UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Campus de Presidente Prudente
Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT)

Criptografia como Recurso Didático: Uma Proposta Metodológica aos Professores de Matemática

Cintia Kohori Rosseto

Orientador
Prof. Dr. Suetônio de Almeida Meira

Presidente Prudente
2018

UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Campus de Presidente Prudente
Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT)

Criptografia como Recurso Didático: Uma Proposta Metodológica aos Professores de Matemática

Cintia Kohori Rosseto

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre, junto ao programa de Mestrado Profissional em Matemática em Rede Nacional da Faculdade de Ciências e Tecnologia da Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de Presidente Prudente.

Orientador
Prof. Dr. Suetônio de Almeida Meira

Presidente Prudente
2018

Rosseto, Cintia Kohori
Criptografia como recurso didático: uma proposta metodológica aos professores de matemática / Cintia Kohori Rosseto . -- São José do Rio Preto, 2018
84 f. : il.

Orientador: Suetônio de Almeida Meira
Dissertação (mestrado profissional) – Universidade Estadual Paulista “Júlio de Mesquita Filho”, Instituto de Biociências, Letras e Ciências Exatas

1. Matemática (Ensino médio) - Estudo e ensino. 2. Funções (Matemática) 3. Criptografia. 4. Aprendizagem. 5. Prática de ensino. 6. Matemática - Metodologia. I. Universidade Estadual Paulista "Júlio de Mesquita Filho". Instituto de Biociências, Letras e Ciências Exatas. II. Título.

CDU – 51(07)

Ficha catalográfica elaborada pela Biblioteca do IBILCE
UNESP - Câmpus de São José do Rio Preto

TERMO DE APROVAÇÃO

Cintia Kohori Rosseto

Criptografia como Recurso Didático: Uma Proposta Metodológica aos Professores de Matemática

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional da Faculdade de Ciências e Tecnologia da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Prof. Dr. Suetônio de Almeida Meira
FCT/UNESP - Campus de Presidente Prudente
Orientador

Prof. Dr. José Roberto Nogueira
FCT/UNESP - Presidente Prudente

Profª. Drª. Dayene Miralha de Carvalho Sano
Universidade do Oeste Paulista - UNOESTE

Presidente Prudente, 26 de janeiro de 2018

Dedico este trabalho ao meu marido Douglas, pela compreensão, incentivo e apoio ao longo desta jornada.

Agradecimentos

À Deus, por me proporcionar forças nas horas de desânimo.

Ao meu marido, por ser meu companheiro em todos os momentos.

Aos familiares e amigos, em especial ao meu pai, fonte de inspiração, que sempre me apoiou e incentivou.

A todos os professores do programa PROFMAT da UNESP de Presidente Prudente, em especial ao meu orientador Prof. Dr. Suetônio de Almeida Meira, pelos ensinamentos, disposição e paciência, e ao Prof. Dr. Marco Antônio Piteri, pelos conselhos e incentivo.

Aos amigos da turma do PROFMAT, pela parceria e colaboração ao longo desses 3 anos.

À CAPES e SBM pelo apoio financeiro e oportunidade de estudo e crescimento.

À todos que, de alguma forma, contribuíram para realização deste trabalho.

A mente que se abre a uma nova ideia
jamais voltará ao seu tamanho original.
Albert Einstein

Resumo

A criptografia tem como objetivo básico, transmitir uma mensagem a um destinatário sem que outra pessoa possa conhecer seu conteúdo, para que isso ocorra usa como ferramenta os recursos matemáticas. A preocupação com a privacidade e segurança é muito antiga, ao longo do tempo muitos códigos foram usados e utilizados principalmente para proteger segredos militares. Com o advento da comunicação eletrônica, muitas atividades essenciais passaram a depender do sigilo na troca de mensagens, principalmente aquelas que envolvem transações financeiras e uso seguro da internet. O presente trabalho trata a Criptografia como ferramenta de ensino nas aulas de Matemática, tendo em vista que o ensino da matemática está cada vez mais comprometido, principalmente por conta do desinteresse dos alunos e da grande defasagem com a qual chegam no Ensino Fundamental II. Diante disto, propomos a utilização de temas que tragam significado à aprendizagem e cativem o aluno. A criptografia pode ser abordada em vários conteúdos do Ensino Fundamental e Médio, como funções e matrizes, assuntos abordados no presente trabalho. Pretendemos, com a utilização da Criptografia no ensino dos conteúdos matemáticos, proporcionar sentido prático ao conteúdo estudado de forma que a aprendizagem se torne significativa para o aluno. Apresentaremos alguns modelos de atividades que abordam o tema criptografia e poderão ser aplicados no Ensino Fundamental e no Ensino Médio.

Palavras-chave: Criptografia, Funções, Aprendizagem.

Abstract

Encryption has the basic purpose of transmitting a message to a recipient without anyone else being able to know its contents, so that this occurs using the mathematical resources as a tool. The concern with privacy and security is very old, over time many codes have been used and used mainly to protect military secrets. With the advent of electronic communication, many essential activities depend on secrecy in the exchange of messages, especially those involving financial transactions and safe use of the internet. The present work treats Cryptography as a teaching tool in Mathematics classes, considering that the teaching of mathematics is increasingly compromised, mainly due to the lack of interest of the students and the large gap with which they arrive in Elementary School II. In view of this, we propose the use of themes that bring meaning to learning and captivate the student. The cryptography can be approached in several contents of Elementary and Middle School, like functions and matrices, subjects approached in the present work. We intend, with the use of Cryptography in the teaching of mathematical contents, to provide meaning practice to the content studied so that learning becomes meaningful for the student.We will present some models of activities that approach the subject of encryption and database is not Elementary and High School.

Keywords: Cryptography, Functions, Learning.

Lista de Figuras

Sumário

1 Introdução

Um dos desafios encontrados pelos professores de Matemática é fazer com que os alunos não só aprendam os conteúdos, mas se interessem pela disciplina. Cria-se, desde os anos iniciais, um estigma de que a Matemática é difícil, além disso, muitas vezes os conteúdos são simplesmente "jogados".

Muitos alunos chegam ao Ensino Fundamental II com defasagem, desinteresse e bloqueio em aprender Matemática. Ao questionarmos sobre a importância da disciplina, todos afirmam que esta é importante no nosso dia a dia, mas ainda assim não se interessam em aprendê-la, dizem que é difícil e que só gostam dos assuntos que entendem. Embora o aluno reconheça a importância em aprender matemática, não vêem sentido em aprendê-la, pois os exemplos dados não condizem com sua realidade.

O PCN de matemática sugere "alguns caminhos para fazer Matemática na sala de aula", entre eles está a história da matemática, e foi a partir da história que este trabalho se desenvolveu.

> (...) o ensino de Matemática prestará sua contribuição à medida que forem exploradas metodologias que priorizem a criação de estratégias, a comprovação, a justificativa, a argumentação, o espírito crítico, e favoreçam a criatividade, o trabalho coletivo, a iniciativa pessoal e a autonomia advinda do desenvolvimento da confiança na própria capacidade de conhecer e enfrentar desafios.(PCN, 1997, pag. 31)

Partindo do princípio que a Matemática se torna interessante para a aprendizagem quando praticada de forma integrada e relacionada a outros conhecimentos, abordando assuntos de interesse do aluno, elaboramos este trabalho, onde o tema Criptografia é apresentado como gerador de atividades didáticas, permitindo o aprofundamento dos conteúdos desenvolvidos nas aulas de Matemática de maneira que o aluno se sinta estimulado, desencadeando um processo de construção de novos conhecimentos.

No ano de 2016, em comemoração ao Dia Nacional da Matemática (06 de maio), resolvemos presentear os alunos dos nonos anos da Escola Municipal de Lucélia-SP com um filme, visto que uma das reclamações dos alunos é a ausência de filmes nas aulas de Matemática. Foi exibido o filme O Jogo da Imitação (2014) que foi baseado na vida do matemático inglês Alan Turing (1912 - 1954) e retrata sua contribuição

no campo da Criptoanálise e consequentemente, importância para o fim da Segunda Guerra Mundial (1939 - 1945).

Alguns alunos demonstraram interesse no tema Criptografia, pesquisaram sobre o assunto e então elaboramos um trabalho que foi apresentado no IX Congresso de Iniciação Científica Junior, na cidade de Adamantina-SP. O trabalho foi bastante elogiado, proporcionando aos alunos o certificado de menção honrosa.

A criptografia, além de um assunto instigante, é muito abrangente, envolve diversos conteúdos tratados tanto no Ensino Fundamental quanto no Ensino Médio, assim pode ser utilizado como meio de atrair o aluno, tornando as aulas interessantes e significativas. Como disse Lima (2007, pag. 144) "A falta de aplicações para os temas estudados em classe é o defeito mais gritante do ensino da Matemática em todas as séries escolares."

Nos capítulos seguintes apresentamos o conceito de criptografia, um breve apanhado histórico, definimos conceitos básicos de funções, matrizes e teoria dos números, que serão base para o desenvolvimento das atividades propostas. Apresentamos também atividades que podem ser desenvolvidas no Ensino Fundamental e Médio, e os resultados obtidos no decorrer do desenvolvimento deste trabalho.

2 Criptografia

> Durante milhares de anos, reis, rainhas e generais dependeram de comunicações eficientes de modo a governar seus países e comandar seus exércitos. Ao mesmo tempo, todos estavam cientes das consequências de suas mensagens caírem em mãos erradas, revelando segredos preciosos a nações rivais ou divulgando informações vitais para forças inimigas. Foi a ameaça da interceptação pelo inimigo que motivou o desenvolvimento de códigos e cifras, técnicas para mascarar uma mensagem de modo que só o destinatário possa ler seu conteúdo. (Singh, Simon, 2004, pag. 11)

2.1 Conceito

A criptologia é a ciência que reúne as técnicas e os conhecimentos necessários para a ocultação de informações (criptografia) e a quebra das informações ocultas (criptoanálise). Existem duas maneiras diferentes de escrever uma informação, uma é ocultando a presença da mensagem (esteganografia) e a outra, ocultando apenas o sentido da mensagem (criptografia).

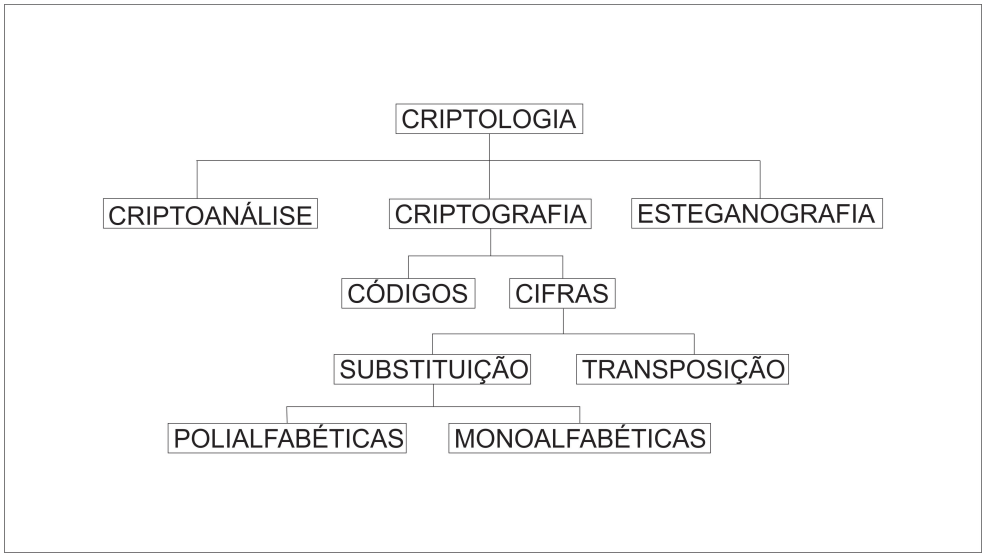


Figura 2.1: Organograma das divisões da Criptografia.

A criptoanálise é responsável por decifrar e ler as mensagens cifradas, sem ter acesso

a chave. Sua criação se deve ao aprimoramento dos conhecimentos em matemática, estatística e linguística.

> (...) além de empregar cifras, os estudiosos árabes foram capazes de quebrá-las. Eles inventaram a criptoanálise, a ciência que permite decifrar uma mensagem sem conhecer a chave. Enquanto o criptógrafo desenvolve métodos de escrita secreta, é o criptoanalista que luta para encontrar fraquezas nesses métodos, de modo a quebrar a mensagem secreta. Os criptoanalistas árabes tiveram sucesso na descoberta de um método para quebrar a cifra de substituição monoalfabética, uma cifra que tinha permanecido invulnerável durante vários séculos. (Singh, Simon, 2004, pag. 32)

A esteganografia é a arte de esconder uma mensagem ou informação, ocultando a sua existência. A palavra esteganografia é de origem grega, *steganos* significa coberto e *graphein*, significa escrever. Utiliza-se de vários métodos para comunicações secretas, como imagens, sons, vídeos, assinaturas digitais, tintas invisíveis, micropontos (forma de esteganografia usada durante a Segunda Guerra Mundial), canais escondidos, entre outros.

Já a criptografia não está preocupada em esconder a mensagem, mas sim, torná-la ininteligível, escondendo o significado da mensagem de maneira que somente aquele que obtiver a chave conseguirá ter acesso ao seu conteúdo. A palavra criptografia também tem origem grega, *kriptos* significa oculto e *graphos*, escrever. Podemos criptografar usando códigos ou cifras.

Os códigos são símbolos (palavras, letras, números, etc.) usados para representar uma informação. Por exemplo, código de barras, código binário, código morse.

As cifras são divididas em:

- **cifra de transposição:** as letras são rearranjadas, apenas trocam de posição (anagramas). Exemplo: Scytalae ou Bastão de Licurgo.

- **cifra de substituição:** Esse tipo de criptografia prevaleceu durante o primeiro milênio, devido a sua simplicidade e força. Nesse sistema cada letra é substituída por outra letra ou símbolo. Assim, cada letra do alfabeto original é trocado por uma letra do alfabeto cifrado, que pode ser qualquer rearranjo do alfabeto original. Existem dois métodos de substituição, monoalfabética e polialfabética.

2.2 História

A criptografia está presente em diversas situações do nosso dia a dia, com o advento da era digital tudo ao nosso redor passou a utilizar algum tipo de código para proteção, sejam os códigos de barras utilizados em supermercados até troca de mensagens.

A preocupação com a privacidade e segurança é muito antiga. Ao longo do tempo muitos códigos foram usados e utilizados principalmente para proteger segredos militares. Cerca de 1900 a.C. essa técnica já era uitilizada pelos egípicos.

Em uma vila egípcia, chamada Menet Khufu, próxima ao rio Nilo, foi encontrado o túmulo de Khnumhotep II, arquiteto do faraó Amenemhet II. No túmulo havia hieróglifos com algumas palavras ou trechos substituídos por outros. Estudiosos da criptografia acreditam que este é o primeiro exemplo documentado da escrita cifrada.

Apresentaremos um pouco da história da Criptografia com o propósito de mostrarmos sua importância ao longo da história da humanidade. Usamos como referência histórica os autores Simon Singh (O Livro dos Códigos) e Sérgio Pereira Couto (Códigos e Cifras).

2.2.1 Pedra de Roseta

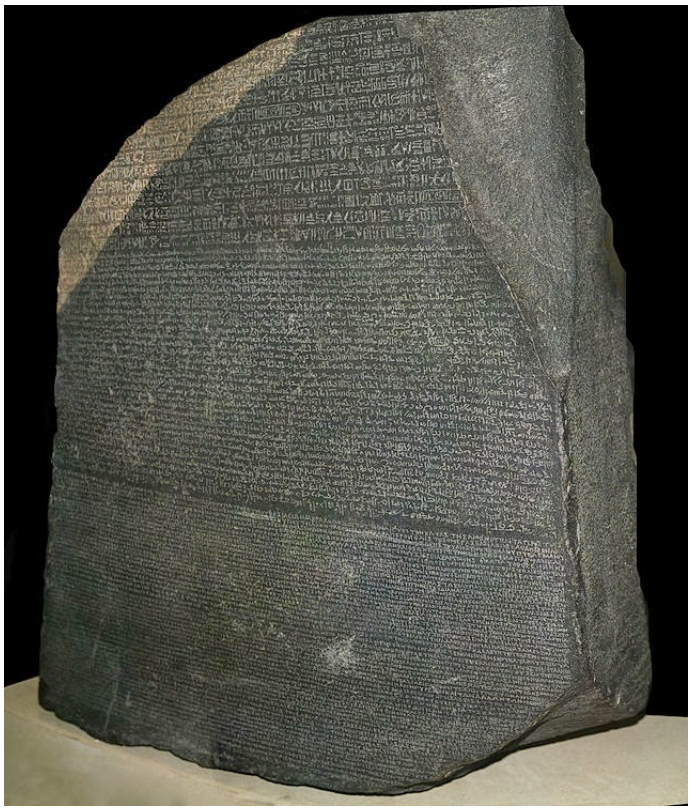


Figura 2.2: Pedra de Roseta.

Os hieróglifos são considerados a forma mais antiga de escrita, *hieros* significa sagrado e *glyphos*, escrita. Eram usados por sacerdotes, escribas, membros da realeza e funcionários de altos cargos.

A famosa Pedra de Rosetta, exposta no *British Museum*, trata-se de uma homenagem ao rei Ptolomeu V, é um fragmento de uma estela de granodiorito do Antigo Egito, encontrada próxima à cidade de El-Rashid, após a derrota de Napoleão para o

Reino Unido.

É de suma importância para a compreensão dos hieróglifos egípcios. Seu valor não está ligado ao conteúdo, mas ao modo como foi escrito. Foram usados três tipos de alfabetos: hieróglifo, demótico e grego, além de ter sido escrito em duas línguas.

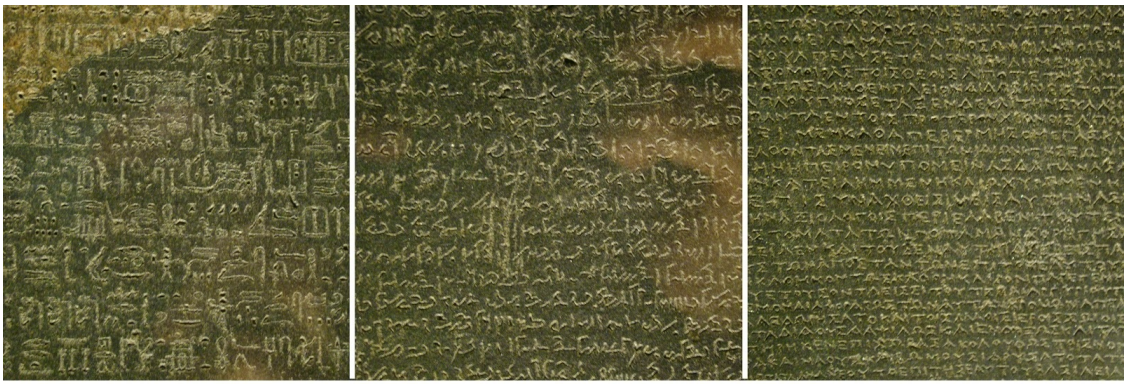


Figura 2.3: Pedra de Roseta - Detalhes.

Champollion, nascido na França em 1790, foi o responsável pela decifração definitiva da Pedra de Rosetta. Ele percebeu que o sistema egípcio empregava sinais que exprimiam ideias e alguns que representavam sons, ou seja, muitos hieróglifos possuíam um valor de efeito fonético.

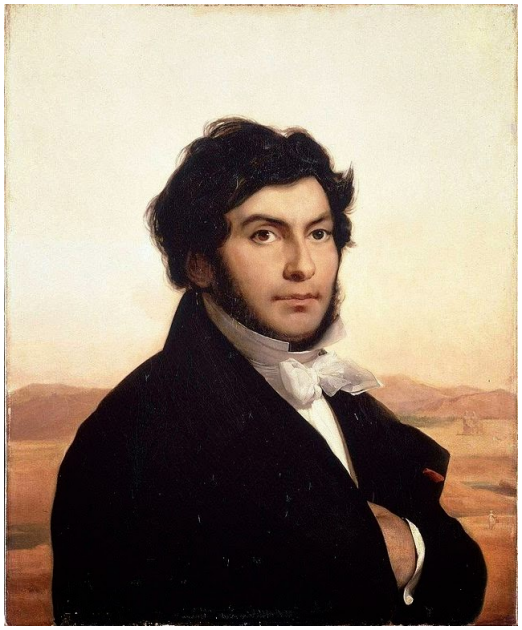


Figura 2.4: Jean-François Champollion.

2.2.2 Bastão de Licurgo

Scytalae ou Bastão de Licurgo era utilizado como meio de transmissão de mensagens criptografadas, embora alguns historiadores considerem o uso desse bastão pelos

espartanos como um mito.

Figura 2.5: Bastão de Licurgo.

Tal bastão era feito de madeira, havia ao seu redor uma tira de couro ou pergaminho, longa e estreita, que era amarrada firmemente. É a cifra de transposição mais antiga, conhecida como o primeiro dispositivo criptográfico militar, com origem no séc. V a.C.

Escrevia-se a mensagem no sentido do comprimento do bastão para, depois, o destinatário poder desenrolar a tira, que trazia letras embaralhadas. Quando o destinatário recebia a tira, enrolava-a num outro bastão com mesmo diâmetro do usado pelo remetente, e assim podia ler a mensagem.

2.2.3 Cifra de César

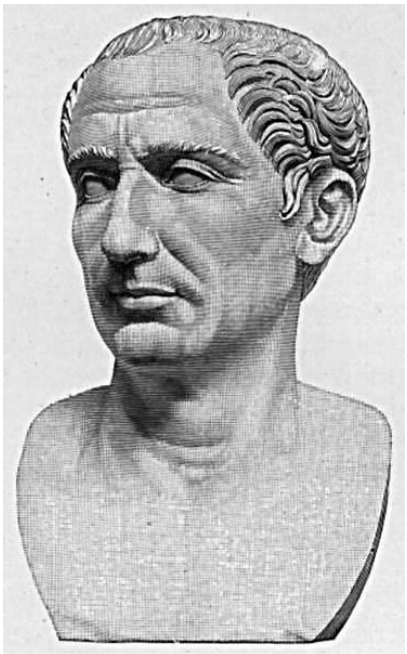


Figura 2.6: Caio Júlio César.

Um dos mais famosos sistemas de criptografia foi elaborado pelo general Júlio César. Era utilizado nas mensagens enviadas a seus generais, em torno de 58 a.C.

O sistema monoalfabético, conhecido como Cifra de César ou cifra de substituição, consistia em trocar cada letra do alfabeto seguindo um padrão bem determinado. Acredita-se que Júlio César substituía cada letra, pela terceira letra que se segue no alfabeto.

> Caso tivesse algum segredo a lhes transmitir, escrevia-lhes em linguagem cifrada, isto é, dispondo as letras em tal ordem que se não podia formar com elas nenhuma palavra. Para decifrá-las, era necessário trocar a quarta letra do alfabeto pela primeira, ou seja, o **d** no lugar do **a**, e assim consecutivamente. (Suetônio, 2002, pag. 64)

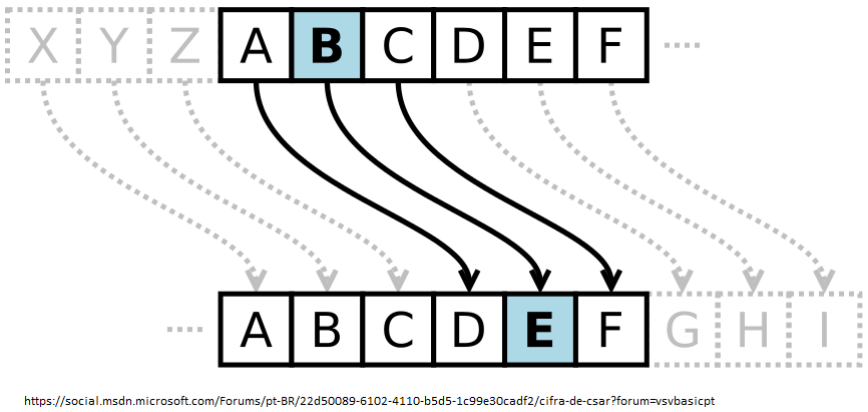


Figura 2.7: Exemplo da Cifra de César.

Otávio Augusto, sobrinho de César e primeiro imperador romano, também fazia uso de técnica semelhante. Nas palavras de Suetônio (2002, pag. 164) "Todas as vezes que escrevia em linguagem cifrada, trocava o "b" pelo "a", o "c" pelo "b" e assim por diante. Em vez de "z" escrevia "a"."

Apesar da simplicidade da cifra usada por César, presume-se que nenhum inimigo tenha conseguido ler as mensagens, tendo em vista que a maioria de seus inimigos eram analfabetos ou acreditavam estarem escritas em lingua estrangeira.

Não há registro daquela época de nenhuma técnica para resolver as cifras de substituição. Os registros mais recentes datam dos trabalhos de Al-Kindi, no século IX, oriunda da descoberta da análise de frequência.

2.2.4 Cifra de Vigenère

A cifra de Vigenère é uma versão simplificada da cifra de substituição polialfabética, inventada em 1465, por Leon Battista Alberti, conhecido como pai da criptologia ocidental. Recebeu esse nome em homenagem a Blaise de Vigenère, diplomata e criptógrafo francês, mas o primeiro registro foi descrito por Giovan Batista Belaso em *La cifra del Signore Giovan Batista Belaso*, de 1553.

A força da cifra de Vigenère consiste em que ele usa não apenas um, e sim 26 alfabetos cifrados distintos para criar a mensagem cifrada. [Singh, 2004]. Além da tabela, Vigenère inseriu palavras-chave utilizadas na codificação e na decodificação da mensagem.

CIFRA DE VIGENÈRE

	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
A	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
B	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
C	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
D	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
E	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
F	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
G	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Figura 2.8: Cifra de Vigenère.

Como exemplo, considere que a palavra-chave seja GATO e que a mensagem seja VAMOS ATACAR. Repetiremos a chave até acabarem as letras da mensagem, da seguinte forma:

Chave	G	A	T	O	G	A	T	O	G	A	T
Mensagem	V	A	M	O	S	A	T	A	C	A	R

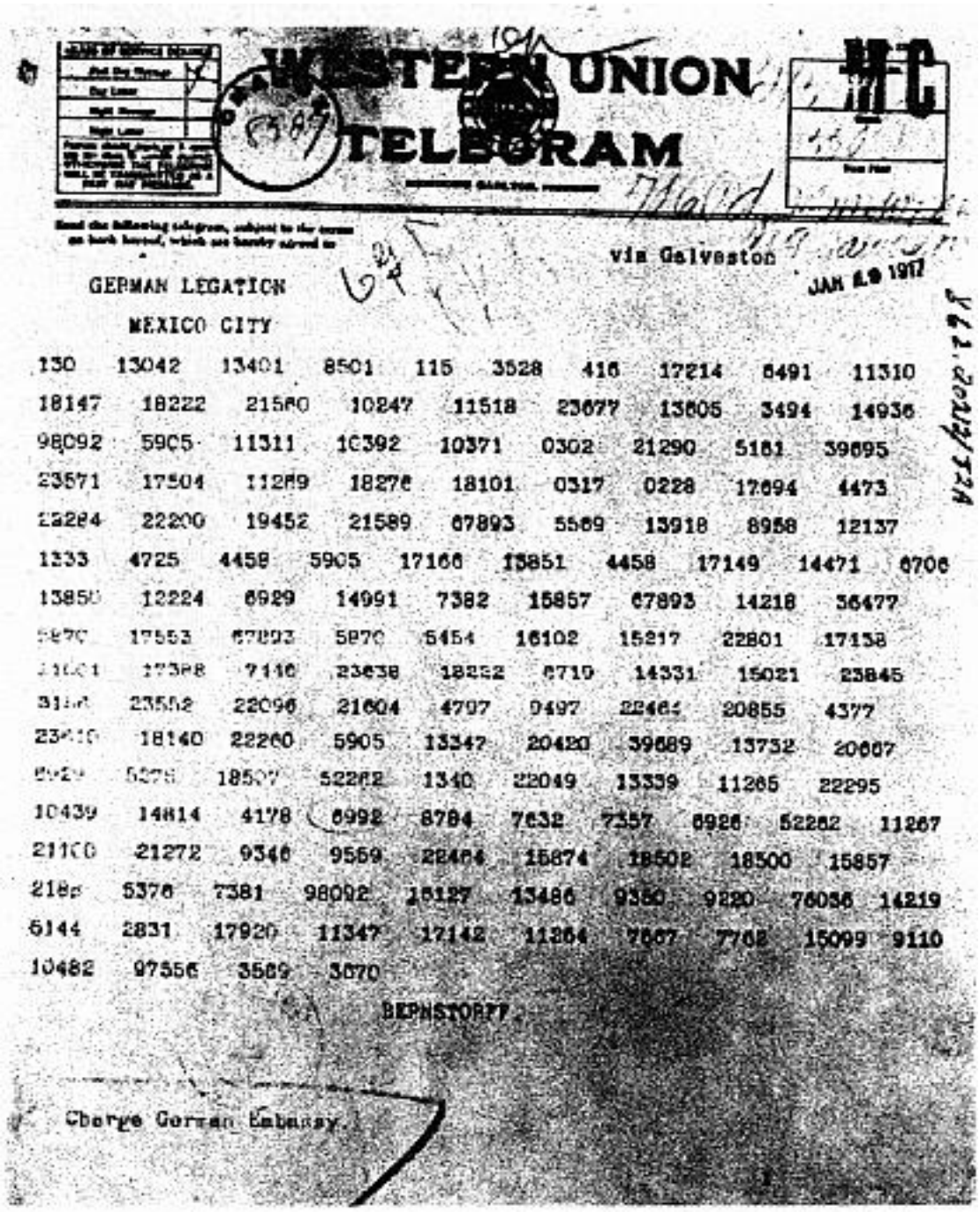
Para codificarmos a mensagem procuraremos na figura 2.8 a interseção da chave (linha) com a mensagem (coluna). Assim,

Chave	G	A	T	O	G	A	T	O	G	A	T
Mensagem	V	A	M	O	S	A	T	A	C	A	R
Codificado	B	A	E	C	Y	A	M	O	I	A	R

2.2.5 A Criptografia na Primeira Guerra

O telegrama de Zimmermann

Durante a Primeira Guerra Mundial (1914 - 1918) os códigos e cifras encontraram um meio fausto para crescer e se desenvolver. Um dos exemplos clássicos é o Telegrama de Zimmermann, considerado por muitos como o documento mais significativo para ilustrar o valor da criptoanálise durante uma guerra.



WESTERN UNION TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
[illegible] 17553 67893 5870 5454 16102 15217 22801 17138
[illegible] 17388 7110 23638 18282 6710 14331 15021 23845
[illegible] 23502 22096 21604 4797 9497 22464 20855 4377
[illegible] 18140 22260 5905 13347 20420 39689 13732 20667
[illegible] 5376 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
218[illegible] 5376 7381 98092 16127 13486 9350 9220 76036 14219
6144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF

Charge German Embassy.

Figura 2.9: Telegrama de Zimmermann.

O telegrama usava um código conhecido como 0075, composto por aproximada-

mente dez mil frases e palavras individuais. Era necessário a posse de um livro código para transmitir a mensagem e um outro para decifrá-la. (Couto, 2008)

Foi codificado e enviado pelo secretário do exterior alemão Arthur Zimmermann, em 16 de janeiro de 1917, para o embaixador alemão Heinrich von Eckhardt, no México. O telegrama foi interceptado e decodificado por criptógrafos britânicos.

O telegrama instruía o embaixador a oferecer ajuda financeira ao México para que entrasse como aliado da Alemanha em um possível conflito com os EUA.

A Cifra ADFGVX

A cifra ADFGX foi introduzida em março de 1918 pelo coronel alemão Fritz Nebel, e em junho de 1918 foi adicionada a letra V à cifra, ficando ADFGVX. Seu nome se deu por serem letras difíceis de serem confundidas quando transmitidas por Código Morse. É uma combinação entre cifras de transposição e o quadrado de Políbio 6 x6 , que inclui as 26 letras do alfabeto e os 10 algarismos, dispostos em ordem randômica.

Como exemplo usamos a mensagem CIÊNCIA DO SIGILO, a chave CIFRA e o seguinte quadrado de Políbio.

	A	D	F	G	V	X
A	B	6	P	2	5	0
D	9	J	L	Q	D	O
F	X	R	V	F	T	3
G	M	1	5	K	W	I
V	C	4	Z	E	8	Y
X	7	A	U	G	H	N

Inicialmente passamos a mensagem pela chave ADFGVX, buscando os equivalentes de cada letra em linha e coluna, ficando dispostos da seguinte forma:

C	I	E	N	C	I	A	D	O	S	I	G	I	L	O
VA	GX	VG	XX	VA	GX	XD	DV	DX	GF	GX	XG	GX	DF	DX

A seguir, a mensagem cifrada é organizada em uma tabela baseada na chave CIFRA. Depois ordenamos a chave por ordem alfabética e transpomos a mensagem cifrada.

C	I	F	R	A		A	C	F	I	R
V	A	G	X	V		V	V	G	A	X
G	X	X	V	A		A	G	X	X	V
G	X	X	D	D		D	G	X	X	D
V	D	X	G	F		F	V	X	D	G
G	X	X	G	G		G	G	X	X	G
X	D	F	D	X		X	X	F	D	D

A mensagem final, que será transmitida via rádio, será lida por coluna, ficando assim VA DF GX VG GV GX GX XX XF AX XD XDXV DG GD.

2.2.6 A Criptografia na Segunda Guerra

Alan Turing e a Máquina Enigma

A máquina Enigma, uma das mais famosas, foi usada pelos alemães durante a Segunda Guerra Mundial (1939 - 1945). Antes, era usada comercialmente e possuía vários modelos. O modelo adotado pelos nazistas era conhecido como *Wehrmacht Enigma*. Estima-se que 40 mil dessas máquinas estiveram em uso durante a guerra.

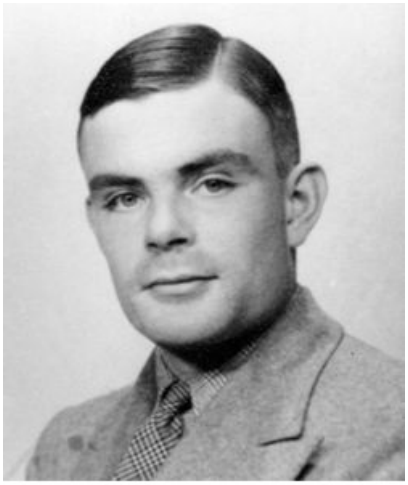
http://m.blogs.ne10.uol.com.br/mundobit/2015/01/21/como-funcionava-enigma-maquina-nazista-que-quase-venceu-segunda-guerra/

Figura 2.10: Máquina Enigma.

A Enigma possui uma combinação de sistemas mecânicos e elétricos. Seu mecanismo consiste em um teclado com 26 letras e um conjunto três de rotores dispostos em fila, além de um mecanismo de avanço que faz andar alguns rotores uma posição quando uma tecla é pressionada. Os alemães acrescentaram ainda um quarto rotor,

chamado "refletor", assim, nenhuma letra da mensagem seria cifrada nela mesma. Também acrescentaram um dispositivo chamado *stecker*, que garantia a troca de pares de letras por outras sem importar qual unidade fosse usada para o processo. Com todo esse aperfeiçoamento, a máquina atingiu um total de 150 000 000 000 000 000 000 de combinações.

Em 1939 foi criado o centro de criptologia em *Bletchley Park*, Inglaterra, conhecido como *Station X*, com a finalidade de "quebrar" a Enigma. Entre os matemáticos contratados estava Alan Turing.



https://pt.wikipedia.org/wiki/Alan_Turing

Figura 2.11: Alan Turing.

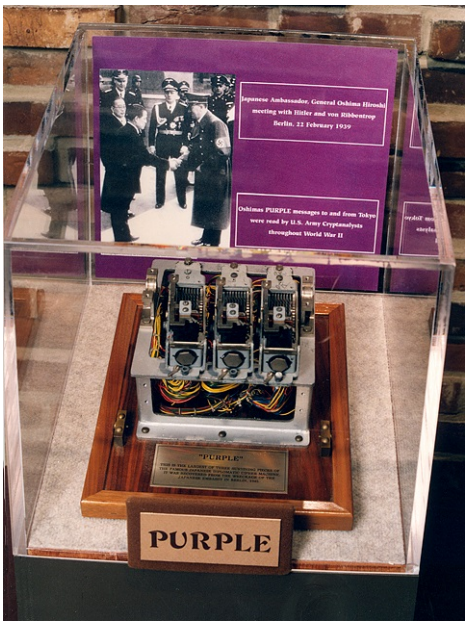
Alan Turing (1912 - 1954), considerado "pai da computação", foi um matemático, lógico e criptoanalista. Seu ápice deve-se a II Guerra Mundial, quando foi trabalhar em Bletchley Park, uma instalação militar secreta que tinha como objetivo "quebrar" os códigos alemães. Os códigos eram produzidos pela Máquina Enigma e trocados diariamente, dificultando ainda mais a decodificação. Turing desenvolveu a bomba eletromecânica (*bombe*), que auxiliava na decodificação das mensagens secretas. Além de contribuir para o fim da guerra, criou a Máquina de Turing, um protótipo dos computadores modernos, e também desenvolveu o Teste de Turing, uma espécie de inteligencia artificial.

Os aliados, depois de criar e executar uma operação de codinome ULTRA, decifraram o código que fez com que o fim da guerra, de acordo com alguns historiadores, se antecipasse por pelo menos um ano.

A Máquina Púrpura

Ainda no cenário da Segunda Guerra Mundial outra máquina de cifragem se destacou, a Máquina Púrpura, usada pelos japoneses. A versão "Vermelha", anterior a

Púrpura, já havia sido "quebrada" pelos norte-americanos, no entanto, a Marinha japonesa não admitia tal fato, assim, a Máquina Púrpura herdou seu ponto fraco, que era a cifragem separada das vogais e consoantes, conhecida pelos criptoanalistas americanos como "seis-vinte".



https://gl.wikipedia.org/wiki/C%C3%B3digo_P%C3%BArpura

Figura 2.12: Máquina Púrpua.

As técnicas usadas para decrifrar a Púrpura eram semelhantes às usadas para decifrar a Enigma. Os japoneses acreditavam que sua máquina seria indecifrável, mas sua cifra acabou sendo descoberta por um grupo do Serviço de Inteligência de Sinais do Exército norte-americano, liderado pelos criptologistas William Friedman e Frank Rowlett.

A Púrpura era uma máquina singular, usava botões de fase como elemento criptográfico, além da divisão das letras em vogais e consoantes.

2.2.7 Criptografia na Atualidade

Com o advento da comunicação eletrônica, muitas atividades essenciais passaram a depender do sigilo na troca de mensagens, principalmente aquelas que envolvem transações financeiras e uso seguro da internet.

Apresentaremos algumas aplicações da criptografia na atualidade.

Protocolo SSL

O protocolo SSL (Secure Sockets Layer) foi desenvolvido pela Netscape Communications, em 1994. É um protocolo de segurança que cria uma conexão criptografada

entre um servidor web e um navegador (browser), garantindo que os dados transmitidos entre os dois pontos não sejam interceptados, mantendo-os sigilosos e seguros. Um servidor web protegido por esse protocolo inicia sua URL com https://. Os principais bancos utilizam esse protocolo, como Banco do Brasil, Caixa Federal, Itaú e Santander.

Whatsapp

A criptografia de ponta-a-ponta do WhatsApp garante que apenas a pessoa que envia e a pessoa que recebe a mensagem possam ler o que é enviado, nem o próprio WhatsApp tem acesso. As mensagens estão seguras com um cadeado e somente quem envia e quem recebe possuem a chave para ler a mensagem. Ainda, cada mensagem enviada tem um cadeado e uma chave.

Bluetooth

O Bluetooth é uma tecnologia para redes sem fio que fornece mobilidade, rapidez e agilidade nas comunicações, este tipo de rede se comunica por ondas de rádio, o que a torna mais vulnerável a diversos tipos de ameaças à segurança da informação. Os requisitos de segurança para aplicações Bluetooth são baseados na necessidade do usuário, mercado e no tipo de informação envolvida. Algumas aplicações não necessitam de nenhuma medida de segurança já outras requerem altos níveis de segurança.

De forma geral podem ser utilizados três tipos de algoritmos de criptografia para redes Bluetooth, chave secreta (simétrico), chave pública (assimétrico) e *hashing*, onde na chave secreta os usuários compartilham uma única chave, por isso existe um grande esforço em gerenciar essas chaves, na chave pública, cada participante tem um chave, que não é compartilhada com nenhum outro usuário, e uma chave pública conhecida por todos, a mensagem é criptografada usando a chave pública e descriptografada pelo destinatário usando a chave pública (algoritmo RSA), já no *hashing* (função *hash*) não há o envolvimento de chaves, no lugar das chaves uma mensagem grande e aleatória é condensada de forma a fixar seu tamanho, este tipo de função calcula um teste por soma (*checksum*), um *checksum* criptográfico protege o receptor de uma mudança maliciosa da mensagem.

Protocolo SSH (Secure Shell)

O *Secure Shell* é um protocolo criptográfico para operação de serviços de rede de forma segura sobre uma rede insegura, o uso mais comum desse protocolo é para login remoto a sistemas de computadores pelos usuários.

O SSH usa criptografia de chaves públicas para autenticar o computador e permitir a autenticação do usuário. Há muitas formas de usar o SSH, uma delas é usar pares de chaves pública-privada geradas de forma automática para simplesmente encriptar a conexão de rede e permitir autenticação por senha, outra maneira é usar um par de

chaves pública-privada geradas manualmente para realizar autenticação, permitindo que usuários ou programas loguem sem ter que especificar uma senha.

2.2.8 Cadastro de Pessoas Físicas - CPF

O CPF é o numero de inscrição do contribuinte junto à Receita Federal do Brasil, foi criado em 1965 para que pudessem ser coletadas informações dos contribuintes obrigados a apresentar declaração de rendimentos. Hoje o CPF não se limita a apenas as informações do imposto de renda e se tornou de suma importância no cotidiano dos brasileiros. Desde 1º de dezembro de 2015 o CPF é emitido junto com a Certidão de Nascimento, evitando assim fraudes e problemas com homônimos.

O CPF é formado por 11 dígitos onde os 8 primeiros referem-se ao cadastro da pessoa física propriamente dito, o 9º digito refere-se a região fiscal onde foi efetuada o registro, e os dois últimos são dígitos verificadores.

3 Fundamentação Teórica

Neste capítulo abordaremos alguns conceitos necessários para compreensão e execução das atividades propostas no trabalho.

3.1 Funções

Quando relacionamos duas grandezas que dependem uma da outra, estamos usando o conceito de função. Este é um importante conceito da matemática, que está presente na maioria dos campos de conhecimento humano.

Esse conceito sofreu grande evolução no decorrer da história. A ideia de função que temos atualmente esta diretamente relacionada à teoria dos conjuntos, desenvolvida principalmente a partir do século XIX.

Nesse processo, diversos matemáticos contribuíram significativamente, como Gottfried Wilhelm Leibniz (1646 - 1716), Isaac Newton (1642 - 1727), Leonhard Euler (1707 - 1783), Joseph Fourier (1768 - 1830), entre outros.

3.1.1 Definição de Função Real

Dados dois conjuntos A, $B \in \mathbb{R}$, não vazios, uma função $f : A \to B$ é uma relação que associa a cada elemento $x \in A$ um único elemento $y \in B$, $f(x) = y$.

A é chamado domínio ou campo de definição.
B é chamado contradomínio.
$Im(f) = \{y \in B | \exists x \in A\}$ com $f(x) = y$ é chamado conjunto imagem de f.

3.1.2 Função Afim

Uma função $f : \mathbb{R} \to \mathbb{R}$ chama-se **afim** quando existem constantes $a, b \in \mathbb{R}$ tais que $f(x) = ax + b$ para todo $x \in \mathbb{R}$.

3.1.3 Função Injetiva, Sobrejetiva e Bijetiva

Função Injetiva

Uma função f de A em B é *injetiva* se, e somente se, quaisquer que sejam x_1 e x_2 de A, se $x_1 \neq x_2$, então $f(x_1) \neq f(x_2)$.

$$\boxed{\begin{array}{l} f : A \to B \\ f \text{ é injetiva} \Leftrightarrow (\forall x_1, x_1 \in A, \forall x_2 \in A)(x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)) \end{array}}$$

Função Sobrejetiva

Uma função f de A em B é sobrejetiva se, e somente se, para todo y pertencente a B existe um elemento x pertencente a A tal que $f(x) = y$.

$$\boxed{\begin{array}{l} f : A \to B \\ f \text{ é sobrejetiva} \Leftrightarrow (\forall y, y \in B, \exists\ x,\ x \in A \mid f(x) = y) \end{array}}$$

Função Bijetiva

Uma função f de A em B é bijetiva se, e somente se, f é injetiva e sobrejetiva.

$$\boxed{\begin{array}{l} f : A \to B \\ f \text{ é bijetiva} \Leftrightarrow (\forall y, y \in B, \exists|\ x,\ x \in A \mid f(x) = y) \end{array}}$$

Caracterização da Função Afim

Teorema 3.1. *Seja $f : \mathbb{R} \to \mathbb{R}$ uma função injetiva. Se o acréscimo $f(x+h) - f(x) = \varphi(h)$ depender apenas de h, mas, não de x, então f é uma função afim.*

Demonstração: Suporemos que a função f seja crescente. Então $\varphi : \mathbb{R} \to \mathbb{R}$ também é crescente, com $\varphi(0) = 0$. Além disso, para quaisquer $h, k \in \mathbb{R}$ temos:

$$\begin{aligned} \varphi(h+k) &= f(x+h+k) - f(x) \\ &= f((x+k)+h) - f(x+k) + f(x+k) - f(x) \\ &= \varphi(h) + \varphi(k) \end{aligned}$$

Logo, pelo Teorema da Proporcionalidade, pondo-se $a = \varphi(1)$, tem-se $\varphi(h) = a.h$ para todo $h \in \mathbb{R}$. Isto quer dizer que $f(x+h) - f(x) = ah$. Chamando $f(0)$ de b, resulta $f(h) = ah + b$, ou seja, $f(x) = ax + b$ para todo $x \in \mathbb{R}$.

■

3.1.4 Função Composta

Seja f uma função de um conjunto A em um conjunto B e seja g uma função de B em um conjunto C. Chama-se *função composta* de g e f à função h de A em C em que a imagem de cada x é obtida pelo seguinte procedimento:

i. aplica-se a x a função f, obtendo-se $f(x)$;

ii. aplica-se a $f(x)$ a função g, obtendo-se $g(f(x))$.

Indica-se $h(x) = g(f(x))$ para todo $x \in A$.

3.1.5 Função Inversa

Definição 3.1. *Se f é uma função bijetiva de A em B, a relação inversa de f é uma função de B em A que denominamos função inversa de f e indicamos por f^{-1}, tal que $f^{-1} : B \to A$.*
$y \in B$ é tal que $f^{-1}(y) = x$ onde x é o único elemento em A que satisfaz $f(x) = y$.

Teorema 3.2. *Seja $f : A \to B$. A função f admite inversa f^{-1} de B em A se, e somente se, f é bijetiva.*

Demonstração:

i. Se f^{-1} é uma função de B em A, então f é bijetiva.

   - Para todo $y \in B$ existe um $x \in A$ tal que $f^{-1}(y) = x$, isto é, $(y, x) \in f^{-1}$, ou ainda, $(x, y) \in f$. Assim f é sobrejetiva.
   - Dados $x_1 \in A$ e $x_2 \in A$, com $x_1 \neq x_2$, se tivermos $f(x_1) = f(x_2) = y$ resultará em $f^{-1}(y) = x_1$ e $f^{-1}(y) = x_2$, o que é absurdo pois y só tem uma imagem em f^{-1}. Assim $f(x_1) \neq f(x_2)$ e f é injetiva.

ii. Se f é bijetiva, então f^{-1} é uma função de B em A.

   - Como f é sobrejetiva, para todo $y \in B$ existe um $x \in A$ tal que $(x, y) \in f$; portanto, $(y, x) \in f^{-1}$.
   - Se $y \in B$, para duas imagens x_1 e x_2 em f^{-1}, vem: $(y, x_1) \in f^{-1}$ e $(y, x_2) \in f^{-1}$; portanto, $(x_1, y) \in f$ e $(x_2, y) \in f$.
     Como f é injetiva, resulta $x_1 = x_2$.

■

Regra prática para determinar a função inversa:

Dada a função bijetiva f de A em B, definida pela sentença de $y = f(x)$, para obtermos a sentença aberta que define f^{-1}, procedemos do seguinte modo:

i. Na sentença $y = f(x)$ fazemos uma mudança de variáveis, isto é, trocamos x por y e y por x, obtendo $x = f(y)$;

ii. Transformamos algebricamente a expressão $x = f(y)$, expressando y em função de x para obtermos $y = f^{-1}(x)$.

3.1.6 Função e Criptografia

O método de codificação deve ser perfeitamente eficaz, ou seja, o receptor deve ser capaz de transformar a informação codificada na informação original, sem ambiguidade ou falta de informação. Para isso, algumas propriedades devem ser seguidas nessas situações:

i. Ao codificar duas informações distintas, elas não podem ser transformadas em uma mesma informação codificada, pois o receptor teria duvidas ao codificá-la;

ii. Uma informação, ao ser codificada, não pode produzir duas informações diferentes;

iii. Toda informação deve ter uma forma codificada, ou seja, toda e qualquer informação deve ser possível de ser transmitida, evitando informações incompletas.

Para que ocorra a codificação, cada informação deve ser transformada em uma única informação codificada e deve aceitar o processo inverso, portanto, devemos encontrar uma transformação (função) bijetiva f. Como f é inversível podemos garantir a revelação das informações.

Usaremos a *função afim* $f(x) = ax + b$. Esta função é sempre bijetiva sobre sua imagem e por isso admite inversa sobre sua imagem.

O método consiste em pegar uma informação e convertê-la em números através de uma função bijetiva e, pela aplicação de sua inversa transformar esses números novamente na informação original.

Primeiramente vamos associar cada letra do alfabeto a um número, como na tabela

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

Agora, escolhemos uma função $f(x)$ que receberá o valor da letra que queremos transmitir e gerar outro valor através de $f(x)$. Suponhamos que f seja a função $f(x) = 3x + 2$, que é chamada de função cifradora.

Escolhemos a palavra MENSAGEM, cada letra da palavra será transformada em um número, que ao passar pela função cifradora será transformada na sequência de números 67 43 70 85 31 39 43 67, esta é a mensagem que o receptor receberá.

$M \to 23$	$f(23) = 3 \times 23 - 2 = 67$
$E \to 15$	$f(15) = 3 \times 15 - 2 = 43$
$N \to 24$	$f(24) = 3 \times 24 - 2 = 70$
$S \to 29$	$f(29) = 3 \times 29 - 2 = 85$
$A \to 11$	$f(11) = 3 \times 11 - 2 = 31$
$G \to 17$	$f(17) = 3 \times 17 - 2 = 49$
$E \to 15$	$f(15) = 3 \times 15 - 2 = 43$
$M \to 23$	$f(23) = 3 \times 23 - 2 = 67$

O receptor ao receber a mensagem codificada, realizará a operação inversa, que nesse caso é $f^{-1}(x) = \frac{x+2}{3}$, recompondo a mensagem original.

$f^{-1}(67) = \frac{67+2}{3} = 23$	$23 \to M$
$f^{-1}(43) = \frac{43+2}{3} = 15$	$15 \to E$
$f^{-1}(70) = \frac{70+2}{3} = 24$	$24 \to N$
$f^{-1}(85) = \frac{85+2}{3} = 29$	$29 \to S$
$f^{-1}(31) = \frac{31+2}{3} = 11$	$11 \to A$
$f^{-1}(49) = \frac{49+2}{3} = 17$	$17 \to G$
$f^{-1}(43) = \frac{43+2}{3} = 15$	$15 \to E$
$f^{-1}(67) = \frac{67+2}{3} = 23$	$23 \to M$

Quanto mais complexo for o código, mais difícil a mensagem fica para ser decifrada.

3.2 Matriz e Determinante

3.2.1 Definição de Matriz

Uma matriz de tipo $m \times n$, onde $m, n \geq 1$ é uma tabela formada por mn elementos dispostos em m linhas e n colunas; se $n = 1$, a matriz é dita *matriz-coluna*; se $m = 1$, *matriz-linha*; se $m = n$, matriz *quadrada de ordem n.*

3.2.2 Adição de Matrizes

Dadas as matrizes $A = (a_{ij})$ e $B = (b_{ij})$ de tipo $m \times n$, chama-se *soma* da matriz A com a matriz B (indica-se $A + B$) a matriz $C = (c_{ij})$, onde $c_{ij} = a_{ij} + b_{ij} (1 \leq i \leq m, 1 \leq j \leq n)$.

Chama-se *diferença* entre a matriz A e a matriz B a soma de A com $-B$ (oposto de B).

3.2.3 Produto de um Número Real por uma Matriz

Dada uma matriz $A = (a_{ij})$ e um número real t, chama-se *produto de t por A* a matriz $B = (b_{ij})$, onde $b_{ij} = ta_{ij} (1 \leq i \leq m, 1 \leq j \leq n)$. Indica-se por tA.

3.2.4 Produto de Matrizes

Dada uma matriz $A = (a_{ij})$ de tipo $m \times n$, e uma matriz $B = (b_{jk})$, de tipo $n \times p$, chama-se *produto de A por B* (indica-se AB) a matriz $C = (c_{ik})$, de tipo $m \times p$, onde

$$c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk} = a_{i1} b_{1k} + a_{i2} b_{2k} + \ldots + a_{in} b_{nk}$$

3.2.5 Matriz Transposta

Dada uma matriz $A = (a_{ij})$ de tipo $m \times n$, chama-se *transposta de A* a matriz $B = (b_{ji})$, de tipo $n \times m$, onde $b_{ji} = a_{ij} (1 \leq i \leq m, 1 \leq j \leq n)$. A matriz transposta de A indica-se por A^t.

Para achar a matriz transposta de A basta trocar linhas por colunas.

3.2.6 Definição de Determinante

Coinsideraremos o conjunto das *matrizes quadradas* de elementos reais. Seja A uma matriz de ordem n desse conjunto. Chamamos *determinante da matriz A* o número que podemos obter operando com os elementos A da seguinta forma:

i. Se A *é de ordem* $n = 1$, então $\det A$ é o único elemento de A

$$A = [a_{11}] \rightarrow \det A = a_{11}$$

ii. Se A *é de ordem* $n = 2$, o prudto dos elementos da diagonal principal menos o produto dos elementos da diagonal secundária.

$$\mathrm{A} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \rightarrow \det = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

iii. Se A *é de ordem* $n = 3$, isto é,

$$\mathrm{A} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

definimos $\det A = a_{11}.a_{22}.a_{33} + a_{12}.a_{23}.a_{31} + a_{13}.a_{21}.a_{32} - a_{13}.a_{22}.a_{31} - a_{11}.a_{23}.a_{32} - a_{12}.a_{21}.a_{33}$

3.2.7 Matrizes Inversíveis

Uma matriz quadrada A de ordem n se diz *inversível* se existe uma matriz B tal que $AB = BA = I_n$. A matriz B se diz *inversa* de A e se indica por A^{-1}.

Se A é inversível, então a sua inversa é única: com efeito, se B e B' são inversas de A, temos

$$B = BI_n = B(AB') = (BA)B' = I_nB' = B'$$

Teorema 3.3. *Se A é inversível, então a sua inversa é inversível e $(A^{-1})^{-1} = A$. Se A e B são inversíveis, o produto é inversível e $(AB)^{-1} = B^{-1}A^{-1}$.*

Demonstração: A primeira parte é imediata. O leitor deve observar, na segunda parte, que a inversa do produto é igual ao produto das inversas *na ordem contrária* (compare com a transposta do produto). Para provar, seja $C = AB$ e $D = B^{-1}A^{-1}$. Então

$$CD = (AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AIA^{-1} = AA^{-1} = AA^{-1} = I$$

Da mesma forma $DC = I$. Portnto D é inversa de C.

■

Caracterização das matrizes inversíveis

Teorema 3.4. *A matriz quadrada A é inversível se, e somente se, $\det A \neq 0$.*

3.2.8 Matriz e Criptografia: Cifras de Hill

As cifras de Hill são baseadas em transformações matriciais e utilizam um sistema poligráfico, foi inventada por Lester S. Hill em 1929.

Atribuiremos um número a cada letra do alfabeto da seguinte forma:

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

Codificaremos a frase VAMOS CODIFICAR, para isso devemos transformar pares sucessivos de texto em texto cifrado. Devemos escolher uma matriz quadrada, para facilitar escolheremos uma matriz 2×2.

$$\mathrm{A} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

Agruparemos letras sucessivas de texto em pares, substituindo cada letra por seu valor numérico. Caso tenha um número ímpar de letras, acrescentaremos uma letra fictícia para completar o último par.

V	A	M	O	S	C	O	D	I	F	I	C	A	R
22	1	13	15	19	3	15	4	9	6	9	3	1	18

Converteremos cada par sucessivo p_1 e p_2 de letras de texto em um vetor-coluna.

$$\mathrm{p} = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$$

e formaremos o produto Ap (vetor cifrado).

A matriz cifradora deve ser inversível módulo 26.

$$\text{Usaremos a matriz } \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$$

Para cifrar o par VA efetuaremos o produto matricial

$$\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 22 \\ 1 \end{bmatrix} = \begin{bmatrix} 116 \\ 47 \end{bmatrix}$$

Sempre que ocorrer um inteiro maior do que 25, ele será substituído pelo resto da divisão deste inteiro por 26.

$$\text{Assim, } \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 22 \\ 1 \end{bmatrix} = \begin{bmatrix} 116 \\ 47 \end{bmatrix} \equiv \begin{bmatrix} 12 \\ 21 \end{bmatrix} (\mod 26)$$

que fornecerá o texto cifrado LU.

Os cálculos para os demais vetores cifrados são

$$\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 13 \\ 15 \end{bmatrix} = \begin{bmatrix} 155 \\ 71 \end{bmatrix} \equiv \begin{bmatrix} 25 \\ 19 \end{bmatrix} (\mod 26)$$

$$\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 19 \\ 3 \end{bmatrix} = \begin{bmatrix} 113 \\ 47 \end{bmatrix} \equiv \begin{bmatrix} 9 \\ 21 \end{bmatrix} (\mod 26)$$

$$\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 15 \\ 4 \end{bmatrix} = \begin{bmatrix} 99 \\ 42 \end{bmatrix} \equiv \begin{bmatrix} 21 \\ 16 \end{bmatrix} (\mod 26)$$

$$\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 9 \\ 6 \end{bmatrix} = \begin{bmatrix} 81 \\ 36 \end{bmatrix} \equiv \begin{bmatrix} 3 \\ 10 \end{bmatrix} (\mod 26)$$

$$\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 9 \\ 3 \end{bmatrix} = \begin{bmatrix} 63 \\ 27 \end{bmatrix} \equiv \begin{bmatrix} 11 \\ 1 \end{bmatrix} (\mod 26)$$

$$\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 18 \end{bmatrix} = \begin{bmatrix} 113 \\ 56 \end{bmatrix} \equiv \begin{bmatrix} 9 \\ 4 \end{bmatrix} (\mod 26)$$

A mensagem transmitida será LUYSIUUPCJKAID.

Para decifrar devemos multiplicar cada vetor cifrado pelo inverso de A, que será obtido da seguinte forma:

$$A^{-1} = (a_{11}.a_{22} - a_{12}.a_{21})^{-1} \begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix} (\mod 26)$$

onde $(a_{11}.a_{22} - a_{12}.a_{21})^{-1}$ é o recíproco do resíduo de $(a_{11}.a_{22} - a_{12}.a_{21})(\mod 26)$.

Para auxiliar os cálculos abaixo, forneceremos a tabela de recíprocos módulo 26.

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Assim,

$$\det A = \begin{vmatrix} 5 & 6 \\ 2 & 3 \end{vmatrix} = 15 - 12 = 3$$

$$A^{-1} = 3^{-1} \begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix} = 9 \begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix} = \begin{bmatrix} 27 & -54 \\ -18 & 45 \end{bmatrix} \equiv \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} (\mod 26)$$

Os cálculos para decifrar os vetores cifrados são

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \begin{bmatrix} 12 \\ 21 \end{bmatrix} = \begin{bmatrix} 516 \\ 495 \end{bmatrix} \equiv \begin{bmatrix} 22 \\ 1 \end{bmatrix} (\mod 26)$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \begin{bmatrix} 25 \\ 19 \end{bmatrix} = \begin{bmatrix} 481 \\ 561 \end{bmatrix} \equiv \begin{bmatrix} 13 \\ 15 \end{bmatrix} (\mod 26)$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \begin{bmatrix} 9 \\ 21 \end{bmatrix} = \begin{bmatrix} 513 \\ 471 \end{bmatrix} \equiv \begin{bmatrix} 19 \\ 3 \end{bmatrix} (\mod 26)$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \begin{bmatrix} 21 \\ 16 \end{bmatrix} = \begin{bmatrix} 405 \\ 472 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 4 \end{bmatrix} (\mod 26)$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \begin{bmatrix} 3 \\ 10 \end{bmatrix} = \begin{bmatrix} 243 \\ 214 \end{bmatrix} \equiv \begin{bmatrix} 9 \\ 6 \end{bmatrix} (\mod 26)$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \begin{bmatrix} 11 \\ 1 \end{bmatrix} = \begin{bmatrix} 35 \\ 107 \end{bmatrix} \equiv \begin{bmatrix} 9 \\ 3 \end{bmatrix} (\mod 26)$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \begin{bmatrix} 9 \\ 4 \end{bmatrix} = \begin{bmatrix} 105 \\ 148 \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 18 \end{bmatrix} (\mod 26)$$

Os equivalentes alfabeticos destes vetores são VA MO SC OD IF IC AR que fornecem a mensagem "vamos codificar".

O leitor interessado em aprender mais sobre esta aplicação pode consultar o livro “Álgebra Linear com Aplicações” de Anton, H e Rorres, C.

3.3 Teoria dos Números

3.3.1 Divisibilidade

Dados dois números inteiros a e b, diremos que a *divide* b, escrevendo $a|b$, quando existir $c \in \mathbb{Z}$ tal que $b = ca$. Nesse caso, diremos também que a é um *divisor* ou um *fator* de b ou, ainda, que b é um *múltiplo* de a ou que b é *divisível* por a.

3.3.2 Divisão Euclidiana

Sejam a e b dois números inteiros com $b \neq 0$. Existem dois únicos números inteiros q e r tais que

$$a = bq + r, \text{ com } a \leq r < |b|.$$

Demonstração:

Considere o conjunto

$$S = \{x = a - by; y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\}).$$

Existência: Pela Propriedade Arquimediana, existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$, logo $a - nb > 0$, o que mostra que S é não vazio. O conjunto S é limitado inferiormente por 0, logo, pelo Princípio da Boa Ordenação, temos que S possui um menor elemento r. Suponhamos então que $r = a - bq$. Sabemos que $r \geq 0$. Vamos mostrar que $r < |b|$. Suponhamos por absurdo que $r \geq |b|$. Portanto, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$, logo $0 \leq s < r$. Mas isso contradiz o fato de r ser o menor elemento de S, pois $s = a - (q \pm 1)b \in S$, com $s < r$.

Unicidade: Suponha que $a = bq + r = bq' + r'$, onde $q, q', r, r' \in \mathbb{Z}, 0 \leq r < |b|$ e $0 \leq r' < |b|$. Assim, temos que $-|b| < r \leq r' - r \leq r' < |b|$. Logo, $|r' - r| < |b|$. Por outro lado, $b(q - q') = r' - r$, o que implica que

$$|b||q - q'| = |r' - r| < |b|,$$

o que só é possível se $q = q'$ e consequentemetne, $r = r'$.

■

3.3.3 Máximo Divisor Comum

Sejam datos dois inteiros a e b, distintos ou não. Um número inteiro d será dito um *divisor comum* de a e b se $d|a$ e $d|b$.

Diremos que um número inteiro $d \geq 0$ é um *máximo divisor comum* (mdc) de a e b, se possuir as seguintes propriedades:

i. d é um divisor comum de a e b, e

ii. d é divisível por todo divisor comum de a e b.

3.3.4 Números Primos

Definição 3.2. *Um número natural maior do que* 1 *só possui como divisores positivos* 1 *e ele próprio é chamado de número primo.*

Dados dois números primos p e q e um número inteiro a qualquer, decorrem da definição acima os seguintes fatos:

i. Se $p|q$, então $p = q$. De fato, como $p|q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Sendo p primo, tem-se que $p > 1$, o que acarreta $p = q$.

ii. Se $p \nmid a$, então $(p, a) = 1$.
De fato, se $(p, a) = d$, temos que $d|p$ e $d|a$. Portanto, $d = p$ ou $d = 1$. Mas $d \neq p$, pois $p \nmid a$ e, consequentemente, $d = 1$.

Definição 3.3. *Um número maior do que* 1 *e que não é primo será dito composto.*

Portanto, se um número natural $n > 1$ é composto, existirá um divisor natural n_1 de n tal que $1 < n_1 < n$. Logo, existirá um número natural n_2 tal que

$$n = n_1 n_2, \quad com\ 1 < n_1 < n\ e\ 1 < n_2 < n$$

Lema de Euclides

Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p|ab$, então $p|a$ ou $p|b$.

Demonstração:
Basta provar que, se $p|ab$ e $p \nmid a$, então $p|b$. Mas, se $p \nmid a$, temos que $(p, a) = 1$, e o resultado segue-se do Lema de Gauss.
Lema de Gauss: Sejam a, b, e c números inteiros. Se $a|bc$ e $(a, b) = 1$, então $a|c$.
■

Teorema Fundamental da Aritmética

Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.

Demonstração:

Usaremos a segunda forma do Princípio de Indução. Se $n = 2$, o resultado é obviamente verificado.

Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos, então, que n seja composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, \ldots, p_r$. $q_1, \ldots, q_s$ tais que $n_1 = p_1 \ldots p_r$ e $q_1 \ldots q_s$. Portanto, $n = p_1 \ldots p_r q_1 \ldots q_s$.

Vamos, agora, provar a unicidade da escrita. Suponha que tenhamos $n = p_1 \ldots p_r = q_1 \ldots q_s$, são números primos. Como $p_1 | q_1 \ldots q_s$, pelo corolário acima, temos que $p_1 = q_j$ para algum j, que, após reordenarmento de $q_1, \ldots, q_s$, podemos supor que seja q_1. Portanto,

$$p_2 \ldots p_r = q_2 \ldots q_s.$$

Como $p_2 \ldots p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_1 e q_j são iguais aos pares.

■

3.3.5 Congruência

Definição 3.4. *Seja m um número natural. Diremos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se*

$$a \equiv b \mod m$$

.

Quando a relação $a \equiv b \mod m$ for falsa, diremos que a e b não são congruentes.

$$a \not\equiv b \mod m$$

.

Proposição 3.1. *Suponha que $a, b, m \in \mathbb{Z}$, com $m > 1$. Tem-se que $a \equiv b \mod m$ se, e somente se, $m | b - a$.*

Demonstração: Sejam $a = mq + r$, com $0 \leq r < m$, e $b = mq' + r'$, com $0 \leq r' < m$, as divisões euclidianas de a e b por m, respectivamente. Logo,

$$b - a = m(q' - q) + (r' - r)$$

Portanto, $a \equiv b \mod m$, se, e somente se, $r = r'$, o que, em vista da igualdade acima, é equivalente a dizer que $m|b-a$, já que $|r - r'| < m$.

■

Proposição 3.2. *Seja $m \in \mathbb{N}, m > 0$. Para todos $a, b, c \in \mathbb{Z}$, tem-se que*

i. $a \equiv a \mod m$,

ii. *se* $a \equiv b \mod m$, *então* $b \equiv a \mod m$,

iii. *se* $ab \mod m$ *e* $b \equiv c \mod m$, *então* $a \equiv c \mod m$.

Demonstração:

i. $m|0$, ou seja, $m|a-a$, o que implica que $a \equiv a \mod m$.

ii. se $a \equiv b \mod m$, então $b - a = qm$, com $q \in \mathbb{Z}$.

$$a - b = -qm = (-q)m \Rightarrow b \equiv a \mod m$$

iii. se $a \equiv b \mod m$ e $b \equiv c \mod m$, então existem inteiros q_1 e q_2 tais que

$$b - a = q_1 m \text{ e } c - b = q_2 m$$

Portanto,

$$c - a = (b + q_2 m) - (b - q_1 m) = q_2 m + q_1 m = (q_2 + q_1)m$$

e isto significa que $a \equiv c \mod m$.

■

Proposição 3.3. *Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$.*

i. se $a \equiv b \mod m$ e $c \equiv d \mod m$, então $a + c \equiv b + d \mod m$.

ii. se $a \equiv b \mod m$ e $c \equiv d \mod m$, então $ac \equiv bd \mod m$.

Demostração: Suponhamos que $a \equiv b \mod m$ e $c \equiv d \mod m$. Logo, temos que $m|b-a$ e $m|d-c$.

i. basta observar que $m|(b-a)+(d-c)$ e, portanto, $m|(b+d)-(a+c)$, o que prova essa parte do resultado.

ii. basta notar que

$$bd - ac = d(b - a) + a(d - c)$$

e concluir que $m|bd - ac$.

■

Proposição 3.4. *Para todos $n \in \mathbb{N}, a, b \in \mathbb{Z}$, se $a \equiv b \mod m$, então tem-se que $a^n \equiv b^n \mod m$.*

Demonstração: Provaremos por indução. A proposição é verdadeira para $n = 1$ e suponha que seja verdadeira para qualquer natural k. Desta forma temos:

$$a^k \equiv b^k \mod m \text{ e } a \equiv b \mod m$$

Portanto, pela proposição (3.3) acima

$$a^k.b^k.b \mod m \text{ ou } a^{k+1} \equiv b^{k+1} \mod m$$

isto é, a proposição é verdadeira para o natural k+1. Logo, a proposição é verdadeira para todo natural n.

■

3.4 Criptografia RSA

O método de criptografia RSA foi inventado em 1978, por três professores do MIT (*Massachusests Institute of Technology*), R. L. Rivest, A. Shamir e L. Adleman. É um código de chave pública, usado principalmente em aplicações comerciais e bancárias. A segurança do sistema depende da escolha dos números primos a serem utilizados.

Indicamos como aprofundamento do tema a leitura dos livros "Números Inteiros e Criptografia RSA" e "Criptografia" (disponível em PDF), ambos de S. C. Coutinho.

Vamos codificar a mensagem VIDA usando o método RSA. Devemos escolher dois parâmetros, números primos p e q, cujo resto na divisão por 6 tem que ser 5. O produto $p.q = n$ será nossa chave.

Cada letra da mensagem deve ser substituida por um número, que serão separados em blocos, que devem ser números menores que n. Usaremos a tabela:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Escolhemos os parâmetros $p = 5$ e $q = 7$, logo $n = 35$.

Regra para codificar

$$b^{\lambda} \equiv a \mod n, \qquad \lambda \in \mathbb{N}$$

b é o bloco e a é a classe de equivalência.

Escolhemos $\lambda = 7$. Assim,

$V \to 31$	$31^7 \equiv 31 \mod 35$
$I \to 18$	$18^7 \equiv 32 \mod 35$
$D \to 13$	$13^7 \equiv 27 \mod 35$
$A \to 10$	$10^7 \equiv 10 \mod 35$

Portanto, a mensagem codificada será 31322710.

Para decodicar usamos a regra:

$a^d \equiv b \mod n$, onde d é o inverso de $\lambda[\mod (p-1)(q-1)]$.

Assim,

$$7d \equiv 1 \mod (5-1)(7-1)$$

$$7d \equiv 1 \mod (4.6)$$

$$7d \equiv 1 \mod 24$$

$$7.7 \equiv 1 \mod 24$$

Logo, $d = 7$

Portanto,

$31^7 \equiv 31$	mod 35	$31 \to V$
$32^7 \equiv 18$	mod 35	$18 \to I$
$27^7 \equiv 13$	mod 35	$13 \to D$
$10^7 \equiv 10$	mod 35	$10 \to A$

4 O Uso da Criptografia no Estudo de Funções

Neste capítulo discorreremos sobre as atividades desenvolvidas em sala de aula, na escola municipal da cidade de Lucélia-SP.

4.1 Criptografia na Sala de Aula

Foi realizada uma enquete com os alunos de dois nonos anos (9º B e 9º E), na qual queríamos saber a opinião deles sobre a disciplina de Matemática, se gostavam, se achavam importante e sugestões para melhorar as aulas. Todos concordaram que a matemática é importante e está presente no nosso dia a dia, porém muitos disseram não gostar da disciplina, pois tem dificuldade em aprende-la. Sugeriram aulas mais dinâmicas, com aplicações, jogos, filmes e atividades em grupo. Assim, demos continuidade ao trabalho iniciado no ano de 2016.

> Essas aprendizagens só serão possíveis na medida em que o professor proporcionar um ambiente de trabalho que estimule o aluno a criar, comparar, discutir, rever, perguntar e ampliar ideia. (PCN, 1997, pag. 41)

Primeiramente, assistiram o filme O Jogo da Imitação, que se passa durante a Segunda Guerra Mundial e retrata parte da vida do matemático Alan Turing, conhecido como "pai da computação". Na aula seguinte estavam entusiasmados, discutindo sobre o filme, muitos até haviam pesquisado sobre Turing e suas criações.

Aproveitando o entusiasmo, introduzimos algumas noções de criptografia, relatamos um pouco da história e técnicas de criptografia. Seguem algumas atividades aplicadas em sala de aula e no Apêndice A as atividades executadas pelos alunos.

4.1.1 Atividade 1 - Cifra de César

Um dos primeiros sistemas de criptografia conhecido foi elaborado pelo general Júlio César. O sistema de substituição monoalfabético, conhecido como Cifra de César,

consistia em substituir cada letra do alfabeto seguindo um padrão bem determinado. Acredita-se que Júlio César substituia cada letra, pela terceira letra que se segue no alfabeto.

A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	F	G	H	I	J	K	L	M	N	O	P

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Usando a Cifra de César, codifique as mensagens a seguir.

- VIDA
- ULTRA
- ESCOLA
- AMIGO
- MATEMÁTICA
- CRIPTOGRAFIA

Os alunos não tiveram dificuldade em realizar a atividade. Questionaram se poderiam "andar um número de casas diferente de 3". Sugerimos que criassem um alfabeto cifrado diferente do usado por César, escrevessem uma mensagem e enviassem a um colega, sem dizer quantas casas haviam percorrido.

Alguns alunos desistiram, outros criaram vários alfabetos cifrados até conseguir desvendar a mensagem recebida, um aluno alegou ser muito fácil, pois haviam letras que se repetiam na mensagem e que provavelmente era uma vogal, assim rapidamente conseguiu elaborar a tabela correta.

4.1.2 Atividade 2 - Confecção dos discos giratórios

Material:

- Papel cartão ou cartolina
- Canetinha
- Lápis de cor

- Colchetes
- Tesoura sem ponta
- Cola

1º Passo: Preencha o disco maior com as letras do alfabeto, seguindo a ordem original;

2º Passo: Preencha os disco menores, um com as letras do alfabeto em ordem e o outro de forma aleatória;

3º Passo: Recorte os discos e cole sobre o papel cartão;

4º Passo: Perfure o centro dos discos e coloque o colchete.

Os discos foram pré impressos em sulfite, foi utilizado software de desenho para facilitar a divisão do disco em 26 partes iguais, como podemos ver na figura.

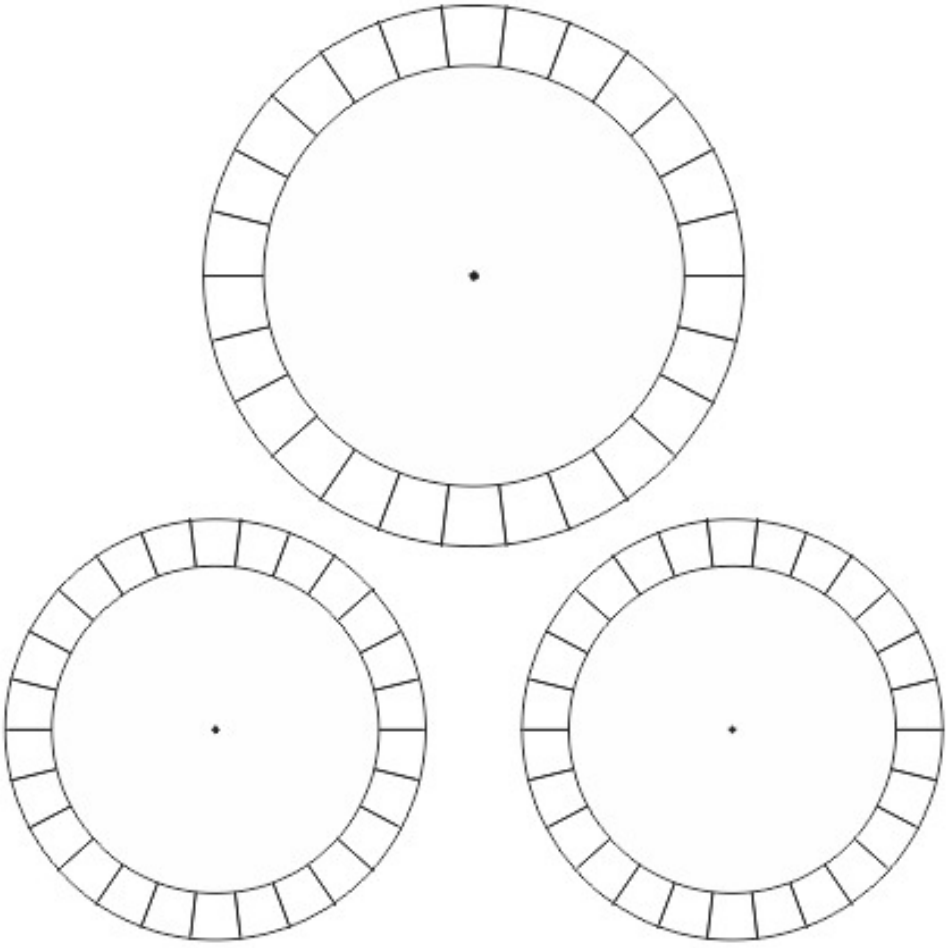


Figura 4.1: Modelo dos Discos.

Na figura abaixo temos um disco pronto, confeccionado pelos alunos.

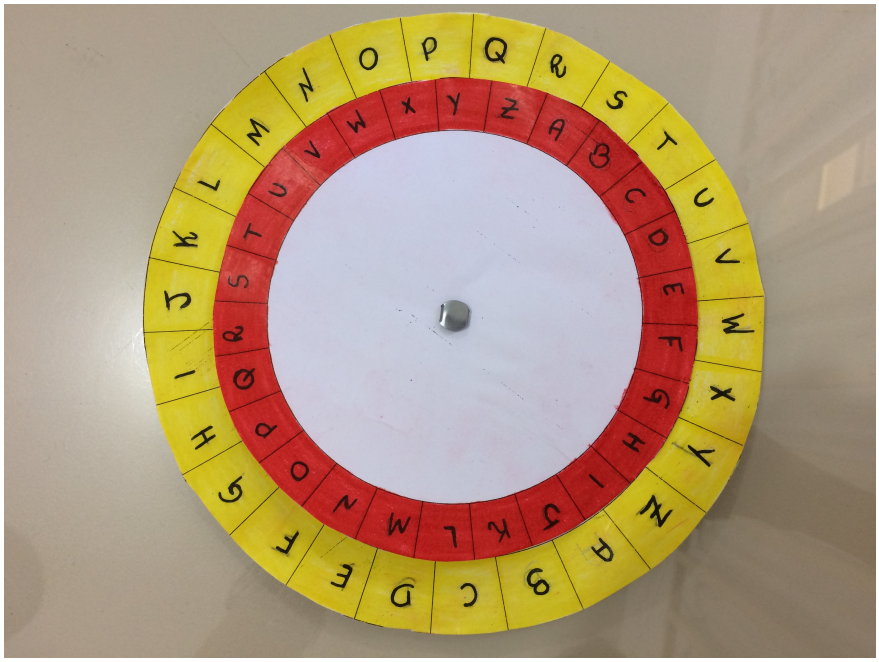


Figura 4.2: Disco Giratório.

4.1.3 Atividade 3 - Cifra de Substituição

Para realização desta atividade, são utilizados dois discos, o disco 1 onde os dois alfabetos estão na ordem original e o disco 2 onde um alfabeto está na ordem original e o outro em ordem aleatória.

Usando o disco 1, responda:

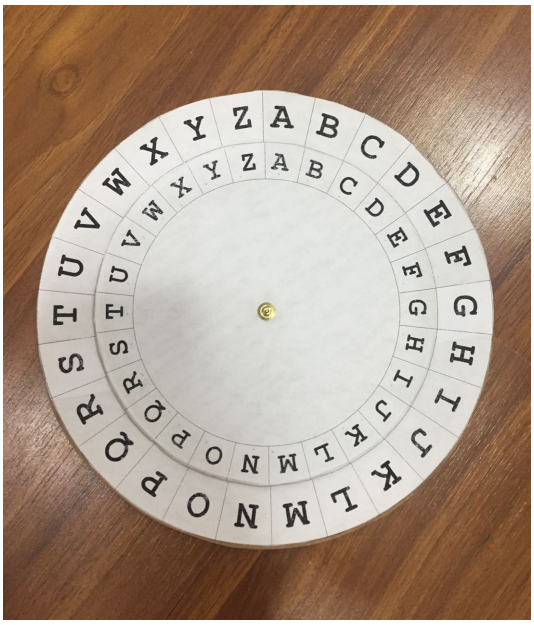


Figura 4.3: Disco 1.

1. Usando a Cifra de César codifique a mensagem CRIPTOGRAFIA.
2. Usando a Cifra de César decodifique a mensagem DPLCDGH.
3. Escolha uma chave e codifique a mensagem MATEMÁTICA.
4. Escolha uma chave, codifique uma mensagem e troque com outra dupla. Eles conseguiram decodificar sua mensagem? Vocês conseguiram decodificar a mensagem deles? Caso tenham conseguido, como fizeram para decodificar sem conhecer a chave?

Usando o disco 2, responda

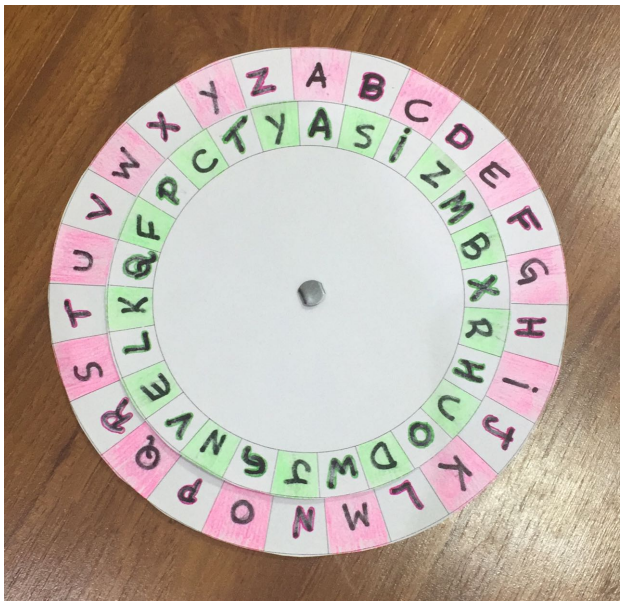


Figura 4.4: Disco 2.

1. Escolha uma chave e codifique a mensagem NÚMERO.
2. Escolha uma chave, codifique uma mensagem e troque com outra dupla. Eles conseguiram decodificar sua mensagem? Vocês conseguiram decodificar a mensagem deles? Caso tenham conseguido, como fizeram para decodificar sem conhecer a chave?

Os alunos questionaram sobre a dificuldade em realizar a atividade utilizando o disco 2, aproveitamos para recordar o conteúdo Possibilidades, estudado no 8º ano.

Após término da atividade, devido ao grande interesse despertado e a empolgação dos alunos, estes pediram para continuar trocando mensagens criptografadas com os colegas.

4.1.4 Atividade 4 - Funções e Criptografia

Para realização desta atividade foi necessário introduzir alguns conceitos que não fazem mais parte do currículo do Estado de São Paulo. Além das noções de função estudadas regularmente, foi ensinado as noções de função injetiva, sobrejetiva, bijetiva e função inversa. Antes de aplicar esta atividade, fizemos outras semelhantes na lousa/caderno.

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

1. Usando a função $f(x) = 2x + 3$, codifique a mensagem CIÊNCIA.
2. Decodifique a mensagem 55 70 37 73 49 70 88 31, sabendo que a função cifradora é $f(x) = 3x - 2$.
3. Escreva uma mensagem e codifique-a usando a função $f(x) = 2x - 6$. (Use 99 no lugar do espaço)
4. Sabendo que a função cifradora é , decodifique a mensagem:

   51599949634731575159993551653157492347995199476349295 1.

   (Considere 99 = espaço).
5. Entregue a mensagem codificada na questão 4 à outros grupo. Eles conseguiram decodificar?

4.2 Resultados

> O significado da atividade matemática para o aluno também resulta das conexões que ele estabelece entre ela e as demais disciplinas, entre ela e seu cotidiano e das conexões que ele percebe entre os diferentes temas matemáticos. (PCN, 1997, pag. 38)

A criptografia como ferramenta de ensino é de grande valia, conseguimos relacionar matemática e história, mostramos aplicações no dia a dia, ressaltamos a importância da matemática e principalmente, cativamos os alunos.

Os alunos envolvidos nas atividades demonstraram mais entusiasmo durante as aulas, maior dedicação e uma melhora significativa no rendimento escolar, além do ganho cultural. A repercussão das atividades resultou na criação da Oficina de Criptografia, que permitiu a participação de alunos dos demais nonos anos.

As atividades foram executadas no segundo e terceiro bimestre, nesse período percebemos uma melhora no desempenho escolar dos alunos. A tabela a seguir mostra uma melhora na média geral da sala na disciplina de matemática.

	1º Bimestre	2º Bimestre	3º Bimestre
9º ano B	6,4	7,2	7,3
9º ano E	5,6	6,1	6,8

5 Outras Atividades Desenvolvidas

5.1 Oficina de Criptografia

A Oficina de Criptografia não fazia parte do projeto inicial, foi desenvolvida em virtude do interesse e procura dos alunos. A princípio, seria oferecida em um único dia, mas a pedido dos alunos foi estendida para dois dias, com duração total de cinco horas. Participaram das atividades cerca de 40 alunos.

Muitos alunos presentes não eram das salas em que foram aplicadas as atividades, a maioria destes sequer tinha ouvido falar de criptografia, se inscreveram para participar por ser uma atividade diferenciada e por verem o entusiasmo dos colegas que ja haviam trabalhado o assunto.

Retomamos e aprofundamos a parte histórica vista em sala de aula, exibimos um video (disponível em `https://youtu.be/5w3zDa7bgLU`) ensinando como funcionava a máquina Enigma e apresentamos algumas técnicas de criptografia. Depois de uma breve discussão, iniciamos as atividades, que foram realizadas em grupo.

> (...) o ensino da Matemática prestará sua contribuição à medida que forem exploradas metodologias que priorizem a criação de estratégias, a comprovação, a justificativa, a argumentação, o espírito crítico, e favoreçam a criatividade, o trabalho coletivo, a iniciativa pessoal e a autonomia advinda do desenvolvimento da confiança na própria capacidade de conhecer e enfrentar desafios. (PCN, 1997, pag. 31)

As atividades realizadas pelos alunos estão no Apêndice B.

5.1.1 Atividade 1 - Cifra de Substituição

Para realizar esta atividade utilizamos o disco 1, já apresentado no capítulo 4 (Figura 4.3).

Esta consiste em escolher uma chave (número de casas percorridas para fazer a substituição) e codificar uma mensagem, que será entregue a outro grupo. Sem saber a chave utilizada, devem tentar decodificar a mensagem e descrever a técnica utilizada.

Os alunos não tiveram dificuldade em realizar a atividade, a maioria girou o disco até achar a solução.

5.1.2 Atividade 2 - Funções

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

- Usando a função afim $f(x) = 3x + 1$, codifique a mensagem CRIPTOGRAFIA.
- Escreva uma mensagem e codifique-a usando a função $f(x) = 2x - 5$. (Considere 99 = espaço)
- Sabendo que a função cifradora é $f(x) = 2x + 3$, decodifique a mensagem:
  25995533596163335129412599339953992925494151395399315399337141 6353.

Para realizar essa atividade, assim como feito em sala de aula, foi preciso aprofundar os conceitos de funções.

5.1.3 Atividade 3 - CPF

O texto desta atividade foi extraído da oficina "Aprendendo Criptologia de Forma Divertida", disponível em `http://www.mat.ufpb.br/bienalsbm/arquivos/Oficinas/PedroMalagutti-TemasInterdisciplinares/Aprendendo_Criptologia_de_Forma_Divertida_Final.pdf`.

O cadastro das pessoas físicas (usado nas declarações de imposto de renda) tem o seguinte formato:

$$X_1X_2X_3X_4X_5X_6X_7X_8 \text{ R - } C_1\ C_2$$

Os oito primeiros números constituem o número básico de inscrição da pessoa física no Cadastro Individual do Contribuinte.

O nono algarismo, indicado pela letra R, indica a região fiscal onde foi efetuada a inscrição. O Dígito C_1 é um número verificador do número formado pelos nove algarismos anteriores (calculado tomando o resto por 11, como no ISBN) e C_2 é o dígito de controle que verifica a exatidão dos dez algarismos anteriores (usando também o resto por 11).

Cálculo de C_1: Cada um dos nove algarismos, a partir da direita é multiplicado sucessivamente por 2, 3, 4, 5, 6, 7, 8, 9, 10 e os produtos resultantes são somados. A soma obtida é então dividida por 11 e C_1 será o quanto falta para 11 do resto desta divisão. Se este complemento for maior ou igual a 10, toma-se o valor 0. Colocamos o valor encontrado de C_1 na sua devida posição para iniciar o cálculo de C_2.

Cálculo de C_2: Cada um dos dez algarismos, a partir da direita, é multiplicado sucessivamente por 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 e os produtos resultantes são somados. O número C_2 é obtido então de maneira análoga a C_1.

- Calcule os dígitos de controle C_1 e C_2 para o CPF 213746059.
- Crie um CPF para nossa região fiscal.

5.1.4 Atividade 4 - Cifra de Vigenère

CIFRA DE VIGENÈRE																									
	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**
A	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
B	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
C	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
D	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
E	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
F	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
G	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Figura 5.1: Cifra de Vigenère.

- Usando a chave CIFRA codifique uma mensagem e depois envie a outro grupo.

A atividade serviu para retomarmos a ideia de coordenadas, estudadas no sétimo e oitavo ano. Os alunos não tiveram dificuldade em realizar a atividade, pois alegaram ser parecido com o jogo Batalha Naval.

5.1.5 Atividade 5 - Cilindro de Thomas Jefferson

Esta atividade foi baseada no vídeo "Introdução a Criptografia - Aula do MIT", disponível em `https://youtu.be/wtwlVqEoyyw`.

Material:

- 6 copos de plástico
- Tiras de papel divididas em 26 partes iguais
- Canetinha
- Fita adesiva
- Tesoura

Os grupos que trocão mensagens deverão proceder da mesma maneira na construção dos copos.

1º passo: Escrever em cada tira de papel o alfabeto, a disposição das letras ficará a critério do grupo;

2º passo: Recortar as tiras e colar nos copos;

3º passo: Numerar os copos.

Para execução da atividade deve ser escolhida uma chave comum entre os dois grupos que irão se comunicar, essa chave são os números de cada copo (como cada grupo tem apenas 6 copos, cada mensagem deve ter no máximo 6 letras).

No exemplo a seguir codificaremos a mensagem GATO, utilizando a chave 5213.

A mensagem será formada rotacionando os copos e alinhando as letras que compõem a mensagem, depois deverá ser escolhida uma outra coluna e esta será a mensagem a ser enviada, no nosso exemplo FBGB.

5.2 Minicurso: Criptografia como Recurso no Ensino de Matemática

Este minicurso foi apresentado no XII Simpósio de Matemática da FCT - UNESP, para alunos do curso de licenciatura em Matemática, com duração total de 4h 30min.

A proposta do minicurso era apresentar aplicações da criptografia como recurso de ensino, na qual não basta simplesmente aplicar uma atividade diferente, é necessário contextualiza-la, de forma que aluno relacione a atividade com o conteúdo que esta sendo estudado. As atividades encontram-se no Apêndice C.

Figura 5.2: Disposição dos copos (chave).

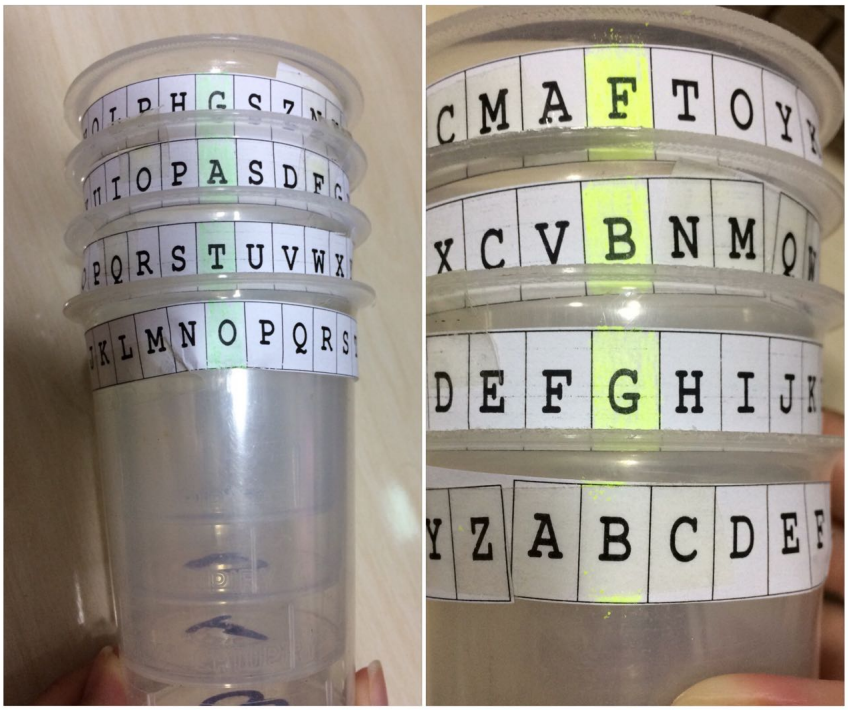


Figura 5.3: Mensagem Original e Mensagem Codificada.

> (...) nem mesmo a exploração de materiais didáticos tem contribuído para uma aprendizagem mais eficaz, por ser realizada em contextos pouco significativos e de forma muitas vezes artificial. (PCN, 1997, pag.)

- Cifra de Substituição

  Esta atividade pode ser utilizada quando o professor for introduzir Funções no 9º ano do Ensino Fundamental, ou durante as aulas de Análise Combinatória, nas quais poderemos questionar os alunos sobre as possibilidades que temos utilizando

cada um dos discos mencionados. Alguns livros didáticos introduzem o conteúdo com uma aplicação, para que o aluno possa ver sentido naquilo que está sendo ensinado. No livro Vontade de Saber de Joamir Souza e Patricia Moreno Pataro, o capítulo que trata funções inicia-se com Criptografia, como observamos na figura abaixo.

capítulo 5 Funções

Criptografia

Você sabe o que é criptografia? É a arte de escrever em códigos, transformando o texto original em um texto cifrado, de maneira a permitir que somente o receptor seja capaz de decifrar. A palavra criptografia se originou do grego, da fusão de *kryptós*, que significa oculto, secreto e *graphía*, escrita.

Existem registros de criptografia na escrita hieroglífica dos egípcios, há cerca de 4 000 anos. Mas foram os militares, com a necessidade de transmitir mensagens com segurança, que desenvolveram essa técnica.

Atualmente a criptografia está presente em diversas situações do nosso dia a dia: quando utilizamos o telefone celular, fazemos operações bancárias e utilizamos o computador. Na telefonia celular, a criptografia evita que suas conversas sejam ouvidas por intrusos. Nos bancos, para que a segurança das movimentações financeiras possa ser preservada, ou seja, para que dados de cartões de crédito, por exemplo, se mantenham sigilosos. E em computadores, de maneira que as informações armazenadas ou transmitidas não possam ser acessadas.

De maneira geral, a criptografia está associada ao uso de senhas, também chamadas chaves. Se a chave estiver correta, torna possível o acesso aos serviços, isto é, pode decifrar a mensagem. Mas se a chave for incorreta, o acesso é negado. Então, quanto mais complexa for a chave, mais difícil as mensagens ficam para serem decifradas.

Na internet
Mais informações sobre criptografia em:
www.mat.ufpb.br/bienalsbm/arquivos/Oficinas_Completos/01Completo.pdf
www.brasilescola.com/informatica/criptografia.htm

* Utilizada pelo exército alemão durante a II Guerra Mundial, a Enigma era uma máquina capaz de codificar mensagens.

82

Um exemplo de criptografia

1 Uma chave de codificação é criada. Nesse exemplo, cada letra do alfabeto é associada a um único outro caracter.

Caracter original	Caracter chave
A	L
B	M
C	N
D	O
E	P
F	Q
G	R
H	S
I	T
J	U
K	V
L	W
M	X
N	Y
O	Z
P	A
Q	B
R	C
S	D
T	E
U	F
V	G
W	H
X	I
Y	J
Z	K

2 A mensagem é escrita e enviada ao destinatário.

MATEMÁTICA SECRETA

3 A mensagem é codificada de acordo com a chave.

XLEPXLETNL DPNCPEL

4 De posse da chave, é feito a decodificação e o receptor pode ler a mensagem original.

MATEMÁTICA SECRETA

Conversando sobre o assunto

a) De acordo com o texto, porque a criptografia é importante?
b) De acordo com o exemplo apresentado, decodifique a mensagem NCTAEZRCLQTL? criptografia
c) Junte-se a um colega, elabore uma chave de criptografia e codifiquem algumas mensagens. Resposta pessoal.

a) É importante para que as pessoas mantenham a segurança e a privacidade em diversas situações, como em bancos, nas telefonias e nos computadores.

83

Figura 5.4: Vontade de Saber pag. 82 e 83.

- Funções e Criptografia

  O objetivo desta atividade é tornar as aulas menos exaustivas, com ela podemos ensinar o cálculos de funções de forma atrativa, pois realizando os cálculos corretamente os alunos conseguirão comunicar-se com os colegas.

- Cifra de Vigenère

  O professor poderá utilizar esta atividade quando for ensinar aos alunos a localizar as coordenadas no Plano Cartesiano.

- Cifra ADFGVX

  A Cifra ADFGVX pode ser utilizada quando o professor for introduzir Matrizes no 2º ano do Ensino Médio e ainda, podemos aproveitar para fazer um resgate histórico, pois essa Cifra foi usada pelos alemães durante a Primeira Guerra Mundial.

- Cifras de Hill

Este é um exemplo de atividade que pode ser inserido quando o professor ensinar produto matricial, em vez der propor exercícios maçantes podemos utilizar esta atividade, com a mesma finalidade, mas sem que o aluno fique entediado.

- CPF

  Um dos contextos em que podemos utilizar esta atividade é na revisão das operações básicas, principalmente as divisões, que são uma das maiores dificuldades dos alunos.

- Criptografia RSA

  Vamos demonstrar o funcionamento do sistema de criptografia RSA (capitulo 3.4) utilizando números primos pequenos. O objetivo da atividade é despertar o interesse dos alunos nas aulas de Matemática, mostrando um método muito utilizado na atualidade, além de recordar alguns conceitos já estudados, como números primos, divisibilidade e propriedades da potenciação.

Considerações Finais

Esperamos com este trabalho incentivar mais professores a fazerem uso da contextualização para efetivar o ensino da Matemática, de forma que o aluno desperte para realidade que a Matemática faz parte de sua vida.

Propomos atividades didáticas que unem os conteúdos matemáticos a um tema atual, apresentando aplicações e situações de uso ao longo da história. São atividades que podem ser utilizadas pelos professores para revisar, fixar, aprofundar e exercitar os conteúdos ensinados.

As atividades desenvolvidas apresentaram rendimento benéfico, como pudemos verificar nos resultados apresentados no Capítulo 4.2 e também nos questionários aplicados aos alunos que participaram da Oficina (Apêndice B) e Minicurso (Apêndice C).

Além da melhora no rendimento escolar, percebemos mais empatia e disposição durante as aulas. Os alunos sentiram-se motivados, uma vez que puderam, não só compreender, como também aplicar os conceitos muitas vezes abstratos para eles.

Usando a criptografia como ferramenta no ensino da Matemática, atribuímos significado ao conceito estudado, de forma que o aluno se sinta motivado a aprendê-lo. Assim, ressaltamos a importância de inserir o uso de assuntos ligados a realidade do aluno, que estimulem o empenho dos mesmo nas aulas, contribuindo de forma significativa para sua aprendizagem.

Pensar o futuro da educação é descriptografar a cada dia o interesse das novas gerações e adaptar novas maneiras de transmitir o conhecimento.

Referências

ANTON, Howard; RORRES, Chris. *Álgebra linear com aplicações*. trad. Claus Ivo Doering. 8 ed. Porto Alegre. Bookman. 2001.

BRASIL, Secretaria da Educação Fundamental. *Parâmetros Curriculares Nacionais: Matemática*. MEC. 1997.

CAROLI, Alésio de; CALLIOLI, Carlos A.; FEITOSA, Miguel O. *Matrizes, vetores, geometria analítica: teoria e exercícios*. 1 ed. São Paulo. Nobel. 1984.

COUTINHO, Severino Collier. *Criptografia*. 1 ed. Rio de Janeiro. IMPA. 2015.
== COUTINHO, Severino Collier. *Números Inteiros e Criptografia RSA* 1 ed. Rio de Janeiro. IMPA. 2014.

COUTO, Sergio Pereira. *Códigos & Cifras* da antiguidade à era moderna. 1 ed. Rio de Janeiro. Novaterra. 2008.

HEFEZ, Abramo. *Aritmética*. Coleção PROFMAT. 1 ed. Rio de Janeiro. SBM. 2014.

IEZZI, Gelson; HAZZAN, Samuel. *Fundamentos de Matemática Elementar*. Volume 4: sequências, matrizes, determinantes, sistemas. 7 ed. São Paulo. Atual. 2004.

LIMA, Elon Lages. *Matemática e Ensino*. 3 ed. Rio de Janeiro. SBM. 2007.

LIMA, Elon Lages; *et al*. *A Matemática do Ensino Médio*. Volume 1. 10 ed. Rio de Janeiro. SBM. 2010.

LIMA, Elon Lages; *et al*. *A Matemática do Ensino Médio*. Volume 3. 6 ed. Rio de Janeiro. SBM. 2006.

MALAGUTTI, Pedro Luiz; BEZERRA, Débora de Jesus; RODRIGUES, Vânia Cristina da Silva. *Aprendendo Criptologia de Forma Diertida*. Disponível em < `http://www.mat.ufpb.br/bienalsbm/arquivos/Oficinas/PedroMalagutti-TemasInter`

disciplinares/Aprendendo_Criptologia_de_Forma_Divertida_Final.pdf>. Acesso em 09 jan 2018.

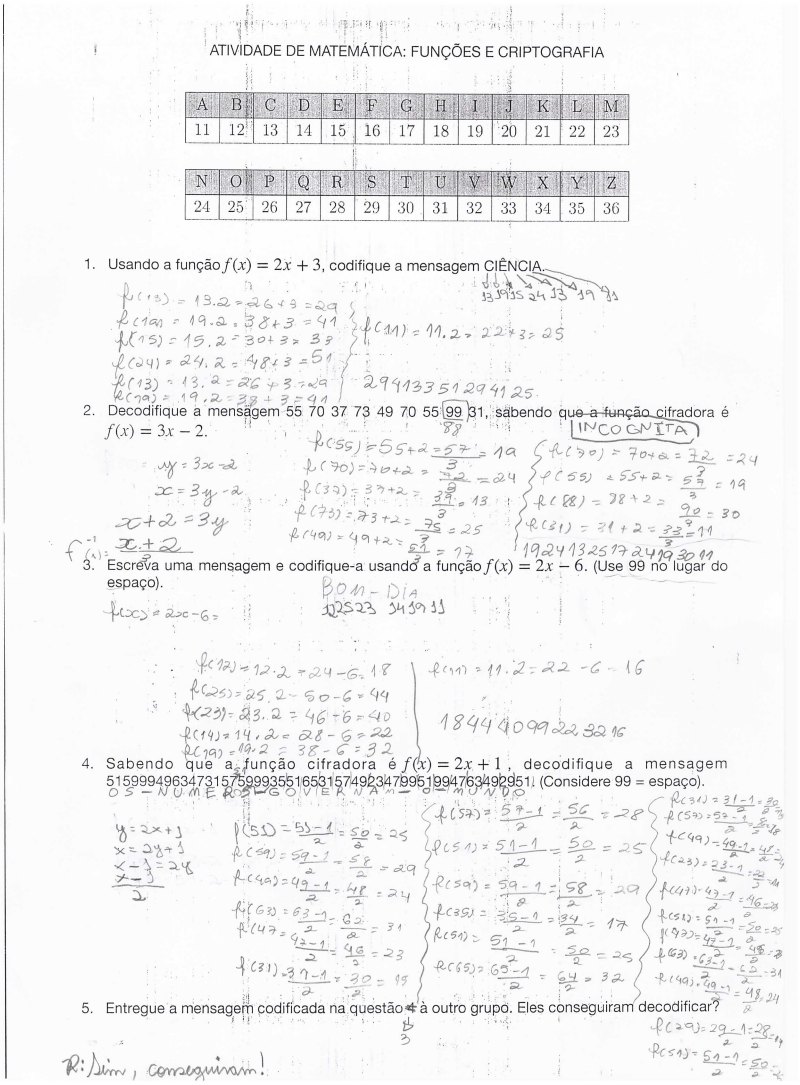
SINGH, Simon. *O Livro dos Códigos*. trad. Jorge Calife. 4 ed. Rio de Janeiro. Record. 2004.

SOUZA, Joelmir Roberto de; PATARO, Patricia Rosana Moreno. *Vontade de saber matemática, 9º ano*. 2 ed. São Paulo. FTD. 2012.

STURTEVANT, Dan. *Introdução a Criptografia - Aula do MIT*. Disponível em https://youtu.be/wtwlVqEoyyw. Acesso em 21 jun 2017.

SUETÔNIO. *A Vida dos Doze Césares*. trad. Sady-Garibaldi. 2 ed. São Paulo. Ediouro. 2002.

A Apêndice A - Atidades Desenvovidas em Sala de Aula



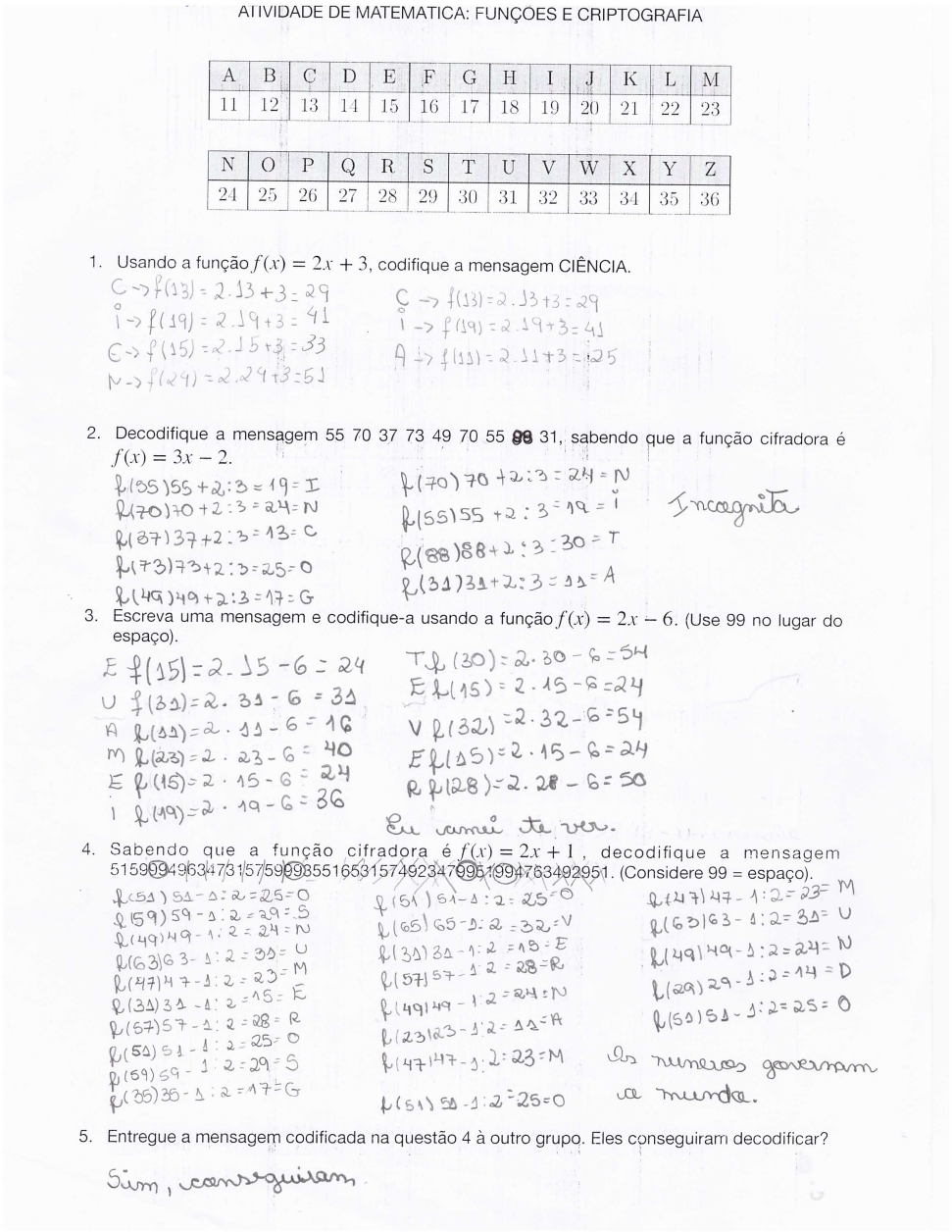
ATIVIDADE DE MATEMÁTICA: FUNÇÕES E CRIPTOGRAFIA

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

1. Usando a função $f(x) = 2x + 3$, codifique a mensagem CIÊNCIA.
2. Decodifique a mensagem 55 70 37 73 49 70 55 99 31, sabendo que a função cifradora é $f(x) = 3x - 2$.
3. Escreva uma mensagem e codifique-a usando a função $f(x) = 2x - 6$. (Use 99 no lugar do espaço).
4. Sabendo que a função cifradora é $f(x) = 2x + 1$, decodifique a mensagem 515999496347315759993551653157492347995199476349295111 (Considere 99 = espaço).
5. Entregue a mensagem codificada na questão 4 à outro grupo. Eles conseguiram decodificar?

Figura A.1: Atividade.



ATIVIDADE DE MATEMATICA: FUNÇÕES E CRIPTOGRAFIA

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

1. Usando a função $f(x) = 2x + 3$, codifique a mensagem CIÊNCIA.

C -> f(13) = 2.13 + 3 = 29
I -> f(19) = 2.19 + 3 = 41
E -> f(15) = 2.15 + 3 = 33
N -> f(24) = 2.24 + 3 = 51

C -> f(13) = 2.13 + 3 = 29
I -> f(19) = 2.19 + 3 = 41
A -> f(11) = 2.11 + 3 = 25

2. Decodifique a mensagem 55 70 37 73 49 70 55 88 31, sabendo que a função cifradora é $f(x) = 3x - 2$.

f(55)55 + 2 : 3 = 19 = I
f(70)70 + 2 : 3 = 24 = N
f(37)37 + 2 : 3 = 13 = C
f(73)73 + 2 : 3 = 25 = O
f(49)49 + 2 : 3 = 17 = G

f(70) 70 + 2 : 3 = 24 = N
f(55)55 + 2 : 3 = 19 = I
f(88)88 + 2 : 3 = 30 = T
f(31)31 + 2 : 3 = 11 = A

Incognita

3. Escreva uma mensagem e codifique-a usando a função $f(x) = 2x - 6$. (Use 99 no lugar do espaço).

E f(15) = 2.15 - 6 = 24
U f(31) = 2.31 - 6 = 31
A f(11) = 2.11 - 6 = 16
M f(23) = 2.23 - 6 = 40
E f(15) = 2.15 - 6 = 24
I f(19) = 2.19 - 6 = 36

T f(30) = 2.30 - 6 = 54
E f(15) = 2.15 - 6 = 24
V f(32) = 2.32 - 6 = 54
E f(15) = 2.15 - 6 = 24
R f(28) = 2.28 - 6 = 50

Eu vamos te ver.

4. Sabendo que a função cifradora é $f(x) = 2x + 1$, decodifique a mensagem 51599949634731575999855165315749234799519947634992951. (Considere 99 = espaço).

f(51)51 - 1 : 2 = 25 = O
f(59)59 - 1 : 2 = 29 = S
f(49)49 - 1 : 2 = 24 = N
f(63)63 - 1 : 2 = 31 = U
f(47)47 - 1 : 2 = 23 = M
f(31)31 - 1 : 2 = 15 = E
f(57)57 - 1 : 2 = 28 = R
f(51)51 - 1 : 2 = 25 = O
f(59)59 - 1 : 2 = 29 = S
f(35)35 - 1 : 2 = 17 = G

f(51)51 - 1 : 2 = 25 = O
f(65)65 - 1 : 2 = 32 = V
f(31)31 - 1 : 2 = 15 = E
f(57)57 - 1 : 2 = 28 = R
f(49)49 - 1 : 2 = 24 = N
f(23)23 - 1 : 2 = 11 = A
f(47)47 - 1 : 2 = 23 = M
f(51)51 - 1 : 2 = 25 = O

f(47)47 - 1 : 2 = 23 = M
f(63)63 - 1 : 2 = 31 = U
f(49)49 - 1 : 2 = 24 = N
f(29)29 - 1 : 2 = 14 = D
f(51)51 - 1 : 2 = 25 = O

Os numeros governam a mundo.

5. Entregue a mensagem codificada na questão 4 à outro grupo. Eles conseguiram decodificar?

Sim, conseguiram

Figura A.2: Atividade.

Figura A.3: Confecção dos Discos.

Figura A.4: Confecção dos Discos.

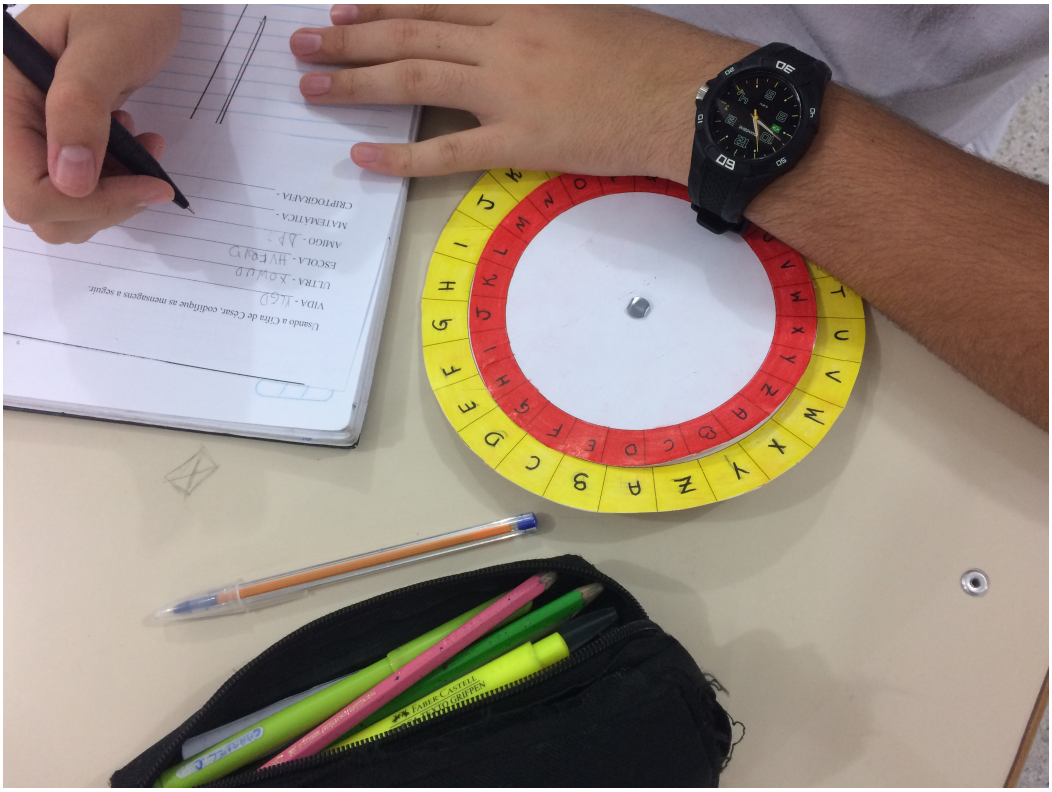


Figura A.5: Resolvendo as Atividades.

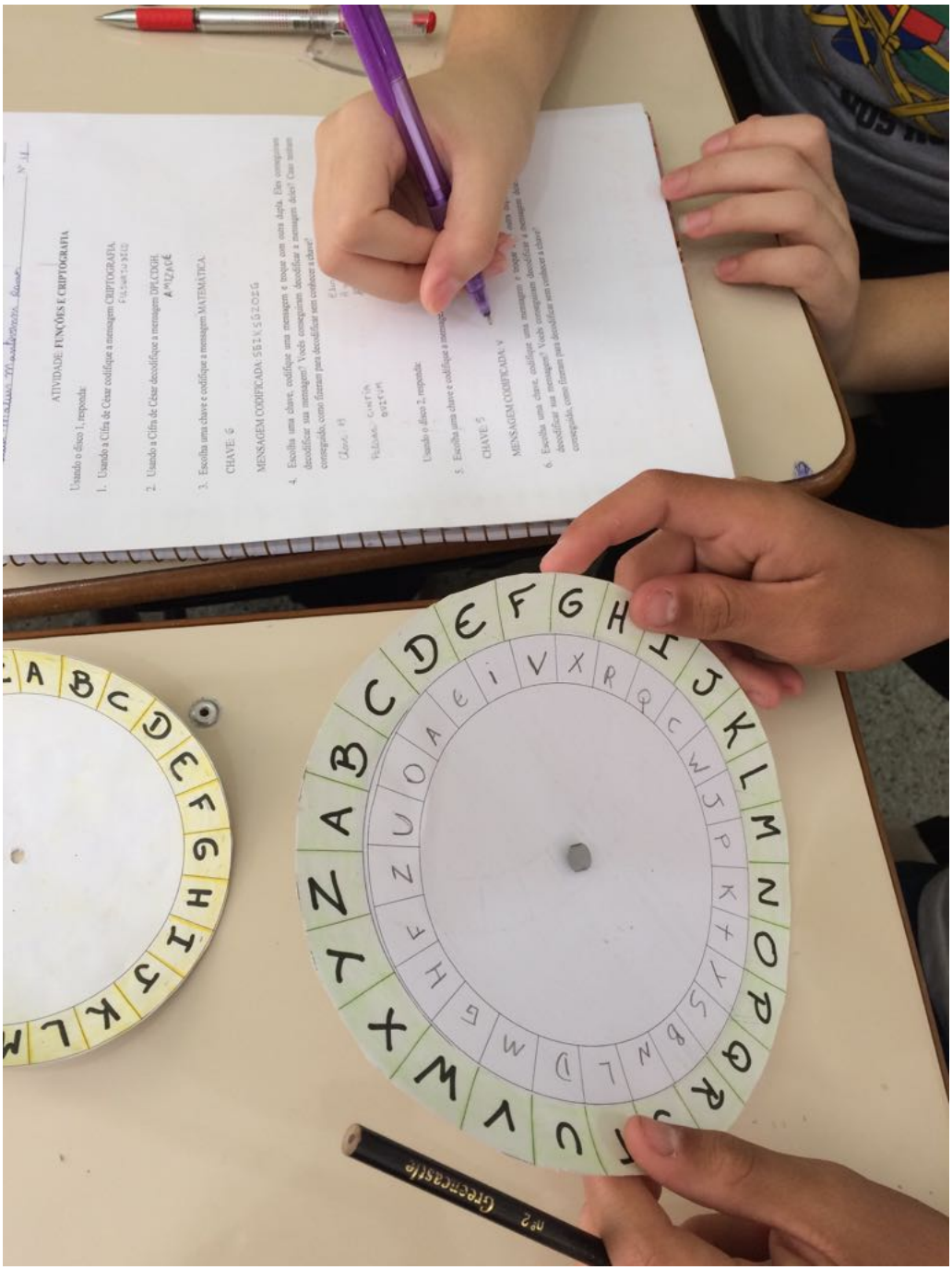


Figura A.6: Resolvendo as Atividades.

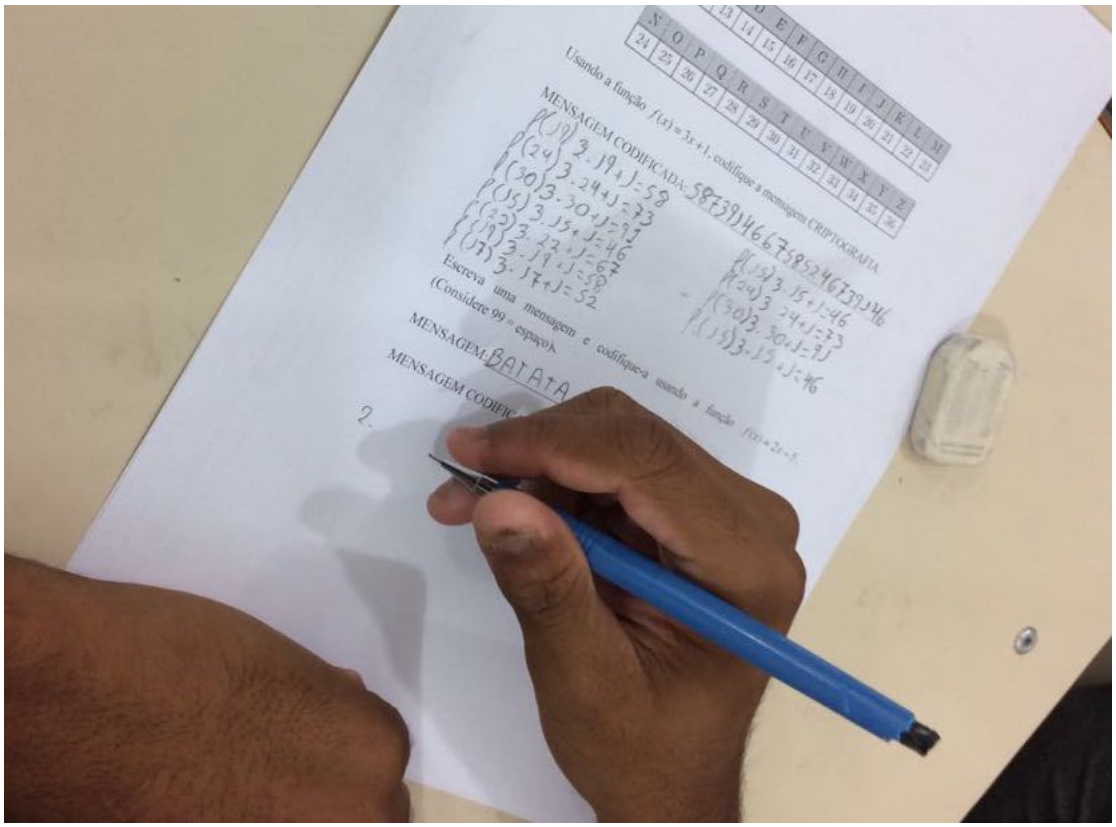
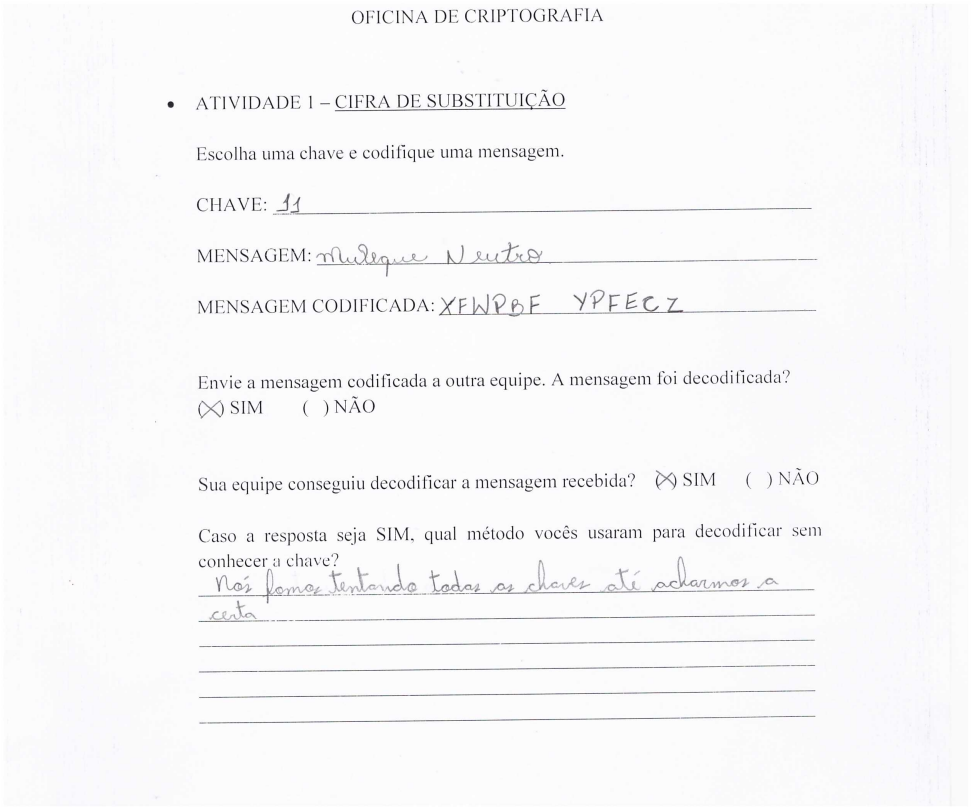


Figura A.7: Resolvendo as Atividades.

B Apêndice B - Oficina de Criptografia



OFICINA DE CRIPTOGRAFIA

- ATIVIDADE 1 – CIFRA DE SUBSTITUIÇÃO

Escolha uma chave e codifique uma mensagem.

CHAVE: 11

MENSAGEM: Mudeque Neutro

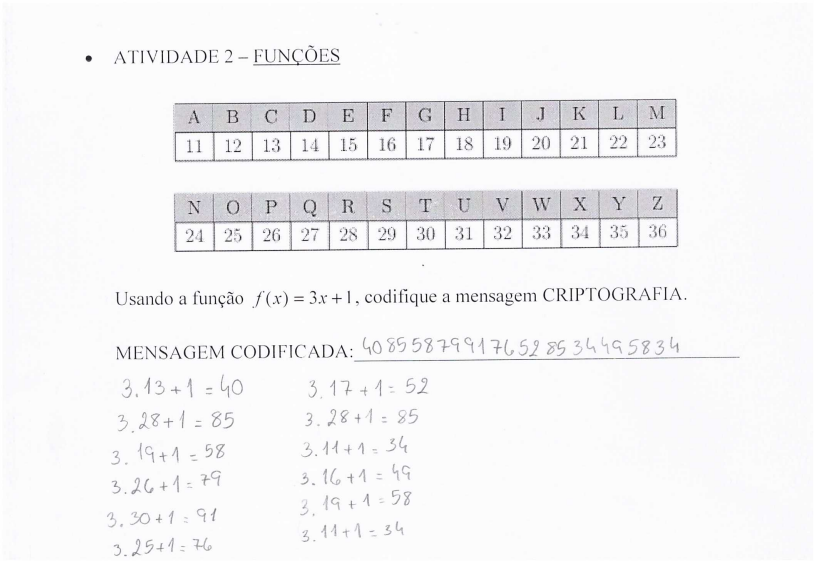
MENSAGEM CODIFICADA: XFWPBF YPFECZ

Envie a mensagem codificada a outra equipe. A mensagem foi decodificada?
(X) SIM ( ) NÃO

Sua equipe conseguiu decodificar a mensagem recebida? (X) SIM ( ) NÃO

Caso a resposta seja SIM, qual método vocês usaram para decodificar sem conhecer a chave?
Nós fomos tentando todas as chaves até acharmos a certa

Figura B.1: Atividade 1 - Cifra de Substituição.



- ATIVIDADE 2 – FUNÇÕES

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23

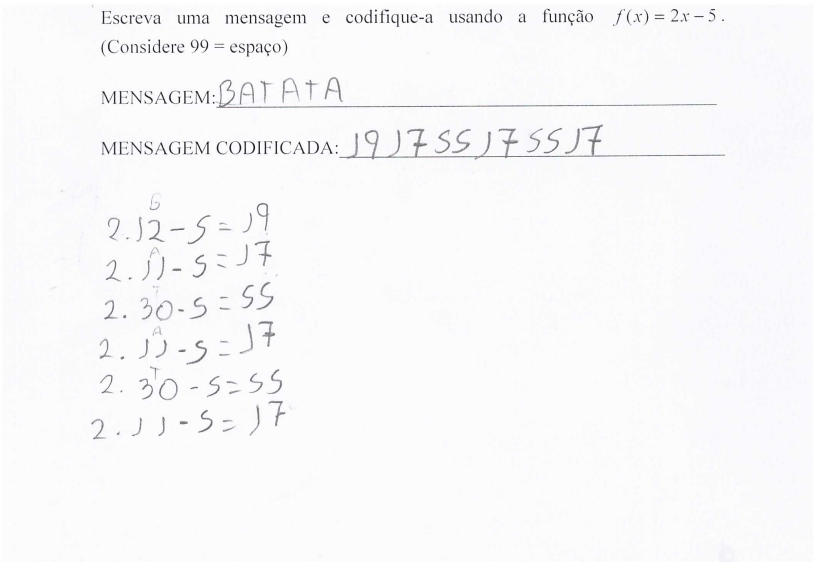
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

Usando a função $f(x) = 3x + 1$, codifique a mensagem CRIPTOGRAFIA.

MENSAGEM CODIFICADA: 40 85 58 79 91 76 52 85 34 49 58 34

3. 13 + 1 = 40
3. 28 + 1 = 85
3. 19 + 1 = 58
3. 26 + 1 = 79
3. 30 + 1 = 91
3. 25 + 1 = 76
3. 17 + 1 = 52
3. 28 + 1 = 85
3. 11 + 1 = 34
3. 16 + 1 = 49
3. 19 + 1 = 58
3. 11 + 1 = 34

Figura B.2: Atividade 2.1 - Funções.



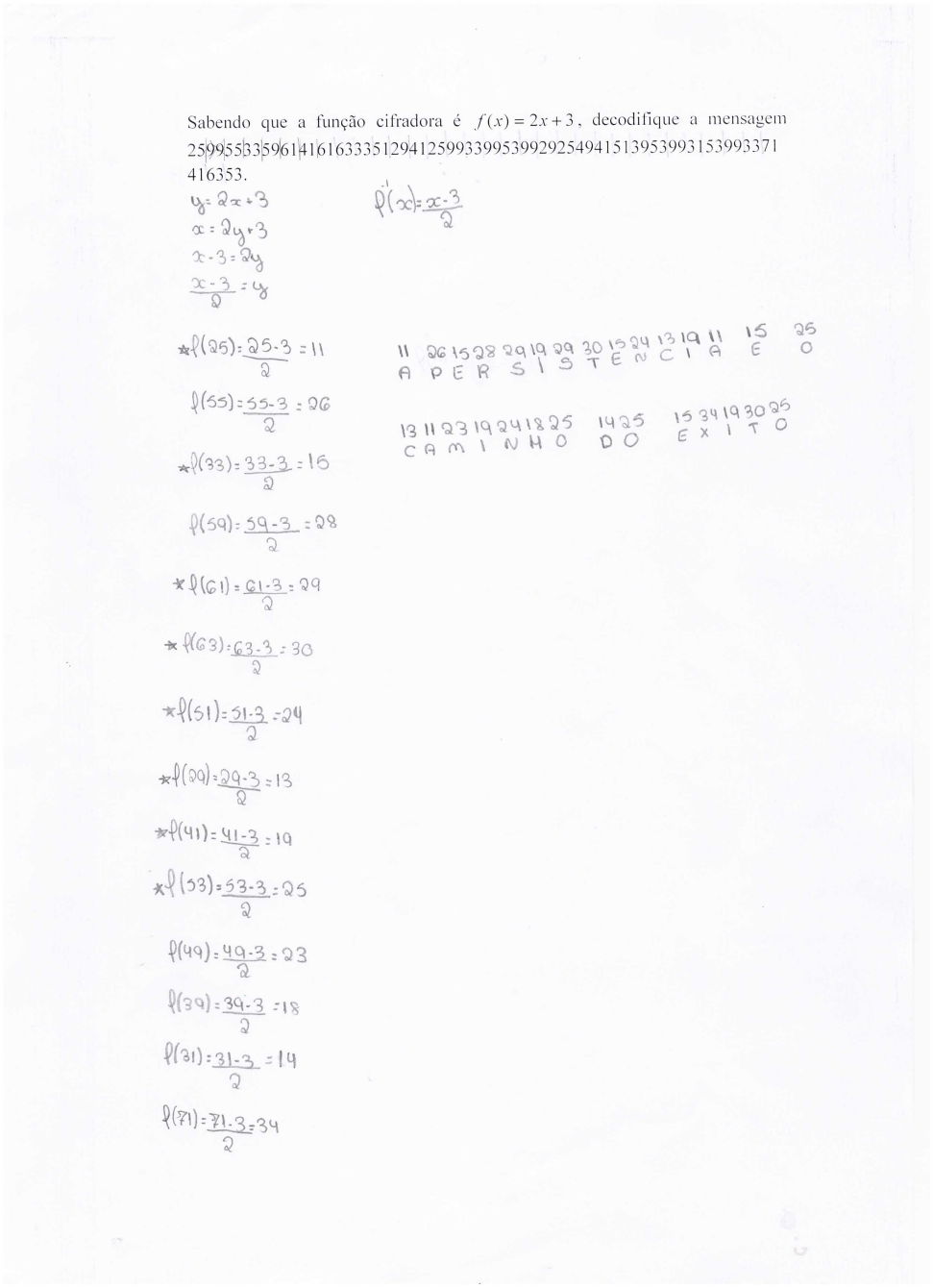
Escreva uma mensagem e codifique-a usando a função $f(x) = 2x - 5$.
(Considere 99 = espaço)

MENSAGEM: BATATA

MENSAGEM CODIFICADA: 19 17 55 17 55 17

G
2. 12 - 5 = 19
A
2. 11 - 5 = 17
T
2. 30 - 5 = 55
A
2. 11 - 5 = 17
T
2. 30 - 5 = 55
2. 11 - 5 = 17

Figura B.3: Atividade 2.2 - Funções.



Sabendo que a função cifradora é $f(x) = 2x + 3$, decodifique a mensagem 259955335961416163335129412599339953992925494151395399315399337141 6353.

$y = 2x + 3$

$x = 2y + 3$

$x - 3 = 2y$

$\frac{x-3}{2} = y$

$f^{-1}(x) = \frac{x-3}{2}$

$f(25) = \frac{25-3}{2} = 11$

$f(55) = \frac{55-3}{2} = 26$

$f(33) = \frac{33-3}{2} = 15$

$f(59) = \frac{59-3}{2} = 28$

$f(61) = \frac{61-3}{2} = 29$

$f(63) = \frac{63-3}{2} = 30$

$f(51) = \frac{51-3}{2} = 24$

$f(29) = \frac{29-3}{2} = 13$

$f(41) = \frac{41-3}{2} = 19$

$f(53) = \frac{53-3}{2} = 25$

$f(49) = \frac{49-3}{2} = 23$

$f(39) = \frac{39-3}{2} = 18$

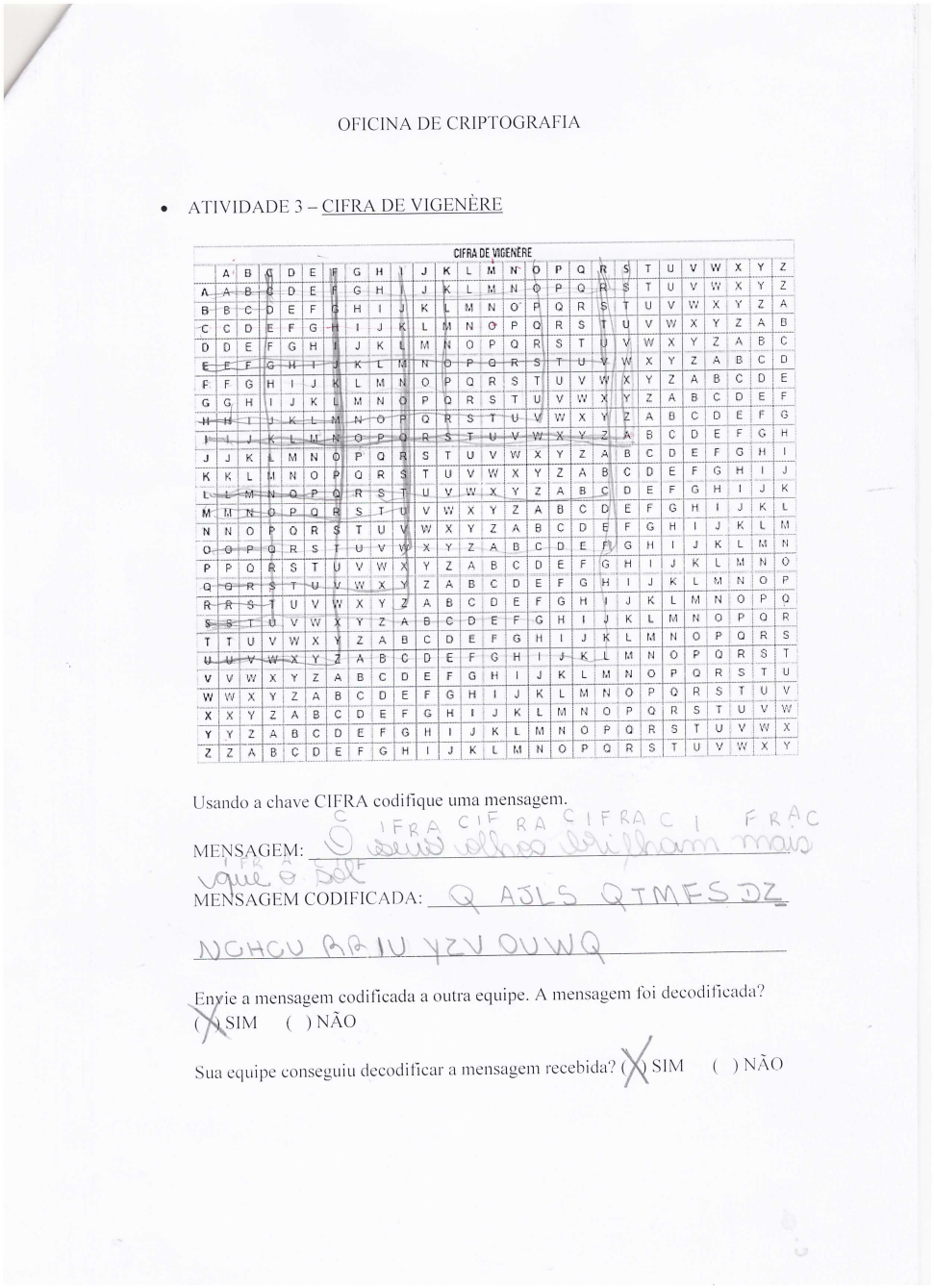
$f(31) = \frac{31-3}{2} = 14$

$f(71) = \frac{71-3}{2} = 34$

11 26 15 28 29 19 29 30 15 24 13 19 11 15 25
A P E R S I S T E N C I A E O

13 11 23 19 24 18 25 14 25 15 34 19 30 25
C A M I N H O D O E X I T O

Figura B.4: Atividade 2.3 - Funções.



OFICINA DE CRIPTOGRAFIA

- ATIVIDADE 3 – CIFRA DE VIGENÈRE

CIFRA DE VIGENÈRE

	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
A	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
B	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
C	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
D	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
E	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
F	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
G	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Usando a chave CIFRA codifique uma mensagem.

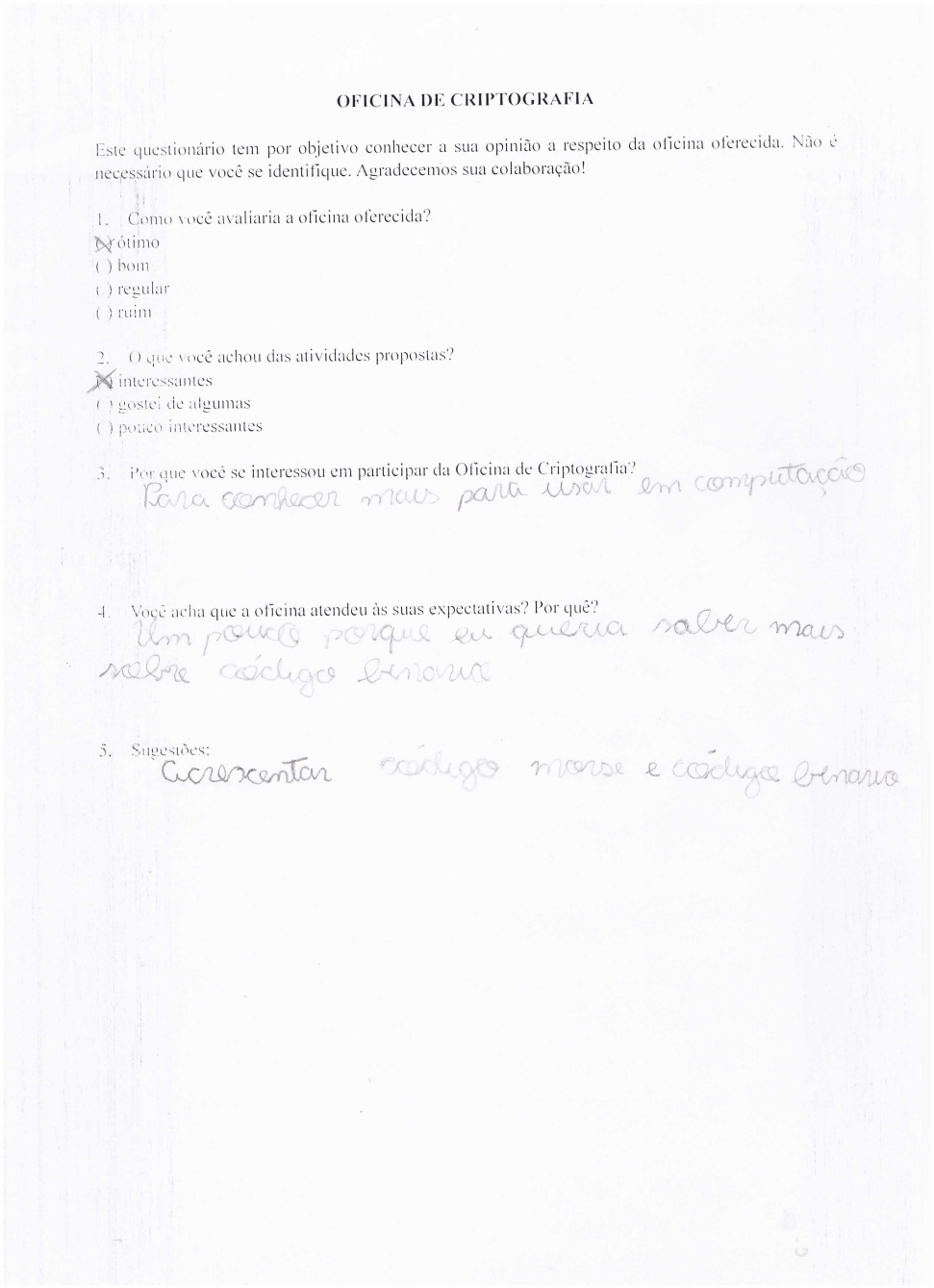
MENSAGEM: O seus olhos brilham mais que o Sol

MENSAGEM CODIFICADA: Q AJLS QTMFSDZ NGHCU RRIU YZV OUWQ

Envie a mensagem codificada a outra equipe. A mensagem foi decodificada?
(X) SIM ( ) NÃO

Sua equipe conseguiu decodificar a mensagem recebida? (X) SIM ( ) NÃO

Figura B.5: Atividade 3 - Cifra de Vigenère.



OFICINA DE CRIPTOGRAFIA

Este questionário tem por objetivo conhecer a sua opinião a respeito da oficina oferecida. Não é necessário que você se identifique. Agradecemos sua colaboração!

1. Como você avaliaria a oficina oferecida?
(X) ótimo
( ) bom
( ) regular
( ) ruim

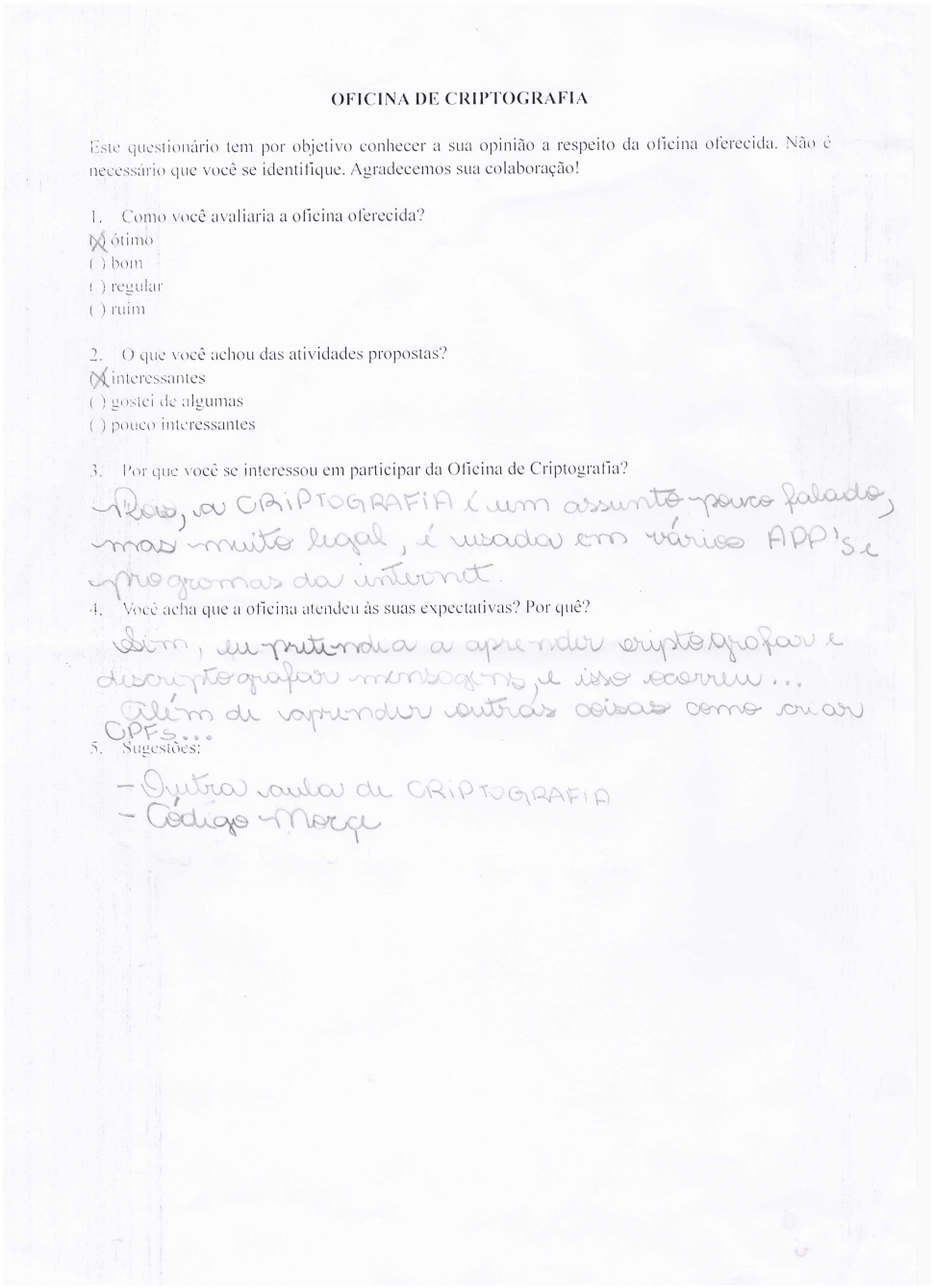
2. O que você achou das atividades propostas?
(X) interessantes
( ) gostei de algumas
( ) pouco interessantes

3. Por que você se interessou em participar da Oficina de Criptografia?
Para conhecer mais para usar em computação

4. Você acha que a oficina atendeu às suas expectativas? Por quê?
Um pouco porque eu queria saber mais sobre código binário

5. Sugestões:
Acrescentar código morse e código binário

Figura B.6: Questionário de Reação.



OFICINA DE CRIPTOGRAFIA

Este questionário tem por objetivo conhecer a sua opinião a respeito da oficina oferecida. Não é necessário que você se identifique. Agradecemos sua colaboração!

1. Como você avaliaria a oficina oferecida?
(X) ótimo
( ) bom
( ) regular
( ) ruim

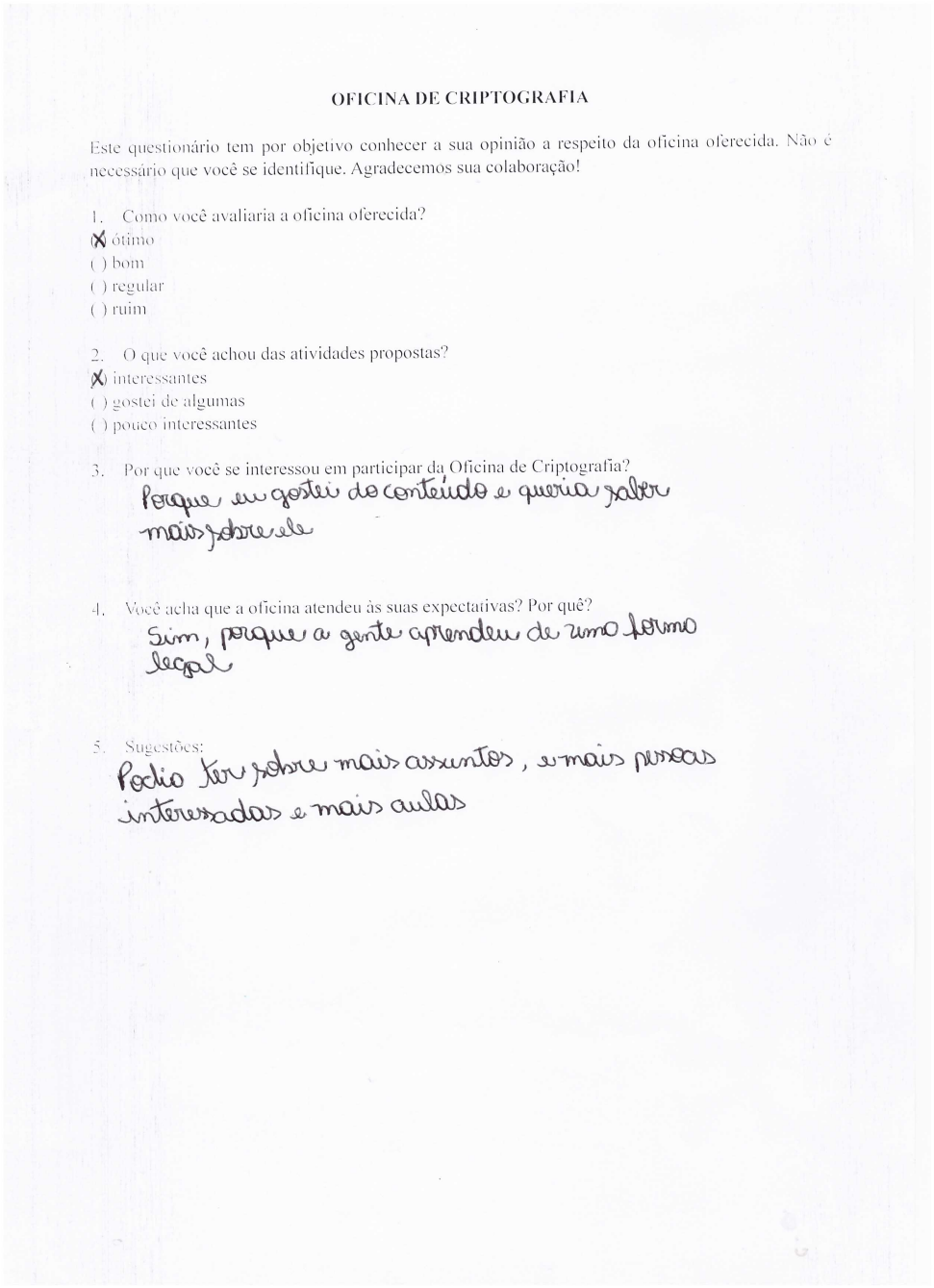
2. O que você achou das atividades propostas?
(X) interessantes
( ) gostei de algumas
( ) pouco interessantes

3. Por que você se interessou em participar da Oficina de Criptografia?
Pois, a CRIPTOGRAFIA é um assunto pouco falado, mas muito legal, é usada em vários APP's e programas da internet.

4. Você acha que a oficina atendeu às suas expectativas? Por quê?
Sim, eu pretendia a aprender criptografar e descriptografar mensagens, e isso ocorreu... Além de aprender outras coisas como criar OPF's...

5. Sugestões:
- Outra aula de CRIPTOGRAFIA
- Código Morse

Figura B.7: Questionário de Reação.



OFICINA DE CRIPTOGRAFIA

Este questionário tem por objetivo conhecer a sua opinião a respeito da oficina oferecida. Não é necessário que você se identifique. Agradecemos sua colaboração!

1. Como você avaliaria a oficina oferecida?
(X) ótimo
( ) bom
( ) regular
( ) ruim

2. O que você achou das atividades propostas?
(X) interessantes
( ) gostei de algumas
( ) pouco interessantes

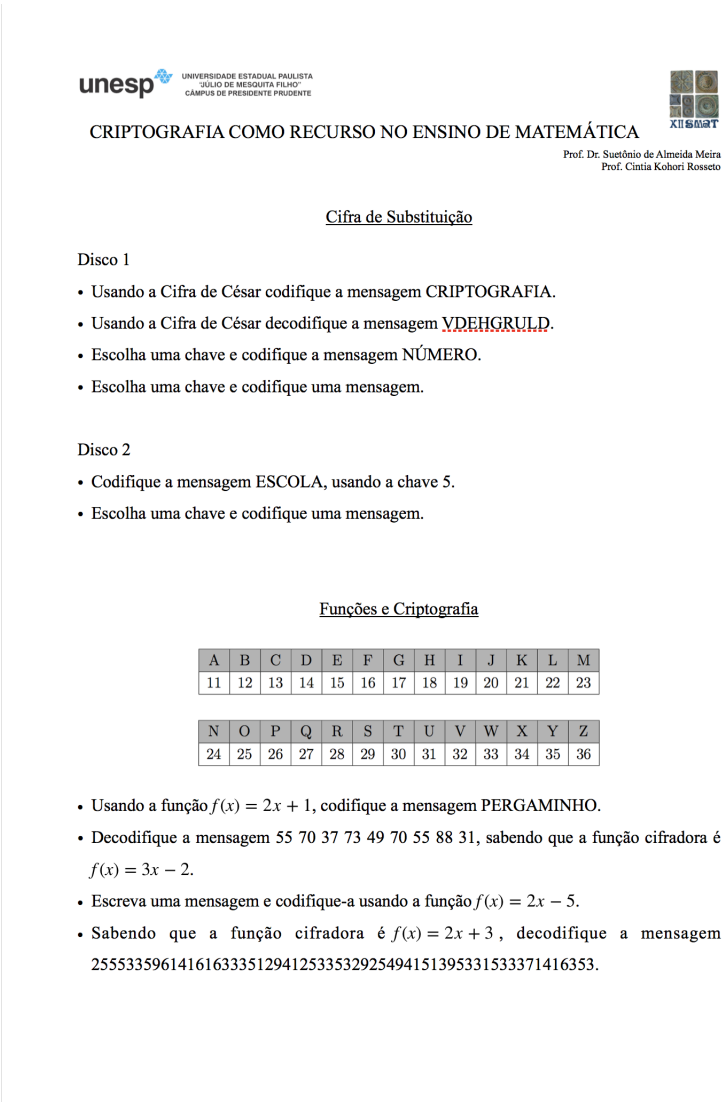
3. Por que você se interessou em participar da Oficina de Criptografia?
Porque eu gostei do conteúdo e queria saber mais sobre ele

4. Você acha que a oficina atendeu às suas expectativas? Por quê?
Sim, porque a gente aprendeu de uma forma legal

5. Sugestões:
Podia ter sobre mais assuntos, e mais pessoas interessadas e mais aulas

Figura B.8: Questionário de Reação.

C Apêndice C - Minicurso: Criptografia Como Recurso no Ensino de Matemática



unesp UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO" CÂMPUS DE PRESIDENTE PRUDENTE

CRIPTOGRAFIA COMO RECURSO NO ENSINO DE MATEMÁTICA

Prof. Dr. Suetônio de Almeida Meira
Prof. Cintia Kohori Rosseto

Cifra de Substituição

Disco 1

- Usando a Cifra de César codifique a mensagem CRIPTOGRAFIA.
- Usando a Cifra de César decodifique a mensagem VDEHGRULD.
- Escolha uma chave e codifique a mensagem NÚMERO.
- Escolha uma chave e codifique uma mensagem.

Disco 2

- Codifique a mensagem ESCOLA, usando a chave 5.
- Escolha uma chave e codifique uma mensagem.

Funções e Criptografia

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

- Usando a função $f(x) = 2x + 1$, codifique a mensagem PERGAMINHO.
- Decodifique a mensagem 55 70 37 73 49 70 55 88 31, sabendo que a função cifradora é $f(x) = 3x - 2$.
- Escreva uma mensagem e codifique-a usando a função $f(x) = 2x - 5$.
- Sabendo que a função cifradora é $f(x) = 2x + 3$, decodifique a mensagem 25553359614161633351294125335329254941513953315333714163 53.

Figura C.1: Atividade 1 - Cifra de Substituição e Funções.

unesp UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO" CÂMPUS DE PRESIDENTE PRUDENTE

XII SNMAT

CRIPTOGRAFIA COMO RECURSO NO ENSINO DE MATEMÁTICA

Prof. Dr. Suetônio de Almeida Meira
Prof. Cintia Kohori Rosseto

Cifras de Hill

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

- Usando a cifra de classe 2 $A=\begin{bmatrix} 2 & 3 \\ 1 & 5 \end{bmatrix}$, codifique a mensagem BOM DIA AMIGO SOL.
- Sabendo que a matriz cifradora é $A = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$, decodifique a mensagem LUYSIUUPCJKAID.

CPF

O número de inscrição no CPF é composto de onze dígitos decimais, sendo os oito primeiros aleatoriamente designados no momento da inscrição. Já o nono dígito indica a região fiscal responsável pela inscrição. Por fim, o décimo e o décimo-primeiro são dígitos verificadores calculados de acordo com um algoritmo definido pela Receita Federal.

Cálculo de C_1: Cada um dos nove algarismos, a partir da direita é multiplicado sucessivamente por 2, 3, 4, 5, 6, 7, 8, 9, 10 e os produtos resultantes são somados. A soma obtida é então dividida por 11 e C_1 será o quanto falta para 11 do resto desta divisão.

Cálculo de C_2: Cada um dos dez algarismos, a partir da direita, é multiplicado sucessivamente por 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 e os produtos resultantes são somados. O número C_2 é obtido então de maneira análoga a C_1.

- Calcule os dígitos de controle C_1 e C_2 para o seguinte CPF:

$$357.321.189 - C_1C_2$$

- Verifique se o CPF 123.456.785-78 é válido.

Figura C.2: Atividade 1 - Cifra de Hill e CPF.

unesp UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO" CÂMPUS DE PRESIDENTE PRUDENTE

XII SMaT

CRIPTOGRAFIA COMO RECURSO NO ENSINO DE MATEMÁTICA

Prof. Dr. Suetônio de Almeida Meira
Prof. Cintia Kohori Rosseto

Cifra de Vigenère

CIFRA DE VIGENÈRE

	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
A	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
B	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
C	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
D	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
E	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
F	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
G	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

- Usando a chave DIA codifique a mensagem VAMOS ESTUDAR.
- Usando a chave VIDA decodifique a mensagem VUDTZUDTDKDNVWPEIBH.
- Usando a chave CIFRA codifique uma mensagem.

Figura C.3: Atividade 1 - Cifra de Vigenère.

unesp UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO" CÂMPUS DE PRESIDENTE PRUDENTE

XII SMaT

CRIPTOGRAFIA COMO RECURSO NO ENSINO DE MATEMÁTICA

Prof. Dr. Suetônio de Almeida Meira
Prof. Cintia Kohori Rosseto

Cifra ADFGVX

	A	D	F	G	V	X
A	J	W	C	V	N	P
D	B	L	Z	I	3	F
F	Q	0	A	8	R	6
G	1	M	4	S	7	T
V	H	5	K	X	D	9
X	U	E	Y	O	2	G

Usando a palavra-chave LAR, codifique a mensagem BEM VINDOS.

Figura C.4: Atividade 1 - Cifra ADFGVX.

unesp UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO" CÂMPUS DE PRESIDENTE PRUDENTE

XII SNMAT

CRIPTOGRAFIA COMO RECURSO NO ENSINO DE MATEMÁTICA

Prof. Dr. Suetônio de Almeida Meira
Prof. Cintia Kohori Rosseto

RSA

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Codifique a mensagem RSA sabendo que os parâmetros são $p = 5$ e $q = 11$, e $\lambda = 3$.

Regra para codificar: $b^{\lambda} \equiv a(mod \quad n)$

Chave de codificação: $n = pq$

Pré-codificação:

Mensagem codificada:

Figura C.5: Atividade 1 - RSA.

unesp UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO" CÂMPUS DE PRESIDENTE PRUDENTE

XII SMAT

CRIPTOGRAFIA COMO RECURSO NO ENSINO DE MATEMÁTICA

Prof. Dr. Suetônio de Almeida Meira
Prof. Cintia Kohori Rosseto

Este questionário tem por objetivo conhecer a sua opinião a respeito do minicurso oferecido. Não é necessário que você se identifique. Agradecemos sua colaboração!

1. Como você avaliaria o minicurso oferecido?
(X) ótimo
( ) bom
( ) regular
( ) ruim

2. O que você achou das atividades propostas?
(X) interessantes
( ) gostei de algumas
( ) pouco interessantes

3. Por que você se interessou por este minicurso?
Me interesso muito por esse assunto, e fiquei curiosa em como poderia incluí-lo na sala de aula.

4. Você acha que o minicurso atendeu às suas expectativas? Por quê?
Sim. Eu aprendi muita coisa em tão pouco tempo, as aulas foram práticas e as atividades muito bem elaboradas.

5. Sugestões:
Gostaria que tivesse durado mais, foi muito bom!

Figura C.6: Questionário de Reaçãoo.

unesp UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO" CÂMPUS DE PRESIDENTE PRUDENTE

XII SMAT

CRIPTOGRAFIA COMO RECURSO NO ENSINO DE MATEMÁTICA

Prof. Dr. Suetônio de Almeida Meira
Prof. Cintia Kohori Rosseto

Este questionário tem por objetivo conhecer a sua opinião a respeito do minicurso oferecido. Não é necessário que você se identifique. Agradecemos sua colaboração!

1. Como você avaliaria o minicurso oferecido?
(X) ótimo
( ) bom
( ) regular
( ) ruim

2. O que você achou das atividades propostas?
(X) interessantes
( ) gostei de algumas
( ) pouco interessantes

3. Por que você se interessou por este minicurso?
Adoro o assunto relacionado a criptografia, cifras, mensagens ocultas

4. Você acha que o minicurso atendeu às suas expectativas? Por quê?
Sim, inclusive superou minhas expectativas. Aprendi cifras das quais nunca tinha ouvido falar antes.

5. Sugestões: não possuo sugestoes

Figura C.7: Questionário de Reação.

unesp UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO" CÂMPUS DE PRESIDENTE PRUDENTE

XII SNaT

CRIPTOGRAFIA COMO RECURSO NO ENSINO DE MATEMÁTICA

Prof. Dr. Suetônio de Almeida Meira
Prof. Cintia Kohori Rosseto

Este questionário tem por objetivo conhecer a sua opinião a respeito do minicurso oferecido. Não é necessário que você se identifique. Agradecemos sua colaboração!

1. Como você avaliaria o minicurso oferecido?
(x) ótimo
( ) bom
( ) regular
( ) ruim

2. O que você achou das atividades propostas?
(x) interessantes
( ) gostei de algumas
( ) pouco interessantes

3. Por que você se interessou por este minicurso?
Me interessei pela temática do minicurso pois tinha a proposta de uma intervenção de conteúdo que motivaria os alunos, fazendo com que eles se interessassem um pouco mais pela matemática.

4. Você acha que o minicurso atendeu às suas expectativas? Por quê?
Atendeu, pois deu para ter uma visão de conteúdo dinâmico onde eu mesma tive a vontade de aplicá-lo em turmas futuras.

5. Sugestões:
O tempo do minicurso foi muito curto, isto não se deu por uma ma administração de tempo, mas por algo cronológico mesmo, creio se fosse maior conseguiriamos trabalhar mais as atividades, além de tentativas de dinamizar as aulas.

Figura C.8: Questionário de Reação.