UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL

INSTITUTO DE MATEMÁTICA

PROGRAMA DE PÓS GRADUAÇÃO

MATEMÁTICA EM REDE NACIONAL

MESTRADO PROFISSIONAL

EDGARD JOSÉ DOS SANTOS ARINOS

# CRIPTOGRAFIA: APLICAÇÕES NO ENSINO FUNDAMENTAL E MÉDIO.

CAMPO GRANDE

DEZEMBRO DE 2014

**UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL**

**INSTITUTO DE MATEMÁTICA**

**PROGRAMA DE PÓS GRADUAÇÃO**

**MATEMÁTICA EM REDE NACIONAL**

**MESTRADO PROFISSIONAL**

**EDGARD JOSÉ DOS SANTOS ARINOS**

# CRIPTOGRAFIA: APLICAÇÕES NO ENSINO FUNDAMENTAL E MÉDIO.

**Orientadora: Prof.ª Dr.ª Janete de Paula Ferrareze Silva**

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Instituto de Matemática - INMA/UFMS, como parte dos requisitos para obtenção do título de Mestre.

**CAMPO GRANDE**

**DEZEMBRO DE 2014**

# CRIPTOGRAFIA: APLICAÇÕES NO ENSINO FUNDAMENTAL E MÉDIO.

**EDGARD JOSÉ DOS SANTOS ARINOS**

Dissertação submetida ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Instituto de Matemática, da Universidade Federal de Mato Grosso do Sul, como parte dos requisitos para obtenção do título de Mestre.

Aprovado pela Banca Examinadora:

Prof. Dr.ª Janete de Paula Ferrareze Silva - UFMS

Prof. Dr. Jair da Silva - UFMS

Prof. Dr.ª Maristela Missio - UEMS

**CAMPO GRANDE**

**DEZEMBRO DE 2014**

**Epígrafe**

"O estudo, a busca da verdade e da beleza são domínios em que nos é consentido sermos crianças por toda a vida."

Albert Einstein

## AGRADECIMENTOS

Ao fim desta caminhada aproveito para agradecer àqueles que, direta ou indiretamente, influenciaram nesta conquista, por isso agradeço:

A Deus, por me abençoar com saúde e forças necessárias para enfrentar os obstáculos, concedendo mais uma oportunidade de crescimento em minha vida.

A minha esposa Camila Aparecida de Mello Arinos, pelo apoio e compreensão.

Meus filhos o maior presente que Deus me deu, Natan Benitez Arinos e Emanuel Lucas de Mello Arinos.

Aos meus pais, Juracy de Campos Arinos e Catharina Quevedo dos Santos, pela dedicação em proporcionar-me os princípios e valores fundamentais para minha formação.

A minha orientadora Profª. Drª. Janete de Paula Ferrareze Silva, pelos valiosos conselhos e sugestões que contribuíram na realização deste trabalho.

A todos os professores do PROFMAT, pelo profissionalismo, incentivo e qualidade das aulas.

Aos colegas do PROFMAT, pelos momentos de convivência e conhecimentos compartilhados. Em particular a Antônio Cézare de Araújo Giansante, Eder Regiolli Dias, Eliel Gonçalves Villa Nova, Max Deyvis Lesseski da Silva, Silvio Rogério Alves Esquinca, Viviam Ciarini de Souza Amorim, Wagner da Silva Maciel e Wilkler Garcia Magalhães pela amizade e companheirismo.

A CAPES, pelo apoio financeiro. Por fim, a todos que contribuíram para que essa conquista fosse possível.

## Resumo

Algumas discussões no ensino de matemática evidenciam a importância do desenvolvimento do processo de ensino e aprendizagem com atividades didáticas envolvendo temas atuais, com assuntos de interesse dos alunos, que estimulem a curiosidade e que desencadeiem um processo cognitivo que permita a construção de novos conhecimentos. Neste trabalho apresentamos a criptografia como fator motivador para o aprendizado de matemática, pois ela surgiu da necessidade de proteger mensagens e informações secretas.

Nosso principal objetivo foi apresentar uma ferramenta que pode tornar as aulas mais dinâmicas e atraentes, almejando assim uma melhor compreensão dos conceitos matemáticos que estão relacionados com a criptografia. Para isso contamos um pouco da história da criptografia ao passar dos anos e apresentamos algumas atividades relacionadas a ela, que terão como foco os alunos do Ensino Fundamental e Médio. Diante de toda a história relatada e das atividades apresentadas percebemos que a criptografia é uma ferramenta que pode contribuir no aprendizado da matemática.



**Palavra Chave:** esteganografia, criptografia, codificação, decodificação.

**Abstract**

Some discussions in the teaching of Mathematics emphasize the importance of the development of teaching and learning processes with the use of didactic activities involving current issues, with issues of students interest which stimulate curiosity and set off a cognitive process that allows the construction of new knowledge. This paper shows the encryption as a motivating factor for learning Mathematics, because it arose from the need to protect messages and secret information.

Our main goal was to present a tool that can make classes more dynamic and attractive, aiming to achieve a better understanding of the mathematical concepts related to encryption. For that, we told a little of the history of cryptography over the years and we presented some activities related to it, the focus will be on the students of elementary and high school. Before all the history reported and the activities presented we realized that encryption is a tool that can contribute to the learning of Mathematics.

Keywords: steganography, encryption, encoding, decoding.

# Lista de Tabelas

# Lista de Figuras

# Sumário

# Capítulo 1

# Introdução.

Nesse trabalho apresentaremos a evolução da criptografia que é derivada da palavra grega kriptos, cujo significado é "oculto" e graphein que significa "escrever", ao passar dos anos e observamos algumas atividades que podem ser discutidas em sala de aula, com o objetivo de apreciar uma informação pouco discutida mas que estão presentes em nossa tecnologia computacional.

Percebemos que este assunto de forma equivocada não é contemplado pelo currículo escolar mas que pode ser apresentado de forma contextualizada. Neste trabalho exemplificamos algumas formas simples de sua apresentação, procurando esclarecer com exemplos a utilização desta técnica aos nossos alunos.

A criptografia esta em nosso cotidiano, mesmo que a maior parte das pessoas não tenham muitas convicções do que se trata. Podemos afirmar que ela sempre esteve em nosso meio, pois uma das principais ferramentas que utiliza a criptografia são os aparelhos eletrônicos que necessitam de sigilo em alguns campos de sua programação, se fazendo necessário a criação de senhas criptografadas para manter a segurança. Hoje percebe-se que o aparelho eletrônico que mais utiliza estes principios é o computador, que é de fácil acesso por quase toda a população, pois muitos tem contato em casa, na escola ou mesmo no trabalho.

No capítulo 2, com a história da criptografia, vemos que enquanto alguns de-

senvolvem métodos para deixar esses tipos de transações eletrônicas mais seguras, outros estudam meios para quebrar esta segurança, e desta forma estamos em constante evolução. Percebemos neste capítulo, que o computador é uma ferramenta que surgiu da evolução da criptografia e sua necessidade de ocultar informações. Com isso, uma das utilidades do computador no início, foi de facilitar o envio de mensagens codificadas, mas fica a pergunta, será que este sigilo é realmente eficaz? Será que sempre existe sigilo quando acessamos a internet, o nosso e-mail, nossa conta bancária, nossas redes sociais? Ou seja, mais ainda, será que ao fazer uma compra pela web, nosso cartão não será clonado?

Além disso, no capítulo 2 relatamos como a necessidade de esconder mensagem se transformou no que é hoje a criptografia, pois há muito tempo, governantes, imperadores, reis e grupos fechados procuravam se comunicar em secredo. Eles ansiavam que estas informações fossem sigilosas e que só a pessoa a quem estivesse destinada a mensagem pudesse conhecer o seu teor. Com isso foram criados códigos e cifras que dificultavam o entendimento do que estava se querendo passar. Esta técnica recebe o nome de criptografia e ao passar do tempo foi necessário que estes códigos ficassem cada vez mais complexos, dificultando-se ainda mais sua decodificação pelas pessoas não autorizadas. A criptografia foi ganhando aplicações por um motivo bem clássico, as guerras, pois os povos aliados precisavam se comunicar de forma sigilosa e se uma de suas mensagens fosse interceptada, seu inimigo não poderia decifrar, para que sua estratégia não fosse conhecida. Ao passar do tempo isso foi evoluindo, criando assim outros problemas ou soluções e ganhando outras necessidades, um exemplo disso, é a privacidade no envio de uma mensagem, sabendo que só o destinatário conhecerá seu teor.

No capítulo 3 apresentamos propostas que poderão ser aplicadas a alunos do ensino fundamental e médio. São questões referentes a aritmética modular, funções, matrizes e análise combinatória. Sabendo que todos estes assuntos estão previstos no currículo básico da matemática, vincularemos cada um deles à criptografia de forma simples podendo assim assegurar que esta pode fazer parte de nosso cotidiano e que existem várias técnicas eficientes para se fazer isso.

# Capítulo 2

# A Evolução Histórica da Criptografia.

Neste capítulo iremos apresentar a evolução histórica desde a arte de esconder mensagens, que recebe o nome de esteganografia, até chegar a escrita em cifras ou em códigos que é conhecida com o nome de criptografia, a qual é utilizada até hoje. A criptografia deriva da palavra grega *kriptos*, que significa "oculto" e *graphein* que significa "escrever". A criptografia é tão antiga quanto a própria escrita; já estava presente no sistema de escrita hieroglífica dos egípcios e os romanos também utilizavam códigos secretos para comunicar planos de batalha. [SINGH 21]. O objetivo da criptografia não é esconder a existência de uma mensagem, e sim de ocultar o seu significado, dificultando o entendimento e apreciação dos dados, diferente da esteganografia que apenas escondia informações que se descobertas não dificultaria o conhecimento da mensagem, o processo utilizado pela criptografia é conhecido como *encriptação*. As referências utilizadas neste capítulo foram [2]; [12]; [14] e [22].

Há muito tempo atrás a.C. já se fazia necessário criar técnicas para esconder informações secretas, a primeira delas, descrita pelo filósofo Heródoto, recebe o nome de esteganografia, e será esclarecida mais adiante. Em seus relatos Heródoto demonstra que isso foi um processo muito utilizado nas guerras, e que existiu várias formas de esconder mensagens, mas a maioria, se não todas, eram extremamente simples para serem descobertas. Por isso, perceberemos que com o passar do tempo se fez necessário criar ferramentas

mais eficientes, que salvaguardassem melhor as informações secretas. Em seguida, surgiu a transposição que seria uma sutil adaptação dos textos em tabelas, que eram preenchidas de maneira que o texto ficasse misturado. Este principio foi utilizado pelo Bastão de Licurgo. Depois surgiram métodos de substituição, como por exemplo o utilizado pelo imperador de Roma, Júlio César, o qual se baseava na movimentação das letras do alfabeto, no início de forma sequêncial.

Com o passar do tempo estes tipos de ferramentas ficaram conhecidas, se fazendo necessária mudanças em sua transposição. Estas mudanças só aconteceram algum tempo depois pelo italiano Leon Battista Alberti quando utilizou o "Disco de Alberti", que recebeu o seu nome por ter sido sua criação. O disco nada mais era que o alfabeto misturado de forma que só o criador do disco pudesse codificar e decodificar, e desta vez o alfabeto não seguia uma sequência, era totalmente desordenado. Esta invenção também foi superada e precisou passar por ajustes. Estes ajustes foram feitos pelo francês Blaise de Vigenère, que antes de codificar o texto criou uma palavra chave e a partir desta palavra chave é que o texto era codificado, dificultando em muito o processo de decodificação pelos especialistas em quebrar códigos secretos, os chamados criptonalistas. Esta criação ficou por muito tempo até que se tornasse de fácil violabilidade. O processo criado por Vigenère só foi superado pela criação de uma máquina com o nome de Enigma, que utilizava o mesmo raciocínio por ele desenvolvido, mas era mais eficiente na codificação e decodificação de mensagens, e o mais importante é que esta máquina criava códigos que nesta época só eram quebrados por pessoas que possuíssem outra máquina igual. Posterior a Enigma foi criada uma outra máquina com nome de Bomba que decodificava mensagens transmitidas pela Enigma. Neste mesmo período foi criada outra, mais eficiente, a Colossos, a qual era mais rápida que a Bomba na decodificação das mensagens enviadas pela máquina Enigma.

Todas estas máquinas, Criadas para codificar e decodificar mensagens, foram o alicerce para a invenção de algo atual, o computador. Após o computador as técnicas de codificação e decodificação ganharam novos rumos, pois agora a ideia é enviar mensagem em

um lugar de comum acesso a todos mais só tendo um interessado a reconhecer os detalhes. Surgiu então a ideia da criptografia simétrica e assimétrica, e suas ramificações que hoje é o que há de mais conhecido na criptografia.

## 2.1 Evolução sem computadores

A evolução da criptografia aconteceu naturalmente, pois se fazia necessário comunicar-se através de mensagens secretas. As mudanças aconteceram gradativamente começando pela arte ou ciência de cobrir mensagens que é chamada de esteganografia. Em paralelo com o desenvolvimento da esteganografia, houve a evolução da criptografia.

### 2.1.1 Esteganografia.

O nome esteganografia é derivado da palavra *steganó* cuja o significado é "coberto" e *graphein* que significa "escrever". Um dos primeiros textos sobre códigos secretos foi escrito pelo geógrafo e historiador grego Heródoto (485 a.C. - 420 a.C.), ver [14]. Ele foi o primeiro a considerar um problema filosófico como um projeto de pesquisa que podia revelar conhecimento do comportamento humano. Por esse motivo ele recebeu o título de "o pai da História".

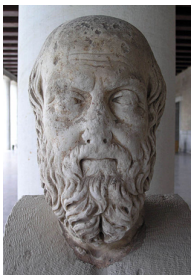


Figura 2.1.1: Heródoto(485 a.C. - 420 a.C.) [7].

Na sua principal obra, conhecida por "as histórias de Heródoto", é retratada a história dos conflitos entre a Pérsia e a Grécia no início do século V a.C. Segundo Heródoto, a

habilidade da escrita secreta foi a causa de a Grécia não ter sido conquistada por Xerxes, cuja intenção, à época, era formar um grande exército para invadir a Grécia. Para a infelicidade de Xerxes, o plano da invasão foi testemunhado por Demarato, um grego que foi expulso da sua terra natal e vivia em uma cidade persa chamada Susa. Mesmo sendo um exilado, ele ainda tinha um sentimento de lealdade com a Grécia e decidiu enviar uma mensagem para advertir os espartanos dos planos de invasão de Xerxes. O principal desafio era como enviar essa mensagem sem que ela fosse interceptada pelos guardas [14]. A estratégia de Demarato foi apenas ocultar a mensagem. Assim os gregos, que não estavam se preparando para uma batalha, começaram a se armar. Heródoto também narra outro incidente no qual a ocultação foi suficiente para garantir a transmissão segura da mensagem. É a história de Histaeu, que queria encorajar Aristágora de Mileto 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.

Entre alguns exemplos similares àqueles relatados por Heródoto, estão a escrita de uma mensagem secreta em uma tira de seda fina, que era amassada formando uma pequena bola, coberta com cera e engolida por um mensageiro; a tinta invisível usada na escrita, que após um suave aquecimento, adere a cor marrom; e a mensagem no ovo cozido, que baseava-se em escrever uma mensagem sobre a casca desse ovo com uma tinta especial que penetrava essa casca e estampava o ovo. Todas estas formas foram muito utilizadas por volta do século V a.C, pois mesmo sendo uma forma primitiva de envio de mensagens ainda assim possuía uma certa segurança e teve ainda uma boa longevidade.

Podemos citar um outro exemplo, utilizado durante a Segunda Guerra Mundial, por agentes alemães, que atuavam na América Latina. Eles utilizaram uma técnica de transmissão de mensagem que consiste em microfilmar uma página de texto, reduzindo-o ao tamanho de um ponto. Este ponto era colocado sobre um ponto final de um documento aparentemente ostensivo, um documento que se podia mostrar. O receptor, ao receber a mensagem,

procurava pelo ponto e ampliava-o para ter acesso a informação. Os aliados descobriram a técnica em 1941 e passaram a interceptar a comunicação.

As duas histórias contadas por Heródoto, bem como os outros exemplos citados nessa seção, não são consideradas comunicações seguras, pois foram obtidas simplesmente escondendo a mensagem. O principal problema deste tipo de técnica é que caso a mensagem seja descoberta, poderá ser lida por qualquer pessoa. Esse era o problema maior da esteganografia.

### 2.1.2 Transposição.

A transposição utizava-se de uma sutil adaptação dos textos em tabelas, que eram preenchidas da esquerda para a direita, linha após linha e depois reescritas em uma tira de couro seguindo a sequência das letras de cima para baixo, coluna após coluna deixando assim o texto misturado de forma que só seria conhecido por quem possuísse a técnica de reconstrução da tabela. A transposição, consiste em trocar a posição das letras da mensagem original, promovendo uma permutação das letras segundo um algoritmo e uma chave bem determinadas. Esta técnica foi uma forma simples e na época eficiente de enviar mensagens secretas para que os inimigos não descobrissem. A transposição exigia que o envio e recebimento já tivesse todos os detalhes bem definidos, ou seja, que a forma de criar a mensagem já estivesse bem acordada por ambos pois assim não teria erro de interpretação. Para esta técnica era necessário criatividade e discrição, e esta caracteristica o bastão de Licurgo tinha, por isso foi uma das ferramentas relatadas.

#### 2.1.2.1 Bastão de Licurgo.

Desde o momento em que a técnica de criptografar mensagens se tornou compreensível, a criptografia passou a utilizar dois métodos fundamentais, a transposição e a substituição. Um exemplo histórico do uso do método de Transposição, está no primeiro aparelho criptográfico militar que se tem conhecimento, o Bastão de Licurgo, que data do

século V a.C. Era um bastão de madeira ao redor do qual enrolava-se uma tira de couro longa e estreita. O remetente escrevia a mensagem ao longo do bastão e depois desenrolava a tira de couro, a qual passava a conter apenas um monte de letras sem sentido algum. O mensageiro poderia utilizar a tira como um cinto, com as letras voltadas para dentro (Esteganografia), e o destinatário ao receber do mensageiro a tira de couro, a enrolaria em um bastão com as mesmas dimensões do bastão do remetente. O formato do bastão seria a chave desta cifra.

Figura 2.1.2: Bastão de Licurgo [21].

Um outro exemplo de transposição foi a Tabela Espartana, um método utilizado na Grécia Antiga em 90d.C., conforme descrito por Plutarco no livro "Vida de homens ilustres". Este método consistia de uma tabela comum, onde a chave do código era o número de colunas da tabela, já que o número de linhas dependeria do tamanho da mensagem. A mensagem era escrita nas células da tabela, da esquerda para a direita e de cima para baixo (ou de outra forma previamente combinada) e o texto cifrado era obtido tomando-se as letras em outro sentido e direção. Por exemplo, o texto "MESTRADO PROFISSIONAL EM MATEMATICA" em uma tabela com 5 colunas, utilizando a letra H no lugar do espaço, seria representado como na figura abaixo:

| | | | | |
|---|---|---|---|---|
| M | E | S | T | R |
| A | D | O | H | P |
| R | O | F | I | S |
| S | I | O | N | A |
| L | H | E | M | H |
| M | A | T | E | M |
| A | T | I | C | A |

Tabela 2.1.1: Tabela Espartana.

Tomando o texto na tabela, de cima para baixo, teremos o seguinte texto ininteligível:

MARSL MAEDO IHATS OFOET ITHIN MECRP SAHMA

*Observação* 1. É usual separarmos o texto ininteligível em blocos de 5 letras, indepente da chave do código. Quando a quantidade de letras do texto não for múltipla de 5, completa-se o último bloco do texto ininteligível com letras aleatórias. Este modelo também poderia ser usado com o Bastão de Licurgo.

### 2.1.3 Substituição.

A substituição tem por base a permutação do alfabeto, ou seja, trocar cada letra ou símbolo por outro. Esta técnica foi renovadora em relação as que existiam, pois no início de sua criação era fácil codificar e decodificar, quando se tinha a chave código, atendendo assim a necessidade de sua criação que era esconder mensagens dos inimigos de guerra. Um dos primeiros relatos que se tem notícia sobre este tipo de mensagem foi na época do Imperador Júlio César, que usou a substituição de posição da letra do alfabeto utilizado, para encobrir as mensagens. Em outros períodos da história se fez necessário aperfeiçoar esta ferramenta e com isso surgiram outras ideias que vieram a dificultar que pessoas não autorizadas desvendassem as mensagens. Na verdade continuava a substituição mas agora bem mais refinada, buscando dificultar ainda mais a decodificação, para garantir mais sigilo. Nas próximas seções, verificaremos a evolução desta ferramenta, observando as várias formas de executar esta mesma manobra e onde foi utilizada.

#### 2.1.3.1 Código de César.

Este tipo de codificação era usado pelo ditador romano Júlio César para comunicar-se com as legiões romanas em combate pela Europa. César ficou conhecido como um dos

maiores gênios militares, responsável por uma das primeiras ou primeira mensagem que utilizava a criptografia, com a motivação de manter secretas suas táticas militares.

Figura 2.1.3: Júlio César (100 - 44 a.C.) [8].

Sua invenção um tanto quanto simples, se avaliada hoje, seria conhecida como substituição monoalfabética, pois a codificação nada mais é que substituir uma letra do alfabeto pela que está três posições a frente. Na prática, a letra "a" é substituída pela letra "d"; a letra "b", pela "e"; a letra "c", pela "f" e assim sucessivamente. A utilização deste código era muito simples, pois a sua codificação era fácil, mas também era fácil "quebrar", ou seja, era fácil a decodificação da mensagem por pessoas que não fossem os legítimos donos.

*Observação* 2. Mesmo sendo apresentada a movimentação de três posições como exemplo de César, ainda assim sabe-se que poderia acontecer movimentações de k posições.

| Letra | Codificação | Letra | Codificação |
|---|---|---|---|
| A | D | G | J |
| B | E | H | L |
| C | F | I | M |
| D | G | J | N |
| E | H | L | O |
| F | I | M | P |

| Letra | Codificação | Letra | Codificação |
|---|---|---|---|
| N | Q | T | X |
| O | R | U | Z |
| P | S | V | A |
| Q | T | X | B |
| R | U | Z | C |
| S | V | | |

Tabela 2.1.2: Tabela utilizada para codificação dos textos.

A seguir, apresentamos um exemplo do que acontecia naquela época:

**Exemplo 1.** Consideremos a seguinte mensagem codificada.

RXYLUDP GR LSLUDQJD DV PDUJHQV SODFLGDV GH XP SRYR KHURLFR R EUDGR UHWXPEDQWH H R VRO GD OLEHUGDGH HP UDLRV IXOJLGRV EULOKRX QR FHX GD SDWULD QHVVH LQVWDQWH VH R SHQKRU GHVVD LJXDOGDGH FRQVHJXLPRV FRQTXLVWDU FRP EUDFR IRUWH HP WHX VHLR, R OLEHUGDGH GHVDILD R QRVVR SHLWR D SURSULD PRUWH R SDWULD DPDGD LGRODWUDGD VDOYH VDOYH EUDVLO XP VRQKR LQWHQVR XP UDLR YLYLGR GH DPRU H GH HVSHUDQFD D WHUUD GHVFH VH HP WHX IRUPRVR FHX ULVRQKR H OLPSLGR D LPDJHP GR FUXCHLUR UHVSODQGHFH JLJDQWH SHOD SURSULD QDWXUHCD HV EHOR, HV IRUWH, LPSDYLGR FRORVVR H R WHX IXWXUR HVSHOKD HVVD JUDQGHCD WHUUD DGRUDGD HQWUH RXWUDV PLO HV WX EUDVLO R SDWULD DPDGD GRV ILOKRV GHVWH VROR HV PDH JHQWLO SDWULD DPDGD EUDVLO.

É claro que você notou que o parágrafo acima foi codificado e que neste código a acentuação e a pontuação não serão importantes. Esta mensagem está decodificada a seguir, perceba que o texto não lhe é desconhecido.

OUVIRAM DO IPIRANGA AS MARGENS PLACIDAS DE UM POVO HEROICO O BRADO RETUMBANTE E O SOL DA LIBERDADE EM RAIOS FULGIDOS BRILHOU NO CEU DA PATRIA NESSE INSTANTE SE O PENHOR DESSA IGUALDADE CONSEGUIMOS CONQUISTAR COM BRACO FORTE EM TEU SEIO, O LIBERDADE DESAFIA O NOSSO PEITO A PROPRIA MORTE O PATRIA AMADA IDOLATRADA SALVE SALVE BRASIL UM SONHO INTENSO UM RAIO VIVIDO DE AMOR E DE ESPERANCA A TERRA DESCE SE EM TEU FORMOSO CEU RISONHO E LIMPIDO A IMAGEM DO CRUZEIRO RESPLANDECE GIGANTE PELA PROPRIA NATUREZA ES BELO, ES FORTE, IMPAVIDO COLOSSO E O TEU FUTURO ESPELHA ESSA GRANDEZA TERRA ADORADA ENTRE OUTRAS MIL ES TU BRASIL O PATRIA AMADA DOS FILHOS DESTE SOLO ES MAE GENTIL PATRIA AMADA BRASIL.

Em [3], BORTOLOSSI indica um programa de sua autoria, que codifica e decodifica textos utilizando técnicas de substituição. Este programa foi utilizado para codificar e decodificar o texto acima. Com isso percebemos que para a época isso deveria funcionar muito bem, até é claro que alguém percebesse como tudo foi feito. Veremos na próxima seção, como o texto do exemplo 1 pode ser decodificado.

#### 2.1.3.2 Criptoanalistas árabes.

No século IX um matemático árabe, que trabalhava na "Casa da sabedoria de Bagdad", escreveu um livro manuscrito sobre o deciframento de mensagens criptográficas. O nome deste árabe é Abu Yusuf Yaqub ibn Ishaq al-Sabbah Al-Kindi, mas nos referimos a ele simplesmente como Al-Kindi, conhecido como "o filósofo dos árabes". Autor de 290 livros sobre Medicina, Astronomia, Matemática, Linguística e Música, seu maior trabalho só foi descoberto em 1987, no Arquivo Otomano Sulaimaniyyah em Istambul, e se intitula: "Um manuscrito sobre a decifração de mensagens criptográficas". Nesse livro é descrito o método da análise das frequências, o qual permite "romper" todas as cifras de substituição monoalfabéticas, ou seja, cifras de substituição a partir das quais cada letra do texto claro é substituída por outra letra no texto cifrado, de forma constante.

Figura 2.1.4: Imagem artística de Al-Kindi [21].

Al-Kindi foi o primeiro a estudar a frequência de letra nos idiomas mais conhecidos. Seu método consiste em decifrar uma mensagem codificada, quando se conhece o idioma, e para isso, deve-se encontrar um texto diferente, na mesma língua, suficientemente longo para preencher uma página e fazer essa análise das frequências. A letra que aparecer com maior frequência no texto é chamada de "primeira", a segunda mais frequente recebe o nome de "segunda" e assim por diante, até todas as letras do texto serem contadas. Em seguida, examina-se o texto cujo deciframento será feito e os símbolos também são classificados com relação à frequência. O símbolo que aparecer com maior frequência é substituído pela "primeira", o segundo símbolo mais frequente é substituído pela "segunda" e assim por diante, até todos os símbolos serem convertidos.

Para poder aplicar a análise das frequências, precisamos conhecer qual é a porcentagem de aparição de cada letra nos textos de uma determinada língua. A frequência média de cada letra na Língua Portuguesa está apresentada na tabela a seguir:

| Letra | % | Letra | % |
|---|---|---|---|
| A | 14,64 | H | 1,28 |
| B | 1,04 | I | 6,18 |
| C | 3,88 | J | 0,40 |
| D | 4,10 | K | 0,00 |
| E | 12,57 | L | 2,78 |
| F | 1,02 | M | 4,75 |
| G | 1,30 | N | 5,05 |

| Letra | % | Letra | % |
|---|---|---|---|
| O | 10,73 | U | 4,64 |
| P | 2,52 | V | 1,70 |
| Q | 1,20 | X | 0,21 |
| R | 6,53 | Y | 0,00 |
| S | 7,81 | W | 0,00 |
| T | 4,34 | Z | 0,47 |

Tabela 2.1.3: Frequência das letras na língua portuguesa.

Assim, contando apenas a frequência de cada símbolo no texto, podemos descobrir a letra que é correspondente. Lembre-se, que isso só pode ser definido se o texto for longo. Pois o contrário a isso pode causar problema de precisão, coforme veremos no exemplo a seguir encontrado em [5].

**Exemplo 2.** Consideremos a frase "Zuza zoou de Zezé". A letra mais frequente é o "z" que aparece 5 vezes em um texto de 14 letras. A porcentagem de z, cerca de 35% no texto acima,

é diferente da frequência nos textos usuais, cerca de 0,47%. Já o “a” apareceu uma só vez, cerca de 7%, sendo que usualmente a frequência é de 14%. Assim concluimos que usando o método de contagem de frequência, não será muito fácil perceber que a decodificação deste parágrafo vai resultar nesta mensagem.

A seguir apresentamos um exemplo de decodificação de um texto utilizando a frequência das letras.

**Exemplo 3.** Consideremos a mensagem codificada a seguir, encontrada em [16].

urtklm tr dqapuakcftr ltr iasqtr aj nmqsuouar lacfdqa t jakrtoaj tetfxm a cmjniasa t steait ntqt qaofrsqtq tr ruersfsufcmar akcmksqtltr.

Buscando facilitar a decodificação e sabendo que os espaço representam as separações da palavras, iremos ajeitar as palavras conforme for acontecendo a decodificação.

u r t k l m t r d q a p u a k c f t r l t r

i a s q t r a j n m q s u o u a r l a c f d q a t

j a k r t o a j t e t f x m a c m j n i a s a t

s t e a i t n t q t q a o f r s q t q t r

r u e r s f s u f c m a r a k c m k s q t l t r

Utilizando [2], encontramos a frequência das letras do texto codificado, a qual apresentamos na tabela a seguir.

| Letra | % | Letra | % |
|---|---|---|---|
| a | 13,79 | h | 0,00 |
| b | 0,00 | i | 2,59 |
| c | 4,31 | j | 3,45 |
| d | 1,72 | k | 4,31 |
| e | 2,58 | l | 3,55 |
| f | 5,17 | m | 5,17 |
| g | 0,00 | n | 2,59 |

| Letra | % | Letra | % |
|---|---|---|---|
| o | 2,59 | u | 5,17 |
| p | 0,86 | v | 0,00 |
| q | 7,76 | w | 0,00 |
| r | 11,21 | x | 0,86 |
| s | 6,90 | y | 0,00 |
| t | 15,52 | z | 0,00 |

Tabela 2.1.4: Frequência das letras do texto codificada.

Através de um comparativo podemos buscar a decodificação da mensagem observando a frequência média. Faremos isso utilizando a tabela a seguir que nos fornece a identificação das letras do alfabeto com os códigos utilizados no texto. Esta tabela foi construida a partir da análise de frequência apresentada na tabela [2.1.3.2].

*Observação* 3. Na Tabela [2.1.5], as letras que estão em itálico e negrito não aparecerem em nenhum momento no texto.

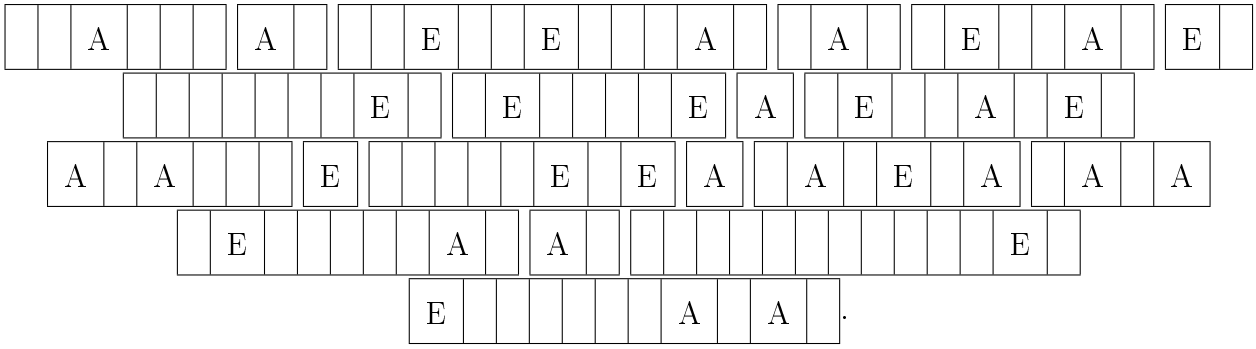
| Frequência da letra no código | Frequência da letra na língua portuguesa |
|---|---|
| t | A |
| a | E |
| r | O |
| q | S |
| s | R |
| f | I |
| m | D |
| u | T |
| c | L |
| k | M |
| j | U |
| l | N |
| e | P |
| i | C |
| n | B |
| o | F |
| d | G |
| p | V |
| x | H |
| ***b*** | Q |
| ***g*** | Z |
| ***h*** | J |
| ***v*** | ***K*** |
| ***w*** | ***W*** |
| ***y*** | ***X*** |
| ***z*** | ***Y*** |

Tabela 2.1.5: Comparação entre as frequência em ordem decrescente de porcentagem.

*Observação* 4. Vale a pena ressaltar que isso é apenas um estudo, ou seja, estamos fazendo

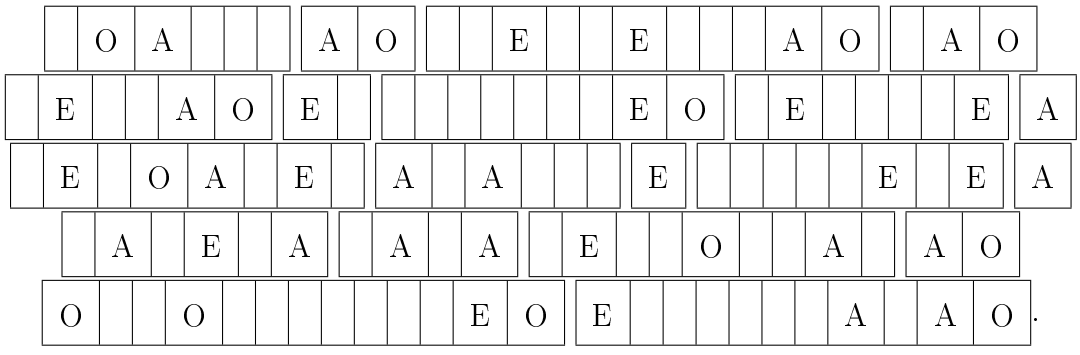
uma especulação, assim, as identificações apresentadas na tabela poderão ser mudadas coforme a necessidade no processo de decodficação da mensagem.

Analisando a frequência de cada letra no texto, note que a letra que aparece com maior frequência é a letra “t” e há uma grande possibilidade de ela ser a letra “A” no texto original. A letra que aparece com a segunda maior frequência é a letra “a” e, como fizemos anteriormente, há uma grande possibilidade de ela ser a letra “E”. Substituindo essas informações no texto, temos:

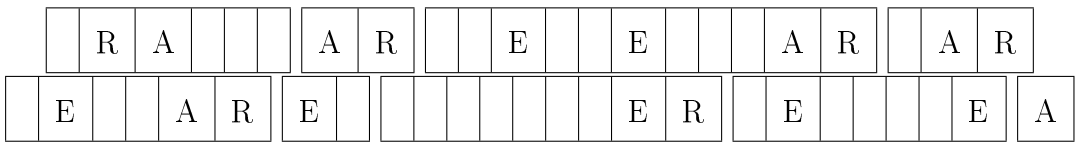


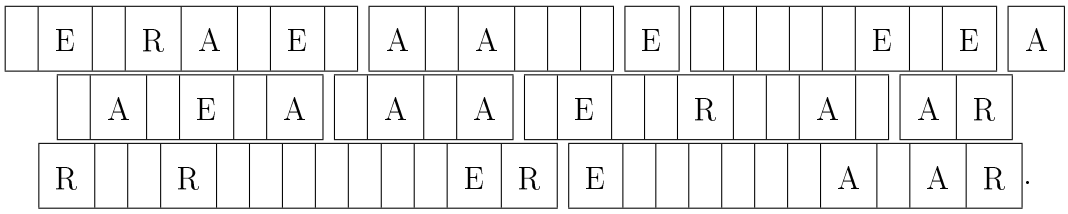

Depois da substituição das possíveis relações, o texto ficou organizado como está acima. A letra “r” é a terceira letra com maior frequência, então ela pode estar codificando as letras “O”, “R” ou “S”. Vamos substituir essa letra por cada uma das letras que estamos especulando para ver se algum dos textos faz sentido.

Substituindo a letra “r” por “O”:

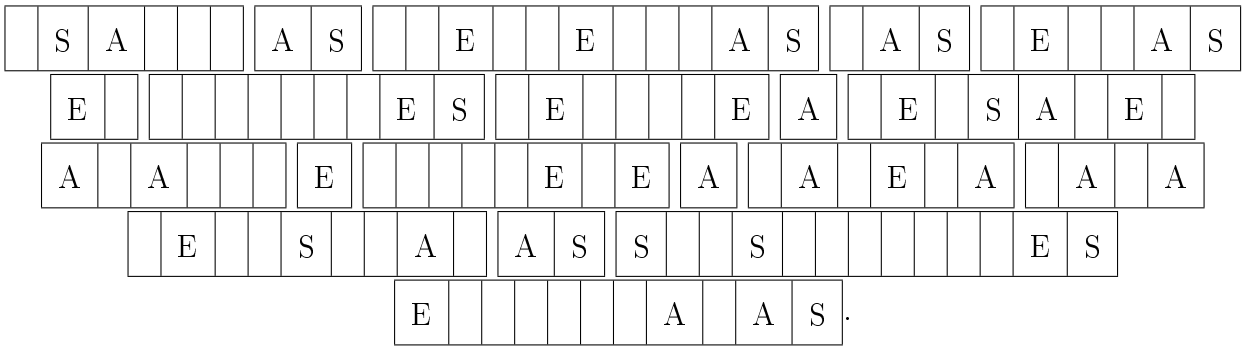



Substituindo “r” por “R”, temos:

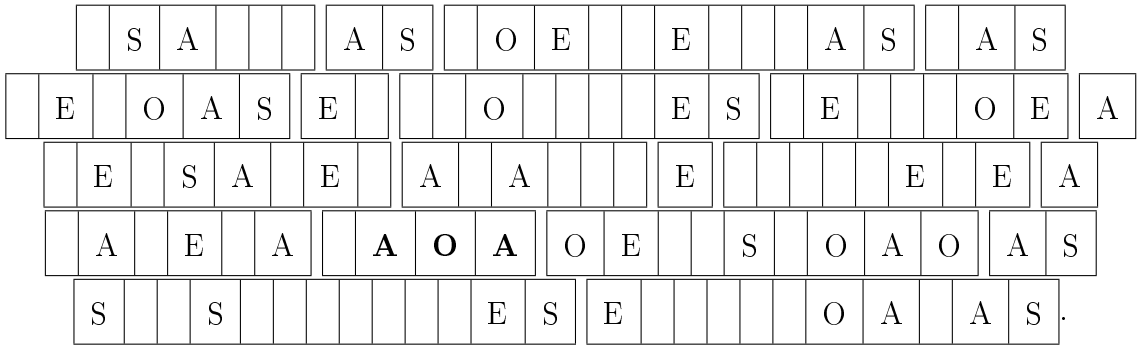




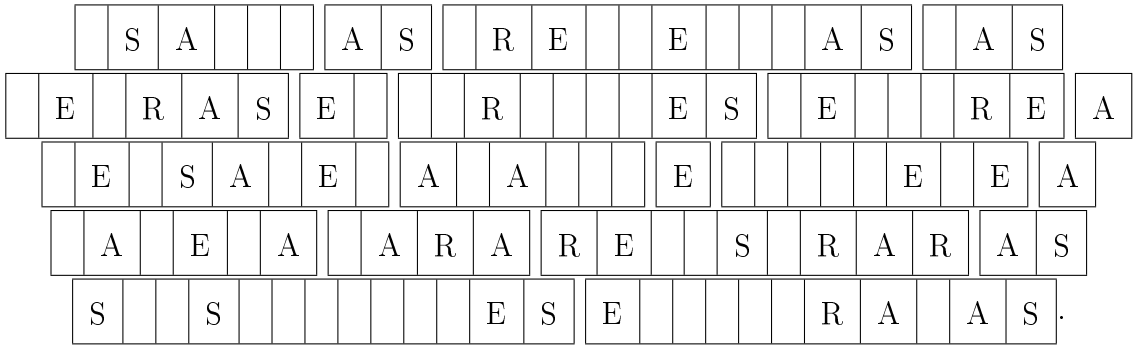

Finalmente, substituindo “r” por “S”, a mensagem fica:



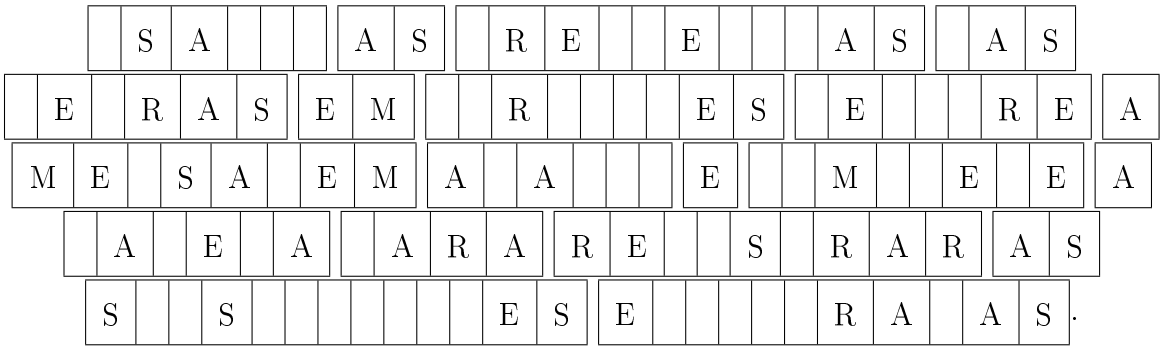

Diante das três possibilidades, a que mais faz sentido é a terceira, ou seja, quando trocamos “r” por “S”. A quarta letra é a “q”, então, provavelmente ela será “O” ou “R”. Se a letra “q” foi substituída por “O”, obtemos:



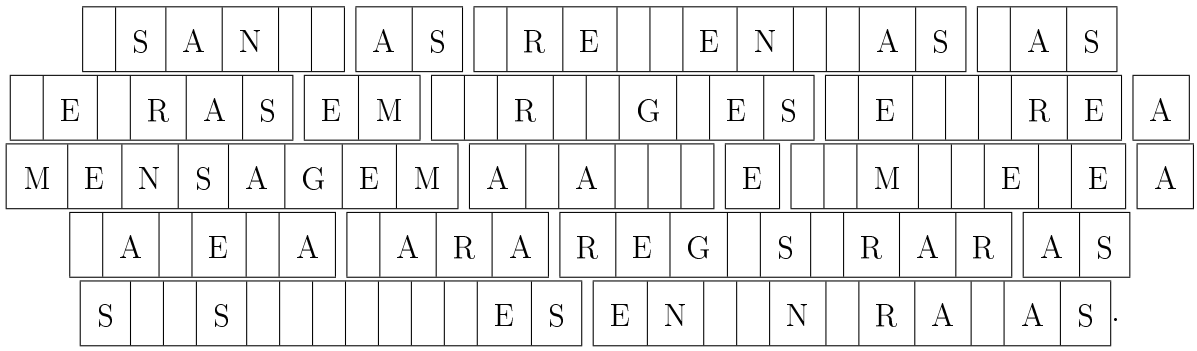

Se a letra “q” foi substituída por “R”, obtemos



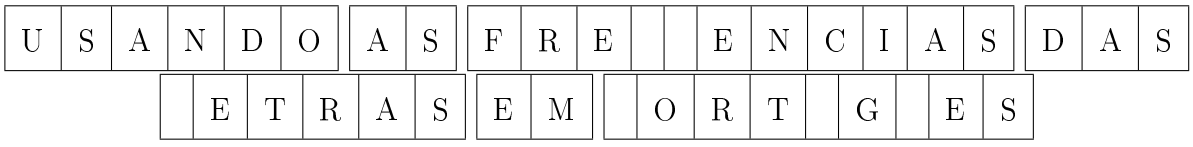
Na primeira opção temos algo que se torna absurdo na Língua Portuguesa. Isso se dá pelo fato da palavra _AOA aparecer no texto. Logo, iremos optar pela segunda possibilidade. Note que a palavra "Ej" pode ser "EM", ou seja, a letra "j" pode ter sido substituída pela letra "M" no momento da codificação. Assim:

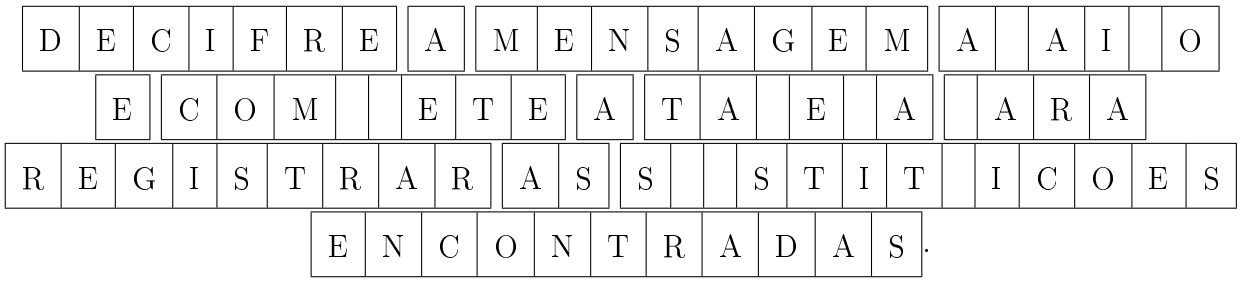



Realmente isso faz muito sentido, pois apareceu a palavra ME_SA_EM, haja vista, claramente, que ela representa a palavra MENSAGEM, ou seja, no texto cifrado, a letra "k" foi trocada por "N" e a letra "o" foi substituída por "G". Analisando mais uma vez o texto:

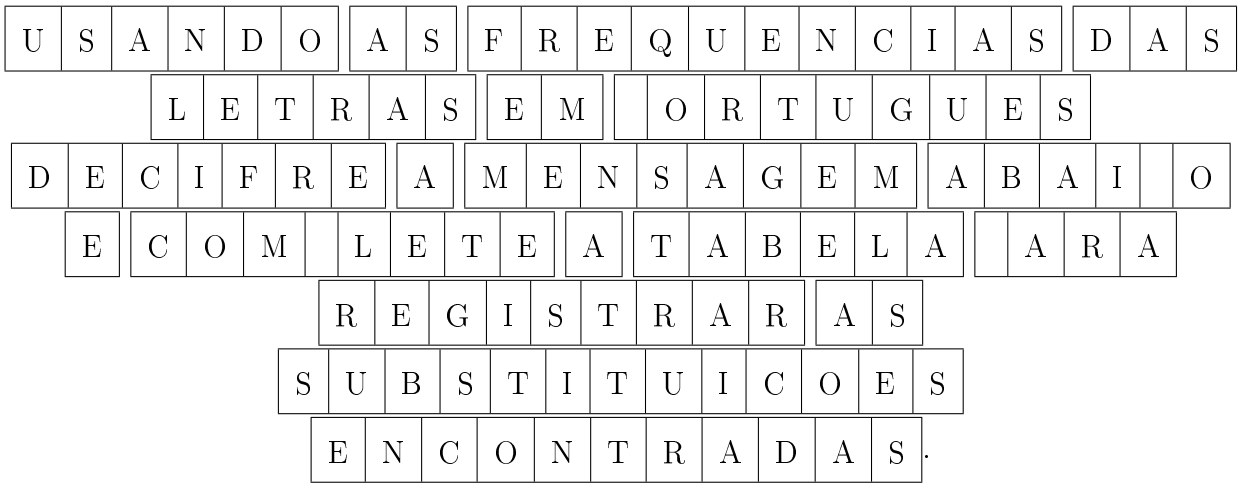



Podemos observar que a palavra USAN_ _ deve ser USANDO e REG_S_RAR deve ser REGISTRAR. Desta forma, percebemos que "l" é "D", "m" é "O", "f" é "I" e "s" é "T". Assim a palavra _ E_ _ _RE deve ser DECIFRE. Desta forma, percebemos que "d" é "F". Substituindo essas letras no texto obtemos:

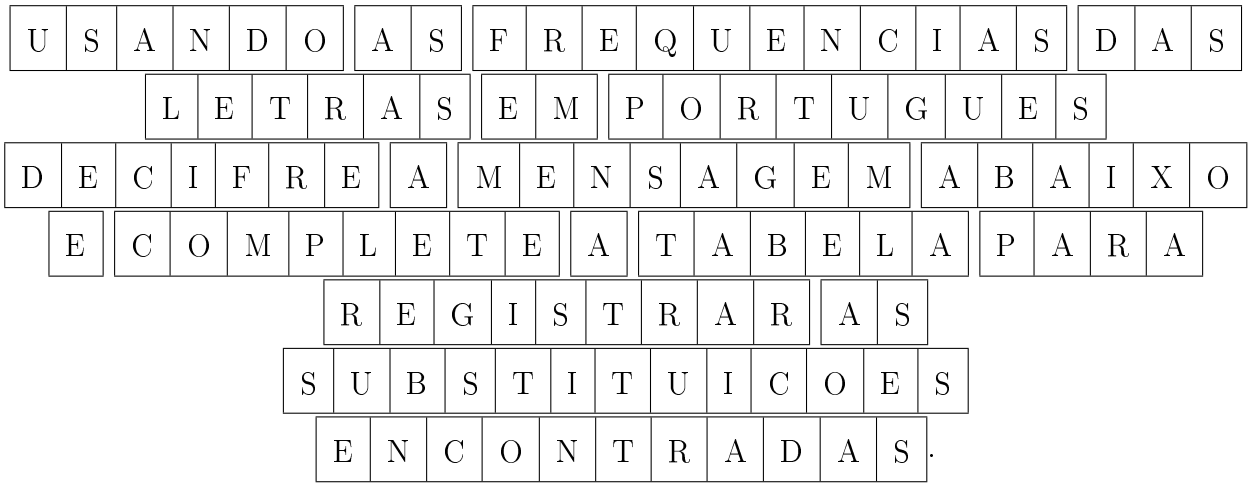





Note que S_ _STIT_ICOES é SUBSTITUIÇÕES, FRE_ _ENCIAS é FREQUÊNCIAS, _ETRAS é LETRAS. Assim, "u" é "U", "e" é "B", "p" é "Q" e "i" é "L". Logo:




Finalmente, note que a letra "n" é a letra "P" e a letra "x" é "X". Logo chegamos a mensagem original:




*Observação* 5. Note que não foi tão difícil descriptografar a mensagem, visto que foi possível manter a estrutura da Língua Portuguesa, só omitindo acentos e trocando ç por c. Poderíamos

ter juntado os artigos, preposições entre outros nas palavras próximas. Isso já tornaria o texto mais difícil de ser decifrado.

Apesar de ser um método que requer muito tempo para ser decifrado, os chamados "criptoanalistas" foram evoluindo nos seus métodos tanto no mundo árabe quanto na Europa, destruindo a segurança deste método, ou seja, qualquer um que enviasse uma mensagem codificada tinha que aceitar a possibilidade de que um especialista inimigo poderia interceptá-la e conhecer os segredos mais preciosos.

#### 2.1.3.3 As cifras monoalfabéticas e polialfabéticas.

Mesmo com a vulnerabilidade do método da substituição monoalfabética diante da análise de frequências, durante toda a Idade Média a Europa ainda utilizava esta técnica de criptografia. Na realidade, o avanço científico nesta época foi lento, sendo que grande parte do conhecimento sobre a criptografia era considerado magia negra. A criação da criptoanálise como ciência, a partir da definição do método da análise de frequências, deu início a uma permanente luta entre os criadores e os quebradores de códigos, o que desde aquela época, vem beneficiando ambas as partes. A reação a análise de frequências, com a criação de novas técnicas para criptografar mensagens, só ocorreu com o início do Renascimento, em 1450. Nesta época, correspondências sigilosas que tratavam de política externa, assuntos militares e economia, estavam vulneráveis e necessitavam ser melhor salvaguardadas. A primeira reação foi a utilização de códigos de substituição plurialfabéticas, proposto por Simeone de Crema, em 1452. Este código consistia em atribuir a cada letra do alfabeto, uma certa quantidade de símbolos, dependendo de sua frequência no alfabeto. A letra a, por exemplo, possui uma frequência dez vezes maior que algumas consoantes, por isso, deve ter uma maior quantidade de símbolos correspondentes. Veja a seguir um exemplo de tabela para uma cifra plurialfabeticas.

| Alfabeto original | Símbolos | Alfabeto original | Símbolos |
|---|---|---|---|
| A | w, e, ! ou @ | N | c |
| B | q | O | p, a, s ou % |
| C | h | P | d ou * |
| D | j | Q | v |
| E | r, t, y ou # | R | f ou ( |
| F | k | S | g ou + |
| G | l | T | b |
| H | ç | U | o ou & |
| I | u, i ou $ | V | n |
| J | ? | W | m |
| K | § | X | > |
| L | z | Y | $\pi$ |
| M | x | Z | £ |

Tabela 2.1.6: Tabela de cifras plurialfabeticas.

Desta forma, a frase MESTRADO PROFISSIONAL EM MATEMATICA, substituindo os espaços, aleatoriamente, por algarismos seria transformada em:

XRGBF WJP7D (AKU+ GISCE Z1TX8 X!BYX @BSHW

Apesar da cifra plurialfabética anular, em parte, a análise de frequências, algumas fragilidades ainda persistiram neste código. O fato da maioria das consoantes estar associada a uma única cifra, permite que se analise as cifras associadas as vogais, buscando no texto ininteligível as cifras das raízes NHA, NHO e QUE.

Certamente esta cifra dificultou bastante o trabalho dos criptoanalistas e este trabalho poderia ter ficado ainda mais difícil se usassem várias cifras também para as consoantes. Porém, não podemos esquecer que naquela época a criptografia era utilizada essencialmente para o comércio e nos campos de batalha, onde a necessidade de decifrar uma mensagem de forma simples e rápida era essencial. Por isso, a cifra plurialfabetica não atendeu totalmente as necessidades para uma comunicação simples e seguras.

A criptografia necessitava de uma cifra mais resistente aos ataques dos criptoanalistas. Para superar a fragilidade das cifras plurialfabética, o italiano Leon Battista Alberti

(1404 - 1472), nascido em Génova e conhecido como arquiteto criou em 1470, a primeira cifra polialfabética, através dos Discos de Alberti.

Um exemplo da utilização de uma cifra plurialfabética foi o código do Rei Felipe II da Espanha. No final do século XVI, o Império Espanhol dominava grande parte do mundo e os militares espanhóis se comunicavam utilizando a chamada Cifra Espanhola, que consistia de uma cifra plurialfabética composta por mais de 500 caracteres, com cada vogal sendo representada por três símbolos diferentes, cada consoante por dois símbolos e uma grande variedade de símbolos para a substituição dos dígrafos e das palavras curtas mais utilizadas. Além disso, o código era alterado a cada três anos. Por se tratar de uma variação da cifra monoalfabética, a complexidade do código não resistiu ao ataque feito pelo matemático francês Francois Viéte (1540 - 1603), que utilizou engenhosamente a análise de frequência, para que este código fosse quebrado.

Figura 2.1.5: Disco de Alberti. [10]

Esta foi a primeira ideia de mecanização dos processos de cifragem e decifragem. O disco externo é fixo e contêm as letras, algarismos e símbolos da mensagem original e o disco interno é móvel e fornece os respectivos símbolos correspondentes. Para cifrar uma mensagem utilizava-se uma quantidade de discos ajustados em posições diferentes e fazia-se a respectiva correspondência das letras do texto original, ordenadamente pelos discos. Por exemplo, para três discos teremos a primeira letra da mensagem codificada no primeiro disco,

a segunda letra no segundo disco, a terceira letra no terceiro disco, a quarta letra novamente no primeiro disco e assim sucessivamente.

O avanço principal do método de Alberti consiste em não permitir que a mesma letra do texto original apareça como uma única letra do alfabeto cifrado, ou seja, ele é o primeiro personagem que se tem notícia que utilizou a cifra de substituição polialfabética. Nesse método ele utilizava alternadamente dois alfabetos de César, causando uma enorme dificuldade para os criptoanalistas, pois a análise das frequências era insuficiente para decifrar as mensagens.

| Alfabeto original | Alfabeto cifrado 1 | Alfabeto cifrado 2 |
|---|---|---|
| a | X | F |
| b | F | R |
| c | O | O |
| d | R | A |
| e | I | L |
| f | H | M |
| g | J | E |
| h | K | G |
| i | N | H |
| j | G | I |
| k | M | J |
| l | E | K |
| m | Z | N |
| n | B | P |
| o | Y | Y |
| p | P | Z |
| q | A | B |
| r | L | C |
| s | Q | D |
| t | D | Q |
| u | C | S |
| v | T | T |
| w | U | U |
| x | S | V |
| y | V | W |
| z | W | X |

Tabela 2.1.7: Modelo de cifragem de Alberti.

Alberti não conseguiu desenvolver a sua ideia completamente pois o seu método não funcionava de forma sistemática. Com isso, este sistema passou por aperfeiçoamento, primeiramente por Johannes Trithemius (1462 - 1516), depois pelo italiano Giovanni Porta (1541 - 1615), e, por fim, pelo nosso próximo personagem: Blaise de Vigenère (1523 - 1596).

Blaise de Vigenère foi um diplomata francês do século XVI. Em razão da diplomacia, entrou em contato com o mundo da criptografia e quando encerrou sua carreira, dedicou grande parte do seu tempo a esta arte. Em 1586, publicou o livro Traité des chiffres où secrètes manières d'escrire, no qual expôs seu novo método de criptografar mensagens, baseado na cifra de César, a partir das ideias de Alberti. Sua técnica consistia em cifrar a primeira letra utilizando o método de César, deslocando três unidades; a segunda letra, deslocando 7; e assim por diante, deslocando arbitrariamente. Este método resiste à análise de frequências, pois cada letra se codifica de muitas formas distintas. Mas, se trocarmos arbitrariamente a cifra de César, nem nós mesmos seremos capazes de decifrá-la. Para não se perder na própria encriptação, Vigenère utilizou o conceito de palavra chave, o qual descreveremos a seguir.

Vamos imaginar que nos dão a chave VIGENERE. Se quisermos cifrar uma mensagem com esta chave procederemos do seguinte modo: para cifrar a primeira letra, utilizamos o alfabeto de César que começa por V, ou seja, quando $k = 21$ na cifra de César; para cifrar a segunda letra, utilizamos o alfabeto que começa por I, isto é, quando $k = 8$; a terceira com G, quando $k = 6$ e assim por diante, até chegar à oitava letra. Para a nona letra voltamos a utilizar o alfabeto na letra V. Neste exemplo, utilizamos seis alfabetos diferentes. Caso sejam escolhidas outras palavras (ou frases) chave, podemos variar muito o resultado do criptograma.

Para a realização prática deste método utiliza-se uma tabela que contém todos os alfabetos possíveis de serem utilizados. Para complicar ainda mais o trabalho dos criptoanalistas, basta elencar chaves bem mais longas e com poucas letras repetidas. Quanto mais alfabetos empregarmos, mais difícil será realizar a criptoanálise, ao método de Vigenère.

| 1 | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 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 |
| 3 | 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 |
| 4 | 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 |
| 5 | 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 |
| 6 | 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 |
| 7 | 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 |
| 8 | 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 |
| 9 | 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 |
| 10 | 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 |
| 11 | 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 |
| 12 | 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 |
| 13 | 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 |
| 14 | 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 |
| 15 | 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 |
| 16 | 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 |
| 17 | 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 |
| 18 | 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 |
| 19 | 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 |
| 20 | 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 |
| 21 | 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 |
| 22 | 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 |
| 23 | 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 |
| 24 | 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 |
| 25 | 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 |
| 26 | 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 |

Figura 2.1.6: O quadrado de Vigenère

Para decifrar a mensagem, o destinatário precisa saber que linha do quadrado de Vigenère foi usada para a cifragem de cada letra, e para isso, utiliza-se uma palavra-chave. Vejamos a seguir, um exemplo de cifragem usando o método de Vigenère.

**Exemplo 4.** Considere a palavra-chave ROMA para cifrar o texto INVADIR A CIDADE. As linhas do quadro de Vigenère a serem utilizadas são aquelas em que o alfabeto começa por R, O, M e A, apresentadas a seguir.

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 1 | 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 |
| | 2 | 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 |
| | 3 | 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 |
| | 4 | 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 |
| | 5 | 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 |
| | 6 | 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 |
| | 7 | 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 |
| | 8 | 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 |
| | 9 | 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 |
| 1 | 10 | 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 |
| | 11 | 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 |
| | 12 | 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 |
| 2 | 13 | 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 |
| | 14 | 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 |
| 3 | 15 | 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 |
| | 16 | 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 |
| | 17 | 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 |
| | 18 | 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 |
| | 19 | 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 |
| | 20 | 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 |
| | 21 | 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 |
| | 22 | 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 |
| | 23 | 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 |
| | 24 | 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 |
| | 25 | 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 |
| | 26 | 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 |

Figura 2.1.7: Cifragem de frase “invadir a cidade”

Assim, a letra “I” será substituída pela letra correspondente no alfabeto que começa pela letra “R”, ou seja, a letra “Z”;

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| R (10 posição) | 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 |

Figura 2.1.8: Codifica de Vigenève primeiro passo.

a letra “N” será substituída pela letra correspondente no alfabeto que começa pela letra “O”, ou seja, a letra “B”

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| O (13 posição) | 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 |

Figura 2.1.9: Codifica de Vigenève segundo passo.

a letra “V” será substituída pela letra correspondente no alfabeto que começa pela letra “M”, ou seja, a letra “H”

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| M (15 posição) | 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 |

Figura 2.1.10: Codifica de Vigenève terceiro passo.

a letra “A” será substituída pela letra correspondente no alfabeto que começa pela letra “A”, ou seja, a letra “A”

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| A (1 posição) | 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 |

Figura 2.1.11: Codifica de Vigenève quarto passo.

e assim por diante, até chegarmos ao texto cifrado ZBHAUWD R OIUOPE.

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Palavra Chave: | R | O | M | A | R | O | M | A | R | O | M | A | R | O | M | A |
| Texto original: | I | N | V | A | D | I | R | | A | | C | I | D | A | D | E |
| Texto cifrado: | Z | B | H | A | U | W | D | | R | | O | I | U | O | P | E |

Tabela 2.1.8: Cifragem de frase “invadir a cidade” utilizando a palavra chave.

*Observação* 6. Apresentaremos mais detalhes deste método no capítulo de Aplicações de criptografia em sala de aula, mais precisamente utilizando-o nos estudos sobre aritmética modular.

Apesar da potência deste método, ele veio a ser utilizado muito tarde, devido à complexidade do mesmo. Além disso ele resistiu durante muitos séculos às tentativas dos criptoanalistas de quebrá-lo, tanto que chegou a ser conhecido como "Le chiffre indéchiffrable" que significa a cifra indecifrável.

Uma explicação mais ampla de como este método funciona matematicamente será feito no capítulo 3.

Na prática, a decodificação deste método é totalmente inviável para ser executado de forma manual, por isso, durante séculos este foi o método mais eficiente para codificar mensagens. Por isso, a cifra ficou por quase 200 anos sem ser usada e quando foi utilizada mais intensamente, durou ainda um pouco mais de 100 anos, resistindo até 1856 quando o matemático Inglês Charles Babbage (1791 - 1871) descreve um método para quebrar a cifra de Vigenère. Veremos mais detalhes na seção 2.2

#### 2.1.3.4 Código em blocos.

Esta é uma maneira simples de tornar a contagem de frequência inviável [12]. Para utilizá-lo, subdividimos a mensagem em blocos de várias letras e embaralhamos estes blocos. Por isso, este método de criptografar é conhecido como código de blocos. Para codificar um texto, utilizando este método, seguimos os seguintes passos: Primeiramente eliminamos os espaços e completamos a mensagem com um "A" no final, caso tenha uma quantidade ímpar de letras; em seguida subdividimos a mensagem em blocos de duas letras; depois refletimos cada bloco; e por último permutamos alguns blocos trocando o primeiro com o último, o segundo com a penúltimo, mas deixando os outros como estão. Vejamos um exemplo a seguir.

**Exemplo 5.** Considere a mensagem AMO MINHA PATRIA.

Aplicando o método, passo a passo, à mensagem acima, obtemos primeiro

AMOMINHAPATRIA

depois

AM-OM-IN-HA-PA-TR-IA

em seguida

MA-MO-NI-AH-AP-RT-AI

e, finalmente,

AI-RT-NI-AH-AP-MO-MA

que nos dá a mensagem codificada

AIRTNIAHAPMOMA.

Percebemos que não ajuda em nada trabalhar com a contagem de frequência média porque esta não muda em nenhum momento, o que acontece é que as letras são misturadas em blocos. Dificultando assim a decodificação da mensagem.

## 2.2 Máquina de cifragem.

O matemático Inglês Charles Babbage foi uma das personalidades mais incomuns da área científica [12]; [13]; [22]. Relata-se que era filho de família nobre e foi deserdado por ter uma vida extravagante. Gastou sua fortuna implementando ideias e máquinas, nem todas bem sucedidas. No entanto, uma das máquinas desenvolvidas por Babbage é reconhecida nos dias atuais como o primeiro protótipo de um computador.

Babbage quebrou a cifra de Vigenère utilizando uma técnica que se resumiu em determinar o comprimento k da palavra chave. Para isso, ele atribuia valores para k, que

variavam de 1 até 26, e em seguida dividia a mensagem criptografada em k textos. As letras que formam cada texto estão a uma distância k uma das outras no texto original cifrado, por exemplo, se k = 4, o primeiro texto será formado pelas letras que estão nas posições 1, 5, 9 e assim por diante. Após esta etapa, ele aplicava a análise de frequência em cada um dos textos, visando buscar repetições que indiquem dígrafos e trígrafos tais como *que, nha, nhe, nho, não, ai* e *ou.* Encontrados estes digrafos e trígrafos, Babbage utilizava o valor de k como comprimento da palavra chave, e a partir daí poderia descobrí-la. A quebra da cifra de Vigenère instaurou um clima de insegurança na transmissão secreta de mensagens e a Idade Moderna termina da mesma forma como começou, com os criadores de códigos em busca de uma nova cifra que pudesse reestabelecer a comunicação segura.

Em 1918 o inventor alemão Arthur Scherbius e seu amigo Richard Ritter fundaram uma empresa, a Scherbius&Ritter. Um dos projetos desta empresa era substituir os sistemas de Criptografia inadequados, usados na Primeira Guerra Mundial, a partir da troca de cifras de papel e lápis por uma forma de cifragem que usasse a tecnologia do século XX. Engenheiro eletricista de formação, ele patenteou a invenção de uma máquina de cifra mecânica, a qual era basicamente uma versão elétrica do disco de Alberti, mais tarde vendida como a máquina Enigma. Em 1925, Scherbius produziu a Enigma em grande escala, pois as autoridades alemãs acreditavam na segurança absoluta que ela proporcionava. Trinta mil máquinas foram adquiridas e utilizadas, nas duas décadas seguintes, pelo exército alemão.

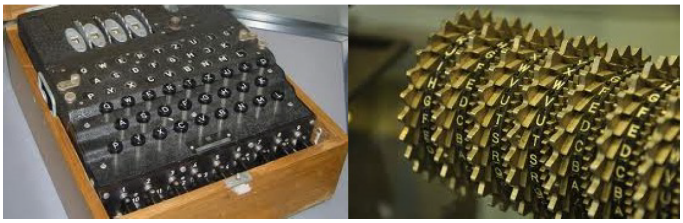


Figura 2.2.1: Máquina elétrica Enigma de criptografia.

A Enigma lembrava uma máquina de escrever. Era constituída de um teclado,

um painel luminoso, uma câmara com três misturadores, um refletor e um painel frontal com cabos elétricos. A mensagem era cifrada e decifrada usando o mesmo tipo de máquina. A chave para a utilização da Enigma dependia de uma configuração de montagem, que compreendia a ordem e a posição dos misturadores, conexão dos cabos emparelhando duas letras no painel frontal e a posição do refletor. Para cifrar uma mensagem, o operador teclava uma letra e o comando estimulava o circuito elétrico e as letras cifradas apareciam, uma a uma, no painel luminoso.

A seguir apresentamos algumas figuras que representam um exemplo de utilização da máquina Enigma de três rotores. Tais figuras podem ser obtidas em [9].

Primeiramente ajustaremos alguns parâmetros, conforme figuras 2.2.2 e 2.2.3 e em seguida escrevemos a mensagem desejada no campo "output" aparecerá a mensagem codificada, conforme podemos observar nas figuras 2.2.4, 2.2.5 e 2.2.6.

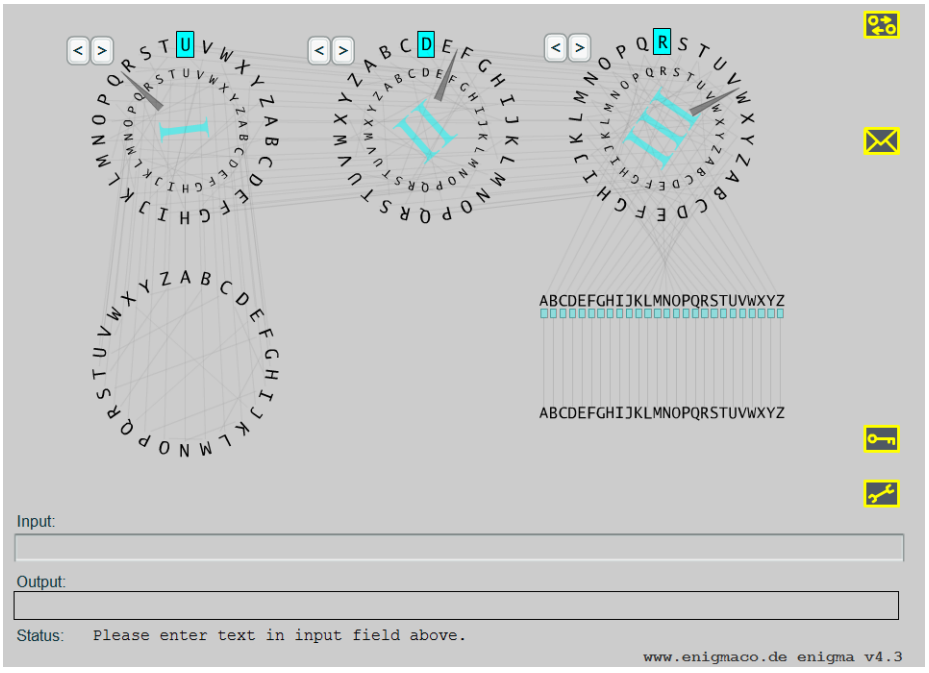



Figura 2.2.2: Padrões para a criptografia.

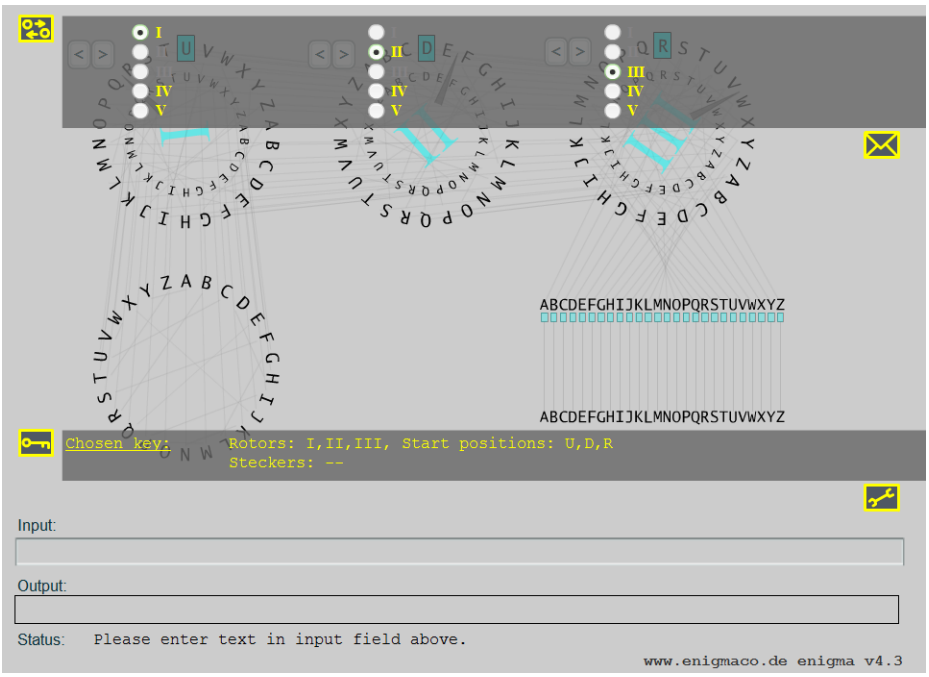



Figura 2.2.3: Padrões para a criptografia.

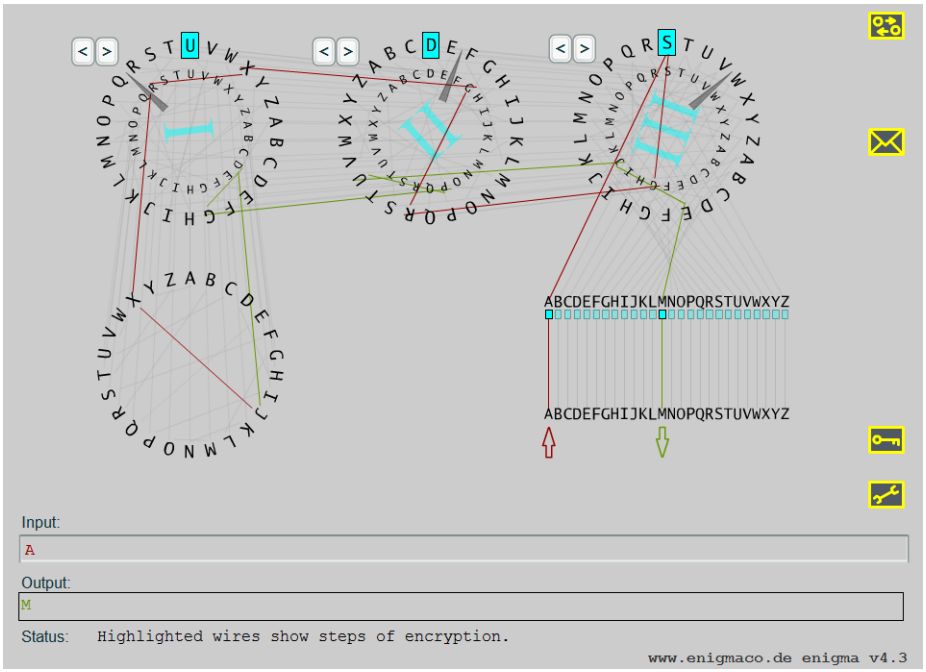



Figura 2.2.4: Parâmetros iniciais.

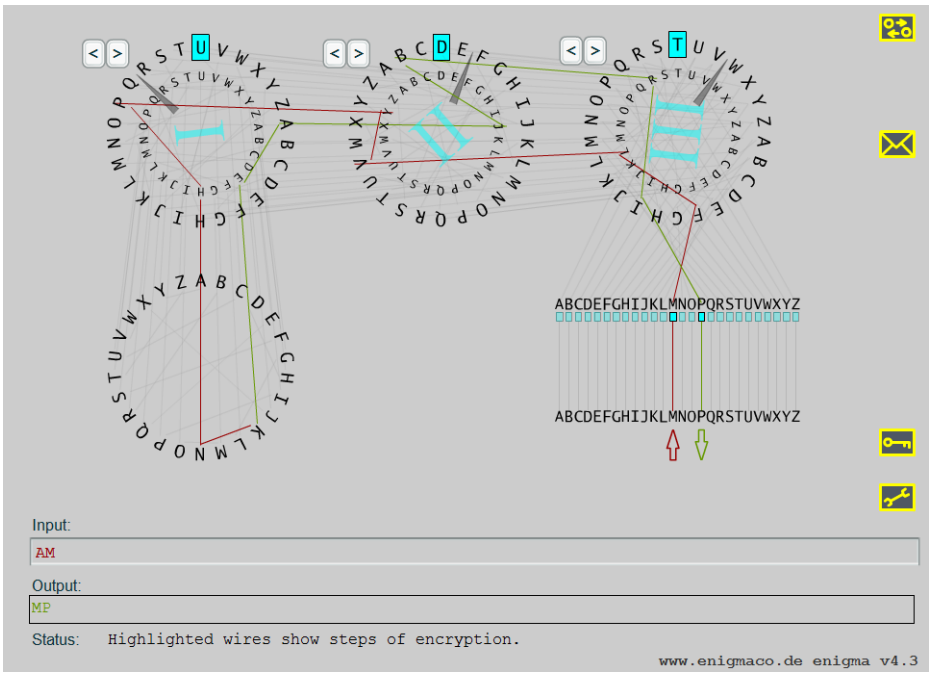



Figura 2.2.5: Parâmetros iniciais.

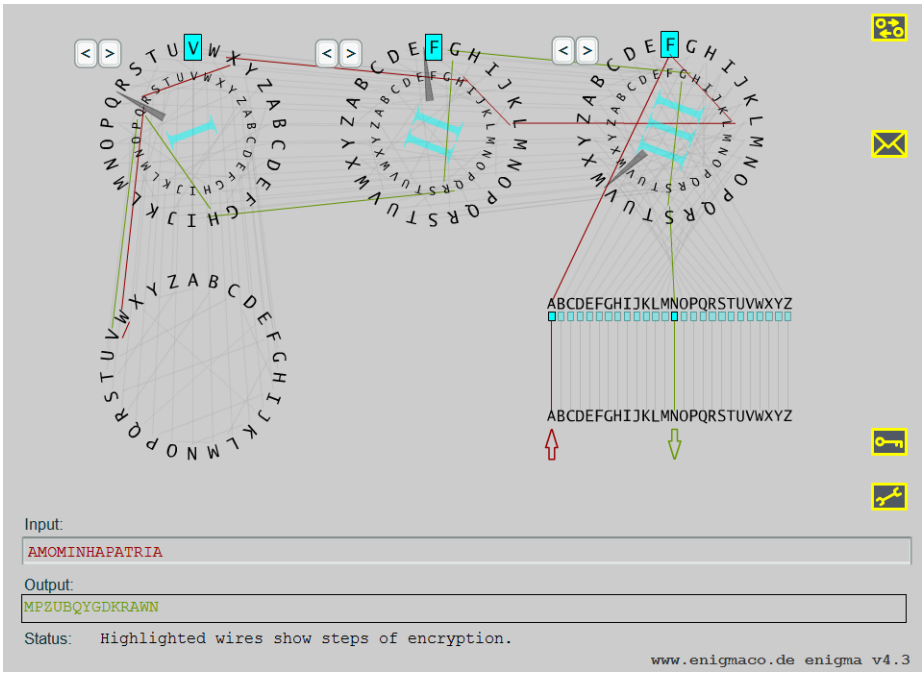



Figura 2.2.6: Exemplo de codificação da máquina Enigma.[9]

A Enigma era extremamente forte e por aproximadamente treze anos, os criptoanalistas franceses e britânicos acreditaram que mensagens cifradas por ela eram indecifráveis sem o conhecimento da chave. Após um árduo trabalho, o criptoanalista Alan Turing conseguiu vencer tal desafio na primeira metade da década de 40. Isso foi feito em Bletchley Park, onde ficava a sede da Escola de Cifras e Códigos do Governo da Inglaterra (GC&CS), a partir do surgimento dos criptoanalistas poloneses. Essa identificação se deu pelo desenvolvimento de máquinas chamadas "bombas". A quebra das cifras da Enigma deu aos Aliados uma vantagem fundamental, que, de acordo com historiadores, reduziu em dois anos a guerra, salvando muitas vidas.

Outro aparelho que tinha como finalidade decifrar mensagens foi desenvolvido na Inglaterra com base nas ideias de Turing. Denominado de "Colossos", foi utilizado para decifrar as codificações feitas pela máquina Lorenz, empregada nas comunicações de Hitler e seus generais.

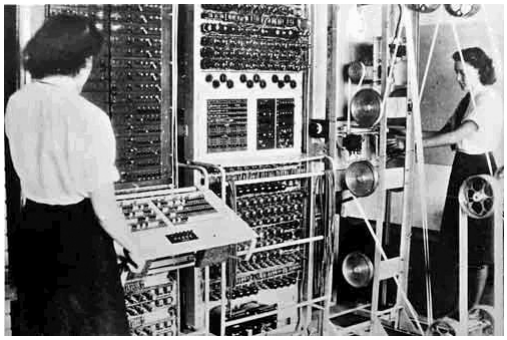


Figura 2.2.7: Colossos: percursor do computador.

O Colossos apresentou duas vantagens em relação às bombas: a primeira é que era constituído de válvulas eletrônicas bem mais rápidas do que os antigos eletromecânicos utilizados nas bombas e a segunda é o fato de serem programáveis, o que fez com que ele fosse considerado o precursor do computador moderno. Em razão disto, podemos dizer que o computador teve origem na criptoanálise.

## 2.3 Criptografia nos computadores.

Na criptografia mecânica é fundamental a ocultação pública da chave e também é desejável manter segredo sobre a estrutura da máquina que produz a cifragem. Com o desenvolvimento e aperfeiçoamento dos computadores, a incrível capacidade de realizar mais de um milhão de operações por segundo e a necessidade de uso da criptografia pelo comércio e bancos, os algoritmos criptográficos passam a ser de conhecimento público e o segredo passa a residir exclusivamente na chave. As criptografias simétrica e assimétrica que aprentaremos a seguir possui essas características.

### 2.3.1 Criptografia Simétrica.

Os algoritmos de chave simétrica (também chamado chave privada) são uma classe de algoritmos para a criptografia, que usam chaves criptográficas relacionadas para as operações de cifragem e decifragem. Usa-se uma única chave, partilhada por ambos os interlocutores, na premissa de que esta é conhecida apenas por eles, a qual pode ser usada para manter um canal confidencial de informação. Ela é conhecida também por secretkey ou symmetric-key encryption. Esta chave pode ser uma palavra, frase ou uma sequência aleatória de números e/ou símbolos. O tamanho da chave é medido em bits e, por regra, quanto maior for a chave, mais seguro será o documento codificado. O esquema dessa criptografia pode ser resumido na figura 2.3.1.

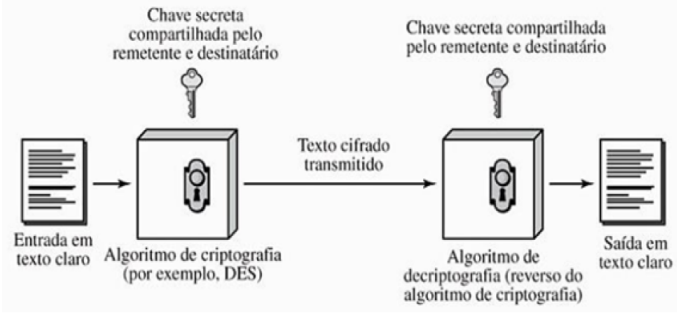



Figura 2.3.1: Criptografia simétrica.

A operação de chave simétrica é mais simples que a assimétrica, pois pode existir uma única chave entre as operações, no entanto, para um remetente e um destinatário se comunicarem utilizando este método, eles têm que concordar quanto ao valor da chave e têm que manter isso em segredo. Se eles estão em localizações físicas diferentes, deverão confiar em um mensageiro, telefone, SMS, e-mail ou outro meio seguro de comunicação para prevenir a revelação da chave secreta antes da transmissão.

Como fazer com que o destinatário receba a chave sem alguém interceptá-la? Veremos mais adiante que isto se tornou um problema quase axiomático na informática, conhecido como “o problema da troca de chaves”. Vejamos a seguir, os principais algoritmos simétricos. Além desses podemos citar também outros algoritmos de chave privada, são eles: 3DES, Blowfish, Twofish, RC4 e CAST.

DES - O Data Encryption Standard é o algoritmo simétrico mais disseminado no mundo, até a padronização do AES. Foi criado pela IBM em 1977 e, apesar de permitir cerca de 72 quatrilhões de combinações (256 bits), seu tamanho de chave (56 bits) é considerado pequeno, tendo sido quebrado por "força bruta"em 1997 em um desafio lançado na Internet.

AES - O Advanced Encryption Standard é uma cifra de bloco, anunciado pelo NIST em 2003, fruto de concurso para escolha de um novo algoritmo de chave simétrica para proteger informações. Foi adotado como método padrão pelo governo dos Estados Unidos pela eficiência demonstrada. É um dos algoritmos mais populares, desde 2006, usado para Criptografia de chave simétrica, sendo considerado como o padrão substituto do DES. O AES tem um tamanho de bloco fixo em 128 bits e uma chave com tamanho de 128, 192 ou 256 bits, é rápido tanto em software quanto em hardware, é relativamente fácil de executar e requer pouca memória.

O 3DES é uma simples variação do DES, utilizando-o em três ciframentos sucessivos, podendo empregar uma versão com duas ou com três chaves diferentes. É seguro, porém muito lento para ser um algoritmo padrão.

O IDEA - International Data Encryption Algorithm - foi criado em 1991 por James Massey e Xuejia Lai e possui patente da suca ASCOM Systec. O algoritmo é estruturado seguindo as mesmas linhas gerais do DES. Na maioria dos microprocessadores, uma implementação por software do IDEA é mais rápida do que uma implementação por software do DES. O IDEA é utilizado principalmente no mercado financeiro e no PGP, o programa para criptografia de e-mail pessoal mais disseminado no mundo.

Por mais de dois mil anos, desde a época da cifra de César até a década de 70, a comunicação cifrada exigia que as duas partes comunicantes compartilhassem um segredo em comum, a chave simétrica usada para cifrar e decifrar. Uma dificuldade dessa abordagem é que as duas partes têm que escolher, conjuntamente e de alguma maneira, qual é a chave. Mas, para isso, é preciso comunicação segura. Uma alternativa seria um encontro entre as partes para que escolhessem, pessoalmente, a chave. Porém, no atual mundo em rede, o mais provável e que as partes comunicantes nunca possam se encontrar. No intuito de solucionar este problema, vários cientistas na década de 70 voltaram suas pesquisas para a busca de uma solução. Porém, em 1976, Diffie e Hellman apresentaram um algoritmo conhecido como Diffie Hellman Key Exchange, que tornou possível a comunicação por criptografia sem a necessidade de compartilhamento antecipado de uma chave secreta comum. Uma abordagem da comunicação segura radicalmente diferente e de uma elegância que levou ao desenvolvimento dos atuais sistemas de criptografia de chaves públicas. Este novo método será apresentado na próxima seção.

### 2.3.2 Criptografia Assimétrica.

A criptografia assimétrica (ou de chave pública) transforma um texto claro em texto cifrado usando uma de duas chaves e um algoritmo de criptografia. Usando a outra chave associada e um algoritmo de decriptografia, o texto claro é recuperado a partir do texto cifrado. A chave pública pode ficar disponível para qualquer pessoa que queira se comunicar, de modo seguro inclusive os intrusos, mas a chave privada deverá ficar em poder

apenas de cada titular. Primeiramente, o remetente busca a chave pública do destinatário, em seguida, ele criptografa sua mensagem usando a chave pública do destinatário e um algoritmo criptográfico. O destinatário recebe a mensagem criptografada e usa sua chave privada e um algoritmo de decriptografia para decifrar a mensagem recebida. Dessa forma, duas pessoas podem trocar mensagens secretas sem que nenhuma delas necessite permutar alguma chave. Para ilustrar essa situação, vamos utilizar o esquema dos cadeados no exemplo a seguir.

**Exemplo 6.** Alice deseja enviar uma carta a Bob que não seja interceptada. Bob distribui milhares de cadeados abertos iguais pelas agências de correios do mundo todo, mas somente ele tem a chave que abre esses cadeados. Assim, Alice vai até uma agência dos correios, pede o cadeado referente a Bob e tranca a carta com esse cadeado. Note que ela não pode mais abrir o cadeado, somente Bob pode fazer isso. Assim, mesmo que outra pessoa tente interceptar a mensagem, somente Bob pode abri-lo.

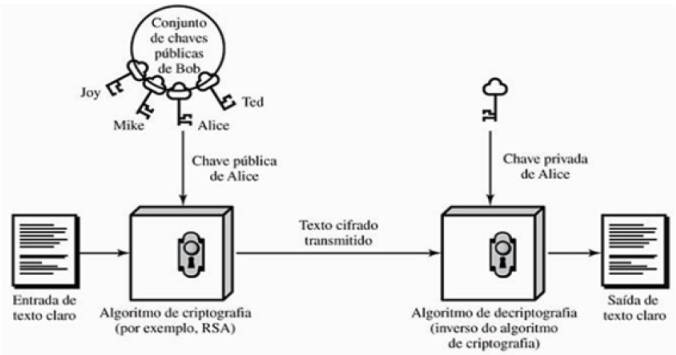



Figura 2.3.2: criptografia assimétrica [19].

De acordo com [SINGH 21] esse modelo de criptografia foi criado na década de 70 pelo matemático Clifford Cocks, que trabalhava no serviço secreto inglês, porém, como o seu trabalho não foi divulgado, a primeira evidência pública foi em 1976 com Diffie e Hellman. Eles mudaram os rumos da criptografia desenvolvendo a criptografia assimétrica na tentativa de solucionar o problema da troca de chaves. Conforme foi dito por Diffie: "Afinal, qual

é a vantagem de desenvolver criptossistemas impenetráveis, se seus usuários forem forçados a compartilhar suas chaves com um Centro de Distribuição de Chaves - CDC - que pode estar sujeito a roubo ou suborno?". A principal vantagem deste método é a sua segurança, pois não é preciso (nem se deve) compartilhar a chave privada. Deve-se destacar que na criptografia assimétrica, o tempo de processamento de mensagens é muitas vezes maior do que a criptografia simétrica, dando maior dificuldade para o criptoanalista que deseja decifrar a mensagem.

A figura anterior, de forma simplificada, a criptografia assimétrica.

Usando a notação da figura 2.3.2, mostraremos os procedimentos que levarão a codificação e decodificação de qualquer mensagem m. Será apresentado a seguir a linguagem adotada para representrar cada procedimento: $m$ "texto claro", $e_b$ "chave pública" , $e_b(m)$ "texto cifrado transmitido", $d_b$ "chave privada e $d_b(e_b(m))$ "saída de texto claro ". Neste caso, podemos permutar as chaves criptográficas pública e privada e obter o mesmo resultado, isto é, $e_b(d_b(m)) = d_b(e_b(m)) = m$.

O uso da criptografia de chave pública é, portanto, conceitualmente simples, mas apresenta duas preocupações. A primeira preocupação diz respeito ao conhecimento público da chave e do algoritmo de criptografia, isto é, embora um intruso que intercepte a mensagem cifrada veja apenas dados ininteligíveis, ele conhece tanto a chave quanto o algoritmo usado para a criptografia. Assim, um intruso pode montar um ataque para decodificar mensagens, ou parte delas, que suspeite que tenham sido enviadas. Fica claro que, para a criptografia de chave pública funcionar, a escolha de chaves e de códigos de criptografia/decriptografia deve ser feita de tal forma que seja praticamente impossível para um intruso determinar a chave privada do destinatário. A segunda preocupação se refere ao envio da mensagem cifrada, ou seja, como a chave criptográfica do destinatário é pública, qualquer um pode enviar uma mensagem cifrada para ele. Neste caso, se faz necessário o uso de uma assinatura digital, que visa garantir a autenticidade de quem envia a mensagem, associada a integridade do seu conteúdo, vinculando um remetente a mensagem. Vejamos a seguir, alguns tipos de

algoritmos assimétricos.

O RSA - É um algoritmo assimétrico que possui este nome devido a seus inventores: Ron Rivest, Adi Shamir e Len Adleman, que o criaram em 1977 no Massachusetts Institute of Technology (MIT). Atualmente é um algoritmo de chave pública amplamente utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecidas até o momento. O RSA utiliza números primos e parte da premissa de que é fácil multiplicar dois números primos para obter um terceiro número, porém, é muito difícil recuperar os dois primos a partir daquele terceiro número dado, ou seja, o que é difícil no processo é a fatoração. Por exemplo, os fatores primos de 3.337 são 47 e 71. Gerar a chave pública envolve multiplicar dois primos grandes, que é um processo simples, no entanto, derivar a chave privada a partir da chave pública envolve fatorar um grande número, que é um processo mais complexo. Se o número for grande o suficiente e bem escolhido, então ninguém pode fazer isto em um curto período tempo. Assim, a segurança do RSA baseia-se na dificuldade de fatoração de números grandes. Uma chave RSA de 512 bits foi quebrada em 1999 pelo Instituto Nacional de Pesquisa da Holanda, com o apoio de cientistas de mais seis países. Levou cerca de sete meses e foram utilizadas 300 estações de trabalho para a quebra. Um fato preocupante é que cerca de 95% dos sites de comércio eletrônico utilizam chaves RSA de 512 bits.

O ElGamal é outro algoritmo de chave pública utilizado para gerenciamento de chaves. O algoritmo envolve a manipulação matemática de grandes quantidades de dados-numéricas. Sua segurança advêm de algo denominado problema do logaritmo discreto. O algoritmo obtêm sua segurança da dificuldade de se calcular logaritmos discretos em um corpo finito, o que lembra bastante o problema da fatoração.

Diffie-Hellman é também baseado no problema do logaritmo discreto, trata-se do criptossistema de chave pública mais antigo ainda em uso. O conceito de chave pública, aliás, foi introduzido pelos autores deste criptossistema em 1976. O problema desse método é que ele não permite ciframento. O sistema foi projetado para permitir a dois indivíduos

entrarem em um acordo ao compartilharem um segredo tal como uma chave, muito embora eles somente troquem mensagens em público.

Curvas Elípticas - Em 1985, Neal Koblitz e V. S. Miller propuseram de forma independente a utilização de curvas elípticas para sistemas criptográficos de chave pública. Eles não chegaram a inventar um novo algoritmo criptográfico com curvas elípticas sobre corpos finitos, mas implementaram algoritmos de chave pública já existentes, como o algoritmo de Diffie-Hellman, usando curvas elípticas. Eles possuem o potencial de criação de sistemas criptográficos de chave pública mais seguros, com chaves de menor tamanho. Desta forma, fica resolvido um dos maiores problemas dos algoritmos de chave pública: o grande tamanho de suas chaves. Porém, os algoritmos de curvas elípticas atuais, embora possuam o potencial de serem rápidos, são em geral mais demorados do que o RSA.

Durante algum tempo, muito se discutiu sobre a melhor forma de se criptografar, se utilizando um sistema simétrico ou assimétrico. Na realidade, como mostra a tabela 2.3.1 a seguir, existem vantagens e desvantagens nos dois métodos, dependendo do contexto e das condições, a escolha do melhor sistema pode variar.

| | Criptografia simétrica | Criptografia assimétrica |
|---|---|---|
| Forma de criptografar uma mensagem | Técnica de substituição e permutação | Funções matemáticas |
| Velocidade | Rápido | Lento |
| Distribuição de chave | Complexo | Simples |
| Assinatura digital | Não necessita | Necessita |

Tabela 2.3.1: Figura de comparação de chave pública e chave privada.

### 2.3.3 Conclusões

Vimos anteriormente que a forma de criptografar uma mensagem fazendo uso de chave pública, através de técnicas avançadas e complexas utilizando funções matemáticas, acarreta em um índice de dificuldade a ação de intrusos, maior do que se utilizássemos criptografia

simétrica. Porém, dependendo da situação e dos recursos disponíveis, a complexidade excessiva pode tornar impraticável cifrar e decifrar uma mensagem. Por exemplo, em um campo de batalha, digamos que o Comandante de uma Unidade deseje trocar mensagens simples de orientação com os Comandantes de Subunidades, através de um mensageiro, porém não queira que estas mensagens sejam ostensivas. O Comandante poderia se reunir previamente com os Comandantes de Subunidade e trocar chaves simétricas para este tipo de comunicação. Porém, há situações onde a velocidade e a disponibilidade de equipamentos não são um empecilho; digamos que a maior dificuldade seja reunir as partes comunicantes. Obviamente, a utilização de criptografia de chave pública seria mais oportuna nesse caso. Na prática, o que tem sido utilizado são algoritmos híbridos que utilizam as vantagens de cada um dos sistemas, como por exemplo, o PGP (Pretty Good Privacy) para correio eletrônico, o IPSec, o S/MIME (Secure Multipurpose Internet Mail Extensions), entre outros.

A partir do início de 1990, começa o trabalho de pesquisa para a construção de computadores quânticos e o desenvolvimento de uma criptografia quântica. Segundo [19] os primeiros ensaios experimentais são publicados por Charles H. Bennett, GillesBrassard e colaboradores, relatando o uso de fótons para transmitir um fluxo de bits. Em um computador quântico a velocidade será muito maior que no mais moderno dos computadores de nossa época. No momento, a pesquisa e o desenvolvimento de computadores quânticos ainda é incipiente e guardada em segredo, mas quando esta tecnologia se tornar uma realidade, novos desafios darão continuidade a esta rica história da criptografia.

# Capítulo 3

# Aplicações da criptografia em sala de aula.

Nas Orientações Curriculares para o Ensino Médio (2006) [1], consta que o aluno de ser capaz de utilizar a Matemática na resolução de problemas do cotidiano e para modelar fenômenos das distintas áreas do conhecimento. Consta também que o aluno compreenda a Matemática como conhecimento social que foi construído ao longo da história, entendendo a sua importância no desenvolvimento científico e tecnológico. Sabemos que a matemática enfrenta diversos desafios na busca de aliar o interesse discente e a formação do cidadão, partindo do pressuposto que a educação se concretiza nesta relação. Portanto, aproximar a linguagem matemática da realidade é o foco de estratégias educacionais, para que os alunos se tornem cidadãos conscientes, apropriando-se de conhecimentos matemáticos fundamentais para uma formação crítica de nossa sociedade.

Neste contexto, a criptografia pode ser um elemento motivador para o processo de ensino e aprendizagem da Matemática, pois seu desenvolvimento histórico e sua aplicabilidade disponibilizam ao professor muitos exemplos contextualizados, ao mesmo tempo em que promovem uma interessante ligação com as ciências sociais e sociedade. Descreveremos exemplos da correlação entre matemática e criptografia, ressaltando que a forma de abordagem

dos conteúdos não são, necessariamente, a mais real utilização da aplicação da criptografia, mas servem para embasar o conhecimento dos professores que se propuserem a ensinar este assunto aos seus alunos do Ensino Fundamental e Médio. Este capítulo possui vários exemplos de atividades para aplicação com estudantes do Ensino Fundamental e Médio.

Alguns conceitos que são absolutamente fundamentais para a Criptografia são congruência, função no sentido matemático de uma transformação, combinação entre outros. Neste capítulo, abordamos algumas definições preliminares que servirão como base para a aplicação em técnicas de cifragem por substituição e transposição apresentadas na seção de atividades. As referências utilizadas neste capítulo foram [2]; [4]; [5]; [12]; [13]; [16]; [21].

## 3.1 Conceitos Preliminares.

### 3.1.1 Congruência.

**Definição 1.** Seja dado um número inteiro m maior do que 1. Diremos que dois números inteiros a e b são congruentes módulo m se a e b possuírem mesmo resto quando divididos por m. Neste caso, simbolizaremos esta situação como segue:

$a \equiv b \bmod m$.

Quando a e b não são congruentes módulo m, escreve-se

$a \not\equiv b \bmod m$.

**Exemplo 7.** Alguns exemplos:

$15 \equiv 8 \bmod 7$, pois o restos das divisões de 15 e de 8 por 7 são os mesmos (iguais a 1).

$27 \equiv 32 \bmod 5$, pois os restos das divisões de 27 e 32 por 5 são os mesmos (iguais a 2).

$31 \not\equiv 29 \bmod 3$, pois o resto da divisão de 31 por 3 é 1, enquanto o resto da divisão de 29 por 3 é 2.

Para mostrar que a ≡ b mod m não é necessário efetuar a divisão de a e de b por m, como mostrado a seguir.

**Proposição 1.** *Tem-se que $a \equiv b \ mod \ m$ se e somente se m divide b - a.*

*Demonstração.* De fato, pelo algoritmo da divisão, existe $q_1$, $q_2$, $r_1, r_2 \in \mathbb{Z}$ tais que

$$a = mq_1 + r_1 \text{ e } b = mq_2 + r_2;$$

onde $0 \leq r_1 < m$ e $0 \leq r_2 < m$. Sem perda de generalidade, podemos supor que $r_1 \leq r_2$ (se o contrário ocorrer, basta trocar os papéis de $r_1$ *e* $r_2$). Assim, podemos escrever

$$b - a = m\,(q_2 - q_1) + r_2 - r_1.$$

Logo, m divide (b - a) se, e somente se, m divide $(r_2 - r_1)$. Por ser $0 \leq r_2 - r_1 < m$, segue que m divide (b - a) se, e somente, se $r_2 - r_1 = 0$, ou seja, m divide (b-a)se, e somente se, $r_2 = r_1$.

□

Com base nessa definição, vamos atribuir um equivalente numérico a cada letra do alfabeto a = 0, b = 1, c = 2, d = 3, ..., z = 25, que será relacionado ao código de Cesar com congruência.

| Número Associado | Alfabeto | Número Associado | Alfabeto |
|---|---|---|---|
| 00 | A | 13 | N |
| 01 | B | 14 | O |
| 02 | C | 15 | P |
| 03 | D | 16 | Q |
| 04 | E | 17 | R |
| 05 | F | 18 | S |
| 06 | G | 19 | T |
| 07 | H | 10 | U |
| 08 | I | 21 | V |
| 09 | J | 22 | W |
| 10 | K | 23 | X |
| 11 | L | 24 | Y |
| 12 | M | 25 | Z |

Tabela 3.1.1: Substituição de letras por números.

Podemos expressar um algoritmo da seguinte maneira: substitua cada letra no texto original, que vamos chamar de texto p, pela letra do texto cifrado, que vamos chamar de C. Aplicando a notação utilizada na aritmética modular, temos:

$$C \equiv (p + 3) \bmod 26 \text{ (deslocamento de três casas)}$$

Embora [21] só mencione que César deslocava as letras em três casas, fica claro que podemos fazer um deslocamento de qualquer quantidade, de modo que o algoritmo de César fique representado por

$$C \equiv (p + k) \bmod 26; \text{ com } k \in \mathbb{Z} \text{ fixo e } 1 \leq k \leq 25$$

No que diz respeito a decodificar o texto por este método, bastará fazer, no máximo, 25 tentativas, pois o texto não é o original, por isso uma possibilidade é excluída, ou seja, quando $k = 0$. Costuma-se dizer que é um método de decodificação utilizando a "força bruta".

O método de César mais geral é aquele em que efetuamos uma permutação arbitrária das 26 letras do alfabeto. Como existem 26! permutações distintas de um conjunto de 26 elementos, existe uma grande quantidade de cifras distintas. Para tentar decodificar um texto utilizando a força bruta, no caso da substituição monoalfabética, fazemos uma relação entre cada letra do alfabeto original com um outro alfabeto permutado. Assim, considerando que cada letra do alfabeto deve ser substituída por uma letra diferente dela mesma, teremos os $26!\left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + \frac{1}{26!}\right) \cong 1,48 \cdot 10^{26}$ possibilidades de definir a chave deste código, que correspondem as permutações caóticas das 26 letras do alfabeto, o que torna bem mais complicado o ataque por força bruta.

### 3.1.2 O Princípio Multiplicativo da Contagem:

Se uma decisão puder ser tomada de m maneiras diferentes e se, uma vez tomada esta primeira decisão, outra decisão puder ser tomada de n maneiras diferentes, então, no total

serão tomadas m x n decisões.

Há um conceito muito útil para se trabalhar com produtos do tipo acima, ou seja, com produto em que os fatores vão decrescendo de um em um, tal conceito é chamado fatorial. Por exemplo, o fatorial de 3 é $3! = 3 \cdot 2 \cdot 1$. No caso geral, para um inteiro positivo n, define-se $n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$ e, por convenção, $0! = 1$.

### 3.1.3 Funções.

**Definição 2.** Sejam X e Y dois conjuntos quaisquer. Uma função é uma relação $f : X \to Y$ que, a cada elemento $x \in X$, associa um e somente um elemento $y \in Y$ . Além disso,

(i) Os conjuntos X e Y são chamados domínio e contradomínio de f, respectivamente;

(ii) O conjunto $f(X) = \{y \in Y, \exists x \in X, f(x) = y\} \subset Y$ é chamado imagem de f;

(iii) Dado $x \in X$, o (único) elemento $y = f(x) \in Y$ correspondente é chamado imagem de x.

Como estabelecido na Definição 2, uma função é um terno constituído por elementos: domínio, contradomínio e lei de associação (segundo a qual os elementos do domínio estão associados aos do contradomínio). Para que uma função esteja bem definida, é necessário que estes três elementos sejam dados.

### 3.1.4 Funções Compostas

**Definição 3.** Sejam $f : X \to Y$ e $g : U \to V$ duas funções, com $Y \subset U$. A função composta de g com f é a função denotada por $g \circ f$, com domínio em X e contradomínio em V, que a cada elemento $x \in X$ faz corresponder o elemento $y = (g \circ f)(x) = g(f(x)) \in V$ .

### 3.1.5 Função Invertível

Denotemos $I_A$ a função identidade do conjunto A, ou seja, $I_A$: A $\longmapsto$ A é definida por $I_A$(x) = x.

**Definição 4.** Uma função f : X $\to$ Y é invertível se existe uma função g : Y $\to$X tal que

(i) f$\circ$g = $I_y$ ;

(ii) g$\circ$f = $I_x$.

Neste caso, a função g é dita função inversa de f e denotada g = $f^{-1}$.

**Definição 5.** Consideremos uma função f : X $\to$ Y . Dizemos que:

(i) f é sobrejetiva se para todo y $\in$ Y , existe x $\in$ X tal que f(x) = y;

(ii) f é injetiva se $x_1$, $x_2$ $\in$ X, $x_1 \neq x_2 \Rightarrow\ f(x_1) \neq f(x_2)$;

(iii) f é bijetiva se é sobrejetiva e injetiva.

Há ainda formas equivalentes de enunciar as definições acima:

1. f é sobrejetiva se, e somente se, f(X) = Y ;

2. f é injetiva se, e somente se, $x_1$, $x_2$ $\in$ X, $f(x_1) = f(x_2) \Rightarrow\ x_1 = x_2$;

3. f é injetiva se, e somente se, para todo y $\in$ f(X), existe um único x $\in$ X tal que f(x) = y;

4. f é bijetiva se, e somente se, para todo y $\in$ Y , existe um único x $\in$ X tal que f(x) = y.

**Teorema 1.** *Uma função f : X $\to$ Y é invertível se, e somente se, é bijetiva.*

*Demonstração.* ($\Rightarrow$) Por hipótese, existe g : Y $\to$ X tal que: (i) f$\circ$g = $I_y$ e (ii) g$\circ$f = $I_x$. Tomemos y $\in$ Y qualquer. Seja x = g(y). Da condição (i) acima, segue que f(x) = f(g(y)) = f$\circ$g(y) = $I_y$(y) = y. Então, f é sobrejetiva. Tomemos $x_1$, $x_2$ $\in$ X tais que $f(x_1) = f(x_2)$. Logo, g($f(x_1)$) = g($f(x_2)$), ou seja, g$\circ f(x_1)$ = g$\circ f(x_2)$. Da condição (ii), segue que $I_x(x_1)$ = $I_x(x_2)$, logo, $x_1 = x_2$. Então, f é injetiva, concluindo assim que f é bijetora.

($\Leftarrow$) Por hipótese, f é bijetiva. Desejamos construir uma função g : Y $\to$ X satisfazendo as condições (i) e (ii) da denição de função invertível. Dado y $\in$ Y qualquer, como f é sobrejetiva, existe x $\in$ X tal que f(x) = y e, como f é injetiva, o elemento x com esta propriedade é único. Assim, definimos g(y) como o único x $\in$ X tal que f(x) = y. Agora seja dado x $\in$ X. Temos que f(x) = y, para algum y $\in$ Y. Pela definição g(y) = x de g temos que assim (g$\circ f$)($x$) = g($f(x)$)= g(y) = x, ou seja g$\circ$f = $I_x$. Portanto f é invertível. $\square$

.

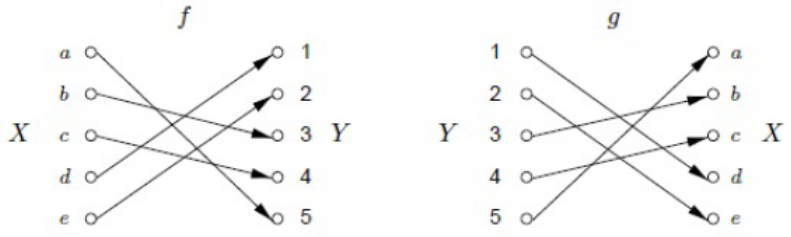



Figura 3.1.1: Uma bijeção de f e sua inversa g = $f^{-1}$.

*Observação* 7. A função g obtida na demonstração do teorema anterior de f é chamada a função inversa de f e é denotada por g = $f^{-1}$. Em criptografia a bijeções são utilizadas como ferramentas para encriptar mensagens e sua inversa para decriptar.

Permutações são funções que são utilizadas frequentemente em várias construções criptográficas. Apresentamos a seguir a definição de permutação.

**Definição 6.** Seja S um conjunto finito. Uma permutação p sobre S é uma bijeção de S sobre ele mesmo, ou seja, uma aplicação p : S $\to$ S que é uma bijeção.

**Definição 7.** Seja S um conjunto finito e seja f : S$\to$S uma bijeção. A função f é dita uma involução se f =$f^{-1}$. Equivalentemente podemos dizer que f é uma involução se f(f(x)) = x para todo x $\in$ S.

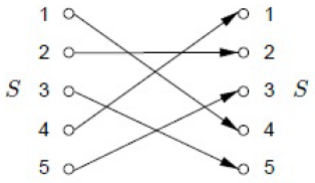



Figura 3.1.2: Uma involução sobre um conjunto S com 5 elementos.

## 3.2 Atividades que serão aplicadas.

O objetivo principal desta secção é buscar conteúdos que estimulem a curiosidade e que desencadeiem um melhor desempenho no processo de ensino e aprendizagem da Matemática. Dessa forma, a intenção de elaborar as atividades aqui propostas foi de aplicar o conhecimento obtido neste trabalho sobre criptografia, no ambiente escolar.

No ensino atual, a necessidade de contextualizar o que ensinamos tornou-se imprescindível frente a facilidade de acesso a todo tipo de informação que nossos alunos desfrutam, seja via internet, pela televisão ou por outro meio de comunicação. O ensino da matemática é, certamente, o mais questionado neste sentido, onde vários educadores se debruçam sobre o problema, propondo abordagens e atividades para preencher essa lacuna. No entanto, é comum encontrarmos contextos equivocados ou mau elaborados, onde a matemática é trabalhada da mesma forma como já é feito tradicionalmente, apenas sendo inserida em enredos infantis ou não condizentes com a realidade. Também é comum achar que contextualização e aplicação são sinônimos. Contextualizar a matemática e tentar colocar o conceito dentro de um enredo visando aproximá-lo de uma realidade concreta, o que nem sempre é viável. Aplicação da matemática é a utilização de técnicas matemáticas, geralmente avançadas, para resolver problemas ou modelar fenômenos relacionados à ciência e tecnologia. Portanto, aplicar matemática é para profissionais especializados. A matemática é a linguagem das Ciências e seu aprendizado é a base para o desenvolvimento do pensamento científico

e tecnológico de nossos estudantes, como já declarado pelo Filosofo Francês, Auguste Comte:

> "Toda a Educação Científica que não se inicia com a matemática é, naturalmente, imperfeita na sua base."

Nas próximas seções, estão propostas atividades dentro do enredo da criptografia, envolvendo o ensino de divisibilidade, funções, análise combinatória e matrizes para estudantes do Ensino Fundamental e Médio. Estas atividades foram elaboradas à luz da metodologia de Resolução de Problemas, visando superar o modelo da simples memorização dos conteúdos, o qual é insuficiente para atender aos anseios dos jovens estudantes de nossa sociedade contemporânea.

Em [19], POLYA argumenta que a resolução de problemas apresenta um conjunto de quatro fases: Compreender o problema; elaborar um plano ; executar o plano ; fazer a verificação. Os Parâmetros Curriculares Nacionais - Matemática [1, p. 43] indicam que no processo de ensino e aprendizagem, conceitos, ideias e métodos devem ser abordados mediante a exploração de problemas, ou seja, de situações em que os alunos precisem desenvolver algum tipo de estratégia para resolvê-las. Em [18], ONUCHIC afirma que fazer da compreensão o ponto central do ensino da Matemática deveria ser o objetivo de professores e de educadores em geral, aspecto que só vem a reforçar o próprio trabalho na perspectiva da solução de problemas, uma vez que este é um meio poderoso para promover compreensão. Neste sentido, as atividades visam atender um conjunto de competências e habilidades, conforme constam da matriz de referência do ENEM, que proporcionarão ao professor uma orientação didática atual.

No Ensino Fundamental teremos uma competência e algumas habilidades que serão mais exploradas. A competência 15 - Valorizar o trabalho em grupo, sendo capaz de ação crítica e cooperativa para a construção coletiva do conhecimento, a habilidade 44 - Elaborar, individualmente e em grupo, relatos orais e outras formas de registros acerca do tema em estudo, considerando informações obtidas por meio de observação, experimentação, textos ou outras fontes, a habilidade 45 - Confrontar as diferentes explicações individuais e coletivas, inclusive as de caráter histórico, para reelaborar suas ideias e interpretações, a

habilidade 46 - Elaborar perguntas e hipóteses, selecionando e organizando dados e ideias para resolver problemas e a habilidade 47 - Participar de debates coletivos para a solução de problemas, colocando suas ideias por escrito ou oralmente e reconsiderando sua opinião em face de evidências obtidas por diversas fontes de informação.

No entanto no Ensino Médio serão outros os parâmetros, também teremos uma competência e algumas habilidades que serão mais exploradas. A competência 5 - Analisar, argumentar e posicionar-se criticamente em relação a temas de ciência e tecnologia, a habilidade 19 - Identificar representações algébricas que expressem a relação entre grandezas, a habilidade 20 - Interpretar gráfico cartesiano que represente relações entre grandezas, a habilidade 21 - Resolver situação-problema cuja modelagem envolva conhecimentos algébricos, a habilidade 22 - Utilizar conhecimentos algébricos/geométricos como recurso para a construção de argumentação e a habilidade 23 - Avaliar propostas de intervenção na realidade utilizando conhecimentos algébricos.

Em cada atividade necessitarão de conhecimentos prévios, ou seja, se por algum motivo o aluno não absorveu esses conhecimentos a atividade será encarada com dificuldades. Dessa forma, ao perceber essas dificuldades o docente deverá dar uma atenção especial a esse aluno.

### 3.2.1 Ensino Fundamental.

Começaremos utilizando algumas atividades com ideias simples, para apresentar para o professor do Ensino Fundamental, como este poderá orientar seu aluno no trabalho com criptografia. Primeiramente incluiremos uma introdução contendo informações importantes para a aplicação das atividades, com o objetivo que os professores possam orientar seus alunos no manuseio do material disponível, apresentando o conhecimento matemático de uma forma mais atrativa.

#### 3.2.1.1 Atividade 1.

**Objetivo Geral.** Introduzir a criptografia em sala de aula como fator motivacional para verificar a aprendizagem dos alunos com respeito a comparação e substituição de símbolos conhecidos.

**Objetivo Específico.** Reconhecer uma chave código que pode ser utilizada para codificar e decodificar textos; Comparar as letras e os números que estão relacionados e fazer a substituição; Relacionar as várias formas de codificação e decodificação de mensagens.

**Público Alvo.** Estudantes do $6^{o}$ ano do Ensino Fundamental, segundo os Parâmetros Curriculares Nacionais (PCN).

**Pré-requisito.** Os alunos deverão saber númeração arábica, alfabeto arábico e somar números consecutivos.

**Materiais.** Os materiais utilizados nesta atividade são lápis, borracha, folha contendo a atividade e folha a parte para produção do disco de codificação.

**Recomendação Metodológica.** Esta atividade será aplicada em sala de aula ao final de números naturais. Os alunos responderão as atividades e, posteriormente, se reunirão em duplas para discutir os resultados obtidos. Ao término da discussão, o docente auxiliará os alunos para que os mesmos possam responder na lousa o que foi observado em todo este trabalho.

**Possíveis Continuações ou Desdobramentos.** O docente poderá associar este conteúdo com outros instrumentos já existentes que possam ser usados com a caracteristica de misturar letras ou números e como isso ter a capacidade de criar uma associação entre eles. E poderá associar este conteúdo ao programa disponível na internet [2]; e ajudar os alunos a utilizá-lo.

Podemos basear esta atividade na Subseção 2.1.3.3 que descreve o trabalho em um Disco de Alberti.

**Atividade:** O disco de Alberti é um método para codificar palavras que consiste em escolher um número de 1 a 26, chamado chave do código, e girar o disco interno do aparelho ilustrado na figura 3.2.1 até que essa chave corresponda à letra A. Depois disso, as letras da palavra são substituídas pelos números correspondentes, separados por tracinhos. Por exemplo, na figura abaixo a chave é 5 e a palavra PAI é codificada como 20-5-13.

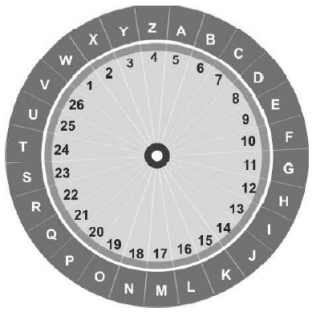



Figura 3.2.1: Chave de código circular.

(a) Usando a chave indicada na figura 3.2.1, descubra qual palavra foi codificada como 23-25-7-25-22-13.

(b) Codifique DECIFRE-ME usando a chave 20.

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

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

SOLUÇÕES e COMENTÁRIOS:

(a) SUCURI

(b) 24-25-23-3-26-12-25-7-25

(c) GATO

(d) n+n+1+n+2=52 $\rightarrow$ 3n=49, não existe n natural tal que isso seja verdade, logo nenhuma codificação vai gerar esta soma.

#### 3.2.1.2 Atividade 2.

**Objetivo Geral.** Introduzir a criptografia em sala de aula como fator motivacional para verificar a aprendizagem dos alunos com respeito a utilização de codificação com mais de uma ferramenta.

**Objetivo Específico.** Reconhecer as chaves código que poderão ser utilizadas para codificar e decodificar textos; Comparar as letras e os números que estão relacionados e fazer a substituição; Relacionar as várias formas de codificação e decodificação de mensagens.

**Público Alvo.** Estudantes do $7^{o}$ ano do Ensino Fundamental, segundo os Parâmetros Curriculares Nacionais (PCN).

**Pré-requisito.** Os alunos deverão saber númeração arábica, alfabeto arábico e utilizar tabelas de organização de dados.

**Materiais.** Os materiais utilizados nesta atividade são lápis, borracha e a folha contendo a atividade.

**Recomendação Metodológica.** Esta atividade será aplicada em sala de aula ao final da apresentação de números interiros. Os alunos responderão as atividades e, posteriormente, se reunirão em duplas para discutir os resultados obtidos. Ao término da discussão, o docente auxiliará os alunos para que os mesmos possam responder na lousa o que foi observado em todo este trabalho.

Podemos basear esta atividade no código de Vigenère, subsubseção 2.1.3.3, e na definção de congruência, subseção 3.1.1.

**Possíveis Continuações ou Desdobramentos.** O docente poderá associar este conteúdo com outros instrumentos já existentes que possam ser usados com a característica de observação de como uma sequência pode ser trabalhada com números e letras, tendo como finalidade apresentar um intervalo de repetição em sua codificação e decodificação.

Esta atividade tem como objetivo mostrar que a decodificação pode ser trabalhosa mais é um processo fácil de se entender.

**Atividade:** O código de Viginère é um método que necessita de uma chave que é uma palavra conhecida unicamente pela pessoa que transmitirá a mensagem e o receptor que conhecerá o seu teor. A chave pode ser uma palavra simples com poucas letras e de preferência com letras diferentes. Um exemplo que explica bem esta ferramenta esta na tabela 2.1.8.

(a) Utilize a chave "DIA" decodifique a frase, WMNKW R CRVHHKIPMNWW.

(b) Codifique DECIFRE-ME usando a chave DIA, isso te fornecerá os valores para os k's, $k_1$=3, $k_2$= 8 e $k_3$=0, como apresentado no exemplo na tabela 2.1.8.

(c) Francisco codificou uma palavra com a chave DIA, mas por descuido colocou no lugar do espaço uma letra qualquer ficando assim DBAFIRHIGRZA. Substituindo o espaço no local adquado, qual foi a mensagem que Francisco pretendia enviar?

SOLUÇÕES e COMENTÁRIOS:

(a) TENHO O CONHECIMENTO.

| PALAVRA CHAVE | D | I | A | D | I | A | D | I | A | D | I | A | D | I | A | D | I | A | D | I |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| TEXTO CODIFICADO | W | M | N | K | W | | R | | C | R | V | H | H | K | I | P | M | N | W | W |
| TEXTO DECODIFICADO | T | E | N | H | O | | O | | C | O | N | H | E | C | I | M | E | N | T | O |

Figura 3.2.2: Resposta utilizando tabela.

(b) GMCLNRH-MH.

| PALAVRA CHAVE | D | I | A | D | I | A | D | I | A | D |
|---|---|---|---|---|---|---|---|---|---|---|
| TEXTO ORIGINAL | D | E | C | I | F | R | E | | M | E |
| TEXTO CODIFICADO | G | M | C | L | N | R | H | | M | H |

Figura 3.2.3: Resposta utilizando tabela.

neste item poderemos fazer de forma fragmentada, verificando todas as letras que sofreram o mesmo deslocamento e ajusta-las no mesmo momento, como no caso das letras D, I e E, que estão ligadas ao D da palavra chave, estas letras sofreram um deslocamento de 3 casas, ficando com sua substituição nas letras G, L e H. Como estamos utilizando um exemplo simples não parece ser muito viável, mas se o texto fosse longo tanto para a codigicação como decodificação seria muito valida esta proposta.

(c) a mensagem decodificada foi "ATACAREAGORA" o que Francisco pretendia era "ATACAR AGORA".

#### 3.2.1.3 Atividade 3.

**Objetivo Geral.** Introduzir a criptografia em sala de aula como fator motivacional para verificar a aprendizagem dos alunos com respeito a organização de informações em tabelas.

**Objetivo Específico.** Reconhecer uma tabela e saber como organizá-la; associar letras e números e reorganizá-los; Retomar a ideia de diagramas por meio do esquema de flechas; Relacionar a tabela à várias sentenças de codificação e decodificação de mensagens.

**Público Alvo.** Estudantes do $8^{o}$ e $9^{o}$ anos do Ensino Fundamental, segundo os Parâmetros Curriculares Nacionais (PCN).

**Pré-requisito.** Os alunos deverão saber como criar uma tabela, sequência numérica, representar o esquema de flechas e cálcular a soma de números consecutivos.

**Materiais.** Os materiais utilizados nesta atividade são lápis, borracha e a folha contendo a atividade.

**Recomendação Metodológica.** Esta atividade será aplicada em sala de aula ao final da disciplina de estatística. Os alunos responderão as atividades e, posteriormente, se reunirão em duplas para discutir os resultados obtidos. Ao término da discussão, o docente auxiliará os alunos para que os mesmos possam responder na lousa o que foi observado em todo este trabalho.

**Possíveis Continuações ou Desdobramentos.** O docente poderá associar este conteúdo com outras formas de organizar tabelas com mais níveis e subníveis, basta ter cuidado na escolha da lei de formação destas, para isso poderá mudar os valores associados as letras desta atividade.

Vimos na subseção3.1.3, definição 3, que uma função é um terno constituído por elementos: domínio, contradomínio e lei de associação uma função também pode ser organizada na forma matricial como veremos a seguir, (lembrando que, como os alunos não viram esta matéria, pode-se apresentar o nome, mas não é necessária as propriedades pois ainda não serão usadas).

**Atividade:** Seja S = {1, 2, 3, 4, 5, 6, ..., 26}. Considere a permutação p : S→ S definida por p(1) = 6 ; p(2) = 5 ; p(3) = 4 ; p(4) = 2 ; p(5) = 3; p(6) =11 ; p(7) = 10 ; p(8) = 9 ; p(9) = 7 ; p(10) = 8 e assim sucessivamente, também representada pela forma de coordenadas , (1,6); (2,5); (3,4); (4,2); (5,3); (6,11); (7,10); (8,9); (9,7); (10,8) . A partir dessa permutação, estabelecemos a relação entre as letras e os números como na tabela a seguir. Nesse caso, dizemosque a permutação p é a chave da codificação.

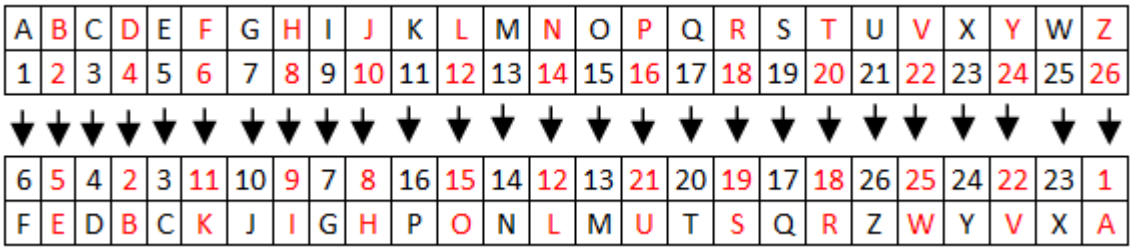



Figura 3.2.4: Figura com permutação entre números e letras

Considere a matriz $P = \begin{pmatrix} 4 & 21 & 16 & 12 & 1 \\ 2 & 26 & 21 & 15 & 6 \end{pmatrix}$. A primeira linha da matriz representa o Domínio, ou seja, os valores de entrada, $\begin{bmatrix} D & U & P & L & A \\ 4 & 21 & 16 & 12 & 1 \end{bmatrix}$ que neste caso é "DUPLA" e a segunda linha a Imagem p, ou seja, os valores que serão a resposta da codificação $\begin{bmatrix} 2 & 26 & 21 & 15 & 6 \\ B & Z & U & O & F \end{bmatrix}$ que neste caso é a palavra "BZUOF".

Como permutações são bijeções, elas possuem inversa. Se uma permutação for escrita na forma matricial, sua inversa é facilmente encontrada, basta trocar a posição das linhas da matriz. No exemplo acima, a inversa de P é dada por

$$P^{-1} = \begin{pmatrix} 2 & 26 & 21 & 15 & 6 \\ 4 & 21 & 16 & 12 & 1 \end{pmatrix}$$

e a partir dela, podemos reverter o processo, como indicado abaixo.

$$\begin{bmatrix} B & Z & U & O & F \end{bmatrix} \leftrightarrow \begin{bmatrix} 2 & 26 & 21 & 15 & 6 \end{bmatrix} \leftrightarrow$$
$$\leftrightarrow \begin{bmatrix} 4 & 21 & 16 & 12 & 1 \end{bmatrix} \leftrightarrow \begin{bmatrix} D & U & P & L & A \end{bmatrix}.$$

(a) Usando a chave indicada no conjunto S, apresente a matriz de codificação da palavra e depois decodifique a palavra USMWF .

(b) Codifique DECIFRE-ME usando a chave e apresente a matriz de codificação.

SOLUÇÕES e COMENTÁRIOS:

(a) $\left[\begin{array}{ccccc} U & S & M & W & F \end{array}\right] \leftrightarrow \left[\begin{array}{ccccc} 21 & 19 & 13 & 25 & 6 \end{array}\right] \leftrightarrow$

$\leftrightarrow \left[\begin{array}{ccccc} 16 & 18 & 15 & 22 & 1 \end{array}\right] \leftrightarrow \left[\begin{array}{ccccc} P & R & O & V & A \end{array}\right].$

(b) $\left[\begin{array}{cccccccccc} D & E & C & I & F & R & E & - & M & E \end{array}\right] \leftrightarrow \left[\begin{array}{cccccccccc} 4 & 5 & 3 & 9 & 6 & 18 & 5 & - & 13 & 5 \end{array}\right] \leftrightarrow$

$\leftrightarrow \left[\begin{array}{cccccccccc} 2 & 3 & 4 & 7 & 11 & 19 & 3 & - & 14 & 3 \end{array}\right] \leftrightarrow \left[\begin{array}{cccccccccc} B & C & D & G & K & S & C & - & N & C \end{array}\right].$

### 3.2.2 Ensino Médio.

Neste momento já estamos produzindo mais ferramentas que podem favorecer o entendimento e aprofundamento dessas ideias, buscamos então, mostrar o aperfeiçoamento das atividades do Ensino Fundamental contemplando alguns assuntos do currículo escolar do Ensino Médio, por exemplo, funções: polinomiais, modulares, exponenciais, logarítmicas e trigonometricas. Todas as atividades que forem propostas servirão também para as subsequentes. A criptografia vai trazer grande vantagem no aperfeiçoamento destas matérias, pois o aluno que aprender os princípios da criptografia, para a decodificação deve entender bem como é feita a inversa destas funções.

#### 3.2.2.1 Atividade 4.

**Objetivo Geral.** Introduzir a criptografia em sala de aula como fator motivacional para verificar a aprendizagem dos alunos com respeito a funções inversas.

**Objetivo Específico.** Reconhecer a função; Calcular o valor numérico de uma função e definir com clareza domínio e imagem; Retomar a ideia de diagramas por meio do esquema de flechas; Relacionar a função com à codificação e decodificação de mensagens.

**Público Alvo.** Estudantes da 1ª série do Ensino Médio, segundo os Parâmetros Curriculares Nacionais (PCN).

**Pré-requisito.** Os alunos deverão saber a definição de função constante e função do 1º grau; representação de funções por meio do esquema de flechas e cálculo do valor numérico para funções.

**Materiais.** Os materiais utilizados nesta atividade são lápis, borracha e a folha contendo a atividade.

**Recomendação Metodológica.** Esta atividade será aplicada em sala de aula ao final do conteúdo de funções definidas por várias sentenças. Os alunos responderão as atividades e, posteriormente, se reunirão em duplas para discutir os resultados obtidos. Ao término da discussão, o docente pode responder a atividade ou propor aos alunos que respondam na lousa.

**Possíveis Continuações ou Desdobramentos.** O docente poderá associar este conteúdo com outras funções estudadas na 1ª série do Ensino Médio, basta ter cuidado na escolha da lei de formação destas, para isso poderá mudar os valores associados as letras desta atividade.

**Atividade.** Luiz deseja enviar uma mensagem sigilosa para José, a qual deverá ser cifrada da seguinte maneira: Primeiramente cada letra por um número, conforme a tabela abaixo e em seguida aplicamos o número correspondente na função f(x) = 3x - 2, obtendo assim a mensagem cifrada. Por exemplo, a letra m corresponde ao número 13, que é transformado pela função em f(13) = 3.13 - 2 = 37, ou seja, a letra m e cifrada pelo número 37 (m $\mapsto$ 37).

| 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 | 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 |

Figura 3.2.5: Relação entre alfabeto e número.

RESPONDA:

conforme exemplo anterior,

1) CIFRE a mensagem aberta: O dolar vai subir.

2) DECIFRE a mensagem cifrada: 1-58-1-49-61-13-1-43-1- 37-1-40-22-13-7-13-52. Explicite a função utilizada para a decifrá-la.

3) Complete os espacos abaixo:

| LETRA | | TABELA | | CÓDIGO |
|---|---|---|---|---|
| A | → | 1 | → | 1 |
| E | → | 5 | → | |
| I | → | 9 | → | |
| O | → | | → | |
| U | → | | → | |
| | ← | 12 | → | |
| | ← | | ← | 49 |
| | ← | | ← | 64 |

Figura 3.2.6: Resposta da questão 3

4) Utilizando algumas cifras já calculados, complete a tabela abaixo e, em seguida, troque mensagens cifradas com um amigo.

| 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 | 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 |
| 1 | 4 | 7 | | 13 | | | | | | | | | | | | | | | | | | | | | |

Figura 3.2.7: Característica da codificação.

5) Identique o Domínio e a Imagem da função CIFRADORA e da função DECIFRADORA.

6) Se a função CIFRADORA fosse alterada para g(x) = 3x + 1, o que devemos mudar para que as informação da figura 3.2.3 para não alterarmos o código de cada letra ?

7) Considerando a possibilidade de mudança na tabela, como feito no item 6), e que a função CIFRADORA seja da forma f(x) = Ax+B, discuta sobre os possíveis valores para A e B.

SOLUÇÕES e COMENTÁRIOS:

1) Neste item o estudante irá consultar a tabela e determinar a imagem de alguns valores, obtendo a cifra das letras da mensagem. Ao montar a mensagem cifrada, fica explícita a ideia de transformação.

o corresponde ao 15 , f(15) = 43 , o $\longmapsto$ 43.

d corresponde ao 4 , f(4) = 10 , d $\longmapsto$ 10.

l corresponde ao 12 , f(12) = 34 , l $\longmapsto$ 34.

a corresponde ao 1 , f(1) = 1 , a $\longmapsto$ 1.

r corresponde ao 18 , f(18) = 52 , r $\longmapsto$ 52.

v corresponde ao 22 , f(22) = 64 , v $\longmapsto$ 64.

i corresponde ao 9 , f(9) = 25 , i $\longmapsto$ 25.

s corresponde ao 19 , f(19) = 55 , s $\longmapsto$ 55.

u corresponde ao 21 , f(21) = 61 , u $\longmapsto$ 61.

b corresponde ao 2 , f(2) = 4 , b $\longmapsto$ 4.

A mensagem codicadaca: 43 - 10 - 43 - 34 - 1 - 52 - 64 - 1 - 25 - 55 - 61 - 4 - 25 - 52.

2) Neste item, naturalmente a maioria dos estudantes fará tentativas utilizando alguns códigos já encontrados no item 1 e conjecturando a respeito dos demais. Porém, é necessário que o professor induza os estudantes a determinar e aplicar a função inversa. Neste momento não há necessidade de enfatizar as condições para obter a inversa, pois a função escolhida deve ser bijetora. A necessidade que a função seja bijetora para obter a sua inversa será abordada na atividade 5. Novamente fica explícita a ideia de transformação.

A função inversa é $y = \frac{x+2}{3}$ e

$1 \longmapsto$ a ; $58 \longmapsto$ t ; $49 \longmapsto$ q ; $61 \longmapsto$ u ; $13 \longmapsto$ e ; $43 \longmapsto$ o $37 \longmapsto$ m ; $40 \longmapsto$ n ; $22 \longmapsto$ h ; $7 \longmapsto$ c ; $52 \longmapsto$ r

Portanto, a mensagem aberta é ATAQUE AO AMANHECER.

3) Neste item, a visualização das transformações, direta e inversa, ficam explicitadas de forma mais concreta.

| LETRA | | TABELA | | CÓDIGO |
|---|---|---|---|---|
| A | → | 1 | → | 1 |
| E | → | 5 | → | 13 |
| I | → | 9 | → | 25 |
| O | → | 15 | → | 43 |
| U | → | | → | 61 |
| L | ← | 12 | → | 34 |
| Q | ← | 17 | ← | 49 |
| V | ← | | ← | 64 |

Figura 3.2.8: Figura com a questão 3 completa.

4) Ao preencher a tabela, espera-se que os estudantes percebam algumas propriedades da sequência de cifras geradas pela função afim, principalmente que são números em sequência que deixam resto 1 quando divididos por 3, o que ajudará na resolução dos próximos itens. É importante que o professor induza os estudantes a esta percepção. É bem interessante fazer com que os estudantes troquem mensagens com outros, da mesma sala ou não, utilizando a técnica vista e criando suas próprias chaves. A troca dessas mensagens via telefone celular, em ambientes onde o uso seja acessível a todos, e algo que costuma motivar a atividade.

| 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 | 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 |
| 1 | 4 | 7 | 10 | 13 | 16 | 19 | 22 | 25 | 28 | 31 | 34 | 37 | 40 | 43 | 46 | 49 | 52 | 55 | 58 | 61 | 64 | 67 | 70 | 73 | 76 |

Figura 3.2.9: Tabela com todas as suas codificações.

5) Neste item, num primeiro momento peça apenas que os estudantes identiquem o domínio da função cifradora, {1, 2, 3, ..., 26}, a sua imagem, {1, 4, 7, 10, ..., 76} e que percebam que o domínio da função decifradora é a imagem da função cifradora e que sua imagem é igual ao domínio da função cifradora. Depois peça para que eles representem esses conjuntos por uma característica comum de seus elementos e faça {1, 2, 3, ..., 26} = {x ∈ Z | 1≤ x ≤ 26} como exemplo. Ao representarem o conjunto imagem, geralmente por {3x - 2 ∈ Z | 1≤ x ≤ 26}, mostre que existem outras possibilidades, como {3x + 1 ∈ Z | 0 ≤ x ≤ 25}, o que já indicará o que fazer no item 6). Também é interessante mostrar aos estudantes a representação formal das funções, f : A → B , definida por f(x) = 3x - 2, enfatizando que ao mudar o domínio e o contradomínio, constroí-se uma nova função (transformação).

6) Neste item, o estudante pode recorrer ao item 5 e responderá com suas palavras, que basta fazer o x variar de 0 a 25. É muito importante que o professor enfatize que a mudança na lei de formação e no Domínio da função, vai gerar uma nova função mas que executa o mesmo tipo de transformação.

7) Nesta discussão, mediada pelo professor, é importante que se conclua que existem várias formas de representação de números inteiros que deixam resto 1 quando divididos por 3, o que levará a conclusão de que A = 3 e que B é qualquer número inteiro que deixa resto 1 quando dividido por 3. Escreva no quadro várias destas formas. Pode-se também, em caráter apenas ilustrativo, mostrar que existe uma forma de representação dessa família de números, que é B ≡1 (mod 3).

#### 3.2.2.2 Atividade 5.

**Objetivo Geral.** Reconhecer a função; Calcular o valor numérico de uma função e definir com clareza domínio e imagem; Relacionar a função com à codificação e decodificação de mensagens.

**Objetivo Específico.** Reconhecer uma matriz definir algumas de suas propriedades; Calcular utilizando as propriedades matriciais para produzir a palavra codificada; Retomar a ideia de diagramas por meio do esquema de flechas; Relacionar a matriz com outras sentenças da codificação e decodificação das mensagens.

**Público Alvo.** Estudantes da 2ª série do Ensino Médio, segundo os Parâmetros Curriculares Nacionais (PCN).

**Pré-requisito.** Os alunos deverão saber a definição de função constante e função do 1º grau e cálculo do valor numérico para funções definidas por várias sentenças.

**Materiais.** Os materiais utilizados nesta atividade são lápis, borracha e a folha contendo a atividade.

**Recomendação Metodológica.** Esta atividade será aplicada em sala de aula ao final do conteúdo de funções. Os alunos responderão as atividades e, posteriormente, se reunirão em duplas para discutir os resultados obtidos. Ao término da discussão, o docente pode responder a atividade ou propor aos alunos que respondam na lousa.

**Possíveis Continuações ou Desdobramentos.** O docente poderá associar este conteúdo com outros conteúdos como funções estudadas na 1ª série do Ensino Médio, basta ter cuidado na escolha da lei de formação destas.

**Atividade.** Para enviar uma mensagem sigilosa, José substitui as letras da mensagem aberta por números, conforme a tabela a seguir e transforma esses números aplicando-os na função cifradora $f(x) = x^2 - 8x + 17$.

| 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 | 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 |

Figura 3.2.10: Relação entre alfabeto e número.

RESPONDA:

1) CIFRE a palavra MATEMÁTICA.

2) DECIFRE a mensagem cifrada: 5 - 10 - 5 - 197 - 26 - 2 - 10 - 1 - 2 - 5 - 10 - 2 - 10.

3) Explique porque a utilização da função f não foi uma boa escolha para a função cifradora.

4) Construa o gráfico que reprenta a função $f : R \to R$ definida por $f(x) = x^2 - 8x + 17$.

5) O que pode ser feito para deixar a função f em condições de ser utilizada como função cifradora? Qual a característica dessa função?

SOLUÇÕES E COMENTÁRIOS

1) De forma análoga ao item 1 da atividade 5, ao montar a mensagem cifrada, fica explícita a ideia de transformação. É importante observar que as letras E e C possuem a mesma cifra, 2. O desejável é que algum grupo faça esta observação. Caso isto não ocorra, o professor deve direcionar os estudantes a observarem este fato.

M corresponde ao 13 , f(13) = 82 , M $\mapsto$ 82.

A corresponde ao 1 , f(1) = 10 , A $\mapsto$ 10.

T corresponde ao 20 , f(20) = 257 , T $\mapsto$ 257.

E corresponde ao 5 , f(5) = 2 , E $\mapsto$ 2.

I corresponde ao 9 , f(9) = 26 , I $\mapsto$ 26.

C correspondeao 3 , f(3) = 3 , C $\mapsto$ 2.

A mensagem cifrada fica 82 - 10 - 257 - 2 - 82 - 10 - 257 - 26 - 2 - 82.

2) Neste item, os estudantes necessitarão determinar a função inversa. Para isso, caberá ao professor rever a técnica de completar o quadrado para fatorar o polinômio, que consiste de uma técnica importante e bastante utilizada nas disciplinas de Cálculo e Geometria Analítica. Apresentamos a seguir o cálculo da inversa de f, utilizando a técnica de completar quadrado.

$y = x^2 - 8x + 17 \Rightarrow y - 1 = (x-4)^2 \Rightarrow x = 4 \pm \sqrt{y-1}$ com $y \geq 1$.

Temos então que a função decodificadora é $f^{-1}(x) = 4 + \sqrt{x-1}$,ou $f^{-1}(x) = 4 - \sqrt{x-1}$, com $x \geq 1$. Apesar da importância em observar que $x \geq 1$, ressalta-se que esta condição se cumpre naturalmente.

Ao aplicar a mensagem cifrada na função decifradora, apresentada anteriormente, obtém-se o seguinte:

$$5 \begin{matrix} \mapsto 6 \mapsto F \\ \mapsto 2 \mapsto B \end{matrix} ; 10 \begin{matrix} \mapsto 7 \mapsto G \\ \mapsto 1 \mapsto A \end{matrix} ; 197 \begin{matrix} \mapsto \ 18 \mapsto \ R \\ \mapsto -10 \mapsto \notin D_{f^{-1}} \end{matrix} ; 26 \begin{matrix} \mapsto 9 \mapsto F \\ \mapsto -1 \mapsto \notin D_{f^{-1}} \end{matrix} ;$$

$$2 \begin{matrix} \mapsto 5 \mapsto E \\ \mapsto 3 \mapsto C \end{matrix} ; 1 \mapsto 4 \mapsto D.$$

Nesta situação, o estudante terá que fazer algumas tentativas para chegar à mensagem FÁBRICA DE FACA. Deve-se ressaltar que num texto longo, tal tarefa pode ser exaustiva, comprometendo a simplicidade do algoritmo.

3) Neste item a resposta é livre, porém deve-se enfatizar a importância de que letras diferentes tenham cifras distintas. Insere-se neste momento a ideia de bijeção como condição suciente para a escolha da função cifradora.

4)

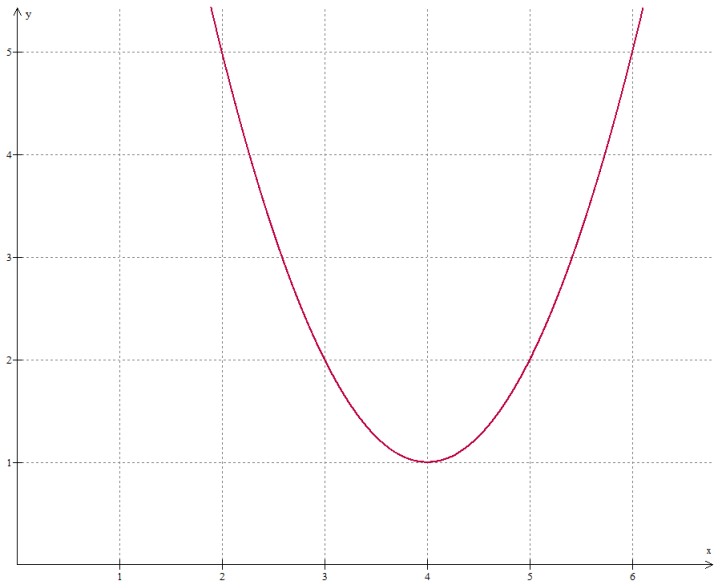



Figura 3.2.11: Gráfico da função quadrática

5) Neste item pretende-se que os estudantes observem que para tornar uma função quadrática bijetora, basta tomar como domínio um subconjunto de $[x_v, +\infty[$ (ou, analogamente, $]-\infty, x_v]$) e, para contradomínio, o correspondente subconjunto de $[y_v, +\infty[$ (ou de $]-\infty, y_v]$). Para melhor compreensão deste fato, pode-se ilustrar com um gráfico.

#### 3.2.2.3 Atividade 6.

**Objetivo Geral.** Explora o conceito de bijeção como condição necessária e suficiente para a inversão de uma função.

**Objetivo Específico.** Reconhecer uma função definir algumas de suas propriedades.

**Público Alvo.** Estudantes da 1ª série do Ensino Médio, segundo os Parâmetros Curriculares Nacionais (PCN).

**Pré-requisito.** Os alunos deverão saber a definição de funções.

**Materiais.** Os materiais utilizados nesta atividade são lápis, borracha e a folha contendo a atividade.

**Recomendação Metodológica.** Esta atividade será aplicada em sala de aula ao final do conteúdo de funções definidas por várias sentenças. Os alunos responderão as atividades e, posteriormente, se reunirão em duplas para discutir os resultados obtidos. Ao término da discussão, o docente pode responder a atividade ou propor aos alunos que respondam na lousa.

**Possíveis Continuações ou Desdobramentos.** O docente poderá apresentar todo o conteúdo de funções e seus conceitos estudados na 1ª série do Ensino Médio, basta ter cuidado na escolha da lei de formação destas.

**Detalhes da Atividade.** Para cada uma das funções cifradoras abaixo, estipule valores para as letras do alfabeto e determine a função decifradora.

| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $f_1(x) = -3x + 5$ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| $f_1^{-1}(x) =$ | | | | | | | | | | | | | | | | | | | | | | | | | | |

Figura 3.2.12: Função do primeiro grau.

COMENTÁRIO: Neste item basta observar que, por se tratar de uma função afim, qualquer valor distinto estipulado para as letras do alfabeto estabelece uma bijeção. A determinação da função decifradora é simples.

| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $f_2(x) = 2x^2 - 3x + 1$ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| $f_2^{-1}(x) =$ | | | | | | | | | | | | | | | | | | | | | | | | | | |

Figura 3.2.13: Função do segundo grau.

COMENTÁRIO: A função utilizada para decifrar as mensagens é obtida completando quadrado.

| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $f_3(x) = x^2 + 6x - 2$ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| $f_3^{-1}(x) =$ | | | | | | | | | | | | | | | | | | | | | | | | | | |

Figura 3.2.14: Função do segundo grau.

COMENTÁRIO: É necessário estipular um valor para as letras do alfabeto valores

maiores ou iguais ao valor de $x_v$, ou ainda valores menores ou iguais ao valor de $x_v$ para que se estabeleça uma bijeção. A determinação da função decifradora se obtém completando quadrado.

| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $f_4(x) = \lvert x-4 \rvert$ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| $f_4^{-1}(x) =$ | | | | | | | | | | | | | | | | | | | | | | | | | | |

Figura 3.2.15: Função modular.

COMENTÁRIO: Neste item, deve-se sugerir aos estudantes que façam uma análise do gráfico. O professor, a partir daí, pode explorar mais detalhes das funções modulares, como por exemplo, o gráfico desta função.

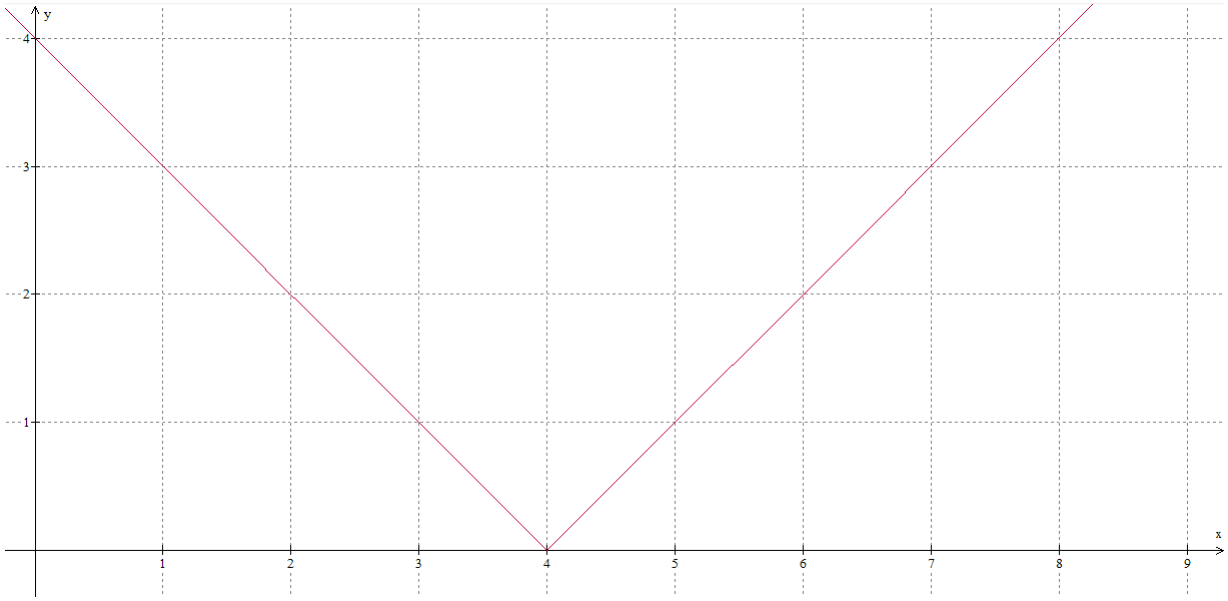



Figura 3.2.16: Grafico da função modular.

| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $f_5(x) = \lvert x^2 - 4x - 5 \rvert$ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| $f_5^{-1}(x) =$ | | | | | | | | | | | | | | | | | | | | | | | | | | |

Figura 3.2.17: Função modular.

COMENTÁRIO: Neste item, deve-se sugerir aos estudantes que façam uma análise do gráfico.

| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $f_6(x) = 3^{x+1}$ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| $f_6^{-1}(x) =$ | | | | | | | | | | | | | | | | | | | | | | | | | | |

Figura 3.2.18: Função exponencial.

COMENTÁRIO: Neste item, deve-se sugerir aos estudantes que façam uma análise do gráfico. O professor, a partir daí, pode explorar mais detalhes das funções exponenciais, que é a inversa de uma função logarítmica.

| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $f_7(x) = \log_5(x+3)$ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| $f_7^{-1}(x) =$ | | | | | | | | | | | | | | | | | | | | | | | | | | |

Figura 3.2.19: Função logaritmica.

COMENTÁRIO: Neste item, deve-se sugerir aos estudantes que façam uma análise do gráfico. O professor, a partir daí, pode explorar mais detalhes das funções logarítmicas, que é a inversa de uma função exponencial.

#### 3.2.2.4 Atividade 7. [11]

**Objetivo Geral.** Introduzir a criptografia em sala de aula como fator motivacional para verificar a aprendizagem dos alunos a respeito de matrizes e algumas de suas propriedades.

**Objetivo Específico.** Reconhecer uma matriz; Definir algumas de suas propriedades; Utilizando as propriedades matriciais produzir a palavra codificada; Relacionar a matriz com outras sentenças da codificação e decodificação da mensagens.

**Público Alvo.** Estudantes da 2ª série do Ensino Médio, segundo os Parâmetros Curriculares Nacionais (PCN).

**Pré-requisito.** Os alunos deverão saber a definição de matrizes e algumas de suas propriedades, uma delas a multiplicação de matrizes.

**Materiais.** Os materiais utilizados nesta atividade são lápis, borracha e a folha contendo a atividade.

**Recomendação Metodológica.** Esta atividade será aplicada em sala de aula ao final do conteúdo de funções definidas por várias sentenças. Os alunos responderão as atividades e, posteriormente, se reunirão em duplas para discutir os resultados obtidos. Ao término da discussão, o docente pode responder a atividade ou propor aos alunos que respondam na lousa.

**Exemplo 8.** Para codificar uma mensagem usando este método é necessário que, primeiramente, cada letra do nosso alfabeto e símbolos desejados sejam associados a vetores 2 x 1. A seguir, apresentamos uma tabela com um exemplo para essa associação.

| A | B | C | D | E | F | G | H | I | J |
|---|---|---|---|---|---|---|---|---|---|
| $\begin{pmatrix}0\\0\end{pmatrix}$ | $\begin{pmatrix}1\\0\end{pmatrix}$ | $\begin{pmatrix}2\\0\end{pmatrix}$ | $\begin{pmatrix}3\\0\end{pmatrix}$ | $\begin{pmatrix}4\\0\end{pmatrix}$ | $\begin{pmatrix}0\\1\end{pmatrix}$ | $\begin{pmatrix}1\\1\end{pmatrix}$ | $\begin{pmatrix}2\\1\end{pmatrix}$ | $\begin{pmatrix}3\\1\end{pmatrix}$ | $\begin{pmatrix}4\\1\end{pmatrix}$ |

| K | L | M | N | O | P | Q | R | S | T |
|---|---|---|---|---|---|---|---|---|---|
| $\begin{pmatrix}0\\2\end{pmatrix}$ | $\begin{pmatrix}1\\2\end{pmatrix}$ | $\begin{pmatrix}2\\2\end{pmatrix}$ | $\begin{pmatrix}3\\2\end{pmatrix}$ | $\begin{pmatrix}4\\2\end{pmatrix}$ | $\begin{pmatrix}0\\3\end{pmatrix}$ | $\begin{pmatrix}1\\3\end{pmatrix}$ | $\begin{pmatrix}2\\3\end{pmatrix}$ | $\begin{pmatrix}3\\3\end{pmatrix}$ | $\begin{pmatrix}4\\3\end{pmatrix}$ |

| U | V | W | X | Y | Z | espaço | . | , | ? |
|---|---|---|---|---|---|---|---|---|---|
| $\begin{pmatrix}0\\4\end{pmatrix}$ | $\begin{pmatrix}1\\4\end{pmatrix}$ | $\begin{pmatrix}2\\4\end{pmatrix}$ | $\begin{pmatrix}3\\4\end{pmatrix}$ | $\begin{pmatrix}4\\4\end{pmatrix}$ | $\begin{pmatrix}0\\5\end{pmatrix}$ | $\begin{pmatrix}1\\5\end{pmatrix}$ | $\begin{pmatrix}2\\5\end{pmatrix}$ | $\begin{pmatrix}3\\5\end{pmatrix}$ | $\begin{pmatrix}4\\5\end{pmatrix}$ |

Tabela 3.2.1: Exemplo de associação de letras e vetores.

Podemos representar esses vetores como pontos de um plano, como mostra a figura 3.2.20 a seguir:

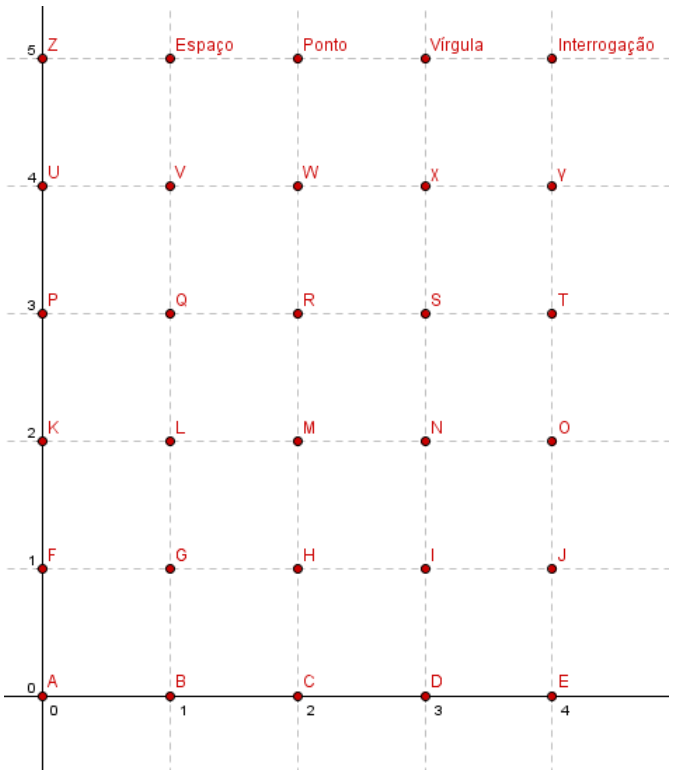



Figura 3.2.20: Representação dos pontos em coordenadas.

Decidida qual associação usar, construímos uma matriz M de apenas 2 linhas e codificamos uma mensagem. Para isso, basta colocar os vetores que representam as letras da mensagem um na frente do outro. Vamos, apresentar exemplo a seguir exemplo.

**Exemplo 9.** Para colocar a mensagem "BOA AULA." em uma matriz, usando a associação da tabela 3.2.1, escrevemos:

$$M = (BOA\,AULA.).$$

Substituindo pelo vetor associado temos

$$M = \begin{pmatrix} 1 & 4 & 0 & 1 & 0 & 0 & 1 & 0 & 2 \\ 0 & 2 & 0 & 5 & 0 & 4 & 2 & 0 & 5 \end{pmatrix}.$$

Agora, criamos uma matriz 2 x 2 para usar como chave. Ela deve ser invertível para garantir que a mensagem poderá ser decodificada. Podemos usar, por exemplo, a matriz C mostrada a seguir:

$$C = (GL).$$

$$C = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Por fim, criptografamos a mensagem M, transformando-a em uma matriz M' . Para isso, devemos fazer a multiplicação C. M. Usando o exemplo de mensagem, temos:

$$M' = C.M = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 4 & 0 & 1 & 0 & 0 & 1 & 0 & 2 \\ 0 & 2 & 0 & 5 & 0 & 4 & 2 & 0 & 5 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 6 & 0 & 6 & 0 & 4 & 3 & 0 & 7 \\ 1 & 8 & 0 & 11 & 0 & 8 & 5 & 0 & 12 \end{pmatrix}.$$

$$M' = \begin{pmatrix} 1 & 6 & 0 & 6 & 0 & 4 & 3 & 0 & 7 \\ 1 & 8 & 0 & 11 & 0 & 8 & 5 & 0 & 12 \end{pmatrix}.$$

Podendo apresentar o resultado da palavra como 1-1-6-8-0-0-6-11-0-0-4-8-3-5-0-0-7-12.

*Observação* 8. Deixar os alunos pensarem bastante antes de dizer que para decodificar a mensagem basta encontrar a matriz inversa de C e multiplicar por M' pois

$$M = (C^{-1}.C).M$$

$$= C^{-1}.(C.M)$$

$$= C^{-1}.M'$$

Vejamos no exemplo a seguir um outro método que podemos utilizar onde substituír cada letra por um número como na tabela 3.2.10.

**Exemplo 10.** Codificando a palavra MATEMÁTICA utilizando a tabela 3.2.10, ficaria 13-1-20-5-13-1-20-9-3-1. Lembrando que a palavra não esta em forma matricial, deverá ser organizada matricialmente completando as colunas da esquerda para direta de cima para baixo. ficando assim com a matriz,

$$M = \begin{pmatrix} 13 & 20 & 13 & 20 & 3 \\ 1 & 5 & 1 & 9 & 1 \end{pmatrix}.$$

Agora que foram apresentados alguns exemplo para os alunos, entendemos que já sabem criptografar uma mensagem, assim devem praticar. Nesta etapa, cada grupo deverá inventar uma frase com no máximo 20 caracteres e codificá-la.

**Atividade.** De acordo com os Exemplos (colocar os números), faça o que se pede. Utilize a chave $A = \begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix}$.

1) Cifre a palavra MATEMÁTICA utilizando a forma apresentada no Exemplo.

2) Decifre o texto cifrado (42 - 57 - 50 - 57 - 70 - 65 - 50 - 61 - 14 - 19 - 20 - 12) utilizando a forma do Exemplo.

3) Usando a chave OI referente à pela tabela 3.2.1, descubra qual palavra foi codificada sabendo que $M' = \begin{bmatrix} 4 & 22 & 14 & 19 & 25 & 17 & 0 & 4 & 0 & 10 & 11 & 22 \\ 2 & 10 & 6 & 7 & 11 & 7 & 0 & 2 & 0 & 4 & 5 & 10 \end{bmatrix}$.

*Observação* 9. Em seguida, os alunos poderão trocar mensagens com outro grupo, sempre fornecendo apenas a matriz codificada (M') e a chave (C). O desafio é decifrar a mensagem do outro grupo, utilizando uma das duas técnicas. Fazendo isso, eles estarão fixando conteúdos como multiplicação e inversão de matrizes de um modo mais atrativo.

SOLUÇÕES e COMENTÁRIOS:

1) Como M corresponde ao 13 , A corresponde ao 1 , T corresponde ao 20 , E corresponde ao 5 , I corresponde ao 9 e C corresponde ao 3 , temos

$$C = \begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix} . \begin{pmatrix} 13 & 20 & 13 & 20 & 3 \\ 1 & 5 & 1 & 9 & 1 \end{pmatrix} = \begin{pmatrix} 28 & 50 & 28 & 58 & 8 \\ 16 & 35 & 16 & 47 & 6 \end{pmatrix}.$$

Logo, o texto cifrado e (28 - 16 - 50 - 35 - 28 - 16 - 58 - 47 - 8 - 6).

2) Para decifrar o texto, utilizamos as propriedades da matriz invertível. Sabendo que C = A.M, sendo C a mensagem criptografada, A a chave e M a mensagem original, temos que

$$\text{C} = \text{A.M} \Rightarrow A^{-1}.\text{A.M} = A^{-1}.\text{C} \Rightarrow \text{M} = A^{-1}.\text{C}$$

ou seja, para decifrar a mensagem multiplica-se a matriz inversa de A à esquerda da matriz C.

*Observação* 10. A inversa de uma matriz $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de ordem 2, é dada por

$$B^{-1} = \frac{1}{detB} . \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

De fato, como $B^{-1}.B = I$, temos que $\begin{pmatrix} a & b \\ c & d \end{pmatrix} . \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, que gera o seguinte sistema:

$$\begin{cases} ax + bz = 1 \\ ay + bw = 0 \\ cx + dz = 0 \\ cy + dw = 1 \end{cases}$$

cuja a solução é (x, y, z, w), sendo $x = \frac{d}{ad-bc} = \frac{1}{detB}.d$; $y = \frac{-b}{ad-bc} = \frac{1}{detB}.(-b)$; $z = \frac{-c}{ad-bc} = \frac{1}{detB}.(-c)$; $w = \frac{a}{ad-bc} = \frac{1}{detB}.a$.

Logo $B^{-1} = \frac{1}{detB}. \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Aplicando o resultado ao problema, temos que detA = 4 e, assim,

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

Logo,

$$M = \begin{pmatrix} \frac{3}{4} & -\frac{1}{2} \\ -\frac{1}{4} & \frac{1}{2} \end{pmatrix} . \begin{pmatrix} 42 & 50 & 70 & 50 & 14 & 20 \\ 57 & 57 & 65 & 61 & 19 & 12 \end{pmatrix} = \begin{pmatrix} 3 & 9 & 20 & 7 & 1 & 9 \\ 18 & 16 & 15 & 18 & 6 & 1 \end{pmatrix},$$

o que gera o texto aberto CRIPTOGRAFIA.

3) Temos que a chave é $OI = \begin{bmatrix} 4 & 3 \\ 2 & 1 \end{bmatrix}$. Assim, $A = \begin{pmatrix} \frac{3}{4} & -\frac{1}{2} \\ -\frac{1}{4} & \frac{1}{2} \end{pmatrix}$.Logo, M = $A^{-1}$.M'= $\begin{bmatrix} 1 & 4 & 2 & 1 & 4 & 2 & 0 & 1 & 0 & 1 & 2 & 4 \\ 0 & 2 & 2 & 5 & 3 & 3 & 0 & 0 & 0 & 2 & 1 & 2 \end{bmatrix}$ que relata o texto

$[BOM\,TRABALHO]$.

#### 3.2.2.5 Atividade 8.

**Objetivo Geral.** Explora o Princípio das gavetas de Dirichlet.

**Objetivo Especifico.** Reconhecer problemas que necessitem de análise combinatória; Contar o número símbolos que poderam ser usados; Relacionar a análise combinatória na codificação e decodificação de mensagens.

**Público Alvo.** Estudantes da 2ª série do Ensino Médio, segundo os Parâmetros Curriculares Nacionais (PCN).

**Pré-requisito.** Os alunos deverão saber a definição de análise combinatória e cálculo do princípio fundamental da contagem.

**Materiais.** Os materiais utilizados nesta atividade são lápis, borracha e a folha contendo a atividade.

**Recomendação Metodológica.** Esta atividade será aplicada em sala de aula ao final do conteúdo de funções definidas por várias sentenças. Os alunos responderão as atividades e, posteriormente, se reunirão em duplas para discutir os resultados obtidos. Ao término da discussão, o docente pode responder a atividade ou propor aos alunos que respondam na lousa.

**Possíveis Continuações ou Desdobramentos.** O docente poderá associar este conteúdo com outros e se julgar interessante poderá usar funções estudadas na 1ª série do Ensino Médio, basta ter cuidado na escolha da lei de formação destas, para isso poderá mudar os valores associados as letras desta atividade.

**Atividade.** O texto abaixo, de autoria do Filosofo Francês Auguste Comte, será criptografado utilizando-se a cifra de Vigenère com a palavra chave CIFRA.

> "Toda a Educação Científica que não se inicia com a matemática é, naturalmente, imperfeita na sua base."

Mostre que a letra "e" será cifrada pelo menos 3 vezes com a mesma cifra.

SOLUÇÕES e COMENTÁRIOS:

Podemos encontrar em [21] o seguinte princípio:

**Princípio das gavetas de Dirichlet**: Se n objetos forem colocados em no máximo (n - 1) gavetas, então pelo menos uma delas conterá pelo menos dois objetos.

Considerando que no texto a letra "e" aparece 11 vezes e que a palavra chave, que define o alfabeto permutado que será utilizado, possui 5 letras, pode-se concluir, pelo Princípio das gavetas de Dirichlet, que ao colocar 11 objetos em 5 gavetas, pelo menos uma gaveta conterá pelo menos 3 objetos. Portanto, no texto a letra "e" será cifrada pelo menos 3 vezes pela mesma cifra.

#### 3.2.2.6 Atividade 9.

**Objetivo Geral.** Introduzir a criptografia em sala de aula como fator motivacional para verificar a aprendizagem dos alunos com respeito a análise combinatória.

**Objetivo Específico.** Reconhecer problemas que necessitem de análise combinatória; Contar o número símbolos que poderam ser usados; Relacionar a análise combinatória na codificação e decodificação de mensagens.

**Público Alvo.** Estudantes da 2ª série do Ensino Médio, segundo os Parâmetros Curriculares Nacionais (PCN).

**Pré-requisito.** Os alunos deverão saber a definição de análise combinatória e cálculo do princípio fundamental da contagem.

**Materiais.** Os materiais utilizados nesta atividade são lápis, borracha e a folha contendo a atividade.

**Recomendação Metodológica.** Esta atividade será aplicada em sala de aula ao final do conteúdo de funções definidas por várias sentenças. Os alunos responderão as atividades e, posteriormente, se reunirão em duplas para discutir os resultados obtidos. Ao término da discussão, o docente pode responder a atividade ou propor aos alunos que respondam na lousa.

**Possíveis Continuações ou Desdobramentos.** O docente poderá associar este conteúdo com outros e se julgarem interessante poderam usar funções estudadas na 1ª série do Ensino Médio, basta ter cuidado na escolha da lei de formação destas, para isso poderá mudar os valores associados as letras desta atividade.

**Atividade.** Digamos que no planeta Plunct os alfabetos fossem formados por apenas três símbolos:

★ ♦ *e* ■.

| | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 1 | 2 | 3 | 1 | 2 | 3 | 1 | 2 | 3 | 1 | 2 | 3 | 1 | 2 | 3 | 1 | 2 | 3 |
| ★ | ♦ | ■ | ★ | ♦ | ■ | ★ | ♦ | ■ | ★ | ♦ | ■ | ★ | ♦ | ■ | ★ | ♦ | ■ | ★ | ♦ | ■ |
| 1 | 2 | 3 | 1 | 2 | 3 | 1 | 2 | 3 | 1 | 2 | 3 | 1 | 2 | 3 | 1 | 2 | 3 | 1 | 2 | 3 |
| ★ | ♦ | ■ | ■ | ★ | ♦ | ♦ | ■ | ★ | ★ | ■ | ♦ | ■ | ♦ | ★ | ♦ | ★ | ■ |

Tabela 3.2.2: Maneiras de permutar.

Poderíamos criptografar mensagens de seis maneiras diferentes:

A primeira dessas maneiras é a "trivial" pois é aquela em que cada símbolo é representado por ele mesmo e não serve para codificar nada. Sem listar as mensagens, poderíamos concluir que existem seis maneiras diferentes de permutar as letras deste alfabeto? É claro que sim: para a primeira letra existem 3 possibilidades de codificação, para a segunda apenas duas e para a terceira resta somente uma possibilidade. Pelo Princípio Multiplicativo da Contagem, são $3 \cdot 2 \cdot 1 = 6$ as possibilidades .

São três as possibilidades que mantém a "ordem usual" ★ → ♦ → ■ → ★ (1→2→3→1) inalterada, isso ocorre quando observamos os três primeiro exemplos da tabela 3.2.2.

Tentando criar uma forma de representação da comunicação entre os habitantes do planeta Plunct com a nossa espécie foi criado uma outra representação. Organizamos a tabela 3.2.2 com o seguinte princípio, para cada seis símbolos que gere uma tabela será associada uma letra. A primeira é associada ao F, a segunda ao O, a terceira ao C, a quata ao A, a quinta ao B e a sexta ao L,por exemplo, a forma de representar o F é ★♦■★♦■, podendo assim criar algumas palavras.

(a) utilizando a associação dada acima, qual a palavra que é representada pelos símbolos a seguir?

★♦■★♦■★♦■■★♦★♦■♦■★★♦■★■♦.

(b) Como ficará a codificação da palavra "BOLA".

(c) Qual outras palavras podem ser feitas utilizando este critério de montagem? E como ficariam com os símbolos de planeta Plunct?

SOLUÇÕES e COMENTÁRIOS:

(a) Se for agrupada de seis em seis elementos perceberemos que a palavra que esta codificada é "FOCA".

(b) ★♦■■♦★★♦■■★♦★♦■♦★■★♦■★■♦.

(c) Esta parte ficará a cargo da criatividade do grupo.

# Capítulo 4

# Conclusão.

O ensino de matemática, conforme prevê os Parâmetros Curriculares Nacionais para o Ensino Médio, deve permitir aos estudantes "compreender as ciências como construções humanas, entendendo como elas se desenvolvem por acumulação, continuidade ou ruptura de paradigmas, relacionando o desenvolvimento científico com a transformação da sociedade; analisar qualitativamente dados quantitativos, representados gráfica ou algebricamente, relacionados a contextos socioeconômicos, científicos ou cotidianos; entender a relação entre o desenvolvimento das ciências naturais e o desenvolvimento tecnológico; e compreender conceitos, procedimentos e estratégias matemáticas, e aplicá-las a situações diversas no contexto das ciências, da tecnologia e das atividades cotidianas." A temática apresentada neste trabalho é naturalmente vocacionada a um contexto histórico do desenvolvimento da ciência e da tecnologia, além de apropriar-se de conceitos matemáticos que podem ser desenvolvidos em atividades acessíveis aos estudantes do Ensino Fundamental e Médio, retirando a matemática do isolamento didático que tradicionalmente se confina no contexto escolar. No ensino de divisibilidade, funções, análise combinatória e matrizes, a criptografia mostra uma aplicabilidade coerente, interessante e atual da matemática, o que certamente proporcionará aos estudantes uma maior motivação para o aprendizado desses conceitos. A ideia de bijeção e da observação e manipulação do domínio de uma função para torná-la bijetora, mostram

uma dinâmica diferenciada do estudo das funções e da análise de seus gráficos; em análise combinatória, cada cifra monoalfabética, utilizando as próprias letras do alfabeto, produz um exemplo mais natural do conceito de permutação caótica; e a utilização de cifras em bloco para fugir da análise de frequência, enfatiza a importância do conceito. A forma atual em que a criptografia está inserida, induz a utilização de recursos tecnológicos, como a calculadora e o computador, proporcionando aos estudantes as competências e habilidades necessárias para sua formação como cidadão de uma sociedade comprometida com o futuro.

# Referências Bibliográficas

[1] ANTON, Howard et al. (2002) Algebra Linear com Aplicações. Bookman

[2] BORTOLOSSI, Humberto J. (2013). Estatistíca das Letras, Palavras e Períodos. In Revista do Professor de Matemática 82, p 26, 3º quadrimestre : São Paulo: Sociedade Brasileira de Matemática.

[3] BRASIL, Orientações curriculares para o ensino médio. Ciências da natureza, matemática e suas tecnologias. Brasília: Ministério da Educação, Secretaria de Educação Básica, 2006. Disponível em: http://portal.mec.gov.br/seb/ arquivos/pdf/book_volume_02_internet.pdf. Acesso em 01 julho 2014.

[4] CARVALHO, Paulo Cezar Pinto. (2012) Métodos de Contagem e Probabilidade. Programa de Iniciação Científica da OBMEP, Vol. 2. OBMEP.

[5] COUTINHO, S. C. (2008) Criptografia. Programa de Iniciação Científica da OBMEP, Vol. 7. OBMEP.

[6] COUTINHO, S. C. (2000) Números inteiros e Criptografia RSA. Série de Computação e Matemática n. 2. 2 ed. Rio de Janeiro, IMPA e SBM.

[7] Disponível em: http://commons.wikimedia.org/wiki/File:AGMA_H%C3%A9rodote.jpg. Acesso em: 01 de julho de 2014.

[8] Disponível em: http://site.margaritasemcensura.com/wp-content/uploads/2012/01/0601home1.jpg. Acesso em: 01 de julho de 2014.

[9] Disponível em: http://www.enigmaco.de/enigma/enigma.swf. Acesso em: 01 de julho de 2014.

[10] Disponível em: http://www.mateureka.it/notizie/grafometro-incertezza-dimensionale-disco-cifrante-le-nuove-acquisizione-del-mateureka.html. Acesso em: 01 de julho de 2014.

[11] Disponível em: http:// portal.mec.gov.br/seb/ arquivos/pdf/EnsMed/ expensmat_3_2.pdf. Acesso em: 01 de julho de 2014.

[12] HEFEZ, Abramo (2011), Elementos da aritmética. 2 ed. Rio de Janeiro: SBM.

[13] HEFEZ, Abramo (2012) Iniciação a Aritmética. Programa de Iniciação Científica da OBMEP, Vol. 1. OBMEP.

[14] LARCHER, P. H., Heródoto História. Rio de Janeiro (1950). Disponível em: http://www.ebooksbrasil.org/eLibris/historiaherodoto.html. Acesso em: 01 de julho de 2014.

[15] LIPSCHUTZ, Seymour (1971) Coleção Schaum. Rio de Janeiro. McGraw-Hill do Brasil.

[16] MALAGUTTI, Pedro Luiz (2008) Atividades de Contagem a partir da Criptografia. Programa de Iniciação Científica da OBMEP, Vol. 10. OBMEP.

[17] MORGADO, Augusto Cesar de Oliveira et al. (2006) Análise Combinatória e Probabilidade. SBM

[18] ONUCHIC, Lourdes de La Rosa. (1999) Ensino-Aprendizagem de Matematica Atráves da Resolução de Problemas. São Paulo, Editora UNESP.

[19] PAINE, Stephen. (2002) Criptografia e Segurança: o guia oficial RSA. Rio de Janeiro. Editora Campus.

[20] POLYA, George. (1995) A Arte de Resolver Problemas. Rio de Janeiro, Interciência.

[21] SINGH, Simon. (2001). O Livro dos Códigos. Rio de Janeiro. Record.

[22] STALLINGS, Willian; traduzido por Daniel Vieira (2008), Criptografia e segurança de redes. 4 ed. São Paulo: Pearson Prentice Hall.

[23] TAMAROZZI, A. C. (2003).Codificando e decifrando mensagens. In Revista do Professor de Matemática 45, São Paulo: Sociedade Brasileira de Matemática.