unesp UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
CAMPUS DE GUARATINGUETÁ

ANA FLÁVIA CESÁRIO MACHADO ALCKMIN NOGUEIRA

Proposta de atividades usando Criptografia nas aulas de Matemáticas

Guaratinguetá - SP
2017

Ana Flávia Cesário Machado Alckmin Nogueira

Proposta de atividades usando Criptografia nas aulas de Matemáticas

Trabalho de Graduação apresentado ao Conselho de Curso de Graduação em Licenciatura em Matemática da Faculdade de Engenharia do Campus de Guaratinguetá, Universidade Estadual Paulista, como parte dos requisitos para obtenção do diploma de Graduação em Licenciatura em Matemática.

Orientadora: Profª Drª Ana Paula Marins Chiaradia

Guaratinguetá - SP
2017

Nogueira, Ana Flávia Cesário Machado Alckmin
N778p Proposta de atividades usando criptografia nas aulas de matemática / Ana Flávia Cesário Machado Alckmin – Guaratinguetá, 2017.
94 f. : il.
Bibliografia: f. 91-94

Trabalho de Graduação em Licenciatura em Matemática – Universidade Estadual Paulista, Faculdade de Engenharia de Guaratinguetá, 2017.
Orientadora: Profª Drª Ana Paula Marins Chiaradia

1. Criptografia. 2. Matemática – Estudo e ensino. 3. Educação básica. I. Título

CDU 51

Luciana Máximo
Bibliotecária/CRB-8 3595

unesp UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
CAMPUS DE GUARATINGUETÁ

ANA FLÁVIA CESÁRIO MACHADO ALCKMIN NOGUEIRA

ESTE TRABALHO DE GRADUAÇÃO FOI JULGADO ADEQUADO COMO PARTE DO REQUISITO PARA A OBTENÇÃO DO DIPLOMA DE **"GRADUADO EM LICENCIATURA EM MATEMÁTICA"**

APROVADO EM SUA FORMA FINAL PELO CONSELHO DE CURSO DE GRADUAÇÃO EM LICENCIATURA EM MATEMÁTICA

Profª. Drª. Silvia Maria Giuliatti Winter
Coordenadora

BANCA EXAMINADORA:

Profª. Drª. ANA PAULA MARINS CHIARADIA
Orientadora/UNESP-FEG

Profª. Drª Silvia Maria Giuliatti Winter
UNESP-FEG

Prof. Dr. Rafael Sfair de Oliveira
UNESP-FEG

Outubro de 2017

Outubro de 2017

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus, fonte da vida e da graça. Agradeço pela minha vida, pelos meus estudos, minha família e meus amigos.

A minha orientadora, *Profª. Drª. Ana Paula Marins Chiaradia*. Sem a sua orientação, dedicação e auxílio, o estudo aqui apresentado não seria o mesmo.

Aos meus pais *Renato e Gigrielli*, que apesar das dificuldades enfrentadas, sempre incentivaram meus estudos, me apoiaram em todas as decisões, acreditaram em mim, e estiveram presentes em minha vida dando muito amor.

Ao meu irmão *Júnior* que com sua serenidade muitas vezes me tranquilizou.

Ao meu namorado *William* que sempre me apoiou.

Aos funcionários da Biblioteca do Campus de Guaratinguetá pela dedicação, presteza e principalmente pela vontade de ajudar.

Aos funcionários da Faculdade de Engenharia do Campus de Guaratinguetá pela dedicação e alegria no atendimento.

A todos que direta ou indiretamente contribuíram para a elaboração deste trabalho.

“A Matemática é a rainha das Ciências e a Teoria dos Números é a rainha das Matemáticas”.

K. F. Gauss

RESUMO

O presente trabalho visa estudar a relação entre a Matemática e a Criptografia, para isso são apresentados conteúdos matemáticos necessários para compreensão dos métodos criptográficos, a descrição desses métodos, e *software* e aplicativos que podem ser aplicados em sala de aula para alunos tanto do Ensino Fundamental II quanto do Ensino Médio. Os métodos aqui estudados são: a Cifra de César, a Cifra de Vigenère, a Cifra de Hill, a máquina Enigma e o método RSA, que são os mais utilizados e conhecidos. Primeiramente é apresentada a definição e a história do desenvolvimento da Criptografia, em seguida são apresentados conceitos matemáticos importantes para o entendimento do funcionamento dos métodos, a descrição dos métodos e por fim *software* e aplicativos que podem ser aplicados na Educação Básica.

PALAVRAS-CHAVE: Criptografia. Cifra de César. Cifra de Vigenère. Criptografia RSA. Educação Básica.

ABSTRACT

This paper has as objective to study the relations between Mathematics and Cryptography, to achieve this goal, we present mathematical contents necessary to understand the cryptographic methods, the description of these methods, and software and applications that can be applied in the classroom for students of both Elementary School II and High School. The methods studied here are: Caesar Cipher, Vigenère Cipher, Hill Cipher, Enigma machine and RSA method, which are the most widely used and known. Firstly, the definition and history of the development of Cryptography are presented, and important mathematical concepts are presented for the understanding of the methods functioning, the description of the methods and finally software and applications that can be applied in Elementary School.

KEYWORDS: Cryptography. Caesar Cipher. Vigenère Cipher. Cryptography RSA. Elementary School.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

O tema proposto, a utilização da Criptografia, além de estar diretamente relacionado com a Matemática, é fundamental em toda a história da humanidade, sendo praticado e aprimorado desde a antiguidade até a atualidade. A necessidade de guardar segredos, assim como o desejo de desvendá-los, acompanha o homem desde os primórdios da sociedade.

Ao longo do tempo, foram desenvolvidos diversos modos de manter o sigilo de uma mensagem quando interceptada por um terceiro indivíduo. As maneiras de escrever uma mensagem incompreensível a um interceptador foram se aprimorando ao longo dos anos, passando por diversas modificações até chegar à que se tem atualmente. A ciência responsável pelo desenvolvimento de processos para transmissão de mensagens secretas, ou seja, que nem todos consigam ler denomina-se Criptografia. Utilizar códigos consiste na substituição de uma palavra ou frase por outra palavra. Uma outra técnica também utilizada para se manter o sigilo de um determinado conteúdo é Esteganografia, que abrange estudos referentes à ocultação de uma mensagem. É importante ressaltar que a Criptografia oculta o significado da mensagem, mas não a mensagem em si, enquanto a Esteganografia oculta a existência da mensagem.

Embora não se saiba ao certo como e onde surgiu a Criptografia, existem alguns registros históricos que apontam o quão antiga é essa ciência. Segundo Fiarresga (2010), o primeiro relato documentado da utilização da arte de ocultar informações na escrita de cerca 1900 a.C. numa vila Egípcia, a estratégia presente no documento era a de códigos, algumas palavras e trechos foram substituídos por outros. Uma maneira de enviar uma mensagem a uma pessoa sem que o texto seja compreensível a qualquer um que tente interceptar a mensagem é através da utilização de códigos.

Cerca de 200 a.C., o grego Políbio desenvolveu uma tabela 5×5, conhecida atualmente por quadrado de Políbio (Tabela 1), baseavam-se nela para escrever a mensagem criptografada. Esta tabela utilizava a cifra de substituição, a qual consiste na substituição de uma letra por outra. Para se criptografar uma mensagem utilizando ao quadrado de Políbio, localiza-se a letra que se deseja cifrar na tabela e deve-se substituí-la pela letra da linha e da coluna correspondente, nessa ordem. Por exemplo, ao cifrar a palavra ANO tem-se a sequência AACCCD. Têm-se também registros da criptografia mais conhecida da idade

antiga, uma cifra de substituição utilizada pelo imperador romano Júlio César por volta de 100 a.C. que ficou mais tarde conhecida como Cifra de César (MATSUMOTO, 2014).

Tabela 1 – Quadrado de Políbio

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

Fonte: Fiarresga (2010)

Juntamente com todo desenvolvimento da sociedade desenvolveu-se também outras técnicas de cifragem, mais seguras e mais sofisticadas. A Matemática é a principal base dessa evolução, sendo que quanto mais avançada é a cifra, mais é necessário um aprofundamento matemático para sua compreensão. O principal ramo da matemática utilizado na Criptografia é a teoria dos números, mas deve-se ressaltar também a importância do estudo de matrizes e sistemas lineares, o que implica na importância da álgebra linear (GODINHO et. al. 2011).

Apesar de os números primos serem conhecidos e estudados há mais de 2000 anos, ainda existem muitas questões sem respostas. Até a metade do século XX acreditava-se que os primos não tivessem utilidade prática (FIARRESGA, 2010). Contudo, juntamente com a evolução da época, o alemão Arthur Scherbius formado em engenharia elétrica desenvolveu uma máquina de cifragem usando rotores, máquina mecânica utilizada para encriptação de mensagens, posteriormente reconhecida como a máquina Enigma, uma versão elétrica do disco de Alberti. (MARQUES, 2013). Leon Battista Alberti (1404-1472) de origem italiana o precursor da criação da cifra poli alfabética. Alberti foi pintor, compositor, poeta e filósofo, por volta de 1640 escreveu um ensaio sobre Criptografia, sugerindo a utilização de mais de um alfabeto para cifragem sendo utilizados alternadamente (SINHG, 2004). Portanto, a Criptografia também teve grande evolução, foi então que surgiu a impossibilidade de decifrar uma mensagem somente com o esforço humano quando esta possuía muitas configurações. Após a quebra do código da máquina enigma, começaram a ser desenvolvidos os

computadores e, juntamente com eles, a criptografia computacional. Foi então que surgiu uma grande utilidade prática dos números primos. Principalmente pela sua utilização na criptografia, os estudos sobre esse conjunto vêm crescendo muito nos últimos anos. Embora existam muitas questões ainda não respondidas, o que se sabe é suficiente para se obter um resultado eficaz de sua utilização. Na prática é essa falta de conhecimento que torna o método atual eficiente, isso será mais bem compreendido com o conhecimento da principal cifra utilizada atualmente, a Criptografia RSA, que será apresentada no Capítulo 5 (MARQUES, 2013).

> De fato, este estudo cobre bem mais do que cifragem e decifragem, é um ramo especializado da teoria da informação com muitas contribuições de outros campos da matemática e do conhecimento científico (GODINHO, et. al, 2011, p.27)

Portanto, o trabalho tem como objetivo estudar conceitos e métodos da Criptografia, ou seja, busca a compreensão do que é e como é usada a criptografia, sendo o principal objetivo compreender a relação da matemática com os processos citados e o quão fundamental é a matemática para o desenvolvimento de tal ciência, a Criptografia. Consequentemente tem também como objetivo o estudo da teoria dos números, o qual é a base para o desenvolvimento e compreensão do conceito.

Com o crescente desenvolvimento da tecnologia seu uso está cada vez mais presente na vida de todos, de inúmeras maneiras, em diversas situações. A maioria dos adolescentes possui grande facilidade em manipular aparelhos eletrônicos e digitais, pois desde cedo são apresentados a esses aparelhos e, naturalmente, os exploram e os utilizam. Portanto, é necessário que as escolas acompanhem esse desenvolvimento, sendo assim utilizem novas tecnologias, caso contrário, as escolas tornar-se-ão ultrapassadas. É inevitável a utilização de novas tecnologias, portanto é necessário que haja uma reflexão sobre os modos de se trabalhar em sala de aula para que sejam utilizadas da melhor maneira possível. É preciso que haja estudos e planejamentos para que se trabalhe de maneira adequada. As ferramentas utilizadas devem trazer benefícios para a aprendizagem e não problemas (GOMES et al., 2016).

Apesar de todo avanço tecnológico apresentado na sociedade, trabalhar com novas tecnologias de informação e comunicação ainda é um desafio para algumas escolas e professores. Entretanto a necessidade dessas ferramentas serem trabalhadas nas escolas vem aumento, principalmente devido sua crescente utilização em diversas situações diárias. Esse

recurso pode trazer benefícios no processo ensino-aprendizagem, como por exemplo, a quantidade de informações disponíveis na internet, mídias, *softwares* e aplicativos podem auxiliar na aprendizagem quando exploradas corretamente.

Existe uma polêmica quanto ao uso de celulares e *tablets* em sala de aula, visto que muitos professores considerarem um problema o uso desses aparelhos no ambiente acadêmico, é importante ressaltar que devem haver limites para que não haja má utilização. É indiscutível que uma boa utilização traz benefícios. A utilização do celular em sala de aula constitui uma ferramenta pedagógica interessante, quando bem desenvolvida, pois estimula o interesse pelo assunto e é um modo de tornar a aula interativa. Por isso os professores precisam conseguir atenção e foco dos alunos, além de criar um ambiente interativo e enriquecedor (GOMES et al., 2016).

Com tanta informação de fácil acesso não há mais a visão de que o professor é o detentor de todo conhecimento, e é preciso que o professor se adeque a esse novo quadro. É importante que o professor busque se atualizar não apenas dentro de sua especialidade, mas também dentro das tecnologias que podem auxiliar sua prática pedagógica (OLIVEIRA et al., 2017).

Trata-se de uma pesquisa qualitativa visto que foram feitos levantamento de dados sobre o tema para buscar melhor compreendê-lo, e aprofundar conhecimentos.

O trabalho está estruturado da seguinte forma, no Capítulo 2 são apresentados resumos de artigos relacionados a Criptografia que foram utilizados como base. No Capítulo 3 é discorrido sobre a história, o surgimento e o desenvolvimento dos principais métodos criptográficos. Já no capítulo seguinte são apresentados os principais resultados matemáticos necessários para a compreensão dos métodos aqui descritos. No Capítulo 5 são comentados detalhadamente os principais métodos criptográficos utilizados desde seu surgimento até os dias atuais. No capítulo 6 são apresentados alguns softwares e aplicativos de Criptografia, ferramentas que são sugeridas como iniciativa de se introduzir o tema em sala de aula utilizando novas tecnologias. E por fim são apresentadas as conclusões e sugestões de trabalhos futuros.

Sendo de conhecimento geral a dificuldade de despertar interesse e motivar alunos quando se trata de Matemática, no Capítulo 6 é apresentada uma proposta de atividades que

podem ser aplicadas para turmas do Ensino Fundamental II e Ensino Médio, visando levar aos alunos história, conteúdos matemáticos e aplicabilidade dos processos através de atividades que usam novas tecnologias.

2 REVISÃO DA LITERATURA

Este capítulo apresenta uma revisão da literatura acerca do tema Criptografia. Alguns textos abordaram a história da Criptografia e fizeram uma descrição de diversos métodos criptográficos, nos quais a Matemática se faz presente por meio da teoria dos números ou álgebra linear. Foram também estudados textos que abordam o ensino da Criptografia.

Podem-se encontrar trabalhos na Literatura que utilizam a Criptografia de forma simples para ensinar Matemática na Educação Básica.

Baseado em sua experiência como professor, Borges (2008) ressalta que a maioria dos alunos não tem atenção quando se trata de abstração ou generalização e reconhece a dificuldade encontrada pelo professor de mostrar aplicações de certos conteúdos, visto que muitas aplicações exigem um nível elevado de conhecimento matemático para sua compreensão plena. Contudo, torna-se fácil quando se trata de Criptografia como estratégia para despertar curiosidade e aguçar a imaginação, sendo que conteúdos elementares de Matemática são suficientes para uma boa introdução ao tema. O autor cita filmes relacionados à segurança da informação, apresenta de forma resumida a Cifra de César, também expõe a ideia sobre chaves assimétricas, método Diffie-Hellman e RSA. Ressalta a questão da segurança nos algoritmos. Apresenta também Criptografia com curvas elípticas.

O principal objetivo de Marques (2013) é de proporcionar ao professor conteúdo suficiente para que este possa preparar a sua aula de modo mais motivador. Ele acredita que criptografia é um assunto extremamente importante nos dias atuais. Primeiramente, é apresentada a definição de Criptografia e como se deu sua evolução ao longo da história da humanidade. E é apresentado o problema da troca de chaves, criptografia simétrica e a assimétrica, conteúdos matemáticos importantes para compreensão dos algoritmos, a importância do logaritmo discreto na troca de chaves de Diffie- Hellman, e, por último, atividades para serem aplicadas em sala de aula.

Matsumoto (2014) acredita que apresentar a história da Criptografia, sua aplicabilidade e sua ligação com a Matemática pode despertar nos alunos um maior interesse e também uma reflexão sobre a grande importância da Matemática. Ela acredita que a motivação norteia nosso aprendizado, em vista disso foram elaboradas e aplicadas algumas atividades

diferenciadas daquelas habitualmente trabalhadas, e por fim foi feita a análise dos resultados obtidos.

Para o desenvolvimento de seu trabalho, Castro (2014) discorre sobre aspectos da criptografia do ponto de vista histórico e funcional, apresenta elementos matemáticos necessários para sua compreensão, questões como o porquê da Criptografia funcionar e o porquê de ela realmente ser segura. O texto é voltado para professores, espera-se que sirva como um estímulo aos mesmos para trabalharem em sala de aula com seus alunos.

Em Ganassoli e Schankoski (2015) é feita breve história sobre a Criptografia, os principais códigos, cifras e a Criptografia utilizada pelo homem até a atualidade. Faz um breve estudo sobre a aritmética modular, principal ferramenta utilizada hoje para criptografar de forma segura e eficaz no método RSA, situando historicamente e descrevendo sua implementação. A partir disto, fazem uma sugestão de várias atividades, para serem aplicadas com alunos a partir do 6º ano do Ensino Fundamental II até a 3ª série do Ensino Médio, que englobam diversos conteúdos de matemática, análise combinatória, matrizes, funções, divisão, e algumas atividades de aritmética modular e RSA.

A seguir são apresentados trabalhos que relacionam a Criptografia com as áreas da Matemática como álgebra linear e teoria dos números.

Pinto (2005) apresenta a história dos números primos, mostra a argumentação de Euclides para provar que o conjunto dos números primos é infinito, e apresentas algumas utilidades de tal conceito ao longo da história e na atualidade. Ele faz alguns questionamentos sobre o ensino dos números primos e o que aconteceria se tivesse uma fórmula matemática que gerasse todos os números primos. Discute o que é proposto nos PCNs em relação ao ensino dos números primos no ensino fundamental e analisa alguns livros didáticos sobre os assuntos comparando com o que é proposto pelos PCNs.

Da Silva (2006) fez um levantamento de dados em livros e artigos sobre a Criptografia RSA, e discorreu sobre seu surgimento, desenvolvimento, detalhamento do método e aplicabilidade. Ressaltando que a teoria dos números e a teoria da complexidade algorítmica são os dois principais ramos da Matemática relacionados à Criptografia, em que o primeiro se volta para conceitos e elaboração dos métodos, o segundo está relacionado à eficiência dos métodos, como tempo e custos operacionais.

Segundo Godinho (2011) é comum associar a Criptografia à teoria dos números, pois grande parte dos algoritmos desenvolvidos a utilizam como a principal base matemática necessária. Contudo, ao que se refere à Matemática utilizada na Criptografia é válido ressaltar a importância da álgebra linear. Uma técnica também utilizada para codificar e decodificar mensagens é a eliminação Gaussiana. Além de ser objeto de estudo da Matemática e Computação, a álgebra linear abrange também a teoria da comunicação.

Jesus (2013) discorre sobre o tema Criptografia, apresentando conceitos, nomenclaturas, história e desenvolvimento ao longo dos anos, dando destaque as principais ocasiões em que foi utilizada. Devido à importância da Matemática para a elaboração dos métodos, são apresentados alguns resultados, com enfoque em matrizes e aritmética modular. Para concluir o trabalho são apresentados problemas para alunos do Ensino Médio.

Em Oliveira (2013) o trabalho é voltado para auxiliar o planejamento das aulas de professores do Ensino Médio. Primeiramente são apresentados tópicos de Teoria dos Números, voltado principalmente a Aritmética Modular, equações diofantinas, e Criptografia. Posteriormente são apresentadas quatro aplicações de aritmética modular. Além disto, apresenta o uso do software Microsoft Excel®.

A seguir são apresentados alguns trabalhos que tratam dos métodos criptográficos de forma mais simples que possam ser usados para um estudo inicial.

Andrade e Silva (2012) buscaram avaliar a relação entre a velocidade do processo de codificação e decodificação de Criptografia RSA e a segurança de informações. Visto que a segurança das informações codificadas pela Criptografia RSA está na dificuldade de se encontrar a chave de decodificação, o que é calculado através da fatoração de um número n, quando este possui grande quantidade de dígitos torna-se um processo impraticável, porém aumenta-se também o tempo gasto para codificar a informação. O processo foi simulado utilizando chaves aleatórias de 1024, 2048 e 4096 bits. Concluiram que o aumento do tamanho da chave provoca um aumento do tempo gasto para Criptografar.

O DES (*Data Encryption Standard*) é um método criptográfico de chave simétrica que surgiu na década de 70 e se tornou padrão no mundo durante pouco mais de 20 anos. Em 1997, visando garantir a segurança, foi iniciado um projeto que iria analisar diversos algoritmos e o vencedor iria substituir o algoritmo DES, sendo que este já não era mais

considerado seguro. Hinz (2000) dividiu seu trabalho em duas partes, na primeira delas é feita uma descrição do método DES e dos cinco algoritmos que foram para fase final do projeto, são eles MARS, RC6, Rijndael, Serpent e Twofish. Já na segunda parte é feito um estudo comparativo entre os seis algoritmos, analisando requisitos de memória, velocidade no processamento, complexidade computacional e funções criptográficas quanto à vantagens e desvantagens.

Cavalcanti (2002) realizou um estudo das propriedades criptográficas de uma sequência linear de terceira ordem sobre um corpo finito F_P. Assim como um algoritmo computacional para calcular o k-ésimo termo de uma sequência característica de ordem 3. Ao processo de codificação é possível associar uma função, sendo P a mensagem original e C a cifrada, *f:* P $\rightarrow$ C, tal que *f(u)=c*, em que *u* representa cada mensagem unitária de P e *c* cada mensagem unitária de C. E para a decodificação basta calcular a função inversa de *f*. Dois algoritmos são analisados: o GH-PKD, que é seguro devido à dificuldade de solucionar logaritmos discretos, e o RSA, cuja segurança baseia-se na dificuldade de fatorar um grande número inteiro composto em um produto de dois primos.

Freire (2007) fez algumas comparações entre métodos criptográficos com relação à Matemática necessária para seu desenvolvimento. Os métodos estudados foram: a Cifra de César, a Cifra de Vigenère, a máquina Enigma, o método RSA e o esquema Rafaela. Após ter sido apresentada uma breve contextualização histórica do surgimento e do desenvolvimento da Criptografia, foram descritos os criptossistemas.

3 DESENVOLVIMENTO DA CRIPTOGRAFIA

Sem dúvida um dos maiores progressos da humanidade foi o desenvolvimento da escrita. Tal criação nos trouxe uma melhor organização dos pensamentos, e consequentemente maior consciência sobre os fatos. Antes do surgimento da escrita todo conhecimento era transmitido oralmente, ou seja, pela fala, deste modo quando um rei queria comunicar algo a alguma pessoa, ou ele deveria se dirigir até essa pessoa ou enviar seu comunicado através de um terceiro indivíduo. Todo tipo de conhecimento e valores que uma geração havia desenvolvido ou pensado era transmitido a outras gerações pela fala. Este não era o melhor meio de transmissão, pois os ensinamentos poderiam ser esquecidos, confundidos, ou até mesmo não passados para outra geração. A escrita veio, por tanto, para garantir a transmissão de ensinamentos de maneira eficaz. Há mais de 4.000 anos tem-se a possibilidade de se transmitir conhecimento através de registros, os quais qualquer indivíduo alfabetizado na língua em questão é capaz de ler. Contudo, o surgimento da escrita não foi realizado de um dia para o outro, foi sendo desenvolvido aos poucos, e também assim, gradativamente todas as outras ciências tiveram seu surgimento (GOMES, 2007).

Juntamente com a evolução da escrita surgiu também a necessidade de manter o sigilo do conteúdo de mensagens. Então, se fossem utilizados os meios tradicionais de uma língua para escrever uma mensagem, como o alfabeto no caso da língua portuguesa, qualquer indivíduo que conhecesse a língua poderia interpretá-la. Foi então que se desenvolveu a ideia da escrita por códigos, a qual consiste na utilização de uma palavra ou frase para substituir uma palavra. O que motivou o desenvolvimento de códigos foi a ameaça do conteúdo de uma mensagem ser interceptada e lida por um inimigo. Com o tempo perceberam que seria possível avançar ainda mais nas comunicações. Foram desenvolvidas as cifras, que possuem a mesma ideia base do código, porém se diferem pelo fato das cifras substituírem cada letra de uma palavra por outra, não toda palavra ou frase por outra palavra.

Assim foi que surgiu a ciência responsável pela transmissão de mensagens sigilosas que é denominada Criptografia. A palavra Criptografia tem sua origem do grego “Kryptós =oculto” e “Graphien = ecrita”, portanto, significa escrita oculta (ou secreta).Veja a Figura 1 que é uma ilustração da definição de palavra Criptografia.

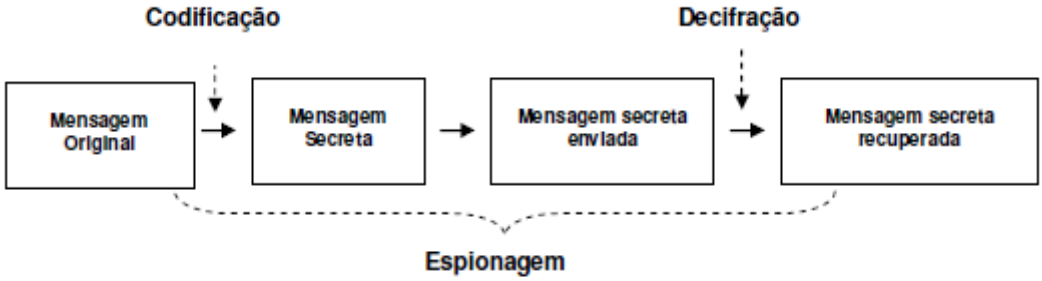
Figura 1 – Significado da palavra Criptografia

Fonte: Bezerra et. al. (2017)

A Criptografia visa a transmissão de mensagens restritas ao legítimo destinatário em meios não seguros, como por exemplo, a transmissão de mensagens de imperadores aos exércitos em meio às guerras na Idade Média e Moderna. Têm-se indícios das primeiras utilizações dessa ciência datados de antes de Cristo. A princípio era utilizada principalmente em assuntos militares e diplomáticos. Atualmente sua utilidade se estendeu para muitas outras áreas como a transmissão de mensagens pela internet, em geral qualquer atividade *online* que exija sigilo como fichas médicas em hospitais, atividades bancárias, tratamento e circulação de dados científicos (GODINHO et. al., 2011).

Para transmitir uma mensagem de texto de modo seguro, sem que uma pessoa qualquer seja capaz de ler, primeiramente deve ser feita a codificação (ou encriptação) do conteúdo, processo que transforma um texto que era compreensível a todos que conhecessem a língua em outro ilegível devido à utilização de símbolos diferentes. A mensagem estando escrita em códigos ou em cifras pode circular livremente em quaisquer meios, mesmo esse não sendo seguro, pois se espera que o único capaz de interpretar os códigos seja o legítimo receptor da mensagem, e para lê-la ele utilizará uma "chave" para decodificação da mensagem, processo inverso da codificação. Chave é um protocolo acordado entre o transmissor e o receptor. Decodificar (ou desencriptar) é o nome dado ao procedimento realizado pelo destinatário legítimo de uma mensagem para interpretá-la. Veja a Figura 2 que ilustra estas definições. Não se deve confundir decodificar com a palavra decifrar, já que decifrar é a denominação para a leitura de uma mensagem sem ser o legítimo destinatário, ou seja, decifrar é quebrar o código de cifração.

Figura 2 – Codificação e Decifração.



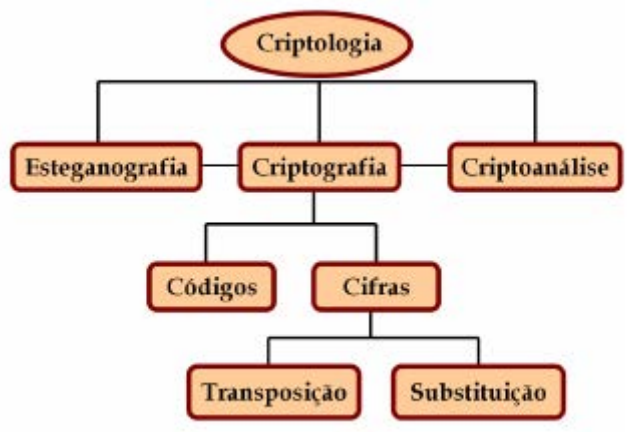
Fonte: Bezerra et. al. (2017)

Além da Criptografia, a Esteganografia estuda os métodos para esconder a existência da mensagem, como na área de segurança monetária, na autenticação de documentos, em imagens e nas gravações de música, filmes e outras.

Com o surgimento da Criptografia foram desenvolvidas também duas outras ciências: a Criptoanálise e a Criptologia. Enquanto a Criptografia preocupa-se com a transmissão segura de mensagens, a Criptoanálise possui como objeto de estudo as decifrações, ou seja, interpretar uma mensagem não sendo o legítimo destinatário. A Criptologia é a ciência que engloba as duas citadas anteriormente, a Criptografia e a Criptoanálise (HINZ, 2000).

Portanto, Criptografia é a ciência de escrever em cifras ou em códigos, tornando a mensagem incompreensível, permitindo apenas ao destinatário desejado decifrar ou decodificar a mensagem com clareza, utilizando a chave. Dois métodos são utilizados: transposição e substituição. A substituição é subdividida em outras duas técnicas: Código e Cifras (Figura 3). Historicamente a mais usada, a Cifra é uma técnica mais fundamental, em que as letras são substituídas no lugar de palavras. Enquanto, o Código envolve a substituição de uma palavra ou frase por uma outra palavra, um número ou um símbolo.

Figura 3 – Áreas da Criptologia



Fonte: Bezerra et. al. (2017)

> Embora ambos, criptografar e codificar, utilizam o método da substituição, então se pode usar simultaneamente as duas formas, o que torna aparentemente a mensagem mais segura, mas é um engano, pois a parte cifrada pode ser decifrada usando análise de frequência, e a parte codificada é decodificada deduzindo-se a partir do contexto (GANASSOLI e SHCHANKOSI, 2015).

Os métodos vêm evoluindo há mais de dois milênios, um algoritmo de cifração criado e considerado eficiente é utilizado por um determinado tempo suficientemente longo até que seja criado um método que consiga decifrar a mensagem, isto é, até que um terceiro indivíduo consiga ler o conteúdo da mensagem original. Então o algoritmo deixa de ser seguro, sendo assim o algoritmo não poderá mais ser usado, sendo a solução para transformar em um processo de cifração seguro novamente aprimorar o método existente ou deixar de usá-lo e desenvolver um novo algoritmo.

Portanto, todos os diferentes métodos de criptografia foram desenvolvidos e estudados ao longo do tempo, passando por diversas etapas até chegar aos métodos existentes atualmente. De modo mais generalizado a criptografia pode ser dividida em três grandes fases, são elas: a criptografia manual, a criptografia por máquinas e a criptografia computacional (ou em redes) (FRANÇA, 2005).

Utilizado na Idade Antiga, um dos registros mais antigos existentes de criptografia é o da Cifra de César.

Em meio as suas batalhas como líder do Império Romano, cerca de 50 a.C. o Imperador Júlio César (Figura 4) pela necessidade de se comunicar com seu exército, enviava mensagens sigilosas a seus generais. Para realização de tal ato, foi utilizado um processo de criptografia,

constituído basicamente da substituição de uma letra do alfabeto por outra deslocada algumas posições à frente, esse deslocamento denomina-se chave da codificação.

Figura 4– Júlio César

Fonte: Infobiografias (2017)

Ele usou um deslocamento de três casas para a direita, isso quer dizer que a sequência (FIARRESGA, 2010):

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

Tornou-se a sequência:

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

Com esse processo ele poderia transformar qualquer palavra conhecida em outra sem significado aparente, por exemplo, a mensagem “CESAR” se torna “FHVDU”. Apesar de ser facilmente quebrado, esse modo de codificação foi bem-sucedido na época, visto que a maioria dos inimigos era analfabeta e quem sabia ler acreditava que a mensagem estivesse escrita em outra língua.

Entretanto, decifrar um texto codificado pela Cifra de César sem saber sua chave de codificação, isto é, decodificar a mensagem mesmo sem ser o real receptor, não é uma tarefa difícil. Pois é possível basear-se em uma análise estatística das letras do alfabeto. Existem letras mais e menos frequentes em cada alfabeto, e com isso é possível analisar os símbolos mais frequentes na mensagem codificada, e assim chegar à chave de codificação. A Tabela 2 contém informações sobre a frequência das letras na língua portuguesa.

Tabela 2– Frequência das letras na língua portuguesa

Letra	Frequência	Letra	Frequência
A	14,63%	N	5,05%
B	1,04%	O	10,73%
C	3,88%	P	2,52%
D	4,99%	Q	1,20%
E	12,57%	R	6,53%
F	1,02%	S	7,81%
G	1,30%	T	4,34%
H	1,28%	U	4,63%
I	6,18%	V	1,67%
J	0,40%	W	0,01%
K	0,02%	X	0,21%
L	2,78%	Y	0,01%
M	4,74%	Z	0,47%

Fonte: Ribeiro (2006)

Durante a Idade Média, surgiu a Criptoanálise. Foi então que se percebeu que seria necessária a elaboração de códigos mais complexos, pois os usados anteriormente começaram a ser facilmente decifrados.

A partir da Cifra de César foram desenvolvidas outras maneiras mais elaboradas de criptografar uma mensagem. O italiano Leon Battista Alberti (1404-1472), dentre outras atividades, dedicou-se ao estudo de cifras e, por volta de 1440, propôs a utilização de dois ou mais alfabetos cifrados alternados. Ele foi o precursor da cifra de substituição poli alfabética. Quando a substituição se utiliza apenas um alfabeto é chamada de mono alfabética (Cifra de César) e usando mais de um alfabeto é chamada de poli alfabética. (MARQUES, 2013).

A máquina criptográfica de Alberti reproduzia um deslocamento simples de César através de dois discos que continham o alfabeto original gravado e outro alfabeto cifrado e podiam ser girados, como mostra a Figura 5. Esta máquina podia gerar uma cifra poli alfabética, bastava girar o segundo disco durante a mensagem (GANASSOLI e SCHANKOSKI, 2015).

Figura 5–Disco de Alberti

Fonte: GeoGebra (2016)

Durante a Idade Moderna foram desenvolvidas as cifras poli alfabéticas, como a Cifra de Vigenère e a Cifra de Hill (BEZERRA et. al., 2010).

Em 1586, o diplomata francês Blaise de Vigenère (1523-1596), Figura 6, publicou o seu livro de criptografia, *Traité dês chiffres ou secretes manières d'escrire*, no qual escreve sobre seu método de codificação que é baseado na Cifra de César e nas ideias de Alberti.

Figura 6– Blaisé Vigenère

Fonte: Wikipédia (2013)

Esse método foi adotado para evitar a quebra do código pela análise de frequência. Embora hoje se saiba que é relativamente simples a decifração, esse método de codificação foi altamente eficaz na época, sendo quebrado somente após cerca de 300 anos de utilização. Pode-se dizer que a Cifra de Vigenère é um aprimoramento da Cifra de César, pois possui basicamente a mesma ideia, diferindo apenas na função de substituição que não é a mesma para todas as letras, isto é, substituição poli alfabética. A Cifra de Vigenère pode ser vista como uma sequência de Cifras de César, visto que para cada letra utiliza-se uma chave

diferente, isto é, uma substituição diferente. Mas para realizar as substituições é necessário um padrão, e o padrão desse método consiste em se basear em uma palavra ou frase. Portanto, para a codificação será utilizada uma palavra-chave.

Se para codificar uma mensagem através da Cifra de César desloca-se cada letra uma quantidade fixa de posições, na Cifra de Vigenère trabalha-se com diferentes variações de posições. Toma-se como base uma palavra, por exemplo, “CIFRA”, e para codificar uma mensagem será utilizada uma sequência de cinco diferentes deslocamentos. Utilizar a letra A como chave significa não realizar nenhum deslocamento, pois o A se tornaria A, ou seja, deslocou zero posição. Utilizar a letra C como chave significa deslocar duas casas para a direita, o A se torna C, o B se torna D e continuando o processo para todas as letras do alfabeto, sendo que X se torna Z, Y se torna A e Z se torna B. Utilizar a letra F para cifração significa deslocar o alfabeto cinco posições para a direita, o A se torna F, o B se torna G, e assim sucessivamente. Utilizar a letra I para codificar significa deslocar oito posições para a direita, o A se torna I, o B se torna J, e assim por diante. Por último, utilizar a letra R como chave é deslocar o alfabeto dezessete posições a direita, o A se torna R e o B se torna S. Portanto, para codificar uma frase com a palavra “CIFRA” desloca-se respectivamente cada letra da mensagem dois, oito, cinco, dezessete e zero, posições no alfabeto, sendo que após deslocar zero voltamos a deslocar dois, depois oito e assim se forma o ciclo. Para codificar “TRABALHO” utilizando a Cifra de Vigenère com a palavra-chave “CIFRA”, esquematiza-se:

T R A B A L H O

C I F R A C I F

Utiliza-se tal disposição para facilitar o processo de cifração. O que deve ser feito é deslocar T em duas posições a direita, R em oito posições a direita, A em cinco posições a direita, B em dezessete posições a direita, A em zero posição a direita, L em duas posições a direita (quando são utilizadas todas as letras da palavra-chave, ou seja, todas as diferentes posições, deve-se recomeçar o processo da primeira letra), H em oito posições e O em cinco posições. Sendo assim a codificação da palavra “TRABALHO” utilizando como chave “CIFRA” é “VZFSANPT”.

Quanto maior o tamanho da mensagem mais o processo é penoso. Portanto, para auxiliar na codificação e decodificação de mensagens utilizando essa Cifra foi desenvolvida

uma tabela, denominada Régua de Saint-Cyr, também conhecida como “Quadrado de Vigenère”, mostrada na Figura 7.

Figura 7 –Régua de Saint-Cyr.

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

Fonte: Caetano

A tabela facilita a codificação, pois pode-se simplesmente através dela encontrar as substituições. Por exemplo, para codificar a frase “TRABALHODE MATEMATICA” com a palavra-chave “CIFRA” utiliza-se o esquema:

T R A B A L H O D E M A T E M A T I C A

C I F R A C I F R A C I F R A C I F R A

Para encontrar a codificação basta tomar a linha da tabela com a letra da chave, no caso da primeira letra é C, e localizar a intersecção com a coluna da letra que se quer codificar, no caso da primeira letra T, e assim obtendo que T codificada na chave C é V. Repetindo esse procedimento para todas as letras da frase "Trabalho de matemática" é obtida a frase "VZFSANPTUEOIYVMABNTA". Para decodificar a frase conhecendo a palavra chave de codificação, realiza-se exatamente o processo inverso.

Quanto maior a frase codificada, menos difícil é encontrar a mensagem original, porém é mais trabalhoso que a decifração da Cifra de César. Fazendo as análises estatísticas dos símbolos é possível chegar ao tamanho da palavra-chave de codificação e decifrar o código.

Entre 1929 e 1931, Lester S. Hill introduziu um método de criptografar em dois artigos: *Cryptography in the Algebraic Alphabet* e *Concerning Certain Linear Transformation Apparatus of Cryptography*, que ficou conhecido como a Cifra de Hill. A Cifra de Hill é classificada como um sistema poligráfico baseado em transformações matriciais. Esta é um sistema de criptografia em que o texto comum é divido em conjuntos de n letras (HOWARD e RORRES, 2001).

A partir do século XX, com a criação da máquina de rotores, começa a segunda era da Criptografia, a Criptografia por máquinas. "As máquinas de rotor são dispositivos de *hardware* sofisticados, anteriores ao computador, que utilizam técnicas de substituição." (STALLING, 2008). Segundo Menezes (1997), o surgimento das máquinas se deu independentemente e quase que simultaneamente em quatro países diferentes, sendo eles: Estados Unidos da América, Alemanha, Holanda e Suécia. Dentre as máquinas de rotores a que mais teve destaque foi criada por Arthur Scherbius, em 1918, na Alemanha, denominada Enigma, utilizada pelos alemães para fins militares durante a Segunda Guerra Mundial. O desenvolvimento desse processo marca uma grande mudança na história da Criptografia, até então se criptografava manualmente e da mesma maneira se fazia a decifração, entretanto com esse novo método, de cifração por máquina, surgiu a impossibilidade de decifrar uma mensagem manualmente, o que gerou a necessidade do desenvolvimento computacional.

Inicialmente a máquina Enigma era composta por três principais elementos, um teclado utilizado para se escrever o conteúdo original de uma mensagem, um misturador responsável pela cifração de cada letra, transformando-a na letra correspondente da mensagem cifrada e um painel que mostra cada letra do texto cifrado por meio de lâmpadas. Veja a Figura 8 que é uma foto da máquina Enigma.

Figura 8– Máquina Enigma

Fonte: Fernandes (2017)

Para uma máquina de três rotores existem 26×26×26 ajustes possíveis dos misturadores, isto é, 17 576 maneiras de codificar/decodificar uma mensagem. Como existem diversos ajustes a serem feitos para a codificação de uma mensagem é necessário que haja um livro de códigos, para que se saiba qual ajuste será utilizado em determinado dia.

Para se emitir uma mensagem, o remetente deve datilografar o texto original, a cada letra datilografada tem-se uma corrente elétrica que passa pelos componentes de cifragem e por fim acende a letra no painel com lâmpadas, essa letra que já está cifrada é anotada e o processo é repetido. Após todas as letras terem sido encriptadas, a mensagem cifrada é codificada por código Morse e transmitida via rádio. Para que o destinatário consiga ter acesso ao conteúdo da mensagem original é preciso que o mesmo possua outra máquina Enigma e uma cópia do livro de códigos contendo o ajuste inicial indicado para aquele dia específico. Após ajustar a máquina devidamente, o receptor decodifica a mensagem em código Morse e datilografa a mensagem recebida (o texto cifrado) para obter o texto original.

Portanto, a máquina e o livro de código não poderiam ser acessíveis aos inimigos, pois a mensagem seria facilmente decifrável, caso um inimigo tenha acesso à máquina, o processo de decifração, embora exaustivo, não é impossível, visto que há 17 576 ajustes possíveis um grupo de dez pessoas conseguiria testar todas as maneiras em um dia. Para que houvesse ainda mais segurança poderia ter-se aumentado o número de misturadores por máquina, porém para isso seria necessário aumentar o tamanho da máquina. Foram desenvolvidas, então, duas estratégias para se aumentar a segurança, uma foi a possibilidade de mover os

misturadores e outra foi a introdução de um painel de tomadas entre o teclado e o primeiro misturador, a inserção do cabo permite a troca de um par de letras.

> Em 1918, Arthur Scherbius desenvolveu uma máquina de criptografia chamada Enigma, utilizada amplamente pela marinha de guerra alemã em 1926, como a principal forma de comunicação A codificação da mensagem pelas máquinas Enigma era de difícil decodificação. Era necessário ter outra máquina idêntica. Saber qual a chave (esquema) utilizada para realizar a codificação.
>
> Em 1928, o exército alemão construiu uma versão conhecida como "Enigma G" – Troca periódica mensal de chaves. O diferencial desta máquina se dá pelo fato de ter sido elétrico-mecânica, funcionando com três (inicialmente) a oito rotores. Aparentava ser uma máquina de escrever, mas quando o usuário pressionava uma tecla, o rotor da esquerda avançava uma posição, provocando a rotação dos demais rotores à direita, sendo que esse movimento dos rotores gerava diferentes combinações de cifragem (Kleinschmidt, 2013, p.5).

Portanto, as substituições eram mono alfabéticas, mas a chave da cifra variava de acordo com o movimento do rotor, e ainda mais quando aumentava-se a quantidade de rotores. As máquinas Enigmas eram tidas como altamente seguras, por 13 anos foram classificadas como indecifráveis sem o conhecimento da chave, isto é, o ajuste feito. Em 1925 o governo alemão as adquiriu para serem utilizadas pelo exército alemão para comunicação. Cerca de 30 mil máquinas foram produzidas em 20 anos (Marques, 2013).

O criptoanalista Alan Turing e sua equipe foram responsáveis por decifrar as mensagens transmitidas pela máquina Enigma emitidas pelos alemães na Segunda Guerra Mundial. Alan Turing era britânico e durantes alguns anos dedicou-se exclusivamente a estudos da cifra por máquinas, liderou um grupo de criptoanalistas que trabalhavam na central em Bletchley Park na Inglaterra, as mensagens transmitidas via rádio por código Morse eram interceptadas e enviadas a essa central. Durante esse estudo foi construída uma máquina tida como precursora dos computadores, até finalmente chegarem ao primeiro computador operacional, denominado Colossus. Em maio de 1941 Turing e sua equipe apoderaram-se do livro de códigos, esse conhecimento juntamente com o Colossus auxiliaram na decifração de mensagens. Estima-se que a descoberta de informações tenha encurtado em dois anos a Guerra (Bezerra et al.).

Após o término da Guerra começaram a serem desenvolvidos os computadores digitais eletrônicos. Os primeiros computadores possuíam grandes dimensões, funcionavam com milhares de válvulas e consumiam muita energia. Ao passar dos anos os computadores foram evoluindo e junto com o desenvolvimento começava uma nova era da Criptografia, a Criptografia computacional. A partir dessa evolução a ciência denominada Criptologia

começou a ganhar cada vez mais espaço, sendo até os dias atuais uma das ciências mais estudadas. A evolução dos computadores exigiu métodos mais eficientes na codificação e decodificação de mensagens, pois o que antes era trabalhoso de ser calculado a mão tornou-se mais fácil.

Com a revolução industrial a Criptografia evoluiu para mecanização e automatização. A Idade Contemporânea tem como principal característica o desenvolvimento computacional, que é responsável pela enorme evolução dos métodos criptográficos. Pois exigiu estudos mais aprofundados na Criptologia, visto que além de algoritmos matemáticos também surgiam algoritmos computacionais, o que facilitou, e muito, a decifração de métodos de cifração existentes até então. Portanto, houve a necessidade de um aprimoramento nos métodos, pois o essencial é que continuassem seguros mesmo com tantos meios que tinham sido desenvolvidos e que podiam auxiliar na decifração (HINZ, 2000).

Para cada um dos métodos de criptografia descritos anteriormente foram desenvolvidos processos para quebrar as cifras, e é por esse motivo que não são métodos aconselháveis para se utilizar atualmente em assunto que exija segurança. Logo, outra ciência que teve grandes avanços juntamente com a Criptografia foi a Criptoanálise. Cada cifra desenvolvida foi utilizada e segura por um tempo, porém houve um determinado momento na história que foram descobertos mecanismos capazes de decifrar as mensagens codificadas por esses processos.

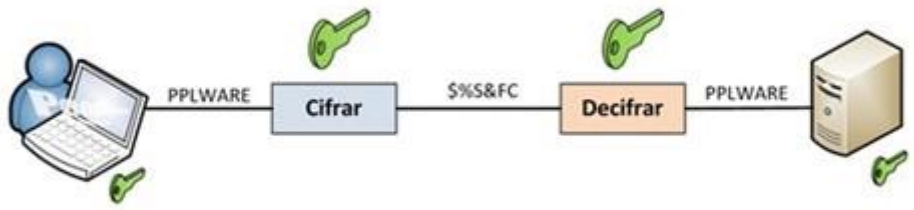
Um método existente e que ainda é considerado seguro é o método RSA. Este método é um sistema de chave assimétrica (pública) desenvolvido em 1978 por R. L. Rivest, A. Shamir e L. Adleman, professores do *Massachussets Institute of Technology* (MIT) e *University of Southern California* (USC), e desde então o método tem grande destaque quanto à utilização. O nome RSA foi assim denominado em função das inicias dos sobrenomes dos responsáveis pelo desenvolvimento do algoritmo.

Codificar e decodificar mensagens pelo método RSA requer duas chaves, uma pública e outra privada.

A chave de codificação classificada como simétrica se caracteriza pelo fato de o emissor e o receptor possuírem a mesma chave, a qual será utilizada tanto na codificação quanto na decodificação, também denominada chave privada. As cifras simétricas, ou seja, as que são criptografadas a partir de chave privada utilizam técnicas de substituição ou transposição. Essa técnica de criptografia era a única utilizada até a década de 1970 quando se deu o

surgimento da Criptografia por chave pública. O único fator que torna o método inseguro é que a mesma chave que é utilizada para criptografar também é utilizada para descriptografar, portanto, uma vez que um indivíduo for capaz de interceptar a mensagem e conseguir encontrar a chave de codificação poderá facilmente decifrar a mensagem e ter acesso ao conteúdo. Logo, o principal desafio para tornar o código seguro é manter o sigilo da chave. A Figura 9 exemplifica o processo de encriptação e desencriptação por meio da chave pública. A mensagem é "PPLWARE" criptografada através de uma chave secreta compartilhada pelo remetente e destinatário. A mensagem é enviada como "S%$&FC" e recebida pelo destinatário que descriptografa para "PPLWARE" usando a chave secreta.

Figura 9: Modelo de Chave Simétrica.



Fonte: Pplware (2016)

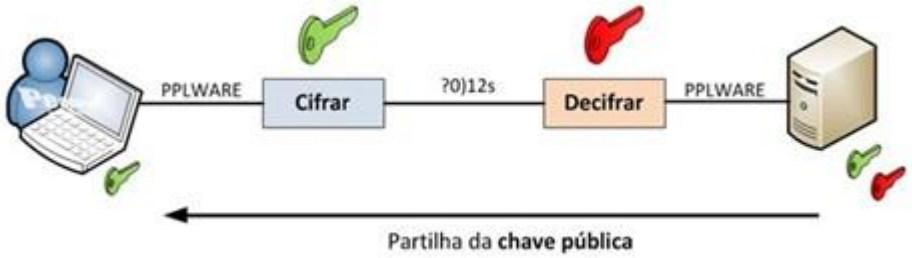
Com o desenvolvimento desse processo houve uma grande mudança quanto aos métodos empregados, foi uma grande revolução na Criptografia, visto que os algoritmos são baseados em funções matemáticas.

Por ser um método criptográfico de chave assimétrica são geradas duas chaves, uma chave para codificar e outra diferente para decodificar, a primeira pode ser conhecida por todos (chave pública), já a segunda não (chave privada). A chave pública pode ter acesso por qualquer usuário e é a utilizada no processo de codificação. A chave privada que somente o receptor pode ter acesso que é a utilizada para decodificar uma mensagem. Esse método de criptografia também é conhecido como Criptografia por chave pública. Logo, um terceiro indivíduo que tente interceptar uma mensagem codificada pelo método RSA conseguirá ter acesso à chave pública e ao texto cifrado, mas ter acesso ao texto cifrado não significa conseguir ter acesso ao texto original, visto que a chave de decodificação não é conhecida o que torna a realização do processo de decifração inviável quando a chave possui grande

comprimento. Somente o verdadeiro receptor é capaz de realizar o processo de decodificação que permite a leitura do conteúdo da mensagem original.

A Figura 10 ilustra a codificação e decodificação por chave pública. A mensagem "PPLWARE" é criptografada através de uma chave pública compartilhada pelo remetente, destinatário e qualquer indivíduo que intercepte a mensagem. "A mensagem é enviada como"?0)12s" e recebida assim pelo destinatário que descriptografa para "PPLWARE" usando a chave secreta, que somente ele tem acesso.

Figura 10 - Modelo de Chave Assimétrica.



Fonte: Pplware (2016)

A chave pública é formada por n e e, tal que $n=pq$, em que p e q são números primos com uma grande quantidade de algarismos, utilizam-se geralmente números primos (p e q) com 512 bits de comprimento. Quando combinados geram a chave n de 1024 bits de comprimento, um pouco mais de 300 dígitos, em algumas operações, como, por exemplo, bancárias utiliza-se chave ainda maior como 2048 bits. A tendência é que com o passar do tempo a chave aumente ainda mais. O número e é um número menor que $\phi(n)$ e tem 1 como máximo divisor comum com $\phi(n)$, ou seja, $mdc(\phi(n),e)=1$. Portanto, a chave (n,e) não é secreta e pode circular sem comprometer o conteúdo da mensagem em quaisquer meios, mesmo os tidos como não seguros, como a internet, por exemplo.

É importante deixar claro que um algoritmo não se torna mais seguro por ser de chave pública ou privada e sim devido ao tamanho da chave utilizada. Portanto, a segurança do algoritmo depende do tamanho da chave.

A Tabela 3 apresenta um breve comparativo entre as chaves simétricas e assimétricas.

Tabela 3 – Comparação entre chave assimétrica e simétrica

	CRIPTOSSISTEMA DE CHAVE SIMÉTRICA	CRIPTOSSISTEMA DE CHAVE ASSIMÉTRICA
VELOCIDADE	Alta	Baixa
CONFIABILIDADE	Boa	Muito Boa
NÍVEL DE SEGURANÇA	Alto	Alto
REQUER UMA TERCEIRA PARTE CONFIÁVEL	Algumas vezes	Sempre
QUANTIDADE DE CHAVES USADAS	Uma	Duas

Fonte: Barbosa et. al. (2003)

Sabe-se, portanto, que a codificação e decodificação de uma mensagem com o algoritmo RSA dependem fundamentalmente da teoria dos números. Logo quando o desejado é codificar uma mensagem com apenas letras não é possível diretamente, pois para o processo é necessário trabalhar-se com números. Este problema é resolvido facilmente: cada símbolo (as letras do alfabeto, o espaço, pontuações, dentre outros) é colocado em correspondência biunívoca com um número de dois algarismos, ou mais, é necessário que todos os símbolos a serem usados correspondam a um número com a quantidade especificada de algarismo para que não haja confusão.

Inicia-se o processo com a pré-codificação da mensagem. Após as letras terem sido associadas aos números, o que se tinha como frase tornou-se uma sequência numérica. Essa sequência será quebrada em blocos, os quais não precisam ter o mesmo tamanho, mas devem seguir a regra: cada bloco deve ter valor menor que n.

Porém existem restrições para sua segurança. Para que este seja seguro deve-se usar um número grande para a chave, o qual interfere na velocidade de codificação e decodificação. Quanto maior a chave, maior o tempo gasto.

Atualmente, utiliza-se a internet para diversas tarefas, a privacidade é importante para empresas e pessoas, e a Criptografia é responsável pela integridade, confidencialidade e autenticidade dessas informações que circulam em meios não seguros. Em uma simples troca de mensagens, em compras no comércio eletrônico, em transações bancárias, entre outras ações que a internet nos proporciona, as informações são protegidas por cifras que foram e

são desenvolvidos pela ciência Criptografia, e a Criptologia garante a confiabilidade dos códigos. São estudados métodos que sejam possíveis de serem aplicados e principalmente sejam seguros. Nesse trabalho está presente a descrição do método RSA por ser um dos principais métodos utilizados atualmente, visto que o objetivo principal é conhecer e entender a matemática por trás dessa ciência, e também será apresentada uma breve explicação de seu desempenho e segurança.

4 BASE MATEMÁTICA

Embora não tenha sido desenvolvida com essa finalidade, a Matemática é fundamental para a Criptografia, cuja estrutura é baseada principalmente em algoritmos matemáticos e computacionais. A teoria dos números que possui como objeto de estudo as propriedades dos números, juntamente com a geometria, é uma das áreas mais antigas da matemática. Desde sua origem até cerca de 1960 era considerada uma área da matemática sem utilidade prática, e atualmente sabe-se que é a base matemática nas aplicações à Criptografia.

Portanto, para que se tenha real compreensão dos métodos criptográficos, são apresentados nesse capítulo conceitos básicos matemáticos extremamente importantes para o entendimento dos métodos de codificação e decodificação. Mais sobre este assunto pode ser encontrado em Santos (2006), Kraus (2015) e Coutinho (2014).

4.1 MATRIZES

A seguir serão definidos alguns conceitos de matrizes e determinante.

Definição: Denomina-se matriz de ordem $m \times n$, uma tabela retangular com m linhas e n colunas com $m \times n$ elementos, como no exemplo abaixo:

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \text{ ou } \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

Podendo ser representada também na forma $A = [a_{ij}]_{mxn}$, em que $i = 1, 2, ...m$, e $j = 1, 2, ..., n$.

Cada elemento da matriz A é representada pela mesma letra em minúsculo e é seguida de dois números subscritos, sendo o primeiro deles o número da linha onde o elemento se encontra e o segundo o número da coluna, ou seja, o elemento a_{23} encontra-se na segunda linha e terceira coluna.

Definição: Seguem definições de matrizes especiais:

- ✓ Matriz linha é a matriz de ordem 1 por n, ou seja, possui apenas uma linha e n colunas.
- ✓ Matriz coluna é a matriz de ordem m por 1, ou seja, possui apenas uma coluna e m linhas.

- ✓Matriz nula é a matriz que possui todos os elementos iguais a 0.
- ✓Matriz quadrada é a matriz que possui o número de linhas igual ao número de colunas.
- ✓Matriz diagonal é uma matriz quadrada que possui todos os elementos fora da diagonal principal nulos.
- ✓A matriz quadrada de ordem *n* que possui todos os elementos da diagonal principal iguais a 1 e os demais elementos iguais a zero é denominada matriz identidade de ordem *n*, notada I_n.
- ✓Matriz transposta: a matriz transposta relativa a matriz $A_{m\times n}$ é definida através da seguinte relação:

$$a_{ij} = a_{ji}^{T} \tag{1}$$

para todo *i* e todo *j*.

- ✓Matriz simétrica é uma matriz quadrada cujos elementos obedecem a seguinte relação:

$$a_{ij} = a_{ji} \tag{2}$$

isto é, $A^T = A$.

4.1.1 Operações com matrizes

Definição: Duas matrizes *A* e *B* só podem ser adicionadas se forem da mesma ordem. Portanto, sendo *A* e *B* matrizes de ordem *m* por *n,* $A_{m\times n} = a_{ij}$, $1 \leq i \leq m$ e $1 \leq j \leq n$ e $B_{m\times n} = b_{ij}$, $1 \leq i \leq m$ e $1 \leq j \leq n$ tem-se que:

$$A+B=C \tag{3}$$

tal que $C = c_{ij}$, $1 \leq i \leq m$ e $1 \leq j \leq n$, em que $c_{ij} = a_{ij} + b_{ij}$, $1 \leq i \leq m$ e $1 \leq j \leq n$.

Definição: Duas matrizes *A* e *B* só podem ser multiplicadas se o número de colunas da primeira matriz for igual ao número de linhas da segunda matriz. Ou seja, só é definido se *A* é da ordem *m* por *n* e *B* é da ordem *n* por *p*,$A_{mn} = a_{ij}$, $1 \leq i \leq m$ e $1 \leq j \leq n$ e$B_{np} = b_{ij}$, $1 \leq i \leq n$ e $1 \leq j \leq p$, o produto é definido tal que

$$A_{m\times n} \,.\, B_{n\times p} = C_{m\times p} \tag{4}$$

em que $c_{ij}=\sum_{k=1}^{n} a_{ik}b_{kj}$, ou seja,

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj},$$

com $1 \leq i \leq m$ e $1 \leq j \leq p$.

Admitem matriz inversa matrizes quadradas com determinantes não nulo. A matriz inversa de A_n é a matriz B_n, tal que

$$A.B = B.A = I_n \tag{5}$$

Nota-se inversa de A por $B = A^{-1}$.

Definição: O determinante de uma matriz quadrada A, de ordem n, é denotado por $det(A)$ ou |A|, e é definido como sendo o número obtido pela soma algébrica dos n! produtos possíveis constituídos por um elemento de cada linha e de cada coluna de A multiplicado por 1 ou por -1, de acordo com a seguinte regra:

"Seja o produto escrito na seguinte forma: $a_{1i} \cdot a_{2j} \cdot a_{3k} \cdot \ldots$($n$ termos).Se a sequência dos índices $i,j,\ k$ é um permutação par em relação a 1,2,3,....,n, então o produto deve ser multiplicado por 1; do contrário, o produto deverá ser multiplicado por -1".

Entenda-se por permutação, o número de trocas necessárias para se ordenar uma sequência $i,j,k...n$.

O determinante é o valor associado à matriz. Por exemplo, para uma matriz A de ordem 2, $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, seu determinante é definido tal que:

$$det\ (A) = a_{11}a_{22} - a_{12}a_{21} \tag{6}$$

4.2 DIVISIBILIDADE

Euclides foi um importante matemático da Grécia antiga. Seu mais importante legado para os dias atuais foi a obra “Os Elementos”, de onde surge toda a base da atualmente chamada Geometria Euclidiana. No livro 7, Euclides trata do método para achar o máximo divisor comum (*mdc*) de dois números inteiros. Esse método é extremamente rápido para mostrar qual o *mdc* de dois inteiros.

Teorema (Divisão de Euclides): Sejam a e b dois inteiros com $b>0$. Existe um único par de inteiros q e r tais que

$$a = bq + r \tag{7}$$

com $0 \leq r < b$ e denomina-se q o quociente e r o resto da divisão euclidiana de a por b.

Sejam *a* e *b* dois inteiros. Dizemos que *b* divide *a*, denotado por $b|a$, ou que *b* é um divisor de *a*, ou ainda que *a* é divisível por *b*, se existir um inteiro *c* tal que $a = b \cdot c$, isto é, $r = 0$. Neste caso, dizemos que a divisão é exata.

A seguir são apresentadas algumas propriedades de divisibilidade para quaisquer $a, b, c \in \mathbb{Z}$:

P1 $1|b$, $\forall b \in \mathbb{Z}$;

P2 $a|0, \forall a \in \mathbb{Z}$;

P3 Se $a|b$, então $(ca)|(cb)$ para $c \neq 0$;

P4 Se $0|b$, então $b = 0$;

P5 Se $d|a$ e $d|b$, então $d|(ax + by)$, para quaisquer $x, y \in \mathbb{Z}$;

P6 Se $d|a$, então $a = 0$ ou $|a| \geq |d|$;

P7 $a|a$, $\forall a \in \mathbb{Z}$. (Simétrica);

P8 Se $a|b$ e $b|c$, então $a|c$ (Transitiva).

P9 Se $a|b$ e $b|a$ então |a|=|b| (Antissimétrica).

Definição: Dados dois inteiros *a* e *b*, não nulos simultaneamente, denomina-se máximo divisor comum, denotado por *mdc(a,b),* o maior inteiro que divide *a* e *b* simultaneamente, tal que:

1) $d \geq 0$ (*d* é um número inteiro não-negativo).
2) $d|a$ e $d|b$ (isto é, *d* é divisor comum de *a* e *b*).
3) Todo número inteiro divisor comum de *a* e *b* também divide *d*, em que *d=mdc(a,b)* (isto é, *d* é único).

Teorema de Bachet-Bézout: Seja *d* o máximo divisor comum de a e b, existem dois inteiros *u* e *v*, tais que

$$d = au + bv \tag{8}$$

Demonstração:

Seja A ={au+bv / u, v $\in \mathbb{Z}$ *}, então todos os elementos pertencentes ao conjunto A são números inteiros. Tomando u, v* $\in \mathbb{Z}$*, tais que* $e = au + bv$*, sendo e o menor inteiro positivo pertencente a A. Para demonstrar este teorema, primeiramente, será provado que* $e|a$*, para tal utilizar-se-á a prova por absurdo. Suponha-se que* $e \nmid a$*. Assim sendo, por definição, existem m, q* $\in \mathbb{Z}$*, com 0 < r < e, tal que* $a = qe + r$*. Portanto,* $r = a - qe = a - q(au +$

$bv) = a - qau - qbv = (1 - qu)a + (-qv)$, *como (1-qu), (-qu)* $\in \mathbb{Z}$*, então conclui-se que r* $\in$ *A, o que é um absurdo pois 0 < r < e* e *é o menor elemento de A. Logo* $c|a$*, e de maneira análoga demonstra-se que* $c|b$.

Como e é divisor comum de a e b, existem inteiros m e n tais que $a = md$ *e* $b = nd$*, e* $e = au + bv$*, tem-se, portanto,* $e = mdu + ndv = d(um + nv)$ *o que implica* $e|d$*. Pela propriedade P6, tem-se que e ≤ d, como e < d não é possível, visto que d é o máximo divisor comum de a e b, concluímos que e = d. Portanto* $d = au + bv$. ♦

O Algoritmo de Euclides permite a determinação do máximo divisor comum de dois números naturais, *a* e *b*, utilizando apenas o teorema da divisão euclidiana.

Teorema 1: Sejam *a, b, q* e *r* números inteiros tais que *a = bq+ r*, então *mdc(a,b)=mdc(b,r).*

Demonstração:

Pelo algoritmo da divisão tem-se a = bq+ r, pela propriedade P5 da divisão, conclui-se que todo divisor de b e r é um divisor de a, isto é, se $d|b$ *e* $d|r$*, então*$d|(bq + r)$*, logo* $d|a$*. Analisando a mesma equação escrita de outra maneira r = a -bq tem-se que todo divisor de a e b é um divisor de r. Logo o conjunto dos divisores comuns de b e r é igual ao conjunto dos divisores de a e b. Portanto, mdc (a,b)= mdc(b,r).* ♦

Teorema 2: Sejam *a* = r_0 e *b* = r_1 números inteiros não-negativos e não nulos simultaneamente. Se o algoritmo da divisão for aplicado sucessivamente para se obter:

$$r_j = q_{j+1}r_{j+1} + r_{j+2}, \tag{9}$$

com *0 ≤*r_{j+2}*<*r_{j+1}*, j = 0, 1, 2,..., n-1* e $r_{n+1} = 0$*, ,*então *mdc(a,b)=*r_n, o último resto não nulo.

Demonstração:

Aplicando o algoritmo da divisão para dividir a = r_0 *por b =* r_1*, tem-se* $r_0 = qr_1 + r_2$*, em seguida dividindo* r_1 *por* r_2 *obtém-se* $r_1 = q_2r_2 + r_3$ *e assim sucessivamente até a obtenção de* $r_{n+1} = 0$*. Como a cada passo o resto é sempre menor que o anterior, e trata-se de números inteiros positivos, após um número finito de passos tem-se um resto nulo. Dada, portanto, a sequência:*

$$r_0 = qr_1 + r_2, \qquad 0 < r_2 < r_1 \tag{10}$$

$$r_1 = q_2r_2 + r_3 0 < r_3 < r_2 \tag{11}$$

$$r_2 = q_3 r_3 + r_4 \quad 0 < r_4 < r_3 \tag{12}$$

$$\vdots \qquad\qquad \vdots$$

$$r_{n-2} = q r_{n-1} + r_n \;\; 0 < r_n < r_{n-1} \tag{13}$$

$$r_{n-1} = q r_n + 0 \qquad r_{n+1} = 0 \tag{14}$$

Da equação (14) conclui-se que r_{n-1} é múltiplo de r_n. Logo, mdc(r_{n-1},r_n)=r_n. Da equação (13) pelo Teorema 1 tem-se mdc (r_{n-2},r_{n-1})=mdc (r_{n-1},r_n)=r_n, e aplicando o Teorema 1 em todas as equações anteriores tem-se:

$$r_n = mdc(r_n, r_{n-1}) = mdc\,(r_{n-2}, r_{n-1}) = \cdots$$

$$= mdc\,(r_1, r_2) = mdc\,(r_0, r_1) = mdc\,(a, b). \blacklozenge$$

4.3 NÚMEROS PRIMOS

Um número inteiro $a \neq 0, \pm 1$ tem pelo menos quatro divisores: ±1 e ±*a*. Esses são os divisores triviais de *a*. Alguns números diferentes de 0 e ±1 só têm os divisores triviais e são os chamados números primos, como ±2, ±3, ±5, ± 7, ...

Um número inteiro a≠ 0,±1 é chamado número composto se tem outros divisores, além dos triviais, , como ±4, ±6, ±8, ±9, ...

Definição: Um número inteiro p é chamado número primo se as seguintes condiçõesse verificam:

i. $p \neq 0$.

ii. $p \neq \pm 1$.

iii. Os únicos divisores de p são ±*1* e ±*p*.

De acordo com a definição, 0 e 1 não são primos nem compostos.

> O nome "primo" é uma herança grega e, naturalmente, não se refere a nenhuma relação de parentesco. Os gregos classificavam os números em *primeiros* ou *indecomponíveis* e *secundários* ou *compostos*. Os números compostos são secundários por serem formados a partir dos primos. Os romanos apenas traduziram literalmente a palavra grega para primeiro, que em latim é *primus*. É daí que vêm nossos números primos. (HEFEZ, 2009)

Definição: Sejam $a, b \in \mathbb{Z}$. Se $mdc(a, b) = 1$, diz-se que a e b são primos entre si.

Teorema fundamental da aritmética: Todo número inteiro maior do que 1 pode ser representado de maneira única na forma

$$n = p_1^{r_1} \ldots . p_k^{r_k} \tag{15}$$

em que $1 < p_1 < p_2 < p_3 < \ldots < p_k$ são números primos e $r_1, \ldots, r_k$ são inteiros positivos. Diz-se que a equação (15) é a decomposição de *n* em produto de números primos.

Demonstração:

(i) A existência da fatoração pode ser provada por indução para n≥2. Admite-se como hipótese "n se escreve como produto de primos". Se n=2, n é primo e o resultado é imediato ($n = p_1 = 2$). Suponha que para todos k tal que $2 \leq k \leq n$ a hipótese é verdadeira, então será provado que é válida também para n+1.Se n+1é primo o resultado é imediato, se n+1 é composto pode-se escrever $n+1 = ab$, $a,b \in \mathbb{Z}$, $1<a<n+1$, $1<b<n+1$. Por hipótese de indução, a e b se decompõem como produto de primos. Portanto, a junção das fatorações de a e b (e reordenando os fatores) obtém-se uma fatoração de n+1. Logo, todo número pode ser escrito como produto de primos.

(ii) A unicidade da fatoração, a menos da ordem dos produtos, provada por indução.

Tomando n o menor número natural tal que n possui diferentes fatores primos em sua decomposição, isto é, n pode ser escrito como diferentes produtos de primos. Seja

$$n = p_1 p_2 \ldots . p_a = q_1 q_2 \ldots . q_b \tag{16}$$

Com $p_1 \leq p_2 \leq \cdots \leq p_a$ *e* $q_1 \leq q_2 \leq \cdots \leq q_b$, p_i *e* q_j *números primos.Então:*

$$p_1 \,|(q_1 q_2 \ldots . q_b) \tag{17}$$

$p_1 \mid q_j$, *para algum j, logo* $p_1 = q_j \geq q_1$. *Analogamente,*

$$q_1 | (p_1 p_2 \ldots . p_a) \tag{18}$$

$q_1 | \, p_i$ *para algum i, logo* $q_1 = p_i \geq p_1$. *Portanto* $p_1 = q_1$. *Pela minimalidade de n,*

$$p_2 \ldots . p_a = q_2 \ldots . q_b \tag{19}$$

É o mesmo produto de primos. ♦

Teorema 3: Seja P o conjunto dos números primos. O conjunto P é infinito.

Demonstração:

Supondo que P seja um conjunto de cardinalidade finita n, em outras palavras, que existam apenas n números primos. Sejam $p_1, \ldots, p_n$ *os elementos de P e tomando N= 1 +* $p_1 \ldots p_n$*. Tem-se N >1, têm-se duas possibilidades, N é primo ou composto. Se N for primo, N é maior que todos os elementos de P, contradizendo nossa suposição, portanto não seria finito o conjunto dos primos. Se N é composto, então existe um* p_k *tal que* $p_k|N$*, mas se* $p_k \in P$ *e* $p_k|N$*, então* $p_k|(1 + p_1 \ldots p_n)$*, como* $p_k|(p_1 \ldots p_n), p_k|1$*, contradizendo nossa suposição, portanto P não seria finito. Logo podemos afirmar que existe uma infinidade de números primos.*♦

4.4 CONGRUÊNCIA

Definição: Sejam *a* e *b* dois números inteiros e *n* um número inteiro estritamente positivo, diz-se que *a* é congruente a *b* módulo de *n*, se *n|(a-b)* e escreve-se:

$$a \equiv b \pmod{n} \tag{20}$$

Proposição 1: Se *a* e *b* são inteiros, temos que $a \equiv b \pmod{n}$ se, e somente se, existir um inteiro *k* tal que $a = b + kn$.

Demonstração:

Pela definição de congruência modular tem-se que se $a \equiv b \pmod{n}$*, então* $n|(a-b)$*, portanto, existe um* $k \in \mathbb{Z}$*. tal que a-b=kn, que é equivalente a a=b+kn. Se existe um inteiro k tal que a=b+kn, então a-b=kn, logo n|(a-b), isto é* $a \equiv b \pmod{n}$.♦

Proposição 2: Se *a, b, n* e *d* são inteiros, *m>0*, as seguintes sentenças são verdadeiras:

1. $a \equiv a \pmod{n}$ (Reflexiva).
2. Se $a \equiv b \pmod{n}$, então $b \equiv a \pmod{n}$ (Simétrica).
3. Se $a \equiv b \pmod{n}$ e $b \equiv d \pmod{n}$, então $a \equiv d \pmod{n}$ (Transitiva).

Demonstração:

1. *Como n|0, então* $n|(a - a)$*, o que implica* $a \equiv a \pmod{n}$.
2. *Se* $a \equiv b \pmod{n}$*, então existe um k inteiro tal que* $a = b + kn$*. Logo b=a-kn, e existe um q inteiro tal que* $q = -k$*, isto é,* $b = a + qn$*, pela Proposição 1,* $b \equiv a \pmod{n}$.
3. *Se* $a \equiv b \pmod{n}$*, então existe um inteiro k tal que a=b+kn, isto é b=a-kn, e se* $b \equiv d \pmod{n}$*, então existe um inteiro q tal que b=d+qn. Logo, a-kn=d+qn, ou seja, a=d+qn+kn, a=d+(q+k)n. Portanto,* $a \equiv d \pmod{n}$♦

Teorema 4: Se *a, b, c* e *n* são inteiros tais que $a \equiv b \pmod n$, então:

1. $a + c \equiv b + c \pmod n$.
2. $a - c \equiv b - c \pmod n$.
3. $ac \equiv bc \pmod n$.

Demonstração:

1. *Como* $a \equiv b \pmod n$, *tem-se* $n|(a-b)$. *Logo,* $n|(a+c-b-c)$,*ou seja,* $n|((a+c)-(b+c))$. *Portanto,* $a + c \equiv b + c \pmod n$.
2. *Como* $a \equiv b \pmod n$, *tem-se* $n|(a-b)$. *Logo,* $n|(a-c-b+c)$,*ou seja,* $n|((a-c)-(b-c))$.*Portanto* $a - c \equiv b - c \pmod n$
3. *Como* $a \equiv b \pmod n$,*tem-se* $n|(a-b)$.*Logo,* $n|c(a+b)$, *ou seja,*$n|(ac+bc)$.*Portanto,* $ac \equiv bc \pmod n$.♦

Teorema 5: Se *a, b, c* e *m* são inteiros e $ac \equiv bc \pmod n$, então $a \equiv b \pmod{\frac{n}{d}}$ em que $d = mdc(c, n)$.

Demonstração:

Pela hipótese, tem-se que $ac \equiv bc \pmod n$,*logo* $ac-bc=kn$, *isto é* $c(a-b)=kn$. *Ao dividir os dois termos por d, tem-se que* $\frac{c}{d}.(a-b) = k.\frac{n}{d}$, *logo* $\frac{n}{d} | \frac{c}{d}.(a-b)$ *e, como mdc* $(\frac{n}{d}, \frac{c}{d})=1$, $\frac{n}{d} | (a-b)$, *o que implica* $a \equiv b \pmod{\frac{n}{d}}$.♦

Definição: Se *h* e *k* são dois inteiros com $h \equiv k \pmod n$ *e* $k<n$, chama-se *k* o resto de *h* módulo *n*.

Definição: O conjunto dos inteiros $\{r_1, r_2, \dots, r_s\}$ é um sistema completo de restos módulo *n* se

- $r_i \not\equiv r_j \pmod n$ para $i \neq j$.
- Para todo inteiro m existe um r_i tal que $m \equiv r_i \pmod n$.

Proposição 3: Se *a, b, k* e *n* são números inteiros com $k>0$ *e* $a \equiv b \pmod n$, *e*então $a^k \equiv b^k \pmod n$.

Demonstração:

Por hipótese, $a \equiv b \pmod n$, *logo*$n|(a-b)$. *Sabendo que é verdadeira a identidade* $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + a^{k-2}b^2 + \cdots + ab^{k-2} + b^{k-1})$, *tem-se que*$a^k - b^k$*émúltiplo de* $a-b$,*logo* $n|(a^k - b^k)$. *Portanto,* $a^k \equiv b^k \pmod n$.♦

Definição: Denomina-se congruência linear em uma variável uma congruência da forma

$$ax \equiv b \ (mod\ n) \tag{21}$$

em que *x* é a variável.

Uma solução $\bar{a}$ de $ax \equiv 1 \ (mod\ n)$ é chamada de inverso de a no módulo *n*.

Proposição 4: Seja *p* um número primo. O inteiro positivo *a* é o seu próprio inverso módulo de *p* se, e somente se, $a \equiv 1 \ (mod\ p)$ ou $a \equiv -1 \ (mod\ p)$

Demonstração:

Supondo a como seu próprio inverso, então $a^2 \equiv 1 \ (mod\ p)$*, o que implica* $p|(a^2 - 1)$*, logo* $p|(a-1)(a+1)$*. Sendo p um número primo* $p|(a-1)$ *ou* $p|(a+1)$*, o que implica* $a \equiv 1 \ (mod\ p)$ *ou* $a \equiv -1 \ (mod\ p)$*.*

A recíproca é imediata visto que se $a \equiv 1 \ (mod\ p)$ *ou* $a \equiv -1 \ (mod\ p)$*, então* $p|(a-1)$ *ou* $p|(a+1)$*. Portanto* $p|(a-1)(a+1)$*, isto é* $p|(a^2-1)$ *o que significa* $a^2 \equiv 1 \ (mod\ p)$*.* ♦

4.5 EULER, FERMAT

Pequeno Teorema de Fermat: Sejam *a* um inteiro e *p* um número primo, se *p* não divide *a*, então

$$a^{p-1} \equiv 1 \ (mod\ p) \tag{22}$$

Demonstração:

Sabe-se que {0, 1, 2, ..., p-1} é um sistema completo de restos módulo p. Isto significa que qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado em correspondência biunívoca com um subconjunto de {0, 1, 2, ..., p-1}. Considerando os números a, 2a, 3a, ..., (p-1)a. Como mdc (a,p)=1, nenhum destes números ia, $1 \leq i \leq p-i$ *é divisível por p, ou seja, nenhum é congruente a zero módulo p. Quaisquer dois deles são incongruentes módulo p, pois* $aj \equiv ak \ (mod\ p)$ *implica j=k, uma vez que j e k são positivos e menores do que p. Tem-se, portanto, um conjunto de p-1 elementos incongruentes módulo p e não divisíveis por p. Logo, cada um deles é congruente a exatamente um dentre os elementos {1, 2, 3, ..., p-1}. Ao se multiplicar as congruências, membro a membro, obtém-se:*

$$a(2a)(3a) \ldots (p-1)a \equiv 1.2.3 \ldots (p-1) \ (mod\ p) \tag{23}$$

ou seja, a^{p-1}*(p-1)! ≡ (p-1)! (mod p). Mas, pelo Teorema 5, como mdc((p-1)!,p)=1, tem-se* $a^{p-1} \equiv 1 (mod \frac{p}{1})$. ♦

Definição: Para todo inteiro $n \geq 1$, o inteiro $\phi(n)$ é o número de inteiros positivos menores do que n e relativamente primos com n. Ou seja, $\phi(n)$ é o número de inteiros k tais que: $1 \leq k \leq n$ e $mdc(k,n)=1$.

Teorema 6: Seja a um inteiro positivo tal que $mdc(a,n)=1$. Se $r_1, r_2, \ldots, r_{\phi(n)}$ é um sistema reduzido de restos módulo n, então $ar_1, a\,r_2, \ldots, ar_{\phi(n)}$ é, também, um sistema reduzido de restos módulo n.

<u>*Demonstração:*</u>

Por hipótese mdc (a, n)=1 e mdc(r_i*,n)=1,logo mdc (*ar_i, n*)=1. Deve ser mostrado que* ar_i *é incongruente a* ar_j *módulo n se i≠j. Como mdc (a,n)=1, da afirmação a* $ar_i \equiv ar_j$ *(mod n) pode-se dizer que* $r_i \equiv r_j$ *(mod n) o que implica i=j. Portanto,*ar_1, ar_2*, ...,* $ar_{\phi(n)}$ *é também um sistema de restos módulo n.* ♦

Teorema de Euler: Se n é um inteiro positivo e a um inteiro com $mdc(a,n)=1$, então

$$a^{\phi(n)} \equiv 1 \ (mod\ n) \tag{24}$$

<u>*Demonstração:*</u>

Como mdc (a,n)=1 e ar_1, ar_2*, ...,* $ar_{\phi(n)}$ *é um sistema de restos módulo n,* ar_i *é congruente s exatamente um dos* r_j*,* $1 \leq j \leq \phi(n)$*. Logo, o produto dos* ar_i *deve ser congruente ao produto dos* r_j *módulo n, isto é:*

$$ar_1 . ar_2 . \ldots . ar_{\phi(n)} \equiv r_1 . r_2 . \ldots . r_{\phi(n)} \ (mod\ n) \tag{25}$$

$$a^{\phi(n)} . r_1 . r_2 . \ldots . r_{\phi(n)} \equiv r_1 . r_2 . \ldots . r_{\phi(n)} \ (mod\ n) \tag{26}$$

Como mdc ($\prod_{i=1}^{\phi(n)} r_i, n) = 1$*, portanto,*

$$a^{\phi(n)} \equiv 1 \ (mod\ n) \ ♦$$

Teorema da Função de Euler: Para todo número primo p e todo inteiro natural $r \geq 1$, então

$$\phi\,(p^r) = p^r - p^{r-1} \tag{27}$$

Demonstração:

Pela definição de $\phi(n)$ sabe-se que $\phi(p^r)$ é o número de inteiros positivos menores que p^r e relativamente primos comp^r. Os únicos números menores que p^r e não primos com p^r são aqueles divisíveis por p. Os múltiplos de p menores que p^r são p^{r-1}, portanto $\phi(p^r) = p^r - p^{r-1}$. ♦

5 MÉTODOS DE CRIPTOGRAFIA

Um algoritmo de Criptografia é uma sequência de passos utilizados para codificar e decodificar uma mensagem. Esses processos são realizados através da chave criptográfica. Para cada método criptográfico diferente há um algoritmo diferente. Serão apresentados alguns métodos de criptografia a seguir.

5.1 CIFRA DE CESAR

O procedimento utilizado pela Cifra de César é denominado substituição mono alfabética, em que letras estão sempre substituídas por uma letra correspondente. Justamente por ser a pioneira na Criptografia, a Cifra de César, dentre os existentes, é um dos métodos mais fáceis de ser utilizado para codificação e decodificação. Pode ser vista matematicamente como uma congruência modular.

Associando cada letra do alfabeto a um número, tem-se a Tabela 4:

TABELA 4 - ASSOCIAÇÃO ALFABETO E NÚMEROS

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

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

Fonte: Autoria própria (2017)

Por exemplo, a função que codifica uma mensagem na Cifra de César pode ser definida como,

$$C(L) \equiv L+3 \pmod{26}, \tag{28}$$

em que L é o número associado a letra do texto original, e $C(L)$ o número da letra que substituirá a original e denomina-se 3 a chave de codificação.E para decodificar a mensagem basta tomarmos a função inversa,

$$D(S) \equiv S+23 \pmod{26} \tag{29}$$

em que S é o número associado a letra da mensagem codificada, e $D(S)$ o número equivalente a letra na mensagem original, $D(S)$ é a função inversa de $C(L)$. Portanto, para decodificar utiliza-se a chave de codificação.

5.2 CIFRA DE VIGENÈRE

Matematicamente a codificação da Cifra de Vigenère pode ser representada como

$$C_i = P_i + a_i \ (mod\ 26), \tag{30}$$

em que C_i representa o valor de cada letra do texto cifrado, P_i representa o valor da letra do texto original e a_i a quantidade de posições que a letra será deslocada. A decodificação pode ser vista como:

$$P_i = C_i - a_i \ (mod\ 26) \tag{31}$$

5.3 CIFRA DE HILL

Seu processo consiste em fazer m combinações lineares dos *n* símbolos do texto original produzindo assim os *m* símbolos criptografados, não se criptografa letra por letra, mas sim um grupo de letras. Nesse tópico serão apresentados os casos em que as letras (ou símbolos) são agrupadas duas a duas. Para o processo de encriptação, é necessário associar cada símbolo de possível utilização como, por exemplo, as letras do alfabeto, os sinais de pontuação, entre outros, a um número inteiro. Feito isso se deve escolher uma matriz quadrada A de ordem 2 que seja composta por números inteiros e admita inversa, o determinante de A deve ser diferente de zero. Essa matriz A será a chave de encriptação, depois os números devem ser escritos na sequência da associação as letras da frase que serão criptografadas, essa associação é apresentada na Tabela 5, agrupando as letras, e respectivamente a sequência numérica, em blocos pares. Caso tenha-se um número ímpar de letras, adiciona-se uma letra arbitrária para completar o último par. Toma-secada par sucessivo como uma matriz coluna. Multiplica-se a matriz coluna pela matriz A, obtendo assim os números referentes ao símbolo da codificação.

Tabela 5–ASSOCIAÇÃO LETRAS E NÚMEROS

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
01	02	03	04	05	06	07	08	09	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	26

Fonte: Autoria própria (2017)

Tomando a matriz $\begin{pmatrix}1 & 1\\ 2 & 1\end{pmatrix}$ como A, então sua inversa é $A^{-1}=\begin{pmatrix}-1 & 1\\ 2 & -1\end{pmatrix}$, associando cada letra do alfabeto aos números correspondentes, para a frase AMOMATEMATICA tem-se a sequência 01 13 15 13 01 20 05 13 1 20 09 03 01, como há um número ímpar de letras, adiciona-se uma letra qualquer no final da última palavra, respectivamente o número correspondente, no final da sequência.

Para codificara frase tomam-se os pares consecutivos:

AM OM AT EM AT IC AA

que correspondem aos pares da sequência numérica:

01 13 1513 01 20 05 1301 2009 03 01 01

Fazendo cada dupla uma matriz coluna, têm-se:

$P_1=\begin{pmatrix}1\\13\end{pmatrix}$, $P_2=\begin{pmatrix}15\\13\end{pmatrix}$, $P_3=\begin{pmatrix}1\\20\end{pmatrix}$,$P_4=\begin{pmatrix}5\\13\end{pmatrix}$, $P_5=\begin{pmatrix}1\\20\end{pmatrix}$,$P_6=\begin{pmatrix}9\\3\end{pmatrix}$e $P_7=\begin{pmatrix}1\\1\end{pmatrix}$.

Codifica-se a mensagem através da seguinte equação:

$$C_i = \mathrm{A}P_i \pmod{m} \tag{32}$$

Então,codificando o primeiro par, AM, obtém-se:

$$\begin{pmatrix}1 & 1\\ 2 & 1\end{pmatrix}\begin{pmatrix}1\\13\end{pmatrix}=\begin{pmatrix}14\\15\end{pmatrix} \pmod{26}.$$

Obtendo assim, pela Tabela 5,a codificação NO. Codificando o segundo par OM, obtém-se:

$$\begin{pmatrix}1 & 1\\ 2 & 1\end{pmatrix}\begin{pmatrix}15\\13\end{pmatrix}=\begin{pmatrix}28\\43\end{pmatrix}=\begin{pmatrix}2\\17\end{pmatrix} \pmod{26}.$$

Obtendo assim, pela Tabela5, a codificação BQ.Codificando o par AT, tem-se:

$$\begin{pmatrix}1 & 1\\ 2 & 1\end{pmatrix}\begin{pmatrix}1\\20\end{pmatrix}=\begin{pmatrix}21\\22\end{pmatrix} \pmod{26}.$$

Obtendo assim, pela Tabela 5, a codificação UV. Codificando o par EM, obtém-se:

$$\begin{pmatrix}1 & 1\\ 2 & 1\end{pmatrix}\begin{pmatrix}5\\13\end{pmatrix}=\begin{pmatrix}18\\43\end{pmatrix} \pmod{26}.$$

Obtendo assim, pela Tabela 5, a codificação RW.Codificando o par AT, obtém-se:

$$\begin{pmatrix}1 & 1\\ 2 & 1\end{pmatrix}\begin{pmatrix}1\\20\end{pmatrix}=\begin{pmatrix}21\\22\end{pmatrix} \pmod{26}.$$

Obtendo assim, pela Tabela 5, a codificação UV.Codificando o par IC, obtém-se:

$$\begin{pmatrix}1 & 1\\ 2 & 1\end{pmatrix}\begin{pmatrix}9\\ 3\end{pmatrix} = \begin{pmatrix}12\\ 21\end{pmatrix} \pmod{26}.$$

Obtendo assim, pela Tabela 5, a codificação LU. Codificando o par AA, obtém-se:

$$\begin{pmatrix}1 & 1\\ 2 & 1\end{pmatrix}\begin{pmatrix}1\\ 1\end{pmatrix} = \begin{pmatrix}2\\ 3\end{pmatrix} \pmod{26}.$$

Obtendo assim, pela Tabela 4, a codificação BC.

Portanto, a frase AMOMATEMATICA cifrada utilizando a Cifra de Hill com a matriz $A = \begin{pmatrix}1 & 1\\ 2 & 1\end{pmatrix}$ é

NOBQUVRWUVLUBC.

Para decodificar realiza-se o mesmo processo, agora com a sequência numérica associada à mensagem cifrada e a matriz utilizada é a inversa de A, a matriz $A^{-1} = \begin{pmatrix}-1 & 1\\ 2 & -1\end{pmatrix}$.

5.4 CRIPTOGRAFIA RSA

Como foi dito anteriormente, codificar e decodificar mensagens pelo método RSA requer duas chaves, uma pública e outra privada. Para codificar devem-se tomar dois números primos *p* e *q*. É importante ressaltar que para que haja segurança é necessário que os números primos escolhidos tenham grande quantidade de algarismos. A chave pública *(n, e)* é formada por $n=pq$, em que *p* e *q* são números primos determinados, e *e* um número inteiro menor que $\phi(n)$, tal que, $mdc(\phi(n),e)=1$.

Para decodificar uma mensagem é necessário possuir a chave privada *(n,d)*, em que *n* é o mesmo da chave pública e *d* é o número inverso de *e* (tomado da chave pública) módulo $\phi(n)$.

É necessário trabalhar com números para aplicação do método, isto é, substituir letras e símbolos por números. Portanto, inicia-se o processo com uma pré-codificação da mensagem, transformando a sequência que se deseja criptografar em uma sequência numérica. Essa sequência será quebrada em blocos, os quais não precisam ter o mesmo tamanho, mas devem seguir a regra: cada bloco deve ter valor menor que *n*.

Com os blocos formados pode-se dar início ao processo de codificação. Denota-se por B_i, $i=1, 2, ..., k$ cada bloco. Para cada B_i tem-se:

$$B^{\phi(n)} \equiv 1\ (mod\ n) \tag{33}$$

em que, pela definição da função de Euler:

$$\phi(n) = \phi(p)\phi(q) = (p-1)(q-1) \tag{34}$$

Denotam-se por $C(B_i)$ cada bloco codificado, e para calculá-los basta utilizar a congruência:

$$B_i^{\,e} \equiv C(B_i)\ \ (mod\ n) \tag{35}$$

Para realizar o processo de decodificação realiza-se o processo inverso, porém para tal é necessário conhecer *d*, *d* é o valor inteiro tal que:

$$ed \equiv 1\ \ (mod\ \phi(n)) \tag{36}$$

Para calcular *d*, portanto, é preciso conhecer $\phi(n)$ e para calcular $\phi(n)$são utilizados os números *p* e *q*. Mas, se *n* é um número de ordem muito grande, fatorar *n* torna-se um processo inviável, por isso somente o legítimo destinatário, que possui os números *p* e *q* é capaz de decodificar, ou seja, ler o conteúdo da mensagem.

Tanto o receptor quanto o emissor precisam ter acesso à chave *(n, e),* e mesmo um terceiro pode ter acesso a essa chave, pois, se *n* possui grande quantidade de dígitos o conhecimento de *(n,e)* não leva a decifração da mensagem. Somente o receptor deve ter acesso a chave *(n,d)* visto que *d* será utilizado para decodificar a mensagem e só é possível calcular *d* a partir de *p* e *q*.

Para decodificar a mensagem utiliza-se a função

$$B_i \equiv C(B_i)^d (mod\ n) \tag{37}$$

em que B_i, *i=1, 2,..., k* é cada bloco do texto original e $C(B_i)$ cada bloco do texto cifrado.

Para que o algoritmo seja considerado seguro e viável deve ser relativamente fácil calcular $B_i^{\,e}\ (mod\ n)$, $C(B_i)^d\ (mod\ n)$, e inviável determinar *d* sendo conhecidos *e* e *n*.

Um exemplo simples do método RSA:

Para que seja fácil a compreensão do algoritmo,serão selecionados *p* e *q* com pequeno comprimento, contudo, é importante relembrar que na prática são tomados números com cerca de 100 dígitos. Seja *p=3* e *q=11*, então *n=33*, o par que forma a chave pública é dado por *(n,e).* Para determinar *e* basta selecionar um número primo menor que *n* e relativamente primo com *n*. Pode-se escolher, por exemplo, *e=7.* Portanto, para calcular *d*, utiliza-se:

$$ed \equiv 1 \ (mod\ \phi(n)) \tag{38}$$

em que *e=7* e $\phi(n)$*=(3-1).(11-1)=20*, logo, *d=3*, visto que:

$$7.3 \equiv 1 \ (mod\ 20)$$

Portanto a chave pública é dada pelo par (33,7) e a chave privada é dada pelo par (33,3).

Para codificar o texto "CRIPTOGRAFIA" primeiramente é necessário associar cada letra do alfabeto a números usando a Tabela 5, e posteriormente escrever a sequência numérica que corresponde ao texto original.

Para que não haja confusão o número 1 será notado como 01, visto que o maior número possui dois algarismos, se caso o maior número possuísse três algarismos o número 1 seria escrito como 001 e o número 13 como 013. Portanto, a palavra CRIPTOGRAFIA é dada pela sequência numérica 031809162015071801060901.

Para codificar a mensagem divide-se a sequência numérica em blocos de maneira que o número máximo de cada bloco seja menor do que *n*. Portanto, serão utilizados os blocos:

031809162015071801060901

Para cifrar cada bloco utiliza-se $B_i{}^e \equiv C(B_i)\ (mod\ n)$, em que B_i é o valor associado a cada bloco da mensagem original e $C(B_i)$ valor associado a cadabloco da mensagem cifrada.

Para B_1=03, tem-se$C(B_1) \equiv (03)^7$ (mod 33) $\Rightarrow C(B_1)$= 09.

Para B_2=18, tem-se $C(B_2) \equiv 18)^7$ (mod 33) $\Rightarrow C(B_2)$= 06.

Para B_3=09, tem-se $C(B_3) \equiv (09)^7$ (mod 33) $\Rightarrow C(B_3)$= 15.

Para B_4=16, tem-se $C(B_4) \equiv (16)^7$ (mod 33) $\Rightarrow C(B_4)$= 25.

Para B_5= 20, tem-se $C(B_5) \equiv (20)^7$ (mod 33) $\Rightarrow C(B_5)$= 26.

Para B_6= 15, tem-se $C(B_6) \equiv (15)^7$ (mod 33) $\Rightarrow C(B_6)$=27.

Para B_7= 07, tem-se$C(B_7) \equiv (07)^7$ (mod 33) $\Rightarrow C(B_7)$= 28.

Para B_8= 18, tem-se $C(B_8) \equiv (18)^7$ (mod 33) $\Rightarrow C(B_8)$= 06.

Para B_9= 01, tem-se $C(B_9) \equiv (01)^7$ (mod 33) $\Rightarrow C(B_9)$= 01.

Para B_{10}=06, tem-se$C(B_{10}) \equiv (06)^7 \pmod{33} \Rightarrow C(B_{10})$= 30.

Para B_{11}=09, tem-se$C(B_{11}) \equiv (09)^7 \pmod{33} \Rightarrow C(B_{11})$=15.

Para B_{12}=01, tem-se$C(B_{12}) \equiv (01)^7 \pmod{33} \Rightarrow C(B_{12})$= 01.

Portanto, a sequência numérica 09 06 15 25 26 27 28 06 01 30 15 01 representa a mensagem original cifrada. Para decifrar a mensagem é necessário *d*, o inverso de *e* módulo *n*. Utiliza-se $B_i \equiv C(B_i)^d \ (mod\ n)$, em que B_i é o valor associado a cada bloco da mensagem original e $C(B_i)$ blocos da mensagem cifrada.

Para $C(B_1)$=09, tem-se $B_1 \equiv (09)^3 \pmod{33} \Rightarrow B_1$= 03

Para $C(B_2)$=06, tem-se $B_2 \equiv (06)^3 \pmod{33} \Rightarrow B_2$= 18

Para $C(B_3)$=15, tem-se $B_3 \equiv (15)^3 \pmod{33} \Rightarrow B_3$= 09

Para $C(B_4)$=25, tem-se $B_4 \equiv (25)^3 \pmod{33} \Rightarrow B_1$= 16

Para $C(B_5)$=26, tem-se $B_5 \equiv (26)^3 \pmod{33} \Rightarrow B_1$= 20

Para $C(B_6)$=27, tem-se $B_6 \equiv (27)^3 \pmod{33} \Rightarrow B_1$= 15

Para $C(B_7)$=28, tem-se $B_7 \equiv (28)^3 \pmod{33} \Rightarrow B_1$= 07

Para $C(B_8)$=06, tem-se $B_8 \equiv (06)^3 \pmod{33} \Rightarrow B_1$= 18

Para $C(B_9)$=01, tem-se $B_9 \equiv (01)^3 \pmod{33} \Rightarrow B_1$= 01

Para $C(B_{10})$=30, tem-se $B_{10} \equiv (30)^3 \pmod{33} \Rightarrow B_1$= 06

Para $C(B_{11})$=15, tem-se $B_{11} \equiv (15)^3 \pmod{33} \Rightarrow B_1$= 09

Para $C(B_{12})$=01, tem-se $B_{12} \equiv (01)^3 \pmod{33} \Rightarrow B_1$= 01

A sequência 03 18 09 16 20 15 07 18 01 06 09 01 refere-se a mensagem original, que pela tabela é possível fazer a correspondência número com a letra e chegar a palavra "CRIPTOGRAFIA".

Portanto, o grande segredo do método RSA está na escolha de *p* e *q,* visto que para realizar o processo de decodificação é necessário conhecê-los e como ainda hoje não existe um algoritmo eficiente para fatoração de um número, o algoritmo é tido seguro para *n* de grande comprimento. Mas não se pode dizer até quando este será seguro visto que existem muitos ataques ao método. Em 1977 estimava-se que uma chave com 155 bits requereria 10^{15}

anos, porém chaves com 155 bits foram atacadas em 8 meses (Barbosa et al., 2003). Atualmente são utilizadas chaves com 300 dígitos (cerca 1000 bits) que devido à grande quantidade de dígitos são consideradas seguras, recomenda-se que p e q tenham a mesma quantidade de dígitos, com o objetivo de dificultar a fatoração de n. Para fatorar um número n com 129 algarismos decimais levaria cinco mil MIPS-anos, sendo que um MIP-ano significa usar um computador que executa um milhão de instruções por segundo durante um ano e utilizando um dos algoritmos mais rápido que se conhece.

A Criptografia RSA além de ser utilizado para codificação e decodificação de mensagens, também é utilizado para gerar assinaturas digitais.

A assinatura digital é utilizada para garantir que o emissor da mensagem seja realmente quem se imagina, para tal o emissor "assina" sua mensagem de modo que comprove a integridade e autenticidade da mesma.

O processo é realizado da seguinte maneira: Sendo P_j e P_m as chaves públicas de João e Maria, respectivamente, as chaves que qualquer um pode ter acesso, e S_j e S_m as chaves privadas (secretas) de João e Maria, respectivamente, aquelas que devem ser mantidas em segredo, pois são as utilizadas na decodificação do conteúdo da mensagem. Se João quer mandar uma mensagem a Maria utilizando o método RSA assinada, ou seja, de modo que Maria tenha certeza que foi João o verdadeiro emissor. João deverá assinar a mensagem, e essa assinatura é feita através das chaves, assim como a codificação do conteúdo da mensagem.

A mensagem enviada a Maria será da forma $N = S_j(P_m(M))$. Sabendo que a mensagem N vem de João, primeiramente Maria aplica P_j, que faz parte a chave pública, e é acessível a qualquer pessoa. P_j é a inversa de S_j, portanto

$$P_j(N) = P_j(S_j(P_m(M)))=P_m(M)$$

A seguir Maria aplica S_m, que é a chave privada de Maria, portanto somente ela tem acesso e é a utilizada para decodificar o texto, assim sendo, tem-se a garantia de que foi João o real emissor da mensagem e é possível ter acesso ao conteúdo.

Tabela 6– ESTIMATIVA DO TEMPO NECESSÁRIO PARA DECIFRAR UM TEXTO CRIPTOGRAFADO PELO MÉTODO RSA

Dígitos	Número de operações	Tempo
50	$1{,}4x10^{10}$	3,9 horas
70	$9{,}0x10^{12}$	104 dias
100	$2{,}3x10^{15}$	74 anos
200	$12,x10^{23}$	$3{,}8x10^{9}$ anos
300	$1{,}5x10^{29}$	$4{,}9x10^{15}$ anos
500	$1{,}3x10^{39}$	$4{,}2x10^{25}$ anos

Fonte: Silva (2006)

As chaves utilizadas na aplicação desse processo tornam o ataque por força bruta impraticável, porém resultam em baixa velocidade para realizar os cálculos necessários.

6 PROPOSTA DE ATIVIDADES INTERATIVAS

Como apresentado nos capítulos anteriores, a Criptografia é uma ciência que utiliza muitos resultados matemáticos, sendo também muito presente no dia a dia de todos que utilizam meios não seguros para trocar informações que não devem ser reveladas a terceiros. Portanto, o estudo da Criptografia é uma boa forma de estimular o interesse dos alunos, sendo sua história e aplicabilidade apresentadas de maneira a despertar a curiosidade dos alunos, e o seu desenvolvimento de maneira a conhecer a importância da matemática nesse processo.

Sendo uma das maiores dificuldades de um professor de Educação Básica despertar o interesse dos alunos, é necessário buscar ferramentas para estimular a curiosidade e mostrar a real importância na história e na atualidade dos assuntos trabalhados, para assim motivá-los. Se o professor conseguir despertar o interesse dos alunos, estes darão maior atenção ao que é ensinado, consequentemente os alunos apresentarão menos dificuldades, pois terão realmente se concentrado, assim todo o processo ensino-aprendizagem torna-se mais natural. Muito tem se falado do uso de tecnologia na Educação, tendo em vista a grande aplicabilidade da Criptografia, sua ligação direta com novas tecnologias e buscando proporcionar o estímulo que o educando precisa, neste capítulo serão apresentados alguns *softwares* e aplicativos sobre Criptografia. Também serão apresentadas atividades que podem ser aplicadas tanto no Ensino Fundamental II e no Ensino Médio e espera-se que sirvam de inspiração para o desenvolvimento de outras atividades.

6.1 *SOFTWARES*

Para introduzir o assunto de Criptografia, pode-se trabalhar a Aritmética Modular usando a Cifra de César. A ideia inicial é usar a Cifra de César para aprender a codificar e decodificar usando substituição.

6.1.1 Roleta de César

O *software* de matemática dinâmica *GeoGebra*® possui inúmeras ferramentas para todos os níveis de ensino, que combina geometria, álgebra, tabelas, gráficos, estatística e

cálculo numa única aplicação.O que possibilita a criação de diversas funções matemáticas, dentre outras aplicações. Em 25 de outubro de 2011, um contribuinte identificado como IMRS adicionou à lista de materiais do *software* GeoGebra online e gratuito um dispositivo para facilitar a cifragem e decifragem de mensagens codificadas pela Cifra de Cesar, denominado “Roleta de César”.

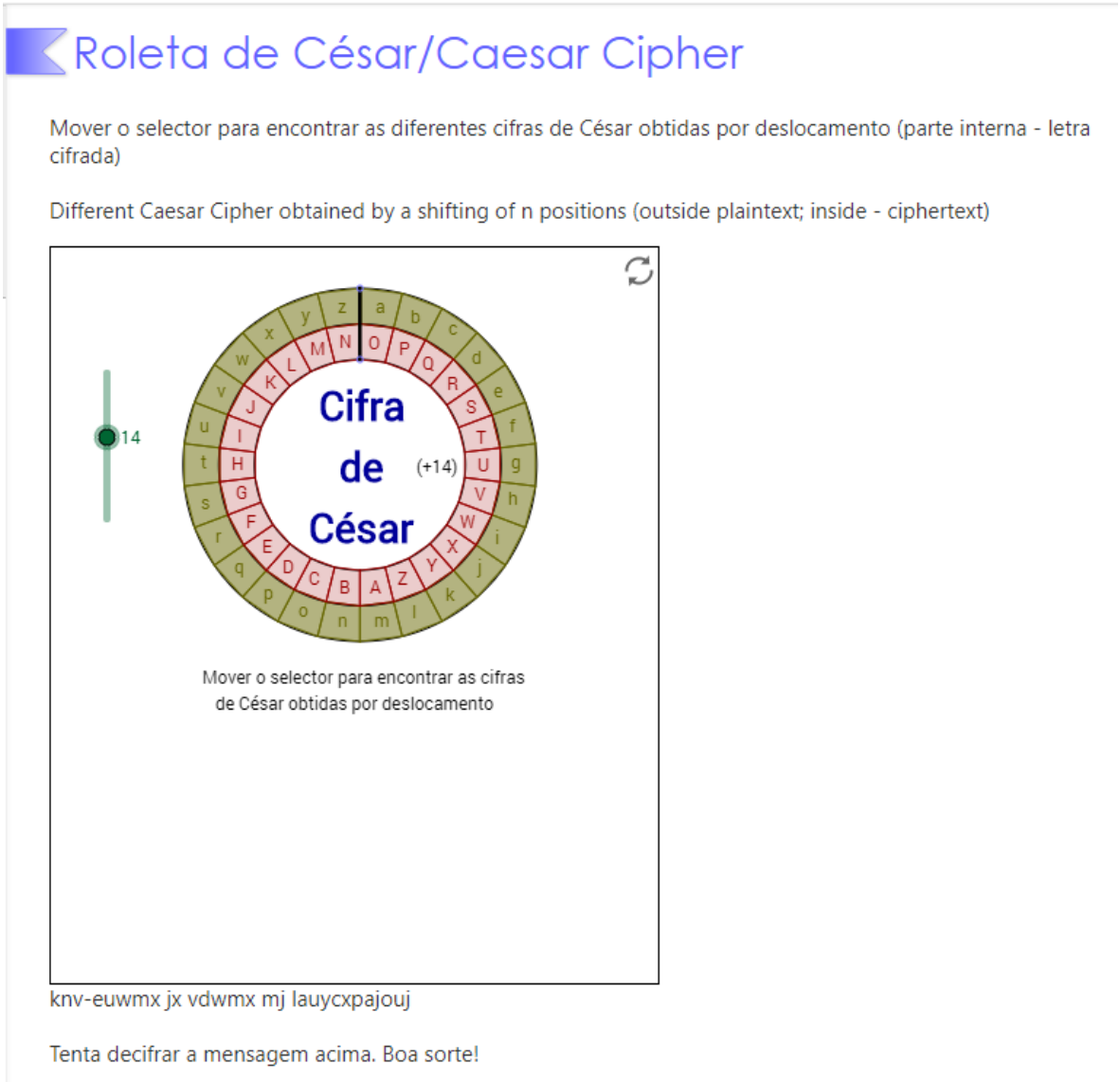


Figura 11 – Roleta de César no *GeoGebra®*.

Fonte: GeoGebra (2017)

A reta vertical a esquerda do disco de cifragem é o mecanismo responsável pela movimentação da circunferência interior, pode-se obter, portanto, 26 cifragens diferentes, sendo que a primeira seria um deslocamento de zero posição, ou seja, seria o próprio alfabeto. A cada posição que se aumenta a coroa circular de cor rosa gira uma unidade para esquerda.

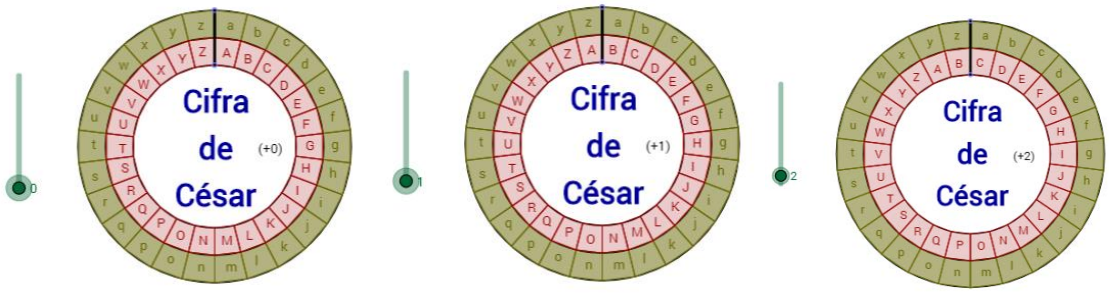


Figura 12 – Exemplos do uso da Roleta de César no *GeoGebra*®.

Fonte: GeoGebra (2017)

Como atividade é sugerido que se tente decifrar a mensagem “knv-euwmx jx vdwmx mj lauycxpajouj”.A mensagem decifrada é “Bem-vindo ao mundo da criptografia”. A roleta de César é uma ótima ferramenta para estimular uma maior participação do aluno no desenvolvimento da atividade. Essa atividade pode ser trabalhada com as turmas do Ensino Fundamental II visto que o grau de dificuldade é baixo, e também com as turmas do Ensino Médio.

Sugestão de Atividade:

Maria encontrou um pedaço de papel em que estava escrito “Dsuhqghqgr d fulswrjudidu”. Sabendo que a mensagem estava criptografada e que a técnica utilizada foi a da Cifra de César, determine o significado do que estava escrito.

Resposta: Aprendendo a Criptografar

6.1.2 Disco para Criptografia de César

Abaixo é apresentado um disco de César desenvolvido por Brian Diniz Amorimda Universidade Federal de Minas Gerais (UFMG) e compartilhado no site em 2012. O funcionamento é basicamente o mesmo do anterior, a diferença está na maneira de movimentar, neste caso deve-se mover o ponto vermelho.

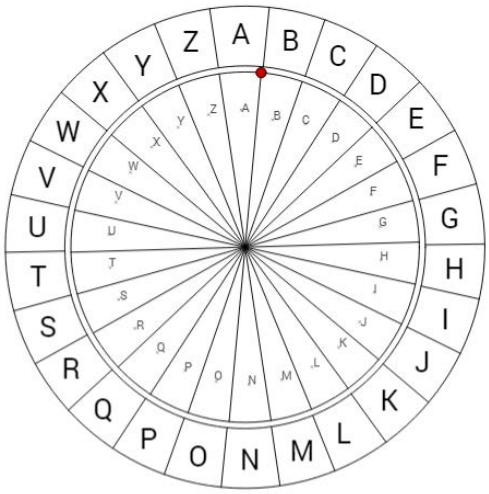


Figura 13 – Disco para Criptografia de César

Fonte: Amorim (2012)

Esta ferramenta assim como a anterior é uma excelente alternativa para ser trabalhada em sala de aula com as turmas do Ensino Fundamental II e a do Ensino Médio. Pode ser disponibilizada uma mensagem sem estar codificada e pedir para que os alunos a codifiquem ou vice-versa, apresentar uma mensagem codificada e pedir que eles a decodifiquem.

Sugestão de atividade

João escreveu em um bilhete uma mensagem para enviar a Paulo, que estava pensando em não mais estudar quando terminasse o Ensino Médio. Quando Paulo recebeu o bilhete leu a seguinte mensagem:

"Y myxromswoxdy o k wksyb bsaeojk aeo kvqeow zyno zyccesb."

A mensagem parecia estar em outra língua, pois, estava criptografada. Contudo João deu uma dica a Paulo, contou-lhe que a mensagem fora criptografada a partir da Cifra estendida de César. Qual foi a mensagem que João mandou a Paulo? Utilize o software apresentado.

Resposta: O conhecimento é a maior riqueza que alguém pode possuir.

6.1.3 Cipher Disk

Ainda trabalhando com o *software GeoGebra®*, a Cifra de César e com o disco, pode ser destacado a atividade abaixo: *Cipher Disk*. A diferença deste para os anteriores está na

facilidade ainda maior para se encriptar uma mensagem, as outras ferramentas facilitam a visualização das substituições que devem ser feitas, contudo a encriptação deve ser feita manualmente, já com esta ferramenta é possível realizar todo o processo pela plataforma. No primeiro campo deve-se escrever a mensagem original quando for desejado codificar uma mensagem, já no segundo campo deve ser escrito a mensagem codificada quando for desejado decodificar. Para determinar o tamanho da chave utiliza-se o segmento de reta horizontal localizado a direita do disco.

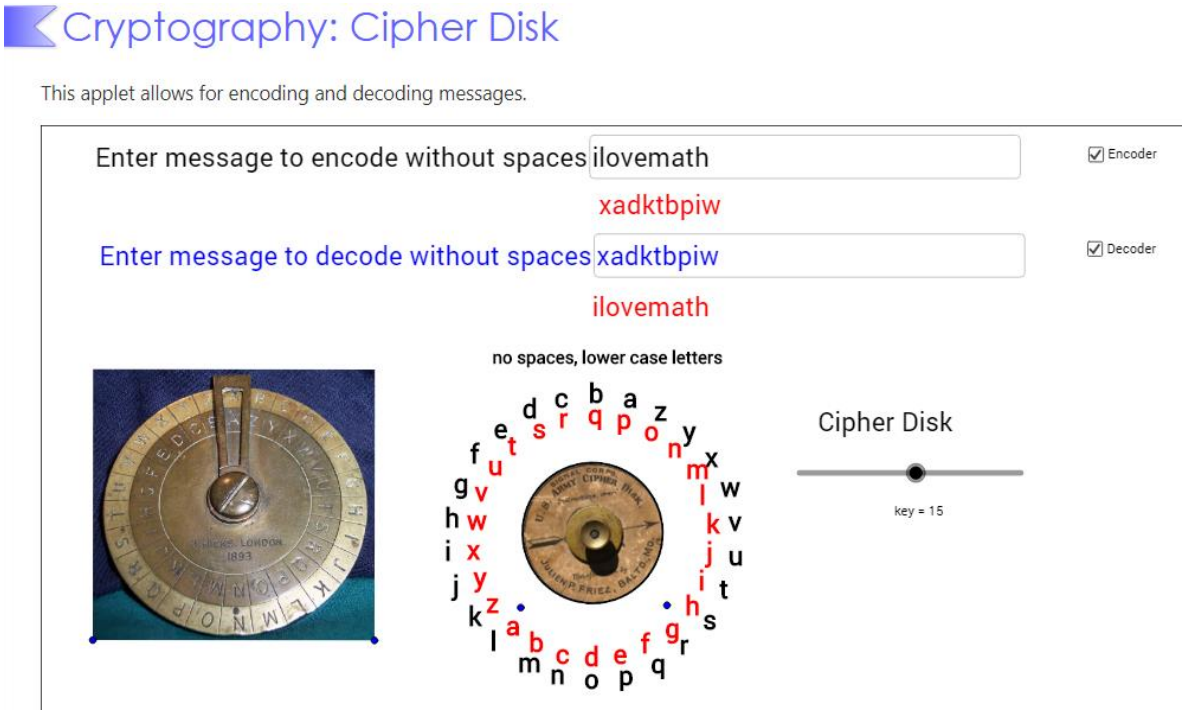


Figura 14 – Cipher Disk no *GeoGebra*®

Fonte: Smiller (2017)

Essa atividade pode ser utilizada como um mecanismo de conferência pelos alunos, visto que quando se escreve a mensagem e se escolhe a chave desejada o próprio programa criptografa e descriptografa a mensagem em questão. Uma boa alternativa para trabalhar com os alunos do Ensino Fundamental II e Ensino Médio é apresentar um dos discos anteriores juntamente com mensagens para que eles codifiquem e decifrem,após o desenvolvimento das atividades, quando os alunos possuírem suas respostas, apresentar essa ferramenta para que eles possam verificar se acertaram.

Sugestão de Atividade

Luan quer fazer um convite a Julia que é fascinada por Matemática, adora estudar e está lendo um livro sobre Criptografia. Como queria que a mensagem tivesse grande importância resolveu enviá-la de maneira diferenciada, optou por Criptografar a mensagem, pois acreditava que assim iria impressionar Júlia, utilizou a Cifra de César e no bilhete escreveu a seguinte mensagem:

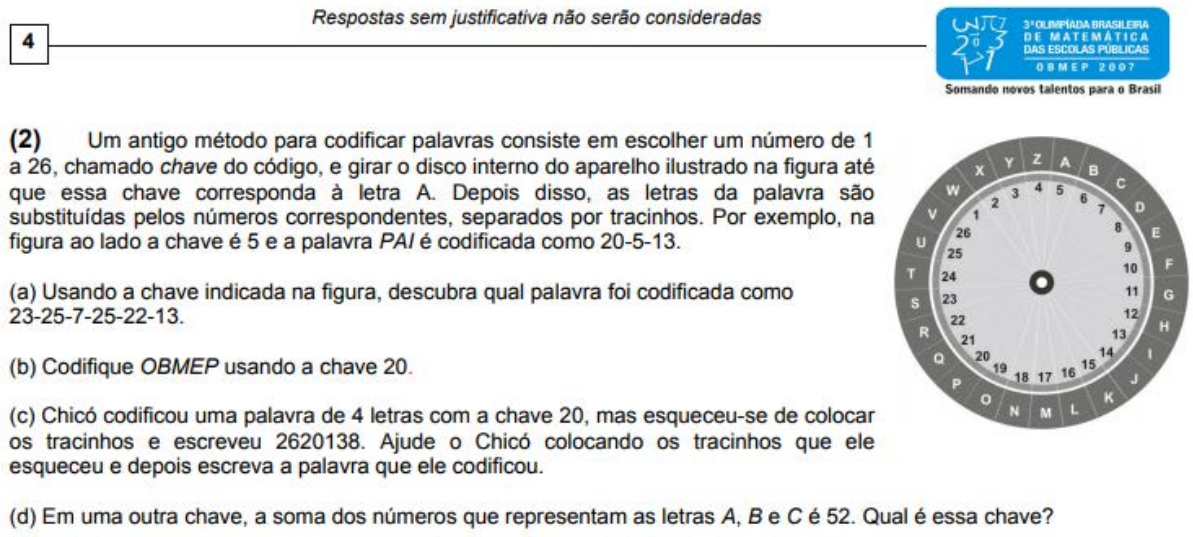
"NGUW SUWALS WKLMVSJ ESLWESLAUS UGEAYG?"

O que Luan escreveu na mensagem? Utilize o software apresentado.

Resposta: Você aceita estudar matemática comigo?

Sugestão de Atividade da OBMEP:

A questão exposta na Figura 15 foi cobrada na prova de segunda fase do Nível 1 da OBMEP em 2017 que é aplicada para alunos dos 6º e 7º anos do Ensino Fundamental II.



Respostas sem justificativa não serão consideradas

4

3ª OLIMPÍADA BRASILEIRA DE MATEMÁTICA DAS ESCOLAS PÚBLICAS
OBMEP 2007
Somando novos talentos para o Brasil

(2) Um antigo método para codificar palavras consiste em escolher um número de 1 a 26, chamado *chave* do código, e girar o disco interno do aparelho ilustrado na figura até que essa chave corresponda à letra A. Depois disso, as letras da palavra são substituídas pelos números correspondentes, separados por tracinhos. Por exemplo, na figura ao lado a chave é 5 e a palavra *PAI* é codificada como 20-5-13.

(a) Usando a chave indicada na figura, descubra qual palavra foi codificada como 23-25-7-25-22-13.

(b) Codifique *OBMEP* usando a chave 20.

(c) Chicó codificou uma palavra de 4 letras com a chave 20, mas esqueceu-se de colocar os tracinhos e escreveu 2620138. Ajude o Chicó colocando os tracinhos que ele esqueceu e depois escreva a palavra que ele codificou.

(d) Em uma outra chave, a soma dos números que representam as letras *A*, *B* e *C* é 52. Qual é essa chave?

Figura 15 – Questão da OBMEP sobre a Cifra de César

Fonte: OBMEP (2017)

O padrão de resposta sugerido pela OBMEP encontra-se na Figura 16.

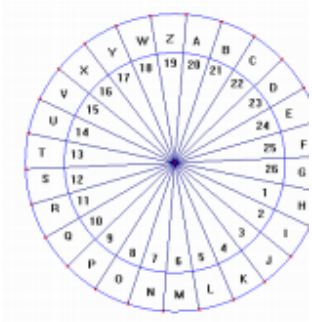
QUESTÃO 2 (a) A partir da figura do enunciado temos 23=S, 25=U, 7=C, 22=R e 13=I. Logo a palavra codificada como 23-25-7-25-22-13 é SUCURI.

(b) Para a chave 20 temos a figura ao lado, onde vemos que O=8, B=21, M=6, E=24 e P=9. Assim, a codificação de OBMEP é 8-21-6-24-9.

Alternativamente, ao passar da chave 5 para a chave 20 devemos somar 15 aos números da figura do enunciado, lembrando que se a soma for maior do que 26 devemos subtrair 26. Assim, temos

$$O = 19+15-26 = 34-26 = 8,\ B = 6+15 = 21,\ M = 17+15-26 = 6,$$
$$E = 9+15 = 24,\ P = 20+15-26 = 9$$

donde OBMEP é codificada como 8-21-6-24-9.



(c) Como não existe letra codificada como 0, um dos números associados a letras na seqüência 2620138 é o 20. À sua direita há três dígitos, mas como não há letra codificada como 138 ou 38, os números associados a letras são o 13 e o 8. Isto dá um total de 3 letras. Portanto, à esquerda de 20 só podemos admitir o 26. Logo, a codificação da palavra é 26-20-13-8, a qual, na chave 20, corresponde a GATO.

(d) Quando somamos três números consecutivos, obtemos um número divisível por 3; por exemplo, $14+15+16 = 45$. Ao somar os números que representam as letras A, B e C nessa certa chave, obtemos 52, que não é um número divisível por 3. Isso mostra que os três números não são consecutivos e isso somente é possível se um dos números for 26 e outro for 1. Como a soma é 52, o terceiro número é $52-27 = 25$. A única codificação de ABC, neste caso, é 25-26-1, ou seja, a chave é 25.

Figura 16 - Padrão de reposta da questão 2 da OBMEP

Fonte: OBMEP (2017)

6.1.4 Criptografar mensagem com matrizes (26 letras)

Também como material de Criptografia presente no *GeoGebra*® existem trabalhos que relacionam o conteúdo de matrizes e determinante. O dispositivo aqui apresentado possui como título *Criptografar mensagem com* matrizes (26 letras), foi acrescido ao *software* por Célio Roberto Januário em maio de 2016. Veja a Figura 17.

Com os seletores (L1 a L26) deve-se escrever a frase que se deseja criptografar, sendo que cada seletor varia de -9 a 26, sendo -9 a 0 os algarismos na ordem crescente e de 1 a 26 as letras do alfabeto, ou seja a frase pode conter palavras e números, com um total de até 26 símbolos. A mensagem é codificada usando a matriz chave 2×2, em que os elementos podem variar de -10 a 10. A multiplicação da matriz formada pela mensagem com a matriz chave gera a matriz codificada Mc 2×13. É imprescindível a verificação do determinante da matriz chave, ele deve ser diferente de zero. Um número mudado na chave altera a matriz criptografada.

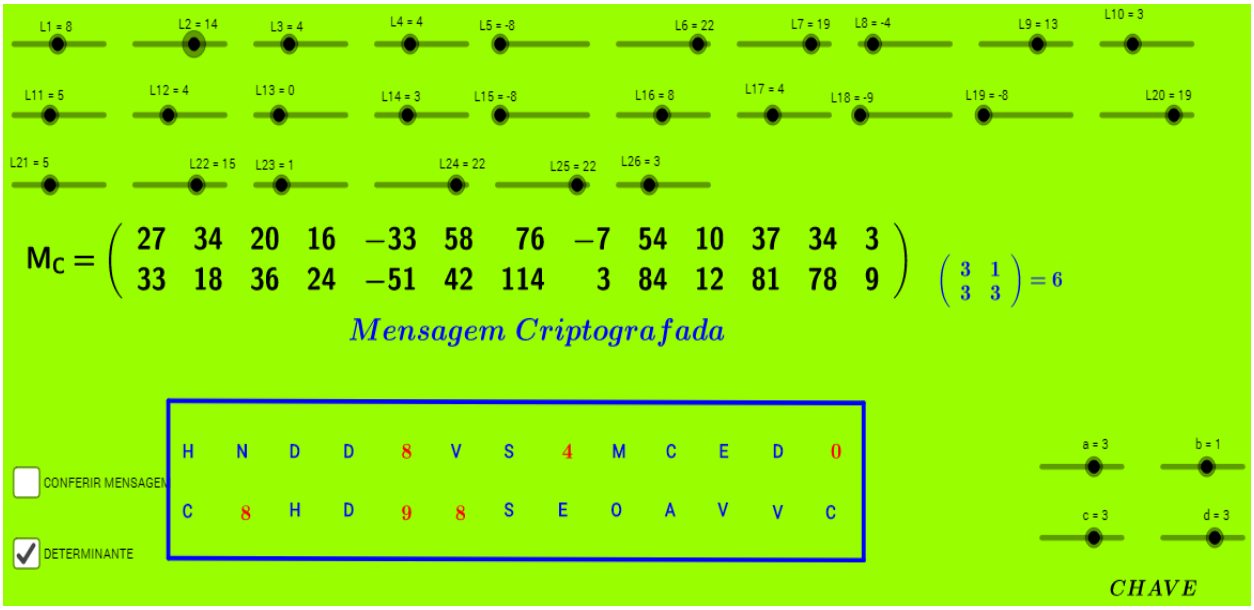


Figura 17 – Tela do *Criptografar mensagem com matrizes (26 letras)*

Fonte: Januário (2017)

No endereço tem-se o processo similar ao apresentado, porém para matrizes com dez letras.

Esse instrumento é uma boa alternativa para se trabalhar multiplicação de matrizes com alunos nos anos finais do Ensino Médio. Ao apresentar a Criptografia e a aplicabilidade que se tem das matrizes nesse campo, poderão ser trabalhados com os alunos mensagens para eles criptografarem e posteriormente podem utilizar essa ferramenta para corrigirem suas respostas.

Sugestão de atividades

Atividade 1

Maria pediu para José entregar um bilhete para Helena, como Maria não queria que José e nenhuma outra pessoa tivessem acesso à mensagem que quisera enviar a Helena, ela resolveu criptografar a mensagem utilizando matrizes, sendo assim determine a matriz presente no bilhete entregue por José, sabendo que a mensagem a ser criptografada é “Passei no vestibular em Araras” e que a matriz chave utilizada para criptografar a mensagem foi $A=\begin{pmatrix}2 & 1\\ 3 & 2\end{pmatrix}$.

Resposta: *Para realizar o cálculo de codificação à mão é necessário calcular o produto AN, em que N é a matriz com as letras associadas a números.*

$$M_C = \begin{pmatrix} 34 & 23 & 50 & 39 & 28 & 23 & 42 & 31 & 62 & 11 & 56 & 41 & 37 \\ 52 & 45 & 81 & 59 & 51 & 37 & 70 & 47 & 102 & 17 & 93 & 62 & 65 \end{pmatrix}$$

Atividade 2

Utilizando a criptografia pelo processo envolvendo matrizes, criptografe a frase MULTIPLICANDO MATRIZES, utilizando a matriz A= $\begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}$ como chave de criptografar.

Resposta:

$$M_C = \begin{pmatrix} 104 & 68 & 136 & 150 & 72 & 178 & 61 & 122 & 9 & 3 & 42 & 12 & 45 \\ 39 & 23 & 52 & 56 & 27 & 68 & 22 & 47 & 3 & 1 & 14 & 4 & 15 \end{pmatrix}$$

6.1.5. "*Simple Caesar Cipher*"

Uma fonte ainda mais rica em ferramentas matemáticas é o mecanismo computacional denominado *Wolfram Alpha*®, está disponível em uma plataforma online parcialmente gratuita, esse dispositivo não se restringe apenas a Matemática, abrange áreas como Biologia, Física, Computação, entre outros. Um dos tópicos existentes no site é Criptografia.

Pode-se ter acesso a demonstração do funcionamento de diferentes programas, o primeiro programa aqui trabalhado é o da Cifra de César (este programa está disponível para download no endereço http://demonstrations.wolfram.com/SimpleCaesarCipher/. Na imagem a seguir a linha horizontal *encoding offset* é iterativa e responsável pela quantidade de deslocamento do alfabeto. Com o programa é possível tanto codificar como também decodificar uma mensagem pela Cifra de César.

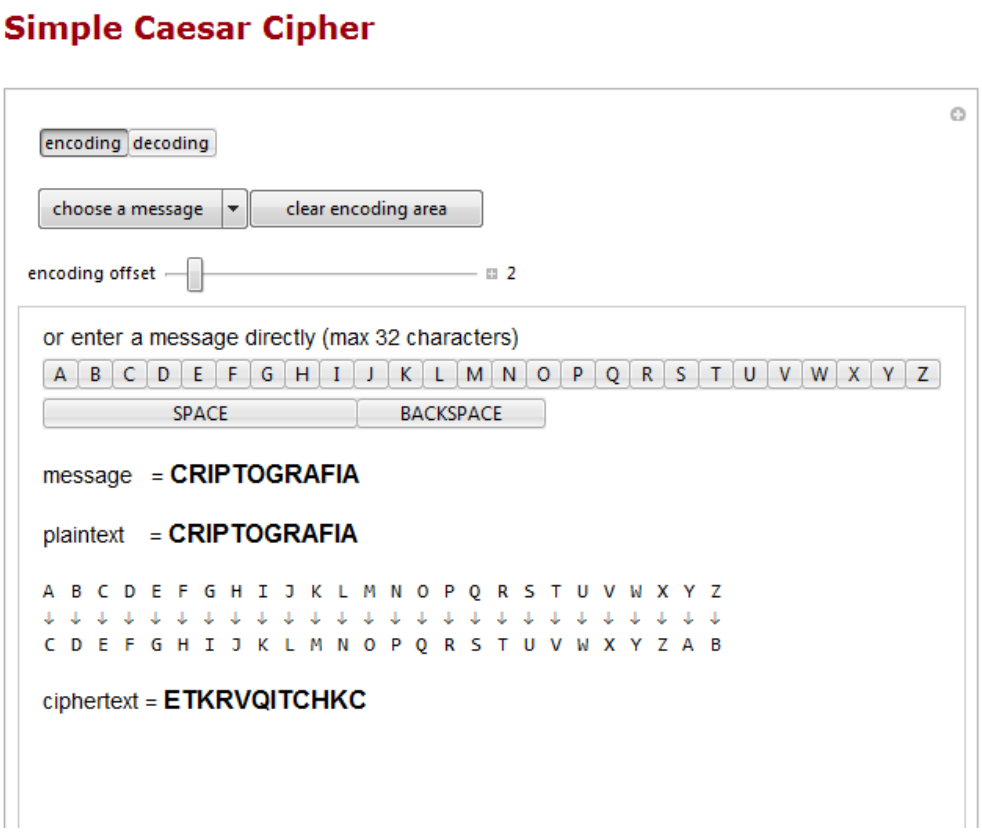


Figura18 – Tela do Simple Caesar Cipher

Fonte: Graham (2013)

Como pode ser observado na Figura 18, para se codificar e decodificar mensagem escreve-se o alfabeto na horizontal e abaixo o mesmo alfabeto com o deslocamento desejado. Essa atividade permite uma excelente visualização das substituições a serem feitas e ainda já disponibiliza a mensagem cifrada quando dado a mensagem original e a chave de codificação, é interessante ressaltar que também é possível realizar o processo inverso.

Por ser de fácil manuseio, o programa pode ser utilizado para auxiliar o desenvolvimento de atividades em salas de aula com alunos do Ensino Fundamental II e Ensino Médio. Podem-se trabalhar atividades de codificação e decodificação de mensagens. É uma excelente alternativa para estimular o interesse dos alunos e ainda pode ser utilizado como meio de verificação, visto que o próprio programa codifica e decodifica mensagens.

Sugestão de Atividade

Após estudarem a Cifra de César, Bruna e Gustavo só trocam mensagens criptografadas por esse método. Bruna perguntou a Gustavo “Qual prova teremos amanhã?” e Gustavo respondeu “Amanhã teremos prova de matemática”. Contudo, sabemos que a

mensagem não foi escrita dessa maneira, visto que ambos utilizam a Cifra de César. Sabendo que Bruna utiliza um deslocamento de 12 posições do alfabeto e Gustavo 21 posições, determine a exata mensagem que foi enviada por Bruna e a que foi enviada por Gustavo.

Resposta: Mensagem da enviada por Bruna "Cgmx bdahm fqdqyae mymztm", enviada por Gustavo "Vhvicv ozmzhjn kmjqv yz hvozhvodxv".

6.1.6 RSA Encrytion and Decryption

Outro programa disponível no *Wolfram Alpha*® é o de Criptografia RSA, este pode ser encontrado no site de endereçohttp://demonstrations.wolfram.com/RSAEncryptionAndDecryption/.

Como se trata de uma demonstração, nem todas as ferramentas existentes estão disponíveis, contudo, as disponibilizadas são suficientes para uma introdução à Criptografia RSA.

Para codificar ou decodificar uma mensagem utiliza-se o processo já descrito anteriormente seguindo os intervalos estipulados pelo programa. O número *n*, produto de dois números primos *p* e *q* no caso desse programa ambos menores que 100, que faz parte tanto da chave pública como da privada deve ser tomado entre 899 e 8633 inclusive. É importante relembrar que a chave pública é formada por *(n,e)* e a chave privada é formada por *(n,d)*, para simplificação de cálculos *e* é determinado e seu valor é 17, e o número *d* varia de acordo com *n*, visto que *d* é o inverso modular de *e* módulo $\phi(n)$.

Primeiramente deve ser escolhido o valor de *n*. No exemplo a seguir foi tomado *n*=899, depois se seleciona as letras que deseja criptografar, sendo que se podem criptografar três letras por vez. No exemplo das Figuras 19a e 19b foi criptografada a sequência AAA. O próximo passo é enviar a mensagem que é cifrada pelos métodos já vistos (Figura 20), como é sabido, para criptografar com o método RSA é necessário trabalhar com números. A associação aqui estabelecida para obter-se as letras associadas a números é a da tabela ASCII. Como no programa em questão não são trabalhados caracteres especiais, como sinais de pontuação e só são trabalhadas letras, é suficiente conhecer apenas uma parte da tabela ASCII (0-127) que se encontrar na Figura 21e um último recurso é a decodificação da mensagem em que é revelado o número *d* da chave privada (Figura 22).

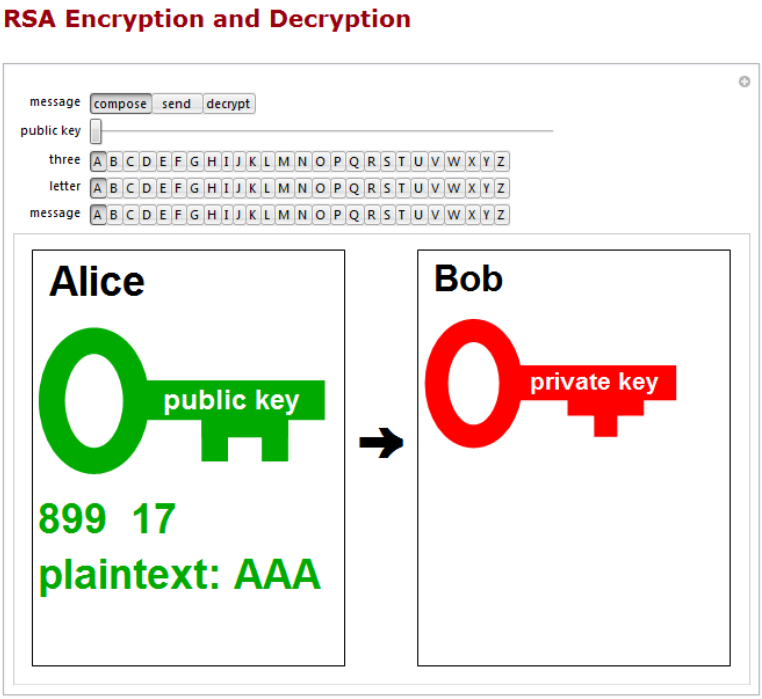


Figura 19a – Primeiro passo para criptografar a sequência AAA.

Fonte: Blinder (2017)

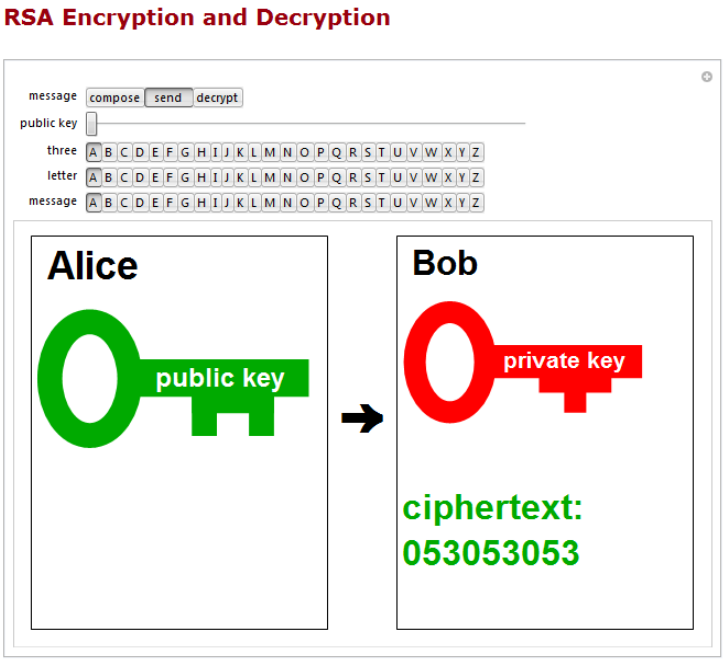


Figura 19b - Segundo passo para criptografar a sequência AAA

Fonte: Blinder (2017)

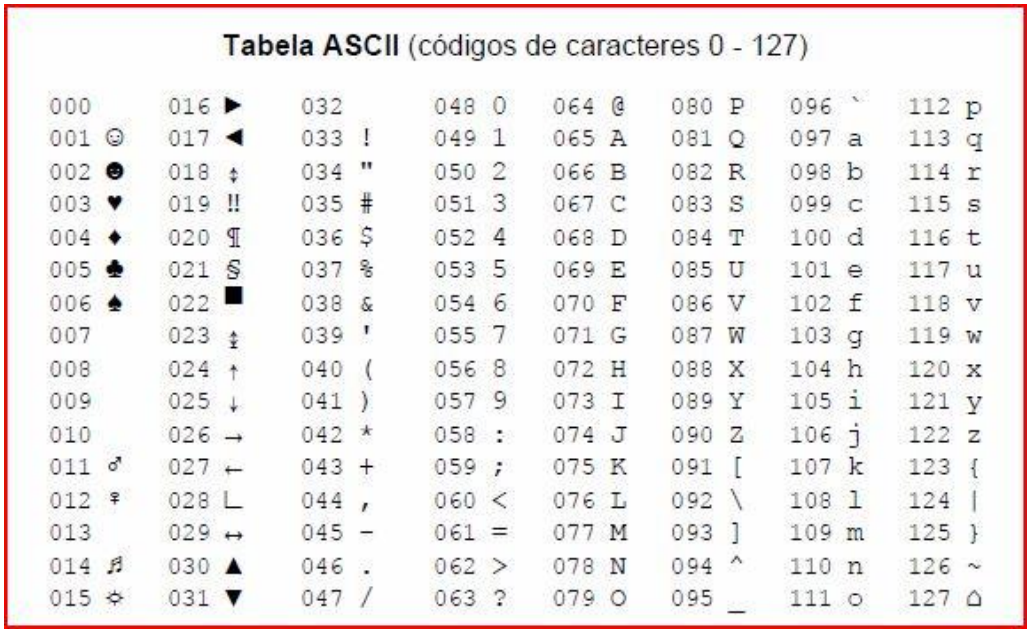


Tabela ASCII (códigos de caracteres 0 - 127)

000	016 ▶	032	048 0	064 @	080 P	096 `	112 p
001 ☺	017 ◀	033 !	049 1	065 A	081 Q	097 a	113 q
002 ☻	018 ↕	034 "	050 2	066 B	082 R	098 b	114 r
003 ♥	019 ‼	035 #	051 3	067 C	083 S	099 c	115 s
004 ♦	020 ¶	036 $	052 4	068 D	084 T	100 d	116 t
005 ♣	021 §	037 %	053 5	069 E	085 U	101 e	117 u
006 ♠	022 ■	038 &	054 6	070 F	086 V	102 f	118 v
007	023 ↨	039 '	055 7	071 G	087 W	103 g	119 w
008	024 ↑	040 (	056 8	072 H	088 X	104 h	120 x
009	025 ↓	041)	057 9	073 I	089 Y	105 i	121 y
010	026 →	042 *	058 :	074 J	090 Z	106 j	122 z
011 ♂	027 ←	043 +	059 ;	075 K	091 [	107 k	123 {
012 ♀	028 ∟	044 ,	060 <	076 L	092 \	108 l	124 |
013	029 ↔	045 -	061 =	077 M	093]	109 m	125 }
014 ♫	030 ▲	046 .	062 >	078 N	094 ^	110 n	126 ~
015 ☼	031 ▼	047 /	063 ?	079 O	095 _	111 o	127 ⌂

Figura 20 – Tabela ASCII

Fonte: Aplicações da Informática (2017)

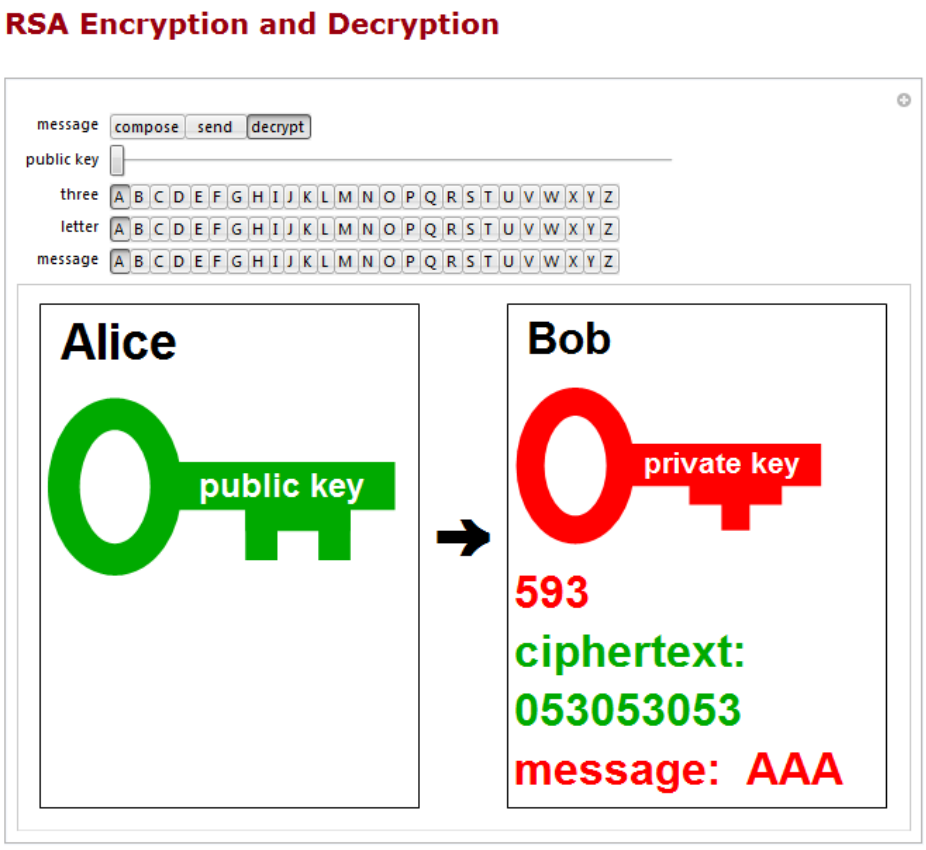


Figura 21 – Decodificação da mensagem AAA.

Fonte: Blinder (2017)

Como pode ser observado na Figura 20, a letra A corresponde ao número 65, portanto para se codificar a mensagem AAA, deve-se codificar o número 65 três vezes sendo a chave pública (17, 899), realizando os cálculos$65^{17} \equiv C\ mod(899)$, obtém-se C=53. Já para se realizar o processe inverso é necessário calcular o número *d*, o inverso modular de *e*, no caso *e*=17, módulo $\phi(n)$. No exemplo anterior tem-se *d*=593.

Esse programa é uma ótima opção para trabalhar a criptografia RSA com alunos da Educação Básica sem utilizar o conceito de congruência e utilizando apenas aritmética modular. As atividades podem ser desenvolvidas com alunos dos anos finais do Ensino Fundamental II e alunos do Ensino Médio.

Após apresentar a Criptografia e o método RSA, deve-se também apresentar e ressaltar a importância da tabela ASCII, não apenas para a Criptografia como também para tudo relacionado a computação, e então pode ser feita uma atividade em que os alunos devem codificar três letras.

Sugestão de atividade

Utilizando o *RSA Encryption and Decryption* do *softwareWolfram Alpha®*, como verificação dos cálculos. Codifique a sequência A A A, sendo n = 899 e d=17.

6.2 APLICATIVOS PARA ANDORID

É possível também encontrar diversos aplicativos de Criptografia. Serão destacados aqui aqueles que mais se aproximam dos métodos explorados neste trabalho.

6.2.1 *Decrypto*

O primeiro apresentado é o *Decrypto,* que possui diversas técnicas de criptografar e descriptografar um texto. O aplicativo possui relativo destaque tendo, até a presente data, mais de 100.000 *downloads*. No menu do aplicativo são disponibilizadas diversas ferramentas, como se pode observar na Figura 22. Para codificar uma mensagem pode-se utilizar diferentes métodos, como é apresentado nas Figuras23a e 23b.

Figura 22 – Tela do aplicativo *Decrypto*

Fonte: Aplicativo *Decrypto* (2017)

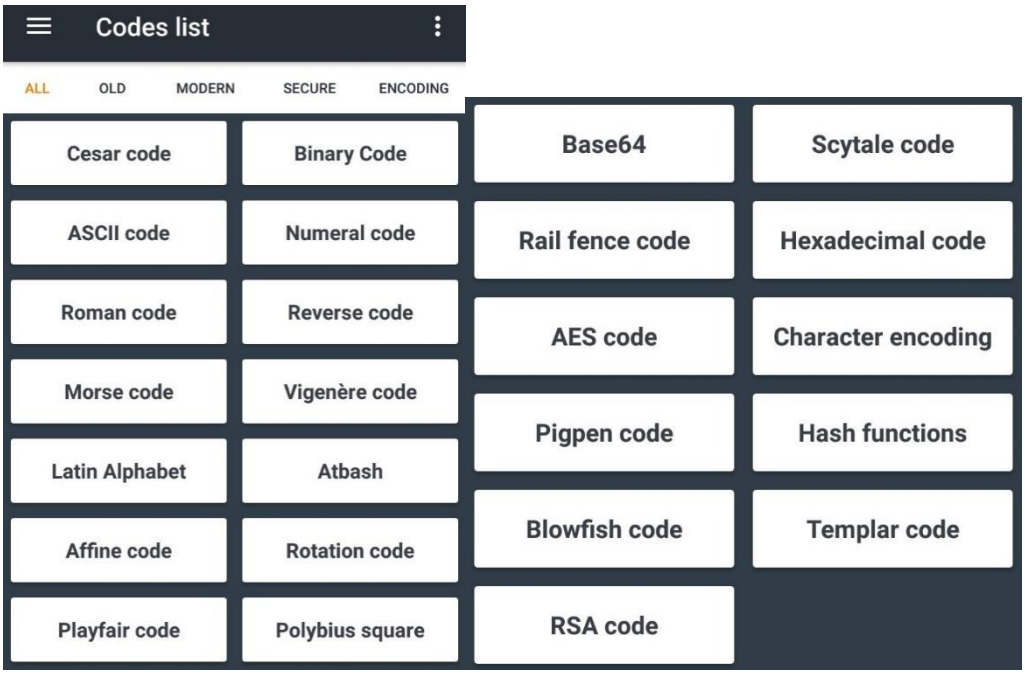


Figura 23 – Métodos de codificar do aplicativo *Decrypto*

Fonte: Aplicativo *Decrypto* (2017)

Tratando-se de codificar, os métodos que serão mostrados são Cifra de Cesar e Cifra de Vigenère, não descartando a importância e eficácia dos outros. Assim como manualmente, para se codificar uma mensagem utilizando a Cifra de César é necessário que se determine a quantidade de deslocamento desejada, é com base nos cálculos da definição que o processo é realizado. Como pode ser observado na Figura 24 da esquerda, existem três principais campos, o primeiro no qual se deve escrever a mensagem, o central que se deve determinar a

chave, ou seja, o deslocamento, e por fim o local em que é dada a mensagem codificada. Se desejasse utilizar a Cifra de Vigenère, o processo é basicamente o mesmo: são três principais campos, no primeiro insere-se a mensagem original, também chamada de texto plano, no segundo a chave, que no caso desse método é uma palavra, e por último é apresentado o resultado final, a mensagem criptografada com a senha escolhida, como na Figura 24 da direita

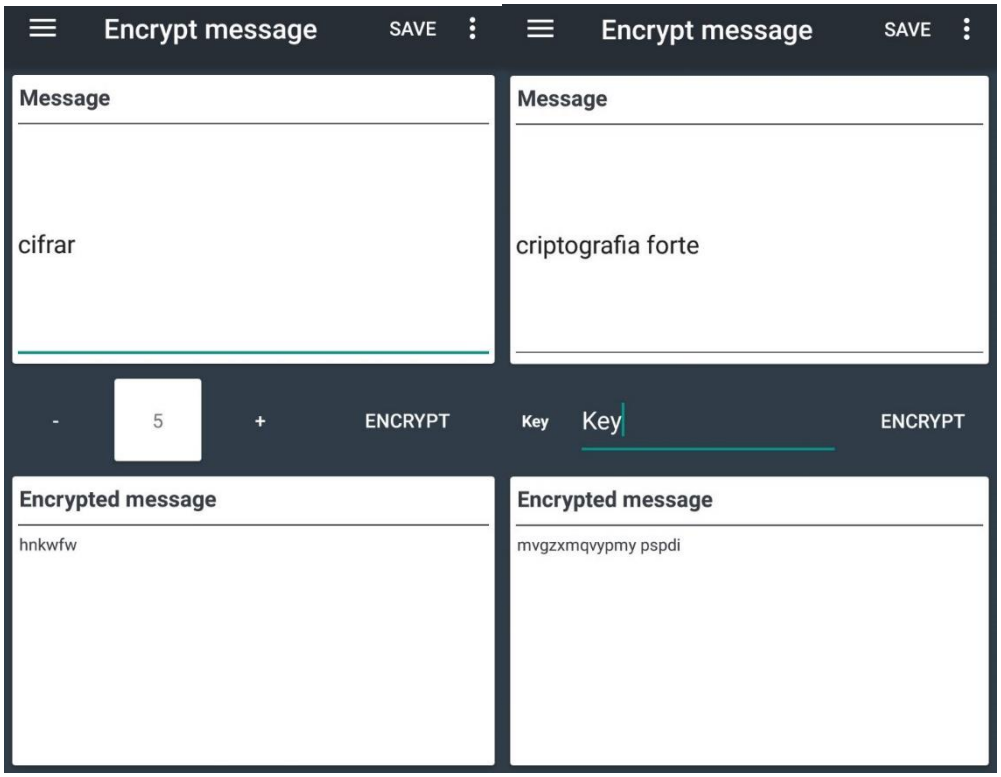


Figura 24 – Métodos de codificar do aplicativo *Decrypto*

Fonte: Aplicativo *Decrypto* (2017)

Um recurso deste aplicativo que também merece destaque é a análise de frequência das letras presentes em um texto.

Foi analisada a primeira parte do hino nacional brasileiro, obtendo como resultado da análise de frequência o seguinte histograma (Figura 25).

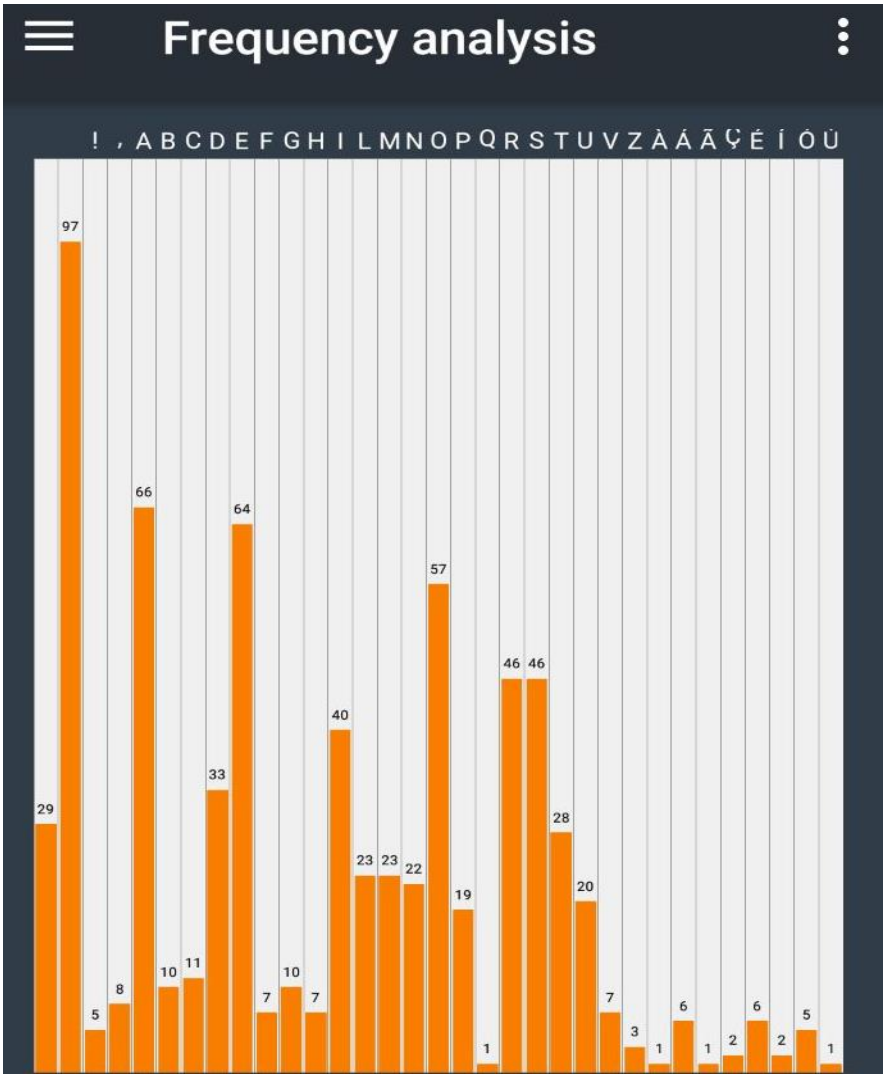


Figura 25 – Análise da frequência de letras do Hino Nacional

Fonte: Aplicativo *Decrypto* (2017)

Esse aplicativo por possuir diversas funções pode estimular ainda mais a curiosidade do aluno e fazer com que o mesmo tenha interesse em explorar as diferentes aplicações. Se viável de ser trabalhado, visto que é necessário ter aparelhos eletrônicos para que se possa instalar os aplicativos, é uma boa alternativa para despertar um maior envolvimento do aluno na atividade. Podem ser desenvolvidas atividades tanto quanto a Cifra de césar, Cifra de Vigenère, como ainda pode-se pedir para que os alunos explorem o aplicativo conhecendo também a tabela ASCII, o código Morse, entre outros.

Sugestão de Atividade

Atividade 1

A seguir é apresentado um poema de um escritor brasileiro que escreve em português.

Jhujhv kv lepspv

Tpuoh alyyh alt whstlpyhz,
Vukl jhuah v Zhiph;
Hz hclz, xbl hxbp nvyqlpht,
Uhv nvyqlpht jvtv sh.
Uvzzv jlb alt thpz lzaylshz,
Uvzzhz chyglhz alt thpz msvylz,
Uvzzvz ivzxblz alt thpz cpkh,
Uvzzh cpkh thpz htvylz.
Lt jpzthy, zvgpuov, h uvpal,
Thpz wyhgly lujvuayv lb sh;
Tpuoh alyyh alt whstlpyhz,
Vukl jhuah v Zhiph.

Tpuoh alyyh alt wyptvylz,
Xbl ahpz uhv lujvuayv lb jh;
Lt jpzthy — zvgpuov, h uvpal —
Thpz wyhgly lujvuayv lb sh;
Tpuoh alyyh alt whstlpyhz,
Vukl jhuah v Zhiph.

Uhv wlytpah Klbz xbl lb tvyyh,
Zlt xbl lb cvsal whyh sh;
Zlt xbl klzmybal vz wyptvylz
Xbl uhv lujvuayv wvy jh;
Zlt xb'pukh hcpzal hz whstlpyhz,
Vukl jhuah v Zhiph

Como você pode observar a mensagem não está clara. Mesmo que mostrada a diversos brasileiros, todos sabendo ler e escrever, ainda assim não é possível dizer o conteúdo do poema, o que se deve ao fato do texto estar criptografado. Ou seja, a mensagem foi propositalmente transformada para que não fosse lida por qualquer pessoa, e sim apenas por aquela que possui a chave para descriptografar, isto é, ter acesso ao real conteúdo da mensagem. Mas o emissor da mensagem não contava que antes de chegar ao destinatário a mensagem fosse interceptada por você, que possui conhecimento sobre Cifras de César. Utilizando o aplicativo *Decrypto*:

a) Faça uma análise de frequência das letras do poema codificado.

b) A partir da análise do item (a) é possível determinar a chave de codificação?

c) Decifre o poema.

Resposta: Poema decifrado

Canção do exílio

Minha terra tem palmeiras,
Onde canta o Sabiá;
As aves, que aqui gorjeiam,
Não gorjeiam como lá.

Nosso céu tem mais estrelas,
Nossas várzeas têm mais flores,
Nossos bosques têm mais vida,
Nossa vida mais amores.

Em cismar, sozinho, à noite,
Mais prazer encontro eu lá;
Minha terra tem palmeiras,
Onde canta o Sabiá.

Minha terra tem primores,
Que tais não encontro eu cá;
Em cismar — sozinho, à noite —
Mais prazer encontro eu lá;
Minha terra tem palmeiras,
Onde canta o Sabiá.

Não permita Deus que eu morra,
Sem que eu volte para lá;
Sem que desfrute os primores
Que não encontro por cá;
Sem qu'inda aviste as palmeiras,
Onde canta o Sabiá.

Gonçalves Dias

Atividade 2

Após ter uma aula sobre Criptografia, Ricardo resolveu adotá-la para diferentes atividades do seu dia. Em seu horário de estudos ele escreveu o nome da disciplina criptografada pela Cifra de Vigenère. O quadro de horários de segunda-feira contém as seguintes informações:

13h30 às 15h00 MMHVMMHZCM

15h30 às 17h00 PAFKUSIVS

Sabendo que a palavra chave utilizada para codificar às mensagens foi AMOR, determine as disciplinas estudadas por Ricardo na segunda-feira. Utilize o aplicativo *Decrypto.*

Resposta: Matemática e Português.

Atividade 3

Como a maioria das crianças, Renato é muito curioso. Ele gosta muito de aprender aplicações práticas da Matemática, o que levou a se encantar pela ciência Criptografia. Após estudar sobre a história e o funcionamento da Cifra de Vigenère, Renato buscou em diversos sites e livros dados criptografados por esse método.

Sendo "GAXRMGVXRGGUKFIEZNGTQOWRFCLF" uma das frases que Renato decifrou. Determine a frase decifrada sabendo que a palavra chave é CIFRA. Utilize o aplicativo *Decrypto*.

Resposta: Essa mensagem foi criptografada.

Atividade 4

Dária e Gilberto receberam um desafio, vencerá quem cifrar corretamente a frase "A união faz a força" no menor tempo, utilizando a Cifra de Vigenère com a palavra-chave FAMILIA. Gilberto terminou a encriptação primeiro, entretanto quem ganhou o desafio foi Dária, pois Gilberto não criptografou corretamente. Qual foi a frase que Dária escreveu em seu papel?

Resposta: F UZQLW FFZ M NZZCF

6.2.2 *RSA calculator*

Um aplicativo também de grande aplicabilidade é o *RSA calculator*, com ele pode-se criptografar utilizando o método RSA. Diferentemente do *software* apresentado da plataforma *Wolfram Alpha®*, esse aplicativo não possui um intervalo fixado para se escolher os números, sendo possível determinar qualquer *p*, q, *e* e *d*. Deve-se ter bastante atenção ao determinar esses números, pois o aplicativo realiza os cálculos dos métodos RSA, mas não verifica se os números apresentados são primos ou não. É interessante ressaltar que ao utilizar valores pequenos para *p*, q, *e* e *d* busca-se apenas mostrar como se aplicar o método, quando se tratar realmente de informações que se deve manter em sigilo são utilizados números primos grandes, com mais de 100 dígitos. A Figura 26 apresenta a tela inicial do aplicativo.

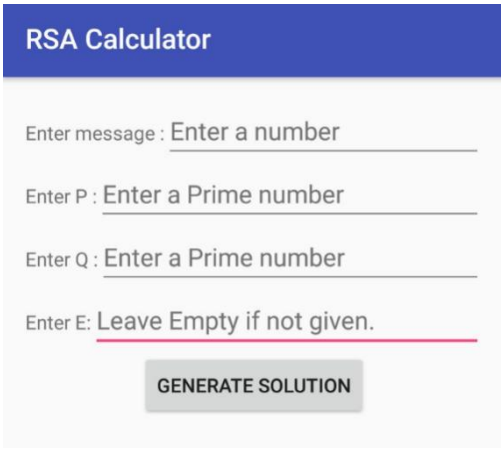


Figura 26: Tela do aplicativo *RSA calculator*

Fonte: Aplicativo *RSA calculator* (2017)

No exemplo anterior foram tomados p=3, q=11, e=7. Esse aplicativo detalha na solução o valor de n, $\phi(n)$, d e da mensagem cifrada. Esse aplicativo pode ser trabalhado com os alunos dos anos finais do Ensino Fundamental II e os alunos do Ensino Médio. Podem ser desenvolvidas atividades em que os alunos devam codificar uma mensagem utilizando o método RSA, e esse mecanismo pode ser utilizado para conferir os cálculos. Veja a Figura 27 que mostra como o aplicativo apresenta o resultado.

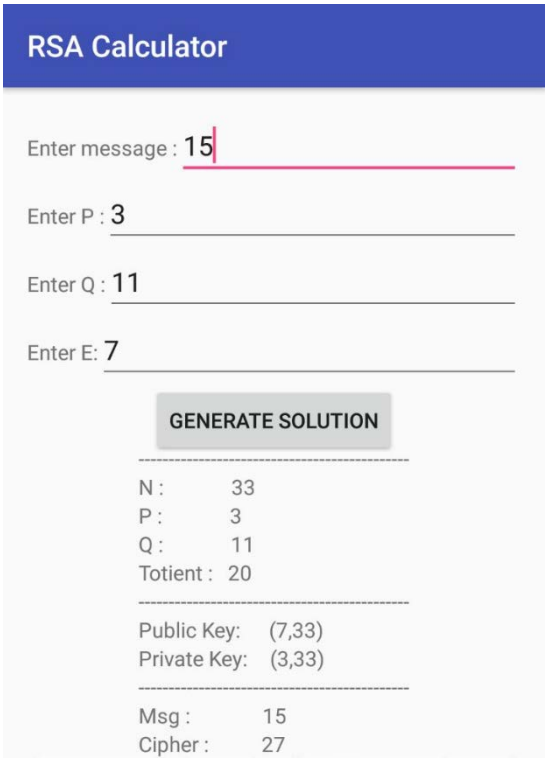


Figura 27: Tela do aplicativo *RSA calculator*

Fonte: Aplicativo *RSA calculator* (2017)

Sugestão de atividades

Com base na tabela ASCII da Figura 20, codifique a mensagem “Criptografia RSA” letra a letra. Utilize o aplicativo *RSA calculator* como verificação dos cálculos.

CONCLUSÃO E TRABALHOS FUTUROS

A Criptografia é crucial para garantir o sigilo e autenticidade de mensagens trocadas em meios não seguros. Com a evolução da tecnologia, os métodos criptográficos também evoluíram e a Matemática é totalmente indispensável para elaboração dos algoritmos que dão origem às cifras.

Após analisar a história e o desenvolvimento dos métodos criptográficos fica claro o quão importante a Criptografia foi, e vêm sendo cada vez mais importante para a sociedade. Nos dias atuais, com a grande utilização de meios não seguros para troca de informações é indispensável que se faça testes para verificar a segurança e eficácia dos métodos que mantém esses dados secretos em sigilo.

Assim como os métodos anteriores foram seguros durante um certo período em suas respectivas épocas, o RSA é seguro atualmente, mas isso não significa que sempre será. Não é possível dizer que o método RSA é indecifrável, e muito menos até quando ele será seguro, ou se ele deixará de ser seguro. É interessante ressaltar a importância da utilização dos números primos para manter a segurança que se tem hoje nesse método. Portanto, se houver o surgimento de um algoritmo de fatoração eficaz, não haverá mais a segurança do método RSA. Sendo assim, os estudos sobre as cifras utilizadas na Criptografia são constantemente questionados e repensados, sujeitos a descoberta de como torná-los não mais úteis e, paralelamente, têm-se o desenvolvimento de novas cifras.

Com o intuito de evidenciar a relação entre a Matemática e a Criptografia e buscando uma maneira de relacionar conteúdos matemáticos trabalhados em salas de aula à diversas situações que podem vir a despertar o interesse dos alunos pelo tema, esse trabalho apresentou um breve resumo histórico da evolução das diferentes cifras utilizadas desde a antiguidades para Criptografar mensagens, o desenvolvimento e aplicações das cifras apresentadas, sendo elas a Cifra de César, Cifra de Vigenère, Cifra de Hill, a máquina Enigma e o método RSA. Por fim foram detalhados alguns *softwares* e aplicativos que exploram as cifras expostas e atividades a serem desenvolvidas com essas ferramentas.

As atividades propostas com o uso de *softwares* e aplicativos busca solucionar alguns problemas encontrados nas escolas, mais especificamente nas salas de aulas, são eles a dificuldade que o professor possui para estimular o interesse dos alunos, ter uma aula dinâmica e interativa, e também a necessidade da utilização de novas tecnologias, visto que a

escola deve acompanhar o avanço tecnológico que ocorre na sociedade. Almeja-se que essa proposta possa contribuir positivamente na elaboração de aulas de Matemática.

Por se tratar de situações tão presentes nos dias atuais, discorrer sobre o tema em salas de aula tem enormes chances de levar a um grande envolvimento dos alunos, despertando curiosidade e vontade de aprender. Espera-se que o presente trabalho contribua positivamente na Educação Básica de jovens e até mesmo adultos e sirva de modelo para o planejamento de aulas de professores.

Com base em tudo que foi apresentado, uma das possibilidades de trabalhos futuros é o desenvolvimento de *softwares* ou aplicativos de Criptografia voltados para utilização em sala de aula, isto é, mais didático, de fácil manipulação e interativo. Uma segunda recomendação é trabalhar com outros métodos criptográficos de maneira similar. Espera-se que sejam realizados trabalhos explorando os métodos conforme estes forem sendo criados.

REFERÊNCIAS BIBLIOGRÁFICAS

AMORIM, B. D. **Disco para Criptografia de César**. GeoGebra®. 2012. Disponível em <https://www.geogebra.org/m/kd6nG76y#material/dp2EHN2z> acesso em Jul. 2017.

ANDRADE, R. S.; SILVA, F. S. **Algoritmo de criptografia RSA: análise entre a segurança e velocidade.**Revista Eventos Pedagógicos. v.3, n.3, p.438-457, Ago. – Dez. 2012

APLICAÇÕES DA INFORMÁTICA. **Tabela ASCII**. Disponível em <http://nunovictor.blogspot.com.br/2015/10/padroes-de-codificacao-de-carateres.html> Acesso: ago. 2017

BARBOSA L. A. M., BRAGHETTO L. F. B., BRISQUI M. L. SILVA S. C. RSA **Criptografia Assimétrica e Assinatura Digital Campinas**. Monografia (Especialização em Redes de Computadores). UNICAMP, Campinas,Jul. 2003. 50p.

BENOIT. **Decrypto Aplicativo para android de Criptografia**. Disponível em < https://play.google.com/store/apps/details?id=info.valky.decryptor&hl=pt_BR>. Acesso em ago. 2017

BEZERRA, D. J., MALAGUTTI P. L., SILVA, V. C. R. **Aprendendo Criptologia de Forma Divertida.** Disponível em <<http://www.mat.ufpb.br/bienalsbm/arquivos/Oficinas/PedroMalagutti-TemasInterdisciplinares/Aprendendo_Criptologia_de_Forma_Divertida_Final.pdf>. Acessado em 22/09/2017

BLINDER, S. M. **RSA Encryption and Decryption**. Wolfram Alpha®. Disponível em <http://demonstrations.wolfram.com/RSAEncryptionAndDecryption/>. Acesso: Ago. 2017.

BORGES, F. Criptografia como ferramenta para o Ensino da Matemática. **Anais da SBMAC**. Pág: 822 a 828. Petrópolis, RJ, 2008.

CAETANO. **Régua de Saint-Cyr.** Disponível em <http://www.dm.ufscar.br/~caetano/iae2004/G6/images/cifravigenere.gif>. Acesso: maio 2017

CASTRO, F. L. **Criptografia RSA: uma abordagem para professores do ensino básico**. Trabalho de Conclusão de Curso (Matemática Pura e Aplicada). UFRGS. Porto Alegre-RS, 2014. 61p.

CAVALCANTI, C. F. A**. Cripto-sistemas com chave pública baseado em extensões cúbicas**. Dissertação de mestrado (Matemática). CCEN-UFPB, João Pessoa, 2002. 73p.

COUTINHO, S. C. **Números inteiros e Criptografia RSA**. Coleção Matemática e aplicações. IMPA, Rio de Janeiro, 2014. 226p.

FERNANDES, C. **Máquina Enigma**. *Brasil Escola*. Disponível em <http://brasilescola.uol.com.br/historiag/maquina-enigma.htm>. Acesso: setembro de 2017.

FIARRESGA, V. M. C. **Criptografia e Matemática**. Dissertação de Mestrado em Matemática para professores. Universidade de Lisboa, Portugal, 2010. 161p.

FRANÇA, W. B. A. **Criptografia**. Trabalho de conclusão de curso. Universidade Católica de Brasília, Brasília, 2005. 14p.

FREIRE, P. B.**A Matemática dos códigos Criptográficos**. Trabalho de Conclusão de Curso. Universidade Católica de Brasília. Brasília. 2007. 22p.

GRAHAM, Andrew. **Simple Cesar cipher**. *Wolfram Alpha®.* Set. 2013 Disponível em <http://demonstrations.wolfram.com/SimpleCaesarCipher/>. Acesso: Ago. 2017.

GANASSOLI, A. P.; SCHANKOSKI F. R.**Criptografia e Matemática**. Dissertação de Mestrado (Curso de Pós-graduação em Matemática para Rede Nacional PROFMAT). UFPR. Curitiba, PR, 2015. 103p.

GEOGEBRA. **Disco de Alberti.** Disponível em <https://cdn.geogebra.org/material/eSvVGLWub7wFVka8XLBNOMruRgYFHHL0/material-AnShymgr-thumb.png>. Acesso: jun. 2016.

GEOGEBRA. Roleta de César. Disponível em <https://www.geogebra.org/m/kF6WJReU> Acesso: jul. 2017.

GOMES, E. C. **A escrita na história da humanidade**. Disponível em <http://www.recantodasletras.com.br/artigos/3781907>. Acessado em 22/09/2007.

GOMES, J. M. A.; LOPES NETA, N. A. **Smartphone em sala de aula: o uso do aplicativo Math X Math em problemas de aritmética.** ISSN 2525-4227, v.02, n.01, Nov. 2016. Disponível em <http://www.maceio.al.gov.br/wp-content/uploads/lucasragucci/pdf/2016/11/4-SMARTPHONE-EM-SALA-DE-AULA-O-USO-DO-APLICATIVO-MATH-X-MATH-EM-PROBLEMAS-DE-ARITM%C3%89TICA.pdf>. Acesso Set. 2017

GODINHO, D. S; CESARIO, G. L.; REIS, J. N.; SARAIVA, R. S., Criptografia: a Importância da Álgebra Linear para decifrá-la.**Anais da II Mostra Integrada de Iniciação Científica**. Ano 2, Nº 2. Vol 2. FACO-CNEC, Osório RS, Jun, 2011.

HEFEZ, A. **Iniciação à Aritmética**. IMPA. Rio de Janeiro- RJ, 2009. 135p

HINZ, M. A. M. **Um estudo descritivo de novos algoritmos de criptografia**. Monografia (Bacharelado em Informática). UFPEL. Pelotas RS, 2000. 58p.

HOWARD, A.; RORRES C.**Álgebra Linear com Aplicações**. 8a edição. Porto Alegre: Bookman,2001. 578p.

INFOBIOGRAFIAS. **Imagem Júlio César.** Disponível em <http://pt..com/fotos/cesar1.jpg > acesso em 28/05/2017.

JESUS, A. L. N. **Criptografia na educação básica: utilização da Criptografia como elemento motivador para o ensino aprendizagem de matrizes**. Dissertação de Mestrado (Curso de Pós-graduação em Matemática para Rede Nacional PROFMAT). UNIVASP, Juazeiro, BA. 2013. 82p.

JANUÁRIO, C. R. **Criptografar mensagens com matrizes**. GeoGebra®. 2017. Disponível em <https://www.geogebra.org/m/nhkfcNW7>. Acesso: Ago. 2017.

KLEINSCHMIDT, J. **Aula Segurança da Informação**. Universidades Federal do ABC. Jul. 2013. Disponível em <http://professor.ufabc.edu.br/~joao.kleinschmidt/aulas/seg2013/aula_02-1_seg.pdf>. Acesso: 03/09/2016.

KRAUS, A. **Cours D'Arithmétique**. Apostila do curso de Aritmética da Université de Paris VI,UPMC, Paris FR 2014/2015. Disponíevl em < https://webusers.imj-prg.fr/~benjamin.girard/Poly_Kraus.pdf>

MARQUES, T. V. **Criptografia: abordagem histórica, protocolo Diffie-Hellman e aplicações em sala de aula**. Dissertação de Mestrado (Curso de Pós-graduação em Matemática para Rede Nacional PROFMAT).CCEN- UFPB. João Pessoa- PB. 2013. 82p.

MATSUMOTO, M. S., **Despertando o interesse do aluno pela Matemática com a Criptografia**. Dissertação de Mestrado (Curso de Pós-graduação em Matemática para Rede Nacional PROFMAT). FACET-UFGD. Dourados/MS, 2014. 56p.

MENEZES, A.; OORSCHOT P.; VANSTONE S.**Handbook of Applied Cryptography**.1997. CCR Press. Boca Raton. Florida. EUA. 810p.

OBMEP. **Prova da 2ª Fase do nível 1**. Disponível em <http://www.obmep.org.br/provas_static/pf2n1-2017.pdf >. Acessado em 21/09/2017.

OLIVEIRA, M. C. **Aritmética: Criptografia e outras aplicações de congruências**. Dissertação de Mestrado (Curso de Pós-graduação em Matemática para Rede Nacional PROFMAT). CCET/UFMS. Campo Grande, MS, 2013. 74p.

OLIVEIRA, C.; MOURA, S. P. **Tic's na Educação: a utilização das tecnologias da informação e comunicação na aprendizagem do aluno**. v. 7, n. 1, Pedagogia em Ação. Periódicos PUC-minas. 2017 Disponível em <http://periodicos.pucminas.br/index.php/pedagogiacao/article/viewFile/11019/8864>. Acesso em Set. 2017.

PINTO, R. C. **Os Números Primos Sob a Visão da Ciência e da Educação no Ensino Fundamental.**Monografia (Especialização em Docência do Ensino Superior). Universidade Candido Mendes. Rio de Janeiro/RJ, 2005. 33p.

PPLWARE. **Modelo de Chave Assimétrica.** Disponível em <https://pplware.sapo.pt/wp-content/uploads/2010/12/crypto_03.jpg > Acesso: ago. 2016

PPLWARE. **Modelo de Chave Simétrica.** Disponível em <https://pplware.sapo.pt/wp-content/uploads/2010/12/crypto_03.jpg > Acesso: ago. 2016

GEORGESCU, S. **Aplicativo RSA calculator**. Disponível em <https://play.google.com/store/apps/details?id=com.g.stefangeorgescu.rsacalculator&hl=pt&source=downloadatoz.com>. Acesso: ago. 2017

SANTOS, J. P. O. **Introdução à Teoria dos números.** IMPA, Rio de Janeiro/RJ, 2006. 198p

SILVA, E. V. P. Introdução à criptografia RSA. **Anais da XII Reunião de Iniciação Científica. Faculdade de Ilha Solteira**. UNESP, Ilha Solteira, 2006. 32p.

SINGH, S. **O livro dos códigos**. Rio de Janeiro: Record. 4ed, 2004. 446p.

SMILLER. **Cipher Disk**. *GeoGebra*® 2017. Disponível em <https://www.geogebra.org/m/kd6nG76y#material/DVTs3745>. Acesso: Ago. 2017.

STALLING, W. **Criptografia e segurança de redes**: princípios e práticas. Prentice Hall Brasil. 4ed. São Paulo, 2008. 492p.

WIKIPEDIA. **Imagem de Blaisé Vigenère**. Disponível em <https://pt.wikipedia.org/wiki/Blaise_de_Vigen%C3%A8re>. Acesso em maio 2017

BIBLIOGRAFIAS CONSULTADA

AVRITZER, D., BUENO, H. P., FARIA M. C., FERNANDES, A. M. V, FERREIRA, M. C. C., SOARES E. F. **Fundamentos de Álgebra**. UFMG, Belo Horizonte-MG. Abr. 2004. 194p. Disponível em <https://pt.scribd.com/doc/98020793/Fundamentos-de-lgebra-UFMG-Dan-Avritzer-e-Outros>

CARVALHO, G. C. A. **Números primos pequenos tópicos**. Dissertação de Mestrado (Curso de Pós-graduação em Matemática para Rede Nacional PROFMAT). UFG . Goiânia. 2013. Disponível em <https://repositorio.bc.ufg.br/tede/bitstream/tede/3443/5/Disserta%C3%A7%C3%A3o%20-%20Glauber%20Cristo%20Alves%20de%20Carvalho%20-%202013.pdf>. Acesso: 06/08/2016

COSTA, D. D**. A Matemática e os códigos secretos: uma introdução à criptografia**. Dissertação de Mestrado (Curso de Pós-graduação em Matemática para Rede Nacional PROFMAT). UEM/PROFMAT. 2014. 67p.

COUTINHO, S. C. **Criptografia**. IMPA, Rio de Janeiro, 2015. 217p.

CRUZEIRO, H. G. C. **Criptossistemas baseados em números primos**. Trabalho de Conclusão de Curso. Universidade Católica de Brasília. Brasília. 2007. 20p.

CUNHA, S. D. **O último teorema de Fermat**. Trabalho de conclusão de curso de bacharelado em matemática. Instituto de Matemática e estatística. UERJ Rio de Janeiro, Mar. 2010. 28p.

KRICHER, T. C. **Um estudo da máquina Enigma.** Trabalho de conclusão de curso. (Curso de Graduação em Ciência da computação) Porto Alegre – RS. Jan. 2013. Disponível em < https://www.lume.ufrgs.br/bitstream/handle/10183/66106/000870987.pdf>.

LEMOS, M. **Criptografia, Números Primos e Algoritmos**. Publicações Matemáticas. Universidade Federal de Pernambuco, Caruaru-PE, 2010. 128p. Disponível em <https://impa.br/wp-content/uploads/2017/04/PM_04.pdf>

LIMA, L. G. **Matrizes e algumas de suas aplicações**. Trabalho de conclusão de curso Licenciatura plena em Matemática. Universidade Estadual da Paraíba. Campo Grande PB. 2011. Disponível em <http://dspace.bc.uepb.edu.br/jspui/bitstream/123456789/475/1/PDF%20-%20Luana%20Gon%c3%a7alves%20Lima.pdf>. Acesso: 07/08/2016

MENEZES, R. **Criptografia e Álgebra**. Monografia. UFMG, Belo Horizonte MG. Mar. 2003. Disponível em <http://www.mat.ufmg.br/~marques/CRIPTOGRAFIA.pdf>. Acesso: 02/09/2016

MORENO, E. D.; PEREIRA, F. D.; CHIARAMONTE, R. B. **Criptografia em S*oftware* e Hardware**. São Paulo: Novatec, 2005. 288 p.

PROBST, R. W. **Números Primo**s. Trabalho de conclusão de curso (Bacharelado em Matemática). Universidade Regional de Blumenau. MG. 2003. Disponível em <http://paginapessoal.utfpr.edu.br/rwprobst/formacao-academica/curriculo/primos.pdf>. Acesso: 06/08/2016

RODNEY. **Matrizes**. Notas de aula.8p. Disponível em <http://www.mat.ufmg.br/~rodney/notas_de_aula/matrizes.pdf>. Acesso Set. 2016.

SALDANHA, Nicolau C. **Divisão euclidiana e o teorema fundamental da aritmética**. Disponível em <http://www.mat.puc-rio.br/~nicolau/papers/mersenne/node4.html>. Acesso: Set. 2016

SANTOS, A. R. SANTOS Patrícia Cristina Souza. **Propriedades de Divisibilidade e Congruências.** II Workshop de Algebra da UFG-CAC. 2013. ////////disponível em <https://ssa_mat.catalao.ufg.br/up/615/o/iiwa-poster-alan_patricia.pdf>. Acesso: Set. 2016

VIDGAL. **Matrizes e Criptografia.** Instituto Federal Minas Gerais. Campus Ouro Preto. Disponível em <http://vidigal.ouropreto.ifmg.edu.br/wp-content/uploads/sites/12/2015/04/MATRIZES-E-CRIPTOGRAFIA.pdf>. Acesso: 27/08/2016