Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

A Utilização da Criptografia para uma Aprendizagem Contextualizada e Significativa

Waldizar Borges de Araújo França

Brasília

2014

Waldizar Borges de Araújo França

A Utilização da Criptografia para uma Aprendizagem Contextualizada e Significativa

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de Mestre Profissional em Matemática.
Área de Concentração: Matemática do Ensino Básico
Orientador: Prof. Dr. Rui Seimetz

Brasília

2014

Ficha catalográfica elaborada pela Biblioteca Central da Universidade de Brasília. Acervo 1016138.

França, Waldizar Borges de Araújo.
F814u A utilização da criptografia para uma aprendizagem contextualizada e significativa / Waldizar Borges de Araújo França. -- 2014.
63 f. : il. ; 30 cm.

Dissertação (mestrado) - Universidade de Brasília, Instituto de Ciências Exatas, Departamento de Matemática, Mestrado Profissional em Matemática, 2014.
Inclui bibliografia.
Orientação: Rui Seimetz.

1. Criptografia. 2. Matemática. 3. Funções (Matemática). 4. Matrizes (Matemática). 5. Análise combinatória. I. Seimetz, Rui. II. Título.

CDU 681.188

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

A Utilização da Criptografia Para Uma Aprendizagem Contextualizada e Significativa.

por

WALDIZAR BORGES DE ARAUJO FRANÇA*

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática-UnB, como requisito parcial para obtenção do grau de

MESTRE EM MATEMÁTICA

Brasília, 06 de junho de 2014.

Comissão Examinadora:

Prof. Dr. Rui Seimetz – MAT/UnB (Orientador)

Prof. Dr. Carlos Alberto Raposo da Cunha – UFSJ/MG

Prof. Dr. Helder de Carvalho Matos – MAT/UnB

* O autor foi bolsista CAPES durante a elaboração desta dissertação.

Waldizar Borges de Araújo França graduou-se em Matemática pela Universidade Católica de Brasília. Professor desde de 2002 em diversos cursos para concursos, pré-vestibular e escolas em Brasília. Servidor público da Secretaria de Educação do DF. Ministra aulas para concursos de Matemática, Raciocínio Lógico, Estatística e Matemática Financeira.

Dedico este trabalho aos meus pais, em especial pela dedicação e apoio em todos os momentos difíceis.

Agradecimentos

Ao meu pai Francisco Borges, que sempre me incentivou e motivou a dar continuidade aos meus estudos e conseguir a formação que alcancei.

A minha mãe Josefa Borges, que sempre investiu na minha educação e me propiciou a oportunidade de me dedicar aos estudos.

A minha querida esposa Rejane Cristina, por estar sempre presente, me apoiando, me encorajando com muito incentivo e carinho.

Ao meu irmão Wagner Borges, que com a sua genialidade me incentivou e aconselhou em diversos momentos.

Aos meus filhos Gustavo e Vítor, por serem minhas eternas fontes de expiração e encherem minha vida de alegria.

Aos colegas professores da UnB, por acreditarem que conseguiríamos.

Aos amigos e familiares, por terem compreendido a minha ausência em muitos momentos nos últimos dois anos.

Agradeço a Secretaria de Educação do DF e a CAPES pelo suporte financeiro que foi de grande valia.

Resumo

Neste trabalho estuda-se os principais conceitos da criptografia e mostra-se a sua evolução ao longo da história, fornecendo dados para que o professor de matemática possa introduzir esse assunto no Ensino Médio. No último capítulo deste trabalho, são propostas atividades, fundamentadas em resolução de problemas, que abordam os conceitos de Funções Afins, Funções Quadráticas, Funções Exponenciais, Funções Logarítmicas, Matrizes e Análise Combinatória. Estas atividades têm como agente motivador a criptografia para codificar e decodificar mensagens.

Palavras-chave: Criptografia; Matemática; Funções; Matrizes; Análise Combinatória.

Abstract

In this work, we study the main concepts of cryptography and show its evolution throughout history, providing data for the mathematics teacher can introduce this subject in high school. In the last chapter of this work are proposed activities based on problem solving, addressing the concepts of Affine, Quadratic Functions, Exponential Functions, Logarithmic Functions, Arrays and Combinatorial Analysis, having as motivator encryption to encode and decode messages.

Keywords: Cryptography; Mathematics; Functions; Matrices; Combinatorics Analises.

Lista de Figuras

Lista de Tabelas

Sumário

Introdução

Este trabalho é parte integrante da Dissertação de Mestrado apresentada ao programa de Pós-Graduação Stricto Sensu Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) da Universidade de Brasília (UnB), intitulado "A Utilização da Criptografia para uma Aprendizagem Contextualizada e Significativa" contendo orientações e sugestões para aplicação de atividades que relacionam conteúdos de Matemática do Ensino Médio, com o objetivo de auxiliar o trabalho do professor em sala de aula, primando por uma aprendizagem contextualizada e significativa.

Desde a antiguidade, o homem tem sentido a necessidade de guardar segredos. Sejam segredos familiares, segredos sentimentais, segredos pessoais, segredos religiosos, ou segredos militares e governamentais. Tão forte quanto à necessidade nata da espécie humana de guardar segredos sobre determinados assuntos é a vontade dos mesmos humanos de desvendar esses segredos. Seja por dinheiro, poder, vingança, curiosidade, arrogância, ou qualquer outro sentimento essa tem sido uma batalha que, ao longo dos anos vem sendo travada entre aqueles que querem guardar segredos e os que querem desvendar esses segredos. Os codificadores buscam criar códigos cada vez mais fortes enquanto os decifradores tornam seus métodos cada vez mais eficazes, ambos utilizando a matemática e diversas outras disciplinas e tecnologias.

Quanto maior o fluxo de informações em redes de telecomunicações, ou maior a quantidade de informação armazenada em meios computacionais, maior é a necessidade de empresas, governos e até de pessoas físicas de se protegerem contra uma nova ameaça que está crescendo proporcionalmente ao desenvolvimento da informática. Trata-se do furto de informação sigilosa e estratégica, armazenada em meios computacionais, ou da adulteração de transações através do poder das telecomunicações. Grande parte dos indivíduos, mesmo aqueles que não lidam com informações secretas, como segredos militares e industriais, utiliza no cotidiano computadores para uma série de atividades. São feitas transações bancárias, compras pela internet, trocas de emails com amigos

e de mensagens em programas de bate-papo, enfim, há uma variedade de informações pessoais nos computadores que são valiosas e que não devem ser examinadas por intrusos.

Pensando na necessidade de se criar ferramentas capazes de proteger a informação e de prover segurança aos dados armazenados e transmitidos pelas organizações, veio a motivação para se estudar Criptografia. Sendo que através por meio desses estudos podem-se criar aplicações que dêem maior segurança às informações digitais. A criptografia estuda os métodos para cifrar ou codificar uma mensagem de modo que só o destinatário legítimo é capaz de interpretar o conteúdo da mensagem sendo ilegível para terceiros e intrusos. Os procedimentos inversos, chamados de decifragem, são os objetivos de estudo da Criptoanálise. O principal propósito da Criptografia é permitir a transmissão de mensagem por canais não seguros empregando técnicas matemáticas para tornar o conteúdo da mensagem restrita ao destinatário legítimo.

Devido à informática estar presente em nossas vidas e de maneira intensa na dos estudantes, acredita-se que o tema criptografia possa deixar os estudos em Matemática mais interessante, servindo como fator motivador para que os estudantes possam exercitar, fixar e aprofundar os conteúdos matemáticos desenvolvidos no Ensino Médio, possibilitando ao professor trabalhar com temas atuais e interligar os conteúdos matemáticos a situações do mundo real.

O objetivo deste trabalho é apresentar atividades didáticas que relacionem os conteúdos matemáticos do Ensino Médio (Funções Afim, Funções Quadráticas, Funções Exponenciais, Funções Logarítmicas, Matrizes e Análise Combinatória) ao tema Criptografia, possibilitando ao estudante de Matemática do Ensino Médio aplicar os conteúdos estudados e estabelecer estratégias na resolução de situações problemas. Acredita-se que a Matemática se torna interessante e motivadora, para a aprendizagem, quando desenvolvida de forma integrada e relacionada a outros conhecimentos.

Esperamos que esse trabalho contribua para que os professores de Matemática visualizem o potencial didático da criptografia, temática do eixo Tratamento das Informações do PCN, e que apresenta material útil para o entendimento de importantes conteúdos matemáticos podendo tornar as aulas de Matemática mais dinâmicas e motivadoras.

Segue uma breve descrição dos assuntos tratados em cada um dos próximos capítulos. No capítulo um, serão trabalhados alguns conceitos básicos da criptografia, mostrando as definições de esteganografia, criptografia e criptoanálise, observando também os principais tipos de cifras.

No capítulo dois, mostraremos a evolução da criptografia ao longo da história observando que foi marcada por três grandes fases: artesanal, mecânica e digital.

No último capítulo, estão propostas atividades que relacionam a criptografia com Funções Afins, Funções Quadráticas, Funções Exponenciais, Funções Logarítmicas, Matrizes e Análise Combinatória.

Capítulo 1

Conceitos Básicos de Criptografia

Nesse capítulo será feita uma abordagem sobre os conceitos da criptografia, apresentando as definições de esteganografia, criptografia e criptoanálise, observando também os tipos de cifras como as de transposição e substituição.

1.1 Esteganografia

A palavra Esteganografia deriva do grego stéganos que significa "oculto" e de egráphein que significa "escrita". É o meio de comunicação secreta obtido através da ocultação de mensagens, sem nenhum tratamento para modificá-la. Consiste, não em fazer com que uma mensagem seja ininteligível, mas em camuflá-la, mascarando a sua presença. Ao contrário da criptografia, que procura esconder a informação da mensagem, a esteganografia procura esconder a existência da mensagem.

A Esteganografia pode ser ocultada por algum processo físico-químico, a exemplo da conhecida "tinta invisível", onde se escreve com suco de limão sobre uma folha de papel branca. Após esta secar, é só aquecer a folha em contato com uma chama que a escrita aparece magicamente.

O grande período em que a esteganografia perdurou, demonstra que ela certamente oferece certa segurança, embora sofra de uma fraqueza fundamental: Se o mensageiro for revistado e a mensagem descoberta, então o conteúdo da comunicação secreta é imediatamente revelado. A interceptação da mensagem compromete toda a sua segurança.

1.2 Criptografia

Paralelamente ao desenvolvimento da Esteganografia, houve a evolução da criptografia, palavra derivada do grego, kriptos, que significa "secreto", e graphia, "escrita". Criptografia é o meio de comunicação cujo objetivo não é ocultar sua existência e sim esconder seu significado, processo conhecido como encriptação. É um ramo especializado da teoria da informação com muitas contribuições de outros campos da matemática e do conhecimento das ciências.

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

O objetivo da Criptografia é proteger o conteúdo de uma mensagem da curiosidade e do interesse de pessoas não autorizadas. Como sabemos, a informação é uma matéria prima e ao mesmo tempo um produto muito caro e estratégico. Informação produz conhecimento, e conhecimento é poder.

Na linguagem da criptografia, os códigos são denominados cifras, as mensagens não codificadas são textos comuns e as mensagens codificadas são textos cifrados ou criptogramas. De onde surgem duas definições: Cifrar é o ato de transformar dados em alguma forma ilegível. Seu propósito é o de garantira privacidade, mantendo a informação escondida de qualquer pessoa não autorizada, mesmo que esta consiga visualizar os dados criptografados; e decifrar é o processo inverso, ou seja, transformar os dados criptografados na sua forma original, inteligível.

Ao se mandar uma mensagem criptografada, quando a mesma for recebida, existem duas alternativas de leitura: ela poderá ser decodificada ou decifrada. Quando se fala em decodificar uma mensagem, se parte do princípio que o receptor da mensagem já conhece o procedimento usado para codificação da mensagem e o usa para retirar o código, podendo desta forma obter a mensagem através da decodificação. Já a palavra decifrada é utilizada quando o receptor da mensagem codificada não é o usuário legítimo a quem ela foi enviada, sendo necessário desvendar qual foi o procedimento utilizado para codificação para somente depois utilizá-lo na decodificação.

A criptografia e a esteganografia são temas independentes e é possível utilizá-las em conjunto gerando uma mensagem com segurança elevadíssima, embora a criptografia

seja mais poderosa, devido sua capacidade de impedir a compreensão imediata da mensagem.

1.3 Tipos de cifras

Os métodos criptográficos desenvolvidos na antiguidade eram baseados essencialmente em técnicas de substituição e transposição simples, pois o uso de cálculos matemáticos complexos era pouco prático. No capítulo seguinte veremos o usa destas técnicas na evolução da criptografia ao longo da história.

1.3.1 Cifras de transposição

As cifras de transposição misturam as letras do texto original de acordo com uma regra reversível qualquer, promovendo uma permutação das letras segundo um algoritmo e uma chave bem determinados.

Na transposição, as letras das mensagens são reorganizadas, gerando um anagrama. Para mensagens curtas, de uma única palavra, o método é inseguro, pois existe um número limitado de possibilidades para organizar as letras. Por exemplo, a palavra **PAZ** só pode ser reorganizada nestas cinco maneiras diferentes: **PZA**, **ZPA**, **APZ**, **AZP**, **ZAP**. Porém, se a palavra ou frase for muito grande torna-se impossível de ser reorganizada, pois uma palavra com 35 letras possui mais de 50.000.000.000.000.000.000.000.000.000.000 de possibilidades de arranjos.

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

1.3.2 Cifras de Substituição

As cifras de substituição produzem criptogramas nos quais as letras do texto original, tratadas individualmente ou em grupos de comprimento constante, são substituídas por outras letras, figuras, símbolos ou uma combinação destes de acordo com um sistema pré-definido.

As tabelas de substituição contêm os caracteres que serão substituídos e os caracteres de substituição. Estas tabelas também são conhecidas como cifrantes ou alfabetos cifrantes.

1.3.2.1 Substituição Monoalfabética

Uma cifra monoalfabética é construída ao fazer corresponder cada letra distinta do alfabeto exatamente a um símbolo distinto.

O sistema que substitui cada um dos caracteres de um texto claro usando outros caracteres (letras, números, símbolos, etc.) conforme uma tabela de substituição pré-estabelecida é o sistema mais antigo que se conhece. As tabelas de substituição contêm os caracteres que serão substituídos e os caracteres de substituição. Estas tabelas também são conhecidas como cifrantes ou alfabetos cifrantes. Quando apenas um cifrante é aplicado, a substituição é chamada de monoalfabética.

Dentre as substituições monoalfabéticas existe a substituição chamada **homofônica**. Homofônico vem do grego (homo=igual e fonia=som) e significa "mesmo som". É o conceito de ter sequências diferentes de letras que são pronunciadas de forma semelhante. Na criptologia, é uma cifra que substitui cada um dos caracteres do texto claro por um de vários símbolos possíveis, todos com o mesmo significado.

Nessa técnica de cifragem, cada letra é substituída por uma variedade de substitutivos, de acordo com seu número potencial proporcional a frequência da letra. Por exemplo, a letra A corresponde, em média, a 14% por cento de todas as letras que aparecem num texto em português, então este possuirá quatorze símbolos para representá-lo. Caso, por exemplo, a letra D corresponda a 5% por cento de um texto em português, este possuirá cinco símbolos para representá-lo.

1.3.2.2 Substituição Polialfabética

Em uma cifra de substituição polialfabética temos que mais de um cifrante é utilizado para cifrar um texto claro. Um alfabeto cifrante é um conjunto de símbolos que serão utilizados para substituir os símbolos (letras) originais. Numa substituição polialfabética utilizam-se múltiplos cifrantes para substituir os caracteres de uma única mensagem.

Uma cifra homofônica pode parecer uma cifra polialfabética, pois cada letra pode ser cifrada de modos diferentes, porém a cifra homofônica não passa de uma cifra

monoalfabética. Uma letra no alfabeto pode ser representada por vários símbolos, mas cada símbolo representa apenas uma letra. Uma vez estabelecido o alfabeto cifrado, este permanece o mesmo durante todo o processo de cifragem.

1.3.3 Criptoanálise

A criptoanálise é o conjunto de técnicas e métodos para decifrar uma escrita de sistema desconhecido. O termo "decifrar" é usado com o significado de descobrir a mensagem original de um criptograma sem possuir a chave de decodificação, ou seja, sem ser o destinatário legítimo.

Assim, foram lançadas as bases para o desenvolvimento da criptografia e da criptoanálise. A criptografia, como a área do conhecimento encarregada de produzir técnicas que permitam a transmissão secreta de mensagens, e a criptoanálise, cuidando da elaboração de técnicas para decifrar mensagens criptografadas.

Algumas técnicas são chamadas de ataque de força bruta, onde na tentativa de decifrar um texto, parte-se para a verificação de todas as chaves possíveis do código utilizado. Temos também Análise de Frequências. Este método consiste em comparar a frequência de aparecimento das letras do alfabeto de uma determinada língua, com a frequência de aparecimento das letras no texto cifrado, fazendo assim uma correspondência entre elas. Técnicas como essas foram empregadas com bastante êxito antes da invenção dos computadores.

Com a utilização generalizada do computador pelo cidadão comum, a criptografia e a criptoanálise assumem um papel fundamental na nossa vida diária: o código do multibanco e a assinatura digital no cartão do cidadão são apenas dois, dos muitos exemplos que poderíamos dar. Neste momento, os objetivos da criptografia são:

- Confidencialidade – mantém o conteúdo da informação secreto para todos exceto para as pessoas que tenham acesso à mesma.
- Integridade da informação – assegura que não há alteração, intencional ou não, da informação por pessoas não autorizadas.
- Autenticação de informação – serve para identificar pessoas ou processos com quem se estabelece comunicação.
- Não repudio – evita que qualquer das partes envolvidas na comunicação negue o envio ou a recepção de uma informação.

Capítulo 2

A Evolução da Criptografia ao longo da História

Da antiguidade aos tempos atuais, vários acontecimentos marcaram a história da Criptografia. Nesta segunda etapa do trabalho, apresentamos os eventos históricos que marcaram a história da criptografia, mostrando a evolução dos métodos de cifragem, fornecendo dados para que o professor de Matemática possa ter ideias de como introduzir este assunto no ensino básico.

Com a escrita, surge a necessidade de transmissão de mensagens confidenciais, compreendidas apenas pelo emissor e pelo receptor. Aparece também o desejo de interceptar mensagens e de decifrá-las. Motivos não faltaram: segredos militares, políticos, religiosos, questões de comércio ou motivos sentimentais.

O desenvolvimento da criptografia desde tempos antigos até a atualidade é marcado por três grandes fases: artesanal, mecânica e digital. Esta divisão em fases tem a vantagem de oferecer uma visão geral, mas possui de certa forma, uma relativa imprecisão, sendo impossível determinar exatamente quando uma fase começa e a outra termina.

Dessa forma, apresenta-se um resumo sobre a história da Criptografia, com a finalidade de entender sua utilidade ao longo da história e de buscar esclarecer conceitos, características e experimentos utilizados por ela.

2.1 Criptografia Artesanal

O período artesanal registra os primeiros indícios de utilização da criptografa, paralelamente com o surgimento da escrita, ocorrendo durante as idades antiga e média. Segue uma sequência de relatos históricos que destacam este período. Estas técnicas têm em comum o fato de poderem ser empregadas usando-se apenas lápis e papel, e poderem ser decifradas praticamente da mesma forma. Atualmente com a ajuda dos computadores, as mensagens criptografadas empregando-se estes algoritmos são facilmente decifradas, por isso caíram rapidamente em desuso.

2.1.1 Heródoto

Um dos primeiros textos sobre códigos secretos foi escrito pelo geógrafo e historiador grego Heródoto (485 a.C. - 420 a.C.). De acordo com Heródoto a Grécia foi salva da conquista por Xerxes (Rei dos Reis da Pérsia) através da técnica da escrita secreta. Durante cinco anos, Xerxes montou secretamente a maior força de combate da história para atacar a Grécia. Demarato, um grego que fora expulso de sua terra natal, vivia numa cidade persa e, apesar de exilado, mantinha um laço de lealdade com a Grécia. Com isso, decidiu escrever uma mensagem para alertar os espartanos sobre a invasão. A mensagem precisou ser escondida para que passasse pelos guardas persas no caminho para a Grécia. A estratégia que Demarato encontrou consistia em simplesmente ocultar a mensagem. Conseguiu isso raspando a cera de um par de tabuletas de madeira, onde escreveu as intenções de Xerxes e depois cobriu novamente as tabuletas com a cera. Com a chegada da tabuleta em seu destino, os gregos se prepararam adequadamente para o ataque e derrotaram a frota persa invasora.

O historiador conta também a história de Histaeu que para transmitir suas instruções com segurança, 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 revelando a mensagem ao destinatário.

Em ambos os relatos, uma mensagem foi escondida de uma determinada maneira. Caso fosse encontrada, seu conteúdo poderia ser lido pelo inimigo, sem nenhum esforço. Este tipo de técnica que oculta amensagem é chamada esteganografia.

2.1.2 O Bastão de Licurgo

Os espartanos usavam o scytale ou bastão de Licurgo, uma cifra de transposição, para transmitir mensagens confidenciais. Foi considerado o primeiro aparelho criptográfico militar, criado no século V a.C. Era um bastão de madeira ao redor do qual se enrolava uma tira de couro longa e estreita. O funcionamento do scytale era bem simples, bastava o remetente escrever a mensagem ao longo do comprimento do instrumento e depois desenrolava a fita, formando uma mensagem contendo letras sem sentido. O mensageiro usava a tira como cinto, com as letras voltadas para dentro (Esteganografia). Para decodificar a mensagem o destinatário deveria possuir um scytale contendo o mesmo diâmetro do que foi usado pelo remetente, e simplesmente enrolava a tira em volta do bastão, formando assim a mensagem. O formato do bastão seria a chave desta cifra. Desta forma, os governantes e generais de Esparta trocavam, com segurança, as suas mensagens secretas.

2.1.3 Código de César

O famoso Julio César (por volta de 60 a.C.) usava um cifrário para comunicar seus planos de batalha aos generais de seu exercito.

Suetônio, escritor romano que viveu no início da era cristã (69 d.C.), em Vida dos Césares, escreveu a biografia dos imperadores romanos de Júlio César a Domiciano. Conta que Júlio César usava na sua correspondência particular um código de substituição muito simples no qual cada letra da mensagem original era substituída pela letra que a seguia em três posições no alfabeto: a letra A era substituída por D, a B por E, e assim até a última letra Z, que é cifrada com a letra C (veja a tabela 2.1).

Tabela 2.1: Código de César

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

Assim o texto **A ESCADA DA SABEDORIA TEM OS DEGRAUS FEITOS DE NÚMEROS**, cifrado pelo código de César, fica:

D HVFDGD GD VDEHGRULD WHP RV GHJUDXV IHLWRV GH QXPHURV

Hoje em dia, porém, se denomina de código de César qualquer cifra na qual cada letra da mensagem original seja substituída por outra deslocada um número fixo de posições, não necessariamente três. Um exemplo é o código que, ainda segundo Suetônio, era usado por Augusto, onde a letra A era substituída por B, a B por C e assim sucessivamente. Como o alfabeto romano possui 26 letras, são possíveis 26 códigos de César, dos quais um (o do deslocamento zero) não altera a mensagem original.

Códigos como o de César padecem de um grande problema: são muito fáceis de "quebrar". Quebrar um código significa ser capaz de ler a mensagem, mesmo não sendo seu destinatário legítimo. Uma simples criptoanálise estatística, baseada na característica estatística da língua, é suficiente para decifrar o texto.

O Código de César é, na realidade, um caso particular do código de Substituição Monoalfabética, onde cada letra ou símbolo é substituído sempre por uma mesma letra ou símbolo.

Podemos expressar o Código de César da seguinte maneira: para cada letra no texto original atribuímos um valor numérico com $a = 0$, $b = 1$, $c = 2$, $d = 3$,..., $z = 25$, que vamos chamar de texto t, substitua-a pela letra do texto cifrado, que vamos chamar de C. Aplicando a notação utilizada na aritmética modular, temos:

$$C \equiv (t + 3) \bmod 26$$

Podemos fazer um deslocamento de qualquer quantidade, de modo que o algoritmo de César fica representado por

$$C \equiv (t + k) \bmod 26, \text{ com } k \text{ pertencendo aos inteiros e } 1 \leq k \leq 25.$$

2.1.4 O Cifrário de Francis Bacon

O Cifrário de Francis Bacon, que foi um filósofo, escritor e político inglês, por volta do século XVI, detalhou seu sistema de substituição usando um alfabeto de 24 letras onde I=J e U=V. Para cada uma das letras do alfabeto é atribuído um grupo de 5 caracteres compostos pelas letras "a" e "b". Como são utilizadas apenas duas letras para a formação dos grupos, considera-se esta cifra como binária. Como os grupos são formados por 5 letras, considera-se a cifra como sendo de 5 bits e cada caractere possui duas possibilidades, podendo assim gerar $2^5 = 32$ grupos e consequentemente representar 32 letras distintas. A formação dos grupos segue uma sequência lógica fácil de memorizar. Além disso, os "a" e "b" podem ser substituídos por 0 e 1, de acordo com a tabela 2.2:

Tabela 2.2: Cifra de Bacon

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

2.1.5 Criptoanalistas Árabes

Durante anos, muitos estudiosos acreditaram que a cifra de substituição era indecifrável. Porém, decifradores descobriram um atalho para quebrar a cifra, revelando o conteúdo da mensagem em minutos. Essa descoberta foi feita no Oriente Médio por estudiosos árabes, que utilizavam uma combinação de linguística, estatística e devoção religiosa.

A criação da criptoanálise, 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. Em qualquer idioma, descobrimos uma frequência relativa; a partir deste fato, foi possível decifrar diversas mensagens e "quebrar" vários códigos monoalfabéticos; isto ocorre porque, geralmente, as letras mais frequentes no texto cifrado representam as letras mais comuns do idioma mesmo que não siga a mesma ordem.

Para isso, deve-se encontrar um texto diferente, na mesma língua, suficiente longo

para preencher uma página e fazer essa análise das frequências. Vale observar que há letras que aparecem com a mesma frequência, mas substituindo os símbolos mais frequentes torna-se mais fácil decifrar o restante, justamente por conhecer o idioma da mensagem e, consequentemente, suas palavras.

2.1.6 A Cifra de Vigenère

Diante da fraqueza apresentada pelas cifras monoalfabéticas, por volta de 1640, o italiano Leon Alberti propôs o uso de dois ou mais alfabetos, usados alternadamente. Levando essa ideia adiante, o francês Blaise de Vigenère criou a cifra que leva seu nome. A força da cifra de Vigenère consiste na utilização de 26 alfabetos cifrados distintos para criar a mensagem cifrada. Para decifrar a mensagem, o destinatário precisa saber que alfabeto usar para cada letra da mensagem, e isso é previamente informado por uma palavra-chave.

A figura 2.1 mostra como deve ser montada a tabela chamada de "quadrado de Vigenère" e segue um exemplo utilizando a palavra-chave $CIFRA$ para o texto **OS NÚMEROS GOVERNAM O MUNDO**.

Tabela 2.3: "Quadrado de Vigenère"

Palavra-chave	C	I	F	R	A	C	I	F	R	A	C	I	F	R	A	C	I	F	R	A	C	I	F
Texto original	**o**	**s**	**n**	**u**	**m**	**e**	**r**	**o**	**s**	**g**	**o**	**v**	**e**	**r**	**n**	**a**	**m**	**o**	**m**	**u**	**n**	**d**	**o**
Texto cifrado	Q	A	S	L	M	G	Z	T	J	G	Q	D	J	I	N	C	U	T	D	U	P	L	T

Observe que a letra "O" será substituída pela letra correspondente no alfabeto que começa pela letra "C", ou seja, a letra "Q"; a letra "S" será substituída pela letra correspondente no alfabeto que começa pela letra "I", ou seja, letra "A" e assim por diante, até encontrar o texto cifrado:

QASLMGZTJGQDJINCUTDUPLT

Este método resiste à análise de frequências, pois cada letra se codifica de muitas formas distintas. Para complicar ainda mais os criptoanalistas do método de Vigenère, basta elencar chaves bem mais longas e com poucas letras repetidas. Quanto mais alfabetos empregarmos, mais difícil será realizar a criptoanálise.

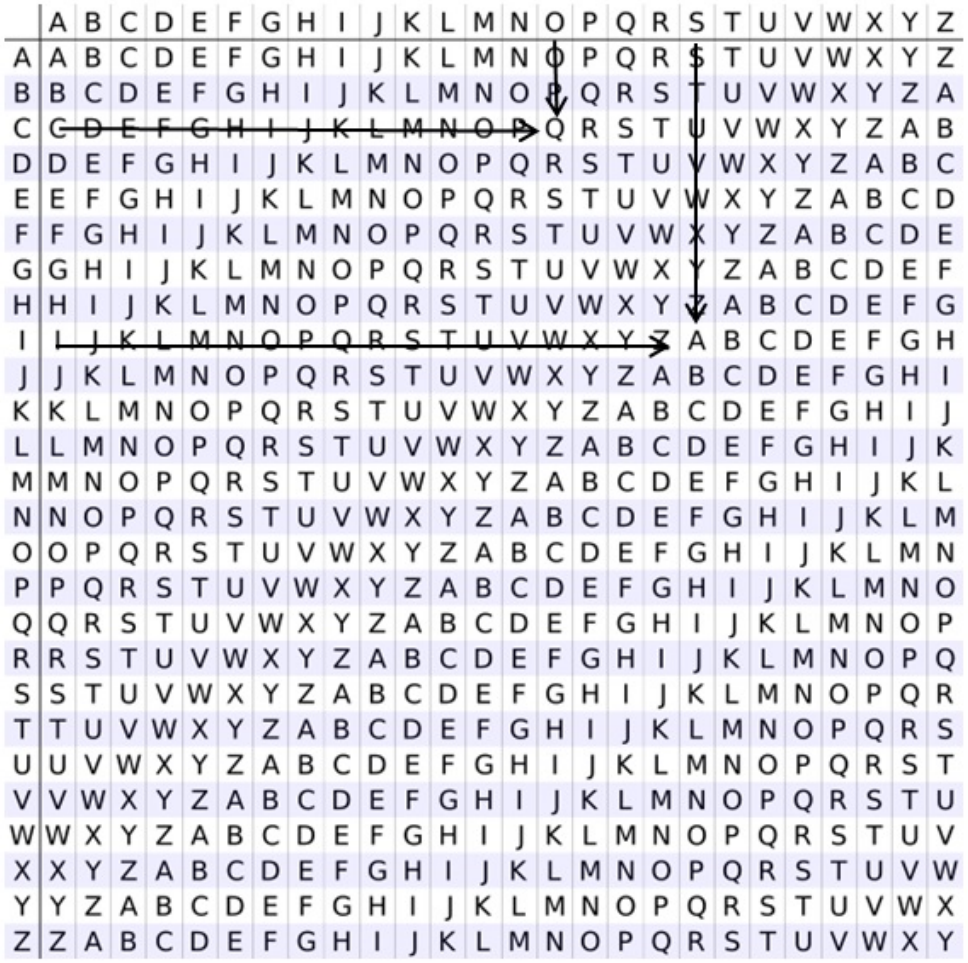


Figura 2.1: O Quadro de Vigenère

No entanto, a cifra de Vigenère era pouco atraente em uma época em que máquinas mecânicas ainda não existiam, o que tornava o ato de cifrar e decifrar muito trabalhoso. Por isso, a cifra ficou em desuso por quase 200 anos 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.

2.1.7 O Código Braille

O Código Braille foi criado por Louis Braille (1809 - 1852), educador francês, que ficou cego aos 3 anos de idade. Interessou-se por um sistema de escrita, apresentado

na escola Charles Barbier, no qual uma mensagem codificada em pontos era cunhada em papel-cartão. Aos 15 anos de idade trabalhou numa adaptação, escrita com um instrumento simples que é um sistema de símbolos onde cada caractere é formado por uma matriz de 6 pontos dos quais pelo menos um se destaca em relação aos outros.

Na figura 2.2 apresentamos um modelo do alfabeto de 26 letras, sinais ortográficos, algarismos e números do sistema Braille.

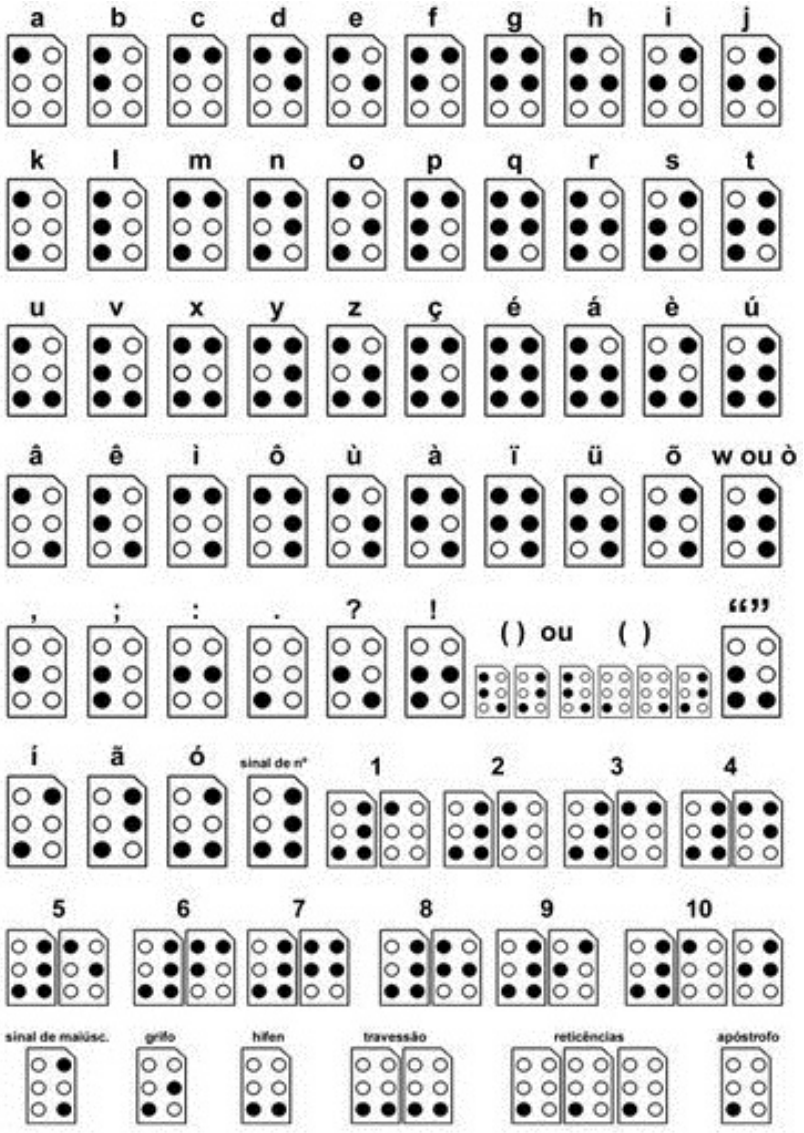


Figura 2.2: O Código Braille

Fonte: http://projetonovavisao.spaceblog.com.br/1231591/O-QUE-E-O-METODO-BRAILLE/

Hoje em dia existem vários dispositivos para escrita em Braille, desde muito simples até sofisticados dispositivos eletrônicos. O mais simples é uma lousa com uma régua perfurada onde, com o auxílio de um estilete, é possível produzir os pontos em relevo. Existem também máquina de escrever especial, impressoras ligadas a computador que produzem os relevos desejados, dispositivos com voz artifical que "lêem" braille, teclados de computador especiais e "anotadores" eletrônicos associados a máquina de calcular, calendário, etc.

2.1.8 Microponto

Em 1941, foi descoberto pelo Federal Bureau of Investigation (FBI) o primeiro microponto. Na Segunda Guerra Mundial, agentes alemães reduziam fotograficamente uma página de texto até transformá-la num ponto com menos de um milímetro de diâmetro. Este microponto era colocado sobre um ponto final, em uma carta de conteúdo totalmente insuspeito. O receptor, ao ter acesso à mensagem, procurava pelo ponto com a informação e ampliava-o a fim de ler a mensagem. Os aliados descobriram a técnica e passaram a interceptar a comunicação.

2.2 Criptografia Mecânica

A Revolução Industrial criou no homem a paixão pelas máquinas e a esperança de substituição do cansativo trabalho manual pelo mecânico. No início da Idade Moderna, com a invenção da Imprensa, aparecem os primeiros indícios da fase mecânica da criptografia. Neste período, iniciada na Inglaterra em 1760, seguida da invenção do telégrafo e do rádio no século seguinte, a fase mecânica se desenvolve e seu apogeu ocorre com as máquinas de cifragens usadas durante a Segunda Guerra Mundial. A máquina alemã Enigma é a mais ilustre representante desta linhagem.

Na criptografia mecânica é fundamental a ocultação pública da chave e também desejável manter segredo sobre a estrutura da máquina que produz a cifragem.

2.2.1 Disco de Cifras

O disco de cifras, criado por Alberti em 1466, é o primeiro sistema polialfabético conhecido e também a primeira máquina criptográfica. O Disco de Cifras é um mis-

turador que pega uma letra do texto normal e a transforma em outra letra no texto cifrado, porém seu inventor sugeriu que fosse mudada a disposição do disco durante uma mensagem, o que iria gerar uma cifra polialfabética, o que dificultaria a sua decodificação, pois desse modo ele estaria mudando o modo de mistura durante a cifragem e isso tornaria a cifra difícil de ser quebrada. Na figura 3.1 mostramos um disco de cifras.

Figura 2.3: Disco de Cifras

Fonte: http://www.cryptomuseum.com/crypto

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

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

2.2.2 O Código Morse

Samuel Morse (1791 - 1872) em 1840 desenvolve o código que recebeu o seu nome. Originalmente, Morse imaginou numerar todas as palavras e em transmitir seus números

através do telégrafo. O receptor, usando um enorme "dicionário", decifraria a mensagem onde as letras do alfabeto foram definidas pelo padrão "ponto e traço". Este novo código reconhecia quatro estados: voltagem-ligada longa (traço), voltagem-ligada curta (ponto), voltagem-desligada longa (espaço entre caracteres e palavras) e voltagem-desligada curta (espaço entre pontos e traços). Cada caractere (letras, números, sinais gráficos) possui seu próprio conjunto único de pontos e traços. Na figura 2.4 apresentamos um modelo do código Morse

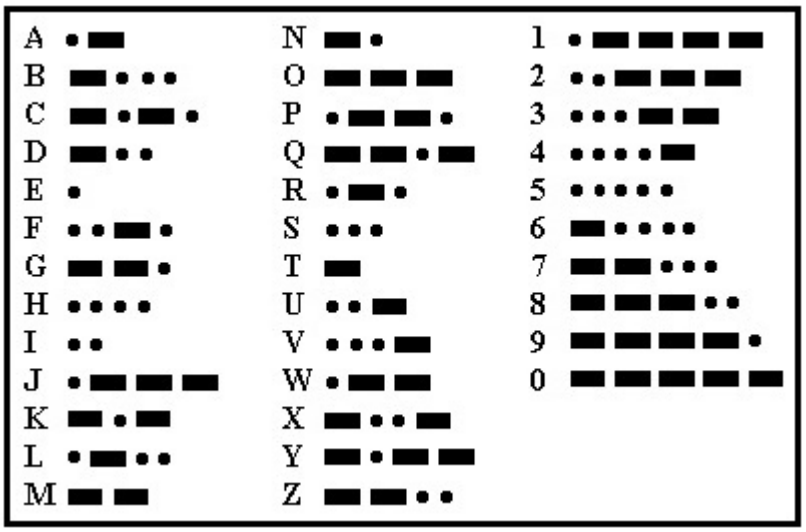


Figura 2.4: O código Morse

Fonte: http://www.cryptomuseum.com/crypto

Podemos traduzir os termos utilizados para os dias de hoje para significarem condições binárias de "1" (ponto) e "0" (traço). O alfabeto Morse é um código baseado em 5 posições, ou seja, não precisa mais do que 5 posições para que todas as letras e números sejam padronizados.

Na realidade, o aspecto mais importante quando se fala de Morse não é o código e sim a possibilidade de transmitir informações à distância. Através dos fios correm sinais elétricos que, devidamente concatenados, representam mensagens.

2.2.3 A Máquina Enigma

Após a Primeira Guerra Mundial, impulsionado pela invenção do telégrafo e do rádio, o alemão Scherbuis criou a máquina Enigma, uma versão elétrica do disco de

cifras, que revolucionou o mundo da criptografia. Esta máquina de cifra, devido ao elevado número de chaves que pode utilizar e à sua complexidade foi usada para fins militares pelos alemães, pois estavam convictos da sua segurança.

A máquina Enigma foi a ferramenta criptográfica mais importante da Alemanha nazista e os alemães apostavam em sua eficiência para vencer a guerra. Consistia de um teclado ligado a uma unidade codificadora. O codificador tinha três rotores separados e as posições dos rotores determinavam como cada letra no teclado seria codificada. O que tornava o código da Enigma tão difícil de quebrar era o enorme número de modos nos quais a máquina podia ser regulada. Em primeiro lugar, os três rotores na máquina eram escolhidos de uma seleção de cinco que podia ser mudada e trocada para confundir os adversários. Em segundo lugar, cada rotor podia ser posicionado em 26 modos diferentes. Isto significava que a máquina podia ser regulada em milhões de modos diferentes. E além das permutações permitidas pelos rotores, as conexões no quadro de chaveamento, na parte detrás da máquina, podiam ser mudadas manualmente para fornecer um total de 150 trilhões de regulagens possíveis. E para aumentar ainda mais a segurança, os três rotores mudavam de orientação continuamente, de modo que, cada vez que a letra era transmitida, a regulagem da máquina, e portanto o código, iria mudar de uma letra para outras. Assim se alguém digitasse "$DODO$" no teclado iria gerar a mensagem "$FSTR$", por exemplo – o "D" e o "O" eram transmitidos duas vezes, mas codificados de modo diferente a cada vez.

A máquina Enigma podia ser configurada de

$$\frac{3!26^3}{10!}\binom{26}{2}\binom{24}{2}\binom{22}{2}\binom{20}{2}\binom{18}{2}\binom{16}{2}\binom{14}{2}\binom{12}{2}\binom{10}{2}\binom{8}{2}$$

maneiras diferentes. Este número na base decimal é igual a 15.896.255.521.782.636.000.

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. Até que após um árduo trabalho, o criptoanalista Alan Turing conseguiu quebrá-la na primeira metade da década de 40. Para realizar o trabalho como uma resposta à alta mecanização da Enigma, Alan Turing e seus colaboradores desenvolveram dois tipos de máquinas para manipular as cifras interceptadas da Enigma: a primeira foi denominada Bomba e a segunda Colossus. Esta última ao ser programável é considerada uma precursora dos modernos computadores. A quebra das cifras da Enigma deu aos Aliados uma vantagem fundamental, que, de acordo com historiadores, encurtou a guerra por mais dois anos, salvando muitas vidas.

2.2.4 Colossus

Em 1943, foi projetado o computador Colossus. Esse computador foi utilizado durante a Segunda Guerra Mundial para decodificar os códigos criados pela Enigma. O Colossus deu início a uma era moderna da criptografia, onde os computadores eram programados com chaves de codificação muito mais complexas do que as utilizadas pela Enigma. Essa nova técnica de criptografia era de uso exclusivo do governo e de militares para guardar informações.

O computador Colossus foi construído no centro de pesquisas dos correios, em Dollis Hill, Londres, e era uma máquina capaz de adaptar-se a diferentes problemas, ou seja, foi a precursora do moderno computador. O Colossus foi destruído depois da Segunda Guerra Mundial e sua planta de construção foi queimada. Com isso, outros cientistas receberam os créditos pela invenção do computador. Em 1945, na Universidade da Pensilvânia, foi criado o ENIAC, Electronic Numerical Integrator And Calculator, que consistia em 18 mil válvulas eletrônicas capazes de realizar cinco mil cálculos por segundo.

2.3 Criptografia Digital

Com o desenvolvimento e aperfeiçoamento dos computadores e 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 a residir exclusivamente na chave. Os sistemas de criptografia clássicos perderam sua eficácia devido à facilidade com que atualmente são decodificados empregando-se qualquer computador doméstico, mas que foram empregados com êxito até princípios do século XX.

Em um moderno computador, a informação é representada através de uma sequência de zeros e uns: são os dígitos binários, mais adequadamente referidos por bits. Portanto, para começar uma cifragem de uma mensagem através do computador, a primeira operação consiste na tradução da mensagem original, em números binários. Existem vários protocolos que fazem a transformação.

Um exemplo é o American Standard Code for Information Interchange (ASCII), que destina a cada letra do alfabeto um número binário de sete dígitos - o que representa uma sequência de zeros e uns. Na tabela 2.4 apresentamos o ASCII.

Tabela 2.4: ASCII

Binary	Character	Binary	Character	Binary	Character
100 0001	A	110 0001	a	011 0000	0
100 0010	B	110 0010	b	011 0001	1
100 0011	C	110 0011	c	011 0010	2
100 0100	D	110 0100	d	011 0011	3
100 0101	E	110 0101	e	011 0100	4
100 0110	F	110 0110	f	011 0101	5
100 0111	G	110 0111	g	011 0110	6
100 1000	H	110 1000	h	011 0111	7
100 1001	I	110 1001	i	011 1000	8
100 1010	J	110 1010	j	011 1001	9
100 1011	K	110 1011	k		
100 1100	L	110 1100	l		
100 1101	M	110 1101	m		
100 1110	N	110 1110	n		
100 1111	O	110 1111	o		
101 0000	P	111 0000	p		
101 0001	Q	111 0001	q		
101 0010	R	111 0010	r		
101 0011	S	111 0011	s		
101 0100	T	111 0100	t		
101 0101	U	111 0101	u		
101 0110	V	111 0110	v		
101 0111	W	111 0111	w		
101 1000	X	111 1000	x		
101 1001	Y	111 1001	y		
101 1010	Z	111 1010	z		

Fonte:
http://drstienecker.com/tech-261-material/29-communication-systems/

Durante toda esta etapa, que cobriu a fase mecânica até o princípio da fase digital com o algoritmo DES, um aspecto permaneceu inalterado: a utilização de chaves privadas, caracterizando uma criptografia simétrica. A seguir temos alguns exemplos deste tipo de criptografia na era digital.

2.3.1 Criptografia Simétrica

A criptografia simétrica (ou de chave privada) transforma um texto claro em um texto cifrado, usando uma chave secreta e um algoritmo de criptografia. O poder da cifra é medido pelo tamanho da chave (num sistema de encriptação, corresponde a um nome, uma palavra, uma frase, etc., que permite, mediante o algoritmo de encriptação, cifrar ou decifrar uma mensagem.), geralmente as chaves de 40 bits são consideradas fracas e as de 256 bits ou mais, as mais fortes. A partir da mesma chave e com o auxílio de um algoritmo de descriptografia, o texto claro é recuperado a partir do texto cifrado.

Esta cifra utiliza uma única chave secreta, logo antes de duas entidades estabelecerem um canal seguro, é preciso que ambos, tanto o emissor quanto ao receptor, compartilhem suas chaves respectivas.

O problema com os Sistemas Criptográficos Simétricos reside na distribuição da chave, que nos métodos implementados eletronicamente são feitos através dos canais eletrônicos (linha telefônica e ondas de rádio), vulneráveis à "escuta" de algum intruso. Portanto, estas devem ser trocadas entre as partes e armazenadas de forma segura, o que nem sempre é possível de se garantir. A criptografia simétrica não garante a identidade de quem enviou ou recebeu a mensagem. A quantidade de usuários em uma rede pode dificultar o gerenciamento das chaves.

2.3.1.1 DES

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

O DES é um algoritmo de criptografia em blocos, composto da substituição de caracteres em blocos de 64 bits, utilizando uma chave de 56 bits. Sua estrutura é composta de 16 estágios de criptografia, executando, durante todo o processo, séries de transposições e substituições de caracteres, bem como, a recombinação de blocos.

A partir de 2001, o DES foi substituído pelo AES (Advanced Encryption Standard), que é aplicado atualmente nas conexões Wi-Fi que nós usamos em nossos lares.

2.3.1.2 AES

O Advanced Encryption Standard (AES) é uma cifra de bloco, anunciado pelo National Institute of Standards and Technology (NIST) em 2003, fruto de concurso para escolha de um novo algoritmo de chave simétrica para proteger informações do governo federal, sendo adotado como padrão pelo governo dos Estados Unidos. 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, ele é rápido tanto em software quanto em hardware, é relativamente fácil de executar e requer pouca memória.

2.3.1.3 IDEA

O International Data Encryption Algorithm (IDEA) foi criado em 1991 por James Massey e Xuejia Lai e possui patente da empresa suíça Ascom Systec. O IDEA é um algoritmo simétrico que utiliza uma chave de 128 bits. Um ataque de força bruta dos mais eficientes precisaria fazer 2^{128} (ou aproximadamente 10^{36}) cifragens para recuperar a chave. Se dispuséssemos de um bilhão de chips que testassem um bilhão de chaves por segundo cada um, ainda assim seriam necessários 10^{13} anos para se realizar a tarefa.

2.3.2 Criptografia Assimétrica

Cifras assimétricas ou de algoritmos de chave pública permitem que a chave seja de domínio público - pode até ser publicada em jornais ou revistas. Qualquer pessoa pode, então, cifrar mensagens utilizando a chave, mas apenas o destinatário e real proprietário da chave será capaz de decifrar o texto porque é o único que conhece a chave decifrante. A chave cifrante também é chamada de chave pública e a chave decifrante de chave privada ou chave secreta.

Mas a característica principal da criptografia assimétrica é a implementação de uma "função bijetiva de mão única", ou seja, uma função fácil de computar em um sentido, mas difícil de ser computada no sentido inverso, caso não se conheça a chave secreta.

Hoje contamos com sofisticados sistemas criptográficos que utilizam a matemática dos números primos para que possamos estar seguros em nossas transações bancárias e troca de informações pela rede virtual.

2.3.2.1 RSA

O mais conhecido dos métodos de criptografia é o RSA. Este código foi inventado 1978, por R. L Rivest, A. Shamir, e L. Adleman. As letras RSA correspondem às iniciais dos inventores do algoritmo. O RSA é um método criptográfico assimétrico muito usado em aplicações comerciais. De modo geral, para codificar uma mensagem usando o RSA é preciso obter dois números primos grandes e para decifrar seria necessário fatorar o produto destes números primos. Neste método quem tem a chave de codificação não tem necessariamente a chave de decodificação.

A premissa por trás do RSA consiste na facilidade de multiplicar dois números primos para obter um terceiro número, mas muito difícil de recuperar os dois números primos a partir daquele terceiro número. Se o número for grande o suficiente e bem escolhido, então ninguém pode fazer isto em uma quantidade de tempo razoável. Assim, a segurança do RSA baseia-se na dificuldade de fatoração de números grandes. O único problema para a segurança da criptografia de chave pública RSA é que, em alguma época no futuro, alguém encontre um método rápido para fatorar estes números primos, mas a grande vantagem desse sistema, de chave pública, é que ela acaba com os problemas da distribuição de chaves.

Existem vários outros códigos de chave pública, mas o RSA continua sendo o mais usado em aplicações comerciais.

2.3.2.2 ElGamal

O El-Gamal é um criptossistema de chave pública criado em 1984 pelo pesquisador Taher El-Gamal. Esse método consiste na solução do logaritmo discreto. Assim, o El-Gamal obtém sua segurança da dificuldade de se calcular logaritmos discretos em um corpo finito, o que lembra bastante o problema da fatoração.

2.3.2.3 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. A técnica de criptografia baseada em curvas elípticas tem sua segurança no fato de não existir nenhum algoritmo sub-exponencial conhecido para resolver o problema do logaritmo discreto em uma curva elíptica simples.

A partir do início de 1990, começa o trabalho de pesquisa para a construção de computadores quânticos e o desenvolvimento de uma criptografia quântica. Os primeiros ensaios experimentais são publicados por Charles H. Bennett, Gilles Brassard 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. Para o leitor interessado nesse sistema de criptografia, ver a referência [5].

Capítulo 3

Desenvolvimento

Nos capítulos anteriores, estudamos a evolução da criptografia ao longo da história, aprendemos vários métodos de codificação e decodificação de mensagens e conceitos da criptografia. Esses capítulos irão servir de base para que o professor possa introduzir as atividades propostas acerca do tema.

Nesse capitulo, foram selecionados alguns métodos de criptografia considerados interessantes do ponto de vista de aplicação de conceitos matemáticos, que nos possibilitaram elaborar atividades, apresentadas a seguir, com objetivo de diminuir as aulas mecânicas, de modo que a criptografia possa ser usada no ensino da matemática, como uma atividade lúdica, voltada para a aprendizagem com significado.

A seguir apresentam-se exemplos de atividades didáticas que podem ser utilizadas pelos professores do Ensino Médio apresentando o tema Criptografia como um recurso didático no Ensino da Matemática.

3.1 Atividade 1

Objetivo Geral

Explorar o conceito de função polinomial do 1º grau na criptografia, visando uma aprendizagem contextualizada e significativa.

Objetivo Específico

- Calcular a imagem de um elemento do domínio da função do 1º grau.

- Determinar a função inversa de uma função do 1º grau.
- Resolver sistemas lineares por meio do método da substituição.
- Obter uma função do 1º grau, a partir de dois pontos.
- Resolver problemas que envolvam o conceito de função.

Público alvo

Estudantes do 1º ano do ensino médio de acordo com os Parâmetros Curriculares Nacionais (PCN).

Estratégias para aplicação da atividade

O professor faz uma breve explicação do que é criptografia, da sua importância ao longo da história e na atualidade. Em seguida, explica o exemplo do texto e os estudantes respondem as atividades. Ao final, os estudantes se reúnem em duplas para trocar funções e mensagens para verificar se o colega consegue decodificá-las.

Atividade 1: Função Afim

Considere que Ana deseja enviar uma mensagem secreta para Gustavo, seguindo os passos do procedimento exemplificado a seguir :

Passo 1: Ana relaciona para cada letra do alfabeto um número, conforme a tabela abaixo:

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

Passo 2: Ana determina um texto a ser codificado e obtém a sequência numérica correspondente ao texto de acordo com a tabela.

Passo 3: Para obter a mensagem cifrada Ana escolhe uma função cifradora $f(x)$ do 1º grau e transmite a Gustavo uma sequência numérica obtida pelas imagens da função f.

Por exemplo: Caso Ana queira enviar a mensagem **AMO MATEMATICA** utilizando a função cifradora $f(x) = 3x - 1$ teremos a seguinte codificação:

Letra	**Sequência numérica**	**Imagem da função** $f(x) = 3x - 1$
A	1	$f(x) = 3x - 1 = 3.1 - 1 = 2$
M	13	$f(x) = 3x - 1 = 3.13 - 1 = 38$
O	15	$f(x) = 3x - 1 = 3.15 - 1 = 44$
T	20	$f(x) = 3x - 1 = 3.20 - 1 = 59$
E	5	$f(x) = 3x - 1 = 3.5 - 1 = 14$
I	9	$f(x) = 3x - 1 = 3.9 - 1 = 26$
C	3	$f(x) = 3x - 1 = 3.3 - 1 = 8$

Portanto a mensagem codificada a ser transmitida é **2-38-44-38-2-59-14-38-2-59-26-8-2**.

Gustavo ao receber a mensagem cifrada, deverá calcular as imagens da inversa da função cifradora.

Gustavo deve encontrar a função inversa de $f(x) = 3x - 1$. Pode-se usar o procedimento abaixo:

$$f(x) = 3x - 1 \Rightarrow y = 3x - 1 \Rightarrow x = \frac{y+1}{3} \Rightarrow f^{-1}(x) = \frac{x+1}{3}$$

Agora Gustavo calcula a imagem da função inversa para cada algarismo da sequência da mensagem codificada.

Algarismo recebido	**Imagem da inversa**	**Letra encontrada**
2	$f^{-1}(x) = \frac{x+1}{3} = \frac{2+1}{3} = 1$	A
38	$f^{-1}(x) = \frac{x+1}{3} = \frac{38+1}{3} = 13$	M
44	$f^{-1}(x) = \frac{x+1}{3} = \frac{44+1}{3} = 15$	O
59	$f^{-1}(x) = \frac{x+1}{3} = \frac{59+1}{3} = 20$	T
14	$f^{-1}(x) = \frac{x+1}{3} = \frac{14+1}{3} = 5$	E
26	$f^{-1}(x) = \frac{x+1}{3} = \frac{26+1}{3} = 1$	I
8	$f^{-1}(x) = \frac{x+1}{3} = \frac{8+1}{3} = 3$	C

Logo, a mensagem decodificada é **AMO MATEMATICA**.

Com base na situação apresentada no texto e nos conhecimentos relativos a funções, faça o que se pede nos itens subsequentes:

a) Cifre a mensagem **A NATUREZA ESTÁ ESCRITA EM LINGUAGEM MATEMÁTICA**, utilizando a função cifradora $f(x) = 2x + 3$.

b) Complete a tabela abaixo:

Letra	**Sequência numérica**	**Imagem da função** $f(x) = 4x - 3$
A	1	$f(x) = 4x - 3 = 4.1 - 3 = 1$
B	2	
C		
	24	
	25	
		101
		89

c) Suponha que Ana e Gustavo estão trocando mensagens através da função cifradora $f(x) = 2x+5$ e Gustavo receba a mensagem **49-23-49-15-41-43-23-19-33-23-17-23-11-7-29-47-45-7-4**. Decodifique a mensagem recebida por Gustavo.

d) Sabendo que a Ana enviou uma mensagem para Gustavo, onde na função cifradora $f(1) = 8$ e $f(4) = 17$, decodifique a palavra **44-20-62-65-26-8-17-50**.

e) Crie uma mensagem e uma função cifradora e codifique a sua mensagem através do procedimento exemplificado no texto e envie para um colega decodificá-la.

Solução comentada

a) Nesse item, o estudante vai consultar a tabela indicada no passo 1 e calcular as imagens pela função $f(x) = 2x + 3$. Seguem os cálculos:

Letra	**Sequência numérica**	**Imagem da função** $f(x) = 2x + 3$
A	1	$f(x) = 2x + 3 = 2.1 + 3 = 5$
N	14	$f(x) = 2x + 3 = 2.14 + 3 = 31$
T	20	$f(x) = 2x + 3 = 2.20 + 3 = 43$
U	21	$f(x) = 2x + 3 = 2.21 + 3 = 45$
R	18	$f(x) = 2x + 3 = 2.18 + 3 = 39$
E	5	$f(x) = 2x + 3 = 2.5 + 3 = 13$
Z	26	$f(x) = 2x + 3 = 2.26 + 3 = 55$
S	19	$f(x) = 2x + 3 = 2.19 + 3 = 41$
C	3	$f(x) = 2x + 3 = 2.3 + 3 = 9$
I	9	$f(x) = 2x + 3 = 2.9 + 3 = 21$
M	13	$f(x) = 2x + 3 = 2.13 + 3 = 29$
L	12	$f(x) = 2x + 3 = 2.12 + 3 = 27$
G	7	$f(x) = 2x + 3 = 2.7 + 3 = 17$

A mensagem cifrada é **5-31-5-43-45-39-13-55-5-13-41-43-5-13-41-9-39-21-43-5-13-29-27-21-31-17-45-5-17-13-29-29-5-43-29-5-43-21-9-5.**

b) Ao completar a tabela, o estudante deve encontrar os seguintes resultados:

Letra	**Sequência numérica**	**Imagem da função** $f(x) = 4x - 3$
A	1	$f(x) = 4x - 3 = 4.1 - 3 = 1$
B	2	**5**
C	**3**	**9**
X	24	**93**
Y	25	**97**
Z	**26**	101
W	**23**	89

c) O estudante deverá encontrar a função inversa da $f(x)$, obtendo a $f^{-1}(x) = \frac{x-5}{2}$ e calcular a imagem da função inversa para cada algarismo. Encontrando a mensagem **VIVER SIGNIFICA LUTAR**.

d) Nesse item o estudante deverá primeiramente encontrar a função cifradora a partir de dois pontos fornecidos dessa função. Como a função dessa atividade é uma função do 1º grau, basta montar um sistema de equações substituindo os pontos na função $f(x) = ax + b$.

$$\begin{cases} a + b = 8 \\ 4a + b = 17 \end{cases} \Rightarrow a = 3 \text{ e } b = 5$$

Portanto a função cifradora é $f(x) = 3x + 5$ e sua inversa é $f^{-1}(x) = \frac{x-5}{3}$. Calculando a imagem da função inversa para cada algarismo, obtemos a palavra: **MESTRADO**.

3.2 Atividade 2

Objetivo Geral

Explorar o conceito de função quadrática na criptografia, visando uma aprendizagem contextualizada e significativa.

Objetivo Específico

- Calcular a imagem de um elemento do domínio da função quadrática.
- Reconhecer a importância do domínio e contra-domínio na obtenção de bijeções.
- Analisar e determinar o domínio, contradomínio e imagem de uma função quadrática.
- Determinar as condições para que uma função quadrática tenha inversa.
- Resolver sistemas lineares por meio do método da substituição.
- Obter uma função quadrática, a partir de três pontos.
- Resolver problemas que envolvam o conceito de função quadrática.

Público alvo

Estudantes do 1º ano do ensino médio de acordo com os Parâmetros Curriculares Nacionais (PCN).

Estratégias para aplicação da atividade

O professor faz uma breve explicação do que é criptografia, da sua importância ao longo da história e na atualidade. Em seguida, explica a situação do texto e os estudantes respondem as atividades.

Atividade 2: Função Quadrática

Para enviar uma mensagem secreta, considere que uma pessoa substitua as letras da mensagem, conforme tabela abaixo, e transforme esses números através das imagens de uma função cifradora do tipo $f(x) = ax^2 + bx + c$, com coeficientes a, b e c pertencentes aos reais e $a \neq 0$.

Tabela para pré-codificação.

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

Para decodificar a mensagem o receptor receberá a mensagem e irá calcular a sua imagem da função inversa, observando as condições de domínio e contradomínio para que uma função quadrática seja invertível.

Com base no procedimento apresentado no texto e nos conhecimentos relativos a funções quadráticas, faça o que se pede nos itens subsequentes:

a) Cifre a mensagem **O MEDO DE PERDER TIRA A VONTADE DE GANHAR**, utilizando a função cifradora $f(x) = 2x^2 + 3x - 1$.

b) Restrinja o domínio e o contradomínio, no conjunto dos números reais, da função $f(x) = 2x^2 + 3x - 1$, para que a função possua inversa, ou seja, para que $f(x)$ seja uma função bijetora.

c) Calcule a inversa da função codificadora $f(x) = 2x^2 + 3x - 1$, determinando seu domínio e contradomínio no conjunto dos números reais.

d) Utilizando a função inversa obtida no item anterior, decodifique a palavra **26-701-188-559-859-494-118-701-4-89-4-701**.

e) Sabendo que uma pessoa enviou uma mensagem, onde na função cifradora $f(1) = 5$, $f(3) = 25$ e $f(4) = 44$, decodifique a palavra **12-940-5-1049-229-412-229-5**.

Solução comentada

a) Nesse item, o estudante vai consultar a tabela indicada e calcular as imagens pela função $f(x) = 2x^2 + 3x - 1$. Seguem os cálculos:

Letra	**Sequência numérica**	**Imagem da função** $f(x) = 2x^2 + 3x - 1$
O	15	$f(x) = 2x^2 + 3x - 1 = 2.15^2 + 3.15 - 1 = 494$
M	13	$f(x) = 2x^2 + 3x - 1 = 2.13^2 + 3.13 - 1 = 376$
E	5	$f(x) = 2x^2 + 3x - 1 = 2.5^2 + 3.5 - 1 = 64$
D	4	$f(x) = 2x^2 + 3x - 1 = 2.4^2 + 3.4 - 1 = 43$
P	16	$f(x) = 2x^2 + 3x - 1 = 2.16^2 + 3.16 - 1 = 559$
R	18	$f(x) = 2x^2 + 3x - 1 = 2.18^2 + 3.18 - 1 = 701$
T	20	$f(x) = 2x^2 + 3x - 1 = 2.20^2 + 3.20 - 1 = 859$
I	9	$f(x) = 2x^2 + 3x - 1 = 2.9^2 + 3.9 - 1 = 188$
A	1	$f(x) = 2x^2 + 3x - 1 = 2.1^2 + 3.1 - 1 = 4$
V	22	$f(x) = 2x^2 + 3x - 1 = 2.22^2 + 3.22 - 1 = 1033$
N	14	$f(x) = 2x^2 + 3x - 1 = 2.14^2 + 3.14 - 1 = 433$
G	7	$f(x) = 2x^2 + 3x - 1 = 2.7^2 + 3.7 - 1 = 188$
H	8	$f(x) = 2x^2 + 3x - 1 = 2.8^2 + 3.8 - 1 = 151$

A mensagem cifrada é **494-376-64-43-494-43-64-559-64-701-43-64-701-859-188-701-4-4-1033-494-433-859-4-43-64-43-64-188-4-433-151-4-701.**

b) Nesse item os estudantes devem notar que para que uma função quadrática seja bijetora, basta limitar o domínio da função para ele seja um subconjunto de $[x_v + \infty[$(ou de $]-\infty, x_v]$) e, para o contradomínio, o correspondente subconjunto de $[y_v + \infty[$(ou de $]-\infty, y_v]$). Para melhor compreensão dessa propriedade, peça para os estudantes desenhar um gráfico da função quadrática.

Calculando $x_v = -\frac{b}{2a} = -\frac{3}{4}$ e $y_v = -\frac{b^2-4ac}{4a} = -\frac{17}{8}$, obtemos o $D_f = [-\frac{3}{4}, +\infty[$ e o $CD_f = [-\frac{17}{8}, +\infty[$.

c) Nesse item o estudante deverá fazer o cálculo da função inversa, podendo seguir o seguinte procedimento:

$$f(x) = 2x^2 + 3x - 1 \Rightarrow y = 2x^2 + 3x - 1 \Rightarrow 2x^2 + 3x - 1 - y = 0$$

Isolamos x de y usando a fórmula de obtenção de raízes de uma equação polinomial de grau 2, onde temos $\triangle = 17 + 8y$ e $x = \frac{-3 \pm \sqrt{17+8y}}{4}$.

A função inversa corresponde a $f^{-1}(x) = \frac{-3+\sqrt{17+8x}}{4}$, onde o domínio da função inversa é o contradomínio de f e vice-versa.

Portanto, $D_f = [-\frac{17}{8}, +\infty[$ e $CD_f = [-\frac{3}{4}, +\infty[$.

d) O estudante deverá através da função inversa da $f(x)$, obtida no item anterior, calcular a imagem da função inversa para cada algarismo. Encontrando a palavra **CRIPTOGRAFAR**.

e) Nesse item o estudante deverá primeiramente encontrar a função cifradora a partir de três pontos fornecidos dessa função. Como a função dessa atividade é uma função quadrática, basta montar um sistema de equações substituindo os pontos na função $f(x) = ax^2 + bx + c$.

$$\begin{cases} a + b + c = 5 \\ 9a + 3b + c = 25 \\ 16a + 4b + c = 44 \end{cases} \Rightarrow a = 3,\ b = -2 \text{ e } c = 4$$

Portanto a função cifradora é $f(x) = 3x^2 - 2x + 4$ e sua inversa é $f^{-1}(x) = \frac{2+\sqrt{-44+12x}}{6}$. Calculando a imagem da função inversa para cada algarismo, obtemos a palavra: **BRASILIA**.

3.3 Atividade 3

Objetivo Geral

Explorar o conceito da função exponencial e logarítmica na criptografia, visando uma aprendizagem contextualizada e significativa utilizando o como recurso didático a calculadora.

Objetivo Específico

- Calcular a imagem de um elemento do domínio da função exponencial.
- Calcular a imagem de um elemento do domínio da função logarítmica.
- Definir uma função exponencial e logarítmica.
- Analisar e determinar o domínio, contradomínio e imagem da função exponencial.
- Analisar, construir, ler e interpretar gráficos da função exponencial e logarítmica.
- Resolver problemas que envolvam o conceito de função exponencial e logarítmica.

Público alvo

Estudantes do 1º ano do ensino médio de acordo com os Parâmetros Curriculares Nacionais (PCN).

Estratégias para aplicação da atividade

O professor faz uma breve explicação do que é criptografia, da sua importância ao longo da história e na atualidade. Em seguida, explica a situação do texto e os estudantes responderão as atividades. Ao final, os estudantes se reúnem em grupos para trocar funções e mensagens para verificar se os colegas conseguem decodificá-las. Nesse momento, a calculadora é um recurso que contribui para realizar os cálculos envolvendo exponenciais e logaritmos. Caso os alunos não saibam manipular a calculadora científica, o professor tem um momento oportuno para orientar os estudantes quanto ao seu uso.

Atividade 3: Função Exponencial e Logarítmica

Alguns sistemas de códigos são criptografados com o uso de funções matemáticas. Para cifrar e decifrar uma mensagem deve-se seguir os seguintes procedimentos:

Passo 1: Crie uma mensagem a ser enviada.

Passo 2: Relacione cada letra do alfabeto, conforme a tabela a seguir:

A -12	B -11	C -10	D -9	E -8	F -7	G -6	H -5	I -4	J -3	K -2	L -1	M 0	N 1	O 2	P 3	Q 4	R 5	S 6	T 7	U 8	V 9	W 10	X 11	Y 12	Z 13

Passo 3: Cifre a mensagem, utilizando a função cifradora $f(x) = 2^x$. A mensagem a ser transmitida são as imagens da função f.

Passo 4: Decodifique a mensagem calculando as imagens através da função inversa. Como a função cifradora é uma função exponencial, teremos como função inversa a função logarítmica. Nesse momento a calculadora é um recurso que contribui para realizar os cálculos.

De acordo com os dados apresentados e com os conhecimentos relativos a funções exponenciais e logarítmicas, resolva os itens subsequentes, utilizando a calculadora científica caso necessário.

a) Cifre a mensagem **DEIXE A MATEMÁTICA ENTRAR NA SUA VIDA.**

b) Mostre que a inversa da função exponencial é a função logarítmica.

c) Decodifique a mensagem.

$$\frac{1}{1024}; 4; 2; 128; \frac{1}{16}; 2; 256; \frac{1}{256}; 64; \frac{1}{256}; \frac{1}{64}; 256; \frac{1}{16}; 2; \frac{1}{512};$$
$$4; \frac{1}{256}; 1; \frac{1}{128}; 32; \frac{1}{256}; 2; 128; \frac{1}{256}.$$

d) Determine os gráficos da função cifradora e decodificadora, observando que são funções inversas.

e) Crie uma mensagem e uma função cifradora e codifique a sua mensagem através do procedimento do texto e envie para um grupo decodificá-la.

Solução comentada

a) Nesse item, o estudante vai consultar a tabela indicada no passo 2 e calcular as imagens pela função $f(x) = 2^x$. Seguem os cálculos:

Letra	**Sequência numérica**	**Imagem da função $f(x) = 2^x$**
D	-9	$f(x) = 2^x = 2^{-9} = \frac{1}{512}$
E	-8	$f(x) = 2^x = 2^{-8} = \frac{1}{256}$
I	-4	$f(x) = 2^x = 2^{-4} = \frac{1}{16}$
X	11	$f(x) = 2^x = 2^{11} = 2048$
A	-12	$f(x) = 2^x = 2^{-12} = \frac{1}{4096}$
M	0	$f(x) = 2^x = 2^0 = 1$
T	7	$f(x) = 2^x = 2^7 = 128$
C	-10	$f(x) = 2^x = 2^{-10} = \frac{1}{1024}$
N	1	$f(x) = 2^x = 2^1 = 2$
R	5	$f(x) = 2^x = 2^5 = 32$
S	6	$f(x) = 2^x = 2^6 = 64$
U	8	$f(x) = 2^x = 2^8 = 256$
V	9	$f(x) = 2^x = 2^9 = 512$

A mensagem cifrada é

$$\frac{1}{512}; \frac{1}{256}; \frac{1}{16}; 2048; \frac{1}{256}; \frac{1}{4096}; 1; \frac{1}{4096}; 128; \frac{1}{256}; 1; \frac{1}{4096}; 128; \frac{1}{16}; \frac{1}{1024}; \frac{1}{4096};$$
$$\frac{1}{256}; 2; 128; 32; \frac{1}{4096}; 32; 2; \frac{1}{4096}; 64; 256; \frac{1}{4096}; 512; \frac{1}{16}; \frac{1}{512}; \frac{1}{4096}.$$

b) Nesse item, o estudante deve primeiramente mostrar que a função exponencial admite inversa.

Dada uma função $f : A \to B$, essa função só terá inversa se f for uma função bijetora, ou seja, injetora e sobrejetora ao mesmo tempo.

Considere a função exponencial, $f(x) = a^x$, onde a base a é um número positivo e diferente de 1, definida para todo x real.

Observe que nestas condições, a^x é um número positivo, para todo $x \in \mathbb{R}$, onde $\mathbb{R}$ é o conjunto dos números reais.

Denotando o conjunto dos números reais positivos por $\mathbb{R}_+^*$, poderemos escrever a função exponencial como segue: $f : \mathbb{R} \to \mathbb{R}_+^*; f(x) = a^x$, com $0 < a \neq 1$.

Função exponencial é bijetora, pois:

i) É injetora, ou seja: elementos distintos possuem imagens distintas.

ii) É sobrejetora, pois o conjunto imagem coincide com o seu contradomínio.

Portanto, a função exponencial, admite uma função inversa.

Agora os estudantes podem calcular a função inversa de $f(x) = a^x$.

$$f(x) = a^x \Rightarrow y = a^x \Rightarrow \log_{=} \log_a^{a^x} \Rightarrow \log_a^y = x \Rightarrow f^{-1}(x) = \log_a^x$$

Logo, a função exponencial é a inversa da função logarítmica e vice-versa.

c) Nesse item, o estudante deverá encontrar a função inversa da $f(x)$, obtendo a $f^{-1}(x) = \log_2^x$ e calcular a imagem da função inversa para cada valor recebido.

Valor recebido	**Imagem da inversa**	**Letra encontrada**
$\frac{1}{1024}$	$f^{-1}(x) = \log_2^x = \log_2^{\frac{1}{1024}} = -10$	C
4	$f^{-1}(x) = \log_2^x = \log_2^4 = 2$	O
2	$f^{-1}(x) = \log_2^x = \log_2^2 = 1$	N
128	$f^{-1}(x) = \log_2^x = \log_2^{128} = 7$	T
$\frac{1}{16}$	$f^{-1}(x) = \log_2^x = \log_2^{\frac{1}{16}} = -4$	I
256	$f^{-1}(x) = \log_2^x = \log_2^{256} = 8$	U
$\frac{1}{256}$	$f^{-1}(x) = \log_2^x = \log_2^{\frac{1}{256}} = -8$	E
64	$f^{-1}(x) = \log_2^x = \log_2^{64} = 6$	S
$\frac{1}{64}$	$f^{-1}(x) = \log_2^x = \log_2^{\frac{1}{64}} = -6$	G
$\frac{1}{512}$	$f^{-1}(x) = \log_2^x = \log_2^{\frac{1}{512}} = -9$	D
1	$f^{-1}(x) = \log_2^x = \log_2^1 = 0$	M
$\frac{1}{128}$	$f^{-1}(x) = \log_2^x = \log_2^{\frac{1}{128}} = -7$	F
32	$f^{-1}(x) = \log_2^x = \log_2^{32} = 25$	R

Encontrando a mensagem **CONTINUE SEGUINDO EM FRENTE**.

d) Se (a, b) for um ponto no gráfico $y = f(x)$, então $b = f(a)$. Isto é equivalente à afirmativa que $a = f^{-1}(b)$, a qual significa que (b, a) é um ponto no gráfico de $y = f^{-1}(x)$. Em resumo, inverter as coordenadas de um ponto no gráfico de f produz um ponto no gráfico de f^{-1}. Analogamente inverter as coordenadas de um ponto no gráfico de f^{-1} produz um ponto no gráfico de f. Contudo, o efeito geométrico de inverter as coordenadas de um ponto é refletir aquele ponto sobre a reta $y = x$.

Isto implica que o gráfico (figura 5) de $y = 2^x$ e o de $y = \log_2^x$ são reflexões um do outro, em relação à reta $y = x$.

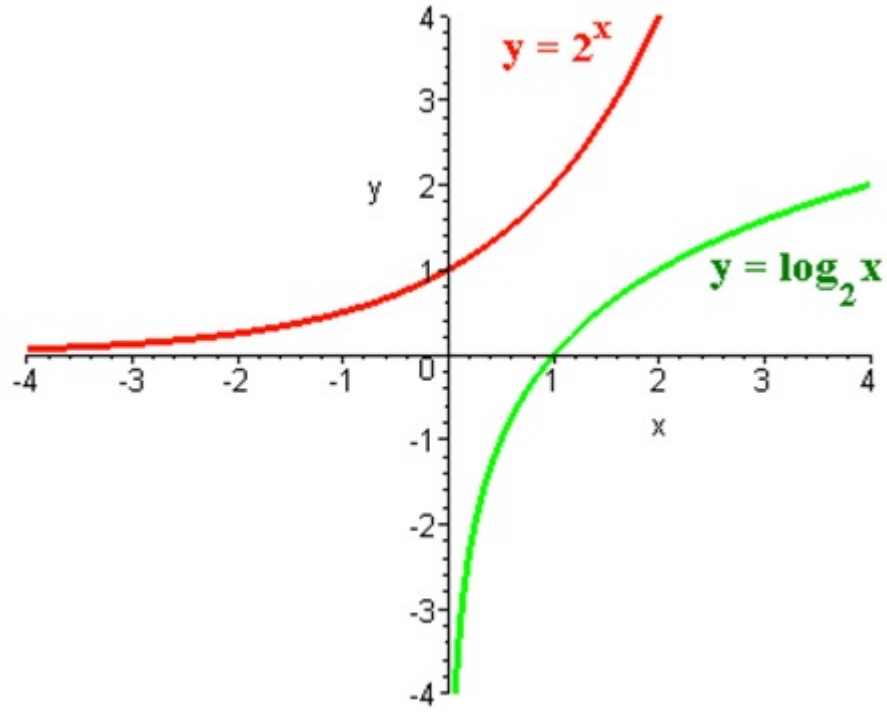


Figura 3.1: Gráfico da função Exponencial e Logarítmica.

3.4 Atividade 4

Objetivo Geral

Explorar o conceito de Matrizes na criptografia, visando uma aprendizagem contextualizada e significativa.

Objetivo Específico

- Desenvolver o conceito de matriz.
- Interpretar e realizar operações com matrizes.
- Reconhecer e aplicar as propriedades das operações com matrizes.
- Determinar a matriz inversa de uma matriz dada.
- Relacionar matrizes com a codificação e decodificação de mensagens.

Público alvo

Estudantes do 2º ano do ensino médio de acordo com os Parâmetros Curriculares Nacionais (PCN).

Estratégias para aplicação da atividade

O professor faz uma breve explicação do que é criptografia, da sua importância ao longo da história e na atualidade. Em seguida, explica a situação do texto e os estudantes responderão as atividades. Ao final, os estudantes se reúnem em grupos para trocar matrizes e mensagens para verificar se os colegas conseguem decodificá-las.

Atividade 4 : Matrizes

Para cifrar uma mensagem evitando a análise de frequência sobre o texto cifrado, utilizamos uma técnica que envolve a multiplicação de matrizes.

Observe a situação hipotética apresentada a seguir:

Maria quer enviar uma mensagem criptografada para João e combinaram previamente a utilização da matriz codificadora $A = \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}$, que servirá como chave para codificação e decodificação.

Para Maria transmitir a mensagem "**OS NÚMEROS GOVERNAM O MUNDO**", ela deve montar uma matriz mensagem $M_{2\times n}$ (2 linhas e n colunas, onde n depende da quantidade de letras do texto a ser cifrado), dispondo a sequência numérica,

de acordo com a tabela de pré-codificação indicada abaixo, associada em colunas e repetindo a última letra do texto, caso o mesmo tenha uma quantidade ímpar de letras.

Tabela para pré-codificação:

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

Mensagem	**O**	**S**	**N**	**U**	**M**	**E**	**R**	**O**	**S**	**G**	**O**	**V**	**E**	**R**	**N**	**A**	**M**	**O**	**M**	**U**	**N**	**D**	**O**
Sequência numérica	15	19	14	21	13	5	18	15	19	7	15	22	5	18	14	1	13	15	13	21	14	4	15

Sendo assim, Maria monta a matriz mensagem $M_{2\times 12}$:

$$M = \begin{bmatrix} 15 & 14 & 13 & 18 & 19 & 15 & 5 & 14 & 13 & 13 & 14 & 15 \\ 19 & 21 & 5 & 15 & 7 & 22 & 18 & 1 & 15 & 21 & 4 & 15 \end{bmatrix}$$

Em seguida, Maria calcula o produto $A \cdot M$:

$$A \cdot M = \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 15 & 14 & 13 & 18 & 19 & 15 & 5 & 14 & 13 & 13 & 14 & 15 \\ 19 & 21 & 5 & 15 & 7 & 22 & 18 & 1 & 15 & 21 & 4 & 15 \end{bmatrix}$$

$$= \begin{bmatrix} 83 & 84 & 49 & 84 & 71 & 89 & 51 & 44 & 69 & 81 & 50 & 75 \\ 34 & 35 & 18 & 33 & 26 & 37 & 23 & 15 & 28 & 34 & 18 & 30 \end{bmatrix} = C$$

Maria obtém a matriz $C_{2\times 12}$, que é a matriz que fornece a mensagem cifrada.

Portanto, a mensagem cifrada, que será enviada para João, é **83-34-84-35-49-18-84-33-71-26-89-37-51-23-44-15-69-28-81-34-50-18-75-30**.

Para reverter o processo (decodificar) e obter a mensagem original, João deve recuperar a matriz mensagem $M_{2\times 12}$, através do seguinte processo:

$$AM = C \Rightarrow A^{-1}(AM) = A^{-1}C \Rightarrow (A^{-1}A)M = A^{-1}C \Rightarrow M = A^{-1}C$$

Para calcular a matriz inversa A^{-1}, João pode aplicar o processo prático, onde dado a matriz codificadora $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, temos que:

$$A^{-1} = \frac{1}{detA} \cdot \begin{bmatrix} \text{d} & \text{-b} \\ \text{-c} & \text{a} \end{bmatrix}, \text{ com } \det A = ad - cd \neq 0$$

$$\text{Como } C = \begin{bmatrix} 83 & 84 & 49 & 84 & 71 & 89 & 51 & 44 & 69 & 81 & 50 & 75 \\ 34 & 35 & 18 & 33 & 26 & 37 & 23 & 15 & 28 & 34 & 18 & 30 \end{bmatrix}, \text{ segue que:}$$

$$A^{-1}C = \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix} \cdot \begin{bmatrix} 83 & 84 & 49 & 84 & 71 & 89 & 51 & 44 & 69 & 81 & 50 & 75 \\ 34 & 35 & 18 & 33 & 26 & 37 & 23 & 15 & 28 & 34 & 18 & 30 \end{bmatrix}$$

$$= \begin{bmatrix} 15 & 14 & 13 & 18 & 19 & 15 & 5 & 14 & 13 & 13 & 14 & 15 \\ 19 & 21 & 5 & 15 & 7 & 22 & 18 & 1 & 15 & 21 & 4 & 15 \end{bmatrix} = M$$

Logo, pela tabela de pré-codificação, João obtém a mensagem original "**OS NÚMEROS GOVERNAM O MUNDO**".

Com base na situação hipotética apresentada, resolva os itens subsequentes:

a) Cifre a mensagem **UM SORRISO VALE MAIS QUE MIL PALAVRAS**, usando a matriz codificadora $A = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix}$

b) Calcule a matriz inversa da matriz codificadora do item a).

c) Decodifique a mensagem **18-53-41-105-15-42-11-28-41-104-39-102-39-98-57-152-31-84-44-116-29-82**, usando a matriz codificadora do item a).

d) Crie uma matriz codificadora de ordem 2 e codifique uma mensagem. Agora, envie a mensagem e a matriz codificadora para um dos grupos e peça para decodificar.

Solução comentada

a) Nesse item, o estudante vai consultar a tabela de pré-codificação e montar a matriz mensagem $M_{2\times 16}$.

$$M = \begin{bmatrix} 21 & 19 & 18 & 9 & 15 & 1 & 5 & 1 & 19 & 21 & 13 & 12 & 1 & 1 & 18 & 19 \\ 13 & 15 & 18 & 19 & 22 & 12 & 13 & 9 & 17 & 5 & 9 & 16 & 12 & 22 & 1 & 19 \end{bmatrix}$$

Em seguida, calcula o produto $A \cdot M$:

$$A \cdot M = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} \cdot \begin{bmatrix} 21 & 19 & 18 & 9 & 15 & 1 & 5 & 1 & 19 & 21 & 13 & 12 & 1 & 1 & 18 & 19 \\ 13 & 15 & 18 & 19 & 22 & 12 & 13 & 9 & 17 & 5 & 9 & 16 & 12 & 22 & 1 & 19 \end{bmatrix}$$

$$= \begin{bmatrix} 55 & 53 & 54 & 37 & 52 & 14 & 23 & 11 & 55 & 47 & 35 & 40 & 14 & 24 & 37 & 57 \\ 144 & 140 & 144 & 102 & 141 & 41 & 64 & 32 & 146 & 120 & 92 & 108 & 41 & 71 & 93 & 152 \end{bmatrix} = C$$

Portanto a mensagem cifrada é **55-144-53-140-54-144-37-102-52-141-14-41-23-64-11-32-55-146-47-120-35-92-40-108-14-41-24-71-37-93-57-152**.

b) Primeiramente, o estudante calcula o determinante da matriz $A = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix}$

$\det A = 2 \cdot 3 - 5 \cdot 1 = 1 \neq 0$, como det$\neq 0$, a matriz A possui inversa.

Agora, aplicando o processo apresentado no texto temos:

$$A^{-1} = \frac{1}{detA} \cdot \begin{bmatrix} \text{d} & \text{-b} \\ \text{-c} & \text{a} \end{bmatrix} = \frac{1}{1} \cdot \begin{bmatrix} 3 & \text{-1} \\ \text{-5} & 2 \end{bmatrix} = \begin{bmatrix} 3 & \text{-1} \\ \text{-5} & 2 \end{bmatrix}$$

Logo, $A^{-1} = \begin{bmatrix} 3 & \text{-1} \\ \text{-5} & 2 \end{bmatrix}$.

c) Nesse item, o estudante deverá reverter o processo de codificação fazendo o produto da matriz inversa, do item a, pela matriz codificada C, obtendo a matriz mensagem $M (M = A^{-1}C)$.

$$A^{-1}C = \begin{bmatrix} 3 & \text{-1} \\ \text{-5} & 2 \end{bmatrix} \cdot \begin{bmatrix} 18 & 41 & 15 & 11 & 41 & 39 & 39 & 57 & 31 & 44 & 29 \\ 53 & 105 & 42 & 28 & 104 & 102 & 98 & 152 & 84 & 116 & 82 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 18 & 3 & 5 & 19 & 15 & 19 & 19 & 9 & 16 & 5 \\ 16 & 5 & 9 & 1 & 3 & 9 & 1 & 19 & 13 & 12 & 19 \end{bmatrix} = M$$

Agora basta, consultar a tabela de pré-codificação, obtendo a mensagem decodificada **APRECIE AS COISAS SIMPLES**.

3.5 Atividade 5

Objetivo Geral

Explorar conceitos matemáticos com a Linguagem Braille e aplicar técnicas básicas de contagem de forma contextualizada e significativa.

Objetivo Específico

- Aplicar o princípio fundamental da contagem.
- Combinações simples.
- Número de subconjuntos.

Público alvo

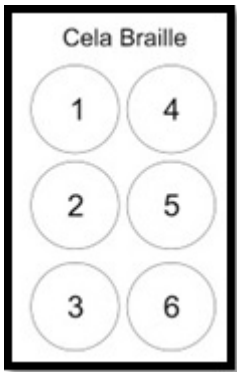
Estudantes do 3º ano do ensino médio de acordo com os Parâmetros Curriculares Nacionais (PCN).

Estratégias para aplicação da atividade

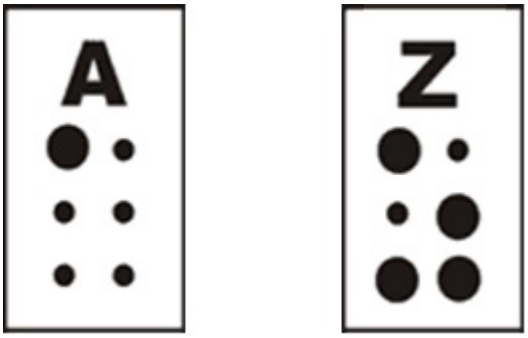
O professor deve pedir para os estudantes pesquisarem sobre o tema observando a sua relevância na nossa sociedade, pois, além de um exercício de aprendizado de criptografia, tal atividade terá um caráter conscientizador, possibilitando que os alunos compreendam a importância de se criar recursos para os portadores de necessidades especiais. Deve-se iniciar a discussão a respeito do número de configurações obtidas no sistema Braille usual 3x2. Nesse momento, o professor, deve evidenciar que cada um dos seis pontos do sistema usual pode ser marcado ou não. Feita essa análise, o professor sugere aos estudantes que resolvam a atividade proposta podendo explorar estratégias diferentes para cada solução.

Atividade 5. A escrita Braille

A escrita Braille é um código que possibilita a comunicação entre as pessoas que conhecem seu funcionamento, sendo o sistema de leitura e escrita mais utilizado pelos deficientes visuais em todo mundo. Esse método tátil consiste em pontos em relevo, dispostos de maneiras diferentes para cada letra do alfabeto, números, símbolos e pontuação. A unidade de leitura onde são assinalados os pontos para representar cada algarismo é denominada CELA. O código Braille é baseado em um arranjo 3x2 de pontos, dispostos em celas, como ilustra a figura abaixo:



Para registrar uma dada letra do alfabeto, alguns desses 6 pontos são marcados ou perfurados, de modo a se tornarem sobressalentes, para que possam ser sentidos com as pontas dos dedos das mãos. Observe as figuras, onde estão representadas duas letras do nosso alfabeto:



Na letra "A" somente o ponto de número 1 foi marcado na cela, enquanto que na letra "Z" foram marcados os pontos 1, 3, 5 e 6 na cela.

Com base no texto, faça o que se pede nos itens a seguir:

a) Calcule o número de configurações que podemos obter na linguagem Braille usual 3x2, utilizando apenas uma cela.

b) Considerando que temos que codificar todas as letras minúsculas e maiúsculas do alfabeto português, todos os algarismos arábicos, 5 símbolos de pontuação e 4 sinais de operação matemáticas, podemos afirmar que utilizando apenas uma cela 3x2 é o suficiente para representar todos esses códigos.

c) Utilizando o mesmo procedimento da linguagem Braille, calcule o número de configurações com um arranjo 3x4.

d) Em um código Braille com um arranjo 3x4, determine o número de configurações que possuem exatamente 5 pontos marcados.

Solução comentada

a) Nesse item, o estudante pode aplicar o princípio fundamental da contagem, onde para a primeira casa há duas possibilidades (ou pode ser marcada ou ficar em branco) e do mesmo modo há duas possibilidades para cada uma das outras cinco casas restantes, o que resulta em:

$$2 \times 2 \times 2 \times 2 \times 2 \times 2 = 2^6 = 64$$

Esse exercício é uma boa oportunidade para o professor mostrar uma aplicação de combinação simples:

Número de pontos marcados	**Quantidade de combinações**
0	$C_{6,0} = \frac{6!}{0!6!} = 1$
1	$C_{6,1} = \frac{6!}{1!6!} = 6$
2	$C_{6,2} = \frac{6!}{2!6!} = 15$
3	$C_{6,3} = \frac{6!}{3!6!} = 20$
4	$C_{6,4} = \frac{6!}{4!6!} = 15$
5	$C_{6,5} = \frac{6!}{5!6!} = 6$
6	$C_{6,6} = \frac{6!}{6!6!} = 1$
Total	64

O professor poderá informar que esse é o mesmo raciocínio para determinar o número total de subconjuntos de $\{1, 2, 3, \ldots, n\}$. Como cada elemento do conjunto pode estar ou não no subconjunto, segue pelo princípio fundamental da contagem que o número total de subconjuntos de $\{1, 2, 3, \ldots, n\}$ é $2 \times 2 \times 2 \times \ldots \times 2 = 2^n$.

b) De acordo com o item, temos que codificar:

Códigos	Frequência
Letras minúsculas	26
Letras maiúsculas	26
Algarismos arábicos	10
Símbolos de pontuação	5
Sinais de operação	4
Total	71

Como, pelo item anterior, temos um total de 64 configurações que pode ser obtidas usando arranjos 3x2, podemos concluir que não é o suficiente para representar todos esses códigos. Isso explica porque no código Braille para representar os algarismos, as letras maiúsculas e alguns símbolos têm que criar códigos com duas ou mais celas.

c) Nesse item, o estudante deve observar que para um arranjo 3x4 temos um total de 12 casas. Aplicando o princípio fundamental da contagem, onde para a primeira casa há duas possibilidades (ou pode ser marcada ou ficar em branco) e do mesmo modo há duas possibilidades para cada uma das outras onze casas restantes, o que resulta em:

$$2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 = 2^{12} = 4096$$

d) Nesse item, basta aplicar uma combinação simples, pois temos doze pontos disponíveis e devemos escolher exatamente 5 desses pontos não importando a ordem da escolha.

$$C_{12,5} = \frac{12!}{5!7!} = 792$$

Considerações Finais

Em virtude dos fatos mencionados, percebemos que a criptografia possui um amplo potencial para enriquecer o ensino da matemática no Ensino Médio e despertar o interesse do estudante, por esse tema estar muito presente no cotidiano. Isto provoca a curiosidade e aguça a imaginação dos estudantes.

As atividades didáticas apresentadas envolvendo códigos possibilitam os estudantes a trabalhar o conceito de criptografia aliados aos conteúdos de matemática do Ensino Médio tornando possível desenvolver estratégias de resolução de problemas. Para o professor, as atividades, são sugestões para revisar, exercitar e aprofundar os conteúdos de Funções Afins, Funções Quadráticas, Funções Exponenciais, Funções Logarítmicas, Matrizes e Análise Combinatória, de forma contextualizada, retirando a matemática do isolamento didático que tradicionalmente temos no contexto escolar.

É imprescindível que, diante dos argumentos expostos, todos os professores de matemática se conscientizem da importância do tratamento da informação como uma ferramenta facilitadora para o ensino da matemática, de modo que, os estudantes construam conhecimentos e desenvolvam aprendizagens sobre os conteúdos matemáticos de forma contextualizada e significativa.

Referências

[1] Alecrim, e., *História e Aplicações da Criptografia, 2005* , Disponível em: $<$ $http://www.infowester.com/criptografia.php>$. Acesso em: 10 de maio 2014.

[2] Buchmann, j., *Introdução a Criptografia*, 1ª ed.,Editora Berkeley, São Paulo-SP, 2002.

[3] BRASIL, MEC/SEF., *Parâmetros Curriculares Nacionais: Matemática*, Brasília, 1997.

[4] Carvalho, p.c.p., *Métodos de Contagem e Probabilidade, Programa de Iniciação Científica da OBMEP, Vol. 2*, 2ª ed.,OBMEP, 2012.

[5] Castillo, c.i., *"Curvas Elípticas"* , Disponível em: $<$ $http://www.portaldoconhecimento.gov.cv/bitstream/10961/2253/1/MONOGRA\_-FIA.pdf>$. Acesso em 10 de maio 2014.

[6] Costa, c.j.,et al., *Criptografia Geral*, Centro de Estudos de Pessoal, 2005.

[7] Coutinho, s.c., *Números inteiros e Criptografia RSA. Série de Computação e Matemática n. 2.*, 2ª ed., Rio de Janeiro: IMPA e SBM, 2000.

[8] Coutinho, s.c., *Criptografia. Programa de Iniciação Científica da OBMEP, Vol. 7.*, OBMEP, 2008.

[9] Fiarresga, v.m.c., *Criptografia e Matemática. Dissertação (Mestrado em Matemática para Professores)*, Universidade de Lisboa, Lisboa, 2010. Disponível em: $<$ $http://repositorio.ul.pt/bitstream/10451/3647/1/ulfc055857\_tm\_Victor\_Fiarres-ga.pdf>$. Acesso em 10 de maio 2014.

[10] Lemos, m., *Criptografia, Números Primos e Algoritmos*, Disponível em: $< http : //www.impa.br/opencms/pt/biblioteca/pm/PM\_04.pdf >$. Acesso em 10 de maio 2014.

[11] Santos, j.p.o., *Introdução à Teoria dos Números*, 3ª ed., Rio de Janeiro, IMPA, 2010.

[12] Singh, s., tradução de Jorge Calife, *O livro dos códigos.*, 6ª ed., Rio de Janeiro, Record, 2007.

[13] Stallings, w., traduzido por Daniel Vieira, *Criptografia e segurança de redes*, 4ª ed., São Paulo, Pearson Prentice Hall, 2008.

[14] Tamarozzi, a.c., *Codificando e Decifrando Mensagens*, Revista do professor de matemática, volume 45, SBM, p. 41-47, 2001.