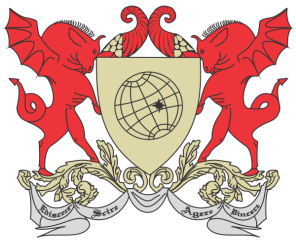
Universidade Federal de Viçosa
Dissertação de Mestrado



Guilherme Inácio Lemos Braga

A CRIPTOGRAFIA COMO RECURSO DIDÁTICO NO ENSINO MÉDIO

FLORESTAL – MINAS GERAIS
2020

GUILHERME INÁCIO LEMOS BRAGA

A CRIPTOGRAFIA COMO RECURSO DIDÁTICO NO ENSINO MÉDIO

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional, para obter o título de *Magister Scientiae*.

Orientador: Alexandre Alvarenga Rocha

Coorientadora: Danielle Franco Nicolau Lara

FLORESTAL – MINAS GERAIS
2020

Ficha catalográfica elaborada pela Biblioteca da Universidade Federal de Viçosa - Campus Florestal

T
B813c
2020

Braga, Guilherme Inácio Lemos, 1992-
A criptografia como recurso didático no ensino médio : . / Guilherme Inácio Lemos Braga. – Florestal, MG, 2020.
70 f. : il. (algumas color.) ; 29 cm.

Inclui anexos.
Orientador: Alexandre Alvarenga Rocha.
Dissertação (mestrado) - Universidade Federal de Viçosa.
Referências bibliográficas: f. 68.

1. Criptografia. 2. RSA. 3. Matemática-ensino médio. I. Universidade Federal de Viçosa. Departamento de Ciências Exatas e Tecnológicas. Mestrado em Matemática. II. Título.

513

Guilherme Inácio Lemos Braga

A CRIPTOGRAFIA COMO RECURSO DIDÁTICO NO ENSINO MÉDIO

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional, para obter o título de *Magister Scientiae*

Aprovada: 21 de fevereiro de 2020.

Assentimento:

Guilherme Inácio Lemos Braga
Autor

Alexandre Alvarenga Rocha
Orientador

Agradecimentos

A gratidão é a maneira mais eficaz de ser contemplado com novas oportunidades. E por isso nunca me canso de agradecer, principalmente a Deus, por não me desamparar na caminhada até aqui. Ele é testemunha de todas as horas de estudo dedicadas ao ingresso e permanência neste curso que foi sonho e hoje se faz muito próximo de se tornar realidade. Pela minha vida, saúde e persistência, meu Pai, muito obrigado!

À minha família, que assistiu aflita todas as minhas angústias e mesmo sem entender a necessidade de tanto esforço nunca me desanimou, meu muito obrigado!

À minha namorada que se mostrou paciente em muitos momentos dessa caminhada, meu muito obrigado!

Aos meus amigos, principalmente aos que fiz durante este curso, que compartilharam comigo as incertezas, os fracassos e as dificuldades superadas na busca desse sonho, meu muito obrigado!

A cada um dos professores que o PROFMAT me apresentou, pela dedicação, conhecimento compartilhado e humanidade, meu muito obrigado!

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

Este trabalho fecha o ciclo mais importante da minha vida até então. E a todos que direta ou indiretamente contribuíram para que eu subisse mais esse degrau, meu muito obrigado!

Resumo

BRAGA, Guilherme Inácio Lemos, M.Sc., Universidade Federal de Viçosa, fevereiro de 2020. **A CRIPTOGRAFIA COMO RECURSO DIDÁTICO NO ENSINO MÉDIO**. Orientador: Alexandre Alvarenga Rocha. Coorientadora: Danielle Franco Nicolau Lara.

A Criptografia é a prática que garante a segurança nos processos de comunicação em todas as áreas de integração. De transações bancárias a simples mensagens de texto, a criptografia está diluída no nosso dia a dia. Com este estudo, nosso objetivo é, além de trazer a conhecimento as principais técnicas de criptografia conhecidas, também usá-las como alternativa didática para os professores nas aulas de matemática do ensino médio, uma vez que a disciplina é uma das principais responsáveis pelo fracasso escolar. Baseando-nos em autores como S.C. Coutinho, reforçamos a eficiência da Criptografia RSA, que é nosso principal objeto de estudo e a partir dele trazemos propostas para sua aplicação em forma de atividades.

Palavras chaves: Criptografia. Códigos. RSA.

Abstract

BRAGA, Guilherme Inácio Lemos, M.Sc., Universidade Federal de Viçosa, February, 2020. **Cryptography as a Didactic Resource in High School**. Adviser: Alexandre Alvarenga Rocha. Co-adviser: Danielle Franco Nicolau Lara.

Encryption is the practice that ensures security in communication processes in all areas of integration. From banking to simple text messaging, encryption is diluted in our daily lives. With this study, our goal is not only to bring to light the main known cryptographic techniques, but also to use them as a didactic alternative for teachers in high school math classes, since discipline is a major culprit for failure. school Based on authors like S.C. Coutinho, we reinforce the efficiency of RSA Cryptography, which is our main object of study and from it we bring proposals for its application in the form of activities.

Keywords: Cryptography. Codes. RSA.

Lista de Figuras

Lista de Tabelas

Sumário

1

Introdução

A criptografia é a arte e ciência de fabricar códigos secretos. De maneira mais precisa, é o estudo das técnicas pelas quais uma informação pode ser modificada de forma a ficar oculta, ininteligível, salvo para o destinatário de direito da mensagem. Portanto, a função da criptografia é proteger uma informação. A palavra criptografia deriva do grego Kryptós, "escondido", e gráphein, "escrita". Figueiredo [2010]

A história da criptografia é precedida pela esteganografia, (steganos, que significa "coberto", e graphein, que significa "escrever"), ou seja, é a arte de se escrever ocultamente. Os primeiros relatos que configuram a utilização desta técnica foram em meados do século V a.C, quando reis e rainhas se comunicavam com seus aliados sem risco de seus inimigos terem conhecimento. Guerras foram vencidas assim e hoje essa técnica é conhecida como criptografia. Embora sejam parecidas, elas se diferem, pois a criptografia tem por função ocultar o significado de uma mensagem, enquanto a esteganografia tem por função ocultar a sua existência. Em termos práticos, uma pode ser utilizada dentro da outra.

Singh [2008] relata que umas das primeiras técnicas de envio de mensagem foi a utilizada por Demerato, um grego exilado que vivia na Pérsia, que decidiu advertir os espartanos dos planos de invasão do rei Persa, Xerxes. A mensagem foi enviada "raspando a cera de um par de tabuletas de madeira e escrevendo embaixo o que Xerxes pretendia fazer, depois a mensagem foi coberta novamente com cera. Deste modo, as tabuletas pareciam estar em branco e não causariam problemas com os guardas ao longo da estrada."

Outra forma que também foi utilizada para envio de mensagens de modo que ficasse oculta, foi a utilizada por Histaeu, rei de Mileto, que raspou a cabeça de um mensageiro e tatuou um plano de revolta contra a dominação persa no seu couro cabeludo e, quando o cabelo cresceu o mensageiro foi enviado ao destinatário. Assim que chegou ao seu destino, o mensageiro informou que a informação que levava estava em seu couro cabeludo e, sendo raspada sua cabeça novamente, o destinatário teve conhecimento da mensagem que lhe fora enviada.

Nesta mesma época outras formas de se ocultar a existência de uma informação, das mais variadas formas, foram amplamente exploradas. Tintas especiais que ao ser submetidas ao calor faziam-se legíveis, técnicas de se escrever dentro de ovos de modo que só depois de retirada a casca o conteúdo pudesse ser visto, a inclusão de uma informação dento de outro texto, entre outras formas que, por perdurarem por tantos anos pareciam

oferecer certa segurança. Acontece que quando eram postas sob uma vigilância rígida, revelavam-se falhas. Muitos desses relatos se encontram na obra *As Histórias*, de Heródoto, (484-425 a.C.) um importante historiador grego da antiguidade.

A necessidade de se proteger uma informação é antiga. A criptografia surgiu para superar as falhas da esteganografia, mas era de uso exclusivo dos governos em situação de guerra, ou para quando desejavam manter sigilo de alguma informação que pudesse trazer riscos nas mãos de inimigos.

As cifras usadas para se camuflar uma informação eram, até a década de 70 do século passado, simétricas, isto é, a chave para codificar e decodificar uma mensagem era a mesma. Mais recentemente, há pouco mais de quarenta anos, é que se fez uso da cifra assimétrica, para a qual existem duas chaves: uma pública, que serve para codificar a mensagem, e outra privada, que serve para decodificá-la.

Os pioneiros em criptografia de chave pública foram Whitfield Diffie e Martin Hellman, dois criptógrafos estadunidenses que desenvolveram e publicaram em 1976 um dos primeiros exemplos práticos de métodos de troca de chaves implementado dentro do campo da criptografia, o algoritmo **Diffie-Hellman**.

Com uma chave simétrica, João criptografa e envia uma mensagem para Maria. A chave usada por ele é a mesma que Maria vai usar para descriptografá-la. Mesmo as chaves sendo iguais, o Intruso não a conhece, logo não pode descobrir o conteúdo da mensagem.

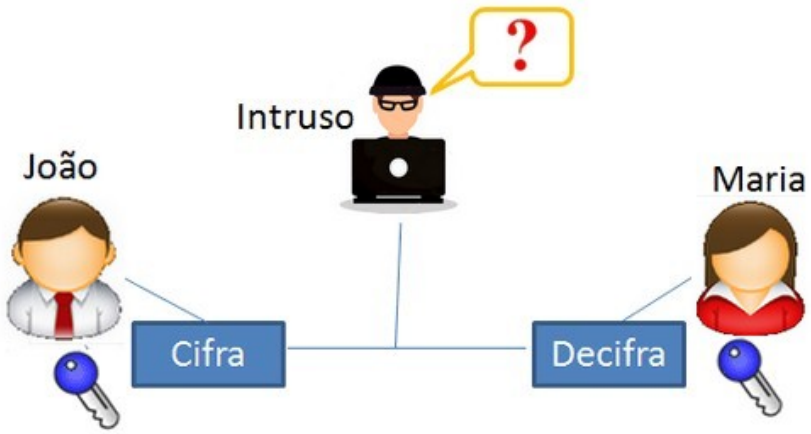


Figura 1.1: Criptografia de chave única (Simétrica)

Com uma chave assimétrica, João codifica uma mensagem utilizando a chave pública de Maria, que ela mesma disponibilizou para o uso de qualquer pessoa. Depois de criptografada a mensagem, João a envia para Maria, pela *internet*. Maria recebe e decodifica a mensagem utilizando sua própria chave privada, que é apenas de seu conhecimento. E só a chave privada da Maria pode decodificar. Assim, o Intruso mesmo tendo a chave pública da Maria, não descriptografa a mensagem. Para responder à mensagem de João, Maria deverá realizar o mesmo procedimento, mas utilizando a chave pública do João. E será a chave privada dele que fará a decodificação da mensagem recebida por Maria.

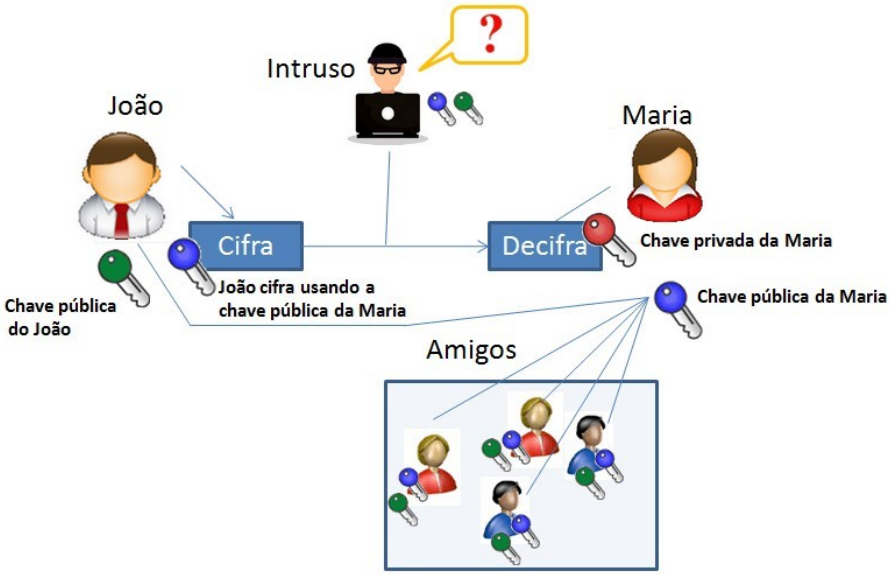


Figura 1.2: Criptografia de chave assimétrica

O histórico da criptografia mostra o uso de diferentes cifras usadas no tratamento de uma informação. As cifras de transposição e substituição ganham destaque. Na primeira, as letras do texto original se mantêm mas em posições alternadas; e na segunda, as letras do texto original são mantidas em suas posições, mas substituídas por outras letras ou caracteres.

Usando uma cifra de transposição, um texto simples como a palavra **PAZ** gera um total $3! - 1 = 5$ anagramas distintos da palavra original: **PZA, APZ, AZP, ZAP, ZPA**. Já palavra **PROFMAT** gera 7! - 1 = 5039 anagramas distintos do original e consequentemente, quanto maior o texto, maiores são as maneiras distintas de se organizar suas letras. Na frase: **Viver significa lutar** existem $P_{19}^{2,4,2,2} = \dfrac{19!}{2!4!2!2!} - 1$ formas de se fazer essa combinação, o que dificulta a retomada do texto original por qualquer estranho.

> *"A transposição efetivamente gera um anagrama incrivelmente difícil e, se as letras forem misturadas ao acaso, sem rima ou fundamento, a decodificação do anagrama se tornará impossível, tanto para o destinatário quanto para o interceptor inimigo."* *Singh [2011]*

Já com uma cifra de substituição, basta que associemos o alfabeto comum a um alfabeto em cifra, ou seja, deve existir uma correspondência biunívoca entre as letras do texto original e as letras do alfabeto pelo qual serão feitas as substituições. Cada letra original é trocada por uma letra ou símbolo do alfabeto em cifra, criando assim uma função bijetiva. A fragilidade desta técnica está no que os criptoanalistas se dedicavam a fazer: analisar a frequência das letras no texto para reconhecer as possíveis substituições correspondentes ao alfabeto usado pra cifragem. As cifras de substituição serão tratadas mais adiante, e suas variações e evolução ao longo dos tempos é o nosso objeto de estudo.

Com a invenção dos computadores e da *internet* a criptografia deixa de ser uma exclusividade dos poderes públicos e passa ser uma necessidade de empresas e pessoas que também buscam sigilo nas suas informações.

A *internet* é um conector de informações que ficam suscetíveis a intercepções de terceiros, causando danos aos responsáveis pela sua emissão e também ao seu receptor. Nas transações bancárias, em compras *on-line*, dados pessoais, senhas, entre outras informações se faz o uso da criptografia, uma vez que, se estas informações não estiverem protegidas (cifradas), elas podem ser alteradas por um *hacker* e usadas de maneira fraudulenta.

De acordo com Stallings and Bressan [2004], atualmente a criptografia vai além da função de gerar privacidade na troca de informações. Ela também tem a função de:

- Autentificar: confirmar que certa informação é verdadeira;
- Irretratabilidade: alguém envia uma informação e depois se nega dizendo que não a enviou (ou alguém se negar dizendo que não recebeu);
- Integridade: garantir que a mensagem não foi modificada durante seu envio.

A criptografia utiliza diversos segmentos da matemática para sua aplicação, dentre os quais podemos citar a aritmética modular nas cifras de César, as cifras de substituição com as funções bijetoras e o RSA com o problema de fatoração de números inteiros.

Neste trabalho veremos alguns dos principais métodos criptográficos usados ao longo da história, acompanharemos a evolução desses métodos até um dos mais recentes deles, o sistema RSA, inventado em 1977, no qual concentraremos este estudo. Descreveremos as funcionalidades desses métodos e a partir disso aplicaremos seus resultados em salas de aula do Ensino Médio.

Temos por objetivo neste levantamento trazer a Criptografia como uma alternativa no ensino da matemática, e fazer dela um recurso diferente, que pode ser explorado pelos professores.

Uma das preocupações quanto ao ensino da matemática nos dias atuais é sua abordagem em sala de aula, que muitas vezes ainda acontece de maneira técnica e pouco aplicável. Mesmo conhecendo inúmeras alternativas didáticas, os professores exploram a tradicional aula de quadro e giz, deixando de atingir muitos alunos, principalmente aqueles com histórico de defasagem no conteúdo.

O tema de criptografia abordado nas turmas de Ensino Médio

> *"Permite interligar os conteúdos matemáticos à situações do mundo real e ajuda a desenvolver habilidades e competências na resolução de problemas, a criar estratégias de resolução, a ter autonomia durante o processo de aprendizagem, com isso, tornando-os mais autoconfiantes e concentrados na realização das atividades."* Olgin *[2011]*

Além de ajudar a criar estratégias para resolução de problemas, alternativas didáticas como essa são recursos que visam o despertar pra matemática por parte do aluno.

> *"Acredita-se que a inclusão de atividades que envolvam conceitos de criptografia pode ajudar a diminuir a existência de aulas mecânicas, onde o professor, através de atividades práticas, poderá mostrar a aplicabilidade dos conceitos trabalhados em sala de aula, relacionando-os a fatos importantes ocorridos na atualidade."* Kripka *[2011]*

Em resumo, no segundo capítulo deste trabalho discorremos sobre a evolução na história de alguns dos principais métodos criptográficos. O terceiro capítulo é destinado a entender o funcionamento e aplicação de alguns métodos usados para criptografar uma mensagem por meio de exemplos e a teoria em que se fundamentam. No quarto capítulo discutiremos estudo do sistema RSA, sua funcionalidade e segurança, e ainda faremos um passo a passo de como aplicar um dos métodos criptográficos mais usuais e seguros que se tem conhecimento. O último capítulo desta pesquisa foi reservado para apresentar algumas propostas de atividades que relacionam os conteúdos de matemática à criptografia, assim como o resultado da aplicação de algumas delas em sala de aula.

2

História da Criptografia

2.1 Citale Espartano e a Cifra de César

Um dos primeiros aparelhos criptográficos que se tem conhecimento é o Cilate Espartano (Figura 2.1), um instrumento militar do século V a.C. utilizado pelos líderes da antiga Esparta para envio de mensagens secretas, que usava uma cifra de transposição.

O cilate consiste num bastão de madeira no qual é enrolado uma tira de couro ou pergaminho. O remetente escreve sua mensagem ao longo do seu comprimento, na tira, que em seguida é desenrolada e a mensagem deixa de fazer sentido. Essa tira é camuflada sendo usada como cinto, ou escondida até que o mensageiro a entregue ao destinatário, que, por sua vez, consegue decifrar a mensagem usando outro cilate com mesmo diâmetro do primeiro usado pelo remetente.

Figura 2.1: Cilate Espartano

O primeiro documento que usou uma cifra de substituição para propósito militar foi feito pelo Imperador Júlio César, em 50 a.C. Esse método de criptografar foi amplamente explorado em guerras e foi objeto de estudo dos criptoanalitas da época.

Para cifrar seu texto, ele alterou as letras deslocando-as em três posições para direita: A se tornava D, B se tornava E, e assim por diante.

A palavra **MATEMÁTICA** se escrita usando a correspondência de César seria **PDWHPDWLFD**. O número de deslocamentos no alfabeto cifrado gera uma novo texto.

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

A segurança da cifra de César era frágil, visto que as correspondências se limitam apenas a 25 transposições distintas, cada uma correspondente a uma letra do alfabeto. Cada correspondência é uma chave, sendo assim qualquer pessoa que se dedique a testar as possíveis chaves pode decifrar um texto.

Singh [2008] descreve que César enviou uma mensagem com fins militares para Cícero e nela reforçava seu método para criptografar substituindo letras latinas por gregas. Qualquer cifra que se baseie em substituições denomina-se cifra de César.

A partir daí, os árabes desenvolveram uma técnica para decifrar as mensagens que usavam esse tipo de substituição, que ficou conhecida como criptoanálise. Observando a frequência das letras na mensagem criptografada era possível supor sua substituição e decifrar a mensagem original. Esta ferramenta, a análise de frequência, é atribuída ao filósofo árabe al-Kindi.

Segundo Singh [2011], *"monoalfabética é o nome dado a qualquer cifra de substituição na qual o alfabeto cifrado pode consistir em símbolos, letras, assim como uma mistura de letras e ou símbolos."*

A partir da observação de al-Kindia, a cifra de substituição monoalfabética caiu em desuso, sendo necessário outras maneiras de cifrar as mensagens.

2.2 O Disco de Alberti e a Cifra de Vigenère

Por volta de 1460, Leon Battista Alberti (1404 - 1472), *"propôs o uso de dois ou mais alfabetos cifrados, usados alternadamente, de modo a confundir os criptoanalistas em potencial"* Singh [2011] como forma de cifrar as mensagens enviadas ao vaticano, o que fez resultar no tratado de Cifris, de 1467, em que Alberti escreveu e constituiu-se o primeiro texto sobre cifras polialfabéticas.

As cifras polialfabéticas são cifras que trabalham com vários alfabetos cifrados, sendo cada letra do texto original substituída pela correspondente no alfabeto cifrado, mas sempre alternando o alfabeto usado.

A vantagem do método de Alberti é que as principais letras, como observadas no método de César, não apareciam necessariamente como uma única letra no texto cifrado. Uma mesma letra aparecia ora substituída por uma, ora substituída por outra letra dos alfabetos usados na cifragem.

Alberti foi um dos primeiros a criar um dispositivo que facilitava o processo criptográfico: o disco de Alberti.

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 setores; em cada um dos setores do disco maior escreveu o alfabeto em letras maiúsculas pela sua ordem normal, mas não continha as letras H, J, K, U, W e Y

(já que no latim essas letras não eram adotadas); nos quatro setores que sobraram colocou os algarismos 1, 2, 3 e 4.

No disco móvel, colocou de uma forma aleatória, em cada um dos setores, as letras do alfabeto, que eram 24, sendo a vigésima quarta o & (et). No disco pequeno – que representa o alfabeto de cifra - escolhe-se uma letra chave, por exemplo a k, alinha-se esta letra alternadamente com as letras de uma palavra-chave no disco maior, e podemos começar a encriptar o texto. Se utilizarmos a palavra-chave DOCE, alinhamos a posição da letra k do disco menor com a letra D e cifrамos a primeira letra do texto simples; em seguida, alinhamos a letra k do disco menor com a letra O do disco maior e cifrамos a segunda letra; após cifrarmos a quarta letra, repetimos o processo de alinhamento até cifrarmos a mensagem toda. Neste caso, temos uma cifra polialfabética, onde se utilizaram quatro alfabetos de cifra. Os mediadores têm que ter conhecimento da letra-chave e da palavra-chave.

Figura 2.2: Disco de Alberti

De acordo com Singh [2011], através do trabalho de Alberti e de outros que contribuíram, como Johannes Tritheminus e Giovanni Porta, o diplomata francês Blaise Vigenère desenvolveu a cifra polialfabética mais conhecida, a cifra de Vigenère.

Esta cifra é semelhante à cifra de Alberti, mas Vigenère passa a trabalhar com uma tabela que consiste no alfabeto escrito 26 vezes em diferentes linhas, cada um deslocado ciclicamente do anterior por uma posição e uma chave para cifrar e decifrar a mensagem. Acreditava-se que esta técnica era imune à análise de frequência pois possui um grande número de possíveis chaves. Isso fez com que essa cifra ficasse conhecida como "le chiffre indéchiffrable"(a cifra indecifrável).

Apesar deste tipo de cifra ser segura, ela foi considerada muito complexa e esse motivo fez com que fosse abandonada durante os dois séculos seguintes após sua descoberta.

> *"Em consequência disso, os criptógrafos buscaram uma cifra intermediária, mais difícil de quebrar do que a cifra monoalfabética direta, mas que fosse mais simples de usar do que a cifra polialfabética." Singh [2011]*

Cria-se a partir disso a Cifra de Substituição Homofônica, na qual cada letra é substituída por uma variedade de símbolos proporcional à sua frequência. Por exemplo, a letra **E** na língua portuguesa poderá ser substituída por 12 símbolos distintos, pois sua frequência é de 12,57% (vide tabela), cada vez que a letra E for aparecer no texto cifrado,

será escolhido ao acaso qual dos 12 símbolos usar, e assim ocorrendo com as demais letras, de modo que no final do texto, cada símbolo representará 1% do texto cifrado, despistando a técnica da análise da frequência.

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

Tabela 2.1: Tabela de frequência das letras em Português

Com uma cifra indecifrável, o trabalho dos criptonalistas precisava de um novo rumo para a história da criptografia. Um novo passo foi dado pelo oficial prussiano Friedrich Kasiski (1805-1881), quase 300 anos depois da invenção da cifra de Vigenère. Em 1863, Kasiski publicou o livro "Die Geheimschriftenund die Dechiffrierkunst" que significa "Escrita secreta e a arte da decifragem" em que relatava o primeiro método para quebrar as cifras polialfabéticas: o Exame de Kasiski. Singh [2011].

O ponto fraco na cifra de Vigenère vinha do fato de que a chave se repetia, por isso, sendo possível descobrir o comprimento da palavra chave, usando a análise de frequência, a mensagem era, enfim, decodificada. Por exemplo, se usada uma palavra chave muito curta como DIA, as correspondências aconteceriam da primeira letra e a cada três letras com a letra D, assim como a segunda letra e três letras depois fariam correspondência com a letra I, e da terceira e a cada três letras depois com a letra A. O processo se repetiria muitas vezes, tornando o texto suscetível à análise.

O matemático inglês Charles Babbage também conseguiu quebrar a cifra de Vigenère antes mesmo de Kasiski, mas por uma opressão do governo essa descoberta só veio à tona em 1887, 24 anos depois da descoberta de Kasiski. Graças às descobertas de Kasiski e Babbage a cifra de Vigenère não era mais segura.

Nada de grande importância foi criado durante a segunda metade do século XIX. Uma nova reencarnação do disco de Alberti criou uma geração de cifras mais difíceis de serem quebradas. O grande divisor de águas na história da criptografia aconteceu durante a Segunda Guerra Mundial.

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

Figura 2.3: Quadro de Vigenère

2.3 A Enigma

A primeira máquina de criptografar foi criada por Alberti, no século XV. Ela reproduzia um deslocamento simples como da cifra de César através de dois círculos que podiam ser girados. Como na sua ideia original, um dos círculos continha o alfabeto original e no outro o cifrado. Para gerar uma cifra polialfabética bastava girar o segundo disco durante a mensagem.

Em 1918, Arthur Scherbius patenteou uma máquina elétrica e mecânica com rotores, que pode ser considerada uma versão elétrica da máquina de Alberti, chamada de Enigma. Ela servia tanto para criptografar como para decriptografar, e foi amplamente usada pelas forças militares alemãs.

Figura 2.4: A Enigma

> *"Já na Segunda Guerra Mundial, os alemães utilizaram uma máquina para criptografar e descriptografar mensagens, chamada Enigma. Nessa época Enigma foi considerada uma máquina extremamente eficiente ao ponto dos franceses e britânicos pensarem que a sua cifra fosse inquebrável. Mesmo com toda a capacidade de cifragem da máquina Enigma e, por isso foi produzida em série, Berlim tinha que enviar agentes para fornecer aos capitães dos barcos U e aos comandantes dos tanques os livros que descreviam as configurações da máquina para codificar as mensagens de cada dia. Naturalmente, se um inimigo pusesse as mãos no livro de códigos, o jogo terminava."Du Sautoy [2007]*

A Enigma se assemelhava a uma máquina de escrever que conhecemos e nela as mensagens eram codificadas e decodificadas.

Dento da Enigma havia uma engrenagem que gerava, a partir dos rotores, milhares de combinações na composição de uma mensagem. Eram ao todo cinco rotores e três destes ficavam dentro da máquina. Cada um deles tinham 26 posições que correspondiam às 26 letras do alfabeto. Usando os transrotores a Enigma gerava $26^3 = 17576$ posições. Além disso, as letras poderiam ser trocadas em um painel de plugues, e assim, ao todo, eram 1 sextilhão de combinações na codificação.

Os operadores autorizados ao uso da Enigma acompanhavam por um livro quais os rotores e plugues que deveriam ser usados naquele dia, assim como sua configuração e reconfiguração diária.

Durante a Segunda Guerra Mundial aconteceu uma choque entre os decifradores britânicos e fazedores de códigos alemães na qual estes últimos se fizeram vencedores. Deu-se uma sequência de momentos nas quais as cifras criadas pela Enigma eram quebradas e em seguida novamente reforçadas.

Os britânicos construíram uma máquina capaz de combater a cifra alemã Lorenz SZ40, cifra resultado de vários aperfeiçoamentos da Enigma, responsável pela comunicação entre Hitler e seus generais. Pela sua estrutura e eficiência, foi considerado o primeiro computador que recebeu o nome de Colossus (figura 2.5), e partir dele foi desenvolvida a criptografia na segunda metade do século XX.

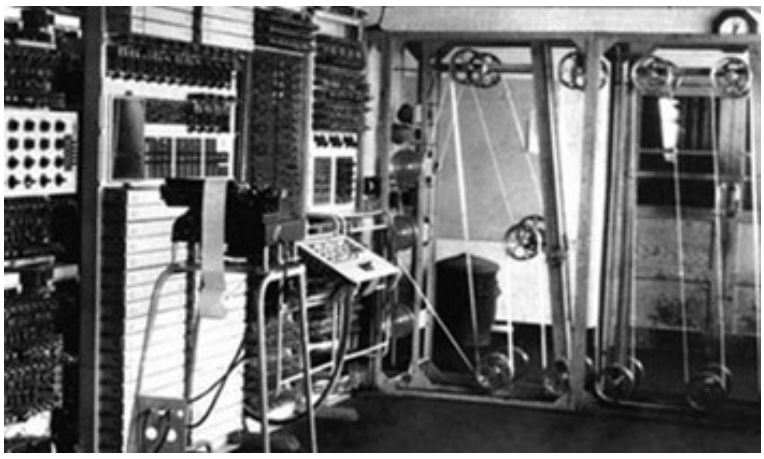


Figura 2.5: Computador Colossus criado para combater a Enigma

A máquina Enigma foi um grande avanço para o mundo da criptografia, pois a partir daí se fez necessário um novo instrumento capaz de gerar códigos mais fortes e resistentes. O próximo grande passo ocorrerá nos anos 70 com o desenvolvimento da criptografia de chave pública e do RSA.

3

Métodos de Criptografia

Nesta seção apresentaremos alguns métodos usados antes que fosse desenvolvido o sistema RSA usado para codificar uma mensagem. Vale ressaltar que nenhum desses métodos tem a eficiência e a segurança no seu objetivo quanto o método que exploraremos no capítulo 4.

3.1 As cifras de substituição

As cifras de substituição são aquelas em que os caracteres da mensagem original são substituídos por outros de um alfabeto pré-definido, mantendo-se a posição das correspondências. Existem substituições simples, que tem como referência um único alfabeto de substituição até substituições polialfabéticas e poligráficas, que usam mais de um alfabeto para a cifragem ou usam símbolos nesse processo.

Para gerar uma cifra de substituição, devemos criar uma regra que vai conduzir a cifragem da mensagem e uma regra oposta para decifrá-la. Utilizaremos as funções, já que elas possibilitam associar dois elementos de maneira ordenada, em especial as funções bijetoras, que fazem o caminho de ida e volta na cifragem e decifragem do texto.

Para prosseguir vamos relembrar os conceitos que usaremos nas funções.

Definição 3.1 (Função): Sejam A e B conjuntos diferentes do vazio. Uma relação f de A em B é uma função se, e somente se, todo elemento de A estiver associado, por meio de f, a um único elemento de B. O conjunto A é chamado domínio da função e o conjunto B contradomínio.

Definição 3.2 (Função Injetora): Uma função f de A em B é dita injetora se para dois elementos distintos x_1 e x_2 do domínio temos $f(x_1) \neq f(x_2)$.

Definição 3.3 (Função Sobrejetora): Uma função f de A em B é sobrejetora, se cada ponto do contradomínio é a imagem de pelo menos um ponto no domínio, isto é, para cada $y \in B$ existe ao menos um $x \in A$ tal que $f(x) = y$.

Definição 3.4 (Função Bijetora): Se uma função f de A em B é injetora e sobrejetora, então dizemos que f é uma função bijetora.

Definição 3.5 (Função Inversa): Seja f uma função de A em B, com domínio A e conjunto imagem B. Então, sua função inversa f^{-1} tem domínio B e conjunto imagem A e é definida por $f^{-1}(y) = x \Leftrightarrow f(x) = y$ para todo $y \in B$.

Teorema 3.6: Uma função f de A em B admite função inversa, se e somente se, f for uma função bijetora.

A prova desse teorema pode ser explorada no livro de Elon Lages Lima, Números e funções reais, SBM, 2012 (Coleção PROFMAT).

A tabela abaixo guiará muitos dos processos de codificação e decodificação de um texto que trataremos neste capítulo. Nela associaremos a cada letra do alfabeto um número pelos quais faremos as conversões necessárias. Veja:

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

Tabela 3.1: Tabela de Conversão

Exemplo 3.1.1: Para o processo de pré-codificação, é necessário que convertamos o texto a ser encriptado em uma sequência numérica a partir da tabela de conversão. O valor das letras nessa tabela corresponde ao domínio da função, que no nosso exemplo será:

$$f(x) = 2x - 1$$

para criptografar a mensagem: **Crescer é um processo**.

Transformando cada letra da mensagem em um número, temos:

2-17-4-18-2-4-17-4-20-12-15-17-14-2-4-18-18-14

Em seguida, basta calcular o valor numérico da função quando aplicamos os números que substituem a mensagem. Sempre que a correspondência passar de 25, deve-se voltar ao início para encontrar a letra correspondente, daí:
$f(2) = 2.2 - 1 = 3$ que corresponde à letra **D**;

$f(17) = 2.17 - 1 = 33$ que corresponde à letra **H**;

$f(4) = 2.4 - 1 = 7$ que corresponde à letra **H**;

$f(18) = 2.18 - 1 = 35$ que corresponde à letra **J**;
$\vdots$
$f(14) = 2.14 - 1 = 27$ que corresponde à letra **B**.

Ao final do processo temos: **DHHJDHHHNXDHBDHJJB**, que numericamente corresponde à sequência

3-33-7-35-3-7-33-7-39-23-29-33-27-3-7-35-35-27.

Para decodificar o texto, precisamos da função inversa de $f(x) = 2x - 1$ que é

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

E aplicando cada elemento gerado no passo anterior nessa função, com auxílio da tabela de substituição, temos:

$f^{-1}(3) = \dfrac{(3+1)}{2} = 2$ que corresponde à letra **C**

$f^{-1}(33) = \dfrac{(33+1)}{2} = 17$ que corresponde à letra **R**

$f^{-1}(7) = \dfrac{(7+1)}{2} = 4$ que corresponde à letra **E**

$f^{-1}(35) = \dfrac{(35+1)}{2} = 18$ que corresponde à letra **S**

$\vdots$

$f^{-1}(27) = \dfrac{(27+1)}{2} = 14$ que corresponde à letra **O**

A partir de então temos novamente a sequência original e com isso conseguimos descriptografar a mensagem.

As cifras de substituição funcionam todas da mesma maneira. Como já discutido no capítulo anterior, a Cifra de César, que foi usada pelo imperador Júlio César para se comunicar com seus subordinados com segurança, tratava-se de reescrever um texto deslocando cada letra desse texto 3 casas para a direita, então para decifrar a mensagem, o receptor precisaria fazer a operação inversa, ou seja, deslocar cada letra do texto cifrado para esquerda em 3 casas.

Todo processo matemático usado na Cifra de César pode ser baseado em aritmética modular, tal como o método RSA, que será assunto do próximo capítulo, mas aqui trataremos esse método com uso de funções de várias sentenças.

Para criptografar uma mensagem usaremos novamente a mesma tabela de conversão e uma função da forma

$$f(x) = \begin{cases} x + L, \text{ se } 0 \leq x \leq 25 - L \\ x + L - 26, \text{ se } 25 - L \ < x \leq 25 \end{cases}$$

onde x representa a posição da letra e L a quantidade de casas que será deslocada.

O termo L da expressão é a chave da cifra. No caso específico do imperador César, o valor de L é 3. Para trabalhar com uma função com duas sentenças, se o valor numérico da função passar de 25, é necessário associar ao início da tabela. A função é bijetora, condição estabelecida para criarmos uma cifra de substituição.

Exemplo 3.1.2: : Para cifrar a mensagem **"A vida é um eco."** usaremos a função

$$f(x) = \begin{cases} x + 12, \text{ se } 0 \leq x \leq 13 \\ x - 14, \text{ se } 13 < x \leq 25 \end{cases}$$

Com essa função conhecemos a quantidade de deslocamentos que serão feitos no momento da cifragem, nesse caso, como $L = 12$, cada letra deve se deslocar 12 posições.

A resolução deste exemplo será apresentada mais adiante, quando traremos sugestões de aplicações em sala de aula deste e outros métodos de criptografar uma mensagem.

É importante ressaltar que os métodos usados para cifrar um texto baseando-se em uma cifra de substituição não são eficazes. Isso acontece porque partir da frequência em que as letras são dispostas no texto cifrado é possível supor sua substituição e decifrar a mensagem original.

3.2 A Cifra de Vigenère

Em alternativa para a fragilidade da cifra de César, o francês Blaise Vigenère criou uma tábua que usava o método de César para criptografar mensagens, mas com todas as 26 possíveis correspondências entre cada letra do alfabeto: em cada linha da tabela se dá uma possível correspondência.

Tomaremos o texto **"Gratidão muda tudo"** para exemplificar o método que a cifra de Vigenère utiliza na cifragem de um texto e usaremos a figura 2.3 para as correspondências que faremos. Para fazê-las precisamos de uma chave de codificação, a nossa será "believe" neste caso.

Para iniciar o processo de cifragem tomaremos na coluna mais à esquerda da tabela cada letra do nosso texto e, na linha mais superior, encontraremos a letra que corresponde à chave. A interseção delas é a letra que devemos substituir no texto original. Assim, a frase "Gratidão muda tudo", ao associarmos à chave temos a correspondência "believeb elie vebe" e, fazendo as interseções temos:

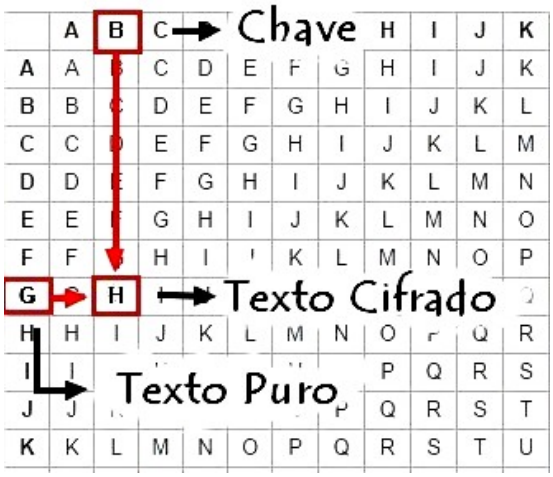


Figura 3.1: Cifragem do texto

Letra **G** na linha com letra **B** na coluna corresponde à letra **H**;
Letra **R** na linha com letra **E** na coluna corresponde à letra **V**;

Letra **A** na linha com letra **L** na coluna corresponde à letra **L**;
Letra **T** na linha com letra **I** na coluna corresponde à letra **B**.
⋮
Letra **O** na linha com letra **E** na coluna corresponde à letra **S**.

E assim, ao final das interseções, temos **HVLBMYEPQFLEOYES** como texto cifrado.

O algoritmo que fundamenta a cifra de Vigenère é também pautado no estudo de congruências. Para entender esse processo, falaremos sobre *Aritmética Modular*.

Definição 3.7 (Congruências): Seja $m > 1$ um número inteiro. Dados $a, b \in \mathbb{Z}$, diz-se que a é côngruo a b módulo m, se, e somente se, $m|(a-b)$ (m divide a diferença entre a e b).

Notação: $a \equiv b \pmod{m}$.

Exemplo 3.2.1:

a) $42 \equiv 2 \pmod{5}$, pois $42 - 2 = 40$ é divisível por 5.

b) $134 \equiv 14 \pmod{15}$, pois $134 - 14 = 120$ é divisível por 15.

Proposição 3.1: (i) $a \equiv a \pmod{m}, \forall\ a \in \mathbb{Z}$

(ii) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$.

(iii) $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

(iv) $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$.

(v) $a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{m}, \forall\ c \in \mathbb{Z}$

(vi) $a \equiv b \pmod{m} \Rightarrow a^r \equiv b^r \pmod{m}, \forall\ r \geq 1$.

Demonstração:

(i) Pois $a - a = 0$ é divisível por m.

(ii) De fato, se $m|(a-b)$, então $m|(b-a)$, pois $b - a = -(a-b)$.

(iii) Como $m|(a-b)$ e $m|(b-c)$, então$m|[(a-b)+(b-c)]$, seja, $m|(a-c)$. Isto equivale à tese.

(iv) Se $a \equiv b$, então $m|(a-b) \Rightarrow (a-b) = k_1 m, k_1 \in \mathbb{Z}$. Se $c \equiv d \pmod{m}$, então $m|(c-d) \Rightarrow (c-d) = k_2 m, k_2 \in \mathbb{Z}$. Somando membro a membro as duas equações, tem-se: $(a-b)+(c-d) = k_1 m + k_2 m \Rightarrow (a+c)-(b+d) = m(k_1+k_2) \Rightarrow (a+c)-(b+d) = km, k \in \mathbb{Z}$. Então: $m|[(a+c)-(b+d)] \Rightarrow (a+c) \equiv (b+d) \pmod{m}$.

(v) Se $a \equiv b$, então $m|(a-b) \Rightarrow (a-b) = k_1 m, k_1 \in \mathbb{Z}$. Multiplicando por c, ambos os membros, tem-se: $c(a-b) = ck_1 m \Rightarrow (ac-bc) = ck_1 m \Rightarrow (ac-bc) = km \Rightarrow m|(ac-bc) \Rightarrow ac \equiv bc \pmod{m}$.

(vi) Provaremos por indução: Para $r = 1$ a implicação é evidente. Supõem-se que $a^r \equiv b^r \pmod{m}$. Então $a^{r+1} \equiv ab^r \pmod{m}$. Por outro lado, de $a \equiv b \pmod{m}$, segue que $ab^r \equiv b^{r+1} \pmod{m}$. Juntando as duas conclusões tiramos $a^{r+1} \equiv b^{r+1} \pmod{m}$.

A equação que criptografa as mensagens é $C \equiv p + k \pmod{26}$ onde C é o texto cifrado, p o texto puro e k a chave de cifragem. Cada letra tem seu valor correspondente na mesma tabela de conversão 3.1 que usamos anteriormente.

Sendo assim, a afirmação *letra **G** na linha com letra **B** na coluna corresponde à letra **H*** pode ser reescrita como

$$C = 6 + 1 \equiv 7 \pmod{26}$$

já que G (texto puro) corresponde ao número 6, B (chave de cifragem) corresponde ao número 1 e 7 corresponde à letra H na tabela de conversão.

A afirmação *letra **R** na linha com letra **E** na coluna corresponde à letra **V*** pode ser reescrita como

$$C = 17 + 4 \equiv 21 \pmod{26}$$

já que R (texto puro) corresponde ao número 17, E (chave de cifragem) corresponde ao número 4 e 21 corresponde à letra V na tabela de conversão.

O processo se dá em todo o texto e a ideia é a mesma na cifra de César quando trabalhamos nela baseando-nos em congruências.

Para descriptografar a mensagem, basta fazer o processo inverso: seguir com a letra correspondente à chave na primeira coluna até que se encontre na linha a letra que corresponde ao texto cifrado. A letra correspondente à essa coluna é o texto puro. Ou seja:

Letra **B** na linha até a letra **H** na mesma linha corresponde à coluna da letra **G**.
Letra **E** na linha até a letra **V** na mesma linha corresponde à coluna da letra **R**.
Letra **L** na linha até a letra **L** na mesma linha corresponde à coluna da letra **A**.
Letra **I** na linha até a letra **B** na mesma linha corresponde à coluna da letra **T**.
⋮
Letra **E** na linha até a letra **S** na mesma linha corresponde à coluna da letra **O**.
E assim por diante, até que se decodifique a mensagem.

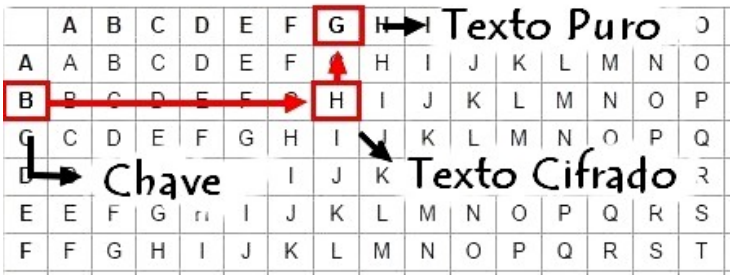


Figura 3.2: Decifrando o texto

A congruência correspondente ao processo de descriptografar é $P \equiv C - k + 26 \pmod{26}$, como antes, C é o texto cifrado, P o texto puro e k a chave de cifragem.

A afirmação *letra* ***B*** *na linha até a letra* ***H*** *na mesma linha corresponde à coluna da letra* ***G*** pode ser reescrita como

$$P = 7 - 1 + 26 \equiv 6 \pmod{26}$$

já que H corresponde ao número 7, B corresponde ao número 1 e 6 corresponde à letra G na tabela de conversão.

A afirmação *letra* ***E*** *na linha até a letra* ***V*** *na mesma linha corresponde à coluna da letra* ***R*** pode ser reescrita como

$$P = 21 - 4 + 26 \equiv 17 \pmod{26}$$

já que a letra V corresponde ao número 21, E corresponde ao número 4 e 17 corresponde à letra R na tabela de conversão.

3.3 A Criptografia com Matrizes

Além dos métodos para criptografar mensagens já discutidos anteriormente, há diversas formas de se fazer este tipo de trabalho. As matrizes são uma alternativa. Um conteúdo que quando se aprende há um questionamento natural: Pra quê serve isso?

Bom, além das importantes aplicações e convencionais para a economia, engenharia e tecnologia, as matrizes podem ser aplicadas no estudo da Criptografia de diversas maneiras, associando a duas matriz as funções de codificar e decodificar um texto. Para entender o processo, precisamos nos lembrar de alguns conceitos.

Definição 3.8: Uma matriz A, $m \times n$ (m por n) é uma tabela de mn números dispostos em m linhas e n colunas, sendo $m, n \in \mathbb{N}$.

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Usamos também a notação $A = (a_{ij})_{m \times n}$. Dizemos que a_{ij} ou $[A]_{ij}$ é o elemento ou a entrada de posição i, j da matriz A. Se $m = n$, dizemos que A é uma matriz quadrada de ordem n e os elementos $a_{11}, a_{22}, \cdots, a_{mn}$ formam a diagonal (principal) de A.

Definição 3.9 (Soma e Diferença de Matrizes): A soma/diferença de duas matrizes de mesma ordem $A = (a_{ij})_{m\times n}$ e $B = (b_{ij})_{m\times n}$ é definida como sendo a matriz $m \times n$

$$C = A + B \text{ ou } C = A + (-B),$$

obtida somando-se/subtraindo-se os elementos correspondentes de A e B, ou seja,

$$c_{ij} = a_{ij} + b_{ij} \text{ ou } c_{ij} = a_{ij} + (-b_{ij})$$

para $i = 1, \cdots, m$ e $j = 1, \cdots, n$.

Definição 3.10 (Multiplicação por um escalar): A multiplicação de uma matriz $A = (a_{ij})_{m\times n}$ por um escalar (número) α é definida pela matriz $m \times n$

$$B = \alpha A,$$

obtida multiplicando-se cada elemento da matriz A pelo escalar α, ou seja,

$$b_{ij} = \alpha a_{ij},$$

para $i = 1, \cdots, m$ e $j = 1, \cdots, n$. Dizemos que a matriz B é um múltiplo escalar da matriz A.

Definição 3.11 (Produto de duas Matrizes): O produto de duas matrizes, tais que o número de colunas da primeira matriz é igual ao número de linhas da segunda, $A = (a_{ij})_{m\times p}$ e $B = (b_{ij})_{p\times n}$ é definido pela matriz $m \times n$

$$C = AB,$$

obtida da seguinte forma

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ip}b_{pj} = \sum_{k=1}^{p} a_{ik}b_{kj},$$

para $i = 1, \cdots, m$ e $j = 1, \cdots, n$.

Exemplo 3.3.1: Seja $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ e $B = \begin{bmatrix} 2 & 1 \\ 0 & 3 \end{bmatrix}$ duas matrizes quadradas de ordem 2. Temos que $A + B$, $A - B$, $3A$ e AB são operações dadas por:

a) $A + B = \begin{bmatrix} 1+2 & 2+1 \\ 3+0 & 4+3 \end{bmatrix} = \begin{bmatrix} 3 & 3 \\ 3 & 7 \end{bmatrix}$

b) $A - B = \begin{bmatrix} 1-2 & 2-1 \\ 3-0 & 4-3 \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ 3 & 1 \end{bmatrix}$

c) $3 \cdot A = \begin{bmatrix} 3\cdot 1 & 3\cdot 2 \\ 3\cdot 3 & 3\cdot 4 \end{bmatrix} = \begin{bmatrix} 3 & 6 \\ 9 & 12 \end{bmatrix}$

d) $AB = \begin{bmatrix} 1\cdot 2 + 2\cdot 0 & 1\cdot 1 + 2\cdot 3 \\ 3\cdot 2 + 4\cdot 0 & 3\cdot 1 + 4\cdot 3 \end{bmatrix} = \begin{bmatrix} 2 & 7 \\ 6 & 15 \end{bmatrix}$

Definição 3.12 (Matriz Inversa): Uma matriz quadrada $A = (a_{ij})_{n\times n}$ é invertível ou não singular, se existe uma matriz $B = (b_{ij})_{n\times n}$ tal que

$$AB = BA = I_n,$$

em que I_n é a matriz identidade. A matriz B é chamada de inversa de A ($B = A^{-1}$). Se A não tem inversa, dizemos que A é não invertível ou singular.

Exemplo 3.3.2: Tomando ainda a matriz $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$. Sua inversa será, se existir, uma matriz $B = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ tal que $A \cdot B = I_n$, ou seja,

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \cdot \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

O produto acima pode ser escrito como sistemas de duas equações lineares
$\begin{cases} a + 2b = 1 \\ 3a + 4b = 0 \end{cases}$ que resolvendo nos dá $a = -2$ e $b = \frac{3}{2}$, e ainda

$\begin{cases} c + 2d = 0 \\ 3c + 4d = 1 \end{cases}$ que resolvendo nos dá $c = 1$ e $d = -\frac{1}{2}$. Sendo assim, a matriz B, inversa de A, é dada por

$$B = \begin{bmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{bmatrix}$$

Para iniciar o processo de cifragem de um texto usando matrizes, precisamos associar o alfabeto, como nos métodos anteriores, à uma tabela de conversão 3.2, que associa cada letra a um número. Neste caso, em particular, usaremos também um caractere vazio.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
1	2	3	4	5	6	7	8	9
J	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**
10	11	12	13	14	15	16	17	18
S	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	
19	20	21	22	23	24	25	26	27

Tabela 3.2: Tabela de Conversão usando Matrizes

Ambos, remetente e destinatário devem ter a mesma tabela para fazer a leitura dos códigos. Vamos cifrar a frase **"Siga em frente"**, pondo nos espaços entre as palavras o número 27, que evitará problemas com a decifragem do texto.

Usaremos a matriz $A = \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix}$ para codificar a mensagem.

Faremos a correspondência das letras com os números dispostos em uma matriz M, de duas linhas (o número de linhas é determinado pela ordem da matriz chave). Caso o texto tenha um número ímpar de caracteres, basta acrescentar caracteres vazios para completar a estrutura da matriz. Assim, **"SIGA EM FRENTE"** corresponde a sequência numérica

19 9 7 1 27 5 13 27 6 18 5 14 20 5

e então, temos a matriz que carrega o texto a ser criptografado

$$M = \begin{bmatrix} 19 & 9 & 7 & 1 & 27 & 5 & 13 \\ 27 & 6 & 18 & 5 & 14 & 20 & 5 \end{bmatrix}$$

Para fazermos a cifragem do texto, basta multiplicarmos a matriz A pela matriz M, tal que, $N = AM$. Ou seja:

$$N = AM = \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 19 & 9 & 7 & 1 & 27 & 5 & 13 \\ 27 & 6 & 18 & 5 & 14 & 20 & 5 \end{bmatrix}$$

$$N = \begin{bmatrix} 84 & 33 & 39 & 8 & 95 & 35 & 44 \\ 65 & 24 & 32 & 7 & 68 & 30 & 31 \end{bmatrix}$$

A matriz N representa o texto codificado:

84 33 39 8 95 35 44 65 24 32 7 68 30 31

O processo para decodificar esse texto depende agora de uma matriz B, inversa de A. Para este exemplo $B = \begin{bmatrix} 1 & -1 \\ -2 & 3 \end{bmatrix}$, é a matriz inversa de A.

Para então decodificar o texto, basta multiplicar a matriz B pela matriz N, tal que, $M = BN$. Ou seja:

$$M = BN = \begin{bmatrix} 1 & -1 \\ -2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 84 & 33 & 39 & 8 & 95 & 35 & 44 \\ 65 & 24 & 32 & 7 & 68 & 30 & 31 \end{bmatrix}$$

$$M = \begin{bmatrix} 19 & 9 & 7 & 1 & 27 & 5 & 13 \\ 27 & 6 & 18 & 5 & 14 & 20 & 5 \end{bmatrix}$$

Em seguida basta novamente associar os números à mesma tabela e obter o texto já decodificado:

19 9 7 1 27 5 13 27 6 18 5 14 20 5 que corresponde a

"SIGA EM FRENTE"

3.4 A Cifra de Hill

A cifra de Hill é um sistema de criptografia polialfabético, criado em 1929 por Lester S. Hill (1891-1961) e que consiste na cifragem da mensagem a ser enviada, quebrando-a em blocos de n letras, utilizando a multiplicação de matrizes.

Como no método descrito na seção anterior, a cifra depende de uma matriz quadrada de ordem n, que possua inversa. Ao texto a ser cifrado é feito uma correspondência de suas letras, por substituição, que será orientada por uma tabela de conversão. A tabela 3.1 já mencionada aqui atende a essas condições.

Ao produto da matriz chave - aquela escolhida para fazer a cifragem do texto - com a matriz que carrega o texto convertido, aplica-se aritmética modular, assunto já discutido neste capítulo.

Caso o número de caracteres (letras) da mensagem a ser cifrada, desconsiderando os espaços entre as palavras, não seja múltiplo de n, completamos o último bloco com letras aleatórias, desde que essas letras não alterem o sentido da mensagem.

Para mostrar como cifrar uma mensagem a partir do método de Hill, tomaremos uma matriz $A_{2\times2}$, invertível, e o texto **"Coisas boas levam tempo"**. A ordem da matriz determina o tamanho dos blocos em que o texto será quebrado. Veja:

Seja $A = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}$ a matriz chave. Associando os números correspondentes às letras do texto, temos a sequência numérica:

2 14 8 18 0 18 1 14 0 18 11 4 21 0 12 19 4 12 15 14.

Para codificar tomam-se os pares consecutivos:

CO IS AS BO AS LE VA MT EM PO

que corresponde aos pares

2 14 8 18 0 18 1 14 0 18 11 4 21 0 12 19 4 12 15 14.

Cada um desses pares deve corresponder a uma matriz P_i, (2×1), com $i = 1, ..., 10$. Assim:

$$P_1 = \begin{bmatrix} 2 \\ 14 \end{bmatrix}, \quad P_2 = \begin{bmatrix} 8 \\ 18 \end{bmatrix}, \quad P_3 = \begin{bmatrix} 0 \\ 18 \end{bmatrix}, \quad P_4 = \begin{bmatrix} 1 \\ 14 \end{bmatrix}, \quad P_5 = \begin{bmatrix} 0 \\ 18 \end{bmatrix}$$

$$P_6 = \begin{bmatrix} 11 \\ 4 \end{bmatrix}, \quad P_7 = \begin{bmatrix} 21 \\ 0 \end{bmatrix}, \quad P_8 = \begin{bmatrix} 12 \\ 19 \end{bmatrix}, \quad P_9 = \begin{bmatrix} 4 \\ 12 \end{bmatrix}, \quad P_{10} = \begin{bmatrix} 15 \\ 14 \end{bmatrix}$$

Efetuamos o produto AP, onde A é a matriz chave, por cada uma das matrizes coluna 2×1, obtidas anteriormente. Em seguida, determinamos o correspondente numérico de AP (mod 26) obtendo, assim, seu correspondente cifrado, ou seja, basta aplicar ao produto a equação:

$$C_i \equiv AP_i \pmod{26}$$

em que C é o bloco cifrado. Temos então:

$$C_1 = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 14 \end{bmatrix} = \begin{bmatrix} 16 \\ 18 \end{bmatrix} \equiv \begin{bmatrix} 16 \\ 18 \end{bmatrix} \pmod{26}$$

$$C_2 = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 8 \\ 18 \end{bmatrix} = \begin{bmatrix} 26 \\ 34 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 8 \end{bmatrix} \pmod{26}$$

$$C_3 = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 18 \end{bmatrix} = \begin{bmatrix} 18 \\ 18 \end{bmatrix} \equiv \begin{bmatrix} 18 \\ 18 \end{bmatrix} \pmod{26}$$

$$\vdots$$

$$C_9 = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ 12 \end{bmatrix} = \begin{bmatrix} 16 \\ 20 \end{bmatrix} \equiv \begin{bmatrix} 16 \\ 20 \end{bmatrix} \pmod{26}$$

$$C_{10} = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 15 \\ 14 \end{bmatrix} = \begin{bmatrix} 29 \\ 44 \end{bmatrix} \equiv \begin{bmatrix} 3 \\ 18 \end{bmatrix} \pmod{26}$$

Portanto, depois de cifrado, o texto corresponde à sequência

16 18 0 8 18 18 15 16 18 18 15 0 21 16 5 17 16 20 3 18

que, associando-os às letras correspondentes na tabela de conversão tem-se:

QSAISSPQSSPAVQFRQUDS

como texto cifrado.

Decifrar esse texto depende de uma matriz B, tal que $B = A^{-1}$, ou seja, B é a matriz inversa de A. O processo para decifrar é análogo ao que ja foi feito para cifrar, sendo assim, associando a cada letra do texto QSAISSPQSSPAFRQUQGDS a um número da tabela de conversão e agrupando-os de dois em dois, tem-se:

16 18 0 8 18 18 15 16 18 18 15 0 21 16 5 17 16 20 3 18

que corresponde às matrizes colunas 2×1 C_i, com $i = 1, ...10$, dadas por:

$$C_1 = \begin{bmatrix}16\\18\end{bmatrix}, \quad C_2 = \begin{bmatrix}0\\8\end{bmatrix}, \quad C_3 = \begin{bmatrix}18\\18\end{bmatrix}, \quad C_4 = \begin{bmatrix}15\\16\end{bmatrix}, \quad C_5 = \begin{bmatrix}18\\18\end{bmatrix}$$
$$C_6 = \begin{bmatrix}15\\0\end{bmatrix}, \quad C_7 = \begin{bmatrix}21\\16\end{bmatrix}, \quad C_8 = \begin{bmatrix}6\\17\end{bmatrix}, \quad C_9 = \begin{bmatrix}16\\20\end{bmatrix}, \quad C_{10} = \begin{bmatrix}3\\18\end{bmatrix}$$

Fazendo agora o produto entre a matriz B, inversa de A, e cada uma das matrizes $C_{i's}$, 2×1, e aplicando a eles a equação

$$P_i \equiv BC_i \pmod{26}$$

em que P é o bloco decifrado, temos de novo a mesma sequência numérica inicialmente gerada. Sendo $B = \begin{bmatrix}-1 & 1\\2 & -1\end{bmatrix}$ a matriz inversa, que será a chave para decifrar o texto, temos:

$$P_1 = \begin{bmatrix}-1 & 1\\2 & -1\end{bmatrix} \cdot \begin{bmatrix}16\\18\end{bmatrix} = \begin{bmatrix}2\\14\end{bmatrix} \equiv \begin{bmatrix}2\\14\end{bmatrix} \pmod{26}$$
$$P_2 = \begin{bmatrix}-1 & 1\\2 & -1\end{bmatrix} \cdot \begin{bmatrix}0\\8\end{bmatrix} = \begin{bmatrix}8\\-8\end{bmatrix} \equiv \begin{bmatrix}8\\18\end{bmatrix} \pmod{26}$$
$$P_3 = \begin{bmatrix}-1 & 1\\2 & -1\end{bmatrix} \cdot \begin{bmatrix}18\\18\end{bmatrix} = \begin{bmatrix}0\\18\end{bmatrix} \equiv \begin{bmatrix}0\\18\end{bmatrix} \pmod{26}$$
$$\vdots$$
$$P_9 = \begin{bmatrix}-1 & 1\\2 & -1\end{bmatrix} \cdot \begin{bmatrix}16\\20\end{bmatrix} = \begin{bmatrix}4\\12\end{bmatrix} \equiv \begin{bmatrix}4\\12\end{bmatrix} \pmod{26}$$
$$P_{10} = \begin{bmatrix}-1 & 1\\2 & -1\end{bmatrix} \cdot \begin{bmatrix}3\\18\end{bmatrix} = \begin{bmatrix}15\\-12\end{bmatrix} \equiv \begin{bmatrix}15\\14\end{bmatrix} \pmod{26}$$

Essas são as correspondências dos pares

2 14 8 18 0 18 1 14 0 18 11 4 21 0 12 19 4 12 15 14.

Com a tabela, voltamos ao texto **"Coisas boas levam tempo"**.

4

Criptografia RSA

Dentre os métodos criptográficos que utilizam uma chave pública, a criptografia RSA é uma das mais utilizada até hoje. O método foi desenvolvido pelos pesquisadores Ron Rivest, Adi Shamir e Len Adleman, do laboratório de ciência da computação do Massachusetts Intitute of Technology - MIT, em 1977 e publicado em 1978. O RSA traz as iniciais dos nomes Rivest, Shamir e Adleman.

A criptografia RSA é pautada em funções matemáticas e relaciona duas chaves, qualquer uma delas pode ser usada para criptografar ou descriptografar uma mensagem. São chamadas de chave pública (ou de cifragem), que fica disponível a todo usuário para criptografar sua mensagem e chave privada (ou de decodificação), que é do conhecimento apenas do destinatário a fim de que ele possa descriptografar a mensagem recebida.

Segundo STALLINGS [2008] "o desenvolvimento da criptografia de chave pública é a maior e talvez a única verdadeira revolução na história da criptografia" e isso se deve ao fato da ineficiência dos algoritmos computacionais de fatoração de números inteiros muito grandes na quebra da chave de decodificação. A seguir, entenderemos como funciona e por que o método RSA é um dos mais seguros dentre os processos de criptografia conhecidos.

4.1 Pré-codificação

Para utilizar o método RSA, primeiro devemos estabelecer uma correspondência entre as letras do nosso alfabeto com uma sequência numérica, na qual cada número será substituído por uma letra. Não faremos distinção entre as letras maiúsculas e minúsculas e também desconsideraremos os acentos das palavras. Os espaços entre as palavras serão substituídos pelo número 99. A tabela 4.1 justifica as correspondências que faremos.

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

Tabela 4.1: Tabela de Conversão RSA

Um cuidado na escolha dos números que farão as correspondências é de que cada letra seja representada por um número de dois algarismos a fim de evitar a ambiguidade no momento de fazer a decodificação da mensagem. Caso representássemos a letra A pelo número 1, a letra B pelo número 2, letra C por 3, e assim por diante, a representação da letra M seria um problema, pois corresponderia ao número 13 e também seria a combinação das letras AC.

O processo de cifragem de uma mensagem usando o método RSA basicamente se resume na escolha de dois números primos distintos que chamaremos de p e q e do produto entre eles, $n = pq$. Omitindo a escolha dos primos e divulgando ao destinatário somente o referido valor de n, há a possibilidade de se decodificar a mensagem. Seria simples se não se tratasse de números primos absurdamente grandes, e que, por consequência, geram n com mais de 200 algarismos. A dificuldade em encontrar primos que satisfaçam ao produto gerado, mesmo com as mais recentes técnicas e computadores, é o que garante o sigilo da mensagem pelos meios onde ela circula até que chegue ao seu destino.

Para exemplificar o funcionamento do método RSA faremos agora um passo a passo de todo o processo para criptografar uma mensagem. No decorrer dos passos ressaltaremos as principais propriedades e teoremas da teoria de números que fundamentam todo o processo.

Neste exemplo faremos a codificação da palavra **PROFMAT**, sendo assim, para a fase da Pré-codificação, temos:

(i) Converter a mensagem para a linguagem numérica com auxilio da tabela de conversão para o método RSA já apresentada:

$$\text{PROFMAT} = \mathbf{25272415221029}$$

(ii) Escolher dois primos p e q quaisquer suficientemente grandes.

Para nosso exemplo, primos menores facilitarão a compreensão do método: tomaremos

$$p = \mathbf{17} \text{ e } q = \mathbf{29}.$$

(iii) Determinar $n = pq$ que será o parâmetro usado na cifragem da mensagem e quebrar em blocos de tamanho menor que n a sequência numérica encontrada em *(i)*. Um cuidado no momento de gerar os blocos é nunca começar um deles com zero, pois, por exemplo, $029 = 29$. Essa falha prejudicaria o processo. Vale ressaltar que os blocos podem ser quebrados de maneiras diversas, desde que obedeçam às condições aqui citadas.

$$n = 17 \cdot 29 = \mathbf{493}$$

E a sequência poderá ser escrita como: **252 - 72 - 415 - 22 - 102 - 9**

4.2 Codificando uma mensagem com RSA

Feita a conversão da mensagem em linguagem numérica, para proceder com a codificação precisamos definir qual será nossa chave pública, aquela que será divulgada para que qualquer pessoa possa criptografar uma mensagem ao emissor. A partir do valor de n temos as próximas definições.

Definição 4.1: Seja p um inteiro, com $p > 1$. Dizemos que p é um número primo se ele for divisível apenas por 1 e por ele mesmo.

Definição 4.2: Seja m um inteiro positivo. A **função fi de Euler**, $\varphi(m)$ é definida como o número de inteiros não negativos menores do que m e que são primos com m. Assim, $\varphi(m) = \#\{a \in \mathbb{Z}_+^* : a < m \text{ e } mdc(a,m) = 1\}$. Observe que, se m for primo, $\varphi(m) = m - 1$.

Definição 4.3: Um sistema reduzido de resíduos módulo m é um conjunto de $\varphi(m)$ inteiros $r_1, r_2, \ldots, r_{\varphi(m)}$ tais que cada elemento deste conjunto é relativamente primo com m, e se $i \neq j$, então $r_i \not\equiv r_j \pmod{m}$.

Teorema 4.4: Sejam $m, n \in \mathbb{N}$ com $mdc(m,n) = 1$. Então $\varphi(mn) = \varphi(m)\varphi(n)$.

Demonstração:

O resultado é facilmente verificado se $m = 1$ ou $n = 1$. Então, vamos supor $m > 1$ e $n > 1$. Assim, consideremos a tabela abaixo formada pelos números naturais de 1 até nm.

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\ 3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m & 2m & 3m & \cdots & mn \end{array}$$

Observe que a tabela acima forma um sistema completo de resíduos módulo nm. Mas, estamos interessados no sistema reduzido de resíduos módulo nm, ou seja, queremos determinar todos os números de 1 a nm que são primos com nm. Assim, queremos determinar t, tal que $mdc(t, nm) = 1$. Mas,

$$mdc(t,mn) = 1 \Rightarrow mdc(t,n) = mdc(t,m) = 1.$$

Dessa forma, para calcular $\varphi(mn)$ devemos determinar na tabela acima os inteiros que são primos com n e m ao mesmo tempo. Assim, se na r-ésima linha tivermos $mdc(m, r) = d > 1$ então nenhum termo dessa linha será primo com nm pois, todos os termos são da forma $km + r$, onde $0 \leq k \leq n - 1$ e estes são todos divisíveis por d. Logo, os elementos que são primos com m estão necessariamente nas colunas restantes e, num total de $\varphi(m)$ elementos. Agora, vejamos quais são os elementos primos com n em cada uma dessas linhas.

Como $mdc(n,m) = 1$, os elementos da linha k, $m + k$, $\ldots$, $(n-1)m + k$ são todos primos com n e formam um sistema completo de resíduos módulo n. Logo, cada uma dessas linhas possui uma quantidade de $\varphi(n)$ elementos primos com n e, consequentemente

primos com nm. Logo, o número de elementos simultaneamente primos com n e m é $\varphi(m)\varphi(n)$. Portanto, $\varphi(mn) = \varphi(m)\varphi(n)$.

□

Teorema 4.5: Sejam a e b dois inteiros positivos. Então existe um inteiro positivo que é o máximo divisor comum de a e b.

Demonstração:

Sejam a e b dois inteiros positivos. Sem perda de generalidade, suponhamos $a \leq b$. Se $a = 1, a = b$ ou $a|b$, então $mdc(a, b) = a$. Dessa forma, vamos supor $1 < a < b$, e $a \nmid b$. Pelo algoritmo da divisão existem r_1 e q_1 inteiros positivos tais que $b = aq_1 + r_1$, com $r_1 < a$. Agora, temos dois casos a analisar:

(i) Se $r_1|a$, então existe k inteiro tal que $a = kr_1$. Como $b = aq_1 + r_1$, e $a = kr_1$, temos $b = kr_1q_1 + r_1 = r_1(kq_1 + 1)$, ou seja, $r_1|b$ e, portanto, $mdc(a, b) = r_1$.

(ii) Se $r_1 \nmid a$, efetuando a divisão de a por r_1, obtemos $a = r_1q_2 + r_2$, com q_2, r_2 inteiros positivos e $r_2 < r_1$. O que nos dá, novamente, duas possibilidades:

1) Se $r_2|r_1$, por uma justificativa análoga à do item i), temos que $mdc(a, b) = r_2$.

2) Se $r_2 \nmid r_1$, efetuando a divisão de r_1 por r_2, obteremos $r_1 = r_2q_3 + r_3$, com $r_3 < r_2$.

Observe que o processo acima é finito, pois, caso contrário, teríamos encontrado uma sequência decrescente de inteiros positivos $a > r_1 > r_2 > r_3 >$. . . que não teria um menor elemento, contrariando assim, o Princípio da Boa Ordem, que diz que todo conjunto $A \subset \mathbb{N}$ não-vazio tem um menor elemento

Logo, sendo r_n este menor elemento, com $r_n|r_{n-1}$, temos que $mdc(a, b) = r_n$. Portanto, quaisquer dois inteiros positivos admitem máximo divisor comum. Vamos representar o algoritmo descrito acima em forma de diagrama.

	q_1	q_2	q_3	$\cdots$	q_{n-1}	q_n	q_{n+1}
b	a	r_1	r_2	$\cdots$	r_{n-2}	r_{n-1}	$r_n = mdc(a,b)$
r_1	r_2	r_3	r_4	$\cdots$	r_n	0	

□

Exemplo 4.2.1: Para determinar o Máximo Divisor Comum (MDC) entre 60 e 96, temos:

	1	1	1	2
96	60	36	24	**12**
36	24	12	0	

Logo, mdc(60,96) = 12.

Sendo assim, com base nas definições apresentadas, procedemos com os próximos passos do processo de cifragem:

(iv) Calcular $\varphi(n) = (p - 1)(q - 1)$, que é a função fi de Euler, com p e q primos.

Sendo assim, no nosso exemplo $\varphi(493) = (17-1)(29-1) = \mathbf{448}$

(v) Determinar o segundo parâmetro que usaremos na codificação que chamaremos de e, de modo que seja co-primo com $\varphi(n)$, ou seja $mdc(e,\varphi(n)) = 1$ e $1 < e < \varphi(n)$.

Para encontrar este número, usaremos o algorítimo estendido de Euclides na busca de um e suficientemente grande que reforce nosso processo, mas podemos buscá-lo testando sequencialmente a partir do número 2: $mdc(448, 2) = 2$, $mdc(448, 3) = 1$. O número 3 atende aos requisitos e por ser um número menor vai facilitar a compreensão dos próximos passos. Tomaremos $e = \mathbf{3}$.

Até aqui descobrimos a chave pública formada pelos parâmetros determinados por (n,e). No nosso exemplo será **(493,3)**.

(vi) Em cada bloco b definido em *(iii)* vamos aplicar a relação $C(b) \equiv b^e \pmod{n}$ onde $C(b)$ é o bloco b cifrado. Esse processo é pautado no estudo das congruências, assunto que já discorremos no capítulo 3 (Definição 3.7).

Aplicando as propriedades de potenciação, para $C(b) \equiv b^e \pmod{n}$, temos:

1º bloco: $C(252) \equiv 252^3 \equiv 228 \pmod{493}$;

2º bloco: $C(72) \equiv 72^3 \equiv 47 \pmod{493}$;

3º bloco: $C(415) \equiv 415^3 \equiv 207 \pmod{493}$;

4º bloco: $C(22) \equiv 22^3 \equiv 295 \pmod{493}$;

5º bloco: $C(102) \equiv 102^3 \equiv 272 \pmod{493}$;

6º bloco: $C(9) \equiv 9^3 \equiv 236 \pmod{493}$;

Depois disso temos a mensagem codificada: **228 - 47 - 207 - 295 - 272 - 236**, que será a mensagem enviada ao destinatário.

Vale ressaltar que a complexabilidade nos cálculos das potências mencionadas ao longo deste exemplo, seriam por si só um adendo neste estudo. As ferramentas computacionais auxiliam os cálculos. Neste caso alinhamos as propriedades de potenciação (produtos de potências com mesma base, potência de potência) ao uso de uma calculadora científica comum para facilitar a compreensão dos passos, e deixá-los acessíveis a qualquer leitor que não se disponha de um recurso melhor.

4.3 Decodificando uma mensagem com RSA

Ao ser recebida pelo destinatário, a mensagem codificada apresenta-se sem sentido caso não seja possível serem feitas as devidas conversões. Neste tópico, assim como

anteriormente, faremos um passo a passo de como decodificar uma mensagem usando o método RSA. Continuaremos usando o exemplo inicialmente proposto para mostrar a funcionalidade do método.

Para isso precisamos descobrir qual a chave privada, ou seja, quais os parâmetros necessários para se fazer a decodificação dos blocos gerados anteriormente. Sendo assim, temos que:

(i) Vamos determinar d, que é o inverso de e, tal que $de \equiv 1 \pmod{\varphi(n)}$. Usaremos o algoritmo estendido de Euclides para determinar esse parâmetro.

Temos então, no nosso exemplo, que $3d \equiv 1 \pmod{448}$, que corresponde dizer que $3d - 448y = 1$, e pelo algoritmo estendido de Euclides

	149	3
448	3	1
1	0	

$1 = 448 - 3 \cdot 149$
$1 = (-448) \cdot (-1) + 3 \cdot (-149)$
$1 = 3 \cdot (-149) - 448 \cdot (-1) \Rightarrow d = -149$ e $y = -1$.

Como $299 \equiv -149 \pmod{448}$ temos que $1 = 3 \cdot (299) - 448 \cdot (-1)$ é equivalente módulo 448. Logo, $d = 299$ é o inverso de e.

Encontramos aqui a chave para decodificar a mensagem, ou seja, a chave privada dada pelos parâmetros

$$(n,d)=\mathbf{(493,299)}.$$

(ii) Aplicar em cada bloco da mensagem já codificada a relação: $D(a) \equiv a^d \pmod{n}$, onde a é um bloco encontrado em *(vi)* no momento da codificação.

Para facilitar os cálculos, vamos usar as propriedades de potenciação alinhadas às propriedades de congruências discutidas na Definição 3.7. Sendo assim, temos que:

$$\begin{aligned}
1^{\text{o}} \text{ bloco} : D(228) &\equiv 228^{299} \pmod{493} \\
&\equiv (228^3)^{99} \cdot 228^2 \pmod{493} \\
&\equiv 139^{99} \cdot 219 \pmod{493} \\
&\equiv (139^4)^{24} \cdot 139^3 \cdot 219 \pmod{493} \\
&\equiv 455^{24} \cdot 139^3 \cdot 219 \pmod{493} \\
&\equiv (455^3)^8 \cdot 139^3 \cdot 219 \pmod{493} \\
&\equiv 344^8 \cdot 248 \cdot 219 \pmod{493} \\
&\equiv (344^2)^4 \cdot 248 \cdot 219 \pmod{493} \\
&\equiv 16^4 \cdot 248 \cdot 219 \pmod{493} \\
&\equiv 460 \cdot 248 \cdot 219 \pmod{493} \\
&\equiv 252 \pmod{493}
\end{aligned}$$

$$
\begin{aligned}
2^{\text{o}} \text{ bloco} : D(47) &\equiv 47^{299} \pmod{493} \\
&\equiv (47^5)^{59} \cdot 47^4 \pmod{493} \\
&\equiv 421^{59} \cdot 460 \pmod{493} \\
&\equiv (421^3)^{19} \cdot 421^2 \cdot (-33) \pmod{493} \\
&\equiv 446^{19} \cdot 254 \cdot (-33) \pmod{493} \\
&\equiv (446^3)^6 \cdot 446 \cdot 254 \cdot (-33) \pmod{493} \\
&\equiv 200^6 \cdot (-47) \cdot 254 \cdot (-33) \pmod{493} \\
&\equiv 200^4 \cdot 200^2 \cdot (-47) \cdot 254 \cdot (-33) \pmod{493} \\
&\equiv 54 \cdot 67 \cdot (-47) \cdot 254 \cdot (-33) \pmod{493} \\
&\equiv 72 \pmod{493}
\end{aligned}
$$

$$
\begin{aligned}
3^{\text{o}} \text{ bloco} : D(207) &\equiv 207^{299} \pmod{493} \\
&\equiv (207^4)^{74} \cdot 207^3 \pmod{493} \\
&\equiv 285^{74} \cdot 180 \pmod{493} \\
&\equiv (285^4)^{18} \cdot 285^2 \cdot 180 \pmod{493} \\
&\equiv 103^{18} \cdot 373 \cdot 180 \pmod{493} \\
&\equiv (103^4)^4 \cdot 103^2 \cdot 373 \cdot 180 \pmod{493} \\
&\equiv 460^4 \cdot 256 \cdot 373 \cdot 180 \pmod{493} \\
&\equiv (460^2)^2 \cdot 256 \cdot 373 \cdot 180 \pmod{493} \\
&\equiv 103^2 \cdot 256 \cdot 373 \cdot 180 \pmod{493} \\
&\equiv 415 \pmod{493}
\end{aligned}
$$

O mesmo se aplica aos demais blocos, e ao final do processo tem-se: **252 - 72 - 415 - 22 - 102 - 9** como sequência numérica da mensagem já decodificada que, com auxílio da tabela de conversão inicial 4.1, desvenda-se a mensagem: **PROFMAT**.

4.4 Por que o RSA funciona e é seguro?

Vimos que para criptografar uma mensagem, é necessário conhecer os parâmetros n e e, que são parâmetros públicos de conhecimento de todos, onde $n = pq$ com p e q primos muito grandes. Já para decodificar uma mensagem precisamos dos parâmetros d e n. Mas para calcular d precisamos saber quem é $\varphi(n)$ e, para isso devemos fatorar n.

Embora pareça simples, na prática, esta etapa é totalmente inviável, já que não existem computadores nem algoritmos suficientemente bons que nos permita fatorar um número muito grande. Atualmente são as implementações comerciais usam chaves públicas que podem variar de 200 a 2467 algarismos.

> *"(...)o tempo necessário para fatorar um número de uns cem algarismos pelo método usual de tentativa é imenso, e excede, em muito, a idade estimada do universo. Entretanto, a afirmação que acabamos de fazer é muito mais forte: não existe nenhum algoritmo conhecido capaz de fatorar inteiros grandes de modo realmente eficiente. Na verdade, não se sabe nem mesmo se é possível*

que um tal algoritmo exista!" Coutinho *[2009]*

Para provar a eficiência desse método, precisamos comprovar que um bloco b de uma mensagem a ser codificada, que satisfaz $1 \leq b \leq n-1$, quando aplicado ao processo de decodificação volta ao bloco inicialmente gerado pela mensagem original, ou seja $D(C(b)) = b$. Precisamos mostrar que $D(C(b)) \equiv b \pmod{n}$. Mas antes ressaltamos a importância do uso do Pequeno Teorema de Fermat.

Teorema 4.6 (Pequeno Teorema de Fermat): Seja p um número primo e $a \in \mathbb{Z}$. Então $a^p \equiv a \pmod{p}$.

Demonstração:
Provaremos por indução sobre a. Para $a = 1$, temos $1 \equiv 1 \pmod{p}$.
Agora, suponhamos que $p|(a^p - a)$. Temos então:

$$\begin{aligned}(a+1)^p - (a+1) &= \binom{p}{0}a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a + \binom{p}{p} - (a+1) \\ &= a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1 - (a+1) \\ &= a^p - a + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1 - 1 \\ &= (a^p - a) + \sum_{k=1}^{p-1}\binom{p}{k}a^{p-k}\end{aligned}$$

Por hipótese de indução $p|(a^p - a)$ e, como $p|\binom{p}{k}$, para todo $1 \leq k \leq p-1$, segue que $p|[(a^p - a) + \sum_{k=1}^{p-1}\binom{p}{k}a^{p-k}]$ e, portanto $p|[(a+1)^p - (a+1)]$. Logo, $a^p \equiv a \pmod{p}$ para todo $a \in \mathbb{Z}$.

□

Corolário 4.7: Se n é um inteiro positivo e a e n são primos entre si, então

$$a^{\varphi(n)} \equiv 1 \pmod{n};$$

em que $\varphi(n) : \mathbb{Z}_+ \to \mathbb{Z}_+$ função de Euler definida por $\varphi(1) = 1$ e, para $n > 1, \varphi(n)$ é igual ao número de inteiros positivos menores que n e relativamente primos com n.

Demonstração:

Sejam $s_1, s_2, \cdots, s_k$ os inteiros de 1 a n, inclusive os extremos, que são primos com n (logo $k = \varphi(n)$). Dividamos cada as_i por n:

$$as_i = nq_i + r_i \ (0 \leq r_i < n).$$

Se existisse um primo p tal que $p|n$ e $p|r_i$, dessa igualdade decorreria que $p|as_i$. Mas então $p|a$ ou $p|s_i$, o que é impossível já que o $mdc(a, n) = 1$ (hipótese) e ainda $mdc(n, s_i) = 1$, devido à escolha dos s_i. Donde n e r_i são primos entre si, para todo $i, 1 \leq i \leq k$.

Mostremos agora que na sequência de restos $r_1, r_2, \cdots, r_k$ não há elementos repetidos. De fato, se $r_i = r_j$ $(1 \leq i, j \leq k;\ i \neq j)$, então $as_i - nq_i = as_j = nq_j$ e portanto $a(s_i - s_j) = n(q_i - q_j)$. Como $mdc(a, n) = 1$, então $n|(s_i - s_j)$. Como $1 \leq s_i, s_j \leq n$, então teríamos que ter $s_i = s_j$, o que não é possível, posto que $i \neq j$.

Disso tudo decorre então que $s_1, s_2, \cdots, s_k = r_1, r_2, \cdots, r_k$. Assim, se multiplicarmos as congruências $as_i \equiv 1 \pmod{n}$ decorrentes de $s_i = nq_i + r_i, (1 \leq i \leq k)$:

$$a^k s_1 s_2 \cdots s_k \equiv (as_1)(as_2) \cdots (as_k) \equiv r_1 r_2 \cdots r_k \pmod{n}$$

os produtos $s_1 s_2 \cdots s_k$ e $r_1 r_2 \cdots r_k$ que nela aparecem são iguais. Como n é primo com cada r_j (ou s_i) e, portanto, com o produto $r_1 r_2 \cdots r_k$, então esse produto pode ser cancelado na última congruência, resultado a tese:

$$a^{\varphi(n)} \equiv 1 \pmod{n};$$

pois $k = \varphi(n)$.

□

Para então demostrar que $D(C(b)) = b \pmod{n}$, por definição de D e C temos que

$$D(C(b)) \equiv (b^e)^d \equiv b^{ed} \pmod{n}. \tag{4.1}$$

Porém d é o inverso de e módulo $\varphi(n)$, logo $ed = 1 + k\varphi(n)$ para algum inteiro k. Como e e d são inteiros maiores que 2 e $\varphi(n) > 0$, então $k > 0$. Substituindo em (4.1)

$$b^{ed} \equiv b^{1+k\varphi(n)} \equiv (b^{\varphi(n)})^k b \pmod{n}.$$

Como $b^{\varphi(n)} \equiv 1 \pmod{n}$, temos que $b^{ed} \equiv b \pmod{n}$. Portanto

$$D(C(b)) \equiv b \pmod{n}$$

e a demonstração estaria completa se pudermos afirmar que $mdc(b,n) = 1$, mas isso nem sempre é verdade.

Para provar tal afirmação, lembremos que $n = pq$, no qual p e q são primos distintos e calcularemos a forma reduzida de b^{ed} módulo p e q. O cálculo é análogo para ambos os primos, logo basta executar um deles. Queremos, portanto, achar a forma reduzida de b^{ed} módulo p. Já sabemos que

$$ed = 1 + k\varphi(n) = 1 + k(p-1)(q-1),$$

logo

$$b^{ed} \equiv b \cdot (b^{p-1})^{(q-1)k} \pmod{p}.$$

Supondo que p não divide b, podemos usar o teorema de Fermat, sendo assim, $b^{p-1} \equiv 1 \pmod{p}$ e obtemos $b^{ed} \equiv b \pmod{p}$.

Se p divide b, então $b \equiv 0 \pmod{p}$ ou seja $D(C(b)) \equiv b \cdot (b^{p-1})^{(q-1)k} \equiv 0 \pmod{p}$. Analogamente, é possível mostrar que $D(C(b)) \equiv b \pmod{q}$ e como p e q são primos,

$$D(C(b)) \equiv b \pmod{n}.$$

□

Apenas isso já é suficiente, pois tanto $D(C(b))$ quanto b estão no intervalo que vai de 1 a $n-1$, logo serão congruentes módulo n só se forem iguais. Isto explica o fato de escolher $b < n$ no passo *(iii)* da pré-codificação, e justifica o fato de ser necessário manter os blocos separados, mesmo depois da codificação. Se não fosse assim, os blocos gerados seriam congruentes após a decodificação, mas não necessariamente iguais.

Exemplificando, de maneira prática, vamos imaginar a seguinte situação: Ana e Beatriz moram em estados diferentes e estão fazendo um investimento financeiro via *internet*. Frequentemente trocam informações sigilosas - contas bancárias, senhas, dados pessoais - que podem ficar suscetíveis à ameaça de um *hacker* ou intruso do mundo virtual. Pensando nisso, toda a comunicação é criptografada antes de ser enviada, e cada uma delas, com porte de suas respectivas chaves podem ler as mensagens sem grandes riscos.

Ana e Beatriz têm, cada uma delas, um par de chaves usadas para codificar e decodificar os textos que são trocados. Essas chaves são distintas porém se completam. Ambas tem uma chave que chamamos de pública (que é usada para codificar os textos por elas mesmas ou até por terceiros) e uma chave privada (de conhecimento apenas delas, usada para decodificar os textos recebidos).

Para que Ana envie uma mensagem à Beatriz, é necessário que ela faça as correspondências segundo a chave pública de Beatriz. Como a chave usada é pública, qualquer pessoa pode conhecer e usá-la para cifrar qualquer tipo de informação. Apenas Beatriz, que tem posse da chave privada pode realmente conhecer o conteúdo dessas mensagens, sejam recebidas por Ana ou não. O mesmo acontece para quando Beatriz quer enviar algum tipo de informação à Ana.

Aplicando o método RSA descrito ao longo deste capítulo, vamos supor que Ana queira enviar uma senha alfabética de seis letras para que Beatriz finalize uma transação bancária. A senha enviada será ***MATRIX***.

Conhecendo a chave pública de Beatriz $(n, e) = (143, 7)$ Ana começa seu trabalho:

(1º) : Converte a mensagem em uma sequência numérica conforme a tabela 4.1

$$M - A - T - R - I - X \Longrightarrow 22 - 10 - 29 - 27 - 18 - 33$$

(2º): Codifica a mensagem com a relação $C(b) \equiv b^e \pmod{n}$, onde b é o bloco gerado no passo anterior, que poderia ter sido reorganizado obedecendo a condição de que cada um deles fosse formado por um número menor que $n = 143$.

Aplicando as propriedades de congruência modular descritas pela Definição 3.7, para $C(b) \equiv b^e \pmod{n}$, temos:

1º bloco: $C(22) \equiv 22^7 \equiv 22 \pmod{143}$;

$2^{\underline{o}}$ bloco: $C(10) \equiv 10^7 \equiv 10 \pmod{143}$;

$3^{\underline{o}}$ bloco: $C(29) \equiv 29^7 \equiv 94 \pmod{143}$;

$4^{\underline{o}}$ bloco: $C(27) \equiv 27^7 \equiv 14 \pmod{143}$;

$5^{\underline{o}}$ bloco: $C(18) \equiv 18^7 \equiv 138 \pmod{143}$;

$6^{\underline{o}}$ bloco: $C(33) \equiv 33^7 \equiv 110 \pmod{143}$;

Sendo assim, a mensagem enviada por Ana será

$$22 \text{ - } 10 \text{ - } 94 \text{ - } 14 \text{ - } 138 \text{ - } 110$$

Recebida a mensagem, Beatriz, com sua chave privada $(n, d) = (143, 103)$ deve proceder com o processo inverso, ou seja, aplicar aos blocos enviados por Ana a relação de congruência $D(a) \equiv a^d \pmod{n}$. Sendo assim, temos:

$$\begin{aligned} 1^{\underline{o}} \text{ bloco} : D(22) &\equiv 64^{103} \pmod{143} \\ &\equiv (22^8)^{12} \cdot 22^7 \pmod{143} \\ &\equiv 55^{12} \cdot 22 \pmod{143} \\ &\equiv (55^4)^3 \cdot 22 \pmod{143} \\ &\equiv 55^3 \cdot 22 \pmod{143} \\ &\equiv 66 \cdot 22 \pmod{143} \\ &\equiv 22 \pmod{143} \end{aligned}$$

$$\begin{aligned} 2^{\underline{o}} \text{ bloco} : D(10) &\equiv 10^{103} \pmod{143} \\ &\equiv (10^8)^{12} \cdot 10^7 \pmod{143} \\ &\equiv 10^{12} \cdot 10 \pmod{143} \\ &\equiv (10^4)^3 \cdot 10 \pmod{143} \\ &\equiv 100^3 \cdot 10 \pmod{143} \\ &\equiv 1 \cdot 10 \pmod{143} \\ &\equiv 10 \pmod{143} \end{aligned}$$

$$\begin{aligned} 3^{\text{o}} \text{ bloco} : D(94) &\equiv 94^{103} \pmod{143} \\ &\equiv (94^5)^{20} \cdot 94^3 \pmod{143} \\ &\equiv 87^{20} \cdot 40 \pmod{143} \\ &\equiv (87^4)^5 \cdot 40 \pmod{143} \\ &\equiv 100^5 \cdot 40 \pmod{143} \\ &\equiv 133 \cdot 40 \pmod{143} \\ &\equiv 29 \pmod{143} \end{aligned}$$

$$\begin{aligned} 4^{\text{o}} \text{ bloco} : D(14) &\equiv 14^{103} \pmod{143} \\ &\equiv (14^8)^{12} \cdot 14^7 \pmod{143} \\ &\equiv 27^{12} \cdot 53 \pmod{143} \\ &\equiv (27^4)^3 \cdot 53 \pmod{143} \\ &\equiv 53^3 \cdot 53 \pmod{143} \\ &\equiv 27 \pmod{143} \end{aligned}$$

E assim Beatriz prosseguirá por todos os blocos até encontrar a sequência 22 - 10 - 29 - 27 - 18 - 33, que é a mesma originalmente gerada por Ana no início de sua cifragem. Com a mesma tabela de conversão usada por Ana, Beatriz conhece a senha recebida: MATRIX.

É importante ressaltar a eficiência desse método baseando-nos nos teoremas e propriedades descritas ao longo do capítulo. Nesse exemplo, as chaves usadas por Ana e Beatriz para se comunicarem não representam segurança alguma, visto que os parâmetros aplicados podem ser facilmente descobertos por alguém com o conhecimento da Teoria dos Números e suas aplicações ao assunto.

Por exemplo, um *hacker* disposto a invadir essa conversa que descrevemos seria capaz de descobrir a chave privada usada no processo a partir da chave pública divulgada por Beatriz. Veja:

Sendo $(n,e) = (143,7)$ a chave pública divulgada por Beatriz, é possível, a partir da fatoração do número 143, encontrar um produto de fatores primos que gera esse valor. Como $143 = 11 \cdot 13$, concluímos que $p = \mathbf{11}$ e $q = \mathbf{13}$.

De posse dos primos que geraram n, podemos usar a função fi de Euler para determinar os possíveis inteiros que são co-primos com n, ou seja, aqueles cujo máximo divisor comum com 143 é igual a 1.

$$\varphi(143) = (11-1)(13-1) = \mathbf{120}$$

Dentre esses valores, selecionamos um inteiro e que satisfaça a condição de o $mdc(e, \varphi(n)) = 1$ com $1 < e < \varphi(n)$. Neste caso Beatriz escolheu $e = 7$, que é o primeiro inteiro co-primo com 143, e assim definiu sua chave pública.

A escolha de e pode variar de acordo com a necessidade para assegurar o sigilo das mensagens. A cada nova conversa Beatriz pode escolher um novo parâmetro que defina sua chave pública. Sendo assim, se faz necessário, a cada nova escolha de e, que Beatriz defina uma nova chave privada. Ela é que possibilitará a leitura das mensagens recebidas.

Ainda a partir dos primos escolhidos e do valor definido para e, podemos descobrir a chave privada que desfaz o processo de encriptação feito pela chave pública. Para isso, basta definir um inteiro d, inverso de e módulo $\varphi(n)$, ou seja, $de \equiv 1 \pmod{\varphi(n)}$. Fazemos isso a partir da existência de um inverso multiplicativo que o satisfaz.

O algorítimo estendido de Euclides nos auxilia nos cálculos: como $7d \equiv 1 \pmod{143}$, isso corresponde dizer que $7d - 143y = 1$, daí

	17	7
120	7	1
1	0	

$1 = 120 - 17 \cdot 7$
$1 = 7 \cdot (-17) + 120 \cdot 1 \Rightarrow d = -17$ e $y = 1$.

Como $103 \equiv -17 \pmod{120}$ temos que $1 = 7 \cdot (103) - 120 \cdot 1$ é equivalente módulo 120. Logo, $d = 103$ é o inverso de e, e assim selecionamos um inteiro que compõe a chave privada.

Conhecendo as chaves, basta aplicar nas equações de congruência correspondentes as propriedades operatórias de potenciação que se completam nos caminhos de ida e volta no processo de criptografar um texto.

5

Aplicações em sala de aula

A matemática ao longo dos tempos trás consigo o rótulo de uma ciência difícil, de domínio de poucos. Desde o momento em que passa a ser vista como uma ciência do conhecimento, ainda na época de Pitágoras, era reservada para a uma classe privilegiada, o que a fez receber um status de nobreza que carrega até os dias atuais.

Por outro lado, o ensino da matemática é marcado por acumular grandes dificuldades e obstáculos quase intransponíveis que colocaram a disciplina na atual situação em que se encontra.

Ensinar matemática vai muito além de se aplicar fórmulas e regras, vai além de saber operar. A matemática exige um trabalho árduo na preparação para a interpretação de problemas, o raciocínio lógico e o pensamento crítico. Por conseguinte, o professor, como mediador do processo de ensino, tem papel fundamental nesse contexto.

Não há dúvidas de que hoje a matemática vem sendo melhor trabalhada nas escolas - até mesmo pelos recursos que estão à disposição do professor - comparada ao ensino técnico e pouco aplicável que se tinha numa época não tão distante da nossa. As tradicionais aulas de quadro e giz aos poucos dão lugar às tecnologias, que ganham lugar de destaque nas salas de aula.

Nesta nova forma de lidar com a disciplina enquanto conteúdo, o material concreto, a calculadora, os *softwares* de computador, aplicativos de celular e jogos educativos são ferramentas aliadas do trabalho do professor e têm papel fundamental na construção do conhecimento. Levar o aluno a compreender e aplicar a teoria trabalhada, em muitos casos, ajuda a combater a aversão pela matemática, resultado de uma caminhada de insucessos.

> *"O Ensino de Matemática costuma provocar duas sensações contraditórias, tanto por parte de quem ensina como por parte de quem aprende: de um lado, a constatação de que se trata de uma área importante do conhecimento; de outro, a insatisfação diante dos resultados negativos obtidos com muita frequência à sua aprendizagem". PCN [1998]*

Para Borin [2007], recursos como esses que citamos nas aulas de matemática:

> *"Tem papel importante no desenvolvimento de habilidades de raciocínio como organização, atenção e concentração, necessárias para o aprendizado, em espe-*

cial da Matemática (...) favorece o desenvolvimento da linguagem, criatividade e raciocínio dedutivo".

Com base nisso, este capítulo é destinado a apresentar algumas atividades aplicáveis em sala de aula que relacionam a criptografia associada à matemática para ser trabalhada com alunos de Ensino Médio. Algumas das propostas podem ser adaptadas para diferentes níveis de ensino e diferentes abordagens dentro do conteúdo trabalhado, que não seja especificamente o estudo da criptografia.

Vale ressaltar também que estas são atividades que abordam diretamente o uso da criptografia quando a teoria por trás delas já foi explora em sala de aula. Por isso, é interessante que o professor crie uma estratégia para garantir a evolução gradativa do conteúdo aplicando outras atividades de nível mais fácil, se necessário, para que o aluno se familiarize com os conceitos das quais a atividade depende e, por fim, consiga resolver as propostas.

Dentre as atividades propostas, algumas delas foram selecionadas para aplicação deste estudo. Os exercícios **5.1.2** (Quebrando o Código de César), **5.1.4** (Utilizando o Disco de Albert), **5.1.6** (A Criptografia e o uso de funções), **5.1.8** (Aplicando a Criptografia RSA) foram aplicados e seus resultados serão apresentados mais a diante.

5.1 Exercícios para aplicação

Exercício 5.1.1 (Filmes): O filme como recurso didático é uma maneira de transformar uma aula puramente teórica em uma aula voltada para a interação e socialização do conteúdo em sala de aula. Ele abre a possibilidade para que os alunos se insiram na construção do conhecimento, contribuindo assim para o enriquecimento do cotidiano escolar. Para o estudo de criptografia, dentre outras obras, temos:

Título: O Jogo Da Imitação
Diretor: Morten Tyldum
Lançamento: 05 de fevereiro de 2015
Gênero: Drama/ Biografia
Duração: 1h55min
Sinopse: A história acompanha a ascensão do cientista Alan Turing no mundo da tecnologia, quando seus conhecimentos inestimáveis em matemática, lógica e ciência da computação contribuíram com as estratégias usadas pelos Estados Unidos durante a Segunda Guerra Mundial. No entanto, a perseguição que sofreu por ser homossexual e os próprios conflitos internos o marcaram profundamente até o fim da vida.

Objetivo: Contextualizar o assunto de criptografia abordado em sala de aula, mostrando como uma equipe é capaz de quebrar os códigos gerados ela Enigma no contexto da Segunda Guerra Mundial.

Recursos didáticos: Sala ou instrumentos de multimídia.

Metodologia: Pode-se pedir um relato sobre o assunto discutido no filme, propor um roda de conversa para ressaltar os pontos fortes ou que despertaram mais a atenção dos alunos, para então introduzir o assunto que pretende ser trabalhado.

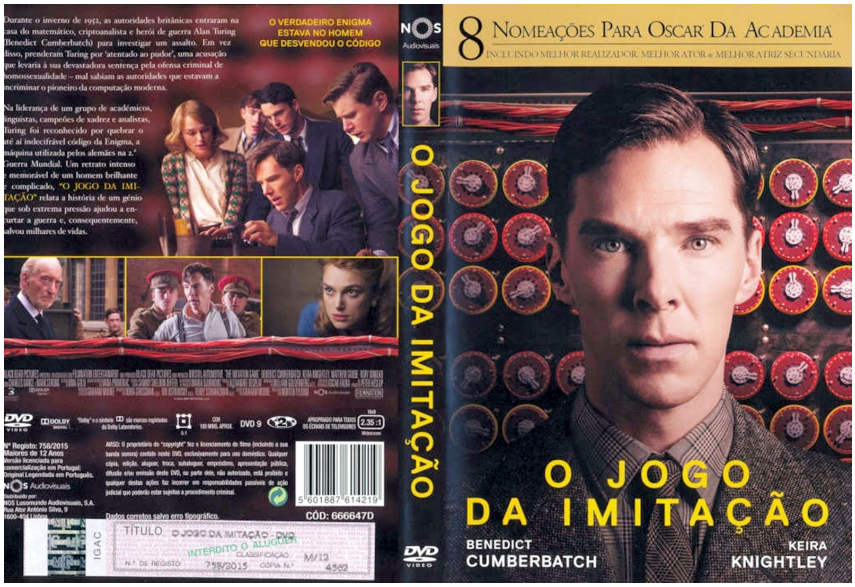


Figura 5.1: Filme: O Jogo da Imitação

Exercício 5.1.2 (Quebrando o código de César): O método de criptografia proposto por Júlio César (100-44 a.C) consistia na substituição das letras correspondentes ao texto original por outra obedecendo a um padrão nessa substituição, como já foi descrito no capítulo 2.

A principal desvantagem nesse processo proposto por César era que a mensagem era facilmente descoberta, mesmo não se conhecendo o padrão utilizado, isso graças a frequência observada nas letras que compõem a mensagem já cifrada.

Com base nisso nossa proposta consiste em decifrar a mensagem, tendo como referência a tabela que relaciona a frequência das letras do nosso alfabeto abaixo.

Descubra qual a mensagem criptografada a seguir usando o método de contagem de frequência com auxílio da tabela de conversão. Para facilitar os espaços entre as palavras foram mantidos.

GLCHU TXH QDR VH HQWHQGH PDWHPDWLFD
H XP DEVXUGR, SRUTXH YRFH H XP HAHPSOR PDWHPDWLFR.
QDR LPSRUWD VH QDR FRQVHJXH UHVROYHU XP ORJDULWPR,
LPSRUWD R TXDQWR YRFH H FDSDC
GH UHFRQKHFHU FRQFHLWRV PDWHPDWLFRV DR VHX UHGRU.
PDWHULDOLCH VHXV VRQKRV H
WHQKD FRUDJHP GH HASRU VXD
PDQHLUD GH HQFDUDU D UHDOLGADH. DPH D
WL PHVPR.
FDPLQKH VHP PHGR GH FDLU.
DSURYHLWH SRUTXH R PXQGR H PDWHPDWLFR

O texto acima é um trecho retirado do poema "A matemática é um determinante em sua vida" de Elaine Rodrigues (BA).

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

***Objetivo**:* Mostrar o funcionamento da cifra de César bem como sua ineficiência no processo de criptografar um texto.

Recursos didáticos: Lápis, borracha e folha contendo a atividade.

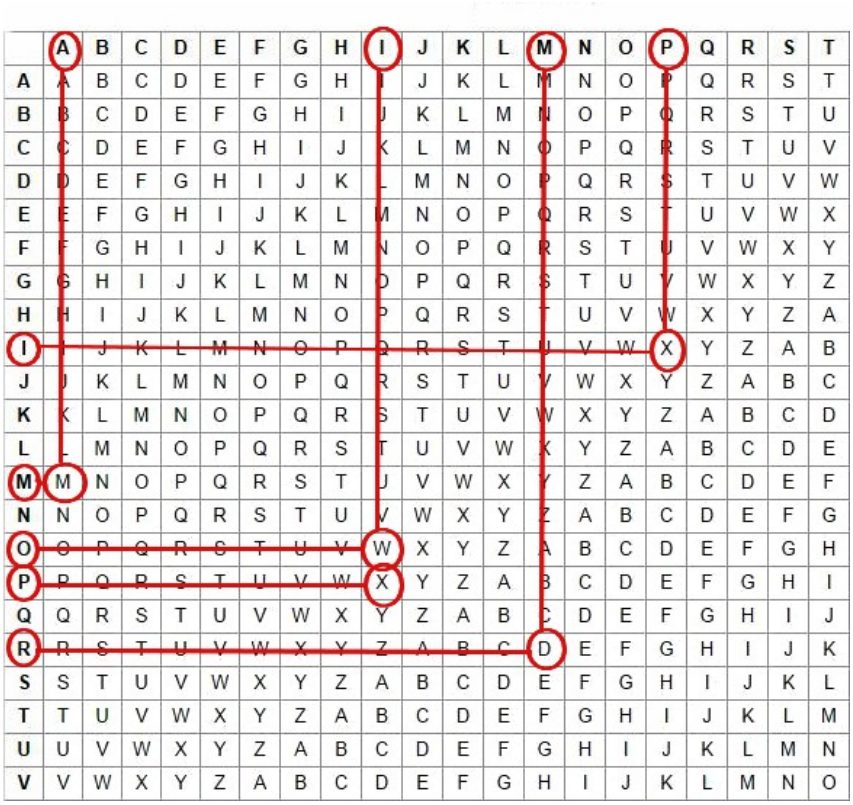
Metodologia: Esta atividade pode ser realizada individualmente ou em grupos, se for em grupos, orientar para que cada membro do grupo seja responsável por um conjunto de caracteres em sua contagem para agilizar o processo.

A atividade pode ser introduzida já nas primeiras séries dos anos finais do ensino fundamental, ou quando o professor já concluiu o conteúdo de porcentagem, pois a simples correspondência entre os deslocamentos entre os alfabetos usados no processo já são suficientes para sua execução.

Exercício 5.1.3 (Usando a Cifra de Vigenère): A cifra de Vigenère é um método de criptografia que usa uma série de diferentes cifras de César baseadas em letras de uma senha.

Por exemplo, como vimos no capítulo 3, usando este método, para cifrar a palavra PRIMO, precisaremos de uma chave - usaremos IMPA - e no quadro de Vigenère fazemos corresponder a primeira letra do texto com a primeira letra da chave, repetindo o processo para as demais letras. Veja:

$$\mathrm{P} + \mathrm{I} \Rightarrow \mathrm{X};\ \mathrm{R} + \mathrm{M} \Rightarrow \mathrm{D};\ \mathrm{I} + \mathrm{P} \Rightarrow X,\ \mathrm{M} + \mathrm{A} \Rightarrow M;\ \mathrm{O} + \mathrm{I} \Rightarrow \mathrm{W}$$



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

Figura 5.2: Correspondências por Vigenère

logo, PRIMO ⇒ XDXMW.

Conforme o método descrito para cifrar um texto, usando o quadro de Vigenère abaixo, crie uma chave para codificar a mensagem: **"Feliz Ano Novo"**

Chave usada na cifragem:

Agora que você já sabe como cifrar um texto a partir do quadro de Vigenère, usando a chave **TRIÂNGULO**, decifre o texto que segue:

XKMRAU Y EIWF IQHOFZ ENV LUEG OXO YIICNV XP GXXCQUM XOL TWM GGGLBAR QNGKHDWWRLE QLE QK KFS LV XEGXCQWVR M NRTBFAT WWRPG I CSLXITN.

Objetivo: Mostrar o uso da cifra de Vigenère na cifragem de um texto.

Recursos didáticos: Quadro de Vigenère impresso, lápis e borracha.

Metodologia: A atividade pode ser executada em grupos ou individual. Ela pode ser introduzida já em séries do ensino fundamental quando o professor introduz o estudo do plano cartesiano, uma vez que se pode associar as coordenadas de um ponto ao processo de substituição de um caractere.

	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

Exercício 5.1.4 (Utilizando o Disco de Albert): Leon Alberti foi o responsável pela criação deste método criptográfico com o intuito de melhorar a Cifra de César, já que agora a análise de frequência não era tão simples de se aplicar, uma vez que o mesmo caractere era substituído em momentos diferentes por caracteres diferentes.

Para iniciar faremos a construção do disco com cartolina a partir do molde.

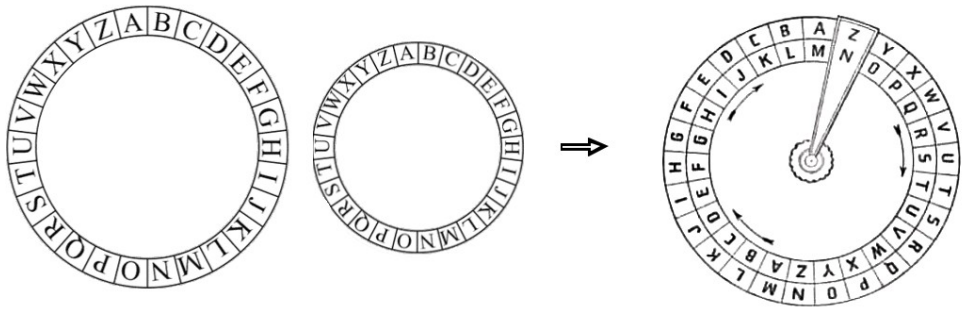


Figura 5.3: Molde para construção do disco de Alberti

Para criptografar usando o Disco de Alberti, é preciso que se escolha uma chave (usaremos a letra k neste exemplo). Posicionando o disco central (de onde retiramos a mensagem

cifrada) com a letra K sob a letra A do disco fixo (disco maior) temos a correspondência entre as letras estabelecida. Basta que se faça as devidas substituições. Sendo assim, com a chave k, a palavra **"FRAÇÃO"** teria a forma **"rmalgy"** já criptografada.

Esta é apenas uma pequena variação, mais simples, do método de Alberti, seu objetivo agora é escolher uma chave para codificar a frase:

"Ajuda seu semelhante a levantar a carga, mas não a levá-la." – Pitágoras.

Crie um pequeno texto a partir de uma chave à sua escolha. Em seguida troque a atividade com um colega e tente decifrar a mensagem por ele criada.

Texto cifrado: *(escreva aqui o seu texto já cifrado)*

Texto decifrado: *(este espaço será preenchido pelo colega que vai decifrar o seu texto)*

Chave usada na cifragem:

Objetivo: Mostrar o funcionamento da cifra do Disco de Alberti e como criptografar um texto a partir dele.

Recursos didáticos: Lápis, borracha e discos para manuseio dos alunos.

Metodologia: A sugestão é que esta atividade seja feita em grupos, cada grupo recebe um disco e uma mensagem para cifrar, depois disso trocam-se as mensagens já cifradas para que o outro grupo a decifre.

Esta também é uma atividade que pode ser desenvolvida em várias etapas do ensino, pois não há nenhum conceito explorado que dificulta sua realização.

Exercício 5.1.5 (O uso da Combinatória na Criptografia): As cifras de transposição tiveram sua importância para história da criptografia. Nesta atividade poremos em prática um pouco dessa técnica, a partir da definição de permutação.

Definição 5.1 (Permutação): Dado um conjunto A tal que $\#A = n$, o número de modos distintos de ordenar todos os n elementos do conjunto A chama-se permutação. Pelo princípio multiplicativo, o total de permutação de n elementos é $n!$.

1) Em uma brincadeira na escola, Arnaldo mandou à Bruna um bilhete enigmático no qual ele escreveu **"GOSTO DE VOCÊ"**, mas as letras da mensagem estavam todas embaralhadas. Pensando nas maneiras que Arnaldo pode escolher para criar essa mensagem responda aos itens:

a) Quantas são as maneira de se embaralhar as letras da palavra GOSTO?

b) Quantas e quais são as maneiras de se embaralhar as letras da palavra VOCÊ?

c) De quantas maneiras Arnaldo poderia ter escrito o bilhete à Ana pensando agora em todas as letras do texto?

2) Ao final de uma prova de matemática havia o seguinte lembrete: **"TEORASBO!"**. Qual é a mensagem decifrada?

3) Em um jogo de codificar mensagens são definidas para uso apenas as letras A, E, I, O, U. Pensando nisso liste todas as chaves possíveis para cifrar um texto iniciadas com a letra A, e responda:

a) Quantas delas não criptografam texto nenhum?

b) Quantas são as chaves possíveis sem a condição de ter o A na posição inicial?

c) Se nesse jogo as letras da palavra **"COLEGIAL"** fossem usadas para a composição das chaves de codificação, quantas delas seriam formadas?

Objetivo: Aplicar o conteúdo de Análise Combinatória ao estudo de criptografia.

Recursos didáticos: Lápis e borracha.

Metodologia: A atividade pode ser executada em grupos ou individual. Ela pode ser introduzida a partir do momento em que se introduz a ideia de formação de anagramas.

Exercício 5.1.6 (A Criptografia e o uso de funções): Nesta atividade vamos propor a resolução do exemplo 3.1.2 apresentado quando discutimos o uso das funções de mais variáveis no processo de cifragem de um texto.

A partir da função:

$$f(x) = \begin{cases} x + 12, \text{ se } 0 \leq x \leq 13 \\ x - 14, \text{ se } 13 < x \leq 25 \end{cases}$$

Usaremos a tabela de conversão 3.1 e o passo a passo a seguir para criptografar **"A vida é um eco."**

Com essa função conhecemos a quantidade de deslocamentos que serão feitos no momento da cifragem, nesse caso, como $L = 12$, cada letra deve se deslocar 12 posições. Sendo assim:

(Passo 1): Converter a mensagem em uma sequência numérica.

(Passo 2): Aplicar em f os valores encontrados no passo anterior para gerar uma nova sequência numérica, com base na tabela de conversão.

A cada novo valor associa-se uma letra, tendo assim o texto cifrado.

Para descriptografar o texto **"Pq a eqg yqxtad. Ea ueea"**, usando a mesma técnica, temos:

(Passo 1): Encontrar a função inversa de f, que neste caso será

$$f^{-1}(x) = \begin{cases} x - 12, \text{ se } 13 < x \leq 25 \\ x + 14, \text{ se } 0 \ \leq x \leq 13 \end{cases}$$

(Passo 2): Aplicar em f^{-1} os valores encontrados no passo anterior. Essa sequência deve ser a mesma inicialmente gerada, e a ela corresponde o texto original. Sempre que uma imagem passar de 25, volte ao início da tabela. A cada novo valor associa-se uma letra, tendo assim o texto decifrado.

Objetivo: Mostrar o uso das funções para criptografar um texto.

Recursos didáticos: Lápis e borracha.

Metodologia: A sugestão é que esta atividade seja feita em grupos, cada grupo recebe uma função e uma mensagem para cifrar, depois disso, trocam-se as mensagens já cifradas para que o outro grupo a decifre.

O conceito de função, domínio, imagem, já devem ser claros no momento da atividade. Em séries a partir do nono ano do ensino fundamental e ensino médio já podem ser trabalhas atividades como essa.

Exercício 5.1.7 (Criptografando com Matrizes): O processo de cifragem de um texto por matriz depende primeiramente de que a matriz escolhida para ser a chave da cifra tenha inversa, ou seja, satisfaça a condição de que $AB = BA = I_n$, em que I_n é a matriz identidade. A matriz B é chamada de inversa de A ($B = A^{-1}$).

Sendo assim, tomando a matriz $A_{3\times3} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 3 & 1 \\ 1 & 2 & 0 \end{bmatrix}$ como chave para sua cifra, faça as correspondências necessárias a partir da tabela de conversão abaixo e criptografe a frase **"O segredo da criatividade é saber como esconder as fontes."** - Albert Einstein.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
1	2	3	4	5	6	7	8	9
J	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**
10	11	12	13	14	15	16	17	18
S	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	
19	20	21	22	23	24	25	26	27

Repare que os caracteres do texto não se quantificam em um múltiplo de três, sendo assim, não se esqueça de completar a sequência para que seja possível criar uma matriz de três linhas.

Agora, a partir da matriz B, inversa de A, decifre o texto representado pela matriz

$$C_{8\times 3} = \begin{pmatrix} 7 & 15 & 19 & 20 & 5 & 27 & 4 & 5 \\ 93 & 29 & 67 & 65 & 13 & 104 & 86 & 81 \\ 61 & 21 & 49 & 38 & 7 & 65 & 58 & 43 \end{pmatrix}$$

Objetivo: Aplicar a multiplicação de matrizes no estudo da Criptografia.

Recursos didáticos: Lápis e borracha.

Metodologia: A atividade pode ser realizada tanto por grupos ou de forma individual. É importante que o conceitos de matriz e suas operações já tenham sido trabalhados com os alunos. Calculadoras *on-line* para os produtos de matrizes e/ou determinação de inversas podem ser explorados se o objetivo do professor for estritamente a aplicação do método discutido.

Este trabalho pode ser realizado com alunos a partir da segunda série do ensino médio, faixa etária em que se trabalham, geralmente, os conceitos de matrizes.

Exercício 5.1.8 (Aplicando a Criptografia RSA): Nesta atividade colocaremos em prática um dos método criptográficos que já provamos ser um dos mais eficientes dentre os conhecidos até hoje: o RSA.

Com o passo a passo a seguir, criptografe a mensagem **"BOA NOITE"**, usando os primos p**=5** e q **= 7**. Para facilitar, os espaços entre as palavras foram mantidos. Durante o processo, identifique as chaves usadas para codificar e decodificar o texto.

(Passo 1): Converter a mensagem em uma sequência numérica conforme a tabela

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

(Passo 2): Determinar o parâmetro $n = p \cdot q$, sendo p e q conhecidos.

(Passo 3): Calcular $\varphi(n)$.

(Passo 4): Determinar o parâmetro e de tal forma que $mdc(e, \varphi(n)) = 1$ com $1 < e < \varphi(n)$.

Para facilitar pode-se usar $e = 3$.

(Passo 5): Quebrar a mensagem em blocos de tamanho $M < n$.

(Passo 6): Codificar a mensagem com a relação $C(b) \equiv b^e \pmod{n}$, onde b é o bloco gerado no passo anterior

Vale lembrar que a chave pública, determinada pelos parâmetros encontrados no passo 2 e 4 são de conhecimento de todos. A chave privada (usada para descriptografar) é de conhecimento apenas daqueles a quem se direciona a mensagem. Agora, faça o processo contrário para descriptografar a mensagem seguindo o passo a passo:

(Passo 1): Determinar d, inverso de e módulo $\varphi(n)$, ou seja, $de \equiv 1 \pmod{\varphi(n)}$.

(Passo 2): Decodificamos a mensagem de acordo com a relação $D(a) \equiv a^d \pmod{n}$, aplicando-a em cada bloco encontrado no final da cifragem.

(Passo 3): Substituir cada bloco numérico por seu correspondente na tabela 4.1 e ler a mensagem.

Objetivo: Trazer ao conhecimento dos alunos o mecanismo por trás da criptografia que é responsável pelo sigilo dos principais elos entre empresas e usuários, ou contato entre pessoas via *internet*.

Recursos didáticos: Lápis, borracha e papel com as principais orientações e passo a passo dos processos de cifragem e deciframento do texto proposto.

Metodologia: Aula expositiva explicando o funcionamento do método RSA. No momento da atividade é sugerido que se façam dois grupos para que um fique responsável pela cifragem e o outro pelo deciframento do texto proposto. O professor deve ser peça importante no passo a passo com esses alunos, para que façam os cálculos corretos e não prejudique o desenrolar da atividade.

A atividade se baseia a todo momento em teoremas e definições que não são tema do currículo de matemática no ensino regular, mas suas aplicações podem sim ser postas em prática por alunos desta faixa etária. A séries finais do ensino médio garantem um melhor resultado, pois subentende-se que até ali, os alunos já tenham bagagem suficiente para entender e realizar a atividade.

Exercício 5.1.9 (A criptografia RSA e a Cifra de César ONLINE): Esta atividade é uma variação dos exercícios acima que tratam da Cifra de César e o método RSA. Ambas possuem endereços eletrônicos que fazem o processo de codificação e decodificação, basta introduzir o texto a ser cifrado e escolher as chaves que farão as conversões.

Objetivo: Aplicar na prática os métodos estudados em teoria, aproximando o aluno da realidade dos processos de criptografia aos quais convivem, muitas as vezes sem conhecimento.

Recursos didáticos: Preferencialmente um laboratório de informática com acesso à *internet*.

Metodologia: Como na aula teórica, a sugestão é que a atividade seja feita em grupos. Um responsável pelo processo de ida e outro pelo processo de volta no método de cifragem escolhido.

Agora, como a praticidade da *internet* é aliada dos alunos, os textos propostos para a atividade podem ser maiores.

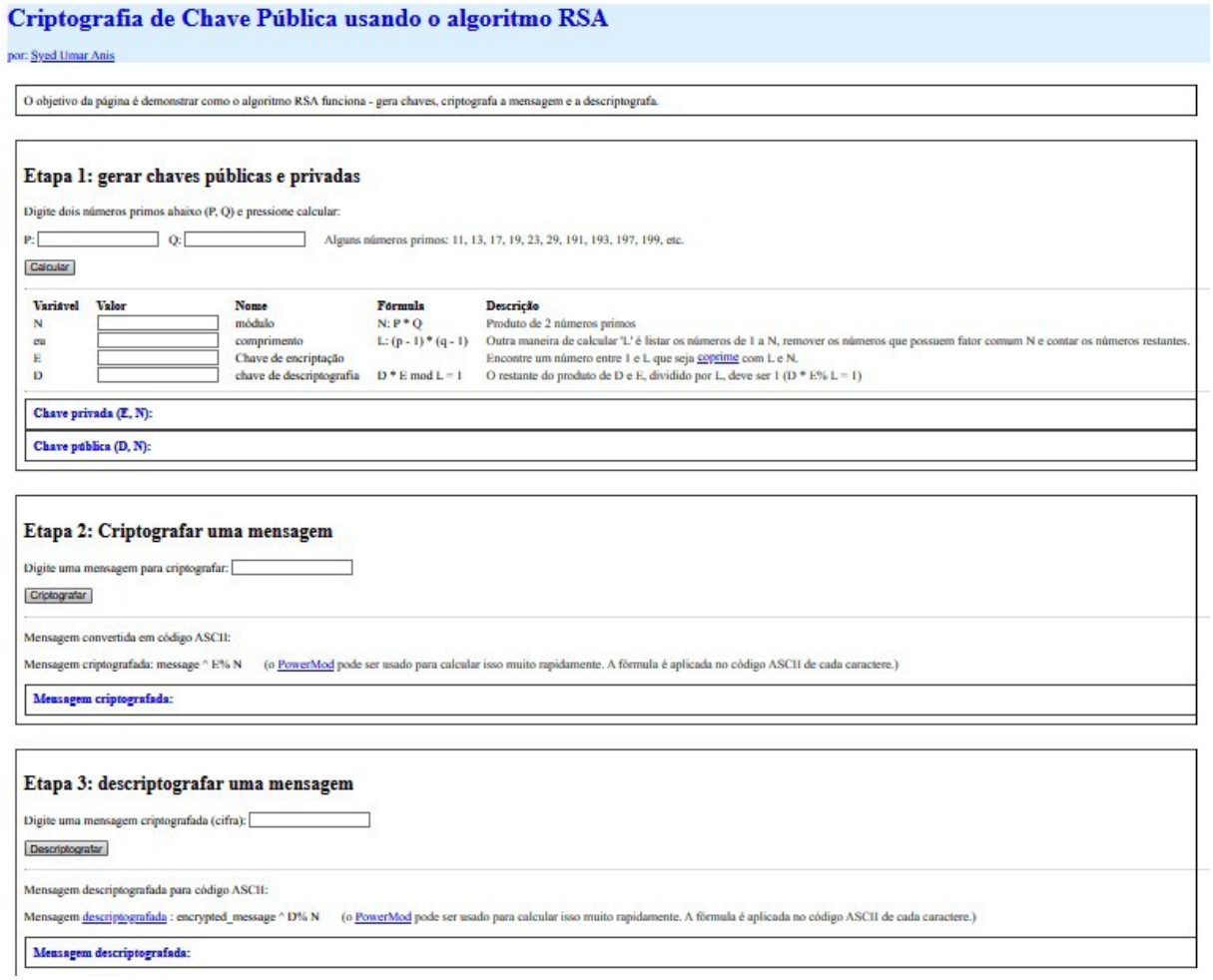


Figura 5.4: A criptografia RSA ONLINE ANIS

Figura 5.5: A cifra de César ONLINE IBICT

5.2 Resultados das aplicações

Após realizadas e discutidas trazemos aqui os resultados e as conclusões obtidos para cada uma das atividades propostas. A aplicação foi voltada para alunos do Ensino Médio, mas em uma das atividades houve também a participação de alunos do Ensino Fundamental.

As aplicações aconteceram em dois momentos, com turmas e escolas diferentes. A primeira aplicação foi feita com alunos do oitavo ano do Ensino Fundamental, de uma escola estadual, no município de Onça de Pitangui, Minas Gerais e a segunda com alunos do terceiro ano do Ensino Médio de uma escola particular de Pitangui, Minas Gerais.

Para ambas aplicações os alunos foram convidados e elas aconteceram nos respetivos contraturnos. Na primeira houve a participação de aproximadamente 10 alunos da turma em questão, na segunda, na qual escolhi trabalhar as técnicas mais elaboradas dos métodos descritos, estavam presentes aproximadamente 15 alunos e o professor regente dessa turma, que me auxiliou no decorrer das atividades.

Para introduzir o assunto, os alunos, em ambos os momentos, conheceram um pouco da origem e história da criptografia até os dias atuais por meio de vídeos e guiados pela teoria discutida neste trabalho.

Em todas as atividades, quando necessário, o uso da calculadora foi feito para facilitar e agilizar os cálculos.

Quebrando o código de César

Esta atividade foi realizada por dois grupos, sua duração foi de aproximadamente 50 minutos. A falha dos alunos na sua realização foi a organização do grupo para contagem das letras e levantamento das frequências, por se tratar de um texto relativamente longo. Mas logo se fez simples quando descobriram a chave que representava a transposição das letras do alfabeto.

Vale ressaltar que quanto maior o texto a ser decifrado, melhor serão as aproximações correspondentes às letras do texto com suas frequências na língua original, como mostrado na tabela apresentada no exercício.

Utilizando o Disco de Alberti

Esta atividade foi a realizada com a turma de oitavo ano do Ensino Fundamental, de forma individual. Sua duração foi de aproximadamente 50 minutos. Nesta turma, os próprios alunos construíram o disco de Alberti que usariam na atividade. Manipular o disco e guiar a codificação por ele deixou alguns alunos confusos, mas os próprios alunos se ajudaram, e por fim conseguiram finalizar a atividade sem grandes dificuldades.

A Criptografia e o uso de funções

Esta atividade foi realizada por grupos de alunos e também individual. Sua duração foi de aproximadamente 30 minutos. Apesar das funções trabalhadas já serem dadas pelo exercício, os conceitos de domínio, imagem e função inversa para mais de uma sentença foram abordados para introduzir a atividade. Alguns alunos concluíram a atividade em menos tempo e serviram de monitores, juntamente com o professor da turma e eu.

Aplicando a Criptografia RSA

Esta era a atividade de maior expectativa dentre as propostas, uma vez que os assuntos nela abordados estão fora do universo das escolas de nível médio.

A introdução ao exercício foi feita de forma simples, ressaltando a importância do uso dos números primos na criptografia RSA, e ainda, mostrando apenas a aplicação dos principais teoremas que são usados. É importante ressaltar que, assuntos como a aritmética modular, por exemplo, necessários para o desenrolar da atividade, foram expostos de maneira simples e com exemplos os alunos entenderam a ideia central (encontrar números com mesmo resto em uma divisão) desses teoremas.

Nesta etapa da aplicação a orientação aos grupos que desenvolveram a atividade foi maior, e seu tempo de duração foi de aproximadamente uma hora. As dificuldades no decorrer da atividades estavam ligadas principalmente às congruências. Os erros de notação apresentados não foram evidenciados, uma vez que eles não influenciaram no desenrolar e compreensão da atividade. De modo geral, a maioria dos alunos conseguiu concluir a atividade com êxito.

Ao concluir esta mesma atividade foi apresentado aos alunos os endereços eletrônicos que fazem tanto criptografias do tipo RSA como as que fazem transposições usando a

Cifra de César online.

As demais atividades apresentadas neste capítulo servem de norte para uso do professor e aplicação em suas aulas.

A CRIPTOGRAFIA COMO RECURSO DIDÁTICO NO ENSINO MÉDIO

Atividade 1: Quebrando o código de César

O método de criptografia proposto por Júlio César (100-44 a.C) consistia na substituição das letras correspondentes ao texto original por outra obedecendo a um padrão nessa substituição. A principal desvantagem nesse processo proposto por César era que a mensagem era facilmente descoberta, mesmo não se conhecendo o padrão utilizado, isso graças a frequência observada nas letras que compõem a mensagem já cifrada. Com base nisso a nossa proposta consiste em decifrar a mensagem, tendo como base uma tabela que relaciona a frequência das letras do nosso alfabeto:

Descubra qual a mensagem criptografada a seguir usando o método de contagem de frequência com auxílio da tabela ao lado. Para facilitar os espaços entre as palavras foram mantidos.

A	14,64%	J	0,40%	S	7,81%
B	1,04%	K	0,02%	T	4,43%
C	3,88%	L	2,78%	U	4,64%
D	4,10%	M	4,75%	V	1,70%
E	12,57%	N	5,05%	W	0,01%
F	1,02%	O	10,73%	X	0,21%
G	1,30%	P	1,20%	Y	0,01%
H	1,28%	Q	2,52%	Z	0,01%
I	6,18%	R	6,53%		

GLCHU TXH QDR VH HQWHQGH PDWHPDWLFD
H XP DEVXUGR, SRUTXH YRFH H XP HAHPSOR
PDWHPDWLFR.
QDR LPSRUWD VH QDR FRQVHJXH UHVROYHU XP
ORJDULWPR,
LPSRUWD R TXDQWR YRFH H FDSDC
GH UHFRQKHFHU FRQFHLWRV PDWHPDWLFRV DR VHX UHGRU.
PDWHULDOLCH VHXV VRQKRV H
WHQKD FRUDJHP GH HASRU VXD
PDQHLUD GH HQFDUDU D UHDOLGGH. DPH D
WL PHVPR.
FDPLQKH VHP PHGR GH FDLU.
DSURYHLWH SRUTXH R PXQGR H PDWHPDWLFR

G.10 W:18
L.1512 P:25
C.1. F:14
H:14 J:1
V:18 A:1.
T:3. Y:3.
X:12 E:1
Q.12
D:28
R.31
V:11

b
• dizer que não se entende matemática é um absurdo, porque você é um exemplo matemático
Não importa se não consegue resolver um logaritmo, importa o quanto você é capaz de se conhecer conceitos matemáticos ao seu redor.
Materialize seus sonhos e tenha coragem de expor sua maneira de encarar a realidade. Ame e ti mesmo.
Caminhe sem medo de cair.
Aproveite porque o mundo é matemático.

D B C D
1 1 1 1
A E F G

103
+19
+69
251
-30
221

Figura 5.6: Atividade 1

CRIPTOGRAFIA
COMO RECURSO DIDÁTICO NO ENSINO MÉDIO

Atividade 2: Utilizando o Disco de Alberti

Leon Alberti foi o responsável pela criação deste método criptográfico com o intuito de melhorar a Cifra de César, já que agora a análise de frequência não era tão simples de se aplicar, uma vez que o mesmo caractere era substituído em momentos diferentes por caracteres diferentes.

Para criptografar usando o Disco de Alberti, é preciso que se escolha uma chave (usaremos a letra k neste exemplo). Posicionando o disco central (de onde retiramos a mensagem cifrada) com a letra K sob a letra A do disco fixo (disco maior) temos a correspondência entre as letras estabelecida. Basta que se faça as devidas substituições. Sendo assim, com a chave k, a "FRAÇÃO" teria a forma "rmalgy" já criptografada.

Esta é apenas uma pequena variação do método de Alberti, seu objetivo agora é escolher uma chave para codificar a frase: **"Ajuda seu semelhante a levantar a carga, mas não a levá-la."** – Pitágoras.

"OXIRO GSI GSASZVOBHS O ZSJOBHOF O QOFUO,
AOG BOC O ZSJO-ZO." chave A/O

Crie um pequeno texto a partir de uma chave à sua escolha. Em seguida troque a atividade com um colega e tente decifrar a mensagem por ele criada.

Texto cifrado: (escreva aqui o seu texto já cifrado)

"DYNK KMKY DOW CEK BOKSKY"

Texto decifrado: (este espaço será preenchido pelo colega que vai decifrar o seu texto)

"Toda ação tem uma reação!"

Chave usada na cifragem: A/K

Figura 5.7: Atividade 2

A CRIPTOGRAFIA
COMO RECURSO DIDÁTICO NO ENSINO MÉDIO

Atividade 3: A Criptografia e o uso de funções

A partir da função: $f(x) = \begin{cases} x + 12, \text{ se } 0 \leq x \leq 13 \\ x - 14, \text{ se } 13 < x \leq 25 \end{cases}$

Usaremos a tabela de conversão e o passo a passo a seguir para criptografar **"A vida é um eco."**

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

Passo 1: Converter a mensagem em uma sequência numérica.

0, 21, 8, 3, 0, 4, 20, 12, 4, 2, 14

Passo 2: Aplicar em f os valores encontrados no passo anterior para gerar uma nova sequência numérica, com base na tabela de conversão.

$f(0) = 0 + 12 = 12$
$f(21) = 21 - 14 = 7$
$f(8) = 8 + 12 = 20$
$f(3) = 3 + 12 = 15$
$f(0) = 0 + 12 = 12$
$f(4) = 4 + 12 = 16$
$f(20) = 20 - 14 = 6$

$f(12) = 12 + 12 = 24$
$f(4) = 4 + 12 = 16$
$f(2) = 2 + 12 = 14$
$f(14) = 14 - 14 = 0$

A cada novo valor associa-se uma letra, tendo assim o texto cifrado. MHUPMQGYQOA

Para descriptografar o texto "**Pq a eqg yqxtad. Ea ueea**", usando a mesma técnica, temos:

Passo 1: Encontrar a função inversa de f, que neste caso será $f^{-1}(x) = \begin{cases} x - 12, \text{ se } 13 < x \leq 25 \\ x + 14, \text{ se } 0 \leq x \leq 13 \end{cases}$

Passo 2: Converter a mensagem criptografada em uma sequência.

15, 16, 0, 4, 16, 6, 24, 16, 23, 19, 0, 3, 4, 0, 20, 4, 4, 0

Passo 3: Aplicar em f^{-1} os valores encontrados no passo anterior. Essa sequência deve ser a mesma inicialmente gerada, e a ela corresponde o texto original. Sempre que uma imagem passar de 25, volte ao início da tabela.

$f^{-1}(15) = 15 - 12 = 3$
$f^{-1}(16) = 16 - 12 = 4$
$f^{-1}(0) = 0 + 14 = 14$
$f^{-1}(4) = 4 + 14 = 18$
$f^{-1}(16) = 16 - 12 = 4$
$f^{-1}(6) = 6 + 14 = 20$

$f^{-1}(24) = 24 - 12 = 12$
$f^{-1}(16) = 16 - 12 = 4$
$f^{-1}(23) = 23 - 12 = 11$
$f^{-1}(19) = 19 - 12 = 7$
$f^{-1}(0) = 0 + 14 = 14$
$f^{-1}(3) = 3 + 14 = 17$
$f^{-1}(4) = 4 + 14 = 18$

$f^{-1}(0) = 0 + 14 = 14$
$f^{-1}(20) = 20 - 12 = 8$
$f^{-1}(4) = 4 + 14 = 18$
$f^{-1}(4) = 4 + 14 = 18$
$f^{-1}(0) = 0 + 14 = 14$

A cada novo valor associa-se uma letra, tendo assim o texto decifrado. Até o meu melhor vai voar.

Figura 5.8: Atividade 3

CRIPTOGRAFIA
COMO RECURSO DIDÁTICO NO ENSINO MÉDIO

Atividade 4: Aplicando a Criptografia RSA

Nesta atividade poremos em prática o método criptográfico que já provamos ser o mais eficiente dentre os conhecidos até hoje: o RSA. Usando o passo a passo a seguir, criptografe a mensagem **BOA NOITE**, usando os primos $p = 5$ e $q = 7$. Para facilitar os espaços entre as palavras foram mantidos.

Passo 1- Converter a mensagem em uma sequência numérica conforme a tabela

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

11 24 10 23 24 18 29 14

Passo 2 –Determinar o parâmetro $n = p.q$, sendo p e q conhecidos. $N = 5.7 = 35$

Passo 3 - Calcular $\varphi(n)$=(p-1)(q-1)

$(5-1).(7-1) = 24$

Passo 4 – Determinar o parâmetro e de tal forma que $(e, \varphi(n)) = 1$ com $1 < e < \varphi(n)$. Para facilitar pode-se usar $e = 5$.

Passo 5 – Quebrar a mensagem em blocos de tamanho $M < n$.

11 - 2 - 4 - 10 - 2 - 32 - 4 - 18 - 29 - 14

Passo 6 – Codificar a mensagem com a relação $C(b) \equiv b^e \ (mod\ n)$, onde b é o bloco criado no passo anterior

$C(11) \equiv 11^5 \equiv 16 \pmod{35}$
$C(2) \equiv 2^5 \equiv 32 \pmod{35}$
$C(10) \equiv 10^5 \equiv 5 \pmod{35}$
$C(32) \equiv 32^5 \equiv 2 \pmod{35}$
$C(4) \equiv 4^5 \equiv 9 \pmod{35}$
$C(18) \equiv 18^5 \equiv 23 \pmod{35}$
$C(29) \equiv 29^5 \equiv 29 \pmod{35}$
$C(14) \equiv 14^5 \equiv 14 \pmod{35}$

16 - 32 - 9 - 5 - 32 - 2 - 9 - 23 - 29 - 14

Figura 5.9: Atividade 4

Agora, faça o processo contrário para descriptografar a mensagem seguindo o passo a passo:

Passo 1 – Determinar d, inverso de e modulo φ(n), ou seja, $de \equiv 1(mod\ \varphi(n))$.

$5 \cdot d = 1 \bmod 24 \qquad 5 \cdot 5 \equiv 1 \bmod 24 \qquad d = 5$

Passo 2 – Decodificamos a mensagem de acordo com a relação $D(a) \equiv a^d (mod\ n)$, aplicando em cada bloco a encontrado ao final da cifragem

$16^5 \pmod{35} = 11$
$32^5 \pmod{35} = 2$
$9^5 \pmod{35} = 4$
$5^5 \pmod{35} = 10$
$2^5 \pmod{35} = 32$

$32^5 \pmod{35} = 2$
$9^5 \pmod{35} = 4$
$23^5 \pmod{35} = 18$
$29^5 \pmod{35} = 29$
$14^5 \pmod{35} = 14$

Passo 3 – Substituir cada bloco numérico por seu correspondente na tabela e ler a mensagem.

11 24 10 32 24 18 29 14 → Boa noite.

Figura 5.10: Atividade 4

6

Conclusões

A criptografia se fez presente e necessária a partir do momento em que o homem sente a necessidade de proteger suas informações. Por sua história conseguimos acompanhar sua evolução e os principais fatores sociais responsáveis por esse progresso.

Das simples, porém inteligentes formas de se camuflar a existência de um texto pela esteganografia aos algorítimos que sustentam a base da criptografia avançada, percorremos um período de crescimento para a matemática de grande importância para não só os métodos criptográficos aqui descritos, mas para toda estrutura do conhecimento matemático.

Um artifício que deixa de ser exclusividade dos poderes públicos em situação de combate e passa a ser requisito básico no dia a dia da humanidade, a criptografia foi aqui trabalhada de modo a despertar no leitor, professor atuante no ensino de matemática, a inspiração para usar em suas aulas esse assunto tão pouco discutido no ensino regular.

O processo que envolve a construção do conhecimento matemático na atual situação da educação brasileira, principalmente nas escolas públicas, encontra-se em defasagem por diversos fatores que não vem ao caso aqui citar. Fato é que, a cada dia perdemos ainda mais o interesse dos alunos nesse processo, e consequentemente se constrói uma rejeição ao conteúdo, raramente reversível.

Nesse contexto está o professor e sua inquestionável responsabilidade em ser mediador do conhecimento que chega até os alunos. Perante essa situação, o professor por muitas das vezes precisa se desdobrar, ser criativo, inovar nas alternativas de como despertar e incentivar o gosto pela matemática além de ressaltar sua importância.

Esse trabalho procurou, de forma prática, demonstrar como o conhecimento matemático está difundido em assuntos do nosso dia a dia, como na criptografia, e como o professor pode usar desse artifício para criar estratégias em sala de aula, na busca de aplicar os conteúdos trabalhados, diversificar suas aulas e resgatar o interesse do aluno pela disciplina.

A história da criptografia deixa claro o quão necessária a matemática se fez para sua própria evolução, e ressaltar esse aspecto histórico para o aluno pode despertar a curiosidade e dar sentido ao estudo dos conceitos que serão abordados. A prática de cada um dos métodos criptográficos citados, e tantos outros que não foram mencionados aqui, maquiam a formalidade e rigor do conteúdo, fazendo assim as aulas ministradas pelo professor menos cansativas.

Com as atividades propostas e aplicadas, pode-se perceber, por parte dos alunos, que há simpatia pela matemática quando se propõe uma atividade que lhes despertam a curiosidade. Sendo assim, se torna mais fácil discutir e conduzir o conteúdo trabalhado. Aliada do professor nesse tipo de atividade está a tecnologia, que além de contextualizar, ainda ilustra e facilita todo o processo das atividades.

Em resumo, a criptografia se faz um recurso de grande valor quando adotada de maneira correta nas aulas de matemática. O estudo de funções, fatorações, potências e números primos podem ser, além de outros conteúdos, trabalhados de maneira a se fazer entendidos quando aplicados a um assunto tão presente na rotina dos nossos alunos e muitas vezes de conhecimento de poucos.

Referências Bibliográficas

S. U. ANIS. Criptografia de chave pública usando o algoritmo rsa. URL http://umaranis.com/rsa_calculator_demo.html.

J. Borin. *Jogos e resolução de problemas*. 2007.

S. C. Coutinho. *Criptografia*. IMPA, 2009.

M. Du Sautoy. *A música dos números primos: a história de um problema não resolvido na matemática*. Zahar, 2007.

L. M. Figueiredo. Introdução à criptografia. *Fundação CECIERJ. Rio de Janeiro: UFF/CEP-EB*, 2, 2010.

I. B. d. I. e. C. e. T. IBICT. Cifra de césar. URL http://www.codifica.ibict.br/#sobreoibict.

D. d. Kripka, Rosana Maria Luvezute e Oliveira. O uso da criptografia no ensino de matemática (co). In *XIII CONFERÊNCIA INTERAMERICANA DE EDUCAÇÃO MATEMÁTICA*, 2011. URL http://www.lematec.net.br/CDS/XIIICIAEM/artigos/1817.pdf. 2019-09-21.

C. d. A. Olgin. Criptografia e os conteúdos matemáticos do ensino médio (ta). In *XIII Conferência Interamericana de Educação Matemática*, 2011. URL http://www.projetos.unijui.edu.br/matematica/cnem/cnem/principal/cc/PDF/CC9.pdf.

P. C. N. PCN. Matemática. *Secretaria de Educação Fundamental. Brasília: MEC/SEF*, 1998.

S. Singh. *O livro dos códigos: A Ciência do Sigilo - do Antigo Egito à Criptografia Quântica*. Editora Record, 2008.

S. Singh. *O livro dos códigos*. Editora Record, 2011.

W. STALLINGS. Criptografia e segurança de redes, tradução vieira, daniel, 2008.

W. Stallings and Bressan. *Criptografia e segurança de redes*. Pearson Educación, 2004.