimento sobre os avanços de Rejewski, a Inglaterra começou a recrutar estudantes universitários. Esses estudantes eram levados para Bletchley Park[39], em Buckinghamshire, onde ficava a sede da Escola de Cifras e Códigos do Governo (GC&CS). No ano de 1939, os cientistas e matemáticos de Bletchley Park já dominavam as técnicas polonesas de decifragem da Enigma. A constante evolução dessa máquina gerava nos criptoanalistas a frequente necessidade de inovar e retroprojetar as bombas. Era preciso

[39] Para mais informações acessar: <http://www.bletchleypark.org.uk/>.

permanentemente criar estratégias para a quebra da Enigma. Segundo Singh (2008, p. 186), o sucesso dos criptoanalistas de Bletchley Park se deveu à "combinação bizarra de matemáticos, cientistas, linguistas, especialistas na cultura clássica, mestres de xadrez e viciados em palavras cruzadas".

Foi no meio dessa combinação "bizarra" que um personagem em especial apareceu. Alan Turing começou a fazer parte de Bletchley Park no dia 4 de setembro de 1939. Ele passava parte de seu tempo se dedicando à quebra dos códigos e outra parte na sala de pesquisas teóricas de Bletchley. Turing iniciou um trabalho árduo estudando velhas mensagens decifradas. Ele acreditava que se podia prever uma parte da mensagem que ainda não havia sido decifrada apenas baseando-se no momento em que ela foi enviada e de onde. Assim, toda vez que se tivesse um texto cifrado e se conhecesse uma parte dele, ele acreditava ser capaz de decifrar a mensagem toda. Esse método ficou conhecido como *cola*.

Turing tinha certeza de que poderia utilizar as colas para decifrar a Enigma, e assim foi. Depois de estudar os trabalhos de Rejewski e de ter montado o seu próprio circuito elétrico com alguns aperfeiçoamentos, ele percebeu que a combinação das colas, elos e máquinas conectadas eletricamente o levaria à criação de uma máquina de decifração poderosa, chamada *bombas* (em homenagem aos trabalhos de Rejewski). Bletchley foi capaz de financiar as ideias de Turing para poder transformá-las em realidade. Em 1940, Alan Turing finalizou o projeto das bombas e, no mesmo ano, o protótipo da primeira bomba, batizada de *Victory*, chegou a Bletchley.

Victory entrou em ação imediatamente, mas seus resultados não foram satisfatórios. A máquina demorava muito tempo para encontrar as chaves e essa lentidão fez com que Turing aperfeiçoasse o projeto e, depois de quatro meses, a bomba *Agnus Dei*, ou somente *Agnes*, já funcionava da maneira esperada. Depois de dezoito meses, havia quinze bombas funcionando freneticamente, todas elas em busca das chaves da Enigma. No final de 1942, quarenta e nove bombas trabalhavam constantemente e uma nova estação de bombas foi inaugurada em Gayhurst Manor, logo ao norte de Bletchley. Todas essas bombas só se tornaram realidade graças a todo um investimento nesse projeto e a Alan Turing, que foi o grande responsável por encontrar a fraqueza da Enigma e de quebrar a sua cifra, mesmo sob as circunstâncias mais difíceis.

Além das bombas de Turing, os britânicos também inventaram outra máquina de decifragem, a *Colossus*. Ela foi desenvolvida para combater a cifra de *Lorenz*, uma cifra ainda mais poderosa utilizada na segunda metade do século XX. De acordo com Singh (2008, p. 267), essa cifra era utilizada para "codificar a comunicação entre Hitler e seus generais". A

Lorenz SZ40 funcionava de modo muito semelhante à Enigma, entretanto, ela era muito mais difícil de ser quebrada. Mas, mesmo sendo ela uma cifra mais complicada, os criptoanalistas de Bletchley não decepcionaram a Inglaterra e conseguiram realizar a decifração da mesma.

John Tilman e Bill Tutte foram os dois analistas de Bletchley que descobriram uma fraqueza no modo de cifração de Lorenz. Com esse feito, os britânicos tiveram com facilidade as mensagens de Hitler para com seus generais. Singh (2008, p. 267) argumenta que "a quebra da cifra de Lorenz exigia uma mistura de pesquisa, combinação, análise estatística e um julgamento cuidadoso, coisas que estavam além da capacidade técnica das bombas". As bombas davam conta de situações específicas, sendo operadas em alta velocidade, entretanto, não eram muito flexíveis para lidar com as sutilezas da Lorenz.

A Colossus chegou a Bletchley no dia 8 de dezembro de 1943 e era composta por 1.500 válvulas elétricas. Sendo uma máquina totalmente programável, a Colossus teria sido considerada a precursora do moderno computador digital. Mas, infelizmente, após o fim da Segunda Guerra Mundial, esta máquina foi destruída, bem como Bletchley e todo o material de pesquisa que se encontrava nela. Seus funcionários foram proibidos de falarem sobre Bletchley e as plantas de Colossus foram queimadas em caldeiras. Com essa infeliz ação, todas as informações para o primeiro computador moderno foram perdidas e restou a outros cientistas, alguns anos mais tarde, recriarem o computador[40].

O surgimento dos computadores programáveis ajudou os criptoanalistas a desenvolverem e a quebrarem todos os tipos de cifras. Eles usufruíam da velocidade e da flexibilidade desses computadores para pesquisar todas as chaves possíveis até encontrar a correta. Na contramão, os criptógrafos também começaram a explorar os computadores para a criação de cifras mais eficientes. Entretanto, somente aqueles que possuíam os computadores, o que, nos primeiros dias, significava os governos e seus militares, é que podiam explorar a cifração de mensagens por essa máquina[41]. Contudo, depois de alguns anos, essa invenção se tornou comercial, possibilitando a compra e manutenção dos computadores por empresas.

Com o passar do tempo, as empresas estavam cada vez mais munidas de computadores e a cifragem entre elas difundida. Com isso, era preciso padronizar um tipo de cifragem para que as ações entre elas (transferências de dinheiro e negociações comerciais) pudessem ser

[40] Isso ocorreu em 1945, quando J. Presper Eckert e John W. Mauchyl criaram o ENIAC (Electronic Numerical Integrator and Calculator). Essa máquina era composta por 18 mil válvulas eletrônicas que operavam cinco mil cálculos por segundo. Durante muito tempo, o ENIAC foi considerado a mãe de todos os computadores.

[41] Em 1947, a AT&T Bell Laboratories substituiu as válvulas eletrônicas por transístores. Essa mudança barateou os custos do computador, e este se tornou comercial em 1951. Em 1953, a IBM lançou seu primeiro computador, e em 1957 introduziu a linguagem Fortran. Em 1959 houve a invenção do circuito integrado e, em 1960, os computadores já se encontravam mais poderosos e ao mesmo tempo mais baratos.

totalmente eficientes e seguras. Em 1973, o National Bureau of Standards (EUA) pressionou para a criação de um sistema padrão para garantir as comunicações secretas entre empresas. Em resposta, uma cifra da IBM, conhecida como *Lucifer*, foi lançada como sendo uma forte candidata para o padrão tão desejado. Entretanto, uma versão mais simples dessa cifra foi adotada. Em 1976, o DES (Data Encryption Standard) entrou em ação, resolvendo o problema das empresas. Contudo, as dificuldades não se resumiam a apenas padronizar as cifras, visto que agora seria preciso descobrir como as empresas iriam lidar com a *distribuição de chaves*.

O problema da distribuição de chaves era simples. Para que duas empresas pudessem trocar informações, cada uma teria que dispor da mesma cifra, ou seja, ambas teriam que ter em seus computadores cópias da DES, mas só isso não garantiria a decifração da mensagem. Por exemplo, imagine que a empresa C deseja enviar uma mensagem para a empresa D. A empresa C deverá escolher uma chave e usar a DES para criptografar sua mensagem. Assim, ao receber a mensagem criptografada, a empresa D deverá saber qual foi a chave utilizada por C na cifração da mensagem para, só depois, decifrá-la utilizando a DES. Agora, imagine como tais empresas trocariam as informações destas chaves? Eis aí o problema da distribuição de chaves.

O problema da distribuição de chaves e o surgimento de Alice, Bob e Eva

O problema da distribuição de chaves está presente em toda a história da criptografia. Enquanto a necessidade de se ocultar mensagens era apenas dos governantes e militares, esse problema era parcialmente resolvido. Como muitas vezes essas distribuições eram realizadas por uma terceira pessoa, grandes investimentos eram feitos para garantir a segurança desses transmissores. Contudo, com a comercialização dos computadores e a difusão das cifras entre as empresas civis, era necessário desenvolver um meio de distribuição de chaves que não dependesse de terceiros e, muito menos, de altos custos.

É nesse momento da história, com esse exato problema – aparentemente insolúvel –, que surgiram dois dos maiores nomes da história da criptografia: Whitfield Diffie e Martin Hellman. Ambos eram fascinados pela arte das cifras e suas carreiras acadêmicas foram marcadas por várias pesquisas dentro desse ramo. Em 1974, Diffie foi convidado a dar uma palestra no laboratório Thomas J. Watson, da IBM. Ao final de sua apresentação, Alan Konheim, um dos principais especialistas em criptografia da IBM, mencionou para Diffie que, pouco tempo antes, outro pesquisador também havia palestrado sobre a questão da

distribuição de chaves. Seu nome era Martin Hellman e, naquele mesmo dia, Diffie viajou cinco mil quilômetros para encontrar a única pessoa que parecia compartilhar de sua obsessão. Em setembro de 1974, Diffie e Helmman se encontraram e nascia, naquele momento, uma das parcerias mais importantes e ativas da criptografia.

Diffie foi contratado por Hellman como estudante de graduação. Por falta de investimentos em suas pesquisas, ele não pôde empregar seu amigo como um pesquisador, mas isso não foi um problema para Diffie. Ralph Merkle acabou se juntando mais tarde aos dois e, assim, os três iniciaram uma grande empreitada para solucionar o problema da distribuição de chaves. Eles precisavam encontrar um jeito de partilhar o segredo da chave antes que uma mensagem cifrada pudesse ser compartilhada.

É nesse cenário que aparecem os nomes de Alice, Bob e Eva. Três personagens fictícios que se tornaram um padrão nos debates sobre criptografia. Para exemplificar a situação de troca de chaves, vamos pensar no seguinte caso. Suponhamos que Alice deseja enviar uma mensagem para Bob, ou o contrário, e Eva é uma interceptadora inimiga. Toda vez que Alice desejar enviar uma mensagem para Bob, ela terá que cifrar suas mensagens, cada vez com chaves diferentes, para aumentar a segurança. Para que Bob possa ler o conteúdo das mensagens, ele necessita das informações das chaves. Logo, Alice precisa enviar as chaves para Bob. No entanto, Eva está atenta à troca de informações entre eles. Para resolver esse impasse, Alice e Bob poderiam se encontrar e trocar as informações das chaves pessoalmente. Entretanto, embora essa solução seja segura, ela é inviável em termos maiores de comunicações. Sem a chave, Eva é incapaz de decifrar a mensagem interceptada, entretanto, se ela obtiver o conhecimento da chave, o sistema de cifragem se tornará inútil.

Essa situação entre Alice, Bob e Eva pode ser ilustrada por outro cenário. Imaginemos que Alice e Bob não possam se encontrar para realizarem a troca de chaves, sendo obrigados e se comunicarem pelos correios. Suponhamos, agora, que eles vivem em um país em que o sistema de correios é inseguro. Como Alice e Bob poderiam trocar informações nessa situação? A utilização de um sistema de cadeados é uma solução perfeita para esse impasse e é conhecida como sistema simétrico de chave pública. Digamos que Alice deseja enviar uma mensagem para Bob. Ela coloca essa mensagem em uma caixa e a tranca com um cadeado, do qual a chave pertença somente a ela. Essa caixa é enviada para Bob que, por sua vez, não consegue abrir a caixa, já que ele não possui a chave de Alice. Bob então coloca outro cadeado na caixa, do qual somente ele tenha a chave, e a envia de volta para Alice. Alice retira seu cadeado, mas a caixa continua fechada com o cadeado de Bob. Alice envia

novamente a caixa para Bob, que, por fim, consegue abri-la e ler a mensagem enviada por Alice.

Com essa ilustração, fica claro que é possível trocar mensagens secretas em segurança sem necessariamente realizar a troca de chaves. Contudo, quando se tentou ajustar esse cenário em termos de cifragem, observou-se que a ordem das cifrações e decifrações era crucial e deveria obedecer a um esquema: o último estágio da cifragem deveria ser o primeiro a ser decifrado. Embora o modelo dos cadeados não funcionasse no mundo real da criptografia, ele inspirou Diffie e Hellman a investigarem uma estratégia prática para tentar solucionar o problema da distribuição de chaves.

Eles começaram a pesquisar sobre as *funções* matemáticas. A maioria delas é classificada como funções de mão dupla. Em termos criptográficos, isso significa que a decifragem seria exatamente o processo inverso da própria cifragem. Entretanto, Diffie e Hellman não estavam interessados nesses tipos de funções. Suas pesquisas se concentraram nas funções de mão única, aquelas que, embora sejam fáceis de se aplicar, são extremamente difíceis, ou impossíveis de se desfazer. Os dois criptógrafos encontraram na aritmética modular um campo matemático cheio de funções de mão única.

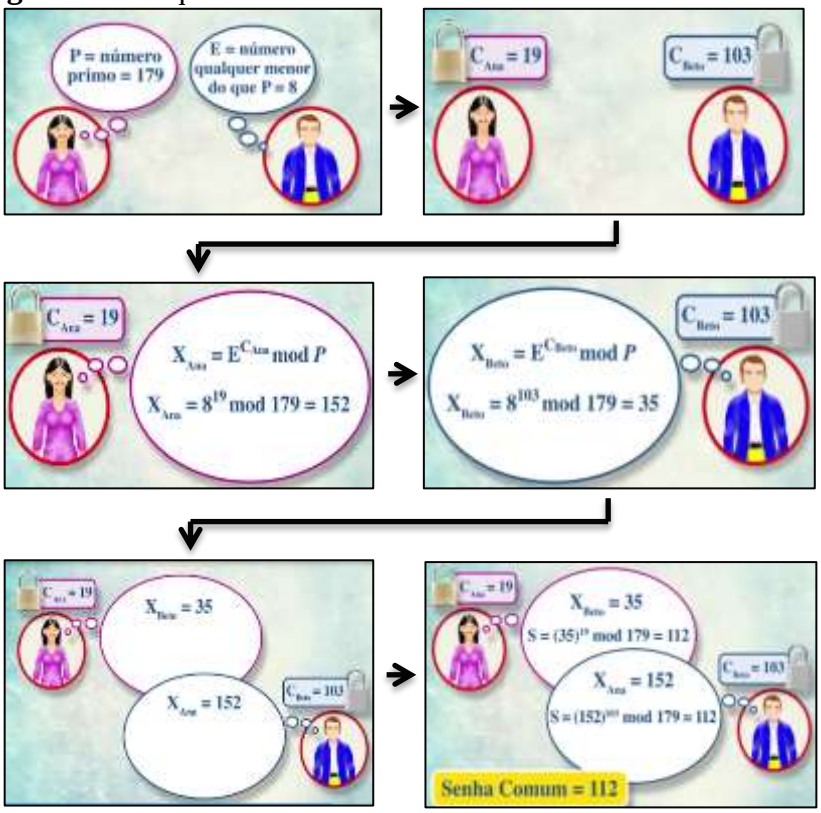
Depois de estudarem por dois anos a aritmética modular e as funções de mão única, Hellman encontrou a solução tão esperada. Na primavera de 1976, ele apresentou a Diffie e a Merkle sua grande ideia: uma função de mão única da forma $Y^X\ (mod\ P)$. O esquema para a troca de chaves de Diffie-Hellman-Merkle, como ficou conhecido, permitia que Alice e Bob trocassem informações seguras sem a necessidade de trocarem as chaves. Conforme afirma Singh (2008, p. 292), "esta é uma das descobertas mais racionais da história da ciência e forçou todo o estabelecimento criptográfico a reescrever suas regras". Na Figura 34, segue uma exemplificação sobre esse esquema.

Apesar de o esquema de troca de chaves de Diffie-Hellman-Merkle apresentar uma solução para o problema da distribuição de chaves, ele não era perfeito. Imaginemos agora que Alice morasse no Brasil e Bob no Japão. Para que o esquema funcionasse de forma rápida, era necessário que ambos estivessem, simultaneamente, conectados por uma rede. No entanto, eles poderiam utilizar *e-mails* como alternativa para desenvolver o esquema, mas essa opção afetaria a agilidade dos *e-mails*. Desse modo, o esquema ainda não era totalmente perfeito e, assim, o problema da distribuição de chaves ainda não havia sido totalmente resolvido.

Diffie foi quem idealizou uma nova forma de se criptografar. Ele foi capaz de arquitetar a chamada *chave assimétrica*. No entanto, embora ele tivesse concebido essa ideia, não foi

capaz de apresentar um exemplo dela. O conceito de Diffie poderia ser resumido da seguinte maneira: Alice e Bob teriam em mãos dois tipos de chaves, a *chave particular* e a *chave pública*. Como os nomes já sugerem, as chaves particulares de Alice e Bob pertenceriam somente a eles e as chaves públicas poderiam ser do conhecimento de qualquer pessoa, inclusive de Eva, a inimiga.

Figura 34 - Esquema da troca de chave de Diffie-Hellman-Merkle.



Fonte: Recortes do vídeo "Criptografia, Chave privada e Chave pública" (2012)[42].

Criação da RSA

Três pesquisadores do Laboratório de Ciência de Computação do MIT[43], nos Estados Unidos, entraram para a história da criptografia com a criação de um sistema de cifras conhecido como RSA, o sistema mais influente na criptografia moderna. Cada letra da sigla corresponde ao sobrenome de seus criadores, a saber, Ron Rivest e Adi Shamir, que eram cientistas de computação, e Leonard Adleman, que era um matemático. Enquanto Rivest e Shamir criavam algoritmos de cifração, Adleman era o responsável por verificar suas possíveis falhas e por conduzir seus amigos nas explorações matemáticas.

[42] Vídeo disponível em: <https://www.youtube.com/watch?v=pEfEgCEKcJ0>. Data de acesso: 19/02/16.
[43] Massachusetts Institute of Technology.

Em abril de 1977, os três amigos passaram a Páscoa juntos, sendo que naquela noite Rivest teria tido um grande *insight*. Ele havia passado a noite toda escrevendo sobre sua descoberta e, na manhã seguinte, entregou para seus companheiros tudo o que havia produzido. Como de costume, Adleman analisou todo o trabalho de Rivest, refazendo-o diversas vezes em busca de falhas, chegando à conclusão de que os estudos de Rivest estavam impecáveis. Nascia, naquele momento, a famosa criptografia RSA, um sistema assimétrico também conhecido como *criptografia de chave pública*.

A existência da RSA foi anunciada pela primeira vez por Martin Gardner, em agosto de 1977. Gardner escreveu um artigo em sua coluna "Jogos Matemáticos", da Scientific American, explicando como a criptografia de chave pública funcionava, e deixou para seus leitores alguns desafios relacionados a ela. A RSA é baseada em uma função modular da forma $C = M^e (mod\ N)$[44], na qual a sua principal segurança está ligada ao valor de *N*, que é o resultado do produto entre dois números primos. A dificuldade de se fatorar *N*, quando este é extremamente grande, é o grande empecilho para a quebra dessa cifra. De fato, para os matemáticos, fatorar sempre foi uma tarefa muito árdua. Desse modo, a RSA, além de acabar com os problemas associados às cifras tradicionais e abolir o problema da distribuição de chaves, oferece, até os dias de hoje, um conforto aos criptógrafos em termos de sua segurança. Atualmente existem vários outros códigos de chave pública, mas o RSA é o mais utilizado em aplicações comerciais.

Hoje em dia, além de a criptografia ser uma parte essencial do mundo virtual, cada dia mais ela vem sendo tema de filmes e seriados de televisão. Inserida em algumas teledramaturgias, a criptografia começou a ganhar mais espaço na literatura, entretanto sua popularização pode ser traçada desde o século XIX.

A popularização da criptografia

A criptografia acabou-se tornando popular durante a segunda metade do século XIX, o mesmo período no qual a evolução das cifras encontrava-se estagnada. O crescente fascínio do público pelas cifras pôde ser notado pela grande utilização das mesmas pelos civis e, posteriormente, em sua repercussão na literatura. Os jovens apaixonados da Inglaterra, proibidos de expressarem seu amor publicamente, utilizavam as colunas dos jornais para

[44] As letras da fórmula $C = M^e (mod\ N)$ representam: *C* = texto cifrado; *M* = mensagem convertida, por exemplo, em ASCII ou em DES; *e* = um número qualquer público; *N* = o produto de dois números primos. Os valores de *e* e *N* formam, juntos, a chave pública. Para mais informações sobre a Criptografia RSA, ver em Sousa (2013).

cifrarem suas declarações. Depois de um tempo, a utilização dos jornais para essas circunstâncias acabou se tornando corriqueira e as mensagens cifradas nesses jornais acabaram sendo apelidadas de "colunas de óbitos". Os próprios jornais passaram a utilizar as cifras como passatempo para seus leitores, motivando-os a decifrarem suas mensagens secretas.

Não demorou muito para que as cifras repercutissem entre a população e chamassem a atenção de escritores, como, por exemplo, Júlio Verne. Esse autor escreveu o romance *Viagem ao centro da terra*, no qual narra uma viagem que depende fortemente na decifração de um pergaminho. Em 1885, Verne também utilizou as cifras como elemento fundamental em seu romance *Mathias Sandorff*. Outro autor conhecido mundialmente é o britânico Sir Arthur Conan Doyle, criador do personagem de ficção Sherlock Holmes. Doyle criou um dos maiores especialistas em criptografia da literatura. Holmes era um detetive com um conjunto de hábitos e habilidades muito peculiares. Em suas diversas histórias, Holmes investiga os casos apresentados a ele e, com uma perspicácia incrível, resolve todos eles, sem grandes dificuldades. No conto *Aventura dos dançarinos*[45], é possível entender a maneira como Holmes realizada a decifração das mensagens.

O escritor Edgar Allan Poe também faz parte dos autores que dedicaram algumas de suas obras a narrar contos envolvendo a criptografia. Em 1843, Poe publicou o conto *O besouro dourado*, o qual contava a história de um homem que encontra um besouro incomum e com ele decifra o local de um tesouro enterrado há muito tempo. Embora esse conto seja fictício, existiu uma história real muito parecida, ou seja, o caso de cifra de Beale envolveu um *cowboy* e uma aventura no Velho Oeste[46]. Em alguns romances, como *O nome da Rosa* (1980) e *O Pêndulo de Foucault* (1988), de Umberto Eco, também pode-se encontrar a criptografia sendo utilizada. Em histórias mais mirabolantes, encontra-se os escritores Carl Sagan, autor de *Contato* (1985), Michel Crichton, escritor de *Esfera* (1987), e Neal Stephenson, criador do *Cryptonomicon* (1999).

O cinema também aderiu à utilização da criptografia em suas tramas. Algumas próximas à realidade e outras nem tanto, como é o caso dos filmes *Quebra de Sigilo* (1992), de Robert Redford, *Código para o inferno* (1998), de Ryne Douglas Pearson, e *A Senha* (2001), de Dominic Sena. Já os filmes que trazem um pouco sobre a história são: *Enigma* (2001), de Michel Apted, *Breaking The Code* (1987), de Hugh Whitemore, *U-571* (2000), de Jonathan Mostow, *Uma Mente Brilhante* (2001), de Ron Howard, e o mais atual, *O Jogo da Imitação*

[45] Para ler esse conto basta acessar: < https://mundosherlock.wordpress.com/arthur-conan-doyle/>.
[46] Para mais informações sobre essa história, ler Singh (2008, p. 100-118).

(2015), de Morten Tyldum. Também existem os filmes que retratam as aventuras do mais famoso personagem de Sir Arthur Conan Doyle, como os recentes *Sherlock Holmes* (2009) e *Sherlock Holmes – O Jogo das Sombras* (2011), ambos de Guy Ritchie.

As emissoras de canais fechados também não ficaram para trás. Diversos seriados foram criados a fim de abordar a criptografia e mostrar sua importância nos dias de hoje. O seriado *Da Vinci Demons* (2013) narra, de modo fictício, a história de Leonardo da Vinci e como os códigos e a arte da mensagem secreta influenciaram sua vida pessoal e social. O seriado *Inteliigence US* (2014) aborda como as agências secretas lidam com a criação das cifras e como as suas descobertas influenciam o curso das decisões diplomáticas. *White Collar* (2010) mostra constantemente situações em que os criminosos utilizam a criptografia para manter suas ações confidenciais, além de apresentar uma temporada inteira sobre a máquina Enigma. Os seriados *Elementary* (2012) e *Sherlock* (2010) são produções baseadas nos contos de Sir Arthur Conan Doyle e o mais novo seriado apresentado nos canais fechados se chama *CSI: Cyber* (2015), o qual, constituindo-se em uma divisão de crimes cibernéticos do FBI, apresenta investigações que fala sobre a criptografia e a criptoanálise dentro do ciberespaço.