UNIVERSIDADE ESTADUAL DO MARANHÃO – UEMA
CAMPUS BALSAS
DEPARTAMENTO DE MATEMÁTICA
CURSO DE LICENCIATURA EM MATEMÁTICA

LUCAS PURIFICAÇÃO MENDES DE SOUZA

A MATEMÁTICA PRESENTE NO DESENVOLVIMENTO DA CRIPTOGRAFIA

BALSAS-MA
2022

LUCAS PURIFICAÇÃO MENDES DE SOUZA

A MATEMÁTICA PRESENTE NO DESENVOLVIMENTO DA CRIPTOGRAFIA

Monografia apresentada ao Departamento de Matemática do Campus Balsas da Universidade Estadual do Maranhão, como requisito básico para a conclusão do Curso de Matemática Licenciatura.

Orientador: Prof. Dr. Antonio Nilson Laurindo Sousa

BALSAS-MA
2022

S729m

Souza, Lucas Purificação Mendes de.

A matemática presente no desenvolvimento da criptografia. / Lucas Purificação Mendes de Souza. – Balsas, 2022.

49 f.

Monografia (Graduação em Matemática) Universidade Estadual do Maranhão – UEMA / Balsas, 2022.

Orientador: Prof. Dr. Antonio Nilson Laurindo Sousa

1. Criptografia. 2. Matemática. 3. Codificação. 4. Decodificação. I. Título.

CDU: 371.3

Elaborado pela bibliotecária Maria da Consolação Coelho Rocha CRB 13/604

LUCAS PURIFICAÇÃO MENDES DE SOUZA

A MATEMÁTICA PRESENTE NO DESENVOLVIMENTO DA CRIPTOGRAFIA

Monografia apresentada ao Departamento de Matemática do Campus Balsas da Universidade Estadual do Maranhão, como requisito básico para a conclusão do Curso de Matemática Licenciatura.

Aprovado em: 12/01/2023

BANCA EXAMINADORA

Prof. Dr. Antonio Nilson Laurindo Sousa (Orientador)
Doutor em Física e Astronomia
Universidade Estadual do Maranhão - UEMA

Prof. Dra. Lourimara Farias Barros Alves
Doutora em Educação em Ciências e Matemática
Universidade Estadual do Maranhão - UEMA

Prof. Dr. Sergio Noleto Turibus
Doutor em Engenharia Nuclear
Universidade Estadual do Maranhão - UEMA

A Deus, aos meus pais, a minha namorada, a meu orientador e aos meus amigos que sempre me apoiaram e incentivaram na produção desta monografia.

AGRADECIMENTOS

Agradeço a Deus primeiramente, que me deu forças e capacidade para concluir mais esta etapa de minha vida.

À meu pai Cirineu e minha mãe Neuzimar, por todo apoio e motivação que sempre me passaram, bem como por tudo que fizeram por mim para que tivesse sempre as melhores condições de vida e estudo para adentrar na universidade e concluí-la.

À minha namorada Helloysa, por todo incentivo, apoio e companheirismo fornecido durante toda esta jornada, por todas as palavras de afeto, esperança e confiança, tanto em dias bastante produtivos quanto naqueles em que não conseguia progredir na pesquisa ou produção.

A todos os colegas de turma, em especial aos meus amigos: Antonio José, Auriana, Carina, Douglas, Jádia, Jaqueline, José Carlos, Kalisson e Nilvan por todo companheirismo e auxílio que me ofertaram tanto na construção desta monografia, quanto em todas as vivências acadêmicas ao longo destes 4 anos de curso.

Ao meu orientador, prof. Dr. Antonio Nilson Laurindo Sousa por todas as orientações, por desde o primeiro momento acreditar na realização desta pesquisa e por ser o responsável por me apresentar o conteúdo de criptografia durante a disciplina de Teoria dos Números, a forma como tal conteúdo foi explanado teve muita importância quanto a escolha do tema.

Aos professores presentes na banca examinadora, prof. Dra. Lourimara Farias Barros Alves e prof. Dr. Sergio Nolêto Turibus, por todas as sugestões abordadas durante a qualificação do projeto, estas foram de grande serventia para a construção desta monografia.

À Universidade Estadual do Maranhão (UEMA), em particular ao Departamento de Matemática do Campus Balsas por me acolher como mais um de seus alunos, por disponibilizar de todas as ferramentas e professores excepcionais que foram essenciais para o meu desenvolvimento como um aluno universitário.

Ademais, a todos aqueles que seja por forma direta ou indireta fizeram parte da minha formação, o meu sincero sentimento de gratidão.

“A teoria também se converte em graça material uma vez que se apossa dos homens.”

(Karl Marx)

RESUMO

Apesar de pouco se imaginar e entender, a criptografia é muito utilizada desde os primórdios da história com o intuito de tornar secretas diversas informações, visto que o ser humano sempre teve, por vários motivos, a necessidade de manter a segurança e a privacidade de mensagens. Com o avançar dos tempos, vários métodos de ocultar uma mensagem foram desenvolvidos, os processos de codificar e decodificar mensagens, foram tornando-se cada vez mais vital. Para isso, a criptografia (Arte de codificar uma mensagem) teve a necessidade de evoluir já que, continuava a ser algo essencial para a humanidade e, para que tal evolução se fizesse possível, foram utilizados diversos conceitos da Matemática. Este trabalho, pretende mostrar a utilização, a importância, a presença da Matemática na dinâmica e confiabilidade de manter secretas mensagens para diversas civilizações existentes ao longo da história humana. Para isso utilizou-se o estudo bibliográfico, buscando observar o que outros autores abordavam sobre a temática. Bem como as demonstrações práticas quanto a funcionalidade dos métodos abordados. Nesta pesquisa, foram encontrados diversos métodos de codificação utilizados no decorrer de sua trajetória, sendo que, ao longo do tempo diversos novos métodos foram criados, ou aprimorados métodos antigos, sendo esses cada vez mais complexos, dado ao fato de que a criptoanálise (área responsável por analisar métodos de decodificação com o objetivo de desvendar os padrões e segredos que as mensagens continham) também apresentava constante evolução. Porém, mesmo com todo o desenvolvimento da criptoanálise sempre houveram métodos de codificação eficientes e, atualmente o método que cumpre com maior segurança sua função é o método RSA, que utiliza de conceitos matemáticos, que envolve o conjunto dos números Inteiros e suas propriedades como base para o seu funcionamento. Em que destaca-se: o produto de números primos “grandes”, congruência modular, entre outros.

Palavras-chave: Criptografia; Matemática; Codificação; Decodificação

ABSTRACT

Although little is imagined and understood, cryptography has been widely used since the dawn of history in order to keep various information secret, since human beings have always had, for various reasons, the need to maintain the security and privacy of messages. As time went on, various methods of hiding a message were developed, the processes of encoding and decoding messages became more and more vital. For this, cryptography (the art of coding a message) had to evolve since it continued to be something essential for humanity and, in order for this evolution to become possible, several concepts of Mathematics were used. This work intends to show the use, importance, the presence of Mathematics in the dynamics and reliability of keeping secret messages for different civilizations throughout human history. For this, a bibliographical study was used, seeking to observe what other authors addressed on the subject. As well as practical demonstrations regarding the functionality of the methods covered. In this research, several coding methods were found used throughout its trajectory, and, over time, several new methods were created, or improved old methods, which are increasingly complex, given the fact that cryptanalysis (an area responsible for analyzing decoding methods with the aim of unveiling the patterns and secrets that the messages contained) also showed constant evolution. However, even with all the development of cryptanalysis, there have always been efficient coding methods, and currently the method that fulfills its function with greater security is the RSA method, which uses mathematical concepts, which involves the set of integers and their properties as a basis for its operation. What stands out: the product of "big" prime numbers, modular congruence, among others.
Key words: Cryptography; Math; Coding; Decoding

LISTA DE ILUSTRAÇÕES

LISTA DE SÍMBOLOS

$\mathbb{Z}$	Números inteiros
$\pm$	Mais ou menos
$+$	Adição
$-$	Subtração
$\cdot$	Multiplicação
$=$	É igual a
$\neq$	É diferente de
$>$	É maior que
$\geq$	É maior ou igual a
$<$	É menor que
$\leq$	É menor ou igual a
$\mid$	Divide
$\nmid$	Não divide
$-a$	Simétrico de a
$\lvert a \rvert$	Módulo de a
a/b	a dividido por b
$a \ mod \ b$	a módulo b
$\equiv$	Congruência
$\not\equiv$	Incongruência
■	Final da demonstração

SUMÁRIO

1 INTRODUÇÃO

Embora seja um termo considerado de senso comum como algo novo e que está associado a evolução tecnológica, existem relatos e documentos que comprovam a existência e a importância de técnicas e artifícios, que possuíam a mesma finalidade, garantir a segurança e transmissão da mensagem, restrita apenas a quem envia e quem recebe, do que hoje se conhece por criptografia, já era utilizada por diversas civilizações antigas, como a egípcia e a mesopotâmica.

Em virtude disso, este trabalho tem por objetivo geral, abordar alguns métodos aplicados em diversas civilizações com o intuito de mostrar a utilização, importância e confiabilidade da criptografia para os povos ao longo do tempo. Para isso, analisou-se os métodos utilizados, investigou-se a motivação de pessoas para se fazer uso de tais artifícios, bem como realizou-se um comparativo para apresentar o progresso da criptografia partindo dos primeiros métodos de codificação até os existentes atualmente, além de, por meio da prática de tais métodos, demonstrar a funcionalidade dos mesmos.

Para o desenvolvimento de tal pesquisa, foram realizados estudos bibliográficos em livros e artigos acadêmicos com o objetivo de observar o que outros autores abordavam sobre a temática, buscando a obtenção de fundamentação teórica, para que assim se tornasse possível tratar do assunto em questão com propriedade e uma maior sustentação. É válido ressaltar que a criptografia atual é uma área bastante sustentada por conceitos matemáticos, desta forma, os estudos bibliográficos foram de grande importância para o seu melhor conhecimento.

Além da pesquisa, foram realizadas demonstrações de codificação de mensagens por métodos apresentados no decorrer da abordagem sobre o tema, com o intuito de observar e apresentar na prática a funcionalidade e evolução da criptografia, começando com as primeiras civilizações em que apresentam comprovações históricas do uso da codificação de mensagens até a criptografia utilizada atualmente pela sociedade moderna.

A motivação em realizar esta pesquisa deu-se durante a apresentação de tal conteúdo na disciplina de Teoria dos Números, a forma como o mesmo foi abordado, instigando a curiosidade quanto a codificação e decodificação de mensagens, teve muita importância na escolha do tema.

No capítulo 2 faz-se um resgate histórico do estudo da criptografia, contemplando desde a “antiguidade” ao longo do tempo e a evolução que se deu a partir da esteganografia (processo de ocultação da mensagem). O surgimento da criptoanálise e alguns métodos de codificação e decodificação de mensagens por diversas civilizações até o momento atual.

No capítulo 3 são destacados conceitos importantes que fundamentam tal teoria, bem como as definições matemáticas, seus axiomas, teoremas e proposições, tendo como elemento de estudo o conjunto dos números Inteiros que dá sustentação sólida à criptografia RSA.

No capítulo 4 implementa-se o algoritmo de alguns métodos de criptografia, dando destaque ao RSA, mostrando o modelo de aplicação matemática, fundamentado no capítulo 3 e, realizando um comparativo deste método em relação aos demais para abordar a confiabilidade de tal.

No capítulo 5 apresenta-se a metodologia escolhida para a elaboração do trabalho de forma melhor detalhada, que se deu por meio de uma pesquisa bibliográfica e por fim a aplicabilidade de forma prática.

Por fim, no capítulo 6 são abordadas as conclusões obtidas pelo autor, após a realização da pesquisa bibliográfica e das demonstrações, referentes a funcionalidade dos métodos apresentados em capítulos anteriores.

2 CRIPTOGRAFIA AO LONGO DA HISTÓRIA

Conforme afirma Sousa (2013, p. 12) “a criptografia é estudada desde a antiguidade”, logo, por mais que o termo “criptografia” ainda não existisse de fato, já que conforme afirma Silva (2019) o mesmo foi criado em 1920. Diversas civilizações antepassadas desenvolveram variados métodos de ocultar informações sigilosas de forma que, apesar de outros possuírem acesso à mensagem, apenas quem realmente era o destinatário saberia que informações continha na mesma.

Mediante a esse fato, neste capítulo serão expostos métodos de codificar as informações utilizados em algumas das principais civilizações dos 4 períodos da história conhecidos por: Idade Antiga, Idade Média, Idade Moderna e Idade Contemporânea.

2.1 Idade Antiga

Primeiro e mais longo período da história até o momento, a Idade Antiga tem seu início por volta do ano de 3500 a.C. marcada pelo primeiro registro de escrita, fator esse que limita a divisão entre pré-história e história e, tem seu fim datado em 476 d.C. com a queda do Império Romano Ocidental.

2.1.1 Egito e a tumba de Khnumhotep II

Uma das primeiras grandes civilizações do planeta é também o local onde há comprovações mais antigas do uso de princípios da criptografia como afirma Kahn (1967, n.p. *apud* ORDONEZ; PEREIRA; CHIARAMONTE, 2005, p. 12):

> O primeiro exemplo documentado da escrita cifrada aconteceu aproximadamente no ano de 1900 a.C, quando o escriba de Khnumhotep II teve a ideia de substituir algumas palavras ou trechos de texto. Caso o documento fosse roubado, o ladrão não encontraria o caminho que o levaria ao tesouro e morreria de fome perdido nas catacumbas da pirâmide.

Os povos egípcios acreditavam que a morte se tratava de uma passagem para outra vida e que necessitariam levar consigo seus bens materiais, com o intuito de usufruir de tais bens em suas próximas encarnações, por isso várias pirâmides continham diversas riquezas e, como consequência eram alvos de ladrões. Para evitar que esses bens fossem roubados o escriba de Khnumhotep II substituiu palavras e trechos de documentos ocultando assim a mensagem para que, quem entrasse com intenção de se apropriar das riquezas acabasse se perdendo na pirâmide, falecendo de fome e sede.

Figura 1 - Tumba de Khnumhotep II

Fonte: Wikipédia (2022)[1]

2.1.2 Mesopotâmia e a esteganografia

Outra civilização antiga que utilizou da criptografia foi a Mesopotâmia que segundo Kahn (1996, n.p. *apud* ARAÚJO, 2018, p. 14) "superou o Egito na questão criptográfica, pois foi por volta de 1500 a.c. chegou a um nível bastante moderno, o primeiro registro do uso da criptografia nesta região está numa fórmula para fazer esmaltes para cerâmica".

Ainda de acordo com Araújo (2018) a esteganografia foi desenvolvida nesse período pelas civilizações do Egito, China, Índia e Mesopotâmia, sendo que o ato de esteganografar consiste em esconder a mensagem propriamente. Sousa (2013, p. 20) corrobora ao relatar que:

> Um exemplo interessante de esteganografia é encontrado em 'As histórias', onde Heródoto narrou os conflitos entre Grécia e Pérsia, ocorridos no século V a.C.. Uma das histórias é a de Histaeu que queria encorajar Aristágora de Mileto a se revoltar contra o rei persa. Para transmitir suas instruções em segurança, Histaeu raspou a cabeça de um mensageiro, escreveu a mensagem no couro cabeludo e esperou que o cabelo crescesse. O mensageiro, que aparentemente não levava nada que o comprometesse, viajou sem ser incomodado. Quando chegou ao seu destino, raspou a cabeça, possibilitando assim a leitura da mensagem pelo destinatário.

Ainda conforme Sousa (2013, p. 21) "com a evolução da esteganografia, houve a evolução da criptografia", sendo que o intuito desse método era ocultar as informações contidas na mensagem e não a mensagem em si como ocorria na esteganografia, portanto, apesar de significarem ações diferentes, tanto a esteganografia quanto a criptografia estão diretamente interligadas já que progrediram juntas.

2.1.3 Esparta e o bastão de Licurgo

A criptografia foi de grande importância para diversos povos também ao se falar de confrontos militares. Um exemplo citado por Singh (2007) é o bastão de Licurgo ou Scytale, que foi utilizado por espartanos durante o século V a.C., como sendo o primeiro de muitos sistemas de criptografia militar.

---

[1] Disponível em: https://en.wikipedia.org/wiki/Khnumhotep_II. Acesso em: 28 Set. 2022

O método em questão consistia em utilizar um bastão no qual o material em que seria escrito a mensagem deveria ser enrolado, após esse primeiro processo a mensagem seria escrita tomando como base o comprimento do bastão, por fim o material era desenrolado, com isso as letras acabavam por ficar em desordem, e assim a mensagem era enviada para o destinatário de modo que para decodificá-la seria necessário portar de um bastão com dimensões semelhantes ao primeiro utilizado.

Figura 2 - Bastão de Licurgo

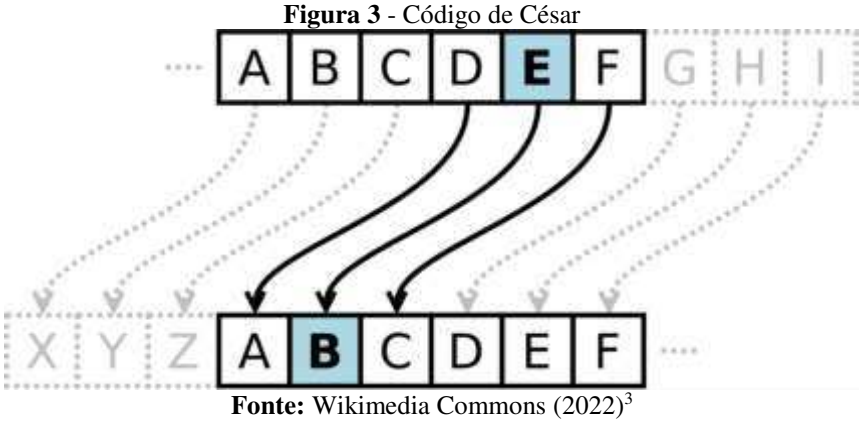
Fonte: Wikipédia (2019)[2]

2.1.4 Roma e a cifra do Imperador

Outra civilização a fazer uso da criptografia a caráter militar foi a romana, segundo Costa (2014, p. 5) "O imperador romano Julio César, utilizava um artifício que consistia em se trocar a letra original pela letra que se encontra a algumas posições a frente pela ordem do alfabeto" de modo que para decodificar a mensagem era necessário, além de entender como funcionava o método, ter conhecimento de quantas posições a frente seria utilizado o artifício, informações essas que apenas o remetente e o destinatário da mensagem possuíam.

Vale ressaltar que "o código de César é o único da antiguidade que é usado até hoje. Atualmente qualquer cifra baseada na substituição cíclica do alfabeto denomina-se de código de César" (ORDONEZ; PEREIRA; CHIARAMONTE, 2005, p. 12).

Figura 3 - Código de César



Fonte: Wikimedia Commons (2022)[3]

[2] Disponível em: https://pt.wikipedia.org/wiki/C%C3%ADtala. Acesso em: 30 Set. 2022
[3] Disponível em: https://commons.wikimedia.org/w/index.php?curid=30693472. Acesso em: 30 Set. 2022

2.1.5 Grécia e o quadro de Políbio

De acordo com Kahn (1996, n.p. *apud* ARAÚJO, 2018, p. 18) “Políbio inventou um sistema de sinalização que foi adotado amplamente como método criptográfico. Ele organizou as letras em quadrado 5x5 e numerou as linhas e colunas”, desse modo cada letra era representada por dois números sendo o primeiro o da linha e o segundo da coluna. A letra “L” por exemplo seria expressa pelo número 31 por estar na terceira linha e na primeira coluna. Vale ressaltar que as letras “I” e “J” ocupam a mesma posição na tabela, sendo esta a posição associada ao número 24.

Assim a mensagem que seria enviada e recebida como uma sequência de números poderia ser traduzida apenas pelas pessoas que tinham conhecimento do método para separar a sequência em pares de números, e acesso ao quadro em questão para verificar qual letra era representada pelo respectivo par.

Figura 4 - Quadro de Políbio

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

Fonte: Acervo Lima (2022)[4]

2.2 Idade Média

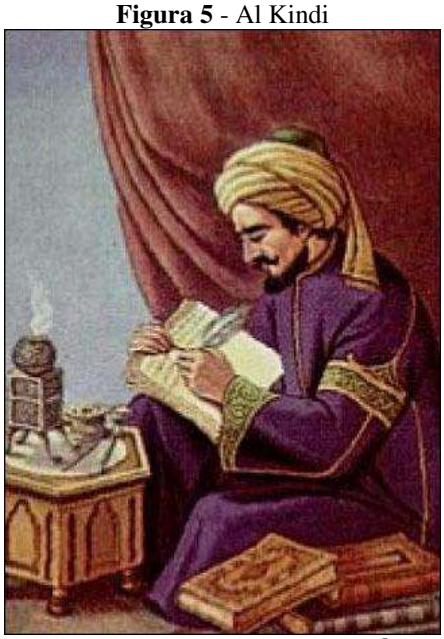
Após o fim da Idade Antiga com a queda do Império Romano Ocidental por volta de 476 d.C. dá-se início à Idade Média período também conhecido por Idade das Trevas. Devido a muitas perseguições religiosas que ocorreram no período e pela crise da peste bubônica que dizimou cerca de um terço da população europeia na época. Essa era, teve seu fim por volta de 1453 d.C. tendo por marco final a conquista de Constantinopla pelos povos otomanos.

Durante esse período não houve tantos desenvolvimentos de meios de criptografar, porém foi na Idade Média que um outro termo associado a criptografia e de muita importância

[4] Disponível em: https://acervolima.com/cifra-quadrada-de-polibio/. Acesso em: 02 Out. 2022

no estudo da área em questão surgiu, sendo esse termo a criptoanálise, conforme afirma Araújo (2018, p. 18) ao dizer que “nesse período se destacou o árabe Al-Kindi (Iraque, 801-853), conhecido como o filósofo dos árabes, foi o precursor da criptoanálise para a substituição monoalfabética”.

Figura 5 - Al Kindi



Fonte: Totally History (2020)[5]

Como o próprio nome dá a entender a criptoanálise se trata do ramo da criptografia destinado a analisar, com o intuito de encontrar o significado de determinados textos cifrados e por consequência descobrir qual o método foi utilizado para criptografar as mensagens em questão, podendo assim desvendar várias informações que podem estar contidas em outras mensagens que utilizaram do mesmo método. As pessoas responsáveis pela criptoanálise como foi Al-Kindi são chamados de criptoanalistas.

2.3 Idade Moderna

Assim como marca o fim da Idade Média, a conquista de Constantinopla marca o início de um novo período: a Idade Moderna. Esse período foi marcado pelas Grandes Navegações e pela revolução industrial que ocorreu na Europa, que foi de grande importância para a economia na época. Outro fator marcante do período foi o surgimento do absolutismo que dava poder absoluto aos monarcas. Esse período foi encerrado em 1789 d.C. pela queda da Bastilha que deu início a Revolução Francesa.

[5] Disponível em: https://totallyhistory.com/al-kindi/. Acesso em: 02 Out. 2022

2.3.1 Itália e o disco de Alberti

Um dos primeiros métodos de criptografia a surgir na Idade Moderna foi desenvolvido na Itália por Leone Battista Alberti que conforme afirma Kahn (1996, n.p. *apud* ARAÚJO, 2018, p. 20) "é conhecido como o pai da criptografia ocidental, ele publicou, em 1466, o livro Modes scribendi in ziferas, onde fala do disco de cifra, o primeiro sistema polialfabético conhecido". Fiarresga (2010, p. 12-13) explica esse instrumento ao afirmar que:

> O disco de cifra era constituído por dois discos concêntricos e de raios diferentes. O disco maior era fixo, e o menor móvel. Alberti dividiu cada uma das circunferências em vinte e quatro sectores; em cada um dos sectores do disco maior escreveu o alfabeto em 13 letras maiúsculas pela sua ordem normal, mas não continha as letras H, J, K, U, W e Y; nos quatro sectores que sobraram colocou os algarismos 1, 2, 3 e 4. No disco móvel, colocou de uma forma aleatória, em cada um dos sectores, as letras do alfabeto, que eram 24, sendo a vigésima quarta o & (et).

Para codificar a mensagem utilizando-se desse método é necessário primeiramente ter uma palavra-chave no disco fixo e uma letra-chave no disco móvel, após essa primeira etapa para codificar a mensagem basta conciliar a letra-chave com a primeira letra da palavra-chave, obtendo assim a primeira letra da mensagem codificada no disco fixo, ao fazer esse mesmo processo com a segunda letra da palavra chave obtêm-se a segunda letra da palavra codificada, seguindo assim até codificar toda a mensagem. Caso chegue na última letra da palavra-chave e a mensagem não tenha terminado basta recomeçar pela primeira letra da palavra-chave.

É importante ressaltar que para decodificar a mensagem é necessário que o destinatário tenha consigo um disco semelhante ao utilizado pelo remetente assim como que o mesmo tenha, além do disco, conhecimento de qual é a palavra-chave utilizada no disco fixo e qual a letra-chave no disco móvel.

Figura 6 - Disco de Alberti

Fonte: Wikipédia (2022)[6]

[6] Disponível em: https://en.wikipedia.org/wiki/Alberti_cipher. Acesso em: 05 Out. 2022

2.3.2 França e a cifra de Vigenère

A cifra de Vigenère é um modelo de criptografia que tem por base a cifra de César, abordada no item 1.1.4, segundo Araújo (2018, p. 24) “a diferença é que numa cifra de César, cada letra do alfabeto é deslocada da sua posição um número fixo de lugares, enquanto na cifra de Vigenère consiste de várias cifras de César com diferentes valores de deslocamento”.

Nesse método o alfabeto é disposto em uma tabela de 26 linhas e 26 colunas, sendo a primeira linha com o alfabeto corrente, a segunda iniciando com a segunda letra do alfabeto, terceira com a terceira letra e assim por diante. Para criptografar mensagens por esse método basta fazer uso de uma palavra-chave de forma que a primeira letra da palavra-chave e a primeira letra da mensagem formem respectivamente a letra da coluna e da linha da tabela, encontrando nesse ponto a letra criptografada, repetindo esse passo com as demais letras se tem toda a mensagem criptografada.

Figura 7 - Cifra de Vigenère

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

Fonte: Wikipédia (2022)[7]

2.3.3 Reino Unido e a cifra do Lord Bacon

“No século XVI, o filósofo inglês Francis Bacon criou uma cifra em que cada letra é substituída por uma sequência de cinco letras, esta sequência é formada unicamente pelas letras A e B” (FIARRESGA, 2020, p. 16), portanto cada letra tem uma sequência única para representá-la, com exceção das letras “I” e “J” assim como “U” e “V” que nesse sistema são representadas pela mesma combinação, e apenas as pessoas que possuíam entendimento do

[7] Disponível em: https://pt.wikipedia.org/wiki/Cifra_de_Vigen%C3%A8re. Acesso em: 08 Out. 2022

funcionamento do código saberiam qual o real significado da mensagem. Esse método ficou conhecido como a cifra de Bacon.

A cifra em questão atualmente recebe outro nome, a mesma “é classificada como decodificação binário de 5 bits” (ARAÚJO, 2018, p.26), em que as letras A e B foram respectivamente substituídas pelos números 0 e 1, vale ressaltar no entanto que o método de ocultar a mensagem segue da mesma forma apenas considerando essa alteração na representação de cada letra.

Figura 8 - Código de Bacon

Letra	Grupo	Binário		Letra	Grupo	Binário
A	aaaaa	00000		N	abbaa	01100
B	aaaab	00001		O	abbab	01101
C	aaaba	00010		P	abbba	01110
D	aaabb	00011		Q	abbbb	01111
E	aabaa	00100		R	baaaa	10000
F	aabab	00101		S	baaab	10001
G	aabba	00110		T	baaba	10010
H	aabbb	00111		U/V	baabb	10011
I/J	abaaa	01000		W	babaa	10100
K	abaab	01001		X	babab	10101
L	ababa	01010		Y	babba	10110
M	ababb	01011		Z	babbb	10111

Fonte: Caballero (2012)[8]

2.4 Idade Contemporânea

Com a queda da Bastilha e o início da Revolução Francesa deu-se início ao período atual, que é chamado de Idade Contemporânea, período de grande avanço na política, visto que os governos absolutistas deram lugar a democracia, de novas revoluções industriais responsáveis pelo desenvolvimento tecnológico, além de guerras marcantes como a primeira e segunda guerra mundial. Por ser o momento atual não existe, até então, um acontecimento que limite o fim do período em questão.

2.4.1 Criptografia nas Guerras Mundiais

Assim como na Idade Antiga, durante a Idade Contemporânea a criptografia teve grande importância a caráter militar nas duas grandes Guerras Mundiais, já que as informações deveriam passar de grupos a outros em segurança, ou seja, mesmo que o grupo que fizesse posse da mensagem fosse interceptado por inimigos, era necessário ter a garantia de que a mensagem

[8] Disponível em: https://encdesarrollo.wordpress.com/2012/09/27/esteganografia-en-redes-sociales-2/. Acesso em: 08 Out. 2022

(que poderia conter importantes estratégias ou informações) não fosse lida e interpretada por pessoas diferentes dos destinatários.

Durante a Primeira Guerra Mundial “os alemães criaram uma nova cifra utilizando o tabuleiro de Polybius, substituindo os números 12345 pelas letras ADFGX, uma palavra chave e uma transposição” (COSTA, 2014, p. 12). O método de criptografar a mensagem seguia o mesmo princípio do tabuleiro de Políbio, porém além da troca dos números pelas letras ADFGX fazia-se uso também de uma palavra-chave que seria responsável por organizar as colunas em ordem alfabética e que por esse motivo a palavra em questão não poderia ter letras repetidas. Para decodificar a mensagem era necessário que o receptor da mesma tivesse conhecimento do método e ainda da palavra-chave.

Conforme afirma Fiarresga (2010, p. 21) “Após a Primeira Guerra Mundial, o alemão Scherbuis criou a máquina Enigma, que revolucionou o mundo da criptografia”, essa máquina foi a responsável por criptografar diversas mensagens dos alemães durante a Segunda Guerra Mundial com um altíssimo grau de segurança o que dificultava que os códigos fossem quebrados por inimigos. Sobre isso, Araújo (2018, p. 29) afirma que:

> Dentre os vários modelos da Enigma, a que mais causou transtorno e assombro na sua ‘quebra’ de códigos foi a Enigma M4, exclusivamente desenvolvida para a divisão U-Boot da Kriegsmarire (Marinha Alemã) teve papel fundamental na Batalha do Atlântico e foi introduzida em 1942, os criptoanalistas de Bletchley Park, a chamaram de Shark-key (Chave-tubarão). Seu código permaneceu sem ser quebrado por nove meses, até outubro de 1942, quando livros de códigos novos foram capturados.

Figura 9 - Máquina Enigma

Fonte: G1 (2015)[9]

[9] Disponível em: https://g1.globo.com/tecnologia/noticia/2015/07/maquina-alema-que-codificava-textos-na-2-guerra-e-leiloada-por-r-733-mil.html. Acesso em: 08 Out. 2022

2.4.2 Os criptoanalistas de Bletchley Park

Diante da criação da máquina Enigma um grande grupo de criptoanalistas, sendo esses matemáticos, estatísticos e engenheiros, foram reunidos na cidade de Bletchley na Inglaterra, em uma instalação militar secreta que ficou conhecida por Bletchley Park. Tal grupo tinha por função decifrar os códigos alemães para auxiliar a força aliada durante a Segunda Guerra Mundial.

Conforme afirma Araújo (2018) os criptoanalistas tiveram como ponto de partida de seus estudos quanto a máquina Enigma, a comprovação de que a mesma possuía falhas, comprovação essa obtida graças ao matemático polonês Marian Rejewski. A partir de tal ponto criptoanalistas, dentre eles Alan Turing (matemático responsável por encontrar a maior fraqueza da Enigma), inventaram uma máquina responsável pela decodificação de mensagens do alto comando alemão.

Figura 10 - Alan Turing

Fonte: Encyclopedia Britannica[10]

É válido ressaltar que, devido à grande importância de manter a decodificação das mensagens inimigas como segredo para vencer a guerra, o grupo era tratado de forma anônima, sendo que "o segredo em torno de Bletchley Park terminou em 1974 com o lançamento do livro The Ultra Secret, de F. W. Winterbotham" (ARAÚJO, 2018, p. 31), de forma que a partir de então todos aqueles que auxiliaram durante a guerra puderam obter o reconhecimento merecido em relação a seus atos.

[10] Disponível em: https://www.britannica.com/biography/Alan-Turing. Acesso em: 09 Out. 2022

Porém o fim do segredo de Bletchley Park trouxe consigo a falta de segurança para alguns, visto que, ainda conforme Araújo (2018, p. 31) “entre os que não sobreviveram ao fim do segredo, estão Alastair Denniston, o primeiro diretor de Bletchley Park, e Alan Turing”.

Figura 11 - Bletchley Park

Fonte: BBC.com[11]

2.4.3 Atualidade e o método RSA

Com o passar do tempo, o trabalho de grandes criptoanalistas e o desenvolvimento de novas tecnologias, diversos métodos de criptografar mensagens foram desvendados e até mesmo máquinas como a Enigma abordada anteriormente tiveram seus segredos descobertos. De modo que não se passa tanta segurança para codificar mensagens na sociedade atual.

Porém, assim como era nos primórdios da história, a sociedade atual continua com a necessidade de ocultar informações de modo a garantir segurança, a privacidade pessoal e profissional. “Desta forma, tornou-se necessário inventar novos códigos, que mesmo com a ajuda de um computador, fossem difíceis de decifrar” (SOUSA, 2013, p. 24).

“Um método usado atualmente que vem conseguindo realizar essa proeza é o RSA” (COSTA, 2014, p. 14), o método em questão foi desenvolvido pelos cientistas informáticos Ronald Rivest e Adi Shamir e pelo matemático Leonard Adleman e a sigla RSA faz alusão aos três em questão, sendo o R de Rivest, o S de Shamir e o A de Adleman. Costa (2014, p. 46) explica os motivos da funcionalidade do método:

> A novidade trazida pelo método RSA é que ele configura um sistema de chave pública, ou seja, opera como uma porta de duas chaves diferentes: a chave A tranca a porta, mas uma chave diferente (B) a destranca. Então, a chave A não precisa ser secreta, e a distribuição de cópias dela não compromete a segurança. Na hipótese de esta porta guardar a entrada da seção segura da página virtual de uma empresa, esta poderia distribuir livremente a chave A para qualquer visitante virtual que quisesse enviar uma mensagem segura, como, por exemplo, o número do cartão de crédito. Embora todos possam codificar seus dados usando a mesma chave, ninguém pode ler as mensagens codificadas dos outros.

[11] Disponível em: https://www.bbc.com/news/uk-54604895. Acesso em 09 Out. 2022

A chave responsável por codificar a mensagem é formada por um par de números (n, λ) onde “n” é o produto de dois números primos, vale ressaltar que quanto maior esses números, mais segura será a mensagem, e “λ” não possui um fator comum a “n”. A chave responsável pela decodificação da mensagem se trata de um certo número “d” sendo este, “um inteiro muito grande e que seja relativamente primos com produto $(p - 1)(q - 1)$” onde “p” e “q” são os números primos utilizados para encontrar “n”. (SOUSA, 2013, p. 48).

3 DEFINIÇÕES

Como já abordado anteriormente, sabe-se que a criptografia é a área responsável por ocultar uma mensagem e torná-la segura quanto a tentativa de interceptação por pessoas indevidas. Ou seja, o documento que continha a mensagem poderia até ser furtado porém, sem o conhecimento do meio utilizado para codificá-la e de que caminhos deveria tomar para traduzir a mesma, jamais a informação seria desvendada.

3.1 Criptografia e suas cifras

Como foi observado no capítulo anterior, no decorrer dos tempos diversos métodos foram desenvolvidos e utilizados por vários povos desde a Idade Antiga até a Idade Contemporânea. Ao longo desse processo de criação a criptografia foi sendo aprimorada e com isso foram surgindo diversos modelos de cifra, tais como a cifra de transposição, a de substituição, as cifras simétricas e assimétricas.

Todo método de decodificar mensagens que se baseia na mudança de posição da letra na mensagem, é considerado como cifra de transposição. Enquanto que, aqueles métodos no qual as letras são trocadas por uma outra ordem de alfabeto ou mesmo por sequências de números, são chamados de cifra de substituição.

Sobre isso, Fiarresga (2010, p.4-5) corrobora ao afirmar que “enquanto na cifra de transposição cada letra conserva a sua identidade, mas muda de posição dentro da mensagem; na cifra de substituição, cada letra conserva a sua posição, mas é substituída por uma outra letra ou símbolo.”

As cifras simétricas são todas aquelas que utilizam o mesmo caminho para codificar e decodificar a mensagem. Ou seja, além da mensagem o remetente tem de passar ao destinatário da mesma o segredo para decodificá-la, o que acaba por se tornar um problema em questão de segurança, visto que esse segredo não pode ser interceptado por terceiros de modo algum. Como solução a esse problema surgem as cifras assimétricas que ao contrário das simétricas, apresenta um caminho específico para codificar a mensagem e outro diferente para decodificá-la.

De forma análoga é como imaginar que na cifra simétrica a chave que é utilizada para trancar uma porta é utilizada também para destrancar a mesma, enquanto que na cifra assimétrica são utilizadas de duas chaves, sendo uma exclusiva para trancar a porta e a outra exclusivamente para a destrancar.

3.2 Alguns conceitos matemáticos na criptografia

Devido à grande associação da criptografia com a matemática, visto que "em muitas aplicações de criptografia, números inteiros têm que ser somados, multiplicados e divididos com resto, a fim de poderem gerar valores muito precisos" (BUCHMANN, 2002, p. 17), serão abordados em seguida alguns conceitos da área que são importantes tanto para que o remetente da mensagem consiga criptografá-la quanto para que o destinatário da mesma consiga a descriptografar e assim desvendar a informação contidas na mensagem.

Definição 1 "Indica-se por $\mathbb{Z}$ o conjunto dos números inteiros, como segue $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$." (SOUSA, 2013, p. 27).

Axioma 1 Sendo a, b e c três números inteiros quaisquer, o conjunto dos inteiros aceita as seguintes propriedades:

(i) "Fechamento: $a + b$ e $a \cdot b$ são inteiros sempre que a e b forem inteiros." (SAMPAIO; CAETANO, 2009, p. 11).

(ii) "Leis comutativas: $a + b = b + a$ e $a \cdot b = b \cdot a$, para quaisquer inteiros a e b." (SAMPAIO; CAETANO, 2009, p. 11).

(iii) "Leis associativas: $(a + b) + c = a + (b + c)$ e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, para quaisquer inteiros a, b e c." (SAMPAIO; CAETANO, 2009, p. 11).

(iv) "Leis de existência de elementos neutros: $a + 0 = 0 + a = a$ e $a \cdot 1 = 1 \cdot a = a$, para todo inteiro a." (SAMPAIO; CAETANO, 2009, p. 11).

(v) "Lei distributiva (da multiplicação em relação a adição): $(a + b) \cdot c = a \cdot c + b \cdot c$." (SAMPAIO; CAETANO, 2009, p. 11).

(vi) "Lei da existência de inversos aditivos: Para cada inteiro a existe um inteiro x tal que $a + x = x + a = 0$. Esse inteiro x é denominado inverso aditivo ou oposto, ainda, simétrico de a, e é denominado por $-a$." (SAMPAIO; CAETANO, 2009, p. 11).

(vii) "Lei do cancelamento da multiplicação: Se a, b e c são inteiros, com $c \neq 0$ e $a \cdot c = b \cdot c$, então $a = b$." (SAMPAIO; CAETANO, 2009, p. 11).

Teorema 1 "Cada inteiro a tem um único inverso aditivo." (SAMPAIO; CAETANO, 2009, p. 12).

Demonstração: Consideremos que existem dois inteiros a_1 e a_2 que sejam simultaneamente inversos aditivos de a, ou seja $a + a_1 = 0$ e $a + a_2 = 0$, portanto, considerando as propriedades expressas no axioma a_1 pode ser reescrito como $a_1 + 0$ já que 0 é o elemento neutro da adição, como dito no início 0 pode ser substituído por $a + a_2$, sendo a nova equação $a_1 = a_1 + (a + a_2)$, por fim utilizando da propriedade associativa tem se que $a_1 = (a_1 + a) +$

a_2, porém, sabe-se que $a + a_1 = 0$, assim que $a_1 = a_2$, o que comprova que a possui apenas um inverso aditivo.

■

Teorema 2 "Se a é um inteiro qualquer, $a \cdot 0 = 0$." (SAMPAIO; CAETANO, 2009, p. 12).

Demonstração: Imaginemos que $a \cdot 0 = x$, para mostrar que $x = 0$, sendo $0 = 0 + 0$ pela propriedade do elemento neutro, tem-se que $x = a \cdot (0 + 0)$ ao utilizar da lei distributiva na equação $x = a \cdot 0 + a \cdot 0$, pelo que foi afirmado no inicio tem-se que $x = x + x$, somando o simétrico de x a ambos os lados temos que $x + (-x) = (x + x) + (-x)$ utilizando da lei associativa tem-se que $0 = x + (x + (-x))$, logo $0 = x + 0$, como 0 se trata do elemento neutro é possível afirmar que $x = 0$.

■

Axioma 2 Sendo a e b dois números inteiros quaisquer podem ser estabelecidas as seguintes leis em relação a sua ordenação:

(i) "Se $a > 0$ e $b > 0$, então $a + b > 0$ e $a \cdot b > 0$." (SAMPAIO; CAETANO, 2009, p. 13).

(ii) "Para cada inteiro a, tem se uma e somente uma das afirmações: $a > 0$, $a = 0$, $-a > 0$." (SAMPAIO; CAETANO, 2009, p. 13).

Definição 2 "Sendo a e b inteiros quaisquer, dizemos que $a < b$ (a é menor que b), ou que $b > a$ (b é maior que a), se $b - a > 0$. Escrevemos $a \leq b$ quando $a < b$ ou $a = b$ e escrevemos $a \geq b$ quando $a > b$ ou $a = b$." (SAMPAIO; CAETANO, 2009, p. 13).

Proposição 1 Considerando os números a, b e c como números inteiros tem-se que:

(i) "se $a > b$ e $c > 0$, então $ac > bc$" (SAMPAIO; CAETANO, 2009, p. 13).

(ii) "se $a > b$ e $c < 0$, então $ac < bc$" (SAMPAIO; CAETANO, 2009, p. 13).

Demonstração:

(i) Conforme a Definição 2 sendo $a > b$ então $a - b > 0$. Pelo item (i) do Axioma 2 temos que $(a - b)c > 0$. Pela lei distributiva tem-se que $ac + (-b)c > 0$, portanto $ac - bc > 0$, logo $ac > bc$.

(ii) Considerando as informações do item passado tem-se que $a - b > 0$, visto que neste caso $c < 0$ ao multiplicar a inequação por (-1) tem-se que $-c > 0$, assim $(a - b) \cdot (-c) > 0$, utilizando da lei distributiva temos que $-ac + bc > 0$, logo prova-se assim que $bc > ac$ ou ainda $ac < bc$.

■

Definição 3 "Se a e b são inteiros, dizemos que $a\ divide\ b$, denotando por $a|b$, se existir um inteiro c tal que $b = ac$." (SANTOS, 2011, p. 3).

Exemplo 1 $6|216$, já que, existe um inteiro, 36, tal que $216 = 6 \cdot 36$.

Teorema 3 Para todo a, b, c, d e e pertencentes ao conjunto dos números inteiros a divisão tem as seguintes propriedades:

(i) "Se $a|b$ e $b|c$, então $a|c$." (BUCHMANN, 2002, p. 13).

(ii) "Se $a|b$ e $b|c$, então $ac|bc$ para todo c." (BUCHMANN, 2002, p. 13).

(iii) "Se $c|a$ e $c|b$, então $c|da + eb$ para todo d e e." (BUCHMANN, 2002, p. 13).

(iv) "Se $a|b$ e $b \neq 0$, então $|a| \leq |b|$." (BUCHMANN, 2002, p. 13).

(v) "Se $a|b$ e $b|a$, então $|a| = |b|$." (BUCHMANN, 2002, p. 13).

Demonstração:

(i) Se $a|b$ e $b|c$ então pela Definição 3 existem k_1 e k_2 tal que $b = ak_1$ e $c = bk_2$, substituindo a primeira equação na segunda tem-se $c = ak_1k_2 = a(k_1k_2)$.

(ii) Se $a|b$, então existe um k tal que $b = ak$, com isso $bc = (ak)c = k(ac)$.

(iii) Se $c|a$ e $c|b$ então existem k_1 e k_2, tal que $a = k_1c$ e $b = k_2c$, o que implica que $da + eb = dk_1c + ek_2c = (dk_1 + ek_2)c$.

(iv) Se $a|b$ e $b \neq 0$, existe um $k \neq 0$ tal que $b = ak$ o que implica dizer que $|b| = |ak| \geq |a|$.

(v) Supondo que Se $a|b$ e $b|a$, implica dizer que se $a = 0$, então $b = 0$. Caso $a \neq 0$ e $b \neq 0$ por (iv) tem-se que $|a| \leq |b|$ e $|b| \leq |a|$ assim $|a| = |b|$.

■

Teorema 4 "Se a e b são números inteiros, sendo $b > 0$, então existem os números inteiros determinados unicamente, q e r, tais que $a = qb + r$ e $0 \leq r < b$, ou seja, $q = \lfloor a/b \rfloor$ e $r = a - bq$." (BUCHMANN, 2002, p. 13).

Demonstração: "Se $a = qb + r$ e $0 \leq r < b$, então $0 \leq [r/b] = a/b - q < 1$. Isso implica que $a/b - 1 < q \leq a/b$; logo $q = \lfloor a/b \rfloor$. Consecutivamente, $q = \lfloor a/b \rfloor$ e $r = a - bq$ satisfazem a afirmativa." (BUCHMANN, 2002, p. 14).

■

Vale ressaltar que as letras q e r presentes no Teorema 4 e em sua demonstração são chamados respectivamente de quociente e de resto da divisão de a por b, para encontrar o valor do resto pode-se escrever então a seguinte equação: $r = a\ mod\ b$ (lê-se a módulo b), sendo a o dividendo e b o divisor.

Definição 4 "Um divisor comum de a e b é um número inteiro que divide ambos, a e b." (BUCHMANN, 2002, p. 20).

Teorema 5 "Entre todos os divisores comuns de dois números inteiros a e b, que não sejam ambos iguais a zero, existe um divisor que é exatamente maior que todos (no que diz respeito $a \leq$). Ele é chamado de máximo divisor comum (mdc) de a e b." (BUCHMANN, 2002, p. 20).

Demonstração: Sendo $a \neq 0$. Conforme o Teorema 3 todos os números divisores de a possuem limites em $|a|$. Logo existe um único divisor comum de a e b que é máximo.

■

Exemplo 2 O (mdc) de 10 e 15 é 5, pois 5 é o maior número que divide simultaneamente 10 e 15.

Um caminho para definir o máximo divisor comum de quaisquer dois números inteiros, com eficiência, é a utilização do algoritmo euclidiano que funciona segundo as duas ideias do teorema que será expresso e demonstrado a seguir.

Teorema 6 Sendo a e b dois números inteiros tem-se que:

(i) "Se $b = 0$, então mdc$(a, b) = |a|$." (BUCHMANN, 2002, p. 23).

(ii) "Se $b \neq 0$, então mdc(a, b) = mdc$(|b|, a \ mod \ |b|)$." (BUCHMANN, 2002, p. 23).

Demonstração:

(i) Está obviamente correta, visto que sendo $b = 0$, o máximo divisor comum calculado seria entre a e 0 e independente do valor atribuído para a, este ainda assim dividiria 0 e por consequência seria o máximo divisor de ambos.

(ii) Por meio do Teorema 4 sabe-se que existe um número inteiro q, onde $a = q|b| + (a \ mod \ |b|)$. Logo o mdc de a e b divide o mdc de $|b|$ e $a \ mod \ |b|$.

■

Exemplo 3 O máximo divisor comum entre 200 e 45 é 5 pois, pelo Teorema 6, tem-se que mdc(200, 45) = mdc(45, 200 mod 45) = mdc(45,20) = mdc(20, 45 mod 20) = mdc(20,5) = mdc(5, 20 mod 5) = mdc(5,0) = 5.

Definição 5 "Dizemos que um inteiro p é primo se $p \neq 0$, $p \neq 1$, $p \neq -1$, e os únicos inteiros divisores de p são 1, p, -1 e $-p$. Dizemos que um inteiro m é composto se $m \neq 0$, $m \neq 1$, $m \neq -1$ e m não for primo." (SAMPAIO; CAETANO, 2009, p. 57).

Teorema 7 "(Teorema Fundamental da Aritmética) Todo inteiro maior do que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos." (SANTOS, 2011, p. 9).

Demonstração: Partindo das ideias de Santos (2011) consideremos n um número inteiro, se n for primo, então o teorema está logicamente provado, supondo que esse mesmo n seja um número composto, existe então um número $p_1 > 1$, que é o menor divisor positivo de n, é possível afirmar que p_1 se trata de um número primo, visto que caso contrário existiria um outro número maior que 1 que dividiria p_1 e por consequência dividiria também n, portanto $n = p_1 n_1$. Caso n_1 se trate de um número primo a demonstração foi concluída, porém se tratando de um número composto e utilizando do mesmo argumento anterior existe um p_2 que é o menor divisor de n_1 e que por consequência também é primo, sendo assim $n_1 = p_2 n_2$ e substituindo na primeira igualdade tem se que $n = p_1 p_2 n_2$.

Esse processo se repete até que $n_k = p_k$, ou seja, se torne um número primo e visto que os primos da sequência não necessariamente são distintos, sendo assim podem se repetir, o número n decomposto pode ser expresso pela seguinte equação $n = {p_1}^{a1} {p_2}^{a2} \dots {p_k}^{ak}$. E assim se prova que todo inteiro pode ser representado por um produto de fatores primos, porém resta ainda comprovar que essa fatoração é única.

Para essa comprovação imaginemos que além do produto $p_1 p_2 \dots p_k$ o número inteiro n pode ser fatorado pelo produto $q_1 q_2 \dots q_k$ onde cada q também é um número primo, porém como $p_1 | n$ ele também divide um dos fatores de q, ou seja, supõe-se que $p_1 | q_1$, entretanto como ambos são primos a única possibilidade dessa divisão ocorrer é caso ambos sejam iguais, assim $p_1 = q_1$ e de forma análoga $p_2 = q_2$, sendo assim sucessivamente até $p_k = q_k$. Portanto ambas as fatorações são iguais e assim conclui-se que há apenas uma única forma de fatorar qualquer número em um produto de números primos.

■

Exemplo 4 O número inteiro 600 pode ser decomposto da seguinte forma $2^3 \cdot 3 \cdot 5^2$, visto que $600 = 2 \cdot 300 = 2 \cdot 2 \cdot 150 = 2 \cdot 2 \cdot 2 \cdot 75 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 25 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5$ e essa multiplicação pode ser representada da seguinte forma $2^3 \cdot 3 \cdot 5^2$.

Definição 6 "Se a e b são inteiros dizemos que a é congruente a b módulo m $(m > 0)$ se $m|(a - b)$. Denotamos isto por $a \equiv b \ (mod\ m)$. Se $m \nmid (a - b)$ dizemos que a é incongruente a b módulo m e denotamos $a \not\equiv b \ (mod\ m)$" (SANTOS, 2011, p. 32).

Exemplo 5 $7 \equiv 3 (mod\ 2)$, já que $2|(7 - 3)$, enquanto isso, pode-se afirmar que $8 \not\equiv 1 \ (mod\ 3)$, já que $3 \nmid (8 - 1)$.

Proposição 2 "Se a e b são inteiros, temos que $a \equiv b \ (mod\ m)$ se, e somente se, e existir um inteiro k tal que $a = b + km$." (SANTOS, 2011, p. 32).

Demonstração: Pela Definição 6, para que $a \equiv b\ (mod\ m)$, o valor m tem que dividir a diferença entre a e b, em outras palavras $(a - b)$ tem de ser igual a um múltiplo de m, logo $a - b = km$, ao utilizar da propriedade aditiva na equação tem se que $a = b + km$, com a existência desse k confirmada ao fazer o caminho da volta tem-se que $km = a - b$, sendo assim $m|km$ e por consequência $m|(a - b)$, logo $a \equiv b\ (mod\ m)$.

■

Proposição 3 "Se a, b, m e d são inteiros, $m > 0$,as seguintes sentenças são verdadeiras:" (SANTOS, 2011, p. 32).

(i) "$a \equiv a\ (mod\ m)$" (SANTOS, 2011, p. 32).

(ii) "Se $a \equiv b\ (mod\ m)$, então $b \equiv a\ (mod\ m)$" (SANTOS, 2011, p. 32).

(iii) "Se $a \equiv b\ (mod\ m)$ e $b \equiv d\ (mod\ m)$, então $a \equiv d\ (mod\ m)$." (SANTOS, 2011, p. 32).

Demonstração:

(i) Visto que qualquer número para m divide 0, então logicamente $m|(a - a)$, portanto pode-se afirmar que $a \equiv a\ (mod\ m)$.

(ii) Se $a \equiv b\ (mod\ m)$ pela Proposição 2 ficou provado a existência de um k de tal forma que $a = b + km$, isolando o número b tem-se que $b = a - km$, o que implica pela mesma proposição que $b \equiv a\ (mod\ m)$.

(iii) Sendo $a \equiv b\ (mod\ m)$ e $b \equiv d\ (mod\ m)$ e pela Definição 6, existem dois números inteiros k_1 e k_2, de forma que $a - b = k_1 m$ e $b - d = k_2 m$, ao somar as duas equações tem-se que $a - d = k_1 m + k_2 m$ evidenciando o termo em comum a equação pode ser reescrita da seguinte forma $a - d = (k_1 + k_2)m$ o que implica afirmar que $a \equiv d\ (mod\ m)$.

■

Ao provar os tópicos dessa proposição, é possível afirmar que a relação de congruência no conjunto dos números inteiros se trata de uma relação de equivalência, visto que se foram comprovadas as propriedades: reflexiva, simétrica e transitiva.

Teorema 8 "Se a, b, c e m são inteiros tais que $a \equiv b\ (mod\ m)$, então" (SANTOS, 2011, p. 33).

(i) "$a + c \equiv b + c (mod\ m)$" (SANTOS, 2011, p. 33).

(ii) "$a - c \equiv b - c (mod\ m)$" (SANTOS, 2011, p. 33).

(iii) "$ac \equiv bc (mod\ m)$" (SANTOS, 2011, p. 33).

Demonstração:

(i) Como foi dito no teorema que $a \equiv b\ (mod\ m)$ tem-se que $a - b = km$, visto que $a - b$ pode ser reescrito da seguinte forma $(a + c) - (b + c)$ sem causar alteração ao resultado da equação tem-se que $a + c \equiv b + c(mod\ m)$.

(ii) Assim como foi possível adicionar o termo c sem modificar o resultado da equação, e considerando também que $a \equiv b\ (mod\ m)$ é possível também reduzir esse mesmo termo sem causar nenhuma alteração, assim $a - b$ pode ser reescrito como $(a - c) - (b - c)$ e portanto $a - c \equiv b - c(mod\ m)$.

(iii) Visto que para $a \equiv b\ (mod\ m)$ a sentença $a - b = km$ tem de ser verdadeira, ao multiplicar todos os termos por c tem se que $ac - bc = ckm$, o que significa que $m|(ac - bc)$ e com isso $ac \equiv bc(mod\ m)$.

■

Teorema 9 "Se a, b, c, d e m são inteiros tais que $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$, então" (SANTOS, 2011, p. 33).

(i) "$a + c \equiv b + d(mod\ m)$" (SANTOS, 2011, p. 33).

(ii) "$a - c \equiv b - d(mod\ m)$" (SANTOS, 2011, p. 33).

(iii) "$ac \equiv bd(mod\ m)$" (SANTOS, 2011, p. 33).

Demonstração:

(i) Se $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$, existem então dois inteiros k_1 e k_2 de tal forma que $a - b = k_1 m$ e $c - d = k_2 m$ ao somar as duas equações tem-se uma nova equação no seguinte formato $a - b + c - d = k_1 m + k_2 m$, ao evidenciar os termos semelhantes obtemos que $(a + c) - (b + d) = (k_1 + k_2)m$ o que implica dizer que $a + c \equiv b + d(mod\ m)$.

(ii) Partindo da mesma ideia utilizada no item (i), basta subtrair ambas as equações que se encontra a seguinte equação $a - b - (c - d) = k_1 m - k_2 m$ ao desenvolver a equação tem-se que $a - b - c + d = k_1 m - k_2 m$ ao organizar a mesma obtém se a equação $(a - c) - (b - d) = (k_1 - k_2)m$ o que em implica afirmar que $a - c \equiv b - d(mod\ m)$.

(iii) Ao multiplicar a equação $a - b = k_1 m$ por c e a equação $c - d = k_2 m$ por b obtém-se que $ac - bc = ck_1 m$ e $bc - bd = bk_2 m$, feito isso ao somar ambas as equações tem-se que $ac - bc + bc - bd = ck_1 m + bk_2 m$, resolvendo-a e evidenciando os termos em comum conclui-se que $ac - bd = (ck_1 + bk_2)m$ o que implica dizer que $ac \equiv bd(mod\ m)$. ■

Teorema 10 (Teorema de Fermat) “Se p é um primo e se p não divide o inteiro a $(p \nmid a)$, então: $a^{p-1} \equiv 1\ (mod\ p)$” (ALENCAR FILHO, 1981, p. 193).

Demonstração: Tendo por base as ideias de Alencar Filho (1981), ao se considerar os $p-1$ primeiros múltiplos de a, ou seja, os números inteiros: $a, 2a, 3a, \dots, (p-1)a$. Nenhum destes é congruente a 0 em módulo p, além disso, dois quaisquer deles são incongruentes em módulo p, isto devido ao fato que se estes fossem congruentes, o fator a seria cancelado devido ao fato que o $\text{mdc}(a, p) = 1$. Logo, cada número inteiro da sequência: $a, 2a, 3a, \dots, (p-1)a$ é congruente em módulo p apenas a um único número inteiro $1, 2, 3, \dots, (p-1)$. Ao multiplicar todas essas $p-1$ congruências, teremos: $a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1)$ $(mod\ p)$, ao simplificar a congruência cancelando os fatores comuns, tem-se a congruência: $a^{p-1} \equiv 1\ (mod\ p)$.

■

4 CRIPTOGRAFIA ANTIGA VS CRIPTOGRAFIA RSA

Com apoio dos conceitos que foram abordados no capítulo anterior, este será destinado a apresentar por meio da prática a funcionalidade de alguns métodos já abordados neste trabalho, que foram e são importantes para garantir a segurança e privacidade daqueles que estão envolvidos na mensagem e após isso realizar um comparativo do avanço dos métodos criptográficos relacionando-os com a criptografia RSA, de forma a além de abordar a motivação desse desenvolvimento, discorrer também sobre a garantia de segurança ao aplicar tais métodos.

4.1 Codificação e decodificação em alguns métodos utilizados no passado

Tendo por base os métodos abordados ao decorrer do capítulo 2, nessa seção será codificada e decodificada a mensagem "CRIPTOGRAFIA" fazendo-se o uso de alguns métodos utilizados nos períodos conhecidos por Idade Antiga, Idade Moderna e Idade Contemporânea (vale ressaltar que durante a Idade Média não surgiram tantos métodos de codificação, o período expressou um avanço na criptoanálise), sendo esses os seguintes métodos: código de César, cifra de Vigenère, quadro de Políbio, cifra ADFGX e cifra de Bacon.

Como já dito anteriormente o código de César se trata de um método na qual todas as letras do alfabeto serão substituídas por letras que estão a uma determinada quantidade de casas a frente. Logo para criptografar a mensagem primeiramente é necessário determinar um número para descrever quantas casas a frente estará a representação de cada letra. Imagina-se nesse exemplo que cada letra foi substituída pela letra que se encontra 3 casas a frente de si, podemos então construir a seguinte tabela:

Quadro 1 - Alfabeto substituído por meio do código de César

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

Fonte: Elaborado pelo autor

Sendo as letras destacadas em negrito o alfabeto corrente e as que estão imediatamente abaixo delas a letra que as representa no código de César, a mensagem "CRIPTOGRAFIA" é codificada e encaminhada ao destinatário da seguinte forma: "FULSWRJUDILD". Para que este consiga decodificar a mensagem em questão é necessário que, além da mensagem

obviamente, o mesmo tenha conhecimento da quantidade de casas a frente que foram utilizadas para substituir cada letra do alfabeto pela letra da mensagem. Visto que no exemplo foi-se utilizado 3 casas a frente porém, essa não é uma lei para a mudança cíclica do alfabeto, o mesmo pode ser alterado em 2 ou 20 casas a sua frente por exemplo.

Apesar de ter sido desenvolvido durante a idade Antiga, a cifra de César continua a ser utilizada até a atualidade, um exemplo disso está na cifra de Vigenère, que se baseia no método romano. Essa cifra como já abordado no tópico 2.3.2, que se encontra no capítulo 2, trata-se de uma tabela de 26 linhas por 26 colunas na qual são dispostas 26 cifras de César sendo a primeira linha o alfabeto corrente, a segunda com o avanço de uma casa, a terceira com o avanço de duas casas e assim sucessivamente, sendo que as linhas e colunas são numeradas pelo alfabeto, a linha 1, por exemplo, é chamada de linha A.

A vantagem desse método em relação a seu antecessor é que a cifra de Vigenère possibilita que uma mesma mensagem seja criptografada por diferentes cifras de César de forma a não ter de seguir apenas uma mudança cíclica do alfabeto. Para que haja codificação por esse método é necessário além da tabela que se tenha uma palavra-chave, visto que a mesma vai ser responsável por mostrar as colunas utilizadas para codificar a mensagem, de forma que cada letra da mensagem indique uma linha, assim por meio do par linha e coluna se encontra a letra criptografada.

Para codificar a mesma mensagem por esse método considera-se a palavra-chave sendo “ALGARISMO”, vale ressaltar que caso a mensagem seja maior que a palavra-chave, basta ao fim da mesma reiniciá-la até que se tenha um respectivo para cada uma das letras da mensagem, assim pode-se construir a seguinte tabela para utilizar na figura 7 com o intuito de encontrar a mensagem criptografada:

Quadro 2 - Linhas e colunas para codificação por Vigenère

Linha:	C	R	I	P	T	O	G	R	A	F	I	A
Coluna:	A	L	G	A	R	I	S	M	O	A	L	G

Fonte: Elaborado pelo autor

Assim ao associar linha e coluna, tem-se que a letra que se encontra na linha C e na coluna A se trata da letra “C”, logo essa será a primeira letra da mensagem criptografada, a letra presente no encontro da linha R com a coluna L se trata também de um “C” portanto essa é a segunda letra da mensagem, ao realizar esse processo com todas as demais letras, obtém-se que a mensagem “CRIPTOGRAFIA” ao ser codificada utilizando deste método, passa a ser “CCOPKWYDOFTG” e assim está pronta para ser enviada ao seu destinatário.

Para que o receptor da mensagem consiga decodificar sabendo que o método utilizado se trata da cifra de Vigenére, além de possuir acesso, conhecimento ao método e sua tabela, é necessário que o mesmo saiba qual a palavra-chave utilizada para codificar, visto que por meio desta ele irá decodificar associando a letra da mensagem criptografada com a letra da palavra-chave que será a coluna da tabela para assim encontrar a letra respectiva a linha dessa tabela, que será a letra da mensagem original, ao fazer esse processo com todas as letras o mesmo irá obter acesso à mensagem decodificada.

Outro método da idade Antiga a ser abordado é o quadro de Políbio, que como apresentado no capítulo 2 consiste em um quadrado 5x5, em que o mesmo transforma cada letra do alfabeto em um número de dois algarismos, sendo esses respectivamente o número da linha e da coluna que representa a sua localização no quadro, conforme representa a seguinte tabela:

Quadro 3 - Alfabeto pelo quadro de Políbio

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

Fonte: Elaborado pelo autor

Pode-se observar que a letra “C” está na primeira linha e terceira coluna logo esta será representada pelo número 13. A letra “R” encontra-se na quarta linha e segunda coluna assim o número que a representa será o número 42, ao fazer isso com as demais letras da mensagem, tem-se que a mesma codificada passa a ser: 134224354434224211212411.

Ao receber essa mensagem, para decodificá-la é necessário ter conhecimento do método de forma a saber que se trata de um quadrado de formato 5x5 e, entender que os números devem ser separados em pares da seguinte forma: 13 42 24 35 44 34 22 42 11 21 24 11, para que assim se tenha a localização referente a linha e coluna nessa ordem respectivamente.

Assim como o código de César, o quadro de Políbio foi importante não só no seu tempo, esse foi importante na Primeira Guerra Mundial, visto que serviu de base para o método de cifragem alemão que ficou conhecido como cifra ADFGX, pois ao invés dos números utilizavam-se dessas letras sendo “A” na posição onde se encontra o número 1, “D” no lugar do número 2 e assim por diante conforme a seguinte tabela:

Quadro 4 - Tabela utilizada na cifra ADFGX

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

Fonte: Elaborado pelo autor

A primeira parte da codificação por esse método segue como o método anterior, a única diferença é que ao invés de se utilizar um par de números para representar cada letra da mensagem é utilizado um par de letras, sendo a primeira letra a letra referente a linha e a segunda referente a coluna. Assim tem-se que a mensagem passa a ser "AFGDDGFXGGFGDDGDAADADGAA".

Após essa primeira etapa é necessário escolher uma palavra-chave, sendo que não há restrição quanto ao tamanho desta. Porém a palavra-chave não pode conter letras iguais em sua composição, desse modo a palavra selecionada para agir como palavra-chave foi "CIFRA". Após isso, se desenvolve uma tabela na qual a primeira linha é composta pelas letras da palavra chave e as demais linhas pelas letras da mensagem cifrada da seguinte maneira:

Quadro 5 - Aplicação da palavra-chave na cifra ADFGX

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

Fonte: Elaborado pelo autor

Após posicionar a mensagem em uma tabela com a palavra-chave, é necessário organizá-la em ordem alfabética em relação a palavra-chave de forma que a primeira linha fique na seguinte ordem: “ACFIR”. Para que isso ocorra é necessário que as colunas sejam alteradas conforme a primeira linha, ou seja, o “A” da primeira linha e todos os demais termos abaixo deste que antes pertenciam a quinta coluna, agora passam a ser da primeira coluna. E assim sucessivamente com os demais termos de modo que a tabela fique da seguinte maneira:

Quadro 6 - Organização da palavra-chave e da mensagem cifrada

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

Fonte: Elaborado pelo autor

Feito isso a mensagem cifrada passa a ser o agrupamento de cada coluna com a exceção dos membros pertencentes a palavra-chave, ou seja, a mensagem criptografada e enviada ao seu respectivo destinatário é então: DGGA AGFDD GXDAA FFGAG DGDDA.

Para decodificar a mensagem o receptor da mesma deverá ter em posse a palavra-chave para primeiramente organizar a mensagem em colunas abaixo da palavra-chave. Lembrando que, primeiramente essa palavra tem de estar com suas letras em ordem alfabética, após isso organizar as colunas de modo a encontrar a palavra-chave na primeira linha. Feito isso a mensagem estará no modelo pré-codificado então basta separá-la em pares e considerar a primeira letra como linha e a segunda como coluna em uma tabela ADFGX, desse modo cada um dos pares da codificação fornecerá uma letra da mensagem original e ao final desse processo o destinatário terá em mãos a mensagem original.

Bacon criou um outro sistema baseado no uso de apenas duas letras, que será apresentado no momento, sendo essas, as letras A e B, ou seja, cada letra do alfabeto pode ser representada por uma determinada combinação de letras A e B. Ressaltando que as letras “I” e “J” são representadas pela mesma combinação, bem como ocorre também com as letras “U” e

"V". Esse sistema é utilizado atualmente porém de forma binária, substituindo respectivamente o A e B por 0 e 1. O sistema de Bacon pode ser representado da seguinte maneira:

Quadro 7 - Alfabeto pela cifra de Bacon

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**
AAAAA	AAAAB	AAABA	AAABB	AABAA	AABAB	AABBA	AABBB
I/J	**K**	**L**	**M**	**N**	**O**	**P**	**Q**
ABAAA	ABAAB	ABABA	ABABB	ABBAA	ABBAB	ABBBA	ABBBB
R	**S**	**T**	**U/V**	**W**	**X**	**Y**	**Z**
BAAAA	BAAAB	BAABA	BAABB	BABAA	BABAB	BABBA	BABBB

Fonte: Elaborado pelo autor

Assim como no exemplo da tabela 1, nesta tabela as letras destacadas em negrito se tratam do alfabeto corrente e a sequência imediatamente abaixo de cada letra se trata da representação da mesma pelo código de Bacon. É válido ressaltar que em todas as sequências se tem exatamente 5 letras, para criptografar a mensagem basta substituir cada letra pela sequência que a representa, logo a mensagem "CRIPTOGRAFIA" ao ser codificada por esse método pode ser encaminhada ao destinatário da seguinte forma: AAABABAAAAABAAAABBBABAABAABBABAABBABAAAAAAAAAAAABABABA AAAAAAA.

Para que o destinatário interprete a mensagem e consiga decodificá-la é necessário que ele tenha conhecimento de como funciona a cifra de Bacon para que caso não tenha consigo uma tabela pronta, possa produzir uma, além disso é necessário lembrar que cada letra é representada por uma sequência de 5 números, assim é possível desmembrar a mensagem da seguinte maneira: AAABA BAAAA ABAAA ABBBA BAABA ABBAB AABBA BAAAA AAAAA AABAB ABAAA AAAAA. E após isso, associar cada sequência com sua respectiva letra, obtendo assim acesso a informação.

4.2 Codificação e decodificação conforme o método RSA

Como já dito anteriormente um método que vem funcionando, quando se trata de criptografar na atualidade, é o método RSA. Tal método se baseia na utilização de dois números para criptografar sendo esses conhecidos por n e λ, de forma que n pode ser encontrado por

meio da multiplicação de dois números primos p e q, vale ressaltar que quanto maior esses números mais segura será a mensagem. Enquanto que λ ao ser associado com n necessita estabelecer uma relação na qual ambos sejam primos entre si, ou seja o máximo divisor comum de λ e n tem de ser 1. Para a decodificação da mensagem ser possível é necessário o uso de uma chave d, de forma que para encontrá-la deve ser estabelecida a relação de congruência: $\lambda \times d \equiv 1\ mod((p-1)\times(q-1))$.

Devido ao fato dessa codificação ser restrita ao uso de números é necessário antes associar cada letra do alfabeto a um determinado número. Ao todo existem 26 letras e, é indicado associar cada uma dessas a um número de dois algarismos, visto que caso contrário poderia haver ambiguidade de informações o que poderia atrapalhar a codificação e decodificação da mensagem, dito isso associaremos da seguinte forma:

Quadro 8 - Pré-codificação para o método RSA

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
10	11	12	13	14	15	16	17	18	19	20	21	22
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
23	24	25	26	27	28	29	30	31	32	33	34	35

Fonte: Elaborado pelo autor

Feito isso substitui-se o nome “CRIPTOGRAFIA” pelos números que representam respectivamente cada letra, ficando assim com o seguinte código: 12-27-18-25-29-24-16-27-10-15-18-10. Após isso tem que se encontrar o valor de a em $b^{\lambda} \equiv a(mod\ n)$, sendo b cada um dos códigos encontrados ao substituir a mensagem por meio da tabela. Posteriormente, substitui-se b por a, para assim obter a mensagem codificada. Considerando-se que no exemplo foi utilizado que $p = 3$ e $q = 11$, logo: $n = 33$ e que $\lambda = 7$.

Assim tendo por base os seguintes cálculos:

$$12^7 \equiv a(mod\ 33) \equiv (12^2)^3 \times 12 \equiv 144^3 \times 12 \equiv 12^3 \times 12 \equiv 12^2 \times 12^2 \equiv 12 \times 12 \equiv \mathbf{12}$$

$12^7 \equiv 12(mod\ 33)$, logo “C” segue sendo 12;

$$27^7 \equiv a(mod\ 33) \equiv [(-6)^2]^3 \times (-6) \equiv 36^3 \times (-6) \equiv 3^3 \times (-6) \equiv (-6)^2 \equiv \mathbf{3}$$

$27^7 \equiv 3(mod\ 33)$, logo “R” passa a ser 3;

$$18^7 \equiv a(mod\ 33) \equiv (18^2)^3 \times 18 \equiv 324^3 \times 18 \equiv 27^3 \times 18 \equiv (-6)^2 \times (-6) \times 18$$
$$\equiv 3 \times (-6) \times 18 \equiv 54 \times (-6) \equiv (-12) \times (-6) \equiv \mathbf{6}$$

$18^7 \equiv 6(mod\ 33)$, logo “I” passa a ser 6;

$$25^7 \equiv a(mod\ 33) \equiv [(-8)^2]^3 \times (-8) \equiv (-2)^3 \times (-8) \equiv (-8) \times (-8) \equiv (-2) \equiv \mathbf{31}$$

$25^7 \equiv 31(mod\ 33)$, logo "P" passa a ser 31;

$$29^7 \equiv a(mod\ 33) \equiv [(-4)^3]^2 \times (-4) \equiv (2)^2 \times (-4) \equiv 4 \times (-4) \equiv (-16) \equiv \mathbf{17}$$

$29^7 \equiv 17(mod\ 33)$, logo "T" passa a ser 17;

$$24^7 \equiv a(mod\ 33) \equiv [(-9)^2]^3 \times (-9) \equiv (15)^3 \times (-9) \equiv 15^2 \times 15 \times (-9)$$
$$\equiv (-6) \times 15 \times (-9) \equiv 15 \times (-12) \equiv (-15) \equiv \mathbf{18}$$

$24^7 \equiv 18(mod\ 33)$, logo "O" passa a ser 18;

$$16^7 \equiv a(mod\ 33) \equiv (16^2)^3 \times 16 \equiv (-8)^3 \times 16 \equiv (-8)^2 \times (-8) \times 16$$
$$\equiv (-2) \times (-8) \times 16 \equiv 16^2 \equiv (-8) \equiv \mathbf{25}$$

$16^7 \equiv 25(mod\ 33)$, logo "G" passa a ser 25;

$$10^7 \equiv a(mod\ 33) \equiv 10^7 \equiv (10^2)^3 \times 10 \equiv 1^3 \times 10 \equiv \mathbf{10}$$

$10^7 \equiv 10(mod\ 33)$, logo "A" passa a ser 10;

$$15^7 \equiv a(mod\ 33) \equiv 15^7 \equiv (15^2)^3 \times 15 \equiv (-6)^3 \times 15 \equiv (-6)^2 \times (-6) \times 15$$
$$\equiv 3 \times (-6) \times 15 \equiv (-6) \times 12 \equiv (-6) \equiv \mathbf{27}$$

$15^7 \equiv 27(mod\ 33)$, logo "F" passa a ser 27.

Como as demais letras do nome são repetidas das que já se tem o código, pode-se concluir que a mensagem "CRIPTOGRAFIA" pelo método RSA passa a ser: 12-3-6-31-17-18-25-3-10-27-6-10.

Para decodificar a mensagem é necessário que o destinatário tenha em sua posse a chave d, nesse caso como se sabe o valor de p, q e λ é possível por meio da fórmula: $\lambda \times d \equiv 1\ mod((p-1) \times (q-1))$ encontrar o valor da chave. Calculando então tem-se que $7d \equiv 1\ (mod(3-1) \times (11-1))$, assim $7d \equiv 1\ (mod\ 20)$, pode-se definir então que $d = 3$. Tendo o valor de d basta encontra o valor de b em $a^d \equiv b(mod\ n)$.

Partindo aos cálculos tem-se que:

$$12^3 \equiv b\ (mod\ 33) \equiv 12^2 \times 12 \equiv 144 \times 12 \equiv 12 \times 12 \equiv \mathbf{12}$$

$12^3 \equiv 12(mod\ 33)$, logo o valor de b é 12;

$$3^3 \equiv b\ (mod\ 33) \equiv \mathbf{27}$$

$3^3 \equiv 27(mod\ 33)$, logo o valor de b é 27;

$$6^3 \equiv b\ (mod\ 33) \equiv 6^2 \times 6 \equiv 36 \times 6 \equiv 3 \times 6 \equiv \mathbf{18}$$

$6^3 \equiv 18(mod\ 33)$, logo o valor de b é 18;

$$31^3 \equiv b\ (mod\ 33) \equiv (-2)^3 \equiv -8 \equiv \mathbf{25}$$

$31^3 \equiv 25(mod\ 33)$, logo o valor de b é 25;

$$17^3 \equiv b\ (mod\ 33) \equiv 17^2 \times 17 \equiv (-8) \times 17 \equiv (-4) \equiv \mathbf{29}$$

$17^3 \equiv 29(mod\ 33)$, logo o valor de b é 29;

$18^3 \equiv b\ (mod\ 33) \equiv 18^2 \times 18 \equiv (-6) \times 18 \equiv (-9) \equiv \mathbf{24}$

$18^3 \equiv 24(mod\ 33)$, logo o valor de b é 24;

$25^3 \equiv b\ (mod\ 33) \equiv (-8)^2 \times (-8) \equiv (-2) \times (-8) \equiv \mathbf{16}$

$25^3 \equiv 16(mod\ 33)$, logo o valor de b é 16;

$10^3 \equiv b\ (mod\ 33) \equiv 10^2 \times 10 \equiv 1 \times 10 \equiv \mathbf{10}$

$10^3 \equiv 10(mod\ 33)$, logo o valor de b é 10;

$27^3 \equiv b\ (mod\ 33) \equiv (-6)^3 \equiv (-6)^2 \times (-6) \equiv 3 \times (-6) \equiv (-18) \equiv \mathbf{15}$

Tendo decodificado todos os números, considerando as repetições, tem-se agora o seguinte código: 12-27-18-25-29-24-16-27-10-15-18-10. Feito isso, basta apenas associar a tabela 8, a qual o destinatário também tem acesso e o mesmo terá a mensagem totalmente decodificada. Vale ainda ressaltar que, isso porém só foi possível devido ao conhecimento dos números p e q para se calcular o valor de d.

4.3 Comparando os métodos

Observa-se que, os primeiros métodos desenvolvidos ainda na Idade Antiga, ao serem analisados atualmente são considerados mais fáceis de decifrar, visto que a sua metodologia é amplamente conhecida e que consistiam apenas em métodos de substituição. Porém, como visto no capítulo inicial, durante algumas "eras" os métodos em questão foram muito importantes para garantir o segredo de informações sigilosas.

Além da importância durante o período, alguns métodos criptográficos da Idade Antiga serviram ainda como base para métodos utilizados em outras "eras". Como o quadro de Políbio por exemplo que foi utilizado como base para a cifra ADFGX, utilizada por alemães durante a Primeira Guerra Mundial, já no decorrer da Idade Contemporânea. Pode-se dizer que tal cifra se trata de um aprimoramento da cifra antiga, a diferença dessa e das demais cifras dos períodos Moderno e Contemporâneo para as mais antigas é que a maioria destas passaram a utilizar de palavras-chave, para aperfeiçoar a forma de criptografar e dificultar que a mensagem fosse descoberta por outros, que não o destinatário da mesma.

Contudo, foi percebido que, ao criptografar por esses métodos no tópico 4.1, para que o receptor da mesma consiga decodificar a mensagem é necessário que esse tenha acesso ao meio que foi utilizado para codificar e à palavra-chave, quando for o caso do método exigir uma. Em outras palavras, além da mensagem codificada deve ser encaminhada também a chave que foi utilizada para codificá-la. O que acaba por apresentar um risco, visto que por diversos meios a

chave dessa mensagem pode ser interceptada, acabando assim com o sigilo das informações presentes na mesma.

Como visto no tópico 4.2 atualmente o método de criptografar mensagens que apresenta êxito na sua função é o método RSA, isso se dá pelo fato de que o método em questão inovou-se em relação aos demais. Visto que, se trata de um método de chave pública, ou seja, a chave utilizada para codificar a mensagem pode ser de domínio público e mesmo assim não irá interferir na segurança do método, já que a chave utilizada para decodificar a mensagem é outra, sendo que, essa apenas o destinatário da mensagem tem acesso.

Outro fator que garante a segurança desse método é que os números utilizados para criar as chaves são pares de números primos, sendo esses indefinidos. Quanto maiores os números utilizados, mais difícil será descobrir a chave, mesmo com a utilização dos meios tecnológicos, uma vez que, a chave que será necessária para desvendar a mensagem é uma chave privada.

5 METODOLOGIA

A presente monografia foi realizada com a utilização de pesquisas de cunho bibliográfico, dispondo de artigos científicos, teses e dissertações encontradas por meio da plataforma Google Acadêmico, com o intuito de observar e analisar o que outros autores abordam sobre a história da criptografia. Ademais, foram utilizados livros físicos, indicados e cedidos pelo orientador do pesquisando relacionados à disciplina de Teoria dos Números. Quanto a esse modelo de pesquisa, Fonseca (2002, p. 32) corrobora ao afirmar que a mesma é realizada:

> [...] a partir do levantamento de referências teóricas já analisadas, e publicadas por meios escritos e eletrônicos, como livros, artigos científicos, páginas de web sites. Qualquer trabalho científico inicia-se com uma pesquisa bibliográfica, que permite ao pesquisador conhecer o que já se estudou sobre o assunto. Existem porém pesquisas científicas que se baseiam unicamente na pesquisa bibliográfica, procurando referências teóricas publicadas com o objetivo de recolher informações ou conhecimentos prévios sobre o problema a respeito do qual se procura a resposta.

O processo de levantamento bibliográfico foi realizado em duas etapas, sendo feito primeiramente uma pesquisa referente aos aspectos históricos, ou seja, quanto a utilização de conceitos da criptografia em diversos períodos da história, tanto na criação de métodos e no uso de instrumentos para codificar e decodificar mensagens, quanto no surgimento de pessoas destinadas a analisar e decifrar tais mensagens, em um segundo momento foram feitas pesquisas relacionadas a conceitos da matemática diretamente relacionados a criptografia.

Além de toda a busca bibliográfica, foram executados também testes de codificação e decodificação de alguns modelos utilizados ao longo da história com a finalidade de apresentar a utilização da criptografia pelos respectivos povos, de forma a demonstrar a funcionalidade de tais métodos, bem como por consequência apresentar o progresso da criptografia com o decorrer do tempo e o avanço dos métodos de codificar e decodificar uma mensagem.

6 CONSIDERAÇÕES FINAIS

Observou-se que, a necessidade de segurança e privacidade de mensagens existe desde as primeiras civilizações com registros históricos a povoarem o planeta, tais como a civilização egípcia e mesopotâmica por exemplo. Logo, é evidente afirmar que conceitos criptográficos existem desde a Idade Antiga, mesmo que a codificação seja de forma primária e considerada básica, se for analisada com os recursos existentes atualmente.

Por mais que apresentem ideias simples, os primeiros métodos criados, ainda durante a Idade Antiga serviram de base para o desenvolvimento de outros métodos utilizados até na Idade Contemporânea. É válido notar ainda que, apesar destes fazerem o uso dos mesmos princípios dos primeiros, eram muito mais complicados de serem decodificados por pessoas as quais não eram o destinatário da mensagem.

Porém, como ocorreu na Idade Média, após a criação de métodos de codificar mensagens, surgiram pessoas destinadas a analisar e estudar as informações criptografadas com o intuito de entender os métodos utilizados para assim, decodificar a mensagem e qualquer outra que utilize de tal método. Essas pessoas passaram a ser chamadas de criptoanalistas e o ato realizado por estes de criptoanálise.

Assim notou-se que, com a criação de um novo método, inicia-se o estudo sobre tal pelos criptoanalistas, com o intuito de “quebrar” o método em questão, como ocorreu a relação entre a criação da máquina Enigma e os estudos realizados pelos criptoanalistas de Bletchley Park, como já visto, os grandes responsáveis pela decodificação de diversas mensagens Alemãs durante a Segunda Guerra Mundial.

Atualmente, com o avanço da tecnologia, criptoanalistas possuem muito mais recursos para desvendar os segredos de diversos métodos de decodificação. Porém, a sociedade tende a continuar apresentando a necessidade de segurança e privacidade, diante disso existem métodos como o RSA que, apesar de toda a tecnologia existente, segue sendo quase impossível de decodificar. Isso pelo fato de que, esse modelo inova ao utilizar chaves diferentes para codificar e decodificar a mensagem de forma que, o segredo para decodificar a mensagem não tem necessidade de ser transmitido com a mesma e, por não ter relação com a chave para decodificar, a chave de codificação em tal método pode ser de acesso público.

Outro fator importante que garante a confiabilidade em tal método é a questão de que para a criação de tais chaves são utilizados números primos. Como se sabe os números primos não possuem padrão, logo podem existir números primos muito extensos e por consequência,

quanto mais extensos os números selecionados mais seguro será a criptografia, visto que será mais difícil encontrar tais números.

Como dito o método RSA envolve a questão de números primos, porém engana-se quem acredita que esse seja o único conceito matemático utilizado em tal método. Conceitos como divisibilidade e congruência são de grande importância para criptografar pelo modelo de codificação em questão. Dito isso o capítulo 3 foi responsável por explanar de forma concreta diversos conceitos relacionados à disciplina de Teoria dos Números, sendo esses, base para a criptografia RSA.

Ao se fazer a codificação de uma mensagem pelo método RSA no item 4.2, verificou-se a importância de cada um desses conceitos para tal codificação mostrando o quão atrelada a Matemática está a criptografia. Ainda nesse exemplo é possível observar ao comparar com outros modelos que o ato de decodificar a mensagem é um tanto quanto mais complexo, visto que, a chave utilizada para codificar não possui utilidade no momento de decodificar e a responsável por decodificar não é de simples encontro já que, como dito anteriormente podem ser utilizados números imensamente extensos, fato esse que impossibilita a descoberta da chave de decodificação.

Assim, apesar de todo o desenvolvimento quanto à criptoanálise é possível afirmar que, a criptografia sempre esteve “um passo à frente” visto que, ao longo de toda história até chegar a sociedade atual, sempre existiram métodos de criptografia que foram úteis para aqueles que estavam a usufruir de tal e que perduraram por um bom tempo até que conseguissem descobrir seus segredos e torná-los métodos obsoletos. Na sociedade atual não é diferente, já que, mesmo com todos os artifícios a serem utilizados para “quebrar” os segredos da criptografia, existem métodos tais como o RSA que seguem apresentando segurança e privacidade a quem está por se comunicar.

REFERÊNCIAS

ALENCAR FILHO, Edgard de. **Teoria elementar dos números**. São Paulo: Nobel, 1981.

ARAÚJO, Emerson Joaquim. **Criptografia: dos rudimentos à atualidade**, 2018. 75f. Dissertação (Mestrado) – Universidade Federal do Estado do Rio de Janeiro, 2018.

BUCHMANN, Johannes A. **Introdução à criptografia**, (tradução). São Paulo: Berkeley Brasil, 2002.

COSTA, Darci Dala. **A Matemática e os Códigos Secretos: Uma Introdução à Criptografia**, 2014. 78f. Dissertação (Mestrado) – Universidade Estadual de Maringá, 2014.

FIARRESGA, Victor Manuel Calhabrês. **Criptografia e Matemática**, 2010. 144f. Dissertação (Mestrado) – Universidade de Lisboa, 2010.

FONSECA, João José Saraiva da. **Metodologia da pesquisa científica**. Fortaleza: UEC, 2002. Apostila.

ORDONEZ, Edward David Moreno; PEREIRA, Fábio Dacêncio; CHIARAMONTE, Rodolfo Barros. **Criptografia em Software e Hardware**. 1. ed. São Paulo: Novatec, 2005.

SAMPAIO, João Carlos Vieira; CAETANO, Paulo Antonio Silvani. **Introdução à teoria dos números: um curso breve**. São Carlos: EdUFSCar, 2009.

SANTOS, José Plínio de Oliveira. **Introdução à teoria dos números**. 3 ed. Rio de Janeiro: IMPA, 2011.

SILVA, Willian Wallace de Matteus. **A evolução da criptografia e suas técnicas ao longo da história**, 2019. 29f. TCC (Graduação) – Instituto Federal Goiano, 2019.

SINGH, Simon. **O Livro dos Códigos**, (tradução). São Paulo: Editora Record, 2004.

SOUSA, Antonio Nilson Laurindo. **Criptografia de Chave Pública, Criptografia RSA**, 2013. 57f. Dissertação (Mestrado) – Universidade Estadual Paulista "Júlio de Mesquita Filho", 2013.