Universidade do Estado do Rio de Janeiro

Centro de Tecnologia e Ciências

Instituto de Matemática e Estatística

Victor Monteiro Ferreira Porto

Criptografia: Da origem aos dias atuais

Rio de Janeiro

2015

Victor Monteiro Ferreira Porto

Criptografia: Da origem aos dias atuais

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, do Instituto de Matemática e Estatística, da Universidade do Estado do Rio de Janeiro.

Orientador: Prof. Dr. Roberto Alfonso Olivares Jara

Rio de Janeiro

2015

CATALOGAÇÃO NA FONTE
UERJ / REDE SIRIUS / BIBLIOTECA CTC-A

P853 Porto, Victor Monteiro Ferreira
Criptografia: Da origem aos dias atuais / Victor Monteiro Ferreira Porto. – 2015.
50 f. : il.

Orientador: Roberto Alfonso Olivares Jara.
Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade do Estado do Rio de Janeiro, Instituto de Matemática e Estatística.

1. Criptografia - História - Teses. 2. Criptografia de dados (Computação) - Teses. I. Jara, Roberto Alfonso Olivares . II. Universidade do Estado do Rio de Janeiro. Instituto de Matemática e Estatística. IV. Título.

CDU 003.26(091)

_____ _____

Assinatura Data

Victor Monteiro Ferreira Porto

Criptografia: Da origem aos dias atuais

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, do Instituto de Matemática e Estatística, da Universidade do Estado do Rio de Janeiro.

Aprovada em 26 de fevereiro de 2015.

Banca Examinadora:

_____

Prof. Dr. Roberto Alfonso Olivares Jara (Orientador)

Instituto de Matemática e Estatística – UERJ

_____

Prof.ª Dra. Patricia Nunes da Silva

Instituto de Matemática e Estatística – UERJ

_____

Prof.ª Dra. Susan Wouters

Universidade Federal Rural do Rio de Janeiro

Rio de Janeiro

2015

DEDICATÓRIA

Dedico este trabalho a minha família que sempre torce por mim e, se mostra presente em toda minha vida me dando força e garra para superar toda e qualquer adversidade.

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus por poder realizar este sonho e por tudo que ele tem feito em minha vida desde o ínicio da minha existência.

Agradeço minha mãe Sandra e meu pai Nelson por serem meus grandes incentivadores em todos os momentos.

Agradeço ao meu orientador Roberto por todo o suporte, empenho e compromisso dados a mim com relação a este trabalho.

Agradeço aos professores do Programa de Mestrado Profissional em Rede Nacional da UERJ por tudo o que compartilharam comigo através de suas aulas.

Agradeço aos meus alunos por seu carinho e atenção me dando apoio para o término desta dissertação.

RESUMO

PORTO, Victor Monteiro Ferreira. *Criptografia: Da origem aos dias atuais*. 2015. 50f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Instituto de Matemática e Estatística, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2015.

Esta pesquisa foi realizada com a intenção de motivar o estudo da criptografia, mostrando que a matemática e a comunicação estão presentes em diversos momentos, tanto no passado quanto no presente. Este trabalho mostra a origem da criptoanálise e toda a sua evolução dando ênfase nos mecanismos de codificação e decodificação através de exemplos práticos. Além disso, alguns métodos criptográficos são destacados como a cifra de substituição monoalfabética, a cifra de Vigenère, a criptografia RSA que é o método mais conhecido de criptografia de chave pública, as cifras de Hill, o método das transformações lineares e o método de Rabin, devido a sua grande importância para a evolução de sistemas computacionais e assinaturas digitais entre outros. Por fim, mostra-se a importância e a necessidade dos recursos criptográficos nos dias de hoje, na tentativa de impedir que hackers e pessoas que fazem mau uso do conhecimento matemático possam causar danos a sociedade, seja por uma simples mensagem ou até mesmo através de situações mais imprudentes como as transações bancárias indevidas.

Palavras-chave: Criptografia. Criptoanálise. Codificação. Decodificação. Cifra de substituição monoalfabética. Cifra de Vigenère. Criptografia RSA. Cifras de Hill. Método das transformações lineares. Método de Rabin.

ABSTRACT

PORTO, Victor Monteiro Ferreira. *Encryption: the origin to the present days.* 2015. 50 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Instituto de Matemática e Estatística, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2015.

This research was conducted with the intention of motivating the study of cryptography, showing that mathematics and the communication are present at various times, both past and present. This work shows the origin of cryptanalysis and all its evolution giving emphasis on coding and decoding mechanisms through practical examples. In addition, some methods cryptographic are highlighted as the monoalphabetic substitution cipher, the Vigenere cipher, RSA encryption that is the best known method of public key cryptography , ciphers Hill, the method of linear transformations and the Rabin method, due to its great importance for the evolution of computer systems and signatures digital among others. Finally, we show the importance and the need for cryptographic resources these days, in an attempt to prevent hackers and people who make bad use of mathematical knowledge can cause damage to society, whether by a simple message or through more situations reckless as improper banking transactions.

Keywords: Cryptography. Cryptanalysis. Coding. Decoding. Monoalphabetic substitution cipher. Vigenere cipher, RSA encryption. Ciphers Hill. Method of linear transformations. Rabin method.

SUMÁRIO

INTRODUÇÃO

Este trabalho pretende apresentar a criptografia e sua história, destacando alguns métodos devido à sua importância nos dias atuais.

A criptografia é a ciência que estuda métodos para codificar uma mensagem de forma que apenas seu destinatário legítimo consiga interpretá-la. Desde os tempos antigos, no decorrer de guerras, códigos decidiram o resultado de batalhas. Conforme a importância da informação, o processo de codificação de mensagens teve um papel fundamental no passado e devido a seu aperfeiçoamento ganhou cada vez mais espaço em nossa sociedade. Tal procedimento é de extrema importância pois o utilizamos atualmente. Nos dias de hoje, é comum utilizar a criptografia em transações bancárias, assinaturas digitais entre outros. Recentemente, um sistema de criptografia empregado no Whatsapp permite total segurança aos usuários, já que apenas os mesmos que trocam conversas, podem ter acesso ao conteúdo. Nesses termos, tampouco a empresa possui acesso a essas mensagens.

Esta obra é voltada para leitores que já possuem uma certa habilidade com a matemática e tenham interesse em conhecer um pouco sobre a criptografia; sua origem, seu desenvolvimento e alguns métodos que obtiveram destaque ao longo dos anos. Para uma maior compreensão é recomendado que o leitor já tenha feito o curso de álgebra 1. Caso contrário, recomenda-se que o leitor faça antes uma leitura prévia do capítulo 3 em Milies e Coelho (2003).

Este trabalho organiza-se em três momentos. No capítulo 1, aborda-se a historicização bem como também as definições ligadas ao tema, sendo explicitadas as formas de metodização iniciais da criptografia. Inclui-se neste último a cifra de substituição monoalfabética, a análise de frequência e a cifra de Vigenère. Vale ressaltar que nos dias de hoje devido aos grandes avanços tecnológicos tais métodos podem ser realizados facilmente com o auxílio de um computador e o software adequado porém, nesse capítulo, vamos ignorar tais recursos para mostrar o funcionamento de tais mecanismos. Já o segundo capítulo retrata a evolução da criptografia incluindo a exposição de quatro métodos: o método de criptografia RSA que é o mais utilizado em aplicações comerciais e na internet, o método das cifras de Hill e das transformações lineares que são baseados em transformações matriciais e o método de Rabin. Por fim, no último capítulo, estaremos retratanto a criptografia na atualidade comentando alguns casos recentes.

1 **HISTÓRIA DA CRIPTOGRAFIA**

Neste capítulo iremos apresentar a criptografia e seu significado, mostrando algumas situações para sua criação (fatos históricos), descrevendo a sua evolução inicial através de exemplos práticos. Porém, para compreendermos melhor o assunto abordado iremos iniciar esse capítulo com o tema comunicação.

1.1 **Comunicação e seus elementos**

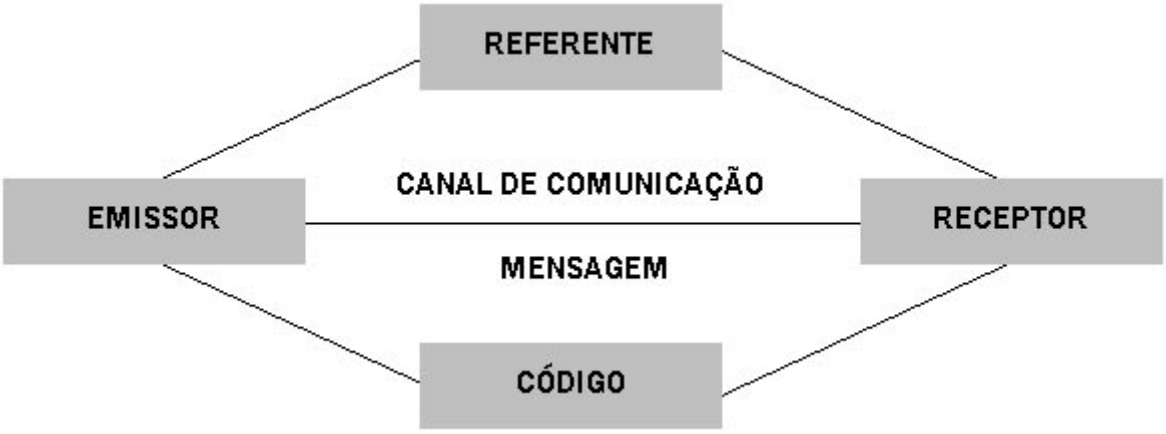
Comunicação é uma palavra derivada do termo latino “communicare”, que significa “partilhar, participar algo, tornar comum”.

Através da comunicação, desde os tempos mais remotos, os seres humanos e animais trocam diferentes informações entre si, o que caracteriza o ato de se comunicar como indispensável e extremamente necessário para o convívio em sociedade.

Na maioria dos casos, a forma de se comunicar consiste em qualquer passagem falada ou escrita que forma um todo significativo, independentemente de sua extensão. Hipoteticamente, por exemplo, um francês resolve viajar de férias para o Brasil. Saindo do aeroporto, esse indivíduo, resolve pegar um taxi e tenta se comunicar com o motorista. Contudo, há um empecilho. Tanto o francês quanto o brasileiro só conhecem apenas o seu idioma de origem. Nessa situação, a comunicação seria frustrada pois, como um não conhece o idioma do outro, não haveria entendimento entre eles.

O processo de comunicação consiste na transmissão de uma informação entre um emissor que codifica a mensagem e um receptor que a descodifica, ou seja, a interpreta. A mensagem é codificada e decodificada num sistema de símbolos ou sinais (código) previamente acordados entre o emissor e o receptor.

Para uma melhor compreensão de tal situação observe o esquema a seguir:



- ✓ Emissor → Indivíduo que emite a mensagem (codifica).
- ✓ Receptor → Indivíduo que recebe a mensagem (decodifica - interpreta).
- ✓ Mensagem → Conjunto de informações transmitidas.
- ✓ Código → Combinação de símbolos ou sinais utilizados na transmissão de uma mensagem. A COMUNICAÇÃO SÓ SE CONCRETIZARÁ, SE O RECEPTOR SOUBER DECODIFICAR A MENSAGEM.
- ✓ Canal de comunicação → Meio por onde a mensagem é transmitida. Esse pode ser via cordas vocais, ar, TV, rádio, jornal, revista e etc.
- ✓ Referente → Situação a que a mensagem se refere, também chamada de contexto.

1.2 **Introdução à criptografia**

Desde os antigos reinados, reis, rainhas, sacerdotes, generais e guerreiros (soldados) procuravam maneiras eficazes de comunicação para comandar suas tropas. A importância de não revelar segredos, táticas e estratégias de guerra aos inimigos motivou o desenvolvimento de códigos e cifras, com o objetivo de que apenas o destinatário pudesse ler o conteúdo. Com isso, as civilizações se organizaram a fim de criar códigos, e em contrapartida, surgiram os decifradores de códigos, criando uma "corrida armamentista intelectual". As diferentes formas e utilidades dadas aos códigos ao longo do tempo mostram uma forte presença da matemática e sua evolução, já que toda informação oculta está sujeita a ser decifrada e quando

isso ocorre, esta deixa de ser útil, sendo necessário a criação de um novo código até que os decifradores identifiquem suas fraquezas, e assim por diante.

No decorrer de guerras, códigos decidiram o resultado de batalhas. Conforme a importância da informação, o processo de codificação de mensagens tem um papel cada vez maior na sociedade.

> "Já se falou que a Primeira Guerra Mundial foi a guerra dos químicos, devido ao emprego, pela primeira vez, do gás mostarda e do cloro, que a Segunda Guerra Mundial foi a guerra dos físicos devido à bomba atômica. De modo semelhante se fala que uma Terceira Guerra Mundial seria a guerra dos matemáticos, pois os matemáticos terão o controle sobre a próxima grande arma de guerra, a informação. Os matemáticos têm sido responsáveis pelo desenvolvimento dos códigos usados atualmente para a proteção das informações militares. E não nos surpreende que os matemáticos também estejam na linha de frente da batalha para tentar decifrar esses códigos."
>
> (SINGH, 2007, p.13)

É comum encontramos na história, situações em que estudiosos desvendaram códigos inimigos, mas mantiveram tal informação em sigilo, a fim de impedir a criação de novos códigos para substituir o descoberto e também, para a obtenção de informações preciosas que pudessem auxiliar nas táticas de batalha.

1.3 **Esteganografia e criptografia**

A palavra esteganografia é de origem grega. "Steganos" significa coberto, e "graphein" significa escrever. Portanto, esteganografia significa uma comunicação secreta, ou seja, a ocultação da mensagem. Um exemplo de esteganografia pode ser encontrado em "As histórias". O autor do livro retrata os conflitos entre Grécia e Pérsia, ocorridos no século V a. C.. Histaeu queria incentivar Aristágora de Mileto a se indispor com o rei persa. Para transmitir seus comandos em segurança, Histaeu raspou a cabeça de um mensageiro, escreveu a mensagem no couro cabeludo e esperou que o cabelo crescesse para enviar a mensagem secretamente. Quando o mensageiro chegou ao seu destino, raspou a cabeça possibilitando a leitura da mensagem. O grande problema para esse meio de comunicação seria o tempo de espera para a mensagem chegar a quem é de direito.

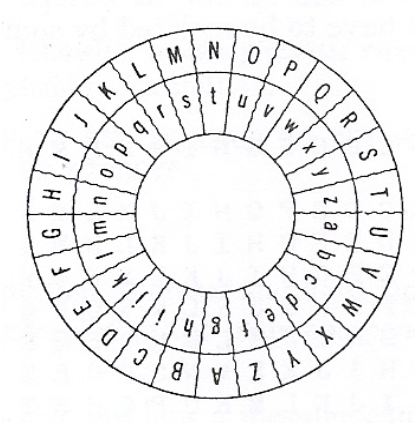
Apesar da prática da esteganografia ter se mantido ao longo dos tempos por oferecer uma certa segurança, tal procedimento possuía uma fraqueza notória. Se por acaso, o mensageiro fosse abordado e revistado por inimigos, o conteúdo da comunicação secreta seria imediatamente revelado o que comprometeria toda a segurança.

Ao mesmo tempo com o desenvolvimento da esteganografia, ocorreu a evolução da criptografia. A palavra criptografia, é de origem grega. “kriptos” significa oculto e “graphein” significa escrever. Diferentemente da esteganografia, a criptografia tem como objetivo ocultar o significado da mensagem e não a mensagem em si. Por exemplo: Suponhamos que desejamos enviar a seguinte mensagem: “Ultimamente o calor no Rio de Janeiro tem sido insuportável.” E para criptografá-la, vamos intercalar as letras da mensagem original com as letras da palavra quente. Desta forma, a mensagem codificada seria: “Quuletnitmeaqmueennttee oq cuaelnotre nqou Reinot deeq Juaennetierqou teenmt seiqduoe inntseuqpuoernttáevqeule.”

A vantagem da criptografia é que se o inimigo interceptar a mensagem codificada, de imediato ela seria ilegível e seu conteúdo não teria exposição. E foi através desses impasses de interceptação de mensagens criptografadas, que se iniciou a criptoanálise, ciência que permite decifrar uma mensagem sem conhecer a chave (forma para decodificação).

1.4 **Cifra de substituição monoalfabética**

Por volta do século X, os árabes utilizaram a criptografia para codificar os segredos de Estado e proteger o registro de impostos. Era utilizado um alfabeto cifrado apenas reorganizando o alfabeto original (ou até mesmo outros símbolos). Essa cifra permaneceu invulnerável por séculos. Era comum deslocar as letras do alfabeto, como por exemplo, a figura a seguir:



Isso significa que ao codificar uma mensagem, a letra A corresponderá à letra g, a letra B corresponderá à letra h, a letra C corresponderá à letra i e assim sucessivamente.

Utilizando esse padrão de ciframento vamos a um exemplo prático. Iremos criptografar a mensagem: “A MINHA COR PREFERIDA É VERDE.”, utilizando a cifra de substituição monoalfabética. Inicialmente devemos escolher o deslocamento criando uma reorganização para o alfabeto. Suponhamos a seguinte:

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

Portanto, para fazer a codificação devemos converter as letras originais para a reorganização cifrada, ou seja, a letra A irá corresponder à letra M, a letra B irá corresponder à letra N, a letra C irá corresponder à letra O e assim por diante. Com isso, temos que nossa mensagem codificada seria:

“A MINHA COR PREFERIDA É VERDE.”

“M YUZTM OAD BDQRQDUPM Q HQDPQ.”

Em seguida, o emissor, envia a mensagem “M YUZTM OAD BDQRQDUPM Q HQDPQ.” para o receptor. E esse, deve decodificá-la para compreender o seu conteúdo.

Para realizar a decodificação o receptor deve escolher uma das palavras cifradas (que contenha ao menos quatro letras para uma boa compreensão) e fazer a correlação adequada para encontrar o deslocamento de cada letra. Após essa escolha coloca-se em colunas o alfabeto reorganizado a partir de cada letra da palavra escolhida. A seguir, deve-se buscar em uma das linhas uma palavra adequada (que faça sentido no idioma em comum para a decodificação) para enfim fazer a correlação de acordo com o deslocamento correto. Por fim, basta traduzir o restante da mensagem.

Voltemos ao exemplo citado. O receptor recebeu a mensagem criptografada:
“M YUZTM OAD BDQRQDUPM Q HQDPQ.” e escolheu ao acaso a cifra HQDPQ.

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

Note que em uma das linhas aparece a palavra verde que seria a única que faz sentido no nosso vocabulário (no caso de encontrar em duas ou mais linhas palavras que façam sentido, o processo deverá ser repetido utilizando outra cifra). Por consequência disso, temos que a letra cifrada H corresponde à letra V da mensagem original, a letra cifrada Q corresponde à letra E da mensagem original, a letra cifrada D corresponde à letra R da mensagem original e a letra cifrada P corresponde à letra D da mensagem original. Tal correspondência deve ser feita para todas as letras do alfabeto. E assim encontramos a seguinte reorganização:

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

Após descobrir o deslocamento correto, basta decodificar a mensagem fazendo o procedimento inverso da codificação e por fim encontrar a mensagem original.

“M YUZTM OAD BDQRQDUPM Q HQDPQ.”

“A MINHA COR PREFERIDA É VERDE.”

1.5 **Análise de frequência**

O auge da análise fe frequência ocorreu no século IX através de pesquisas do cientista Al-Kindi na tentativa de revelar as escritas contidas no Corão. Tal método consiste em analisar a frequência das letras para quebrar códigos. Inicialmente conta-se a frequência de cada letra ou símbolo. Em seguida, examina-se o criptograma que se deseja decifrar relacionando à frequência com que aparece na mensagem. Para isso dar certo deve-se fazer uma correspondência entre as letras e os símbolos mais frequentes.

Analisando, por exemplo, um texto codificado na língua portuguesa, pode-se observar que os símbolos mais frequentes são as vogais. De início a vogal ***a*** e em seguida as vogais ***e*** e ***o***. Como consequência disso ao tentarmos decodificar uma mensagem inicialmente, tentaremos substituir o símbolo mais utilizado pela vogal ***a***. Não sendo possível faremos o mesmo procedimento pela vogal ***e*** e assim sucessivamente até conseguirmos decodificar a mensagem. É claro que para esse processo dar certo faz-se necessário que o decifrador tenha um bom conhecimento da língua em que foi escrita o texto de origem para decifrar com mais facilidade. Como por exemplo, na língua portuguesa, dois símbolos consecutivos iguais só poderiam representar as seguintes situações: cc, oo, rr ou ss.

Como exemplo, vamos decodificar a mensagem criptografada a seguir, utilizando a análise de frequência:

Q weqrtyu rqi yoypiyaq wspy dywsf dqt gquy digdq, hjs s y gquy tykity wyey jt weqleyty as tsfueyaq.

Inicialmente vamos coletar a frequência com que aparece cada letra:

Q = 10	W = 5	E = 5	R = 2	T = 7	Y = 16
U = 4	I = 4	O = 1	P = 2	A= 3	S = 6

D = 4	F = 2	G = 3	H = 1	J = 2	K = 1	L = 1

Observe que a maior frequência é da letra **y**. Logo, possivelmente, esta poderá ser a representação da letra **a**. Vamos observar agora as cifras isoladas. São elas: **Q**, **s** e **y**. Utilizando os conhecimentos da língua portuguesa, sabemos que não podemos ter uma única consoante representando uma palavra portanto, **Q**, **s** e **y** são representações de vogais. E como supomos que a letra **y** representa a vogal **a**, as demais cifras, **Q** e **s**, só podem representa as vogais **e** e **o**, pois sabemos que as vogais i e u separadas não fazem sentido em nossa língua. Na mensagem temos a sequência criptografada **s y**. Com as observações feitas anteriormente,

só poderíamos ter como possibilidades para tal transcrição as vogais **o a** ou **e(é) a**, nessa ordem respectivamente. Novamente utilizando o recurso da língua portuguesa percebemos que **o a** é uma hipótese descartada, o que nos faz deduzir que a letra **s** corresponde a vogal **e** e como consequência disso, a letra **Q** corresponde a vogal **o**.

Façamos agora as substituições das letras cifradas pelas letras deduzidas para termos uma melhor noção da mensagem original. Deixando os demais espaços em lacunas.

O _ _O_ _A_ _O_ A_A_ _A_O _E_A _A_E_ _O_ _O_A _ _ _ _O,
_ _E E A _O_A _A_ _ _A _A_A _ _ _ _O_ _A_A _E _E_ _ _A_O

Na mensagem, há uma cifra (as) de duas letras, onde supostamente a segunda é representada pela vogal **e**. A transcrição dessa passagem só faria sentido se a letra **a** representasse a letra **d** ou a letra **p** e assim teríamos **de** ou **pé**. Num texto, o conectivo de é mais usual que a parte do corpo pé, por esse motivo, vamos supor que a letra **a** seja equivalente a letra **d** na mensagem original.

Na mensagem, há uma cifra (**jt**) de duas letras. Recorrendo novamente à língua portuguesa sabemos que estas duas letras não podem ser formadas por duas consoantes. E não faria muito sentido também, se estas fossem a representação das duas vogais que faltam (**i** e **u**), pois teríamos as possibilidades **iu** (não existe em língua portuguesa) e **ui** (linguagem informal característica de dor, deveria vir normalmente no início ou no fim da frase). Portanto só nos resta a hipótese da cifra **jt** ser composta por uma letra e uma consoante. Partindo dessa premissa as únicas possibilidades que fariam sentido seriam **mi**, **ri**, **si**, **ir**, **tu** ou **um**. Como a expressão **mi** só é utilizada no contexto musical e a expressão **si** além de representar uma nota musical só faria sentido se sua utilização fosse feita em expressões de termino de frases, como para si, sua utilização não é tão usual quanto outra hipótese que veremos logo adiante. Devido a tais fatos vamos de início descartar essas hipóteses. Agora, se por acaso não encontrarmos a solução, voltaremos a considerar tais possibilidades. Utilizando o padrão da norma culta não é comum encontrarmos o pronome pessoal **tu** (normalmente usa-se o pronome você, isso se deve ao fato de ser mais coloquial tal utilização na linguagem escrista além do fato da regionalidade, ou seja, por estarmos no Rio de Janeiro é comum supormos que a mensagem seja realizada entre dois cariocas portanto, o uso do tu não é tão empregado quanto o do pronome você) no meio de um texto. Nos resta apenas as possibilidades **ir** ou **um**. Então, voltemos as suposições, como em língua portuguesa num texto, é muito

mais usual encontramos um artigo do que um verbo, suponhamos que a cifra **jt** seja equivalente a **um**.

Substituindo as novas suposições temos que:

O _ _O_ MA_ _O_ A_A_ _ADO _E_A _A_E_ _OM _O_A _ _ _ _O, _ UE E A _O_A MA_ _MA _A_A UM _ _O_ _AMA DE ME_ _ _ADO

Analogamente, temos que as cifras **dqt** e **hjs** representam **com** e **que** respectivamente. E com isso, obtemos:

O _ _O_ MA_ _O_ A_A_ _ADO _E_A CA_E_ COM _O_A C_ _ CO, QUE E A _O_A MA_ _MA _A_A UM _ _O_ _AMA DE ME_ _ _ADO

A cifra **digdq** apresenta pelo menos duas sílabas e de acordo com a gramática cada sílaba deve conter uma vogal. Na transcrição para a mensagem original já temos a vogal **o** da última sílaba e a primeira sílaba apresenta a carência de vogal. Como a única vogal que falta ser utilizada é a **i**, temos que **i** ou **g** representa **i**. Analisando as possibilidades chegamos à conclusão que **digdq** representa a palavra cinco. Daí segue que:

O _ _O_ MA_ _OI A_A_ IADO _E_A CA_E_ COM NO_A CINCO, QUE E A NO_A MA_ IMA _A_A UM _ _O_ _AMA DE ME_ _ _ADO

Analogamente as cifras **gquy** e **tykity** correspondem as palavras **nota** e **máxima**. Daí temos que:

O _ _O_ MAT _OI A_A_ IADO _E_A CA_E_ COM NOTA CINCO, QUE E A NOTA MÁXIMA _A_A UM _ _O_ _AMA DE ME_T_ADO

Nesse momento percebe-se que a segunda palavra termina com a consoante **t**, algo que seria absurdo supor em alguma palavra da língua portuguesa. Porém, tal fato não deve ser descartado de imediato pois existem palavras estrangeiras no nosso uso diário como hot dog ou até mesmo siglas. Portanto, ao evoluir no processo das subistituições se não encontrarmos

uma mensagem significativa devemos retornar a alguma etapa anterior e refazer as suposições.

Observe que conforme trocamos as letras cifradas pelas letras da mensagem original fica mais fácil de realizar a decodificação. E utilizando mais alguns argumentos análogos chegamos à mensagem inicial.

O PROFMAT FOI AVALIADO PELA CAPES COM NOTA CINCO, QUE É A NOTA MÁXIMA PARA UM PROGRAMA DE MESTRADO

É fácil perceber que este método não é prático para a decodificação de uma mensagem. Tal fato é devido a uma grande quantidade de suposições que precisam ser feitas e averiguadas para termos ou não de imediato a mensagem almejada.

1.6 **Cifra de Vigenère**

Iniciada no século XV pelo italiano Leon Battista Alberti, tal cifra tinha o objetivo de tentar confundir os criptoanalistas, já que todas as cifras da época exigiam um único alfabeto cifrado. Alberti propôs o uso de pelo menos dois alfabetos cifrados usados alternadamente. Apesar de ter avançado com tal ideia, Alberti não conseguiu desenvolvê-la. Esta tarefa ficou a cargo de um grupo de intelectuais que aperfeiçoaram a ideia original (o alemão Johannes Trithemius, o italianao Giovanni Porta e por fim o francês Blaise de Vigenère). Vigenère utilizou as ideias de Alberti, Trithemius e Porta, mesclando-as para formar uma nova cifra.

A cifra de Vigenère consiste em até 26 alfabetos distintos para criar a mensagem cifrada. A vantagem da cifra de Vigenère é que ela é imune à análise de frequência. Além disso, a cifra tem um número enorme de chaves (26^{26} possibilidades).

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

Observe que a cifra de Vigenère utiliza uma tabela que pode ser representada por uma matriz de ordem 26. Além da tabela, para dificultar o deciframento da mensagem criptografada, Vigenère também utiliza uma “palavra chave” tanto na codificação quanto na decodificação que deve ser combinada entre o emissor e o receptor da mensagem.

Para realizar a codificação da mensagem repete-se a “palavra chave” sobre as letras da mensagem a ser codificada, tantas vezes, quantas for necessário. Em seguida basta criptografar cada letra fazendo uma correspondência matricial entre a intersecção da linha e da coluna, onde a linha corresponde a letra da palavra chave e a coluna a letra da mensagem conforme a tabela da página anterior. Para compreendermos melhor tal processo faremos um exemplo prático. Vamos criptografar a seguinte frase: “Euclides é o pai da geometria” e no combinado, tanto para quem codifica a mensagem quanto para quem decodifica, a palavra chave será “UERJ”.

Tomemos a tabela a seguir para melhor compreensão sobrepondo letra a letra da “palavra chave” à mensagem (texto):

Chave	U	E	R	J	U	E	R	J	U	E	R	J	U	E	R	J	U	E	R	J	U	E	R	J
Texto	E	U	C	L	I	D	E	S	É	O	P	A	I	D	A	G	E	O	M	E	T	R	I	A
Cifra																								

A letra da chave indica a linha que deve ser utilizada enquanto a letra da mensagem indica a coluna para a codificação. Na primeira letra da chave e da mensagem deve-se utilizar a linha U e a coluna E, em seguida observa-se a intersecção entre essas duas letras. Tal encontro, equivale a letra criptografada, nesse caso a letra Z. Na segunda letra da chave e da mensagem deve-se utilizar a linha E e a coluna U. Dessa intersecção obtemos a cifra Z. Tal procedimento deve ser realizado até cifrar toda a mensagem. Portanto temos que:

Chave	U	E	R	J	U	E	R	J	U	E	R	J	U	E	R	J	U	E	R	J	U	E	R	J
Texto	E	U	C	L	I	D	E	S	É	O	P	A	I	D	A	G	E	O	M	E	T	R	I	A
Cifra	Z	Z	U	V	D	I	W	C	Z	T	H	K	D	I	S	Q	Z	T	E	O	O	W	A	K

Logo, a mensagem codificada é “Zzuvdiwc z t hkd is qzteoowak”.

Para a realização da decodificação o processo é inverso. A chave indica a linha, a cifra indica o elemento da linha então, basta encontrar a letra correspondente a este elemento, que é exatamente a coluna que corresponde a letra da mensagem.

Voltemos ao exemplo anterior. A frase criptografada é “Zzuvdiwc z t hkd is qzteoowak” e a palavra chave é UERJ. Façamos novamente uma tabela para nos auxiliar:

Chave	U	E	R	J	U	E	R	J	U	E	R	J	U	E	R	J	U	E	R	J	U	E	R	J
Cifra	Z	Z	U	V	D	I	W	C	Z	T	H	K	D	I	S	Q	Z	T	E	O	O	W	A	K
Texto																								

Na primeira letra da chave e da cifra deve-se utilizar a linha U e o elemento Z. Esse elemento pertence a coluna E. Na segunda letra da chave e da cifra deve-se utilizar a linha E e o elemento Z. Esse elemento pertence à coluna U. Na terceira letra da chave e da cifra deve-se utilizar a linha R e o elemento U. Esse elemento pertence à coluna C. Tal procedimento deve ser realizado até decodificar toda a mensagem. Portanto temos que:

Chave	U	E	R	J	U	E	R	J	U	E	R	J	U	E	R	J	U	E	R	J	U	E	R	J
Cifra	Z	Z	U	V	D	I	W	C	Z	T	H	K	D	I	S	Q	Z	T	E	O	O	W	A	K
Texto	E	U	C	L	I	D	E	S	É	O	P	A	I	D	A	G	E	O	M	E	T	R	I	A

Logo, a mensagem original é “Euclides é o pai da geometria”.

Vale ressaltar que dependendo da chave escolhida a cifra de Vigenère acaba retornando a cifra de substituição monoalfabética. Se a chave for composta por apenas uma única letra estaremos nos remetendo a apenas um alfabeto para a criptografia. O leitor pode observar isso repetindo o exemplo anterior utilizando como chave a letra g.

2 EVOLUÇÃO DA CRIPTOGRAFIA

Com os avanços e as descobertas matemáticas, a criptografia não se manteve estagnada. Ela evoluiu com o propósito de dificultar a decodificação de suas cifras. Neste capítulo, serão apresentados quatro métodos criptográficos que surgiram com o passar dos tempos, apresentando seus mecanismos de codificação e decodificação. São eles: Criptografia RSA, cifras de Hill, método das transformações lineares e o método de Rabin.

2.1 Criptografia RSA

O método de criptografia RSA é o mais utilizado em aplicações comerciais e na internet. Permite a identificação de documentos, criptografar dados, criar e verificar assinaturas digitais. Foi criado em 1978 por R. L. Rivest, A. Shamir e L. Adleman, que na época trabalhavam no Massachussets Institute of Technology (M.I.T.). A sigla RSA corresponde as iniciais dos criadores do código. Tal método é baseado no problema do logaritmo discreto.

Para facilitar a compreensão de tal método vamos descrevê-lo por etapas.

1ª Etapa → São escolhidos dois números primos (p e q). Para uma maior segurança, os números utilizados devem ser bem grandes (geralmente maiores que 10^{100} e não muito próximos um do outro). Porém, para facilitar o acompanhamento do processo, usaremos um exemplo com números pequenos. Ou seja, suponhamos $p = 11$ e $q = 19$.

2ª Etapa → Calcula-se a chave pública (chave de segurança que pode se tornar pública sem pôr a segurança da cifra em risco). Escolhido os números primos p e q, a chave pública será o número $N = pq$. Em seguida, calcula-se $\Phi(N)$, onde Φ é a função de Euler definida por $\Phi(N) = \Phi(p)\Phi(q) = (p - 1)(q - 1)$. No exemplo citado, temos que $N = 11 \cdot 19 = 209$ e $\Phi(N) = (11 - 1)(19 - 1) = 10 \cdot 18 = 180$.

Após obtermos o valor de $\Phi(N)$ devemos encontrar um número E qualquer que seja relativamente primo a ΦN, ou seja, mdc $(E, \Phi(N)) = 1$. Para isso vamos utilizar o processo da fatoração para $\Phi(N)$.

180	2
90	2
45	5
9	3
3	3
1	

Como $180 = 2^2 . 3^2 . 5$, para que E e 180 sejam primos entre si, o valor de E não pode ser divisível por 2, nem por 3 e nem por 5. Então, digamos que o número escolhido para E seja 7. A chave pública é dada por (E, N). Portanto em nosso exemplo, a chave pública é (7, 209).

3ª Etapa → Calcula-se a chave privada (chave de segurança que deve ser mantida em sigilo para não comprometer o segredo da mensagem criptografada). Para calcular a chave privada precisamos encontrar um valor D tal que $D . E \equiv 1 \pmod{\Phi(N)}$, em outras palavras, precisamos encontrar o inverso multiplicativo de E no anel $Z_{\Phi(N)}$ (dos números inteiros módulo $\Phi(N)$), que existe pois $(E, \Phi(N)) = 1$.

Como $D . E \equiv 1 \pmod{\Phi N}$ temos que $D . 7 \equiv 1 \pmod{180}$. Para encontrarmos o valor de D utilizaremos o algoritmo de Euclides estendido.

$180 = 25 . 7 + 5$	$180 – 25 . 7 = 5$ (I)
$7 = 1 . 5 + 2$ (II)	Substituindo (I) em (II) temos que :
	$7 = 1 . (180 – 25. 7) + 2$
	$7 = 180 – 25 . 7 + 2$
	$7 – 180 + 25 . 7 = 2$
	$26 . 7 – 180 = 2$
$5 = 2 . 2 + 1$	Substituindo (I) em (II) temos que :
	$7 = 1 . (180 – 25. 7) + 2$
	$7 = 180 – 25 . 7 + 2$
	$7 – 180 + 25 . 7 = 2$
	$26 . 7 – 180 = 2$

Portanto, temos que o inverso multiplicativo de 7 no anel Z_{180} é – 77. Daí segue que $– 77 . 7 \equiv 1 \pmod{180}$, mas como $– 77 \equiv 103 \pmod{180}$, o valor para D é 103.

A chave privada é dada por (D, N). Portanto em nosso exemplo, a chave privada é (103, 209).

4ª Etapa → Criptografa-se a mensagem. Para se começar a cifrar uma mensagem pelo sistema RSA é preciso transformar a mensagem em um número, e isso é feito através do padrão ASCII conforme parte da tabela a seguir:

Caracteres ASCII imprimibles

DEC	HEX	Simbolo	DEC	HEX	Simbolo	DEC	HEX	Simbolo
32	20h	espacio	64	40h	@	96	60h	`
33	21h	!	65	41h	A	97	61h	a
34	22h	"	66	42h	B	98	62h	b
35	23h	#	67	43h	C	99	63h	c
36	24h	$	68	44h	D	100	64h	d
37	25h	%	69	45h	E	101	65h	e
38	26h	&	70	46h	F	102	66h	f
39	27h	'	71	47h	G	103	67h	g
40	28h	(	72	48h	H	104	68h	h
41	29h	)	73	49h	I	105	69h	i
42	2Ah	*	74	4Ah	J	106	6Ah	j
43	2Bh	+	75	4Bh	K	107	6Bh	k
44	2Ch	,	76	4Ch	L	108	6Ch	l
45	2Dh	-	77	4Dh	M	109	6Dh	m
46	2Eh	.	78	4Eh	N	110	6Eh	n
47	2Fh	/	79	4Fh	O	111	6Fh	o
48	30h	0	80	50h	P	112	70h	p
49	31h	1	81	51h	Q	113	71h	q
50	32h	2	82	52h	R	114	72h	r
51	33h	3	83	53h	S	115	73h	s
52	34h	4	84	54h	T	116	74h	t
53	35h	5	85	55h	U	117	75h	u
54	36h	6	86	56h	V	118	76h	v
55	37h	7	87	57h	W	119	77h	w
56	38h	8	88	58h	X	120	78h	x
57	39h	9	89	59h	Y	121	79h	y
58	3Ah	:	90	5Ah	Z	122	7Ah	z
59	3Bh	;	91	5Bh	[	123	7Bh	{
60	3Ch	<	92	5Ch	\	124	7Ch	|
61	3Dh	=	93	5Dh	]	125	7Dh	}
62	3Eh	>	94	5Eh	^	126	7Eh	~
63	3Fh	?	95	5Fh	_	elCodigoASCII.com.ar		

Por exemplo, a mensagem “teorema de fermat.”, convertida em código ASCII, sem os espaços, ficaria:

116101111114101109971001011021011141099711646

Em seguida, deve-se quebrar a mensagem em blocos relativamente pequenos, de modo que cada mensagem, M, fique no intervalo $0 \leq M \leq N$. De preferência essa quebra deve ser feita em bloco de forma que todos fiquem completos, ou seja, o número de dígitos deve ser

divisível pelo número de elementos do bloco. No presente exemplo, um bom tamanho serão blocos de três dígitos. Assim:

$$M_1 = 116 \quad M_2 = 101 \quad M_3 = 111 \quad M_4 = 114 \quad M_5 = 101$$
$$M_6 = 109 \quad M_7 = 971 \quad M_8 = 001 \quad M_9 = 011 \quad M_{10} = 021$$
$$M_{11} = 011 \quad M_{12} = 141 \quad M_{13} = 099 \quad M_{14} = 711 \quad M_{15} = 646$$

Para criptografar a mensagem, basta submeter cada um dos blocos à seguinte cifragem $C = M^E \pmod N$.

$$C_1 = 116^7 \pmod{209} = 52$$
$$C_2 = 101^7 \pmod{209} = 161$$
$$C_3 = 111^7 \pmod{209} = 188$$
$$C_4 = 114^7 \pmod{209} = 38$$
$$C_5 = 101^7 \pmod{209} = 161$$
$$C_6 = 109^7 \pmod{209} = 98$$
$$C_7 = 971^7 \pmod{209} = 185$$
$$C_8 = 001^7 \pmod{209} = 1$$
$$C_9 = 011^7 \pmod{209} = 11$$
$$C_{10} = 021^7 \pmod{209} = 109$$
$$C_{11} = 011^7 \pmod{209} = 11$$
$$C_{12} = 141^7 \pmod{209} = 103$$
$$C_{13} = 099^7 \pmod{209} = 44$$
$$C_{14} = 711^7 \pmod{209} = 160$$
$$C_{15} = 646^7 \pmod{209} = 57$$

Após os cálculos, basta juntar os resultados obtidos na ordem e assim obtermos a mensagem criptografada que no exemplo acima é:

52 161 188 38 161 98 185 1 11 109 11 103 44 160 57

5ª Etapa → Descriptografa-se a mensagem. Para decifrar a mensagem basta submeter cada um dos blocos criptografados (C_1, C_2, ..., C_{15}) à seguinte cifragem $M = C^D \pmod N$.

Voltando ao exemplo proposto. Se o receptor recebeu como mensagem 52 161 188 38 161 98 185 1 11 109 11 103 44 160 57 basta submeter cada bloco a cifragem de decodificação $M = C^D \pmod N$.

$$M_1 = 52^{103} \pmod{209} = 116$$

$$M_2 = 161^{103} \pmod{209} = 101$$

$$M_3 = 188^{103} \pmod{209} = 111$$

$$M_4 = 38^{103} \pmod{209} = 114$$

$$M_5 = 161^{103} \pmod{209} = 101$$

$$M_6 = 98^{103} \pmod{209} = 109$$

$$M_7 = 185^{103} \pmod{209} = 971$$

$$M_8 = 1^{103} \pmod{209} = 1$$

$$M_9 = 11^{103} \pmod{209} = 011$$

$$M_{10} = 109^{103} \pmod{209} = 021$$

$$M_{11} = 11^{103} \pmod{209} = 011$$

$$M_{12} = 103^{103} \pmod{209} = 141$$

$$M_{13} = 44^{103} \pmod{209} = 99$$

$$M_{14} = 160^{103} \pmod{209} = 711$$

$$M_{15} = 57^{103} \pmod{209} = 646$$

Após os cálculos pode-se concluir que a mensagem descriptografada é:

116101111114101109971001011021011141099711646

E retomando a tabela através do padrão ASCII temos que a mensagem inicial foi teorema de Fermat.

Para maiores esclarecimentos, as justificativas do funcionamento desse método podem ser encontradas em Coutinho (2009).

2.2 **Cifras de Hill**

O método criptográfico das cifras de Hill foi criado em 1929 por Lester S. Hill. Tal método é um sistema de criptografia no qual o texto comum é dividido em conjuntos de n letras, cada um dos quais é substituído por um conjunto de n letras cifradas, além de ser baseado em transformações matriciais. Nesse momento não iremos nos aprofundar em tal método, apenas o descreveremos dando um exemplo simbólico. O leitor interessado em maiores esclarecimentos sobre esse método pode consultar o trabalho de Clarrisa Duarte Loureiro de Melo (2014).

Para iniciar, precisamos que cada letra da mensagem a ser transmitida e da mensagem cifrada, excetuando a letra Z, tenha um valor numérico que especifique sua posição no alfabeto padrão. À letra Z será atribuído o valor 0, pois assim estaremos trabalhando com a aritmética módulo 26, conforme tabela abaixo:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**...**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**...**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**0**

Para transformar uma mensagem em cifra devemos seguir os seguintes procedimentos:

Inicialmente, para efetuar a codificação, deve-se escolher uma matriz A de ordem nxn com entradas inteiras tal que seu determinante seja relativamente primo com 26. Isto para garantir que A seja invertível módulo 26.

Para facilitar os cálculos vamos utilizar uma matriz A de ordem 2x2.

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

Em seguida deve-se agrupar as letras sucessivas da mensagem em pares (devido a matriz A ser de ordem 2, caso fosse de ordem 3 seriam trincas e assim sucessivamente). Caso o último par não fique completo, devemos acrescentar uma letra fictícia para completá-lo. Após tal procedimento, substituiremos cada letra da mensagem por seu valor numérico correspondente convertendo cada par sucessivo $p_1\ p_2$ de letras da mensagem em um vetor coluna $\vec{p} = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$. Para finalizar o processo de codificação calcula-se o produto $A\vec{p}$. Esse resultado corresponde ao vetor cifrado que deve ser convertido ao seu equivalente alfabético.

Faremos agora um exemplo simples. Vamos criptografar a palavra PITÁGORAS utilizando o processo das cifras de Hill. Primeiro vamos escolher arbitrariamente uma matriz A de ordem 2x2 com entradas inteiras e (det (A), 26) = 1. Seja A = $\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$. Em seguida, agrupa-se a mensagem em pares de letras. No exemplo descrito temos:

PI TA GO RA S

Como o último par não está completo vamos usar uma letra fictícia para completá-lo. Por exemplo a última letra da mensagem (s). Daí temos:

PI TA GO RA SS

Após tal procedimento substituiremos cada letra da mensagem pelo seu valor numérico correspondente.

PI	TA	GO	RA	SS
16 9	20 1	7 15	18 1	19 19

Em seguida, calcula-se o produto A $\vec{p}$:

Para codificar o par PI efetua-se o produto matricial $\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 16 \\ 9 \end{bmatrix} = \begin{bmatrix} 34 \\ 27 \end{bmatrix}$.

Para codificar o par TA efetua-se o produto matricial $\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 20 \\ 1 \end{bmatrix} = \begin{bmatrix} 22 \\ 3 \end{bmatrix}$.

Para codificar o par GO efetua-se o produto matricial $\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 7 \\ 15 \end{bmatrix} = \begin{bmatrix} 37 \\ 45 \end{bmatrix}$.

Para codificar o par RA efetua-se o produto matricial $\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 18 \\ 1 \end{bmatrix} = \begin{bmatrix} 20 \\ 3 \end{bmatrix}$.

Para codificar o par SS efetua-se o produto matricial $\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 19 \\ 19 \end{bmatrix} = \begin{bmatrix} 57 \\ 57 \end{bmatrix}$.

Nesse momento surge um problema, pois alguns números (34, 27, 37, 45 e 57) não possuem equivalências alfabéticas conforme a tabela utilizada anteriormente. Para resolver este problema utilizaremos a aritmética modular, ou seja, utilizaremos o resto da divisão destes números por 26 para obtermos um inteiro com o equivalente alfabético.

Assim, devemos substituir 34 por 8, 27 por 1, 37 por 11, 45 por 19 e 57 por 5 para obtermos a seguinte cifra:

8 1	22 3	11 19	20 3	5 5
H A	V C	K S	T C	E E

Portanto, a mensagem transmitida seria HAVCKSTCEE.

Para decodificação da cifra de Hill, devemos usar a inversa da matriz codificadora reduzida módulo 26. Nesse método é importante saber quais matrizes são invertíveis na congruência módulo 26. Em geral, uma matriz quadrada A admite inversa se, e só se, det (A) $\neq$ 0. Na aritmética módulo 26, o det (A) deverá ter inverso multiplicativo módulo 26, pois na fórmula da inversa de A aparece o inverso do determinante. Portanto, um número n terá inverso módulo 26 se e somente se mdc (n,26) = 1. Assim, só existirá inversa módulo 26 se o det (A) não for divisível por 2 ou 13.

Sendo assim, dada a matriz A = $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, pode-se obter a inversa de A (mod 26) com det (A) = $ad - bc$ (não divisível por 2 ou 13) , pela expressão $A^{-1} = (ad-bc)^{-1}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ (mod 26) onde $(ad-bc)^{-1}$ é o inverso multiplicativo de det (A).

Para facilitar, a seguir, segue a tabela dos inversos multiplicativos módulo 26.

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

Vamos agora tentar decodificar a mensagem HAVCKSTCEE. Como a mensagem foi codificada pela matriz A = $\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$, primeiramente vamos obter a inversa de A (mod 26). Como det (A) = 3, temos que 9 é seu inverso multiplicativo na congruência módulo 26. Sendo assim, devemos aplicar a relação $A^{-1} = (ad-bc)^{-1}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ (mod 26). Daí segue que:

$$A^{-1} = 9\begin{bmatrix} 3 & -2 \\ -0 & 1 \end{bmatrix} \text{(mod 26)}$$

$$A^{-1} = \begin{bmatrix} 27 & -18 \\ 0 & 9 \end{bmatrix} \text{(mod 26)}$$

$$A^{-1} = \begin{bmatrix} 1 & -18 \\ 0 & 9 \end{bmatrix} (\text{mod } 26)$$

Agora, vamos obter o equivalente numérico do texto cifrado em pares (vetores).

HA	VC	KS	TC	EE
8 1	22 3	11 19	20 3	5 5

Para obter a mensagem original, basta multiplicar a inversa de A por cada vetor acima.

Decodificando HA $\rightarrow \begin{bmatrix} 1 & -18 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 8 \\ 1 \end{bmatrix} = \begin{bmatrix} -10 \\ 9 \end{bmatrix}$.

Decodificando VC $\rightarrow \begin{bmatrix} 1 & -18 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 22 \\ 3 \end{bmatrix} = \begin{bmatrix} -32 \\ 27 \end{bmatrix}$.

Decodificando KS $\rightarrow \begin{bmatrix} 1 & -18 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 11 \\ 19 \end{bmatrix} = \begin{bmatrix} -331 \\ 171 \end{bmatrix}$.

Decodificando TC $\rightarrow \begin{bmatrix} 1 & -18 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 20 \\ 3 \end{bmatrix} = \begin{bmatrix} -34 \\ 27 \end{bmatrix}$.

Decodificando EE $\rightarrow \begin{bmatrix} 1 & -18 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 5 \\ 5 \end{bmatrix} = \begin{bmatrix} -85 \\ 45 \end{bmatrix}$.

Nesse momento surge novamente o mesmo problema, pois alguns número (– 10, – 32, 27, – 331, 171, – 34, 85 e 45) não possuem equivalências alfabéticas conforme a tabela utilizada anteriormente na codificação. Para resolver este problema voltaremos a utilizar a aritmética modular, ou seja, utilizaremos o resto da divisão destes números por 26 para obtermos um inteiro com o equivalente alfabético.

Assim, devemos substituir – 10 por 16, – 32 por 20, 27 por 1, – 331 por 7, 171 por 15, – 34 por 18, – 85 por 19 e 45 por 19 para obtermos a seguinte mensagem:

16 9	20 1	7 15	18 1	19 19
P I	T A	G O	R A	S S

Por fim, chegamos a conclusão que a mensagem original era PITAGORAS (Eliminamos a última letra pois não fazia sentido no contexto da palavra, ou seja, ela foi utilizada apenas para completar o último par).

2.3 **Método das transformações lineares**

O método criptográfico das transformações lineares é baseado nas cifras de Hill utilizando matrizes e suas respectivas inversas como chaves para o procedimento de codificação e decodificação de mensagens. Contudo, tal método é aplicado de uma forma mais simples que o processo utilizado nas cifras de Hill, pois ao invés de transmitir a mensagem codificada em letras, essa, é realizada através de números que correspondem as letras do alfabeto transformadas.

Para compreendermos a aplicação desse método, primeiro devemos associar um número a cada letra do alfabeto. Para isso vamos utilizar a tabela a seguir:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**...**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**...**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**

Em seguida, devem-se substituir as letras pelos números correspondentes para formar o código. Por exemplo, vamos gerar o código da frase “O Rio de Janeiro continua lindo.” da música Aquele abraço de Gilberto Gil. Portanto, temos que:

O	R I O	D E	J A N E I R O	C O N T I N U A	L I N D O.
15	18 9 15	4 5	10 1 14 5 9 18 15	3 15 14 20 9 14 21 1	12 9 14 4 15

Como o método da substituição de letras por números pode ser quebrado facilmente, para dificultar o deciframento do código, neste método devemos utilizar como chave para codificação uma matriz que admita inversa, ou seja, que possua determinante não nulo.

Para codificação, devemos obter os valores dos vetores transformados de acordo com a transformação linear $L: R^n \to R^n$ (tal transformação deve ser previamente combinada), associada à matriz quadrada A de ordem n, ou seja, $L_A\left(\vec{x}\right) = A\vec{x}$. Dessa forma, considera-se como chave para codificação a matriz original A. Em seguida, deve-se agrupar os números associados a mensagem original em vetores de R^n. Vale ressaltar que, se o número de letras não for múltiplo de n, o último vetor ficará incompleto. Portanto, deve-se repetir o último número associado a última letra até completá-lo. E, para finalizar o processo de codificação deve-se utilizar a relação $L_A\left(\vec{x}\right) = A\vec{x}$.

Suponhamos que o acordo prévio da transformação linear seja $L: R^3 \to R^3$ e que a chave seja a matriz $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}$. Para realizar a codificação da mensagem devemos agrupar os números da mensagem original em vetores de R^3, da seguinte forma:

$$\vec{v_1} = \begin{bmatrix} 15 \\ 18 \\ 9 \end{bmatrix}, \quad \vec{v_2} = \begin{bmatrix} 15 \\ 4 \\ 5 \end{bmatrix}, \quad \vec{v_3} = \begin{bmatrix} 10 \\ 1 \\ 14 \end{bmatrix}, \quad \vec{v_4} = \begin{bmatrix} 5 \\ 9 \\ 18 \end{bmatrix}, \quad \vec{v_5} = \begin{bmatrix} 15 \\ 3 \\ 15 \end{bmatrix},$$

$$\vec{v_6} = \begin{bmatrix} 14 \\ 20 \\ 9 \end{bmatrix}, \quad \vec{v_7} = \begin{bmatrix} 14 \\ 21 \\ 1 \end{bmatrix}, \quad \vec{v_8} = \begin{bmatrix} 12 \\ 9 \\ 14 \end{bmatrix} \quad \text{e} \quad \vec{v_9} = \begin{bmatrix} 4 \\ 15 \\ 15 \end{bmatrix}$$

Lembrando que a mensagem tem 26 letras, e como 26 não é múltiplo de três, precisamos completar o último vetor repetindo o último número associado a última letra (no caso acima completamos o vetor $\vec{v_9}$ com o número 15).

Para finalizar, basta utilizarmos a relação $L_A(\vec{x}) = A\vec{x}$ para codificar cada um dos vetores.

Codificando $\vec{v_1} = \begin{bmatrix} 15 \\ 18 \\ 9 \end{bmatrix}$: $L_A(\vec{v_1}) = A\vec{v_1} \Rightarrow L_A\left(\begin{bmatrix} 15 \\ 18 \\ 9 \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}\begin{bmatrix} 15 \\ 18 \\ 9 \end{bmatrix} \Rightarrow L_A(\vec{v_1}) = \begin{bmatrix} 42 \\ 51 \\ 27 \end{bmatrix}$

Codificando $\vec{v_2} = \begin{bmatrix} 15 \\ 4 \\ 5 \end{bmatrix}$: $L_A(\vec{v_2}) = A\vec{v_2} \Rightarrow L_A\left(\begin{bmatrix} 15 \\ 4 \\ 5 \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}\begin{bmatrix} 15 \\ 4 \\ 5 \end{bmatrix} \Rightarrow L_A(\vec{v_2}) = \begin{bmatrix} 24 \\ 29 \\ 9 \end{bmatrix}$

Codificando $\vec{v_3} = \begin{bmatrix} 10 \\ 1 \\ 14 \end{bmatrix}$: $L_A(\vec{v_3}) = A\vec{v_3} \Rightarrow L_A\left(\begin{bmatrix} 10 \\ 1 \\ 14 \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}\begin{bmatrix} 10 \\ 1 \\ 14 \end{bmatrix} \Rightarrow L_A(\vec{v_3}) = \begin{bmatrix} 25 \\ 39 \\ 15 \end{bmatrix}$

Codificando $\vec{v_4} = \begin{bmatrix} 5 \\ 9 \\ 18 \end{bmatrix}$: $L_A(\vec{v_4}) = A\vec{v_4} \Rightarrow L_A\left(\begin{bmatrix} 5 \\ 9 \\ 18 \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}\begin{bmatrix} 5 \\ 9 \\ 18 \end{bmatrix} \Rightarrow L_A(\vec{v_4}) = \begin{bmatrix} 32 \\ 50 \\ 27 \end{bmatrix}$

Codificando $\vec{v_5} = \begin{bmatrix} 15 \\ 3 \\ 15 \end{bmatrix}$: $L_A(\vec{v_5}) = A\vec{v_5} \Rightarrow L_A\left(\begin{bmatrix} 15 \\ 3 \\ 15 \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}\begin{bmatrix} 15 \\ 3 \\ 15 \end{bmatrix} \Rightarrow L_A(\vec{v_5}) = \begin{bmatrix} 33 \\ 48 \\ 18 \end{bmatrix}$

$$\text{Codificando } \overrightarrow{v_6} = \begin{bmatrix} 14 \\ 20 \\ 9 \end{bmatrix} : L_A\left(\overrightarrow{v_6}\right) = A\overrightarrow{v_6} \Rightarrow L_A\left(\begin{bmatrix} 14 \\ 20 \\ 9 \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}\begin{bmatrix} 14 \\ 20 \\ 9 \end{bmatrix} \Rightarrow L_A\left(\overrightarrow{v_6}\right) = \begin{bmatrix} 43 \\ 52 \\ 29 \end{bmatrix}$$

$$\text{Codificando } \overrightarrow{v_7} = \begin{bmatrix} 14 \\ 21 \\ 1 \end{bmatrix} : L_A\left(\overrightarrow{v_7}\right) = A\overrightarrow{v_7} \Rightarrow L_A\left(\begin{bmatrix} 14 \\ 21 \\ 1 \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}\begin{bmatrix} 14 \\ 21 \\ 1 \end{bmatrix} \Rightarrow L_A\left(\overrightarrow{v_7}\right) = \begin{bmatrix} 36 \\ 37 \\ 22 \end{bmatrix}$$

$$\text{Codificando } \overrightarrow{v_8} = \begin{bmatrix} 12 \\ 9 \\ 14 \end{bmatrix} : L_A\left(\overrightarrow{v_8}\right) = A\overrightarrow{v_8} \Rightarrow L_A\left(\begin{bmatrix} 12 \\ 9 \\ 14 \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}\begin{bmatrix} 12 \\ 9 \\ 14 \end{bmatrix} \Rightarrow L_A\left(\overrightarrow{v_8}\right) = \begin{bmatrix} 35 \\ 49 \\ 23 \end{bmatrix}$$

$$\text{Codificando } \overrightarrow{v_9} = \begin{bmatrix} 4 \\ 15 \\ 15 \end{bmatrix} : L_A\left(\overrightarrow{v_9}\right) = A\overrightarrow{v_9} \Rightarrow L_A\left(\begin{bmatrix} 4 \\ 15 \\ 15 \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}\begin{bmatrix} 4 \\ 15 \\ 15 \end{bmatrix} \Rightarrow L_A\left(\overrightarrow{v_9}\right) = \begin{bmatrix} 34 \\ 49 \\ 30 \end{bmatrix}$$

Neste caso, na codificação da mensagem, se obteve:

O	R I O	D E	J A N E I R O	C O N T I N U A	L I N D O O.
15	18 9 15	4 5	10 1 14 5 9 18 15	3 15 14 20 9 14 21 1	12 9 14 4 15 15
42	51 27 24	29 9	25 39 15 32 50 27 33	48 18 43 52 29 36 37 22	35 49 23 34 49 30

Assim, a mensagem codificada a ser enviada seria:

42 51 27 24 29 9 25 39 15 32 50 27 33 48 18 43 52 29 36 37 22 35 49 23 34 49 30.

Para a decodificação, o receptor deve usar a chave assimétrica que seria, neste caso a matriz inversa, para obter a mensagem original. Assim, a decodificação será feita de acordo com a transformação inversa.

Como a transformação linear inversa de L_A que em princípio é denotada por $(L_A)^{-1}$ é dada por $L_{A^{-1}}$. Logo $(L_A)^{-1}\left(\vec{x}\right) = L_{A^{-1}}\left(\vec{x}\right) = A^{-1}\vec{x}$ e, portanto se $L_A\left(\vec{x}\right) = A\vec{x}$, então $(L_A)^{-1}\left(L_A\left(\vec{x}\right)\right) = L_{A^{-1}}\left(L_A\left(\vec{x}\right)\right) = L_{A^{-1}}\left(A\vec{x}\right) = A^{-1}\left(A\vec{x}\right) = A^{-1}A\vec{x} = \vec{x}$.

Neste caso, para cada vetor $\vec{x}$, a decodificação será obtida por $\vec{x} = A^{-1}L_A\left(\vec{x}\right)$.

Voltemos ao exemplo. Suponhamos que a mensagem recebida tenha sido:

42 51 27 24 29 9 25 39 15 32 50 27 33 48 18 43 52 29 36 37 22 35 49 23 34 49 30.

Para realizar a decodificação além da mensagem criptografada precisamos ter a matriz inversa da chave, ou seja, A^{-1}.

Como a matriz $A=\begin{bmatrix}1&1&1\\1&1&2\\0&1&1\end{bmatrix}$, então $A^{-1}=\begin{bmatrix}1&0&-1\\1&-1&1\\-1&1&0\end{bmatrix}$. Portanto, para encontrar a mensagem original, após agrupar os números da mensagem criptografada em vetores de R^3, basta utilizarmos a relação $\vec{x}=A^{-1}L_A\left(\vec{x}\right)$.

$$L_A\left(\vec{v_1}\right)=\begin{bmatrix}42\\51\\27\end{bmatrix},\quad L_A\left(\vec{v_2}\right)=\begin{bmatrix}24\\29\\9\end{bmatrix},\quad L_A\left(\vec{v_3}\right)=\begin{bmatrix}25\\39\\15\end{bmatrix},\quad L_A\left(\vec{v_4}\right)=\begin{bmatrix}32\\50\\27\end{bmatrix},\quad L_A\left(\vec{v_5}\right)=\begin{bmatrix}33\\48\\18\end{bmatrix},$$

$$L_A\left(\vec{v_6}\right)=\begin{bmatrix}43\\52\\29\end{bmatrix},\quad L_A\left(\vec{v_7}\right)=\begin{bmatrix}36\\37\\22\end{bmatrix},\quad L_A\left(\vec{v_8}\right)=\begin{bmatrix}35\\49\\23\end{bmatrix}\quad \text{e}\quad L_A\left(\vec{v_9}\right)=\begin{bmatrix}34\\49\\30\end{bmatrix}.$$

Aplicando a decodificação em cada um dos vetores criptografados:

Decodificação de $L_A\left(\vec{v_1}\right)=\begin{bmatrix}42\\51\\27\end{bmatrix}\Rightarrow A^{-1}\begin{bmatrix}42\\51\\27\end{bmatrix}=\begin{bmatrix}1&0&-1\\1&-1&1\\-1&1&0\end{bmatrix}\begin{bmatrix}42\\51\\27\end{bmatrix}=\begin{bmatrix}15\\18\\9\end{bmatrix}\Rightarrow\vec{v_1}=\begin{bmatrix}15\\18\\9\end{bmatrix}$

Decodificação de $L_A\left(\vec{v_2}\right)=\begin{bmatrix}24\\29\\9\end{bmatrix}\Rightarrow A^{-1}\begin{bmatrix}24\\29\\9\end{bmatrix}=\begin{bmatrix}1&0&-1\\1&-1&1\\-1&1&0\end{bmatrix}\begin{bmatrix}24\\29\\9\end{bmatrix}=\begin{bmatrix}15\\4\\5\end{bmatrix}\Rightarrow\vec{v_2}=\begin{bmatrix}15\\4\\5\end{bmatrix}$

Decodificação de $L_A\left(\vec{v_3}\right)=\begin{bmatrix}25\\39\\15\end{bmatrix}\Rightarrow A^{-1}\begin{bmatrix}25\\39\\15\end{bmatrix}=\begin{bmatrix}1&0&-1\\1&-1&1\\-1&1&0\end{bmatrix}\begin{bmatrix}25\\39\\15\end{bmatrix}=\begin{bmatrix}10\\1\\14\end{bmatrix}\Rightarrow\vec{v_3}=\begin{bmatrix}10\\1\\14\end{bmatrix}$

Decodificação de $L_A\left(\vec{v_4}\right)=\begin{bmatrix}32\\50\\27\end{bmatrix}\Rightarrow A^{-1}\begin{bmatrix}32\\50\\27\end{bmatrix}=\begin{bmatrix}1&0&-1\\1&-1&1\\-1&1&0\end{bmatrix}\begin{bmatrix}32\\50\\27\end{bmatrix}=\begin{bmatrix}5\\9\\18\end{bmatrix}\Rightarrow\vec{v_4}=\begin{bmatrix}5\\9\\18\end{bmatrix}$

Decodificação de $L_A\left(\vec{v_5}\right)=\begin{bmatrix}33\\48\\18\end{bmatrix}\Rightarrow A^{-1}\begin{bmatrix}33\\48\\18\end{bmatrix}=\begin{bmatrix}1&0&-1\\1&-1&1\\-1&1&0\end{bmatrix}\begin{bmatrix}33\\48\\18\end{bmatrix}=\begin{bmatrix}15\\3\\15\end{bmatrix}\Rightarrow\vec{v_5}=\begin{bmatrix}15\\3\\15\end{bmatrix}$

Decodificaçãode $L_A\left(\vec{v_6}\right)=\begin{bmatrix}43\\52\\29\end{bmatrix}\Rightarrow A^{-1}\begin{bmatrix}43\\52\\29\end{bmatrix}=\begin{bmatrix}1&0&-1\\1&-1&1\\-1&1&0\end{bmatrix}\begin{bmatrix}43\\52\\29\end{bmatrix}=\begin{bmatrix}14\\20\\9\end{bmatrix}\Rightarrow\vec{v_6}=\begin{bmatrix}14\\20\\9\end{bmatrix}$

$$\text{Decodificação de } L_A\left(\overrightarrow{v_7}\right)=\begin{bmatrix}36\\37\\22\end{bmatrix} \Rightarrow A^{-1}\begin{bmatrix}36\\37\\22\end{bmatrix}=\begin{bmatrix}1&0&-1\\1&-1&1\\-1&1&0\end{bmatrix}\begin{bmatrix}36\\37\\22\end{bmatrix}=\begin{bmatrix}14\\21\\1\end{bmatrix} \Rightarrow \overrightarrow{v_7}=\begin{bmatrix}14\\21\\1\end{bmatrix}$$

$$\text{Decodificação de } L_A\left(\overrightarrow{v_8}\right)=\begin{bmatrix}35\\49\\23\end{bmatrix} \Rightarrow A^{-1}\begin{bmatrix}35\\49\\23\end{bmatrix}=\begin{bmatrix}1&0&-1\\1&-1&1\\-1&1&0\end{bmatrix}\begin{bmatrix}35\\49\\23\end{bmatrix}=\begin{bmatrix}12\\9\\14\end{bmatrix} \Rightarrow \overrightarrow{v_8}=\begin{bmatrix}12\\9\\14\end{bmatrix}$$

$$\text{Decodificação de } L_A\left(\overrightarrow{v_9}\right)=\begin{bmatrix}34\\49\\30\end{bmatrix} \Rightarrow A^{-1}\begin{bmatrix}34\\49\\30\end{bmatrix}=\begin{bmatrix}1&0&-1\\1&-1&1\\-1&1&0\end{bmatrix}\begin{bmatrix}34\\49\\30\end{bmatrix}=\begin{bmatrix}4\\15\\15\end{bmatrix} \Rightarrow \overrightarrow{v_9}=\begin{bmatrix}4\\15\\15\end{bmatrix}$$

Assim, na decodificação da mensagem se obtém:

42	51 27 24	29 9	25 39 15 32 50 27 33	48 18 43 52 29 36 37 22	35 49 23 34 49 30
15	18 9 15	4 5	10 1 14 5 9 18 15	3 15 14 20 9 14 21 1	12 9 14 4 15
O	R I O	D E	J A N E I R O	C O N T I N U A	L I N D O O.

2.4 **Método de Rabin**

O método de Rabin foi criado em 1979. Tal procedimento é semelhante ao método de criptografia RSA pois nele também deve-se determinar duas chaves para a codificação: uma pública e outra privada.

Geração das chaves na criptografia de Rabin

Para gerar tanto a chave pública quanto a privada temos que:

- ✓ Escolher dois números primos p e q distintos e razoavelmente grandes de forma que p seja próximo de q e $p \equiv q \equiv 3(\mathrm{mod}\,4)$.
- ✓ Calcular $n = p \cdot q$.
- ✓ A chave pública (número que deve ser divulgado para o emissor) é n e a chave privada (números que são mantidos em sigilo pelo receptor) é (p, q).

Etapa de ciframento

Neste momento o emissor deverá codificar a mensagem da seguinte forma:

- ✓ Obter a chave pública *n* do receptor.
- ✓ Converter as letras, números e símbolos da mensagem em números *m* entre 0 e $n - 1$.
- ✓ Para cada número *m*, obtido nas conversões acima, calcula-se $c \equiv m^2 \pmod{n}$.
- ✓ Enviar a mensagem cifrada composta pelos números *c* dos cálculos acima para o receptor.

Etapa do deciframento

Uma vez que o receptor recebe a mensagem codificada composta pelos números c, então ele deverá:

- ✓ Encontrar as quatro raízes quadradas m_j com $j = 1, 2, 3, 4$ de c módulo n.
- ✓ O número *m*, da mensagem original, é um dos m_j.

O receptor deve identificar qual das quatro possibilidades para os m_j é a mensagem enviada. Se a mensagem for um texto, então a identificação é fácil, pois apenas um dos m_j fará sentido. Entretanto, se a mensagem for pequena ou possuir palavras em outros idiomas ou até mesmo uma sequência aleatória de letras, números e símbolos, a descoberta do m_j correto pode ser uma tarefa árdua. Uma forma de solucionar este problema é acrescentar redundâncias binárias na mensagem original convertida para a base binária. Para isto, basta repetir uma quantidade fixa de dígitos no final da mensagem. Assim, o m_j correto irá reproduzir essas redundâncias, enquanto é altamente improvável que uma das outras três raízes quadradas m_j venha reproduzir estas redundâncias. Assim, o receptor, pode escolher corretamente a mensagem enviada.

Antes de partirmos para um exemplo prático, iremos enunciar uma proposição que fornece as quatro raízes quadradas de *a* módulo $n = pq$, para certos *p* e *q*, utilizadas na etapa de deciframento.

Proposição: Seja $a \in \text{IN}$ e $a \equiv z^2 \pmod{pq}$ sendo p e q primos e $p \equiv q \equiv 3 \pmod 4$, então existem somente quatro raízes quadradas de a módulo *pq* e elas são dadas por:

$$z = \pm xpa^{\frac{q+1}{4}} + yqa^{\frac{p+1}{4}} \text{ e } z = \pm xpa^{\frac{q+1}{4}} - yqa^{\frac{p+1}{4}}$$

Sendo que $x, y \in \text{Z}$, podem ser obtidos pelo algoritmo de Euclides estendido de modo que:

$$xp + yq = 1$$

A demonstração da funcionalidade da Criptografia Rabin pode ser encontrada em Mollin (2001).

Vamos ao exemplo. Vamos supor que a mensagem a ser enviada seja PROFMAT UERJ. Tomemos $p = 179$ e $q = 43$. Logo $n = pq = 7697$. Portanto, 7697 é a chave pública e (179,43) é a chave privada. Vamos criptografar letra a letra da mensagem usando a tabela escolhida aleatoriamente (cada letra pode corresponder a qualquer número) a seguir:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

S	T	U	V	W	X	Y	Z	.	0	1	2	3	4	5	6	7	8	9
28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46

Criptografando a letra P:

Utilizando a tabela temos que P corresponde ao $m = 25$. Representando 25 na base binária temos que $25 = 1 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4$, então $m = 11001$. Introduzindo redundâncias, ou seja, repetindo os quatro últimos dígitos, temos $m' = 110011001$, que equivale ao número 409 na base 10. Então, como $c \equiv (m')^2 \pmod{7697}$, temos que $c \equiv 167281 \pmod{7697} \Rightarrow c = 5644$ e c é enviado ao receptor.

Criptografando a letra R:

Utilizando a tabela temos que R corresponde ao $m = 27$. Representando 27 na base binária temos que $27 = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4$, então $m = 11011$. Introduzindo redundâncias, ou seja, repetindo os quatro últimos dígitos, temos

m' = 110111011, que equivale ao número 443 na base 10. Então, como $c \equiv (m')^2 (\mathrm{mod}\, 7697)$, temos que $c \equiv 196249 (\mathrm{mod}\, 7697) \Rightarrow c = 3824$ e c é enviado ao receptor.

Criptografando a letra O:

Utilizando a tabela temos que O corresponde ao m = 24. Representando 24 na base binária temos que $24 = 0 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4$, então m = 11000. Introduzindo redundâncias, ou seja, repetindo os quatro últimos dígitos, temos m' = 110001000, que equivale ao número 392 na base 10. Então, como $c \equiv (m')^2 (\mathrm{mod}\, 7697)$, temos que $c \equiv 153664 (\mathrm{mod}\, 7697) \Rightarrow c = 7421$ e c é enviado ao receptor.

Criptografando a letra F:

Utilizando a tabela temos que F corresponde ao m = 15. Representando 15 na base binária temos que $15 = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3$, então m = 1111. Introduzindo redundâncias, ou seja, repetindo os quatro últimos dígitos, temos m' = 11111111, que equivale ao número 255 na base 10. Então, como $c \equiv (m')^2 (\mathrm{mod}\, 7697)$, temos que $c \equiv 65025 (\mathrm{mod}\, 7697) \Rightarrow c = 3449$ e c é enviado ao receptor.

Criptografando a letra M:

Utilizando a tabela temos que M corresponde ao m = 22. Representando 22 na base binária temos que $22 = 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4$, então m = 10110. Introduzindo redundâncias, ou seja, repetindo os quatro últimos dígitos, temos m' = 101100110, que equivale ao número 358 na base 10. Então, como $c \equiv (m')^2 (\mathrm{mod}\, 7697)$, temos que $c \equiv 128164 (\mathrm{mod}\, 7697) \Rightarrow c = 5012$ e c é enviado ao receptor.

Criptografando a letra A:

Utilizando a tabela temos que A corresponde ao m = 10. Representando 10 na base binária temos que $10 = 0 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3$, então m = 1010. Introduzindo redundâncias, ou seja, repetindo os quatro últimos dígitos, temos m' = 10101010, que

equivale ao número 170 na base 10. Então, como $c \equiv (m')^2 (\mathrm{mod}\, 7697)$, temos que $c \equiv 28900 (\mathrm{mod}\, 7697) \Rightarrow c = 5809$ e c é enviado ao receptor.

Criptografando a letra T:

Utilizando a tabela temos que T corresponde ao m = 29. Representando 29 na base binária temos que $29 = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4$, então m = 11101. Introduzindo redundâncias, ou seja, repetindo os quatro últimos dígitos, temos m' = 111011101, que equivale ao número 477 na base 10. Então, como $c \equiv (m')^2 (\mathrm{mod}\, 7697)$, temos que $c \equiv 227529 (\mathrm{mod}\, 7697) \Rightarrow c = 4316$ e c é enviado ao receptor.

Criptografando a letra U:

Utilizando a tabela temos que U corresponde ao m = 30. Representando 30 na base binária temos que $30 = 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4$, então m = 11110. Introduzindo redundâncias, ou seja, repetindo os quatro últimos dígitos, temos m' = 111101110, que equivale ao número 494 na base 10. Então, como $c \equiv (m')^2 (\mathrm{mod}\, 7697)$, temos que $c \equiv 244036 (\mathrm{mod}\, 7697) \Rightarrow c = 5429$ e c é enviado ao receptor.

Criptografando a letra E:

Utilizando a tabela temos que E corresponde ao m = 14. Representando 14 na base binária temos que $14 = 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3$, então m = 1110. Introduzindo redundâncias, ou seja, repetindo os quatro últimos dígitos, temos m' = 11101110, que equivale ao número 238 na base 10. Então, como $c \equiv (m')^2 (\mathrm{mod}\, 7697)$, temos que $c \equiv 56644 (\mathrm{mod}\, 7697) \Rightarrow c = 2765$ e c é enviado ao receptor.

Criptografando a letra R:

Essa relação já foi criptografada anteriormente, portanto, $c = 3824$ e c é enviado ao receptor.

Criptografando a letra J:

Utilizando a tabela temos que J corresponde ao m = 19. Representando 19 na base binária temos que $19 = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4$, então m = 10011. Introduzindo redundâncias, ou seja, repetindo os quatro últimos dígitos, temos m' = 100110011, que equivale ao número 307 na base 10. Então, como $c \equiv (m')^2 \pmod{7697}$, temos que $c \equiv 94249 \pmod{7697} \Rightarrow c = 1885$ e c é enviado ao receptor.

Portanto, a mensagem, PROFMAT UERJ seria enviada ao receptor da seguinte maneira: 5644 3824 7421 3449 5012 5809 4316 5429 2765 3824 1885.

Para decifrar a mensagem, precisamos encontrar as quatro raízes quadradas de c módulo 7697. Utilizando a proposição, pelo algoritmo de Euclides estendido encontramos x e y de modo que $xp + yq = 1$.

$179 = 4 \cdot 43 + 7$	$179 - 4 \cdot 43 = 7$ (I)
$43 = 6 \cdot 7 + 1$(II)	Substituindo (I) em (II) temos que :
	$43 = 6 \cdot (179 - 4 \cdot 43) + 1$
	$43 = 6 \cdot 179 - 24 \cdot 43 + 1$
	$43 - 6 \cdot 179 + 24 \cdot 43 = 1$
	$(-6) \cdot 179 + 25 \cdot 43 = 1$

Daí concluímos que $x = -6$ e $y = 25$. Para fazermos a decodificação de cada valor de c encontraremos as quatro raízes quadradas de c módulo 7697 utilizando a proposição enunciada anteriormente. Daí segue que:

$$m_1 \equiv \left(xpc^{\frac{q+1}{4}} + yqc^{\frac{p+1}{4}} \right) (\text{mod } pq)$$

$$m_2 \equiv \left(-xpc^{\frac{q+1}{4}} + yqc^{\frac{p+1}{4}} \right) (\text{mod } pq)$$

$$m_3 \equiv \left(xpc^{\frac{q+1}{4}} - yqc^{\frac{p+1}{4}} \right) (\text{mod } pq)$$

$$m_4 \equiv \left(-xpc^{\frac{q+1}{4}} - yqc^{\frac{p+1}{4}} \right) (\text{mod } pq)$$

Decodificação de 5644:

$$m_1 \equiv (-1074 \,.\, 5644^{11} + 1075 \,.\, 5644^{45}) \pmod{7697}$$
$$m_2 \equiv (1074 \,.\, 5644^{11} + 1075 \,.\, 5644^{45}) \pmod{7697}$$
$$m_3 \equiv (-1074 \,.\, 5644^{11} - 1075 \,.\, 5644^{45}) \pmod{7697}$$
$$m_4 \equiv (1074 \,.\, 5644^{11} - 1075 \,.\, 5644^{45}) \pmod{7697}$$

Daí segue que:

$$m_1 \equiv (-1074 \,.\, 3332 + 1075 \,.\, 3094) \pmod{7697}$$
$$m_2 \equiv (1074 \,.\, 3332 + 1075 \,.\, 3094) \pmod{7697}$$
$$m_3 \equiv (-1074 \,.\, 3332 - 1075 \,.\, 3094) \pmod{7697}$$
$$m_4 \equiv (1074 \,.\, 3332 - 1075 \,.\, 3094) \pmod{7697}$$

Portanto,

$$m_1 \equiv (-3578568 + 3326050) \pmod{7697} \Rightarrow m_1 \equiv (-252518) \pmod{7697} \Rightarrow m_1 = 1483.$$
$$m_2 \equiv (3578568 + 3326050) \pmod{7697} \Rightarrow m_2 \equiv (6904618) \pmod{7697} \Rightarrow m_2 = 409.$$
$$m_3 \equiv (-3578568 - 3326050) \pmod{7697} \Rightarrow m_3 \equiv (-6904618) \pmod{7697} \Rightarrow m_3 = 7288.$$
$$m_4 \equiv (3578568 - 3326050) \pmod{7697} \Rightarrow m_4 \equiv (252518) \pmod{7697} \Rightarrow m_4 = 6214.$$

Escrevendo as raízes na forma binária temos que:

$$m_1 = 10111001011.$$
$$m_2 = 110011001.$$
$$m_3 = 1110001111000.$$
$$m_4 = 1100001000110.$$

Note que apenas a raiz m_2 possui redundância. Tirando essa redundância (final 1001) a mensagem original em binário seria 11001 e passando para a base decimal, obtemos o número 25 que corresponde a letra P.

Decodificação de 3824:

$$m_1 \equiv (-1074 \,.\, 3824^{11} + 1075 \,.\, 3824^{45}) \pmod{7697}$$
$$m_2 \equiv (1074 \,.\, 3824^{11} + 1075 \,.\, 3824^{45}) \pmod{7697}$$
$$m_3 \equiv (-1074 \,.\, 3824^{11} - 1075 \,.\, 3824^{45}) \pmod{7697}$$
$$m_4 \equiv (1074 \,.\, 3824^{11} - 1075 \,.\, 3824^{45}) \pmod{7697}$$

Daí segue que:

$$m_1 \equiv (-1074 \,.\, 400 + 1075 \,.\, 4918) \pmod{7697}$$
$$m_2 \equiv (1074 \,.\, 400 + 1075 \,.\, 4918) \pmod{7697}$$
$$m_3 \equiv (-1074 \,.\, 400 - 1075 \,.\, 4918) \pmod{7697}$$
$$m_4 \equiv (1074 \,.\, 400 - 1075 \,.\, 4918) \pmod{7697}$$

Portanto,

$$m_1 \equiv (-429600 + 5286850) \pmod{7697} \Rightarrow m_1 \equiv (4857250) \pmod{7697} \Rightarrow m_1 = 443.$$
$$m_2 \equiv (429600 + 5286850) \pmod{7697} \Rightarrow m_2 \equiv (5716450) \pmod{7697} \Rightarrow m_2 = 5276.$$
$$m_3 \equiv (-429600 - 5286850) \pmod{7697} \Rightarrow m_3 \equiv (-5716450) \pmod{7697} \Rightarrow m_3 = 2421.$$
$$m_4 \equiv (429600 - 5286850) \pmod{7697} \Rightarrow m_4 \equiv (-4857250) \pmod{7697} \Rightarrow m_4 = 7254.$$

Escrevendo as raízes na forma binária temos que:

$$m_1 = 110111011.$$
$$m_2 = 1010010011100.$$
$$m_3 = 100101110101.$$
$$m_4 = 1110001010110.$$

Note que apenas a raiz m_1 possui redundância. Tirando essa redundância (final 1011) a mensagem original em binário seria 11011 e passando para a base decimal, obtemos o número 27 que corresponde a letra R.

Decodificação de 7421:

$$m_1 \equiv (-1074 \,.\, 7421^{11} + 1075 \,.\, 7421^{45}) \pmod{7697}$$
$$m_2 \equiv (1074 \,.\, 7421^{11} + 1075 \,.\, 7421^{45}) \pmod{7697}$$
$$m_3 \equiv (-1074 \,.\, 7421^{11} - 1075 \,.\, 7421^{45}) \pmod{7697}$$
$$m_4 \equiv (1074 \,.\, 7421^{11} - 1075 \,.\, 7421^{45}) \pmod{7697}$$

Daí segue que:

$$m_1 \equiv (-1074 \,.\, 3951 + 1075 \,.\, 145) \pmod{7697}$$
$$m_2 \equiv (1074 \,.\, 3951 + 1075 \,.\, 145) \pmod{7697}$$
$$m_3 \equiv (-1074 \,.\, 3951 - 1075 \,.\, 145) \pmod{7697}$$
$$m_4 \equiv (1074 \,.\, 3951 - 1075 \,.\, 145) \pmod{7697}$$

Portanto,

$$m_1 \equiv (-4243374 + 155875) \pmod{7697} \Rightarrow m_1 \equiv (-4087499) \pmod{7697} \Rightarrow m_1 = 7305.$$
$$m_2 \equiv (4243374 + 155875) \pmod{7697} \Rightarrow m_2 \equiv (4399249) \pmod{7697} \Rightarrow m_2 = 4162.$$
$$m_3 \equiv (-4243374 - 155875) \pmod{7697} \Rightarrow m_3 \equiv (-4399249) \pmod{7697} \Rightarrow m_3 = 3535.$$
$$m_4 \equiv (4243374 - 155875) \pmod{7697} \Rightarrow m_4 \equiv (4087499) \pmod{7697} \Rightarrow m_4 = 392.$$

Escrevendo as raízes na forma binária temos que:

$$m_1 = 1110010001001.$$
$$m_2 = 1000001000010.$$
$$m_3 = 110111001111.$$
$$m_4 = 110001000.$$

Note que apenas a raiz m_4 possui redundância de quatro dígitos conforme as duas cifras anteriores. Tirando essa redundância (final 1000) a mensagem original em binário seria 11000 e passando para a base decimal, obtemos o número 24 que corresponde a letra O.

Analogamente, faz-se a decodificação das demais cifras: 3449, 5012, 5809, 4316, 5429, 2765, 3824 e 1885. E assim, concluímos que a mensagem original era PROFMAT UERJ.

3 **CRIPTOGRAFIA NA ATUALIDADE**

Com o avanço da tecnologia, torna-se cada dia mais sensível a interceptação de dados pessoais por hackers no mundo da internet, pelo qual circulam informações de transações bancárias e comerciais, de todo sigilosas. Assim sendo, nota-se por crucial a importância da criptografia, que estuda métodos de codificação de dados, em modo que apenas seu destinatário legítimo consiga interpretá-lo.

Por exemplo, imagine que uma empresa envia a um banco uma autorização para uma transação bilionária. É notória a necessidade de proteger essa mensagem, objetivando que não seja lida, mesmo que interceptada por um concorrente ou hacker. De outro norte, o banco também necessita ter certeza de que a mensagem foi enviada por um usuário seu, devendo conter, para tanto, uma assinatura. Por conta disto, verifica-se a crucialidade da invenção de novos códigos, que sejam difíceis de se interpretar até mesmo por máquinas computadorizadas.

Desde a década de 70 que estudam a possibilidade de uma codificação indecifrável. Idealizada inicialmente por Whitfield Diffie, Martin Hellman e Ralph Merkle, a cifra assimétrica pretendia uma codificação que não implicasse necessariamente em uma decodificação, de forma a encontrar uma função de mão única, irreversível. A partir dessa condição, iniciou o estudo para encontrar uma função matemática apropriada.

Diffie, em 1975, publicou um resumo de seus ideias e a partir daí vários cientistas se uniram em busca de uma função de mão única. Apesar da ideia do trio funcionar na teoria, não conseguiram descobrir uma função apropriada e, consequentemente, essa cifra não se tornava realidade.

Em 1977, na costa Leste dos Estados Unidos, Ronald Rivest, Adi Shamir e Leonard Adleman, encontraram uma função capaz de colocar em prática a ideias do trio californiano. Surge assim, no Massachusetts Institute of Techology, a criptografia RSA, em homenagem a Rivest, Shamir e Adleman. Até hoje, o RSA é o mais conhecido dos métodos de criptografia de chave pública, nome dado ao sistema de criptografia assimétrica, onde são usadas duas chaves distintas e uma delas é disponibilizada publicamente, uma vez que a chave utilizada para cifrar uma mensagem não é capaz de decifrar a mesma. Tal método criptográfico tornou-se base para outros que surgiriam após sua criação, como o caso do método de Rabin, que vimos no capítulo anterior e também é utilizado nos dias de hoje em transações bancárias.

Recentemente foi criado um sistema de criptografia empregado no whatsapp para acabar com a insatisfação de seus usuários, já que quando uma mensagem era lida pelo receptor, o emissor conseguia identificar essa fato através das setas na coloração azul. Após o desconforto, o Whatsapp criou uma atualização baseado no sistema criptográfico de código aberto capaz de bloquear as setas.

Com a criptografia empregada no WhatsApp, a segurança é ainda maior, já que apenas os usuários que trocam conversas podem ter acesso ao conteúdo. Com isso, nem a empresa possui acesso a essas mensagens, nem sob ordem judicial. Por enquanto, apenas mensagens de texto em conversas individuais são criptografadas, mas em breve, conversas em grupo e conteúdos multimídia também devem receber o recurso.

CONCLUSÕES

Neste trabalho, podemos concluir que o uso da criptografia desde tempos remotos aos dias atuais é praticamente imprescindível. Com o avanço tecnológico através da internet, surgiram novas aplicações como o comércio eletrônico e o home banking. Nestas aplicações, informações confidenciais como número de cartões de crédito, transações financeiras e etc são enviadas e processadas em meios não confiáveis. Porém, para que a chance do comércio eletônico se perpetue, segurança é a palavra chave do negócio.

A confiança do consumidor com relação à transação eletrônica é fundamental. Isso tem ocorrido pela criptografia, pois assim fica garantido que sua senha e o número do seu cartão de crédito não sejam usados por pessoas não autorizadas. Enquanto meios de comunicações suficientemente seguros para proteger esse tipo de informação não surgem, a criptografia aparece como boa alternativa para proteção de dados.

Com a criptografia, três características para a segurança de informações são alcançadas. São elas:

- Privacidade → Proteção contra o acesso de terceiros.
- Autenticidade → Constatação de que o autor do documento é de fato quem diz ser.
- Integridade → Proteção contra modificação dos dados por terceiros.

Por fim, conclui-se que sem a criptografia as transações pela internet seriam inseguras e talvez a transferência de dados bancários não seria tão popular atualmente.

REFERÊNCIAS

ALECRIM, E. *História e aplicações da criptografia.* Disponível em: <http://www.infowester.com/criptografia.php. 2014>. Acesso em: 12 dez. 2014.

ALVARENGA, L. G. *Criptografia clássica e moderna*. Disponível em: <http://www.scribd.com/doc/35442992/Criptografia-Classica-e-Moderna. 2014>. Acesso em: 08 dez. 2014.

COUTINHO, S. C. *Números inteiros e criptografia RSA*. 2. ed. Rio de Janeiro: IMPA, 2009.

COUTINHO, S. C. *Programa de iniciação científica da OBMEP*. Rio de Janeiro: IMPA), 2008.

DOMINGUES, H. H.; IEZZI, G. *Álgebra moderna*. 2. ed. São Paulo: Ed. Atual, 1992.

DOMINGUES, H. H. *Fundamentos de aritmética*. São Paulo: Ed. Atual, 1991.

EVES, H. *Introdução à história da matemática*. São Paulo: Editora da Unicamp, 2004.

FERRONI, M. Quebrando códigos. *Revista Galileu Galilei: Especial Eureca*, 2003.

HOWARD, A.; RORRES, C. *Álgebra linear com aplicações*. 8. ed. Porto Alegre: Ed. Bookmann, 2001.

KOLMAN, B. *Introdução à álgebra linear com aplicações*. Rio de Janeiro: Livros Técnicos e Científicos, 1999.

LUCCHESI, C. L. *Introdução à criptografia computacional*. Campinas-SP: Editora Unicamp, 1986.

MARCACINI, A. T. R. *Direito e informática: uma abordagem jurídica sobre criptografia*. Rio de Janeiro: Ed. Forense, 2002.

MELO, C. D. L. de. *Criptografia no Ensino Médio: uma proposta para o ensino de matrizes*. 2014. Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Instituto de Matemática e Estatística, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2014.

MILIES, C. P.; COELHO, S. P. *Números: uma introdução*. São Paulo: Editora da Universidade de São Paulo, 2003.

MOLLIN, R. A. *Na introduction to cryptography*. New York: Chapman & Hall, 2001.

POZZEBON, R. *Whatsapp adota novo sistema de criptografia*. Disponível em: <http://www.oficinadanet.com.br/post/13673-whatsapp-adota-novo-sistema-de-criptografia. 2015> Acesso em: 20 jan. 2015.

RIVEST, M.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, n. 21, 1978.

ROUTO, T. *Segurança de dados: criptografia em redes de computador*. São Paulo: Ed. E. Blucher, 2000.

SANTOS, J. P. O. *Introdução à teoria dos números.* Rio de Janeiro: IMPA, 1998.(Coleção Matemática Universitária)

SCHEINERMAN, E. R. *Matemática discreta: uma introdução*. São Paulo: Thomson Learning Edições, 2006.

SHOKRANIAN, S. *Criptografia para iniciantes*. Editora: Ed. Universidade de Brasília, 2005.

SILVA, F. T.; PAPINE, F. G. Um pouco da história da criptografia. In: SEMANA ACADÊMICA DA MATEMÁTICA, XXII, 2008, Cascavel. *Resumos*... Cascavel: Centro de Ciências Exatas e Tecnológicas da Universidade Estadual do Oeste, 2008.

SINGH, S. *O livro dos códigos*. São Paulo: Editora Record, 2001.

SINGH, S. *O último teorema de fermat: a história do enigma que confundiu as maiores mentes do mundo durante 358 anos*. Rio de Janeiro: Ed. Record, 1998.

STALLINGS, W. *Criptografia e segurança de redes*. 4. ed. São Paulo: Peason Prentice Hall, 2007.

ZANCABELLA, L. C. *Fundamentos da criptografia*. Florianópolis: INE/UFSC/SC, 2001.