

**UNIVERSIDADE PRESBITERIANA MACKENZIE**  
Centro de Ciências e Humanidades  
Curso de Matemática

CAMILLA ÁVILA FINCATTI

**CRIPTOGRAFIA COMO AGENTE MOTIVADOR NA  
APRENDIZAGEM DA MATEMÁTICA EM SALA DE AULA**

São Paulo

2010

CAMILLA ÁVILA FINCATTI

**CRIPTOGRAFIA COMO AGENTE MOTIVADOR NA  
APRENDIZAGEM DA MATEMÁTICA EM SALA DE AULA**

Trabalho de Conclusão de  
Curso apresentado ao Centro de  
Ciências e Humanidades da  
Universidade Presbiteriana Mackenzie  
como requisito parcial à obtenção do  
grau de Licenciatura em Matemática.

ORIENTADORA: Prof<sup>a</sup>. Ms. Sonia Regina Gouveia

São Paulo

2010

CAMILLA ÁVILA FINCATTI

**CRIPTOGRAFIA COMO AGENTE MOTIVADOR NA  
APRENDIZAGEM DA MATEMÁTICA EM SALA DE AULA**

Trabalho de Conclusão de  
Curso apresentado ao Centro de  
Ciências e Humanidades da  
Universidade Presbiteriana Mackenzie  
como requisito parcial à obtenção do  
grau de Licenciatura em Matemática.

Aprovada em

**BANCA EXAMINADORA**

---

Prof<sup>a</sup>. Ms. Sonia Regina Gouveia – Orientadora  
Universidade Presbiteriana Mackenzie

---

Prof<sup>a</sup>. Dra. Vera Lúcia Antonio Azevedo  
Universidade Presbiteriana Mackenzie

---

Prof<sup>a</sup>. Ms. Eriko Matsui Yamamoto  
Universidade Presbiteriana Mackenzie

## AGRADECIMENTOS

A Deus, por acompanhar-me durante toda a minha vida.

À Prof<sup>a</sup>. Ms. Sonia Regina Gouveia, por ter sido orientadora persistente, com muita paciência, constante acompanhamento e incentivo, me aceitou com todas as minhas restrições e que, com sua competência, me fez concluir esta empreitada.

À Prof<sup>a</sup>. Dra. Vera Lúcia Antonio Azevedo, que sempre colaborou e me incentivou em vários momentos, fazendo-me repensar, prosseguir e nunca desistir.

À Prof<sup>a</sup>. Ms. Eriko Matsui Yamamoto, por compartilhar conosco seus conhecimentos e pelas sugestões apresentadas no decorrer do trabalho.

À Prof<sup>a</sup>. Ms. Renate Gompertz Watanabe, pelo muito que me ensinou durante minha carreira acadêmica, pelos livros que me emprestou e também presenteou, e pelas sugestões apresentadas na fase inicial desse trabalho.

À Prof<sup>a</sup>. Dra. Angela Hum Tchemra, pelas sugestões apresentadas na fase inicial desse trabalho.

À Paulo César Fincatti e Célia Regina Guimarães Ávila, meus queridos pais, por terem proporcionado um ótimo estudo, cursos e viagens pelo mundo com intuito de buscar conhecimento e aprender sobre diferentes culturas.

Ao Fernando Roberto Tarcia de Ávila, meu marido e companheiro, pelo apoio emocional oferecido sempre em hora oportuna e permanecendo ao meu lado durante todo o percurso dessa caminhada.

À Cecília Guimarães Ávila, querida tia, que sempre demonstrou interesse e apoio à realização desse trabalho.

À Débora Cristina Reverse Cunha, amiga de longa data, que nunca me deixou abater.

Aos professores do Curso de Matemática da Graduação do Mackenzie, pelo estímulo à realização desse trabalho.

## RESUMO

O objetivo desse trabalho é apresentar o contexto histórico da criptografia: como surgiu, sua evolução, a importância e suas múltiplas aplicações. Nele é abordada uma breve história das ramificações da escrita secreta até o surgimento da criptografia, os diversos tipos e seus inventores; seus pontos fortes e fracos; o desenvolvimento das primeiras cifras computadorizadas; sua evolução durante as grandes guerras, bem como a eterna batalha entre os criadores e os decifradores de códigos. A importância da criptografia na atualidade, nas mais diversas situações de nosso cotidiano e os benefícios da segurança nessas operações. Por fim, como é possível utilizar a criptografia como agente motivador do ensino da matemática em sala de aula.

Palavras-chave: Matemática. Criptografia. Cifra. Criptoanálise. Chave pública. Função. Matrizes.

## ABSTRACT

The aim of this study is to present the historical context of cryptography: how it emerged, its evolution, importance and its multiple applications. In it is discussed a brief history of the ramifications of secret writing until the encryption, the various types and their inventors, their strengths and weaknesses, the discovery of the mechanization of cryptography, its evolution during the great wars and the eternal battle between code makers and code breakers. The importance of cryptography in everyday life, in various situations of day and the benefits of security in the banking operations. Finally, how to use encryption as a motivator of mathematics teaching in the classroom.

Keywords: Math. Encryption. Cipher. Cryptanalysis. Public key. Functions.  
Matrices

## LISTA DE ILUSTRAÇÕES

Figura 1 - Principais ramificações da ciência da escrita secreta. ....	16
Figura 2 - Modelo de citale feito de madeira .....	18
Figura 3 - Relação ente algoritmo e a chave.....	20
Figura 4 - Disco de cifra de Alberti. ....	33
Figura 5 - Enigma.....	34
Figura 6 - Misturadores da Engima. ....	35
Figura 7 - Painel de tomadas da Enigma. ....	37
Figura 8 - Gráfico da função do primeiro grau com $a > 0$ . ....	52
Figura 9 - Gráfico da função do primeiro grau com $a < 0$ . ....	53
Figura 10 - Gráfico da função do primeiro grau do 1º exemplo.....	53
Figura 11 - Gráfico da função do primeiro grau do 2º exemplo.....	53
Figura 12 - Gráfico do estudo do sinal da função do primeiro grau com $a > 0$ . ....	55
Figura 13 - Gráfico do estudo do sinal da função do primeiro grau com $a < 0$ . ....	55
Figura 14 - Gráfico do estudo do sinal da função do primeiro grau do 1º exemplo...56	
Figura 15 - Gráfico do estudo do sinal da função do primeiro grau do 2º exemplo...56	
Figura 16 - Estudo do sinal da inequação do primeiro grau. ....	58
Figura 17 - Gráfico do estudo do sinal da inequação-produto com $a < 0$ . ....	58
Figura 18 - Gráfico do estudo do sinal da inequação-produto com $a > 0$ . ....	59
Figura 19 - Estudo do sinal da inequação-produto do primeiro grau.....	59
Figura 20 - Gráfico do estudo do sinal da inequação-quociente com $a > 0$ .....	60
Figura 21 - Gráfico do estudo do sinal da inequação-quociente com $a < 0$ .....	60
Figura 22 - Estudo do sinal da inequação-quociente do primeiro grau. ....	61
Figura 23 - Gráfico da função exponencial crescente. ....	76
Figura 24 - Gráfico da função exponencial decrescente. ....	76
Figura 25 - Gráfico da função exponencial do 1º exemplo.....	76
Figura 26 - Gráfico da função exponencial do 2º exemplo.....	76

## LISTA DE TABELAS

Tabela 1 – Tabela base para escrita da cifra de substituição.....	19
Tabela 2 – Quadrado de Vigenère. ....	24
Tabela 3 - Exemplo utilizando a palavra-chave LIVRO. ....	25
Tabela 4 - Exemplo de cifra homofônica para o texto NO SMOKING. ....	26
Tabela 5 - Exemplo de tabela de letras iniciais para cifra de livro.....	27
Tabela 6 – Tabela de repetição usada para quebra da Engima.....	40
Tabela 7 – Lista de correntes para quebra da Engima.....	40
Tabela 8 - Lista de correntes para análise de impactos na alteração de tomadas...	40
Tabela 9 - Tabela de relacionamentos para quebra da Engima.....	41
Tabela 10 – Números binários em ASCII para letras maiúsculas. ....	43
Tabela 11 - Cenário de troca de informações entre Alice e Bob. ....	47
Tabela 12 - Tabela alfa-numérica para exercícios com funções do primeiro grau. ...	61
Tabela 13 - Tabela alfa-numérica para exercícios com matrizes. ....	72
Tabela 14 - Tabela alfa-numérica.....	73
Tabela 15 - Tabela alfa-numérica para exercícios com funções exponenciais. ....	78

## LISTA DE ABREVIATURAS

ARPA	Advanced Research Projects Agency (Agência de Projetos Avançados de Pesquisa)
ARPANet	Advanced Research Projects Agency Network (Rede da Agência de Projetos Avançados de Pesquisa)
ASCII	American Standard Code for Information Interchange (Código Padrão Americano para Troca de Informações)
BITS	Binary Digits (Dígitos binário)
DES	Padrão de Cifragem de Dados (Data Encryption Standard)
ENIAC	Electronic Numerical Integrator And Calculator
IBM	International Business Machines
MB	Megabyte
MHZ	Mega-hertz
NSA	National Security Agency (Agência de Segurança Nacional)
RAM	Random Access Memory (Memória de acesso aleatório)
RSA	Ronald Rivest, Adi Shamir e Leonard Adleman

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO .....</b>	<b>13</b>
<b>2</b>	<b>CONTEXTO HISTÓRICO.....</b>	<b>14</b>
<b>3</b>	<b>ESCRITA SECRETA.....</b>	<b>16</b>
3.1	DEFINIÇÃO DE ESTEGANOGRAFIA.....	16
3.2	DEFINIÇÃO DE CRIPTOGRAFIA .....	16
<b>3.2.1</b>	<b>Transposição .....</b>	<b>17</b>
3.2.1.1	Cerca de ferrovia .....	17
3.2.1.2	Cifra da cerca de três linhas .....	18
3.2.1.3	Citale espartano .....	18
<b>3.2.2</b>	<b>Substituição.....</b>	<b>19</b>
3.2.2.1	Código .....	19
3.2.2.2	Cifra.....	20
<b>4</b>	<b>CRIPTOANÁLISE - A QUEBRA DA CIFRA DE SUBSTITUIÇÃO .....</b>	<b>22</b>
4.1	AVANÇOS NA CIFRA DE SUBSTITUIÇÃO PARA DESEQUILIBRAR A ANÁLISE DE FREQUÊNCIA.....	23
<b>5</b>	<b>CIFRA VIGENÈRE .....</b>	<b>24</b>
<b>6</b>	<b>CIFRA HOMOFÔNICA.....</b>	<b>26</b>
<b>7</b>	<b>CIFRA DE LIVRO.....</b>	<b>27</b>
<b>8</b>	<b>TELÉGRAFO .....</b>	<b>28</b>
<b>9</b>	<b>RÁDIO E CIFRAGEM SEGURA .....</b>	<b>29</b>
<b>10</b>	<b>O TELEGRAMA DE ARTHUR ZIMMERMANN .....</b>	<b>30</b>
<b>11</b>	<b>BLOCO DE CÍFRAS DE UMA ÚNICA VEZ.....</b>	<b>32</b>
<b>12</b>	<b>MECANIZAÇÃO DA CIFRAGEM .....</b>	<b>33</b>
12.1	DISCO DE CIFRA .....	33

12.2	ENIGMA .....	34
12.2.1	A quebra da Enigma .....	38
13	<b>CRIPTOGRAFIA COMPUTADORIZADA .....</b>	<b>42</b>
14	<b>TROCA SEGURA DE CHAVES.....</b>	<b>45</b>
15	<b>CRIPTOGRAFIA DE CHAVE PÚBLICA.....</b>	<b>48</b>
16	<b>RSA – INCORPORAÇÃO DA CHAVE PÚBLICA.....</b>	<b>49</b>
17	<b>A CRIPTOGRAFIA COMO AGENTE MOTIVADOR NO PROCESSO ENSINO-APRENDIZAGEM .....</b>	<b>51</b>
17.1	FUNÇÃO DO PRIMEIRO GRAU .....	52
17.1.1	<b>Pré-requisito .....</b>	<b>52</b>
17.1.2	<b>Definição .....</b>	<b>52</b>
17.1.3	<b>Gráfico.....</b>	<b>52</b>
17.1.4	<b>Coeficientes da função afim .....</b>	<b>54</b>
17.1.5	<b>Zero e equações do primeiro grau .....</b>	<b>54</b>
17.1.6	<b>Sinal da função .....</b>	<b>54</b>
17.1.7	<b>Inequações do primeiro grau.....</b>	<b>57</b>
17.1.8	<b>Aplicação do conceito na criptografia .....</b>	<b>61</b>
17.2	MATRIZES .....	62
17.2.1	<b>Definição .....</b>	<b>62</b>
17.2.2	<b>Matrizes especiais .....</b>	<b>63</b>
17.2.2.1	Matriz linha .....	63
17.2.2.2	Matriz coluna .....	63
17.2.2.3	Matriz nula.....	63
17.2.2.4	Matriz quadrada.....	64
17.2.2.5	Matriz diagonal .....	64
17.2.3	<b>Igualdade de matrizes .....</b>	<b>65</b>
17.2.4	<b>Adição .....</b>	<b>65</b>

17.2.4.1	Matriz oposta.....	66
17.2.4.2	Matriz diferença.....	66
17.2.4.3	Propriedades da adição.....	66
<b>17.2.5</b>	<b>Multiplicação de um número real por uma matriz.....</b>	<b>66</b>
17.2.5.1	Propriedades da multiplicação de um número real por uma matriz.....	67
<b>17.2.6</b>	<b>Multiplicação de matrizes .....</b>	<b>67</b>
17.2.6.1	Observações: .....	67
17.2.6.2	Propriedades da multiplicação de matrizes.....	69
<b>17.2.7</b>	<b>Matriz identidade .....</b>	<b>69</b>
17.2.7.1	Observação:.....	69
<b>17.2.8</b>	<b>Matriz transposta.....</b>	<b>70</b>
17.2.8.1	Propriedades da matriz transposta .....	70
<b>17.2.9</b>	<b>Matriz inversa.....</b>	<b>70</b>
17.2.9.1	Propriedades das matrizes inversíveis.....	71
<b>17.2.10</b>	<b>Aplicação do conceito na criptografia .....</b>	<b>71</b>
17.2.10.1	Matrizes inversas como chaves .....	71
17.2.10.2	Código de César e Matrizes inversas como chaves.....	73
17.3	FUNÇÃO EXPONENCIAL.....	74
<b>17.3.1</b>	<b>Pré-requisito .....</b>	<b>74</b>
<b>17.3.2</b>	<b>Definição .....</b>	<b>74</b>
<b>17.3.3</b>	<b>Propriedades.....</b>	<b>74</b>
<b>17.3.4</b>	<b>Gráfico.....</b>	<b>75</b>
<b>17.3.5</b>	<b>Equações exponenciais .....</b>	<b>77</b>
<b>17.3.6</b>	<b>Inequações exponenciais .....</b>	<b>77</b>
<b>17.3.7</b>	<b>Aplicação do conceito na criptografia .....</b>	<b>78</b>
<b>18</b>	<b>CONSIDERAÇÕES FINAIS .....</b>	<b>80</b>

## 1 INTRODUÇÃO

Por muitos anos, a comunicação foi um instrumento vital para que reis e rainhas governassem seus países e generais comandassem seus exércitos. Porém, caso essas mensagens fossem interceptadas, poderiam revelar informações e segredos preciosos aos rivais. Devido essa ameaça de interceptação, surgiram as técnicas de mascaramento de mensagens, através de códigos e cifras. Em contrapartida, surgiram os decifradores de códigos, que utilizavam métodos para invocar palavras e frases que tivessem significado nessas mensagens codificadas.

A batalha entre os codificadores e decifradores é secular e está em constante evolução. Os codificadores buscam criar códigos cada vez mais fortes enquanto os decifradores tornam seus métodos cada vez mais eficazes, ambos utilizando a matemática e diversas outras disciplinas e tecnologias.

A comunicação torna-se a cada dia uma mercadoria mais valiosa para nossa sociedade e o processo de codificação de mensagens desempenha um papel cada vez maior, já que nossa privacidade pode ser facilmente interceptada. Na internet, por exemplo, a codificação é o único meio de garantir a privacidade e sucesso do mercado digital. Assim como nas atividades civis, a criptografia militar também é de grande importância. Diz-se que a Primeira Guerra Mundial foi dos químicos, devido à utilização do gás mostarda e do cloro, e que a Segunda Guerra Mundial foi dos físicos, devido à criação da bomba atômica. Assim, a Terceira Guerra Mundial poderia ser dos matemáticos, já que a grande arma da guerra seria a informação.

Este trabalho aborda o surgimento e a evolução da criptografia e sua importância no percurso da história da humanidade; as ramificações da escrita secreta; alguns exemplos de criptografia; os pontos fortes e fracos, os diversos tipos e seus inventores. Destaca, ainda, a utilização da criptografia como agente motivador no processo ensino-aprendizagem da matemática, em sala de aula.

O trabalho é de caráter qualitativo, uma vez que identifiquei essa defasagem de conceitos matemáticos nos estudantes com os quais tive experiência. Por ser um assunto muito interessante e que está presente no cotidiano desses alunos, o objetivo do trabalho é apresentar uma maneira motivadora para aplicar a criptografia no estudo da matemática em sala de aula, fazendo com que eles pesquisem e estudem até mesmo fora do âmbito escolar.

## 2 CONTEXTO HISTÓRICO

De acordo com Cícero, filósofo e estadista romano, os primeiros relatos sobre escritas secretas datam do séc. V a.C. De acordo com Heródoto, o pai da História, a Grécia foi salva da conquista por Xerxes (Rei dos Reis da Pérsia) através da técnica da escrita secreta. Durante cinco anos, Xerxes montou secretamente a maior força de combate da história para atacar a Grécia. Demarato, um grego que fora expulso de sua terra natal, vivia numa cidade persa e, apesar de exilado, mantinha um laço de lealdade com a Grécia. Com isso, decidiu escrever uma mensagem para alertar os espartanos sobre a invasão, mas tinha como desafio enviá-la sem que fosse interceptada pelos guardas persas. A estratégia que Demarato encontrou consistia em simplesmente ocultar a mensagem. Conseguiu isso raspando a cera de um par de tabuletas de madeira, onde escreveu as intenções de Xerxes e depois cobriu novamente as tabuletas com a cera. Com a chegada da tabuleta em seu destino, os gregos, então indefesos, armaram-se e prepararam-se para o ataque surpresa de Xerxes.

Outro incidente narrado por Heródoto é a história de Histaeu, que queria encorajar um tirano<sup>1</sup> a se revoltar contra o rei persa. Para transmitir suas instruções com segurança, Histaeu raspou a cabeça do mensageiro, escreveu a mensagem no couro cabeludo e aguardou até que o cabelo voltasse a crescer. O mensageiro partiu e quando chegou ao seu destino, raspou a cabeça e exibiu a mensagem ao destinatário.

Uma das primeiras descrições do uso da escrita secreta, consta do texto Kama-sutra, escrito pelo estudioso brâmane Vatsyayana, no séc. IV a.C. O texto foi baseado em manuscritos onde há uma recomendação de que as mulheres deveriam estudar 64 artes, sendo que uma delas era a arte da escrita secreta, para que pudessem esconder os detalhes de seus relacionamentos.

Nas Guerras de Gália de Júlio César, foi escrito o primeiro documento com fins militares, utilizando um método de escrita secreta conhecida como cifra de substituição. Este documento foi escrito substituindo as letras do alfabeto romano

---

<sup>1</sup> Aristágora de Mileto

por letras gregas, de modo que a mensagem ficasse incompreensível ao seu inimigo.

No primeiro século depois de Cristo, Plínio descreveu que era possível utilizar o “leite” da planta titimálo como tinta invisível. Para ler a mensagem, bastava aquecê-la suavemente, que a mesma deixava de ser transparente, tornado-se marrom.

Os antigos chineses escreviam suas mensagens em seda fina, amassavam até formar uma pequena bola e depois cobriam com cera. O mensageiro engolia a bolinha de cera.

No século XVI, Giovanni Porta, um cientista italiano, descreveu que fazendo uma tinta com uma onça de alume e um quartilho de vinagre, podia-se escrever na casca de um ovo cozido. A solução penetrava na casca, deixando a mensagem marcada na clara endurecida do ovo.

No dia 15 de outubro de 1586, Maria, rainha da Escócia, após 18 anos de prisão, foi julgada por traição, por tramar o assassinato de sua prima, a rainha Elizabeth. Sir Francis Walsingham era o primeiro-secretário de Elizabeth e seu desafio era provar a ligação de Maria com os conspiradores. Maria trocava mensagens com o líder do grupo, Babington, utilizando uma cifra de nomenclatura. Walsingham interceptava essas cartas e encaminhava-as para uma escola de cifras, onde seu secretário Thomas Phelippes conseguiu decifrá-las utilizando um método conhecido como análise de frequência. Após decifrar todas as mensagens, Walsingham forjou uma carta e enviou-a à Maria. Sua resposta poderia incriminá-la, e foi o que aconteceu. Maria apoiava a tentativa de assassinato de Elizabeth, razão pela qual a rainha da Escócia foi decapitada.

Em 1941, foi descoberto pelo FBI o primeiro microponto. Na Segunda Guerra Mundial, agentes alemães reduziam fotograficamente uma página de texto até transformá-la num ponto com menos de um milímetro de diâmetro. Este microponto era então oculto sobre o ponto final de uma carta aparentemente inofensiva.

Espiões do século XX utilizavam a própria urina como tinta invisível.

### 3 ESCRITA SECRETA

A ciência da escrita secreta é dividida nas seguintes principais ramificações, conforme figura 1 abaixo:

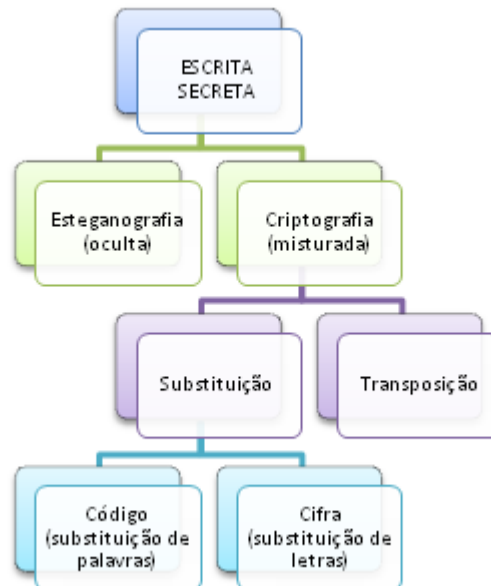


Figura 1 - Principais ramificações da ciência da escrita secreta.

Fonte: Própria.

A criptografia e a esteganografia são ciências independentes e é possível utilizá-las em conjunto gerando uma mensagem com segurança elevadíssima, embora a criptografia seja mais poderosa, devido sua capacidade de impedir a compreensão imediata da mensagem.

#### 3.1 DEFINIÇÃO DE ESTEGANOGRAFIA

Esteganografia [Do gr. stéganos -“oculto”- + gráphein -“escrita”] é o meio de comunicação secreta que é obtido através da ocultação de mensagens.

A esteganografia oferece certa segurança, mas sofre de uma fraqueza fundamental. Se descoberta a mensagem, seu conteúdo é imediatamente revelado.

#### 3.2 DEFINIÇÃO DE CRIPTOGRAFIA

Criptografia [Do gr. kriptós -“escondido”, “oculto”- + gráphein -“escrita”] é o meio de comunicação cujo objetivo não é ocultar sua existência e sim esconder seu significado, processo conhecido como encriptação. É um ramo especializado da teoria da informação com muitas contribuições de outros campos da matemática e do conhecimento.

Em uma mensagem criptografada, o texto é misturado de acordo com um protocolo preestabelecido entre o transmissor e o receptor da mensagem. O receptor reverte o protocolo, tornando a mensagem compreensível. A vantagem da utilização de uma mensagem criptografada está no fato de que a leitura fica incompreensível, para quem desconhece o protocolo de codificação. Neste caso, recriar a mensagem original torna-se uma tarefa difícil ou quase impossível.

A criptografia pode ser dividida em dois ramos, sendo transposição e substituição.

### 3.2.1 Transposição

Na transposição, as letras das mensagens são reorganizadas, gerando um anagrama<sup>2</sup>. Para mensagens curtas, de uma única palavra, o método é inseguro, pois existe um número limitado de possibilidades para organizar as letras. Por exemplo, a palavra pai só pode ser reorganizada nestas cinco maneiras diferentes: PIA, IPA, API, AIP, IAP. Porém, se a palavra ou frase for muito grande torna-se impossível de ser reorganizada, pois uma palavra com 35 letras possui mais de 50.000.000.000.000.000.000.000.000.000 de possibilidades de arranjos.

Uma transposição ao acaso, sem nenhuma regra específica, rima ou fundamento, torna-se uma mensagem de altíssima segurança, porém com a desvantagem de que quando chegar ao destinatário, este não conseguirá decifrar o anagrama. O sistema de rearranjo deve ser previamente combinado, de forma secreta, entre o remetente e o destinatário.

#### 3.2.1.1 Cerca de ferrovia

Um exemplo de rearranjo, utilizado como brincadeira entre estudantes consiste em escrever uma mensagem de modo que as letras fiquem separadas nas linhas de cima e de baixo. A sequência de letras na linha superior é seguida pela inferior criando a mensagem cifrada final, conforme exemplo a seguir:

---

<sup>2</sup> Anagrama - derivado das palavras gregas **ana**, que significa voltar ou repetir, e **graphein**, que significa escrever, resultando do rearranjo das letras de uma palavra ou frase para produzir outras palavras, utilizando todas as letras originais exatamente uma vez.

```

O   G A T O   C O M E U   O   R A T O
      ↓
O   A   O   O   E   O   A   O
  G   T   C   M   U   R   T
      ↓
O A O O E O A O G T C M U R T

```

### 3.2.1.2 Cifra da cerca de três linhas

Existem diversas formas de transposição sistemática, e outra forma seria escrever a mensagem em três linhas separadas ao invés de duas conforme demonstrado no exemplo da "cerca de ferrovia".

### 3.2.1.3 Citale espartano

O primeiro aparelho criptográfico militar para realizar a transposição foi o citale espartano, criado no séc. V a.C. O citale era feito de madeira e à sua volta enrolava-se uma tira de couro, como mostra a figura 2.

O funcionamento do citale era bem simples, bastava o remetente escrever a mensagem ao longo do comprimento do instrumento e depois desenrolava a fita, formando uma mensagem contendo letras sem sentido. Para decodificar a mensagem o destinatário deveria possuir um citale contendo o mesmo diâmetro do que foi usado pelo remetente, e simplesmente enrolava a tira em volta do bastão, formando assim a mensagem.

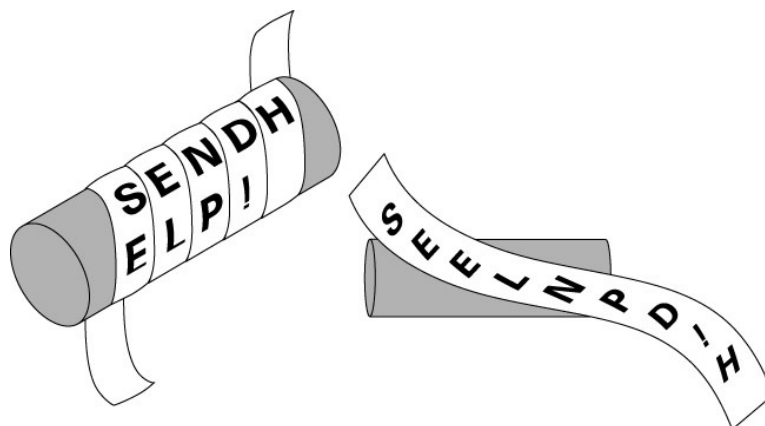


Figura 2 - Modelo de citale feito de madeira

Fonte: Wireless Networks Documentation. <<http://www.wireless-net.org/>>. Acesso em: 11 mar. 2010.

### 3.2.2 Substituição

Na substituição, uma das técnicas recomendadas é que se emparelhe ao acaso as letras do alfabeto, substituindo cada letra por seu par. Aplicando esse princípio, podemos gerar a seguinte tabela como base da escrita da cifra de substituição.

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

Tabela 1 – Tabela base para escrita da cifra de substituição.

Fonte: Própria.

Por exemplo, caso um remetente queira escrever “estarei no local combinado”, a frase ficará da seguinte forma “NDLUCNW EF TFRUT RFYVESF”.

Outra técnica, conhecida como cifra de deslocamento de César<sup>3</sup>, consiste em substituir cada letra da mensagem por outra letra três casas à frente. Um exemplo de uso dessa cifra fica da seguinte maneira:

Alfabeto original	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
Alfabeto cifrado	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
Texto original	e	n	t	r	e	e	m	c	o	n	t	a	t	o												
Texto cifrado	H	Q	W	U	H	H	P	F	R	Q	W	D	W	R												

Por convenção, na criptografia o alfabeto correto é escrito em minúsculas e criptografado em maiúsculas. O texto original (correto) também fica em minúsculas e a mensagem cifrada em maiúsculas.

#### 3.2.2.1 Código

Um código envolve a substituição de uma palavra ou frase, por um símbolo, número ou outra palavra. Por exemplo:

---

<sup>3</sup> Nas Guerras de Gália de Júlio César, foi escrito o primeiro documento com fins militares, utilizando um método de escrita secreta conhecida como cifra de substituição. Este documento foi escrito substituindo-se as letras do alfabeto romano por letras gregas, de modo que a mensagem ficasse incompreensível ao seu inimigo. (SINGH, 2008, p.26)

- Um batalhão da polícia pode definir que a palavra “samurai” signifique “atacar”.
- Um time de vôlei pode combinar antes de uma partida, alguns sinais (símbolos), que representam a maneira de como devem agir na jogada.

### 3.2.2.2 Cifra

Uma alternativa ao código é a cifra, que consiste em substituir as letras de uma palavra. O exemplo mais básico seria trocar uma letra pela próxima letra do alfabeto, assim, a frase “execute o plano” torna-se “fyfdvuf p qmboq”. As cifras são fundamentais na criptografia.

A cifra pode ser denominada como algoritmo, e toda a cifra deve ser acompanhada de uma chave<sup>4</sup> que especifica os detalhes exatos da codificação. O algoritmo consiste em substituir a letra do alfabeto original por uma letra do alfabeto cifrado. A relação entre o algoritmo e a chave é ilustrada na figura 3.

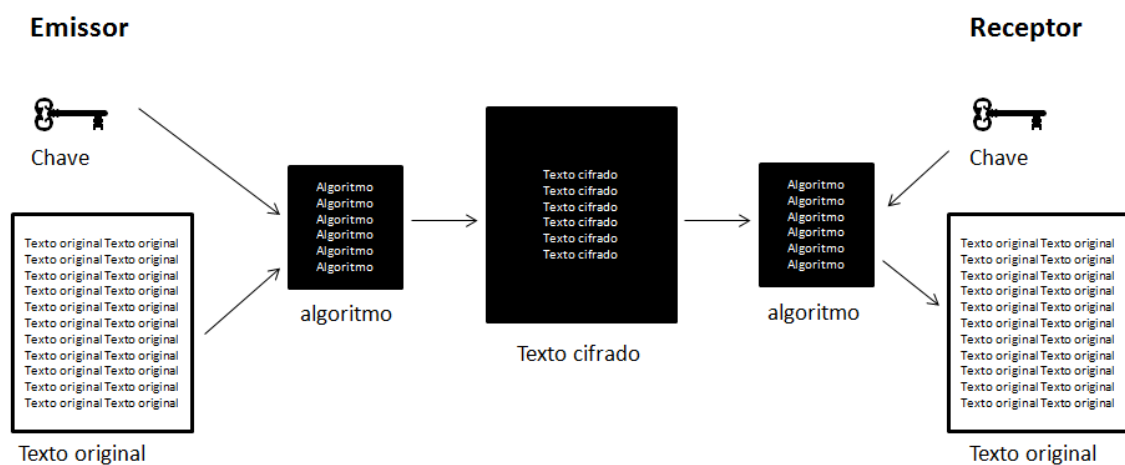


Figura 3 - Relação ente algoritmo e a chave.

Fonte: Própria.

O emissor aplica ao texto um algoritmo cifrado. O receptor converte o texto cifrado na mensagem original utilizando o mesmo algoritmo e chave do

<sup>4</sup> A importância da chave em relação ao algoritmo é um princípio constante da criptografia conforme foi definido pelo linguista holandês Auguste Kerckhoff, no livro *La Cryptographie Militaire*. (SINGH, 2008, p.28)

emissor. Mesmo que haja uma interceptação da mensagem, não será fácil decifrá-la sem conhecer o algoritmo utilizado.

Quanto mais chaves um sistema de código utilizar, maior sua segurança. Por exemplo, caso seja utilizada a cifra de substituição de César, só será necessário checar 25 possibilidades para decifrar a mensagem. Caso seja utilizado um algoritmo de segurança que consista em qualquer rearranjo do alfabeto, existirão 400.000.000.000.000.000.000.000.000 de chaves possíveis para utilizar. Um exemplo de uso de algoritmo de substituição geral ficaria da seguinte maneira:

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

Texto original	i n f o r m e o o b j e t i v o
Texto cifrado	R U I G V L F G G J T F K R W G

“Este é o princípio de Kerckhoff: A segurança de um criptossistema não deve depender da manutenção de um criptoalgoritmo em segredo. A segurança depende apenas de se manter em segredo a chave.” (SINGH, 2008, p.28)

Uma maneira bem simples de se conseguir uma chave é enviando uma palavra-chave ou uma frase-chave como, por exemplo, ALFA ROMEO. Para usar a palavra-chave, o receptor deve remover os espaços e as letras repetidas e então utilizar o resultado como o início do alfabeto. No exemplo, a chave ficaria como ALFROME.

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

A vantagem de utilizar um alfabeto cifrado dessa maneira é que é de fácil memorização.

Durante anos a cifra de substituição foi utilizada como uma das mais fortes artes de escrita secreta.

#### 4 CRIPTOANÁLISE - A QUEBRA DA CIFRA DE SUBSTITUIÇÃO

Durante anos, muitos estudiosos acreditaram que a cifra de substituição era indecifrável. Porém, decifradores descobriram um atalho para quebrar a cifra, revelando o conteúdo da mensagem em minutos. Essa descoberta foi feita no Oriente Médio por estudiosos árabes, que utilizavam uma combinação de linguística, estatística e devoção religiosa. Os árabes eram um povo muito culto, pois se esforçavam para obter o conhecimento de outras civilizações.

Eles inventaram a criptoanálise, que é a ciência que permite decifrar uma mensagem sem conhecer a sua chave.

“Enquanto o criptógrafo desenvolve novos métodos de escrita secreta, é o criptoanalista que luta para encontrar fraquezas nesses métodos, de modo a quebrar a mensagem secreta.” (SINGH, 2008, p.32)

A criptoanálise avançou bastante nas escolas de teologia fundadas em Basra, Kufa e Bagdá, pois os teólogos buscavam revelações de Maomé escondidas no Corão. Os teólogos queriam organizar, cronologicamente, as revelações e faziam isso contando a frequência das palavras em cada revelação. Além das palavras, os teólogos analisavam as letras individualmente e descobriram que algumas letras eram mais comuns que outras; por exemplo, as letras A e L são muito comuns no artigo definido al-, enquanto J é utilizada numa frequência pelo menos 10 vezes menor. Esta observação aparentemente inocente, na verdade serviu como um grande avanço na criptoanálise.

Uma maneira de decifrar uma mensagem codificada, da qual se saiba o idioma, é pegar um texto, suficientemente longo, na mesma língua. Analisa-se então com que frequência cada letra aparece no texto. A letra que aparece mais vezes é batizada de “primeira”, a segunda mais frequente é batizada de “segunda” e assim por diante, até a última letra do alfabeto.

Em seguida deve-se analisar o criptograma e classificar da mesma maneira seus símbolos, sendo, o símbolo mais frequente batizado de “primeiro” e assim por diante. Troca-se então a “primeira” letra de maior frequência pelo “primeiro” símbolo de maior frequência até converter todos os símbolos do criptograma.

Essa técnica é conhecida como análise de frequência e elimina a verificação de encontrar a chave que foi utilizada para cifrar o texto.

Os textos longos têm maior probabilidade de seguir frequências padrão; já para textos curtos essa técnica pode não funcionar direito, uma vez que eles têm maior probabilidade de desviarem, significativamente, das frequências padrão.

#### 4.1 AVANÇOS NA CIFRA DE SUBSTITUIÇÃO PARA DESEQUILIBRAR A ANÁLISE DE FREQUÊNCIA

Uma melhoria muito simples para a segurança da cifra de substituição monoalfabética foram os nulos, símbolos e letras que não representavam nada, mas que confundiriam um interceptador por análise de frequência.

Outra melhoria simples era escrever as palavras com grafia errada de modo que a fonética permanecesse entendível.

##### EZEMPLU DI FRAZI CUM GRUAFIA EIRRAIDA

Usando essa técnica, fica difícil também aplicar a análise de frequência.

Um nível mais alto de substituição é onde uma palavra é representada por outra palavra ou símbolo (código). Enquanto a cifra é definida por uma substituição de letras, o código é definido por substituição de palavras ou frases.

Apesar de o código oferecer mais segurança, há um grande trabalho em se definir uma palavra-código para cada uma das milhares de palavras possíveis de um texto. Fora isso, o remetente e o receptor da mensagem teriam um volumoso livro, e se este livro fosse interceptado, seria necessário criar um novo livro e distribuí-lo de novo aos remetentes e destinatários.

## 5 CIFRA VIGENÈRE

Leon Battista Alberti, nascido em 1404, pintor, compositor, poeta e filósofo, foi uma figura de destaque na Renascença. Por volta de 1440, Alberti escreveu um ensaio do que ele acreditava ser uma nova forma de cifra. Alberti propôs a utilização de dois ou mais alfabetos cifrados, usados alternadamente, para confundir os criptoanalistas potenciais.

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

O avanço principal do sistema de Alberti é que a mesma letra do texto original não aparece como uma única letra do alfabeto cifrado. Alberti não conseguiu desenvolver sua idéia num sistema completo de cifragem e esse sistema foi aperfeiçoado por Johannes Trithemius, alemão nascido em 1462, depois por Giovanni Porta, um cientista italiano nascido em 1535 e finalmente pelo diplomata francês Blaise de Vigenère, nascido em 1523. A força da cifra de Vigenère consiste na utilização de 26 alfabetos cifrados distintos para criar a mensagem cifrada. A tabela abaixo mostra como deve ser montada a tabela chamada de “quadrado de Vigenère”.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	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

Tabela 2 – Quadrado de Vigenère.

Fonte: Própria.

Basicamente a primeira fileira representa um alfabeto cifrado com a cifra de César, com deslocamento de uma letra na sequência do alfabeto. A segunda fileira representa um alfabeto cifrado com a cifra de César, com deslocamento de duas casas e assim por diante para as demais fileiras.

Na cifra de Vigenère, uma linha diferente do quadrado é utilizada para codificar letras diferentes da mensagem. Para decifrar a mensagem o destinatário precisa saber que linha do quadrado de Vigenère foi usada para a cifragem, e para isso utiliza-se uma palavra-chave.

Exemplo utilizando a palavra-chave LIVRO para o texto INFORME O OBJETIVO:

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	
2	8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	
1	11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	
5	14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
4	17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
3	21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	
26	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	

Palavra-chave            L I V R O L I V R O L I V R O L I V  
 Texto original            i n f o r m e o o b j e t i v o  
 Texto cifrado            T V A F F X M J F P U M O Z J Z

Tabela 3 - Exemplo utilizando a palavra-chave LIVRO.

Fonte: Própria.

A grande vantagem é que a cifra é imune à análise de frequência. Esta cifra pertence a uma classe conhecida como polialfabética, pois utiliza vários alfabetos cifrados por mensagem.

## 6 CIFRA HOMOFÔNICA

Homofonia. [Do gr. homophonia] Semelhança de sons ou de pronúncia.

Nessa outra técnica de cifragem, cada letra é substituída por uma variedade de substitutivos, de acordo com seu número potencial proporcional a frequência da letra. Por exemplo, a letra A corresponde a oito por cento de todas as letras que aparecem num texto em inglês, então este possuirá oito símbolos para representá-lo. Caso, por exemplo, a letra B corresponda a dois por cento de um texto em inglês, este possuirá dois símbolos para representá-lo.

Exemplo de cifra homofônica para o texto *NO SMOKING*:

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
09	48	13	01	14	10	06	23	32	15	04	26	22	18	00	38	94	29	11	17	08	34	60	28	21	02
12	81	41	03	16	31	25	39	70			37	27	58	05	95		35	19	20	61		89		52	
33		62	45	24			50	73			51		59	07			40	36	30	63					
47			79	44			56	83			84		66	54			42	76	43						
53				46			65	88					71	72			77	86	49						
67				55			68	93					91	90			80	96	69						
78				57										99					75						
92				64															85						
				74															97						
				82																					
				87																					
				98																					

texto original n o s m o k i n g  
**texto cifrado 18 0 11 22 5 4 32 58 6**

Tabela 4 - Exemplo de cifra homofônica para o texto NO SMOKING.

Fonte: Própria.

Uma cifra homofônica pode parecer uma cifra polialfabética, pois cada letra pode ser cifrada de modos diferentes, porém a cifra homofônica não passa de uma cifra monoalfabética. Uma letra no alfabeto pode ser representada por vários símbolos, mas cada símbolo representa apenas uma letra. Uma vez estabelecido o alfabeto cifrado, este permanece o mesmo durante todo o processo de cifragem.

## 7 CIFRA DE LIVRO

Na cifra de livro, um texto ou um livro é utilizado como chave. O criptógrafo numera sequencialmente cada palavra no texto-chave. Cada número equivale a um substituto para a letra inicial da palavra associada, formando assim um alfabeto conforme exemplo abaixo.

Numeração para identificar as letras iniciais:

<sup>1</sup> FOLHA <sup>2</sup> DE <sup>3</sup> SÃO <sup>4</sup> PAULO					
<sup>5</sup> Escolas <sup>6</sup> de <sup>7</sup> SP <sup>8</sup> usam <sup>9</sup> recreio <sup>10</sup> para <sup>11</sup> aplicar <sup>12</sup> jogos <sup>13</sup> e <sup>14</sup> brincadeiras <sup>15</sup> antigas					
<sup>16</sup> Escolas <sup>17</sup> particulares <sup>18</sup> de <sup>19</sup> São <sup>20</sup> Paulo <sup>21</sup> começaram <sup>22</sup> a <sup>23</sup> organizar <sup>24</sup> a <sup>25</sup> brincadeira <sup>26</sup> das <sup>27</sup> crianças <sup>28</sup> no <sup>29</sup> recreio. <sup>30</sup> Para <sup>31</sup> substituir <sup>32</sup> a <sup>33</sup> correria <sup>34</sup> habitual <sup>35</sup> do <sup>36</sup> intervalo, <sup>37</sup> elas <sup>38</sup> estão <sup>39</sup> oferecendo <sup>40</sup> espaços <sup>41</sup> onde <sup>42</sup> os <sup>43</sup> professores <sup>44</sup> ensinam <sup>45</sup> a <sup>46</sup> brincar <sup>47</sup> com <sup>48</sup> jogos <sup>49</sup> de <sup>50</sup> tabuleiro <sup>51</sup> ou <sup>52</sup> com <sup>53</sup> brinquedos <sup>54</sup> antigos. <sup>55</sup> Há <sup>56</sup> as <sup>57</sup> que <sup>58</sup> oferecem <sup>59</sup> até <sup>60</sup> cantos <sup>61</sup> de <sup>62</sup> leitura. <sup>63</sup> Dessa <sup>64</sup> forma, <sup>65</sup> mantêm <sup>66</sup> a <sup>67</sup> garotada <sup>68</sup> voltada <sup>69</sup> para <sup>70</sup> os <sup>71</sup> estudos.					

Tabela de letras iniciais:

1 = F	13 = E	25 = B	37 = E	49 = D	61 = D
2 = D	14 = B	26 = D	38 = E	50 = T	62 = L
3 = S	15 = A	27 = C	39 = O	51 = O	63 = D
4 = P	16 = E	28 = N	40 = E	52 = C	64 = F
5 = E	17 = P	29 = R	41 = O	53 = B	65 = M
6 = D	18 = D	30 = P	42 = O	54 = A	66 = A
7 = S	19 = S	31 = S	43 = P	55 = H	67 = G
8 = U	20 = P	32 = A	44 = E	56 = A	68 = V
9 = R	21 = C	33 = C	45 = A	57 = Q	69 = P
10 = P	22 = A	34 = H	46 = B	58 = O	70 = O
11 = A	23 = O	35 = D	47 = C	59 = A	71 = E
12 = J	24 = A	36 = I	48 = J	60 = C	

Tabela 5 - Exemplo de tabela de letras iniciais para cifra de livro.

Fonte: Própria.

texto original V a m o s e s t u d a r  
 texto cifrado 68 11 65 23 3 5 7 50 8 2 15 9

O receptor da mensagem também deverá possuir o texto utilizado como chave, assim, com muita facilidade, conseguirá decifrar a mensagem. Caso o texto cifrado seja interceptado, será extremamente difícil decifrá-lo utilizando a técnica de criptoanálise.

## 8 TELÉGRAFO

Antes mesmo da Era Cristã, já se havia observado as propriedades de atração do âmbar friccionado e as da atração magnética do ímã. Em 1858, Giovanni della Porta descreveu o que ele chamou de “telégrafo simpático”, como sendo constituído de duas agulhas de aço magnetizadas por um mesmo ímã. Supunha ele que o movimento provocado na agulha de um dos instrumentos causasse um movimento síncrono com o da outra agulha. Com isso, esperava conseguir o estabelecimento de comunicação entre dois pontos.

Em 1747, na Inglaterra, William Watson demonstrou que a corrente elétrica podia ser transmitida a uma considerável distância por um fio metálico, cujas extremidades, ligadas à terra, formavam o circuito.

Em 1800, Francisco Salvá provou que as correntes voltaicas podiam ser utilizadas para a transmissão de sinais. Mas foi somente em 1819 que Hans Christian Oersted, ao observar o comportamento da agulha magnética, descobriu que esta poderia ser defletida mediante a passagem de uma corrente por um fio que lhe ficasse suficientemente próximo, verificando também que a deflexão variava para a direita ou para a esquerda, conforme o sentido de direção da corrente.

Em 1825, William Sturgeon, na Inglaterra, inventou o eletromagneto. A ação da corrente elétrica no magneto foi aplicada pela primeira vez à telegrafia por André Marie Ampère, em 1820, atendendo a uma sugestão de Pierre Simon Laplace. Segundo este, pequenos magnetos instalados na extremidade de recepção de 26 fios poderiam ser usados para indicar as letras do alfabeto.

Em outubro de 1832, Samuel F.B. Morse, ao voltar da Europa para os Estados Unidos, projetou a construção de um aparelho telegráfico registrador e estabeleceu os princípios relativos a seu código de pontos, traços e intervalos, com base na presença ou ausência de impulsos elétricos. Após introduzir diversos melhoramentos no aparelho, Morse transmitiu, em 1844, o primeiro telegrama pela linha de Washington a Baltimore, numa extensão de 64 quilômetros.

No séc. XX, embora diminuísse consideravelmente a importância dos métodos de Morse, alguns circuitos telegráficos existentes em diversas partes do mundo ainda utilizam os princípios fundamentais do sistema original de Morse. Nesses circuitos, os sinais são emitidos segundo o código de Morse, na forma de pulsações de corrente, curtas ou longas e separadas por intervalos. As pulsações curtas, de duração muito breve, representam os pontos, tendo as correspondentes aos traços uma duração três vezes maior. Os intervalos entre os componentes de uma letra equivalem a um ponto; entre uma letra e outra, a um traço; e entre duas palavras, a dois traços.

## 9 RÁDIO E CIFRAGEM SEGURA

Em 1894, o físico italiano Guglielmo Marconi, inventou uma forma muito poderosa de telecomunicação, aumentando assim a necessidade de uma codificação segura.

Marconi estava realizando experimentos com circuitos elétricos e descobriu que quando um circuito é percorrido por uma corrente elétrica, este induz uma corrente em outro circuito isolado, a alguma distância um do outro. Marconi aperfeiçoou o projeto dos circuitos aumentando a força e acrescentando antenas e como resultado começou a receber e transmitir pulsos de informações através da distância de 2,5 quilômetros. Ele tinha inventado o rádio.

O telégrafo já era bem utilizado há pelo menos meio século, porém, exigia um fio para transportar a mensagem entre o emissor e receptor. No sistema adotado por Marconi, o sinal viajava pelo ar, sem que fosse preciso o emprego de fios.

Em 1896, Marconi conseguiu apoio financeiro na Inglaterra, para aprimorar seu projeto que resultou na transmissão por 53 quilômetros, além do canal da Mancha, até a França. Em 1901, Marconi efetuou a primeira transmissão por uma distância de 3.500 quilômetros, desmistificando que a comunicação era limitada pelo horizonte, ou seja, que as ondas do rádio não seguiriam pela curvatura da Terra.

Com isso, a invenção de Marconi fascinou os militares, que passaram a ver vantagens táticas óbvias, permitindo a comunicação direta entre dois pontos sem a necessidade de um fio.

Pela facilidade de comunicação e de interceptação, o rádio foi utilizado na Primeira Guerra Mundial por todos os lados, porém ninguém tinha certeza de como garantir segurança das informações.

A invenção do rádio e a guerra intensificaram a necessidade de uma cifra segura. Foram criadas diversas cifras, mas uma por uma foram decifradas. A cifra mais famosa utilizada na guerra foi a ADFGVX, mas logo está foi quebrada pelo francês, Georges Painvin.

Desde a quebra da cifra de Vigenère, no séc. XIX, os decifradores de código levavam grande vantagem sobre os criadores de código.

## 10 O TELEGRAMA DE ARTHUR ZIMMERMANN

Os americanos permaneceram neutros durante a Grande Guerra; mas, em 1916, esse cenário mudou quando Arthur Zimmermann foi nomeado ministro das Relações Exteriores.

Os americanos acreditavam que a entrada de Zimmermann marcaria o início de uma nova era diplomática. Contudo, Zimmermann não tinha intenção nenhuma de buscar a paz, na verdade, planejava uma grande ofensiva militar.

Em 1915, um transatlântico americano, com 1.198 passageiros, foi afundado por um submarino alemão. Os Estados Unidos preparavam-se para entrar em guerra, quando a Alemanha garantiu que seus submarinhos emergiriam antes de atacar, assim não haveria ataques acidentais.

Em 1917, Zimmermann compareceu a uma importante reunião, onde as autoridades presentes decidiram pelo início de uma guerra submarina irrestrita.

Os alemães sabiam que seus submarinos eram quase invencíveis se atacassem ainda submersos. A intenção era que realizando ataque a navios mercantes contendo suprimentos, a Grã-Bretanha se renderia em seis meses devido à fome. Mas com isso também fariam com que a América entrasse na guerra, mas já seria tarde quando as tropas chegassem a Europa.

Para tentar desencorajar ainda mais os Estados Unidos a entrarem na Guerra, Zimmermann teve a ideia de propor uma aliança com o México, convencendo-o de que deveria invadir a América para recuperar territórios como Texas, Novo México e Arizona. A Alemanha ajudaria financeiramente e militarmente o México nessa ação. Além disso, Zimmermann queria que o presidente mexicano convencesse os japoneses a atacarem também os Estados Unidos. O objetivo de Zimmermann era criar tantos problemas para os americanos, que não poderiam então enviar tropas para a Europa.

Zimmermann então transmitiu uma mensagem cifrada para a Suécia, por meio de rádio, e de lá foi enviada através de um cabo transatlântico americano, mas como esse cabo passava pela Inglaterra, o telegrama foi interceptado.

O telegrama foi logo enviado para a sala de cifras, onde o decifrador responsável, Montgomery, com a ajuda de Nigel de Grey e William Heinemann,

perceberam que estavam lidando com uma cifra usada apenas em comunicações diplomáticas de alto nível. Eles trataram o telegrama com total urgência e, após algumas horas, conseguiram decifrar parcialmente a mensagem, e assim descobrir os planos terríveis de Zimmermann.

O telegrama tinha uma mortífera ameaça, mas também um grande motivo para os Estados Unidos unirem-se aos aliados.

A mensagem parcialmente cifrada foi enviada para o almirante, Sir William Hall, diretor do Serviço Naval de Informações. O almirante pediu a Montgomery que terminasse de decifrar a mensagem e preferiu manter o telegrama em segredo, pois caso os alemães soubessem que a mensagem de Zimmermann fora decifrada, logo elaborariam um novo sistema de cifragem, e isso sufocaria todo o sistema de interceptação de mensagens dos aliados. Hall estava ciente de que o ataque começaria em duas semanas, e foi isso o que ocorreu. No dia 1º de fevereiro, a Alemanha iniciou uma guerra naval irrestrita; no dia 3 de fevereiro, a resposta dos americanos foi a de que continuariam neutros na guerra.

Montgomery e Grey, 15 dias após terem entrado em contato com Hall, enviaram a mensagem completamente cifrada. Hall, nesse meio tempo, encontrou uma maneira de impedir que os alemães suspeitassem da quebra de sua cifra. A carta de Zimmermann já havia chegado ao México numa versão revisada e decifrada. Hall entrou em contato com um agente britânico infiltrado no Escritório Mexicano de Telégrafos, e obteve a versão mexicana do telegrama de Zimmermann.

O telegrama foi liberado para a imprensa, e os alemães presumiram que o mesmo fora roubado do governo, e não interceptado e decifrado pelos britânicos, a caminho da América.

Zimmermann assumiu publicamente ser o autor do telegrama. Com isso, os Estados Unidos finalmente envolveram-se na guerra, juntando-se aos aliados.

## 11 BLOCO DE CÍFRAS DE UMA ÚNICA VEZ

Enquanto a Primeira Guerra Mundial chegava ao fim, o major Joseph Mauborgne, diretor de pesquisa criptográfica do exército americano, criou o conceito da chave aleatória, que consistia numa série de letras dispostas ao acaso. Ele agregou esse conceito à cifra de Vigenère e com isso elevou o nível de segurança das mensagens. Para aplicar o conceito de Mauborgne, a primeira etapa do sistema era produzir um bloco grosso de papel, com cada folha contendo uma chave única na forma de uma linha de letras em sequência aleatória. Esse bloco deveria no mínimo possuir duas cópias, para que uma ficasse com o remetente e outra com o destinatário da mensagem. Para cada mensagem a cifrar, o remetente aplicaria a cifra de Vigenère usando a primeira folha do bloco como chave. O destinatário da mensagem decifrava facilmente a mensagem usando a chave que estava na primeira folha do bloco, revertendo a cifra de Vigenère. Depois disso, a primeira folha do bloco do remetente e destinatário deveria ser destruída e a próxima mensagem seria cifrada com a seguinte chave aleatória do bloco.

A força desse sistema é que caso a mensagem seja interceptada, seria quase que impossível para o criptoanalista decifrar a mensagem, já que a chave não possui sentido, e o criptoanalista não conseguiria determinar se suas tentativas estariam no caminho correto.

Teoricamente o sistema era perfeito, mas na prática o apresentava duas grandes dificuldades para a época. A primeira era gerar um grande número de chaves aleatórias, sem que houvesse repetição (chave única).

A segunda dificuldade era que esse bloco deveria ser distribuído simultaneamente para todos os remetentes e destinatários das mensagens, e estes deveriam manter sincronizadas as chaves utilizadas.

O sistema é prático apenas para quem realmente necessita de comunicação ultrassegura. Existem rumores de que os presidentes da Rússia e dos Estados Unidos, possuem uma comunicação onde é utilizado o sistema de bloco de cifras de uma única vez.

## 12 MECANIZAÇÃO DA CIFRAGEM

### 12.1 DISCO DE CIFRA

A primeira máquina criptográfica de que se tem registro foi inventada, no séc. XV, pelo arquiteto italiano Leon Alberti, um dos criadores da cifra polialfabética.

A máquina era feita com dois discos de cobre (um maior que o outro), cada disco com um alfabeto ao longo de sua borda. O disco menor era fixado em cima do maior com um pino que agia com um eixo. Os discos podiam ser girados independentemente, e assim poderiam ser usados para cifrar uma mensagem utilizando a cifra de deslocamento simples de César. O disco exterior possui o alfabeto original e o interior o alfabeto cifrado.

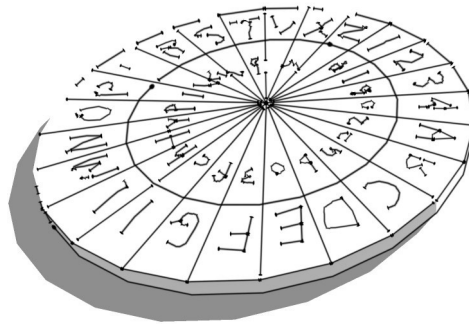


Figura 4 - Disco de cifra de Alberti.

Fonte: Association for Computing Machinery. <<http://www.acm.org/>>. Acesso em: 10 mar. 2010.

Alberti teria utilizado sua invenção para cifrar mensagens utilizando uma cifra polialfabética. Ele conseguia isso, usando uma palavra chave para ajustar cada letra da mensagem.

Por exemplo, para cifrar a palavra gol, usando LER como palavra-chave, devia-se ajustar os discos de modo que o A externo ficasse ao lado do L interno, e com isso conseguia-se a primeira letra da mensagem que era a R, pois essa letra era a que estava ao lado do g. Para cifrar a segunda letra da mensagem, ajustavam-se os discos de modo que o A externo ficasse ao lado do E interno, e assim conseguia-se a segunda letra da mensagem que era a S, pois essa letra era a que estava ao lado do O. O processo continuaria até concluir todas as letras da mensagem.

O disco acelerava o trabalho e reduzia erros. Mesmo sendo um dispositivo básico, foi utilizado por pelo menos uns cinco séculos.

## 12.2 ENIGMA

Em 1918 o inventor alemão Arthur Scherbius e seu amigo Richard Ritter, fundaram a empresa Scherbius & Ritter. Era uma empresa inovadora e um dos projetos era criar novos sistemas de criptografia para substituir os sistemas inadequados que foram utilizados na Primeira Guerra Mundial. Com isso eles criaram a primeira máquina criptográfica, utilizando tecnologia do séc. XX. A invenção chamava-se Enigma (Figura 5), e foi o mais terrível sistema de cifragem da história.



Figura 5 - Enigma.

Fonte: Bob Lord's Home Page. <<http://www.ilord.com/enigma.html>>. Acesso em: 10 mar. 2010.

A máquina, além de componentes engenhosos, e possuía três elementos básicos ligados por fios, sendo um teclado para a entrada das letras do texto original, uma unidade misturadora (Figura 6) que cifra cada letra e um mostrador contendo varias lâmpadas para indicar a letra cifrada.

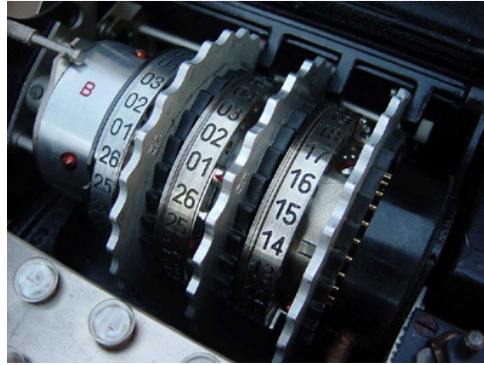


Figura 6 - Misturadores da Engima.

Fonte: Bob Lord's Home Page. <<http://www.ilord.com/enigma.html>>. Acesso em: 10 mar. 2010.

Por exemplo, utilizemos um modelo de máquina Enigma simplificado, que possui apenas seis letras do alfabeto (A, B, C, D, E, F).

Ao teclarmos a, a letra B será iluminada, o que significa que a foi cifrado como B.

Ao teclarmos b, a letra C será iluminada, o que significa que b foi cifrado como C.

Ao teclarmos c, a letra D será iluminada, o que significa que c foi cifrado como D, e assim por diante.

Caso o enigma esteja com a regulação básica, a mensagem aba seria cifrada como BCB, ou seja, estaria utilizando uma cifra monoalfabética.

O misturador é a peça mais importante da máquina, pois é ele que determina como a letra digitada no teclado será cifrada. A cada letra digitada o misturador gira e uma nova cifragem é gerada.

Ou seja, se teclarmos a, a letra B será iluminada, o que significa que a foi cifrado como B. Se teclarmos a novamente, a letra C será iluminada, o que significa que a desta vez foi cifrado como C devido à rotação do misturador.

Porém, se digitarmos seis vezes a letra b, faria com que o misturador retornasse a sua posição original e com isso haveria repetições de cifragem, tornando-se um sistema fraco. Isso foi resolvido introduzindo um segundo misturador. O segundo misturador só se move, quando o primeiro misturador finaliza uma rotação completa. Com isso, consegue-se uma cifragem de um total de

$6 \times 6 = 36$  letras; ou seja, havia 36 ajustes diferentes do misturador, o que equivale a trocar entre 36 alfabetos cifrados.

Scherbius queria aumentar a complexidade de sua invenção e, para isso introduziu um terceiro misturador. Os três misturadores ofereciam uma cifração de um total de  $26 \times 26 \times 26 = 17.576$  letras; ou seja, havia 17.576 ajustes diferentes de misturadores. Além disso, Scherbius acrescentou um refletor ao aparelho.

O refletor era bem parecido com um misturador, porém, este não girava. Apenas os fios entravam por um lado e emergiam pelo mesmo lado. O refletor recebia o sinal e retransmitia através de uma rota diferente.

Para enviar uma mensagem através da Enigma, o operador girava os misturadores para determinar a posição inicial. Havia 17.576 ajustes possíveis e, portanto 17.576 posições iniciais. A disposição inicial determinava como a mensagem seria cifrada, ou seja, era a chave da cifração.

A mensagem era cifrada e transmitida via rádio para o destinatário.

O destinatário precisava ter uma máquina Enigma e também ter conhecimento da chave inicial que determinava o posicionamento dos misturadores. Bastava então digitar a mensagem cifrada, que o painel luminoso indicava cada letra da mensagem original.

Mesmo que a mensagem fosse interceptada por alguém que possuísse uma máquina Enigma, este não conseguiria decifrar facilmente a mensagem, se não possuísse o ajuste inicial da máquina.

Os misturadores poderiam também ser trocados de lugar, fazendo com que afetasse na decifração, já que o arranjo exato é crucial tanto para a cifração como a decifração.

Scherbius acrescentou ainda mais uma evolução à Enigma. Ele introduziu um painel de tomadas (Figura 7) entre o teclado e o primeiro misturador. O operador poderia, através desse painel, trocar algumas letras antes que elas entrassem no misturador. Por exemplo, o operador poderia conectar as tomadas a e b no painel, de modo que quando fosse digitada a letra b, o sinal elétrico seguiria pelo caminho da letra a, e vice-versa. O operador da Enigma poderia configurar até seis pares de letras, pois dispunha de seis tomadas.

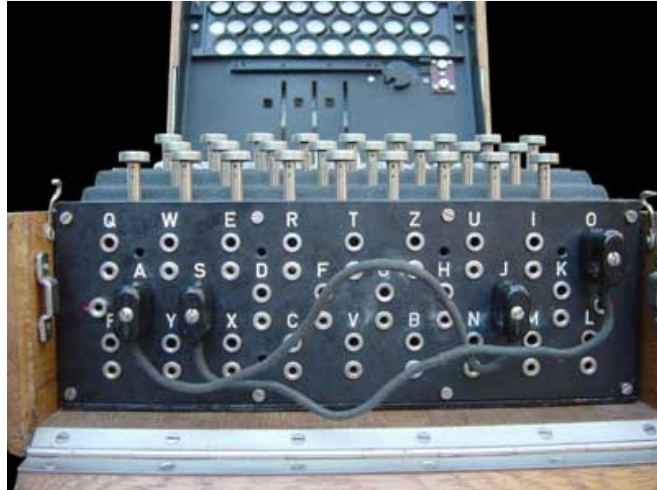


Figura 7 - Painel de tomadas da Enigma.

Fonte: Bob Lord's Home Page. <<http://www.ilord.com/enigma.html>>. Acesso em: 10 mar. 2010.

Com todos esses componentes, a Enigma possuía um enorme número de chaves. A lista abaixo que mostra as possibilidades para cada componente:

- Orientação dos misturadores

Cada misturador, sendo no total de três, podia ser ajustado em 26 orientações diferentes; existem, portanto,

$$26 \times 26 \times 26 = 17.576 \text{ (ajustes)}$$

- Disposição dos misturadores

Os três misturadores poderiam ser ajustados em qualquer uma das seis ordens diferentes:

$$123, 132, 213, 231, 312, 321. \text{ Ou seja, seis (ajustes)}$$

- Painel de tomadas

O número de modos de conectar, e, portanto de trocar seis pares de letras é enorme, sendo:

$$100.391.791.500 \text{ (ajustes)}$$

- Total

O número total de chaves possíveis é a multiplicação dos três números acima, sendo:

$$17.576 \times 6 \times 100.391.791.500 = 10.000.000.000.000.000$$

Ou seja, um interceptador que não conhece a chave, teria que verificar entre 10.000.000.000.000.000 de chaves possíveis.

Nota-se, que o painel de tomadas é o componente que fornece o maior número de chaves. Porém, se Scherbius não tivesse acrescentado o misturador à Enigma, mas somente o quadro de tomadas, a máquina funcionaria apenas como uma cifra de substituição monoalfabética, e com isso os criptoanalistas poderiam decifrá-la pela análise de frequência.

Em 1925, Scherbius produziu a Enigma em grande escala. Trinta mil máquinas foram adquiridas e utilizadas, nas duas décadas seguintes, pelo exército alemão.

### **12.2.1 A quebra da Enigma**

Com a invenção de Scherbius, os alemães tiveram em mãos o sistema de criptografia mais seguro do mundo. No início da Segunda Guerra Mundial, as comunicações estavam protegidas por um nível altíssimo de cifragem, e parecia que a Enigma desempenharia um papel importante na vitória nazista.

Em 1926, os britânicos, passaram a interceptar mensagens dos alemães, mas elas eram completamente confusas. Americanos e franceses também tentavam quebrar a cifra que era produzida pela Enigma, mas perderam as esperanças com os resultados desanimadores.

Logo depois da derrota da Alemanha, os países aliados sentiam-se numa posição confortável e com o tempo perderam o interesse pela criptoanálise. Porém, a Polônia não podia deixar de lado seu interesse em decifrar as mensagens da Enigma, já que havia se tornado um estado independente e era ameaçada constantemente pela Alemanha.

O encarregado por tentar decifrar as cifras da Enigma, na Polônia, era o capitão alemão Maksymilian Ciezki. Ele teve acesso à versão comercial da Enigma, e estudou todos os princípios da máquina; porém, o modelo comercial era diferente do militar. Sem conhecimento da fiação da versão militar, Ciezki não teria chance de decifrar as mensagens. O desespero era tão grande que o militar alemão contratou até uma vidente; é claro que ele não obteve sucesso.

Foi então que surgiu o alemão, Hans-Thilo Schmidt, que trabalhava como administrador das comunicações cifradas da Alemanha, por indicação de seu irmão Rudolph. Schmidt era um descontente, mergulhado na pobreza, já que seus negócios não deram certo. Foi forçado a deixar sua família para trabalhar num estabelecimento altamente secreto. Ressentido, sozinho, e invejando seu irmão perfeito, o resultado foi inevitável. Começou a vender segredos da Enigma para potências estrangeiras. Schmidt obteve dinheiro e vingança, destruindo a segurança da Alemanha e de seu irmão.

Graças a traição de Schmidt, os aliados conseguiram produzir uma réplica da Enigma. Mas somente a máquina não bastava para decifrar as mensagens. Era necessário saber a configuração inicial da máquina que transmitiu a mensagem. Com isso, os poloneses mudaram sua política de recrutamento dos criptoanalistas que trabalhavam para quebrar a Enigma. Ao invés de contratar peritos na estrutura da linguagem, contrataram matemáticos, já que a Enigma usava uma cifra mecânica.

Os alemães usavam uma estratégia para definir a chave que seria utilizada no dia, enviando no início de uma mensagem uma chave repetida duas vezes, ou seja, se o operador escolhesse a chave CFE, ele deveria cifrá-la duas vezes, de modo que CFECFE transformaria-se em PEFNWZ. Os alemães exigiam a repetição para evitar erros causados por interferências.

Contudo, essa regra seria uma grande pista para o matemático Marian Rejewski que tentava encontrar um meio de descobrir a chave diária.

A estratégia de Rejewski era detectar uma repetição que prejudicasse a segurança de uma cifra, ao produzir padrões. A repetição mais óbvia na cifragem da Enigma era a chave da mensagem, repetida duas vezes no início da mensagem.

Por exemplo, as mensagens chegavam com as seguintes chaves cifradas:

	1ª	2ª	3ª	4ª	5ª	6ª
Primeira mensagem	L	O	K	R	G	M
Segunda mensagem	M	V	T	X	Z	E
Terceira mensagem	J	K	T	M	P	E
Quarta mensagem	D	V	Y	P	Z	X

Como Rejewski sabia que a chave possuía três letras, ele percebeu que havia ligação entre a 1ª e 4ª, 2ª e 5ª e 3ª e 6ª letra. Ele montou então uma tabela conforme o exemplo abaixo:

Primeira letra	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
Quarta letra				P						M		R	X													

Tabela 6 – Tabela de repetição usada para quebra da Engima.  
 Fonte: Própria.

Rejewski fez uma lista das correntes anotando todos os elos em cada uma:

A → F → W → A	3 ligações
B → Q → Z → K → V → E → L → R → I → B	9 ligações
C → H → G → O → Y → D → P → C	7 ligações
J → M → X → S → T → N → U → J	7 ligações

Tabela 7 – Lista de correntes para quebra da Engima.  
 Fonte: Própria.

Notou também que diariamente as letras e os tamanhos das correntes mudavam (reflexo da chave diária) e que a disposição do quadro de tomadas não refletia nas correntes. Por exemplo, se alterasse a tomada S e G para T e K, as correntes ficariam da seguinte maneira:

A → F → W → A	3 ligações
B → Q → Z → T → V → E → L → R → I → B	9 ligações
C → H → S → O → Y → D → P → C	7 ligações
J → M → X → G → K → N → U → J	7 ligações

Tabela 8 - Lista de correntes para análise de impactos na alteração de tomadas.  
 Fonte: Própria.

As letras na corrente mudaram, mas os elos permaneceram constantes. Com isso, ao invés de preocupar-se com 10.000.000.000.000.000 de chaves diárias, ele preocupava-se com o número de arranjos entre os misturadores (6) multiplicado pelo número de orientações dos misturadores (17.576), o que resulta em 105.456 ajustes dos misturadores. Esse número é 100 bilhões de vezes menor que o número de chaves diárias.

A equipe de Rejewski começou a tarefa de verificar os 105.456 ajustes dos misturadores, catalogando os comprimentos das correntes. O trabalho durou um ano e com essas informações catalogadas, Rejewski começou a decifrar a Enigma.

Diariamente, ele analisava as seis primeiras letras das mensagens interceptadas e com isso construía uma tabela de relacionamentos. Dessa forma, montou outra tabela contendo três conjuntos de correntes com os seguintes números de correntes e ligações em cada:

4 correntes da 1ª e da 4ª letra com	3, 9, 7 e 7 ligações
4 correntes da 2ª e da 5ª letra com	2, 3, 9 e 12 ligações
5 correntes da 3ª e da 6ª letra com	5, 5, 5, 3 e 8 ligações

Tabela 9 - Tabela de relacionamentos para quebra da Enigma.

Fonte: Própria.

Com essa outra tabela, Rejewski saberia os ajustes dos misturadores para a chave diária, pois as correntes eram como “impressões digitais”.

Ainda faltava estabelecer a disposição dos fios no quadro de tomadas. Rejewski, então, retirou todos os fios do quadro, de modo que este não produzisse nenhum efeito.

Após isso, ele pegava um trecho do texto cifrado interceptado e datilografava na Enigma. Algumas frases reconhecíveis apareciam vagamente, como, por exemplo, alliveinberlin, que poderia significar “arrive in Berlin” (chega a Berlim). Assim ele sabia que as letras R e L conforme exemplo acima, foram ligadas e trocadas por um fio. Estabelecendo a disposição dos fios e descobrindo o ajuste dos misturadores, Rejewski completaria a decifração da chave diária, decifrando todas as mensagens interceptadas no dia.

Ele simplificou a tarefa de encontrar a chave diária, separando o problema de achar os ajustes dos misturadores do problema de detectar a disposição dos cabos no painel de tomadas.

O ataque de Rejewski contra a Enigma foi uma grande realização da criptoanálise.

### 13 CRIPTOGRAFIA COMPUTADORIZADA

Durante a Segunda Guerra Mundial os decifradores britânicos estavam na frente dos criadores de códigos alemães, pois os especialistas de Bletchley Park deram continuidade às iniciativas dos poloneses em desenvolver máquinas para quebra de códigos. Eles inventaram um aparelho decifrador, o Colossus, para combater a Lorenz, uma poderosíssima cifra alemã. Em 1943, a Colossus foi construída no centro de pesquisas dos correios, em Dollis Hill, Londres, e era uma máquina capaz de adaptar-se a diferentes problemas, ou seja, foi a precursora do moderno computador. A Colossus foi destruída depois da Segunda Guerra Mundial e sua planta de construção foi queimada. Com isso, outros cientistas receberam os créditos pela invenção do computador. Em 1945, na Universidade da Pensilvânia, foi criado o ENIAC, Electronic Numerical Integrator And Calculator, que consistia em 18 mil válvulas eletrônicas capazes de realizar cinco mil cálculos por segundo.

Usar um computador para cifrar uma mensagem é muito semelhante às formas tradicionais, mas existem três grandes diferenças significativas entre a cifragem computadorizada e a mecânica (que foi base de cifras como a Enigma). A primeira é que uma máquina de cifra é limitada pelo que se pode construir na prática e o computador pode simular uma máquina de cifragem mais complexa. Por exemplo, o computador pode ser programado para simular uma centena de misturadores cada um com uma rotação específica, em diversos sentidos, alguns desaparecendo, outros aparecendo à medida que a cifragem progride. Uma máquina mecânica com esse conceito é praticamente impossível de ser contruída.

A segunda diferença está na velocidade da cifragem computadorizada em relação à mecânica. A computadorizada é quase que instantânea ou dentro de um tempo razoável.

A terceira diferença é que o computador usa números ao invés de letras do alfabeto. Os computadores trabalham com números binários, sequências de um e zero conhecidas como dígitos binários, ou bits (binary digits). Essa conversão pode ser realizada através de diversos protocolos, tais como o ASCII, American Standard Code for Information Interchange (Código Padrão Americano para Troca de Informações). O ASCII reserva um número binário de sete dígitos para cada letra do alfabeto. Existem 128 (2<sup>7</sup>) maneiras de se arrumar uma combinação

de sete dígitos binários, ou seja, é o suficiente para definir todas as letras minúsculas, pontuação e símbolos.

<u>Números binários em ASCII para letras maiúsculas</u>			
A	0100 0001	N	0100 1110
B	0100 0010	O	0100 1111
C	0100 0011	P	0101 0000
D	0100 0100	Q	0101 0001
E	0100 0101	R	0101 0010
F	0100 0110	S	0101 0011
G	0100 0111	T	0101 0100
H	0100 1000	U	0101 0101
I	0100 1001	V	0101 0110
J	0100 1010	W	0101 0111
K	0100 1011	X	0101 1000
L	0100 1100	Y	0101 1001
M	0100 1101	Z	0101 1010

Tabela 10 – Números binários em ASCII para letras maiúsculas.  
Fonte: Própria.

No início, devido ao alto custo, a computação era utilizada por pessoas ligadas ao governo e ao exército; mas após a invenção do transistor, em 1947, a computação comercial tornou-se realidade. Em 1960, os computadores tornaram-se mais poderosos e baratos e cada vez mais empresas compravam e mantinham computadores, podendo usá-los para cifrar comunicações importantes, tais como transferência de valores e negociações comerciais. À medida que empresas compravam computadores surgia um novo problema, que não existia enquanto o computador era de uso exclusivo do governo e dos militares. Nas empresas não havia padronização no sistema de cifragem, ou seja, não era garantido que uma mensagem enviada por uma empresa poderia ser decifrada, pois não poderia ter o mesmo sistema de cifragem. Foi então que em 1970 a IBM lançou o sistema de cifragem conhecido como Lucifer.

O Lucifer realiza a seguinte operação para cifrar uma mensagem: inicialmente, converte a mensagem numa fileira de dígitos binários; divide a fileira em blocos de 64 dígitos, onde a cifragem é feita separadamente em cada bloco. Finalmente, captura apenas um bloco de 64 dígitos e divide-os em dois blocos de 32 dígitos chamados de Esquerdo0 e Direito0, que passam por uma função “multiladora” que muda os dígitos de acordo com uma substituição complexa. O

Direito<sub>0</sub> multilado é somado ao Esquerdo<sub>0</sub> criando-se um novo bloco de 32 dígitos chamado de Direito<sub>1</sub>. O Direito<sub>0</sub> original é renomeado de Esquerdo<sub>1</sub>. Todo processo é repetido, mas começando pelos novos blocos Esquerdo<sub>1</sub> e Direito<sub>1</sub>. Esse processo é repetido até que se tenham completado 16 rodadas.

O Lucifer era considerado um dos mais poderosos sistemas de cifragem disponíveis comercialmente e foi utilizado por um grande número de organizações. O sistema seria adotado como padrão americano se não fosse a intervenção da NSA (Agência de Segurança Nacional). O Lucifer era tão poderoso que oferecia a possibilidade de um padrão de cifragem além da capacidade da própria NSA em decodificá-lo. Há rumores de que a NSA enfraqueceu um aspecto do Lucifer, diminuindo seu número de chaves possíveis antes de permitir que fosse adotado como padrão. A NSA limitou o número de chaves a aproximadamente 100.000.000.000.000.000 (tecnicamente se fala em 56 bits) e foi oficialmente liberada em 23 de novembro de 1976, batizada como DES, Data Encryption Standard (Padrão de Cifragem de Dados). Um quarto de século depois, a DES continua sendo o padrão oficial americano para a cifragem.

Apesar da força da DES, as empresas ainda lidavam com o grande problema da distribuição de chaves, que tem prejudicado a criptografia ao longo de sua história. Parece uma questão banal, mas para duas partes comunicar-se entre si, é preciso confiar a uma terceira a entrega de uma chave.

## 14 TROCA SEGURA DE CHAVES

Whitfield Diffie foi um grande matemático e criptógrafo norte-americano. Diffie estava particularmente interessado no problema de distribuição de chaves, e sabia que, se encontrasse uma solução, entraria para a história como o maior criptógrafo dos tempos. Ele era motivado pela sua visão de um mundo conectado. Em 1960, o Departamento de Defesa dos Estados Unidos financiou uma organização de pesquisa de ponta chamada Agência de Projetos Avançados de Pesquisa (ARPA – Advanced Research Projects Agency). Surgiu, então, um projeto de redes de computadores conectados, batizado de ARPANet, que, em 1982, originou a internet. Hoje, milhões de pessoas de todas as partes do mundo utilizam-se dela para buscar informações, realizar transações comerciais e trocar e-mails.

Na fase embrionária da ARPANet, Diffie visualizou que essa superestrada de informação seria uma revolução digital. Ele acreditava que as pessoas deveriam ter o direito de garantir sua privacidade, cifrando mensagens, porém, isso exigia uma troca de chaves segura. As grandes corporações e o governo já enfrentavam o problema de distribuição de chave, e para o público doméstico isso poderia ser impossível. Diffie considerou o cenário de uma pessoa querendo realizar uma compra na internet e de como ela poderia enviar um e-mail para o vendedor, fornecendo seus dados bancários de maneira segura, onde apenas comprador e vendedor pudessem decifrá-los. Antes que duas pessoas possam partilhar uma informação secreta (mensagem cifrada) elas devem partilhar outro segredo, a chave para realizar a cifragem. A partir disso, Diffie começou a buscar obcecadamente a solução do problema. Para debater assuntos relacionados à criptografia, por padrão utilizam-se três personagens fictícios batizados de Alice, Bob e Eva. Normalmente discutem-se cenários onde Alice e Bob desejam trocar uma mensagem e Eva, interceptá-la.

Alice sempre enfrenta o problema de distribuição de chaves, pois precisa enviá-la em segurança para Bob, pois só assim conseguiria decifrar a mensagem. Uma maneira de resolver esse problema seria Alice e Bob encontrando-se semanalmente para trocar chaves suficientes que possam durar até o próximo encontro. Porém o primeiro problema surgiria quando Alice ou Bob ficasse doente, impedindo a troca de chaves, paralisando assim a comunicação. Caso Alice e Bob contratassem mensageiros para trocarem as chaves, o custo seria mais alto e o

processo menos seguro, já que envolveria uma terceira pessoa. Durante dois mil anos isso foi considerado um axioma da criptografia. Mas há um meio de desafiar esse axioma.

Supondo que Alice envia mensagens para Bob numa caixa trancada com um cadeado e que somente os dois possuem a chave, ainda assim, seria inevitável a troca de chaves.

Um novo cenário seria Alice enviando uma mensagem altamente secreta numa caixa de ferro com um cadeado (que somente Alice tem a chave) trancado por ela. Bob recebe a caixa e também tranca com seu próprio cadeado (que somente Bob possui a chave). Bob envia a caixa de volta para Alice contendo os dois cadeados. Alice recebe a caixa, destranca seu cadeado e reenvia a caixa somente com o cadeado de Bob. Ele pode então abrir a caixa que possui somente seu cadeado, e para qual possui a chave. Dessa forma foi possível provar que existe uma maneira de trocar uma mensagem segura sem que um precise da chave do outro.

Porém, esse modelo não é muito funcional na realidade, mas serviu de grande inspiração para Diffie procurar um método que solucionaria o problema de distribuição de chaves. Diffie e Martin Hellman (outro criptógrafo) realizaram diversas pesquisas fracassadas até que se concentraram no exame de várias funções matemáticas. A maior parte das funções matemáticas é classificada como funções de mão dupla, pois é fácil fazê-las e desfazê-las. Contudo, Diffie e Hellman não estavam interessados em funções de mão dupla então concentraram seus esforços nas funções de mão única. Uma função de mão única, como o próprio nome sugere, é bem difícil de desfazer. Uma analogia seria misturar tinta amarela com azul para produzir a tinta verde. É muito fácil misturar as tintas, mas quase impossível reverter o processo, o que torna isso uma função de mão única. Foi então que eles seguiram pelo campo da aritmética modular, onde há uma riqueza de funções de mão única. Depois de dois anos estudando a aritmética modular, Hellman provou que Alice e Bob poderiam estabelecer uma chave sem se encontrar, eliminando o axioma que durou séculos. A idéia de Hellman dependia da função de mão única da forma  $Yx \pmod{P}$ . Alice e Bob inicialmente deveriam escolher valores de  $Y$  e  $P$ , com restrição de que  $Y$  deveria ser menor que  $P$ . Eles podem comunicar-se sem preocupar-se com a segurança para trocar os valores, pois mesmo que seja interceptado, isso não

importará como demonstrado na tabela abaixo. Supondo que Alice escolheu 7 (Y=7) e Bob escolheu 11 (P=11), você verá que Alice e Bob poderão cifrar uma mensagem sem se encontrar.

	<b>Alice</b>	<b>Bob</b>
<i>Fase 1</i>	Alice escolhe o 3 por exemplo e mantém em segredo. Vamos chamar de <i>A</i> o número escolhido.	Bob escolhe o 6 por exemplo e mantém em segredo. Vamos chamar de <i>B</i> o número escolhido.
	↓	↓
<i>Fase 2</i>	Alice introduz o 3 na função de mão única $7^A(\text{mod } 11)$ : $7^3(\text{mod } 11) = 343(\text{mod } 11) = 2$	Bob introduz o 6 na função de mão única $7^B(\text{mod } 11)$ : $7^6(\text{mod } 11) = 117.649(\text{mod } 11) = 4$
	↓	↓
<i>Fase 3</i>	Alice atribui o resultado do cálculo de alfa e envia o resultado, 2, para Bob	Bob atribui o resultado do cálculo de beta e envia o resultado, 4, para Alice
	↓	↓
<i>A troca</i>	Esse é um momento crucial pois Alice e Bob estão trocando informações, e nesse momento Eva pode interceptar a mensagem, ou seja, os valores de <i>Y</i> e <i>P</i> ou 2 e 4. Contudo esses valores não são chaves, e por isso não importa que Eva os conheça.	
	↓	↓
<i>Fase 4</i>	Alice pega o resultado de Bob e calcula a solução de $\beta^A(\text{mod } 11)$ : $4^3(\text{mod } 11) = 64(\text{mod } 11)=9$	Bob pega o resultado de Alice e calcula a solução de $\alpha^B(\text{mod } 11)$ : $2^6(\text{mod } 11) = 64(\text{mod } 11)=9$
	↓	↓
<i>A chave</i>	Incrivelmente Alice e Bob terminaram com o mesmo número 9. Está e a chave.	

Tabela 11 - Cenário de troca de informações entre Alice e Bob.

Fonte: Própria.

Embora o sistema pareça perfeito e realmente foi um grande salto, não era perfeito, pois existia o inconveniente de um transmitir para o outro, sem preocupar-se mais com a segurança, os valores de suas partes de chaves. Ou seja, o ideal seria que os dois estivessem conectados ao mesmo tempo, e isso prejudicaria a espontaneidade do e-mail.

De qualquer forma Hellman provou que não era necessário que Alice e Bob se encontrassem para obter uma chave secreta, mas ainda assim o esquema deveria ser mais eficiente.

## 15 CRIPTOGRAFIA DE CHAVE PÚBLICA

O sistema elaborado por Hellman era simétrico, pois ambos, o emissor e receptor, possuem um conhecimento equivalente e usam a mesma chave para cifrar e decifrar. No sistema assimétrico, a chave de cifragem e decifragem não seria idêntica, ou seja, se Alice sabe a chave de cifragem, poderia cifrar uma mensagem, mas não decifrá-la, por isso uma cifra assimétrica é tão especial.

Assim num cenário assimétrico, Alice poderia criar seu próprio par de chaves, sendo uma chave de cifragem e outra de decifragem. Alice manteria em segredo sua chave de decifragem, o que chamamos de *chave particular*. A chave de cifragem, o que chamamos de *chave pública*, seria divulgada para todos que desejam enviar mensagens à Alice. Bob então usa a *chave pública* de Alice para enviar uma mensagem que somente é possível decifrá-la com a *chave particular* de Alice. As grandes vantagens desse sistema são:

- Não há troca de chaves como no sistema de Diffie.
- Bob também não precisa aguardar o recebimento de uma informação de Alice para dar continuidade a sua cifragem.
- Alice não precisa enviar sua *chave pública* em segurança para Bob, pelo contrário, Alice deseja que todos tenham conhecimento de sua *chave pública*.
- O conhecimento da *chave pública*, não ajudará em nada no processo de decifragem para quem não tem o conhecimento da *chave privada*.

Voltando à analogia dos cadeados, podemos visualizar a criptografia assimétrica da seguinte maneira: qualquer pessoa pode fechar (cifrar) um cadeado simplesmente apertando o seu fecho, mas só quem possui a chave pode abri-lo (decifrar). Avançando um pouco mais na analogia, Alice poderia projetar um cadeado e uma chave. Guardaria a chave em segurança, fabricaria e distribuiria milhares de cópias do cadeado para que qualquer pessoa pudesse transmitir uma mensagem de forma segura.

Então, iniciou-se uma nova empreitada em busca de uma função matemática que realizasse o mesmo conceito, e que fosse incorporado num sistema criptográfico operacional.

## 16 RSA – INCORPORAÇÃO DA CHAVE PÚBLICA

Rivest, cientista da computação com uma enorme capacidade para absorver novas idéias; Shamir, outro cientista da computação com um ágil intelecto e grande facilidade em descartar coisas irrelevantes e Adleman, um matemático com grande capacidade em detectar falhas, formavam uma equipe perfeita. Juntos, buscavam uma solução para a criação da seguinte cifra assimétrica:

- Alice deveria criar uma chave pública, e divulgá-la de modo que todos tivessem conhecimento e pudessem usá-la para cifrar mensagens para ela. Como a chave pública deveria ser uma função de mão única, seria praticamente impossível para todos revertê-la e decifrar a mensagem de Alice.
- Alice precisaria decifrar as mensagens enviadas para ela. Ela deveria, portanto possuir uma chave particular, um fragmento especial de informação que possibilitaria reverter o efeito da chave pública. Dessa forma, somente Alice teria o poder de decifrar mensagens enviadas para ela.

O sistema de criptografia assimétrica, criado por eles, ficou conhecido como RSA (iniciais de Rivest, Shamir e Adleman) e é chamado de criptografia de *chave pública*. O núcleo da cifra assimétrica de Rivest estaria numa função de mão única baseada nas funções modulares. Um aspecto particular da cifra é conhecido simplesmente como  $N$ , porque é o  $N$  que torna a função reversível sob certas circunstâncias.

O  $N$  é importante por ser um componente flexível em que cada pessoa pode escolher um valor diferente, personalizando assim sua função de mão única. Voltando ao cenário de Alice, Bob e Eva, para detalhar o conceito, Alice escolhe dois números primos,  $p$  e  $q$ , e os multiplica. O  $N$  é a chave pública de Alice e o  $p$  e  $q$  são a chave particular dela. Por exemplo:  $p = 17.159$  e  $q = 10.247$ , o resultado da multiplicação é  $N = 17.159 \times 10.247 = 175.828.273$ . O resultado de  $N$  será a chave pública de Alice. Caso Bob deseje transmitir uma mensagem para Alice, ele utiliza a chave pública dela, o valor de  $N$  (175.828.273) e o insere na função de mão única que é de conhecimento geral, no caso a cifra RSA. Agora Bob pode cifrar uma mensagem para Alice.

Todos que conhecem o valor de  $N$  (a chave pública) podem deduzir o valor de  $p$  e  $q$ , afinal,  $N$  foi criado a partir de  $p$  e  $q$ . Porém, se o valor for suficientemente grande, será virtualmente impossível deduzir os valores. Isso seria possível realizando uma fatoração. Por exemplo, caso Eva intercepte a chave 408.508.091 e utilize a calculadora para realizar a fatoração, ela levaria uma média de 500 minutos, ou 8 horas para encontrar os valores de  $p$  e  $q$ .

Para aumentar a segurança da chave, basta escolher números primos tão grandes como  $10^{65}$ . Uma estimativa de fatoração utilizando um computador modelo Intel Pentium de 100 Mhz e 8 MB de RAM é de 50 anos. Para importantes transações bancárias,  $N$  deve ser em torno de  $10^{308}$ .

## 17 A CRIPTOGRAFIA COMO AGENTE MOTIVADOR NO PROCESSO ENSINO-APRENDIZAGEM

Há mais de 50 anos, Brownell notou que estudantes do Ensino Fundamental têm grande dificuldade em fazer cálculos com números desprovidos de situações concretas (como por exemplo,  $3 + 8$ ) do que quando é associado a uma unidade (por exemplo, 3 batatas + 8 batatas). Quando as unidades são omitidas, a soma torna-se uma abstração de difícil memorização. O mesmo ocorre com estudantes do Ensino Médio com questões de funções cuja situação não é real. Quando o aluno estuda funções em situações reais (por exemplo, com as relações:  $x = \text{tempo}$  e  $y = \text{espaço}$ , no lançamento de uma bola), consegue chegar com mais facilidade a um resultado matemático, através da situação real exemplificada.

Uma maneira de o professor materializar a matemática seria apresentando aos alunos a origem da criptografia, e a presença dela no cotidiano, através de movimentações bancárias e outras transações eletrônicas presentes na internet. Dessa forma, contando pequenas histórias interessantes, conforme as palavras de Augusto Cury, o aluno ficará fascinado e terá prazer em aprender a matéria. “[...] Não apenas tenha o hábito de dialogar, mas de contar histórias. Cativem seus filhos pela sua inteligência e afetividade, não pela sua autoridade, dinheiro ou poder” (CURY, 2003, p. 47).

Ainda segundo Cury, a humanização do conhecimento tem como objetivo estimular a ousadia, promover perspicácia, cultivar a criatividade, incentivar a sabedoria, expandir a capacidade crítica e formar pensadores.

“[...] A melhor maneira de produzir pessoas que não pensam é nutrilas com um conhecimento sem vida, despersonalizado. [...] Produzir uma nova teoria, é mais complexo do que fazer centena de pesquisas. Mas nem todos valorizam esse trabalho. [...] Por trás de cada informação dada com tanta simplicidade em sala de aula existem as lágrimas, as aventuras e a coragem dos cientistas. Mas os alunos não conseguem enxergá-las. [...] A ciência sem rosto paraliza a inteligência, descaracteriza o ser, o aproxima do nada” (CURY, 2003, p. 135-136).

## 17.1 FUNÇÃO DO PRIMEIRO GRAU

### 17.1.1 Pré-requisito

Para ensinar função do primeiro grau, o aluno deve ter conhecimento de definição de funções, diagrama de flechas, domínio e contradomínio, gráficos, noções básicas do plano cartesiano, construção de gráficos e análise de gráficos.

### 17.1.2 Definição

Chama-se *função do primeiro grau*, ou *função afim*, a qualquer função  $f$  de  $\mathbb{R}$  em  $\mathbb{R}$  dada por uma lei da forma  $f(x) = ax + b$ , onde  $a$  e  $b$  são números reais dados e  $a \neq 0$ .

Na função  $f(x) = ax + b$ , o número  $a$  é chamado de coeficiente de  $x$  e o número  $b$  é chamado termo constante. Exemplos:

$$1^{\circ}) f(x) = 5x - 3, \text{ onde } a = 5 \text{ e } b = -3$$

$$2^{\circ}) f(x) = \frac{x}{3} + \frac{2}{5}, \text{ onde } a = \frac{1}{3} \text{ e } b = \frac{2}{5}$$

$$3^{\circ}) f(x) = 11x, \text{ onde } a = 11 \text{ e } b = 0$$

### 17.1.3 Gráfico

O gráfico de uma função de primeiro grau,  $y = ax + b$ , com  $a \neq 0$ , é uma reta oblíqua aos eixos  $0x$  e  $0y$ .

Na figura 8, quando aumentamos o valor de  $x$ , os correspondentes valores de  $y$  também aumentam. Logo a função é crescente quando o coeficiente de  $x$  é positivo ( $a > 0$ ).

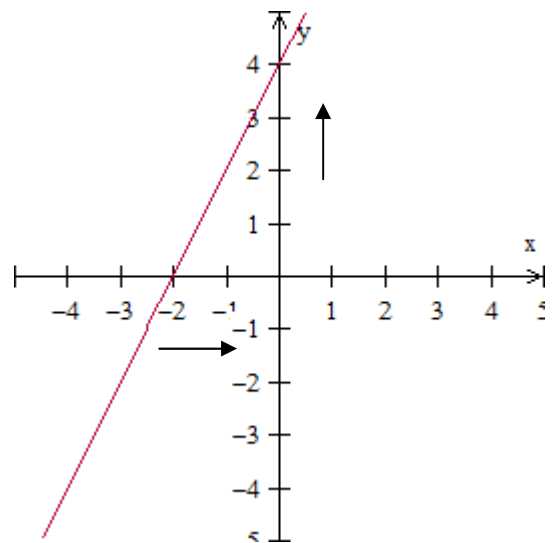


Figura 8 - Gráfico da função do primeiro grau com  $a > 0$ .

Fonte: Própria.

Na figura 9, quando aumentamos o valor de  $x$ , os correspondentes valores de  $y$  diminuem. Logo a função é decrescente quando o coeficiente de  $x$  é negativo ( $a < 0$ ).

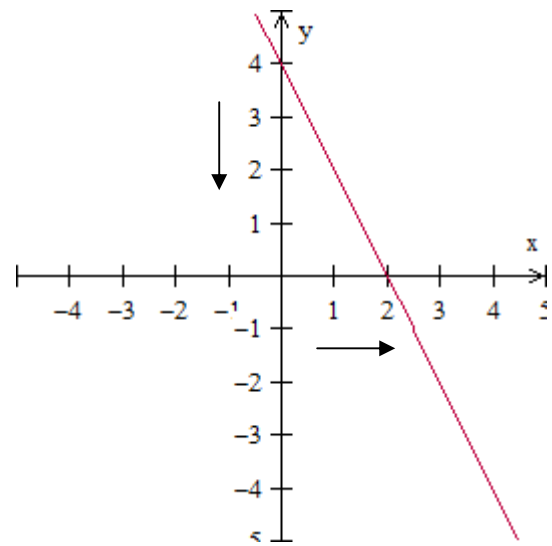


Figura 9 - Gráfico da função do primeiro grau com  $a < 0$ .

Fonte: Própria.

#### Exemplos:

1º)  $y = 3x - 1$

Como o coeficiente de  $x$  é positivo ( $a > 0$ ) a função é crescente. Conforme ilustrado na figura 10.

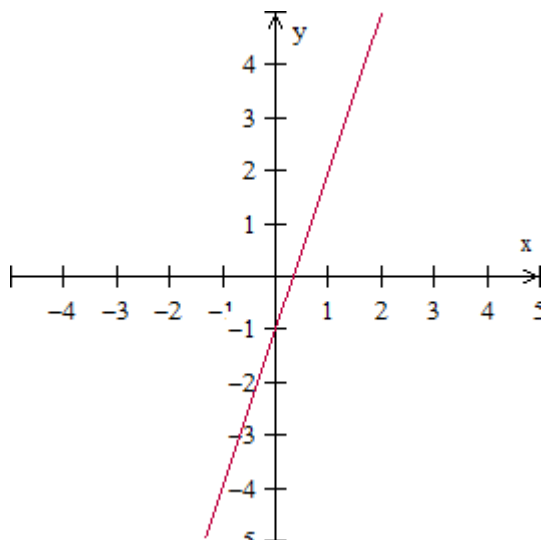


Figura 10 - Gráfico da função do primeiro grau do 1º exemplo.

Fonte: Própria.

2º)  $y = -2x + 3$

Como o coeficiente de  $x$  é negativo ( $a < 0$ ) a função é decrescente. Conforme ilustrado na figura 11.

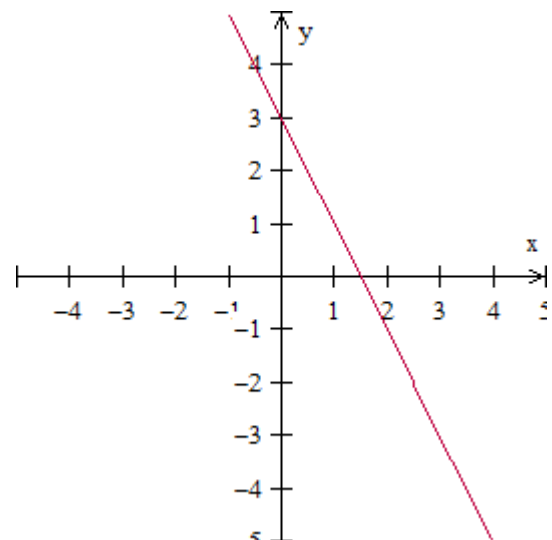


Figura 11 - Gráfico da função do primeiro grau do 2º exemplo.

Fonte: Própria.

### 17.1.4 Coeficientes da função afim

O gráfico da função afim  $y = ax + b$  é uma reta.

O *coeficiente* de  $x$ ,  $a$ , é chamado *coeficiente angular* da reta e, como veremos adiante,  $a$  está ligado à inclinação da reta em relação ao eixo  $Ox$ .

O *termo constante*,  $b$ , é chamado *coeficiente linear* da reta. Para  $x = 0$ , temos  $y = a \cdot 0 + b = b$ .

Assim, o coeficiente linear é a ordenada do ponto em que a reta corta o eixo  $Oy$ .

### 17.1.5 Zero e equações do primeiro grau

Chama-se *zero* ou *raiz* da função do primeiro grau  $f(x) = ax + b$ ,  $a \neq 0$ , o número real  $x$  tal que  $f(x) = 0$ .

Temos:

$$f(x) = 0 \Rightarrow ax + b = 0 \Rightarrow x = -\frac{b}{a}$$

Então, a *raiz* da função  $f(x) = ax + b$  é a solução da equação do primeiro grau  $ax + b = 0$ , ou seja,  $x = -\frac{b}{a}$ .

Exemplos:

1º) Obtenção do *zero* da função  $f(x) = 2x - 5$ :

$$f(x) = 0 \Rightarrow 2x - 5 = 0 \Rightarrow x = \frac{5}{2}$$

2º) Cálculo da *raiz* da função  $g(x) = 3x + 6$ :

$$g(x) = 0 \Rightarrow 3x + 6 = 0 \Rightarrow x = -2$$

### 17.1.6 Sinal da função

Estudar o sinal de uma função qualquer  $y = f(x)$  é determinar os valores de  $x$  para os quais  $y$  é positivo, os valores de  $x$  para os quais  $y$  é zero e os valores de  $x$  para os quais  $y$  é negativo.

Consideremos uma função afim  $y = f(x) = ax + b$  e vamos estudar seu sinal. Já vimos que essa função se anula para  $x = -\frac{b}{a}$  (raiz). Há dois casos possíveis:

1º)  $a > 0$  (a função é crescente)

$$y > 0 \Rightarrow ax + b > 0 \Rightarrow x > -\frac{b}{a}$$

$$y < 0 \Rightarrow ax + b < 0 \Rightarrow x < -\frac{b}{a}$$

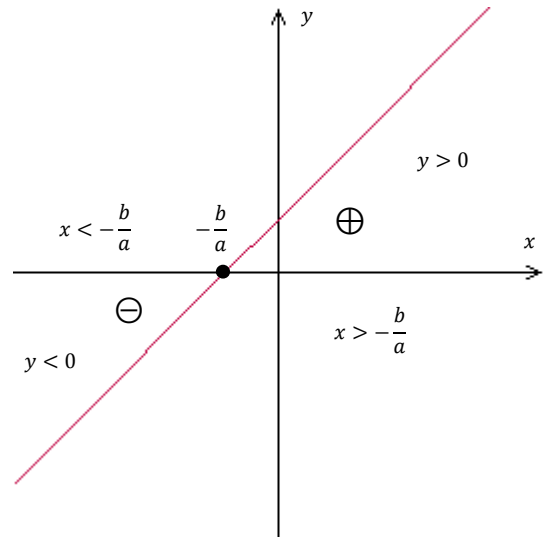


Figura 12 - Gráfico do estudo do sinal da função do primeiro grau com  $a > 0$ .

Fonte: Própria.

Conclusão:  $y$  é positivo para valores de  $x$  maiores que a raiz e  $y$  é negativo para valores de  $x$  menores que a raiz.

2º)  $a < 0$  (a função é decrescente)

$$y > 0 \Rightarrow ax + b > 0 \Rightarrow x < -\frac{b}{a}$$

$$y < 0 \Rightarrow ax + b < 0 \Rightarrow x > -\frac{b}{a}$$

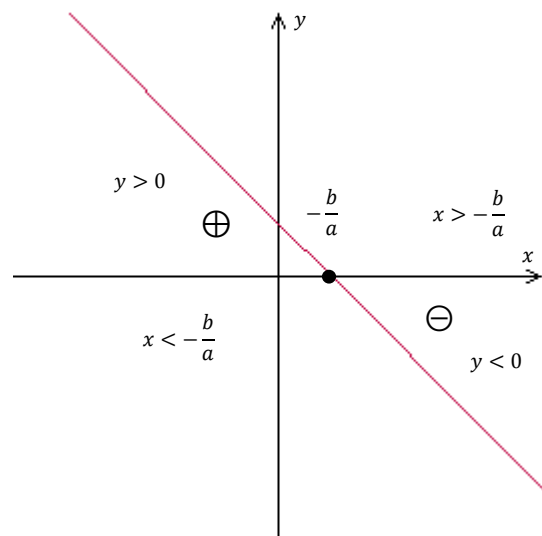


Figura 13 - Gráfico do estudo do sinal da função do primeiro grau com  $a < 0$ .

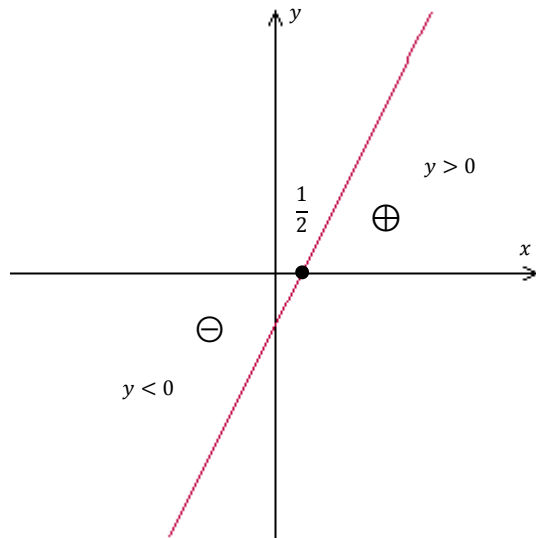
Fonte: Própria.

Conclusão:  $y$  é positivo para valores de  $x$  menores que a raiz e  $y$  é negativo para valores de  $x$  maiores que a raiz.

Exemplos:

1º)  $y = 2x - 1$ :

A função do 1º grau apresenta  $a = 2 > 0$  e raiz  $x = \frac{1}{2}$ . Seu gráfico é crescente e corta o eixo  $0x$  no ponto  $\frac{1}{2}$ .



**Sinal**

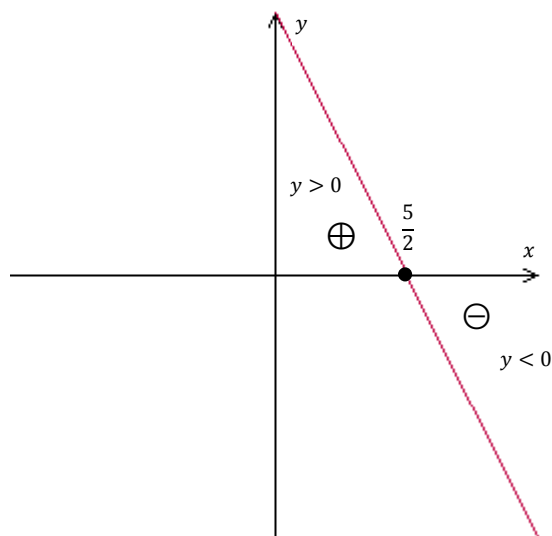
$$y > 0 \Rightarrow x > \frac{1}{2}$$

$$y < 0 \Rightarrow x < \frac{1}{2}$$

Figura 14 - Gráfico do estudo do sinal da função do primeiro grau do 1º exemplo.  
Fonte: Própria.

2º)  $y = -2x + 5$ :

A função do 1º grau apresenta  $a = -2 < 0$  e raiz  $x = \frac{5}{2}$ . Seu gráfico é decrescente e corta o eixo  $0x$  no ponto  $\frac{5}{2}$ .



**Sinal**

$$y > 0 \Rightarrow x < \frac{5}{2}$$

$$y < 0 \Rightarrow x > \frac{5}{2}$$

Figura 15 - Gráfico do estudo do sinal da função do primeiro grau do 2º exemplo.  
Fonte: Própria.

### 17.1.7 Inequações do primeiro grau

Como resolver inequações do 1º grau e inequações em que pode ser aplicado o estudo de sinal da função afim. Exemplos:

$$1^{\circ} 4(x + 1) - 5 \leq 2(x + 3):$$

Essa inequação pode ser resolvida sem o estudo de sinal da função afim.

1º passo: desenvolver os parênteses:

$$4x + (4 - 5) \leq 2x + 6$$

2º passo: passar todos os termos que contêm a incógnita  $x$  para o 1º membro:

$$4x - 1 - 2x \leq 6$$

3º passo: passar todos os termos constantes para o 2º membro:

$$4x - 2x \leq 6 + 1$$

$$2x \leq 7$$

4º passo: dividir os dois membros pelo coeficiente de  $x$ :

$$x \leq \frac{7}{2}$$

$$S = \left\{ x \in R \mid x \leq \frac{7}{2} \right\}$$

(IEZZI; DOLCE; DEGENSZAJN; PÉRIGO, 1997, p. 44).

2º) Duas inequações simultâneas:  $1 \leq 2x + 3 < x + 5$

$$1 \leq 2x + 3 \text{ (I) e } 2x + 3 < x + 5 \text{ (II)}$$

Resolvendo a (I)  $1 \leq 2x + 3$ :

$$1 \leq 2x + 3 \Rightarrow -2x \leq 3 - 1 \Rightarrow -2x \leq 2 \Rightarrow x \geq -1$$

(Observação: ao dividir ambos os membros por um número negativo, devemos inverter o sentido da desigualdade.)

Resolvendo a (II)  $2x + 3 < x + 5$ :

$$2x + 3 < x + 5 \Rightarrow 2x - x < 5 - 3 \Rightarrow x < 2$$

Procura-se a interseção das duas soluções:

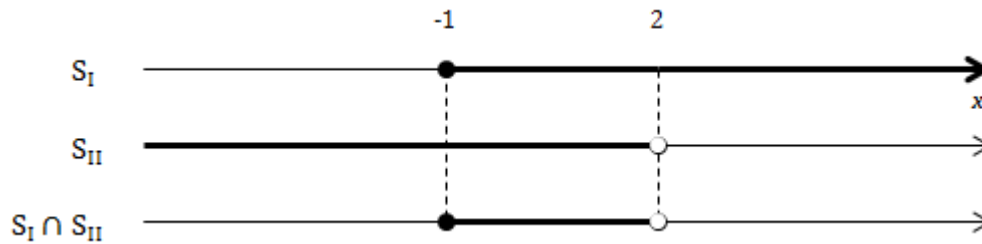


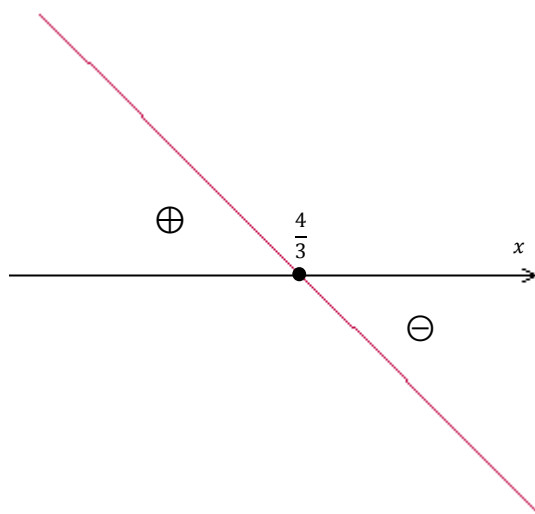
Figura 16 - Estudo do sinal da inequação do primeiro grau.

Fonte: Própria.

Solução final:  $-1 \leq x < 2 \Rightarrow S = \{x \in \mathbb{R} | -1 \leq x < 2\}$

3º) Inequação-produto  $(4 - 3x)(2x - 7) > 0$  :

Façamos  $y_1 = 4 - 3x$  e estudemos o sinal de  $y_1$ . Temos  $a = -3 < 0$  e raiz  $x = \frac{4}{3}$ . Então:



**Sinal**

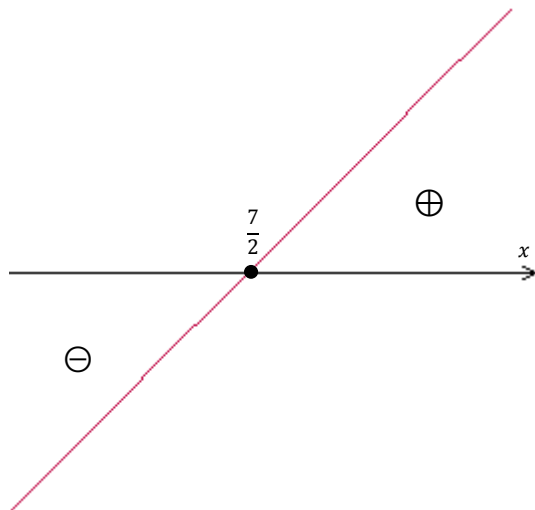
$$y_1 > 0 \Rightarrow x < \frac{4}{3}$$

$$y_1 < 0 \Rightarrow x > \frac{4}{3}$$

Figura 17 - Gráfico do estudo do sinal da inequação-produto com  $a < 0$ .

Fonte: Própria.

Façamos  $y_2 = 2x - 7$  e estudemos o sinal de  $y_2$ . Temos  $a = 2 > 0$  e raiz  $x = \frac{7}{2}$ . Então:



**Sinal**

$$y_2 > 0 \Rightarrow x > \frac{7}{2}$$

$$y_2 < 0 \Rightarrow x < \frac{7}{2}$$

Figura 18 - Gráfico do estudo do sinal da inequação-produto com  $a > 0$ .

Fonte: Própria.

Estudemos agora o sinal do produto  $y_1 \cdot y_2$ :

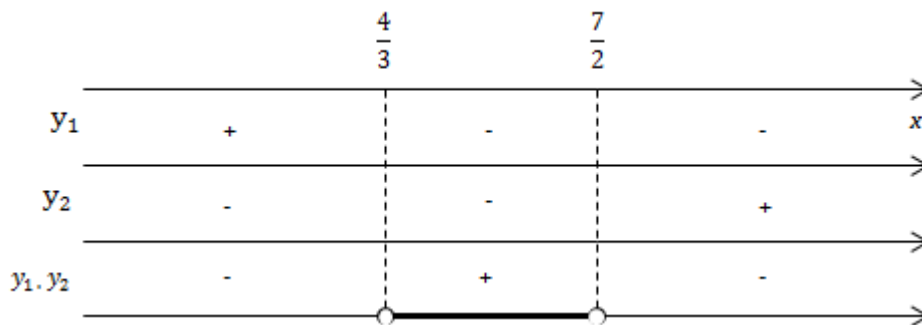


Figura 19 - Estudo do sinal da inequação-produto do primeiro grau.

Fonte: Própria.

A inequação pergunta: “para que valores de  $x$  temos  $y_1 \cdot y_2 > 0$ ?”.

Resposta:  $\frac{4}{3} < x < \frac{7}{2}$ .

4º) Inequação-quociente  $\frac{10x-15}{5-4x} \leq 0$ :

Estudo de sinal de  $y_1 = 10x - 15$

$a = 10 > 0$  e raiz  $x = \frac{3}{2}$

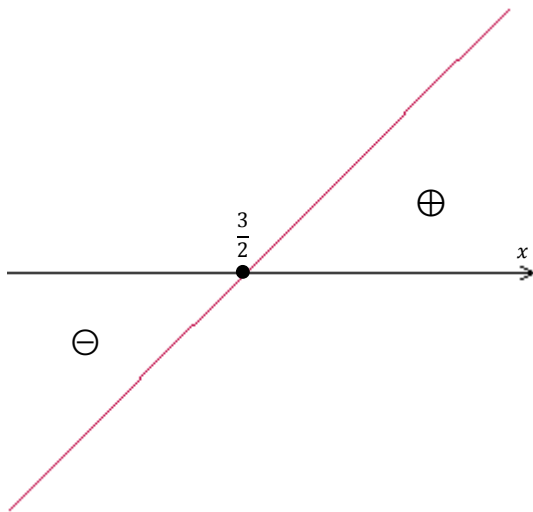


Figura 20 - Gráfico do estudo do sinal da inequação-quociente com  $a > 0$

Fonte: Própria.

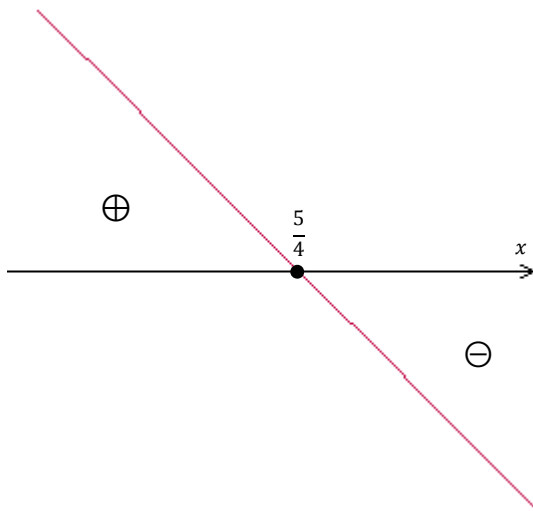
### Sinal

$$y_1 > 0 \Rightarrow x > \frac{3}{2}$$

$$y_1 < 0 \Rightarrow x < \frac{3}{2}$$

Estudo de sinal de  $y_2 = 5 - 4x$

$$a = -4 < 0 \text{ e raiz } x = \frac{5}{4}$$



### Sinal

$$y_2 > 0 \Rightarrow x < \frac{5}{4}$$

$$y_2 < 0 \Rightarrow x > \frac{5}{4}$$

Figura 21 - Gráfico do estudo do sinal da inequação-quociente com  $a < 0$

Fonte: Própria.

Estudo de sinal do quociente  $\frac{y_1}{y_2}$

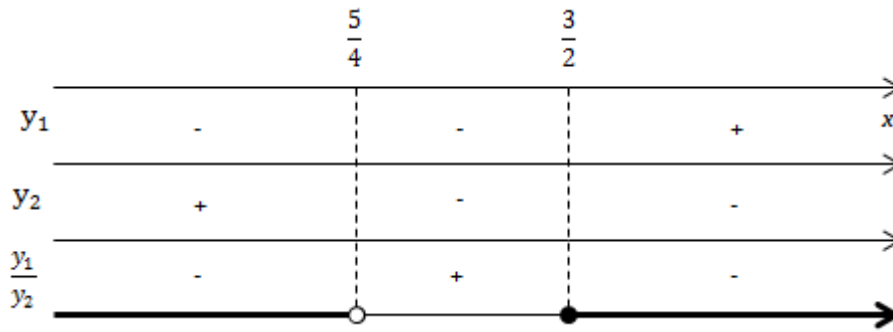


Figura 22 - Estudo do sinal da inequação-quociente do primeiro grau.  
 Fonte: Própria.

A inequação pergunta: “para que valores de  $x$  temos  $\frac{y_1}{y_2} \leq 0$ ?”.

Resposta:  $x < \frac{5}{4}$  ou  $x \geq \frac{3}{2}$ . (Notemos que  $\frac{y_1}{y_2} = 0$  ocorre para  $y_1 = 0$  e  $y_2 \neq 0$ . Isso nos obriga a incluir apenas a raiz de  $y_1$ .)

### 17.1.8 Aplicação do conceito na criptografia

O professor realiza uma pequena demonstração mostrando uma mensagem cifrada aos estudantes e realizando alguns cálculos matemáticos para decifrá-la, com isso o professor terá aguçado a curiosidade.

Ele distribui aos alunos uma tabela, contendo um alfabeto relacionado a números, que será utilizada nos exercícios.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Tabela 12 - Tabela alfa-numérica para exercícios com funções do primeiro grau.  
 Fonte: Própria.

Explica que para cifrar uma mensagem recai no problema de permutar números por meio de uma regra  $f$ . Faz isso de forma prática através das funções  $f(x) = ax + b$  com  $a, b$  inteiros,  $a \neq 0$ , definidas no conjunto  $\{0, 1, \dots, 26\}$ .

Exibe um exemplo de Alice querendo trocar uma mensagem sigilosa com Bob utilizando o alfabeto escolhido.

Explica o que é uma função do primeiro grau conforme citado anteriormente (17.1.2).

Definem juntos uma função cifradora, por exemplo:

$$f(x) = 2x - 3$$

Escolhem uma mensagem:

Estudar é divertido

Associam a sequência numérica:

mensagem e s t u d a r e d i v e r t i d o  
 sequência numérica 5 19 20 21 4 1 18 0 5 0 4 9 22 5 18 20 9 4 15

Obtém a mensagem que será transmitida através das imagens de  $f$ :

7 35 37 39 5 -1 33 -3 7 -3 5 15 41 7 33 37 15 5 27

Decifram a mensagem calculando a imagem da função inversa de  $f^{-1}(x) = \frac{x+3}{2}$  nessa sequência e utilizando a tabela alfabeto-númerica, obtém a mensagem original.

Após os alunos dominarem o processo, o professor divide a sala em dois grupos, onde cada grupo definiria uma função cifradora e uma mensagem. Os grupos devem trocar as funções e mensagens para que sejam decifradas.

## 17.2 MATRIZES

### 17.2.1 Definição

Sendo  $m$  e  $n$  números naturais e não nulos, chama-se *matriz  $m$  por  $n$*  (indica-se  $m \times n$ ) toda tabela  $M$  formada por números reais distribuídos em  $m$  linhas e  $n$  colunas.

Exemplos:

$$1^{\circ}) \begin{bmatrix} 3 & 5 & -1 \\ 0 & \frac{4}{5} & \sqrt{2} \end{bmatrix} \text{ é matriz } 2 \times 3.$$

$$2^{\circ}) \begin{bmatrix} 4 & -3 \\ \frac{3}{7} & 2 \\ 4 & 1 \end{bmatrix} \text{ é matriz } 3 \times 2.$$

$$3^{\circ}) \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \text{ é matriz } 2 \times 2.$$

$$4^{\circ}) [2] \text{ é matriz } 1 \times 1.$$

Em uma matriz qualquer  $M$ , cada elemento é indicado por  $a_{ij}$ , onde o índice  $i$  indica a linha e o índice  $j$  a coluna às quais o elemento pertence. As linhas são numeradas de cima para baixo (de 1 até  $m$ ) e as colunas da esquerda para a direita (de 1 até  $n$ ). Uma matriz  $m \times n$  é representada por:

$$M = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} \text{ ou } M = \left( \begin{array}{cccc} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{array} \right) \text{ ou}$$

$$M = \left\| \begin{array}{cccc} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{array} \right\|$$

Os exemplos acima mostram as três formas possíveis de representação de uma matriz: parênteses, colchetes e dois pares de barras verticais.

Uma matriz  $M$  do tipo  $m \times n$  também pode ser indicada por:

$$M = (a_{ij})$$

$$i \in \{1, 2, 3, \dots, m\} \text{ e } j \in \{1, 2, 3, \dots, n\}$$

$$\text{Ou simplesmente } M = (a_{ij})_{m \times n}.$$

## 17.2.2 Matrizes especiais

Algumas matrizes apresentam uma utilidade maior nesta teoria e por isso recebem nomes especiais:

### 17.2.2.1 Matriz linha

*Matriz linha* é toda matriz do tipo  $1 \times n$ , isto é, possui uma única linha.

Exemplo:

$$[0 \ 9 \ -1 \ 7] \text{ é matriz } 1 \times 4$$

### 17.2.2.2 Matriz coluna

*Matriz coluna* é toda matriz do tipo  $m \times 1$ , isto é, possui uma única coluna. Exemplo:

$$\begin{bmatrix} 5 \\ 1 \\ -3 \end{bmatrix} \text{ é matriz } 3 \times 1$$

### 17.2.2.3 Matriz nula

*Matriz nula* é toda matriz que tem os elementos iguais a zero.

Exemplos:

$$1^{\text{a}}) \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \text{ é a matriz nula do tipo } 2 \times 3.$$

2º)  $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$  é a matriz nula do tipo 2 x 2.

#### 17.2.2.4 Matriz quadrada

*Matriz quadrada de ordem n* é toda matriz do tipo  $n \times n$ , isto é, possui número de linhas e colunas iguais. Exemplo:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{bmatrix}$$

Chama-se *diagonal principal* de uma matriz quadrada de ordem  $n$  o conjunto dos elementos que têm os dois índices iguais, isto é:

$$\{a_{ij} \mid i = j\} = \{a_{11}, a_{22}, a_{33}, \dots, a_{nn}\}$$

Chama-se *diagonal secundária* de uma matriz quadrada de ordem  $n$  o conjunto dos elementos que têm a soma dos índices igual a  $n + 1$ , isto é:

$$\{a_{ij} \mid i + j = n + 1\} = \{a_{1n}, a_{2,n-1}, a_{3,n-2}, \dots, a_{n1}\}$$

Exemplos:

1º) A matriz  $M = \begin{bmatrix} 8 & 9 & -7 \\ 6 & 4 & -5 \\ -1 & 2 & 3 \end{bmatrix}$  é quadrada de ordem 3. Sua diagonal principal é  $\{8, 4, 3\}$  e sua diagonal secundária é  $\{-7, 4, -1\}$ .

2º) A matriz  $M = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \\ 8 & 9 & -1 & -2 \\ -3 & -4 & -5 & -6 \end{bmatrix}$  é quadrada de ordem 4. Sua diagonal principal é  $\{0, 5, -1, -6\}$  e sua diagonal secundária é  $\{3, 6, 9, -3\}$ .

#### 17.2.2.5 Matriz diagonal

*Matriz diagonal* é toda matriz quadrada em que os elementos que não pertencem à diagonal principal são iguais a zero. Exemplos:

1º)  $\begin{bmatrix} 3 & 0 \\ 0 & -2 \end{bmatrix}$

2º)  $\begin{bmatrix} 4 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -3 \end{bmatrix}$

3º)  $\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$

$$4^{\circ}) \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$5^{\circ}) \begin{bmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

### 17.2.3 Igualdade de matrizes

Duas matrizes  $A = (a_{ij})_{m \times n}$  e  $B = (b_{ij})_{m \times n}$  são iguais quando  $a_{ij} = b_{ij}$  para todo  $i (i \in \{1, 2, 3, \dots, m\})$  e todo  $j (j \in \{1, 2, 3, \dots, n\})$ . Isto significa que para as duas matrizes serem iguais, devem ser do mesmo tipo e apresentar todos os elementos correspondentes iguais (elementos com índices iguais). Exemplos:

$$1^{\circ}) \begin{bmatrix} 1 & -3 \\ 7 & -4 \end{bmatrix} = \begin{bmatrix} 1 & -3 \\ 7 & -4 \end{bmatrix} \text{ pois } a_{11} = b_{11}, a_{12} = b_{12}, a_{21} = b_{21} \text{ e } a_{22} = b_{22}.$$

$$2^{\circ}) \begin{bmatrix} 1 & -3 \\ 7 & -4 \end{bmatrix} \neq \begin{bmatrix} 1 & 7 \\ -3 & -4 \end{bmatrix} \text{ pois } a_{12} \neq b_{12} \text{ e } a_{21} \neq b_{21}.$$

3<sup>o</sup>) Determinemos  $a, b, c, d$  de modo que se tenha

$$\begin{pmatrix} a & 1 \\ 1 & b+1 \\ c-2 & d \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \\ 6 & 3 \end{pmatrix}:$$

Observando os elementos correspondentes, devemos ter

$$\begin{cases} a = 2 \\ b + 1 = 1 \Rightarrow b = 0 \\ c - 2 = 6 \Rightarrow c = 8 \\ d = 3 \end{cases}$$

### 17.2.4 Adição

Dadas duas matrizes  $A = (a_{ij})_{m \times n}$  e  $B = (b_{ij})_{m \times n}$ , chama-se *soma*  $A+B$  a matriz  $C = (c_{ij})_{m \times n}$  tal que  $c_{ij} = a_{ij} + b_{ij}$ , para todo  $i$  e todo  $j$ . Isto significa que a soma de duas matrizes  $A$  e  $B$  do tipo  $m \times n$  é uma matriz  $C$  do mesmo tipo em que cada elemento é a soma dos elementos correspondentes em  $A$  e  $B$ . Exemplos:

$$1^{\circ}) \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} + \begin{bmatrix} 4 & -1 & 1 \\ -4 & 0 & -6 \end{bmatrix} = \begin{bmatrix} 1+4 & 2-1 & 3+1 \\ 4-4 & 5+0 & 6-6 \end{bmatrix} = \begin{bmatrix} 5 & 1 & 4 \\ 0 & 5 & 0 \end{bmatrix}$$

$$2^{\circ}) \begin{bmatrix} 7 & 8 \\ 9 & 9 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix} = \begin{bmatrix} 7+0 & 8+1 \\ 9+2 & 9+3 \end{bmatrix} = \begin{bmatrix} 7 & 9 \\ 11 & 12 \end{bmatrix}$$

#### 17.2.4.1 Matriz oposta

Seja a matriz  $A = (a_{ij})_{m \times n}$ . Chama-se oposta de  $A$  a matriz representada por  $-A$ , tal que  $A + (-A) = 0$ , onde  $0$  é a matriz nula do tipo  $m \times n$ .

Da definição, decorre que  $-A$  é sempre obtida de  $A$  trocando-se o sinal de cada um de seus elementos (IEZZI; DOLCE; DEGENSZAJN; PÉRIGO, 1997, p. 365).

Exemplo:

$$\text{Se } A = \begin{pmatrix} 5 & -1 \\ -4 & 3 \end{pmatrix}, \text{ então } -A = \begin{pmatrix} -5 & 1 \\ 4 & -3 \end{pmatrix}.$$

#### 17.2.4.2 Matriz diferença

Dadas duas matrizes,  $A = (a_{ij})_{m \times n}$  e  $B = (b_{ij})_{m \times n}$ , definimos a matriz diferença  $A-B$  como a soma de  $A$  com a oposta de  $B$ ; isto é:  $A - B = A + (-B)$ .

Exemplos:

$$1^{\circ}) \begin{pmatrix} 2 & 5 \\ -1 & 6 \\ 4 & -2 \end{pmatrix} - \begin{pmatrix} -2 & 3 \\ 2 & 5 \\ 3 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 5 \\ -1 & 6 \\ 4 & -2 \end{pmatrix} + \begin{pmatrix} 2 & -3 \\ -2 & -5 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 2 \\ -3 & 1 \\ 1 & -1 \end{pmatrix}$$

$$2^{\circ}) \begin{pmatrix} 0 & 1 \\ -3 & 2 \end{pmatrix} - \begin{pmatrix} 1 & -1 \\ -2 & 5 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -3 & 2 \end{pmatrix} + \begin{pmatrix} -1 & 1 \\ 2 & -5 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ -1 & -3 \end{pmatrix}$$

#### 17.2.4.3 Propriedades da adição

A adição de matrizes do tipo  $m \times n$  apresenta as seguintes propriedades:

- É associativa:  $(A + B) + C = A + (B + C)$  quaisquer que sejam  $A$ ,  $B$  e  $C$  do tipo  $m \times n$ ;
- É comutativa:  $A + B = B + A$  quaisquer que sejam  $A$  e  $B$ , do tipo  $m \times n$ ;
- Tem elemento neutro:  $\exists M/A + M = A$  qualquer que seja  $A$  do tipo  $m \times n$ ;
- Todo elemento tem simétrico: para todo  $A$  do tipo  $m \times n$ :  $\exists A'/A + A' = M$ .

### 17.2.5 Multiplicação de um número real por uma matriz

Dado um número real  $k$ ,  $k \neq 0$  e uma matriz  $A = (a_{ij})_{m \times n}$ , chama-se produto  $kA$  a matriz  $B = (b_{ij})_{m \times n}$  tal que  $(b_{ij})_{m \times n} = k(a_{ij})_{m \times n}$  para todo  $i$  e todo  $j$ .

Isto significa que multiplicar uma matriz  $A$  por um número  $k$  é construir uma matriz  $B$  formada pelos elementos de  $A$  todos multiplicados por  $k$ . Exemplos:

$$1^{\circ}) 3 \cdot \begin{bmatrix} 1 & 7 & 2 \\ 5 & -1 & -2 \end{bmatrix} = \begin{bmatrix} 3 & 21 & 6 \\ 15 & -3 & -6 \end{bmatrix}$$

$$2^{\circ}) \frac{1}{2} \cdot \begin{bmatrix} 0 & 2 & 4 \\ 8 & 6 & 4 \\ 10 & 12 & -6 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 2 \\ 4 & 3 & 2 \\ 5 & 6 & -3 \end{bmatrix}$$

### 17.2.5.1 Propriedades da multiplicação de um número real por uma matriz

A multiplicação de um número real por uma matriz apresenta as seguintes propriedades:

- $a \cdot (b \cdot A) = (ab) \cdot A$
- $a \cdot (A + B) = a \cdot A + a \cdot B$
- $(a + b) \cdot A = a \cdot A + b \cdot A$
- $1 \cdot A = A$

Onde  $A$  e  $B$  são matrizes quaisquer do tipo  $m \times n$  e  $a$  e  $b$  são números reais quaisquer.

## 17.2.6 Multiplicação de matrizes

Dadas duas matrizes  $A = (a_{ij})_{m \times n}$  e  $B = (b_{jk})_{n \times p}$ , chama-se produto  $AB$  a matriz  $C = (c_{ik})_{m \times p}$  tal que:

$$c_{ik} = a_{i1} \cdot b_{1k} + a_{i2} \cdot b_{2k} + a_{i3} \cdot b_{3k} + \dots + a_{in} \cdot b_{nk} = \sum_{j=1}^n a_{ij} b_{jk}$$

Para todo  $i \in \{1, 2, \dots, m\}$  e todo  $k \in \{1, 2, \dots, p\}$ .

### 17.2.6.1 Observações:

- A definição dada garante a existência do produto  $AB$  somente se o número de colunas de  $A$  for igual ao número de linhas de  $B$ , pois  $A$  é do tipo  $m \times n$  e  $B$  é do tipo  $n \times p$ .
- A definição dada afirma que o produto  $AB$  é uma matriz que tem o número de linhas de  $A$  e o número de colunas de  $B$ , pois  $C = AB$  é do tipo  $m \times p$ .

- É muito importante notar que a multiplicação de matrizes não é comutativa, isto é, para duas matrizes quaisquer  $A$  e  $B$  é falso que  $AB = BA$  necessariamente.
- Ainda pela definição, um elemento  $c_{ik}$  da matriz  $AB$  deve ser obtido pelo procedimento seguinte:

- Toma-se a linha  $i$  da matriz  $A$ :

$$\boxed{a_{i1} \ a_{i2} \ a_{i3} \ \dots \ a_{in}} \quad (n \text{ elementos})$$

- Toma-se a coluna  $k$  da matriz  $B$ :

$$\begin{array}{c} \boxed{b_{1k}} \\ b_{2k} \\ b_{3k} \\ \vdots \\ b_{nk} \end{array} \quad (n \text{ elementos})$$

- Coloca-se a linha  $i$  de  $A$  na “vertical” ao lado da coluna  $k$  de  $B$ :

$$\begin{array}{c} \boxed{a_{i1}} \\ a_{i2} \\ a_{i3} \\ \vdots \\ a_{in} \end{array} \quad \begin{array}{c} \boxed{b_{1k}} \\ b_{2k} \\ b_{3k} \\ \vdots \\ b_{nk} \end{array}$$

- Calculam-se os  $n$  produtos dos elementos que ficaram lado a lado:

$$\begin{array}{c} \boxed{a_{i1} \times b_{1k}} \\ a_{i2} \times b_{2k} \\ a_{i3} \times b_{3k} \\ \vdots \\ a_{in} \times b_{nk} \end{array}$$

- Somam-se esses  $n$  produtos, obtendo  $c_{ik}$  (IEZZI; DOLCE; DEGENSZAJN; PÉRIGO, 1997, p. 369).

Exemplo:

$$\text{Dadas } A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \text{ e } B = \begin{bmatrix} 7 \\ 8 \\ 9 \end{bmatrix}, \text{ calcular } AB.$$

Sendo  $A$  do tipo  $2 \times 3$  e  $B$  do tipo  $3 \times 1$ , decorre que existe  $AB$  e é do tipo  $2 \times 1$ . Fazendo  $AB = C$ , devemos calcular  $c_{11}$  e  $c_{21}$ :

$$C = \begin{bmatrix} c_{11} \\ c_{21} \end{bmatrix} = \begin{bmatrix} (1^{\text{a}} \text{l. de } A \times 1^{\text{a}} \text{ c. de } B) \\ (2^{\text{a}} \text{l. de } A \times 1^{\text{a}} \text{ c. de } B) \end{bmatrix} =$$

$$= \begin{bmatrix} \left( \begin{array}{l} 1 \times 7 + \\ +2 \times 8 + \\ +3 \times 9 \end{array} \right) \\ \left( \begin{array}{l} 4 \times 7 + \\ +5 \times 8 + \\ +6 \times 9 \end{array} \right) \end{bmatrix} = \begin{bmatrix} (7 + 16 + 27) \\ (28 + 40 + 54) \end{bmatrix} = \begin{bmatrix} 50 \\ 122 \end{bmatrix}$$

### 17.2.6.2 Propriedades da multiplicação de matrizes

A multiplicação de matrizes apresenta as seguintes propriedades:

- É associativa:  $(AB)C = A(BC)$   
 quaisquer que sejam as matrizes  $A = (a_{ij})_{m \times n}$ ,  $B = (b_{jk})_{n \times p}$  e  $C = (c_{kl})_{p \times r}$ ;
- É distributiva à direita em relação à adição:  $(A + B)C = AC + BC$   
 quaisquer que sejam as matrizes  $A = (a_{ij})_{m \times n}$ ,  $B = (b_{ij})_{m \times n}$  e  $C = (c_{jk})_{n \times p}$ ;
- É distributiva à esquerda:  $C(A + B) = CA + CB$   
 quaisquer que sejam as matrizes  $A = (a_{ij})_{m \times n}$ ,  $B = (b_{ij})_{m \times n}$  e  $C = (c_{ki})_{p \times m}$ ;
- $(kA)B = A(kB) = k(AB)$   
 quaisquer que sejam o número  $k$  e as matrizes  $A = (a_{ij})_{m \times n}$  e  $B = (b_{jk})_{n \times p}$ .

### 17.2.7 Matriz identidade

*Matriz unidade* (ou *matriz identidade*) de ordem  $n$  (indica-se  $I_n$ ) é toda matriz diagonal em que os elementos da diagonal principal são iguais a 1. Exemplos:

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$I_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

#### 17.2.7.1 Observação:

A matriz identidade é o elemento neutro do produto de matrizes, quando este existir. Qualquer que seja a matriz quadrada  $A$ , tem-se  $A.I = A$  e  $I.A = A$ . Exemplos:

$$1^{\circ}) \begin{pmatrix} 2 & 3 \\ 1 & -5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & -5 \end{pmatrix}$$

$$2^{\circ}) \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -2 & 4 & 3 \\ 1 & 5 & 0 \\ 0 & 2 & 1 \end{pmatrix} = \begin{pmatrix} -2 & 4 & 3 \\ 1 & 5 & 0 \\ 0 & 2 & 1 \end{pmatrix}$$

### 17.2.8 Matriz transposta

Dada uma matriz  $A = (a_{ij})_{m \times n}$  chama-se *transposta de A* a matriz  $A^t = (a'_{ji})_{n \times m}$  tal que  $a'_{ji} = a_{ij}$ , para todo  $i$  e todo  $j$ . Isto significa que, por exemplo,  $a'_{11}, a'_{21}, a'_{31}, \dots, a'_{n1}$  são respectivamente iguais a  $a_{11}, a_{12}, a_{13}, \dots, a_{1n}$ ; vale dizer que a 1ª coluna de  $A^t$  é igual à 1ª linha de  $A$ . Repetindo o raciocínio, chegaríamos à conclusão de que as colunas de  $A^t$  são ordenadamente iguais às linhas de  $A$ . Exemplos:

$$1^{\circ}) A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Rightarrow A^t = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

$$2^{\circ}) A = \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} \Rightarrow A^t = \begin{bmatrix} a & d \\ b & e \\ c & f \end{bmatrix}$$

#### 17.2.8.1 Propriedades da matriz transposta

A matriz transposta apresenta as seguintes propriedades:

- $(A^t)^t = A$ , para toda matriz  $A = (a_{ij})_{m \times n}$ ;
- Se  $A = (a_{ij})_{m \times n}$  e  $B = (b_{ij})_{m \times n}$ , então  $(A + B)^t = A^t + B^t$ ,
- Se  $A = (a_{ij})_{m \times n}$  e  $k \in \mathbb{R}$ , então  $(kA)^t = kA^t$ ;
- Se  $A = (a_{ij})_{m \times n}$  e  $B = (b_{ij})_{n \times p}$  então  $(AB)^t = B^t A^t$ .

### 17.2.9 Matriz inversa

Seja  $A$  uma matriz quadrada de ordem  $n$ . Dizemos que  $A$  é a *matriz inversível* se existir uma matriz  $B$  tal que  $AB = BA = I_n$ . Neste caso,  $B$  é dita inversa de  $A$  e indicada por  $A^{-1}$ . Se  $A$  não é inversível, dizemos que  $A$  é uma matriz singular. Exemplo:

A inversa de  $A = \begin{pmatrix} 2 & 0 \\ 4 & -3 \end{pmatrix}$  é  $A^{-1} = \begin{pmatrix} \frac{1}{2} & 0 \\ \frac{2}{3} & -\frac{1}{3} \end{pmatrix}$ , pois:

$$A \cdot A^{-1} = \begin{pmatrix} 2 & 0 \\ 4 & -3 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2} & 0 \\ \frac{2}{3} & -\frac{1}{3} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ e}$$

$$A^{-1} \cdot A = \begin{pmatrix} \frac{1}{2} & 0 \\ \frac{2}{3} & -\frac{1}{3} \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 4 & -3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Existe uma regra prática para o cálculo da inversa de uma matriz quadrada de ordem 2:

$$\text{Seja } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ então } A^{-1} = \frac{1}{\det A} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Aplicando a regra no exemplo anterior, temos:

$$A = \begin{pmatrix} 2 & 0 \\ 4 & -3 \end{pmatrix}, \text{ então } A^{-1} = \frac{1}{-6} \begin{pmatrix} -3 & 0 \\ -4 & 2 \end{pmatrix} \text{ e por tanto } A^{-1} = \begin{pmatrix} \frac{1}{2} & 0 \\ \frac{2}{3} & -\frac{1}{3} \end{pmatrix}.$$

### 17.2.9.1 Propriedades das matrizes inversíveis

Se  $A$  é inversível, então é única a matriz  $B$  tal que  $AB = BA = I_n$ .

## 17.2.10 Aplicação do conceito na criptografia

### 17.2.10.1 Matrizes inversas como chaves

O método criptográfico que o professor deve apresentar utilizará matrizes invertíveis como chaves. Ele deve explicar aos alunos que com esse método as mensagens ficariam mais difíceis de serem decifradas por interceptadores, o que torna o exercício novamente interessante para o estudante.

O professor pode exibir o exemplo de Alice e Bob que combinam previamente a utilização da matriz  $A = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}$  e sua inversa  $A^{-1} = \begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix}$  como chaves, ressaltando que a determinante das matrizes escolhidas tem que ser -1 ou 1, simplesmente para facilitar o cálculo da matriz inversa.

Explica que para Alice transmitir a mensagem “Estudar é divertido”, ela deve montar uma matriz mensagem  $M$  dispondo a sequência numérica associada em colunas, completando as posições restantes com zero, ou seja:

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Tabela 13 - Tabela alfa-numérica para exercícios com matrizes.

Fonte: Própria.

mensagem e s t u d a r e d i v e r t i d o  
sequência numérica 5 19 20 21 4 1 18 0 5 0 4 9 22 5 18 20 9 4 15 0

$$M = \begin{pmatrix} 5 & 20 & 4 & 18 & 5 & 4 & 22 & 18 & 9 & 15 \\ 19 & 21 & 1 & 0 & 0 & 9 & 5 & 20 & 4 & 0 \end{pmatrix}$$

Em seguida, calcula-se:

$$\begin{aligned} AM &= \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 5 & 20 & 4 & 18 & 5 & 4 & 22 & 18 & 9 & 15 \\ 19 & 21 & 1 & 0 & 0 & 9 & 5 & 20 & 4 & 0 \end{pmatrix} = \\ &= \begin{pmatrix} 53 & 102 & 14 & 54 & 15 & 30 & 76 & 94 & 35 & 45 \\ 24 & 41 & 5 & 18 & 5 & 13 & 27 & 38 & 13 & 15 \end{pmatrix} = C \end{aligned}$$

E com isso obtém a seguinte sequência que é mensagem cifrada:

mensagem e s t u d a r e d i v e r t i d o  
sequência numérica 5 19 20 21 4 1 18 0 5 0 4 9 22 5 18 20 9 4 15 0  
mensagem cifrada 53 24 102 41 14 5 54 18 15 5 30 13 76 27 94 38 35 13 45 15

Para reverter o processo (decifrar) e obter a mensagem original, Bob deve restaurar a forma matricial  $AM = C$ , e com sua chave  $A^{-1}$ , recuperar  $M$  através de:  $AM = C \Rightarrow A^{-1}(AM) = A^{-1}C \Rightarrow (A^{-1}A)M = A^{-1}C \Rightarrow I_2M = A^{-1}C \Rightarrow M = A^{-1}C$ .

$$C = \begin{pmatrix} 53 & 102 & 14 & 54 & 15 & 30 & 76 & 94 & 35 & 45 \\ 24 & 41 & 5 & 18 & 5 & 13 & 27 & 38 & 13 & 15 \end{pmatrix}$$

Em seguida, calcula-se:

$$\begin{aligned} A^{-1}C &= \begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix} \begin{pmatrix} 53 & 102 & 14 & 54 & 15 & 30 & 76 & 94 & 35 & 45 \\ 24 & 41 & 5 & 18 & 5 & 13 & 27 & 38 & 13 & 15 \end{pmatrix} = \\ &= \begin{pmatrix} 5 & 20 & 4 & 18 & 5 & 4 & 22 & 18 & 9 & 15 \\ 19 & 21 & 1 & 0 & 0 & 9 & 5 & 20 & 4 & 0 \end{pmatrix} = M \end{aligned}$$

Logo  $M = \begin{pmatrix} e & t & d & r & e & d & v & r & i & o \\ s & u & a & \# & \# & i & e & t & d & \# \end{pmatrix}$  e portanto a mensagem original é “Estudar é divertido”.

17.2.10.2 Código de César e Matrizes inversas como chaves

O outro método criptográfico que o professor deve apresentar pode misturar duas cifras, matrizes e o código de César, para que o aluno utilize mais conceitos matemáticos. Ele deve explicar aos alunos que com esse método as mensagens ficariam ainda mais difíceis de serem decifradas por interceptadores, o que torna o exercício novamente interessante para o estudante.

O professor pode exibir novamente o exemplo de Alice e Bob que combinam previamente a utilização da matriz  $A = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}$  e sua inversa  $A^{-1} = \begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix}$  como chaves.

Explica que para Alice transmitir a mensagem “Estudar é divertido”, ela deve utilizar a cifra de deslocamento de César (três casas) para realizar a primeira fase da cifragem. Para a segunda fase, montar uma matriz mensagem  $M$ . Em seguida, na terceira fase, calcula-se:  $AM$  e com isso obtém a sequência que é mensagem cifrada.Exemplo:

1ª Fase) Deslocamento de César:

Alfabeto original	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	
Alfabeto cifrado	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	
Texto original	e	s	t	u	d	a	r	e	d	i	v	e	r	t	i	d	o										
Texto cifrado	B	P	Q	R	A	X	O	B	A	F	S	B	O	Q	F	A	L										

2ª Fase) Montar uma matriz mensagem  $M$  dispondo a sequência numérica associada em colunas, completando as posições restantes com zero, ou seja:

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Tabela 14 - Tabela alfa-numérica.  
Fonte: Própria.

mensagem	e	s	t	u	d	a	r	e	d	i	v	e	r	t	i	d	o										
sequência numérica	2	16	17	18	1	24	15	0	2	0	1	6	19	2	15	17	6	1	12	0							

3ª Fase) Calcula-se:

$$AM = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 17 & 1 & 15 & 2 & 1 & 19 & 15 & 6 & 12 \\ 16 & 18 & 24 & 0 & 0 & 6 & 2 & 17 & 1 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 38 & 87 & 51 & 45 & 6 & 15 & 61 & 79 & 20 & 36 \\ 18 & 35 & 25 & 15 & 2 & 7 & 21 & 32 & 7 & 12 \end{pmatrix} = C$$

E com isso obtém a seguinte sequência que é mensagem cifrada:

mensagem	e	s	t	u	d	a	r	e	d	i	v	e	r	t	i	d	o			
sequência numérica	2	16	17	18	1	24	15	0	2	0	1	6	19	2	15	17	6	1	12	0
mensagem cifrada	38	18	87	35	51	25	45	15	6	2	15	7	61	21	79	32	20	7	36	12

Para reverter o processo (decifrar) e obter a mensagem original, Bob deve restaurar a forma matricial  $AM = C$ , e com sua chave  $A^{-1}$ , recuperar  $M$  através de:  $A^{-1}(AM) = A^{-1}C \Rightarrow (A^{-1}A)M = A^{-1}C \Rightarrow I_2M = A^{-1}C \Rightarrow M = A^{-1}C$ , e depois, realizar o processo reverso do deslocamento de César. O professor deve deixar claro que na decodificação, a última fase da codificação deve ser a primeira a ser desfeita, ou seja, a ordem do processo é inversa.

## 17.3 FUNÇÃO EXPONENCIAL

### 17.3.1 Pré-requisito

Para ensinar função exponencial, o aluno deve ter conhecimento de potência de expoente natural, potência de expoente inteiro negativo, raiz enésima aritmética e potência de expoente racional.

### 17.3.2 Definição

Chama-se função exponencial qualquer função  $f: \mathbb{R} \rightarrow \mathbb{R}$  dada por uma lei da forma  $f(x) = a^x$ , onde  $a$  é um número real dado,  $a > 0$  e  $a \neq 1$ .

Exemplos:

$$1^\circ) f(x) = 2^x$$

$$2^\circ) f(x) = \left(\frac{1}{2}\right)^x$$

$$3^\circ) f(x) = (\sqrt{2})^x$$

$$4^\circ) f(x) = (0,34)^x$$

### 17.3.3 Propriedades

- Na função exponencial  $y = a^x$ , temos:

$x = 0 \Rightarrow y = a^0 = 1$ , ou seja, o par ordenado  $(0, 1)$  satisfaz a lei  $y = a^x$  para todo  $a (a > 0 \text{ e } a \neq 1)$ . Isso quer dizer que o gráfico de qualquer função exponencial corta o eixo dos  $y$  no ponto de ordenada 1.

- Se  $a > 1$ , então a função  $f(x) = a^x$  é crescente. Portanto, dados os reais  $x_1$  e  $x_2$ , temos:

$\begin{array}{c} \overbrace{\hspace{2cm}}^{\text{sinais iguais}} \\ \downarrow \hspace{0.5cm} \downarrow \\ \text{se } x_1 < x_2, \text{ então } a^{x_1} < a^{x_2} \end{array}$

São crescentes, por exemplo, as funções exponenciais  $f(x) = 2^x$ ,  $f(x) = 3^x$ ,  
 $f(x) = \left(\frac{3}{2}\right)^x$ ,  $f(x) = (1,2)^x$ .

- Se  $0 < a < 1$ , então a função  $f(x) = a^x$  é decrescente. Portanto, dados os reais  $x_1$  e  $x_2$ , temos:

$\begin{array}{c} \overbrace{\hspace{2cm}}^{\text{sinais opostos}} \\ \downarrow \hspace{0.5cm} \downarrow \\ \text{se } x_1 < x_2, \text{ então } a^{x_1} > a^{x_2} \end{array}$

São decrescentes, por exemplo, as funções exponenciais  
 $f(x) = \left(\frac{1}{2}\right)^x$ ,  $f(x) = \left(\frac{1}{3}\right)^x$ ,  $f(x) = \left(\frac{2}{3}\right)^x$ ,  $f(x) = (0,1)^x$ .

- Para todo  $a > 0$  e  $a \neq 1$ , temos:

Se  $a^{x_1} = a^{x_2}$ , então  $x_1 = x_2$

- Para todo  $a > 0$  e todo  $x$  real, temos  $a^x > 0$ ; portanto, o gráfico da função  $y = a^x$  está sempre acima do eixo dos  $x$ .

Se  $a > 1$ , então  $a^x$  aproxima-se de zero quando  $x$  assume valores negativos cada vez menores.

Se  $0 < a < 1$ , então  $a^x$  aproxima-se de zero quando  $x$  assume valores positivos cada vez maiores.

Tudo isso pode ser resumido dizendo-se que o conjunto-imagem da função exponencial  $y = a^x$  é  $Im = \{y \in \mathbb{R} \mid y > 0\} = \mathbb{R}_+^*$  (IEZZI; DOLCE; DEGENSZAJN; PÉRIGO, 1997, p. 97).

### 17.3.4 Gráfico

Representando graficamente a função exponencial  $f(x) = a^x$ , temos:

Para  $a > 1$ , a função é *creciente*.

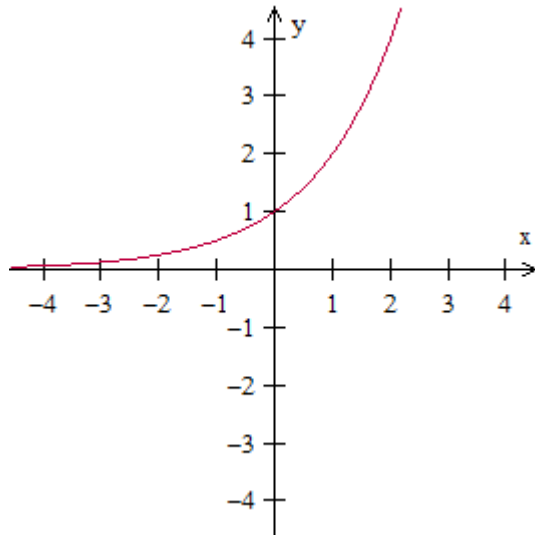


Figura 23 - Gráfico da função exponencial crescente.

Fonte: Própria.

Para  $0 < a < 1$ , a função é *decrecente*.

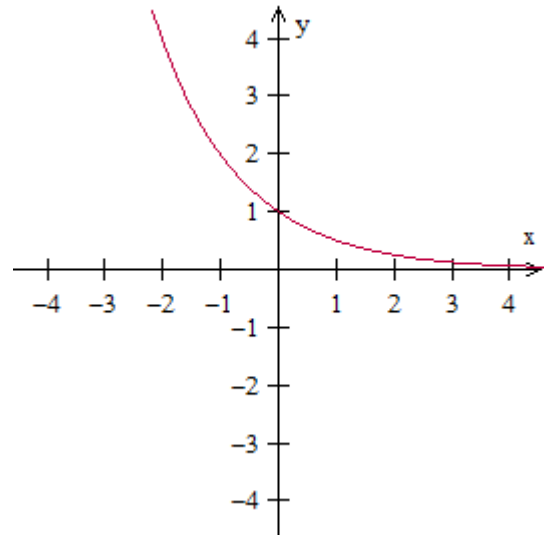


Figura 24 - Gráfico da função exponencial decrescente.

Fonte: Própria.

Exemplos:

1º)  $y = \left(\frac{1}{3}\right)^x$

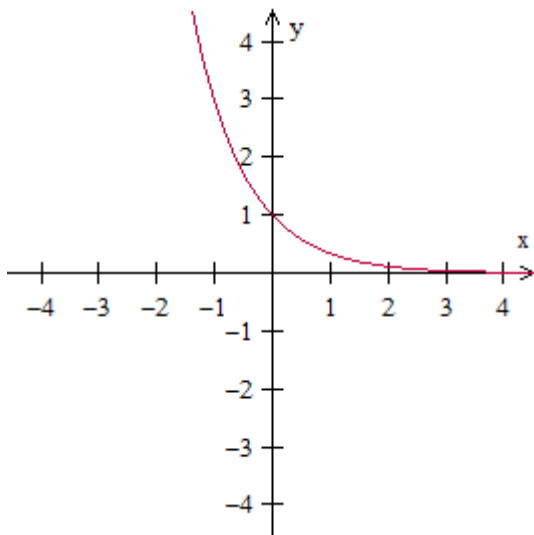


Figura 25 - Gráfico da função exponencial do 1º exemplo.

Fonte: Própria.

2º)  $y = 3^x$

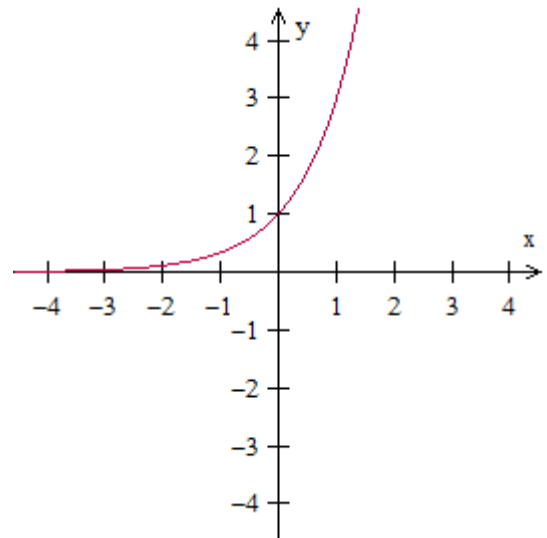


Figura 26 - Gráfico da função exponencial do 2º exemplo.

Fonte: Própria.

Em qualquer caso:

- $D(f) = \mathbb{R}$ .
- $Im(f) = \mathbb{R}_+^*$ .

- A função é injetora, pois para  $x_1$  e  $x_2$  pertencentes ao domínio, se  $x_1 \neq x_2 \Rightarrow a^{x_1} \neq a^{x_2}$ .

### 17.3.5 Equações exponenciais

Uma equação exponencial é aquela que apresenta a incógnita no expoente de pelo menos uma potência.

Por exemplo, são exponenciais as equações  $2^x = 16$ ,  $\left(\frac{1}{8}\right)^x = 81$  e  $4^x - 2^x = 12$ .

Um método usado para resolver equações exponenciais consiste em reduzir ambos os membros da equação a potências de mesma base  $a(0 < a \neq 1)$ , e daí aplicar a propriedade:

$$a^{x_1} = a^{x_2} \Rightarrow x_1 = x_2$$

Quando isso é possível, a equação exponencial é facilmente resolvida.

Exemplos:

$$1^{\circ}) (\sqrt{2})^x = 64 \Rightarrow \left(2^{\frac{1}{2}}\right)^x = 2^6 \Rightarrow \frac{x}{2} = 6 \Rightarrow x = 12 \Rightarrow S = \{12\}$$

$$2^{\circ}) (3^x)^{x+1} = 729 \Rightarrow 3^{x^2+x} = 3^6 \Rightarrow x^2 + x = 6 \Rightarrow x^2 + x - 6 = 0 \Rightarrow x = -3 \text{ ou } x = 2 \Rightarrow S = \{2, -3\}$$

### 17.3.6 Inequações exponenciais

Uma inequação exponencial é aquela que apresenta a incógnita no expoente de pelo menos uma potência.

Por exemplo, são exponenciais as inequações  $2^x > 64$ ,  $\left(\frac{1}{3}\right)^x \leq 27$  e  $4^x - 2^x \leq 12$ .

Um método usado para resolver inequações exponenciais consiste em reduzir ambos os membros da inequação a potências de mesma base  $a(0 < a \neq 1)$ , e daí aplicar a propriedade:

$$a^{x_1} < a^{x_2} \Rightarrow x_1 < x_2 \text{ (se } a > 1)$$

ou

$$a^{x_1} < a^{x_2} \Rightarrow x_1 > x_2 \text{ (se } 0 < a < 1)$$

Exemplos:

$$1^{\circ}) 2^x > 64 \Rightarrow 2^x > 2^6 \Rightarrow x > 6 \Rightarrow S = \{x \in \mathbb{R} | x > 6\}$$

$$2^{\circ}) (2^x)^{x+1} \leq 64 \Rightarrow 2^{x(x+1)} \leq 2^6 \Rightarrow x(x+1) \leq 6 \Rightarrow x^2 + x - 6 \leq 0 \Rightarrow \\ \Rightarrow -3 \leq x \leq 2 \Rightarrow S = \{x \in \mathbb{R} | -3 \leq x \leq 2\}$$

### 17.3.7 Aplicação do conceito na criptografia

O professor pode demonstrar uma mensagem com uma cifra mais elaborada aos estudantes, realizando cálculos de estudos das potências com expoentes positivos e negativos.

Ele distribuiu aos alunos uma tabela contendo um alfabeto relacionado a números que será utilizado nos exercícios.

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
-13	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10	11	12	13

Tabela 15 - Tabela alfa-numérica para exercícios com funções exponenciais.  
Fonte: Própria.

Explica que para cifrar uma mensagem recai no problema de permutar números por meio de uma regra  $f$ . Faz isso de forma prática através das funções  $f(x) = a^x$  onde  $a$  é um número real dado,  $a > 0$  e  $a \neq 1$  definidas no conjunto  $\{-13, -12, -11, \dots, 13\}$ .

Exibe um exemplo de Alice querendo trocar uma mensagem sigilosa com Bob utilizando o alfabeto escolhido.

Explica o que é uma função exponencial conforme citado anteriormente (17.3.2).

Definem juntos uma função cifradora, por exemplo:

$$f(x) = 2^x$$

Escolhem uma mensagem: Estudar é divertido

Associam a sequência numérica:

mensagem e s t u d a r e d i v e r t i d o  
 sequência numérica -9 6 7 8 -10 -13 5 0 -9 0 -10 -5 9 -9 5 7 -5 -10 2

Obtém a mensagem que será transmitida através das imagens de  $f$ :

$\frac{1}{512}$  64 128 256  $\frac{1}{1024}$   $\frac{1}{8192}$  32 1  $\frac{1}{512}$  1  $\frac{1}{1024}$   $\frac{1}{32}$  512  $\frac{1}{512}$  32 128  $\frac{1}{32}$   $\frac{1}{1024}$  4

Decifram a mensagem fatorando cada imagem encontrada e utilizando a tabela alfabeto-númerica, obtém a mensagem original. Exemplos:

1º)  $f(x) = \frac{1}{512}$

Fatorando o denominador

512		2
256		2
128		2
64		2
32		2
16		2
8		2
4		2
2		2
0		<u>2<sup>9</sup></u>

obtemos 2<sup>9</sup>.

Logo reescrevemos essa função sendo  $f(x) = \frac{1}{2^9}$ , sabendo as propriedades de potenciação, temos  $f(x) = 2^{-9}$ .

Como função dada inicialmente era  $f(x) = 2^x$ , isso implica  $2^x = 2^{-9}$  e portanto  $x = -9$ .

2º)  $f(x) = 64$

Fatorando o número

64		2
32		2
16		2
8		2
4		2
2		2
0		<u>2<sup>6</sup></u>

obtemos 2<sup>6</sup>.

Logo reescrevemos essa função sendo  $f(x) = 2^6$ .

Como função dada inicialmente era  $f(x) = 2^x$ , isso implica  $2^x = 2^6$  e portanto  $x = 6$ .

Após os alunos dominarem o processo, o professor divide a sala em grupos, onde cada grupo definiria uma função cifradora e uma mensagem. Os grupos devem trocar as funções e mensagens para que sejam decifradas.

## 18 CONSIDERAÇÕES FINAIS

A criptografia é tão antiga quanto à própria escrita, pois já era encontrada no sistema de escrita hieroglífica dos egípcios. Os romanos utilizavam códigos secretos para comunicar planos de batalha. Durante a guerra, os ingleses ficaram conhecidos por seus esforços na decifração de códigos.

O mais interessante é que a tecnologia de criptografia não mudou muito até meados deste século. Depois da Segunda Guerra Mundial, com a invenção do computador, a área realmente floresceu, incorporando complexos algoritmos matemáticos.

Nos séculos anteriores, a criptografia teve um papel importante na história da humanidade. No presente tornou-se uma ferramenta fundamental, com o surgimento da internet e sua consequente facilidade de processar e transmitir dados de maneira precisa e extremamente rápida.

O trabalho é de caráter qualitativo, pois a pesquisa desse trabalho abrange não somente a parte conceitual e teórica, baseada em pesquisas bibliográficas e em experiências durante estágios realizados numa escola pública da cidade de São Paulo, mas, também, a parte prática, através da realização de aulas de reforços para alunos do Mackenzie, que vieram de diversas escolas e, conseqüentemente, com diferentes graus de conhecimento matemático, de conteúdos do Ensino Fundamental e Médio.

Por ser um assunto muito interessante e que está presente no cotidiano desses alunos, a criptografia é uma maneira motivadora para incentivar o estudo da matemática em sala de aula, fazendo com que eles pesquisem, estudem e utilizem esses conhecimentos em suas vidas.

## REFERÊNCIAS BIBLIOGRÁFICAS

BURNETT, Steve; PAINE, Stephen. Criptografia e Segurança – O guia oficial RSA. 2. ed. São Paulo: Editora Campus, 2002.

CURY, Augusto. Pais brilhantes, Professores fascinantes. 7.ed. Rio de Janeiro: Sextante, 2003.

GENTIL, Nelson; SANTOS, Carlos Alberto Marcondes dos; GRECO, Antônio Carlos; FILHO, Antônio Belloto; GRECO, Sergio Emílio. Matemática para o 2º grau. 11. ed. São Paulo: Editora Ática, 1998.

IEZZI, Gelson; DOLCE, Osvaldo; DEGENSZAJN, David Mauro; PÉRIGO, Roberto. Matemática. São Paulo: Atual Editora Ltda, 1998.

IEZZI, Gelson; DOLCE, Osvaldo; MURAKAMI, Carlos. Fundamentos de Matemática Elementar 2 – Logaritmos. 8. ed. São Paulo: Atual Editora Ltda, 1998.

IEZZI, Gelson; HAZZAN, Samuel. Fundamentos de Matemática Elementar 4 – Sequências, Matrizes, Determinantes e Sistemas. 6. ed. São Paulo: Atual Editora Ltda, 1999.

MORENO, Edward David; PEREIRA, Fabio Dacêncio; CHIARAMONTE, Rodolfo Barros. Criptografia em Software e Hardware. São Paulo: Novatec Editora Ltda, 2005.

MURAKAMI, Carlos; IEZZI, Gelson. Fundamentos de Matemática Elementar 1 – Conjunto e Funções. 8. ed. São Paulo: Atual Editora Ltda, 2005.

SINGH, Simon. O livro dos códigos. 7. ed. Rio de Janeiro: Record, 2008.

TAMAROZZI, Antonio Carlos. Revista do Professor de Matemática. São Paulo, n. 45, 2001.

TKOTZ, Viktoria. Criptografia - Segredos Embalados para Viagem. 1. ed. São Paulo: Novatec Editora Ltda, 2005.

Association for Computing Machinery. Disponível em: <<http://www.acm.org/>>. Acesso em: 10 mar. 2010.

Bob Lord's Home Page. Disponível em: <<http://www.ilord.com/enigma.html>>. Acesso em: 10 mar. 2010.

Wireless Networks Documentation. Disponível em: <<http://www.wireless-net.org/>>. Acesso em: 11 mar. 2010.