

Universidade Federal da Bahia - UFBA
Instituto de Matematica - IM
Sociedade Brasileira de Matematica - SBM
Mestrado Profissional em Matemática em Rede Nacional - PROFMAT
Dissertação de Mestrado

A Arte de Cifrar, Criptografar, Esconder e Salvaguardar como Fontes Motivadoras para Atividades de Matemática Básica

José Luiz dos Santos

Salvador - Bahia
Abril de 2013

A Arte de Cifrar, Criptografar, Esconder e Salvaguardar como Fontes Motivadoras para Atividades de Matemática Básica

José Luiz dos Santos

Dissertação de Mestrado apresentada à Comissão Acadêmica Institucional do PROFMAT-UFBA como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Vinícius Moreira Mello.

Salvador - Bahia
Abril de 2013

A Arte de Cifrar, Criptografar, Esconder e Salvaguardar como Fontes Motivadoras para Atividades de Matemática Básica

José Luiz dos Santos

Dissertação de Mestrado apresentada à Comissão Acadêmica Institucional do PROFMAT-UFBA como requisito parcial para obtenção do título de Mestre em Matemática, aprovada em 04 de abril de 2013.

Banca Examinadora:

Prof. Dr. Vinícius Moreira Mello (Orientador)
UFBA

Prof. Dr. Perfilino Eugênio Ferreira Junior
UFBA

Prof. Dr. Marcelo Miranda Viana da Silva
IMPA

À Deus . . .

. . . por manter-me saudável e com discernimento.

À minha companheira Alexandra . . .

. . . pelos muitos momentos de compreensão, paciência, incentivo e carinho.

À minha prole, José Luiz, Jonathan Luiz, Julia Lis e Juliana Lis . . .

. . . por serem minhas eternas fontes de motivação.

Agradecimentos

Agradeço a todos que acreditaram e que tornaram possível a realização do PROFMAT, que tem resgatado parte da motivação e dignidade dos professores de matemática do ensino básico do Brasil.

Agradeço ao Professor Vinícius Mello pelas orientações claras e precisas.

Agradeço à coordenação e aos professores do PROFMAT/UFBA, pelo empenho e dedicação, o que evidencia vosso compromisso com este programa de mestrado.

Particularmente, agradeço o apoio recebido do Colégio Militar de Salvador, principalmente da tenente Patrícia e do sargento Gomes que me disponibilizaram todos os recursos da biblioteca Olavo Bilac.

"Existe um paralelismo fiel entre o progresso social e a atividade matemática: os países socialmente atrasados são aqueles em que a atividade matemática é nula ou quase nula."(Jacques Chapellon)

Resumo

Tomando por base o enredo da criptografia, este trabalho começa abordando os principais conceitos desta ciência através de um contexto histórico, enfatizando sua influência no atual desenvolvimento da ciência e da tecnologia.

Devido a sua base matemática, explora-se três técnicas criptográficas que aplicam os conceitos de função, análise combinatória, matrizes e aritmética modular como ferramentas.

Aplica-se o conceito de função em cifras de substituição e transposição; utiliza-se o conceito de desordenamento para determinar a quantidade de chaves de uma cifra de substituição monoalfabética; e aplica-se os conceitos de matriz e aritmética modular para explicar o funcionamento da cifra de Hill.

Finalmente, são propostas dez atividades, fundamentadas na técnica de resolução de problemas, que abordam os conceitos de função, análise combinatória e matrizes, tendo como fonte motivadora a arte de cifrar, criptografar, esconder e salvaguardar.

Palavras-chave: Criptografia; Ensino de funções; Ensino de Análise Combinatória; Ensino de matrizes; Aritmética modular.

Abstract

Using the "Art and Science of Enciphering, Encrypting, Hiding, and Safeguarding"as a source of inspiration, this work begins with the key concepts of this science through a historical context, emphasizing its influence on the current development of science and technology. We explore three cryptographic techniques that apply the concepts of function, combinatorics, matrices and modular arithmetic as tools: substitution, transposition and Hill cyphers. Finally, ten activities motivated by cryptography, dealing with the concepts of function, combinatorics and matrices, and based on problem solving techniques are proposed.

Keywords: Cryptography, Teaching functions; Teaching Combinatorial Analysis, Teaching matrices; Modular Arithmetic.

Conteúdo

Capítulo 1

Introdução

Desde o surgimento da espécie humana que a necessidade de comunicação se tornou imprescindível, fosse para alertar sobre algum perigo ou expressar sua cultura ou sentimento. A evolução da comunicação acompanha a evolução biológica e social do homem que está dividida em Pré-História, período anterior à invenção da escrita que data de aproximadamente 5.000 a.C. e História.

A transição da Pré-história para a História se dá por volta de 4.000 a.C. Os historiadores aceitam como certo o aparecimento da escrita na Mesopotâmia e no Egito.

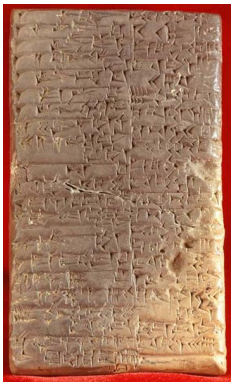


Figura 1.1: A escrita cuneiforme é o primeiro documento escrito que se tem registro.

Se o surgimento da escrita marca o início da história, a invenção da técnica de imprimir ilustrações, símbolos e a própria escrita, promove a pos-

sibilidade de tornar a informação acessível a um número cada vez mais crescente de pessoas, alterando assim o modo de viver e de pensar da sociedade.

Passamos por grandes invenções, como o jornal, que data o seu primeiro exemplar de 59 a.C., em Roma, publicado por Julio César, com o intuito de informar o público sobre os mais importantes acontecimentos sociais e políticos e que, até hoje, tem a mesma função.

A invenção do rádio, com sua primeira transmissão datada de 1.900, foi um marco na história, pois ao contrário do jornal, as ondas do rádio tinham um alcance e velocidade muito superiores. O passo seguinte foi o surgimento da televisão, em 1924, que era a junção dos componentes gráficos de um jornal, como imagens e figuras, com os componentes de áudio do rádio.

Na Era da Tecnologia o computador é o principal elemento, pois no início, em 1943, ele era uma máquina gigantesca, de cálculos, que ocupava uma sala inteira, passando por transformações até que em 1971, surgiu o primeiro microcomputador. Andando lado a lado com a evolução dos computadores, está a Internet, que foi desenvolvida em 1969, para fins militares, na época da Guerra Fria. Não passava de um sistema de comunicação entre as bases militares dos EUA, e tinha o nome de ArpaNet.

Atualmente, a troca de informações através da Internet e de meios móveis tornou-se imprescindível na vida de todos nós. Paralelamente a evolução na forma de trocar informações, está a necessidade de, muitas vezes, fazê-la de forma segura de modo a salvaguardar informações pessoais ou até mesmo segredos de estado ou corporativos.

Historicamente, reis, rainhas e generais dependeram de comunicações eficientes de modo a governar seus reinos e comandar seus exércitos. A habilidade de disfarçar uma mensagem de forma que somente o destinatário possa acessá-la foi motivada pela ameaça de interceptação pelo inimigo. Comandantes militares precisam transmitir ordens a seus comandados sem que o inimigo tome conhecimento da mesma, o que acabaria com a principal arma de um combate, a surpresa.

Líderes políticos precisam trocar informações com seus aliados; as instituições financeiras e as empresas necessitam transmitir informações sigilosas a suas filiais. Existe uma grande variedade de transações que envolvem dinheiro que são feitas de maneira eletrônica, desde compras por cartão de crédito via internet a saques em caixas eletrônicos. A informação referente

a estas transações seguem por linha telefônica ou redes de alta velocidade e estão facilmente sujeitas à escutas. A interconexão dos sistemas informatizados nos leva a um maior cuidado com os ataques em rede, pois a tentativa de acesso indevido a informações sigilosas pode vir de pessoas fisicamente distantes dos sistemas onde a informação está armazenada.

A arte de cifrar, criptografar, esconder e salvaguardar uma informação para transmiti-la de forma que somente o destinatário possa compreendê-la, evitando que seu conteúdo se torne público, é uma preocupação histórica e, ao mesmo tempo, cotidiana. Os processos pelos quais informações enviadas eletronicamente são codificadas dependem, essencialmente, do uso da matemática, mais especificamente da teoria dos números, que é a área da matemática mais utilizada nas aplicações à criptografia. Questões referentes à aritmética modular, funções, matrizes, análise combinatória, são exemplos de assuntos do currículo básico da matemática que são aplicados na criptografia.

Um código envolve a substituição de uma palavra ou frase por uma palavra, um número ou um símbolo. Uma alternativa ao código é a cifra, uma técnica que age num nível mais fundamental, onde as letras, no lugar das palavras, são substituídas.

Da arte de esconder mensagens e permutar frases, a curvas elípticas e criptografia quântica, passando pela criação dos computadores, a história dos códigos, que possui relatos que datam da invenção da escrita, se desenvolveu através dos tempos em uma batalha entre seus criadores e seus decifradores, causando um forte impacto no curso da história da humanidade. Por isso, se fala que uma Terceira Guerra Mundial seria a guerra dos matemáticos, pois eles teriam o controle sobre a grande arma de guerra, a informação.

A importância desta ciência, tanto histórica como científica, não pode passar despercebida pelos currículos escolares, pois mostra de forma contextualizada, a forte ligação que há entre a história da humanidade e a evolução científica de nossa sociedade.

Neste trabalho, o tema criptografia é desenvolvido através de atividades didáticas que aliam conteúdos de matemática do ensino médio a este tema, possibilitando ao professor um trabalho com temas atuais e aos alunos o contato com tecnologias, entre elas a calculadora, tendo como fonte motivadora a arte de cifrar, criptografar, esconder e salvaguardar informações sigilosas. Para atingir este objetivo, no capítulo 2 serão trabalhados alguns conceitos básicos de criptografia, de forma cronológica e contextualizados com fatos

históricos. No capítulo 3, será trabalhado o ensino de funções aplicado a cifras de substituição e transposição, serão utilizadas técnicas de contagem para determinar o número de chaves em uma cifra de substituição monoalfabética e serão aplicadas as teorias sobre matrizes e aritmética modular ao resolver problemas envolvendo a cifra de Hill. No capítulo 4, estão propostas dez atividades que contemplam os conteúdos de função, análise combinatória e matrizes, voltados especificamente para aplicação direta em sala de aula, baseadas nas competências e habilidades constantes da matriz de referência do ENEM.

Capítulo 2

A Influência Histórica da Criptografia no Atual Desenvolvimento Científico e Tecnológico.

A escrita hieroglífica, compreensível apenas aos sacerdodes egípcios, que data de 2.000 a.C., é o primeiro indício histórico da preocupação do homem em tornar textos ininteligíveis. A escrita cuneiforme dos babilônios, ratifica esta tese.

Figura 2.1: Papiros Egípcios.

Porém, os primeiros relatos sobre escrita secreta datam de Heródoto, "o pai da História", que no século V antes de Cristo, em sua obra *"as Histórias"*, escreveu que foi a arte da escrita secreta que salvou a Grécia de ser conquistada por Xerxes, o déspota líder dos persas.

Xerxes passou cinco anos montando secretamente a maior força de combate da história, até que em 480 a.C. ele estava pronto para lançar um ataque surpresa sobre a Grécia. Contudo, os preparativos persas tinham sido teste-

munhados por Desmarato, um grego que vivia na Pérsia e que decidiu enviar uma mensagem para advertir os espartanos dos planos de Xerxes.

A estratégia de Desmarato para conseguir a comunicação secreta consistira em ocultar a mensagem. Para isso, raspara a cera de um par de tabuletas de madeira, escrevera a mensagem e a cobrira novamente com cera. Deste modo, as tabuletas pareceriam estar em branco e não causariam problemas com os guardas ao longo da estrada.

A mensagem chegou ao seu destino e cumpriu o seu objetivo, pois os gregos, ate então indefesos, se armaram e humilharam a esquadra persa em um contra ataque surpresa.

2.1 Escondendo Mensagens e os Primórdios da Arte de Criptografar e Salvaguardar.

A arte de esconder uma mensagem, sem nenhum tratamento para modificá-la, é uma técnica primitiva chamada $esteganografia$, que deriva do grego *Steganos*, coberto, e *graphia*, escrita.

Ainda em *"as Histórias"*, Heródoto relata a história de Histaeu, que para enviar uma mensagem secreta a Aristágora, raspou a cabeça de um mensageiro, escreveu a mensagem no couro cabeludo e esperou o cabelo crescer. O mensageiro, que aparentemente não levava nada que fosse perigoso, chegou ao destinatário e raspou a cabeça, revelando a mensagem.

Apesar de primitiva, a longevidade da $esteganografia$ demonstra que ela oferece uma certa segurança, entretanto trata-se de um procedimento sem fundamento científico. Durante a Segunda Guerra Mundial, agentes alemães que atuavam na América Latina, utilizaram uma técnica de transmissão de mensagem que consistia em microfilmar uma página de texto, reduzindo ao tamanho de um ponto. Este ponto era colocado sobre um ponto final de um documento aparentemente ostensivo. 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. A principal deficiência deste tipo de técnica é que caso a mensagem seja descoberta, poderá ser lida por qualquer pessoa.

Paralelamente ao desenvolvimento da $Esteganografia$, houve a evolução da $criptografia$, palavra derivada do grego, *kriptos*, que significa secreto, e *graphia*, escrita. A $criptografia$ utiliza o conceito de modificar a mensagem original através de processos sistematizados, chamados de *encriptação*, transformando-a em uma mensagem ininteligível.

Uma das formas de trocar mensagens criptografadas requer que transmissor e receptor conheçam o algoritmo utilizado para encriptar a mensagem e a chave utilizada. *Algoritmo* é um conjunto de procedimentos, em sequência organizada, para resolver determinado problema. Nesse caso, por exemplo, poderíamos substituir cada letra da mensagem original por outra, previamente estabelecida, que seria a *chave* do sistema de encriptação. Com isso, uma mensagem criptografada não é compreensível por outra pessoa que não o destinatário, ao qual caberia reverter o *algoritmo* de cifragem, utilizando a *chave* para recriar a mensagem original a partir do texto cifrado.

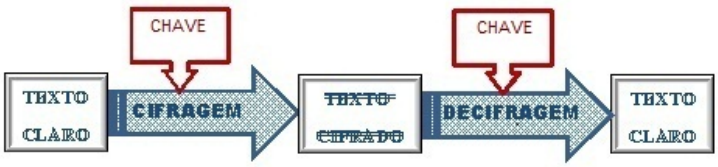


Figura 2.2: Cifragem de uma mensagem.

Apesar da distinção entre esteganografia e criptografia, é possível utilizar um sistema híbrido, onde uma mensagem é criptografada e o texto ininteligível é escondido, como no episódio em que um texto era transformado em um ponto, durante a segunda guerra mundial. Após a descoberta dos aliados, os alemães passaram a tomar a precaução extra de codificar a mensagem antes de microfilmá-la.

Como veremos a seguir, na criptografia clássica, desenvolvida antes do advento do computador, as cifras eram baseadas em apenas duas operações básicas, a transposição e a substituição.

2.2 A Vulnerabilidade da Criptografia Clássica e a Origem da Criptoanálise

Desde o momento em que a técnica de criptografar mensagens se tornou compreensível, a criptografia passou a utilizar dois métodos fundamentais: A *transposição*, que consiste em trocar a posição das letras da mensagem original, promovendo uma permutação das letras segundo um algoritmo e uma chave bem determinados; e a *substituição*, que tem por base a permutação do alfabeto, ou seja, trocar cada letra ou símbolo por outro.

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 destinatário. O formato do bastão seria a chave desta cifra.

Figura 2.3: O Bastão de Licurgo

Um método utilizado na Grécia Antiga, conforme descrito por Plutarco, em 90d.C., no livro *"Vida de homens ilustres"*, era a *Tabela Espartana*, que 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 MATEMÁTICA"em uma tabela com 5 colunas, utilizando a letra H no lugar do espaço, teríamos

o seguinte:

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

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

MARSL MAEDO IHATS OFOET ITHIN MECRP SAHMA

É usual separarmos o texto ininteligível em blocos de 5 letras. Quando a quantidade de letras do texto não for múltipla de 5, completa-se o último bloco do texto ininteligível com letras aleatórias.

O exemplo mais clássico do método da substituição é o chamado *Código de César*, utilizado pelo imperador Romano Júlio César (100 a 44 a.C.) em suas correspondências militares , que utilizava uma chave de substituição bastante elementar. Cada letra da mensagem original era substituída pela letra que ficava a três posições a frente no alfabeto. A tabela abaixo ilustra a ideia.

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 MESTRADO PROFISSIONAL EM MATEMÁTICA, cifrado pelo código de César, ficaria

PHVXUDGRKSURILVVLRQDOKHPKPDXHPDXLFD

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. Existe ainda outros dois tipos de códigos de substituição. A substituição *Homofônica*, onde um caractere pode ser substituído por mais de um caractere diferente e a substituição *Polialfabética*, que é a conjunção de várias cifras de substituição monoalfabética.

Nos dois exemplos acima, existem algumas possibilidades para o texto cifrado. No caso da tabela espartana, considerando apenas uma única forma de escrever o texto original e de tomar o texto ininteligível, teríamos 33 possibilidades, pois a tabela teria de 2 a 34 colunas, já que o texto tem 35 letras. Neste caso, não seria tão complicado testarmos todas as possibilidades até chegarmos a uma que fizesse sentido. Este tipo de tentativa de decifrar um texto, onde parte-se para a verificação de todas as chaves possíveis do código utilizado, chama-se *ataque de 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 se substituída por uma letra diferente dela mesma, teremos $26!(\frac{1}{0!}-\frac{1}{1!}+\frac{1}{2!}-\frac{1}{3!}+\cdots+\frac{1}{26!}) \cong 1,48\times10^{26}$ possibilidades de definir a chave deste código, que correspondem às permutações caóticas das 26 letras do alfabeto, o que torna bem mais complicado o ataque por força bruta. No capítulo 3 estudaremos as permutações caóticas com mais detalhes.

Por volta do ano de 750, apesar do desenvolvimento do povo árabe na área das ciências, a sua grande contribuição não foi na criptografia e sim na *criptoanálise*, ciência que permite decifrar uma mensagem sem conhecer a chave. Esta grande contribuição deve-se a *al-Kindy*, que em seu livro *"Escritos sobre a Decifração de Mensagens Criptográficas"*, definiu o método da *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. Obviamente que algumas suposições e avaliações sobre o texto cifrado ainda terão que ser feitas, mas a quantidade de tentativas diminui consideravelmente. Veja abaixo a tabela de frequência das letras de nosso alfabeto.

a	e	o	p , r , s	i , n	d , m , t	u , c , l	b , f , g , h , j , v , x , z
14,5%	13%	11,5%	8%	6%	5%	4,5%	Menor que 3%

Daí em diante, mesmo ficando explícita 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 moroso, 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 à 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 homofônica, 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 um exemplo de tabela para uma cifra homofônica.

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

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

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

Apesar da cifra homofônica 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 que 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 homofônica não atendeu totalmente às necessidades para uma comunicação simples e segura.

Um exemplo da utilização de uma cifra homofônica 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, qua consistia de uma cifra homofônica 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 *François Viéte* (1540 - 1603), que utilizou engenhosamente a análise de frequência.

Em desvantagem, a criptografia necessitava de uma cifra mais resistente aos ataques dos criptoanalistas. Para superar a fragilidade das cifras homofônicas, o arquiteto italiano *Leon Battista Alberti* criou, em 1470, a primeira cifra polialfabética, através dos *Discos de Alberti*. Esta foi a primeira ideia de mecanização dos processos de cifragem e decifragem.

Figura 2.4: Disco de Alberti

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 teríamos 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. Esta cifra não resistiu muito tempo ao ataque dos criptoanalistas e logo necessitou de um aperfeiçoamento.

Um aprofundamento da ideia de *Alberti* foi feito em 1523 pelo Diplomata Francês *Blaise de Vigenere* (1523 - 1596), publicado em seu livro de título *Tratado das Cifras*.

Esta cifra, conhecida como *Cifra de Vigenere*, tinha como ideia básica para cifrar uma mensagem, utilizar vários discos de Alberti simultaneamente conforme o tamanho de uma palavra chave. A posição inicial de cada disco é definida pelas letras da palavra chave que indica a correspondência com a letra A do disco externo.

Na realidade, ao invés de discos, a cifra de Vigenere utilizava como ferramenta uma matriz com um número de linhas e colunas igual ao número de símbolos utilizados no texto original. Veja abaixo uma tabela com o nosso alfabeto.

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

Figura 2.5: Tabela de Vigenere

Na primeira linha está o alfabeto para os símbolos do texto original e na primeira coluna o alfabeto para os símbolos da palavra chave. Cada letra do texto original é correspondida pelo alfabeto deslocado situado na mesma linha da letra da palavra chave, ordenadamente. Pela tabela, a palavra **MATEMATICA** cifrada com a palavra chave DISCO, ficaria **PILGADBAEO**.

A cifra de Vigenere foi a primeira a ficar imune ao ataque da análise de frequência, o que, por vários anos, parecia ter declarado a vitória dos criadores de códigos.

No entanto, a cifra de Vigenere 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 Vigenere.

O matemático Inglês *Charles Babbage* foi uma das personalidades mais incomuns da área científica. Em [3], relata-se que era filho de família nobre, foi deserdado por ter uma vida extravagante. Gastou sua fortuna implementando ideias e máquinas, nem todas bem sucedidas. Portanto, uma das máquinas desenvolvidas por Babbage é reconhecida nos dias atuais como o primeiro protótipo de um computador.

A técnica utilizada por Babbage para quebrar a cifra de Vigenere se resumiu em determinar o comprimento **k** da palavra chave e depois dividir a mensagem criptografada em **k** textos cujas letras estão a uma distância **k** uma das outras. Após esta etapa, basta aplicar a análise de frequência em cada um dos textos.

A dificuldade então, passa ser descobrir o comprimento da palavra chave. Para isso, uma análise do texto cifrado visando buscar repetições que indiquem dígrafos e trígrafos como *que, nha, nhe, nho, não, ai, ou* são capazes de identificar este comprimento.A quebra da cifra de Vigenere 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.

2.3 A Arte de Cifrar em Tempos Modernos, Atuais e Futuros

O desenvolvimento da criptografia até os dias atuais foi determinado por três períodos: o artesanal, o mecânico e o digital. O período artesanal registra os primeiros indícios de utilização da criptografia, paralelamente com o surgimento da escrita, ocorrendo durante as idades antiga e média. No início da idade moderna, surgem os primeiros indícios do período mecânico, devido a invenção da imprensa.

Impulsionada pela invenção do telégrafo e do rádio, o auge do período mecânico ocorre com o surgimento de máquinas de cifragem utilizadas durante a segunda guerra mundial, onde podemos destacar a máquina alemã *Enigma*. A Revolução Industrial criou no homem a paixão pelas máquinas e a esperança de substituição do cansativo trabalho manual pelo mecânico.

O final do século XIX foi uma época muito difícil para a comunicação segura, pois a cifra de Vigenère, vista como indecifrável, tinha sido quebrada por Babbage. O surgimento do rádio como uma poderosa ferramenta de comunicação, exigia técnicas de cifragem ainda mais fortes e a prova de ataques, pois a comunicação via rádio era aberta e poderia ser facilmente interceptada pelo inimigo.

Com o século XX vieram as guerras mundiais. Nos preparativos para a Primeira Guerra Mundial, todos os países envolvidos contavam com o poder de comunicação do rádio e com a incerteza da comunicação segura. Utilizando a cifra ADFGVX, uma combinação de técnicas de transposição e substituição, os alemães iniciaram uma grande ofensiva em 21 de março de 1918. Com menos de três meses de batalha, os alemães já estavam a 100 quilômetros de Paris e se preparavam para a ofensiva final. Era vital descobrir qual seria o ponto selecionado pelos alemães para neutralizar o efeito surpresa. A esperança da França e dos aliados era decifrar o código ADFGVX. As forças aliadas contavam com um criptoanalista chamado Georges Pavin, que tinha a reputação de ter quebrado todos os códigos alemãs até aquela data. No entanto, em maio de 1918 os franceses tinham interceptado uma mensagem criptografada com a cifra ADFGVX e que Pavin ainda não conseguira decifrar. Após muitos esforços, em junho de 1918 Pavin conseguiu encontrar a chave que decifraria a cifra ADFGVX. A partir daí, todas as mensagens interceptadas poderiam ser lidas, principalmente a que revelou o ponto escolhido pelo exército alemão para o ataque à Paris. Com esta informação, os

aliados reforçaram o local, eliminando o elemento surpresa da tropa alemã que recuou após cinco dias de batalha.

Durante a segunda guerra mundial a criptografia entra definitivamente no período mecânico com o surgimento da máquina de cifrar alemã denominada *Enigma*. Criada em 1918 pelo engenheiro alemão Arthur Scherbius, todos os níveis do Governo a utilizaram para se comunicar de maneira segura e estavam convencidos da impossibilidade da quebra de seu código. Na época, acreditava-se que teria sido descoberta uma máquina impenetrável. No entanto, apesar da complexidade e do alto nível de embaralhamento dos dados, as mensagens transmitidas pela Enigma começaram a ser decifradas frequentemente. A quebra do código da máquina *Enigma* foi um dos maiores triunfos criptoanalíticos de todos os tempos, num empreendimento que envolveu Polonenses, Franceses e Ingleses num esforço conjunto, em plena guerra.

O trabalho começou com o matemático polonês Marian Rejewski, que se baseou em textos cifrados interceptados e em uma lista de três meses de chaves diárias, obtidas através do serviço de espionagem francês. As contribuições de Rejewski foram muito importantes apesar de não conclusivas. Seu trabalho continuou e foi concluído com sucesso pela equipe inglesa liderada por Alan Turing, Gordon Welchman e outros, em Bletchley Park, na Inglaterra.

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 grande dificuldade encontrada pela equipe de Alan Turing ocorreu em função de que os alemães mudavam regularmente a configuração da Enigma. Além das chaves que tinham validade mensal, mudanças contínuas foram implementadas, com destaque para o acréscimo de mais dois misturadores, incrementando, de modo impressionante, o número de chaves possíveis.

A Enigma representou o estágio mais avançado a que se pode chegar com as máquinas de cifrar, com base exclusivamente mecânica e com a utilização de corrente elétrica. O princípio no qual se baseia essa máquina vem de tempos antigos, inspirado nos discos de cifragem de Alberti. Estes discos forneceram o princípio básico de funcionamento dos misturadores, o coração

da Enigma.

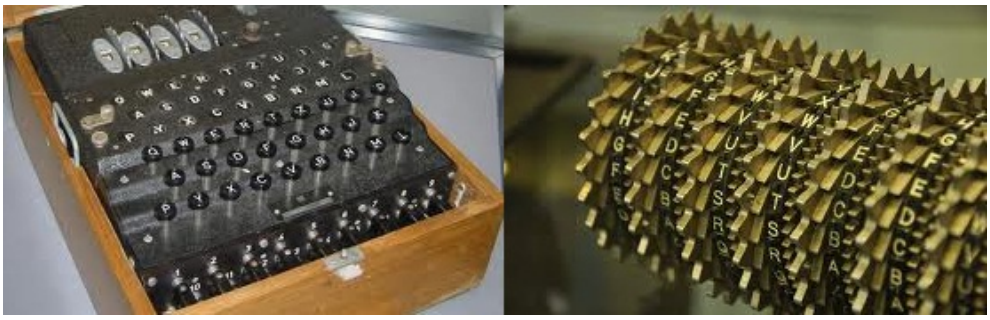


Figura 2.6: A Máquina Enigma

Veja alguns detalhes da estrutura da máquina *Enigma*.

- A mensagem era cifrada e decifrada usando o mesmo tipo de máquina. 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 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.

Na criptografia mecânica é fundamental a ocultação pública da chave e também desejável manter segredo sobre a estrutura da máquina que produz a cifragem. 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 algoritmos de chave simétrica (também chamados de Sistemas de Chave Simétrica, criptografia de chave única, ou criptografia de chave se-

creta) são uma classe de algoritmos para a criptografia, que usam chaves criptográficas relacionadas para as operações de cifragem e decifragem. A operação de chave simétrica é mais simples, pois pode existir uma única chave entre as operações. A chave, na prática, representa um segredo, partilhado entre duas ou mais partes, que podem ser usadas para manter um canal confidencial de informação. Usa-se uma única chave, partilhada por ambos os interlocutores, na premissa de que esta é conhecida apenas por eles.

Avançando até os tempos modernos, alguns tipos de algoritmos simétricos foram desenvolvidos, onde os mais conhecidos e utilizados são descritos abaixo:

O Data Encryption Standard (DES) é o algoritmo simétrico mais disseminado no mundo. Foi criado pela IBM em 1977 e, apesar de permitir cerca de 72 quatrilhões de combinações (256), seu tamanho de chave (56 bits) é considerado pequeno, tendo sido quebrado por "força bruta"em 1997 em um desafio lançado na Internet. O NIST (National Institute of Standards and Technology), que lançou o desafio mencionado, recertificou o DES pela última vez em 1993 e desde então está recomendando o 3DES. O NIST está também propondo um substituto ao DES que deve aceitar chaves de 128, 192 e 256 bits, operar com blocos de 128 bits, ser eficiente, flexível e estar livre de "royalties".

O 3DES é uma simples variação do DES, utilizando-o em três cifamentos 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 suíça 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 é 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.

O uso da criptografia de chaves públicas é bastante simples. Suponha que duas pessoas queiram se comunicar de forma segura. Como mostra a figura 2.7, ao invés de compartilharem uma única chave secreta, o destinatário tem duas chaves: uma chave pública, que está à disposição do mundo todo, inclusive de intrusos, e uma chave privada, que apenas ele conhece. 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.

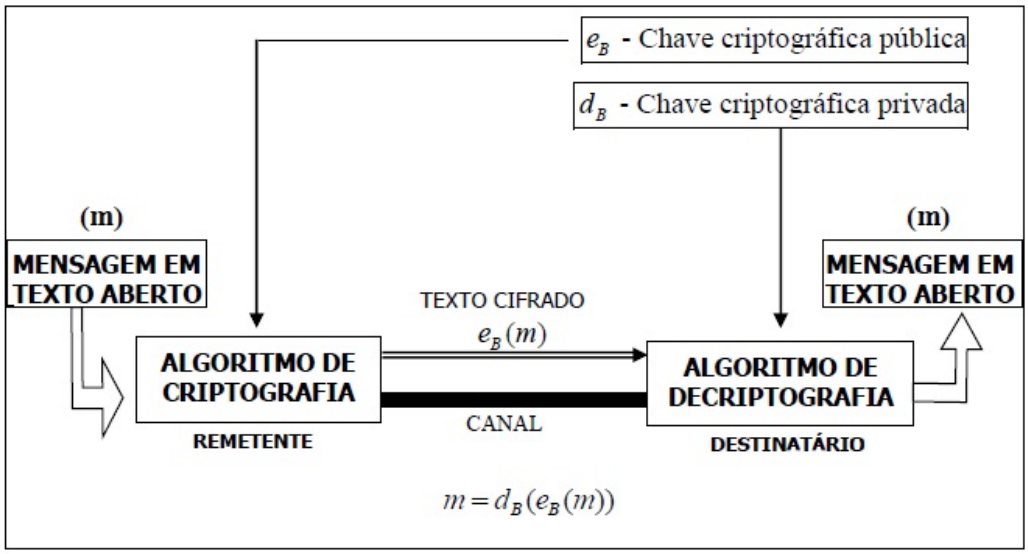


Figura 2.7: Sistema de Criptografia Assimétrica

Usando a notação da figura 2.7, para qualquer mensagem m, $d_b(e_b(m)) = m$, isto é, aplicando a chave pública do destinatário, e_b , e em seguida a sua chave privada, d_b , à mensagem m, recuperamos m. Na realidade, 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 intercepta 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. No caso de uma única chave secreta compartilhada, o fato do remetente conhecer a chave secreta identifica implicitamente o remetente para o destinatário. No caso da criptografia de chave pública isso não acontece, já que qualquer um pode enviar uma mensagem cifrada ao destinatário, usando sua chave pública. Neste caso, se faz necessário o uso de uma assinatura digital, que visa garantir a autenticidade de quem envia a mensagem, associada à integridade do seu conteúdo, vinculando um remetente à 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 MIT. É, atualmente, o algoritmo de chave pública mais amplamente utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecidas até o momento. O RSA utiliza números primos. O RSA 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. Isto é conhecido como fatoração. Por exemplo, os fatores primos de 3.337 são 47 e 71. Gerar a chave pública envolve multiplicar dois primos grandes; qualquer um pode fazer isto. Derivar a chave privada a partir da chave pública envolve fatorar um grande 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. Deste modo, a fatoração representa um limite superior do tempo necessário para quebrar o algoritmo. 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. Sua matemática difere da utilizada no RSA, mas também é um sistema comutativo. O algoritmo envolve a manipulação matemática de grandes quantidades numéricas. Sua segurança advém de algo denominado problema do logaritmo discreto. Assim, o ElGamal obtém sua segurança da dificuldade de se calcular logaritmos discretos em um corpo finito, o que lembra bastante o problema da fatoração.

O Diffie-Hellman também é baseado no problema do logaritmo discreto, sendo o criptosistema de chave pública mais antigo ainda em uso. O conceito de chave pública foi introduzido pelos autores deste criptosistema em 1976. Contudo, ele não permite ciframento nem assinatura digital. O sistema foi projetado para permitir a dois indivíduos entrarem em um acordo ao compartilharem um segredo tal como uma chave, embora eles somente troquem mensagens em público.

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 e Hellman, usando curvas elípticas. Assim, os sistemas criptográficos de curvas elípticas consistem em modificações de outros sistemas, que passam a trabalhar no domínio das curvas elípticas, em vez de trabalharem no domínio dos corpos finitos. Eles possuem o potencial de proverem sistemas criptográficos de chave pública, mais seguros e com chaves de menor tamanho.

Muitos algoritmos de chave pública, como o Diffie - Hellman, o ElGamal e o Schnorr podem ser implementados em curvas elípticas sobre corpos finitos. Assim, 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 abaixo, existem vantagens e desvantagens que, dependendo do contexto e das condições, a escolha do melhor sistema pode variar.

	CRIPTOGRAFIA SIMÉTRICA	CRIPTOGRAFIA DE CHAVE PÚBLICA
FORMAS DE CRIPTOGRAFAR UMA MENSAGEM	Técnicas de Substituição e Permutação	Funções Matemáticas
VELOCIDADE	Rápida	Lenta
DISTRIBUIÇÃO DE CHAVES	Complexa	Simples
ASSINATURA DIGITAL	Não necessita	Necessita

Já 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 à 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 Subunidade, através de um mensageiro, porém não deseja 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. 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. 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

Técnicas Criptográficas que Aplicam Matemática Básica como Ferramenta.

Nas Orientações Curriculares para o Ensino Médio (2006), consta que o aluno seja capaz de utilizar a Matemática na resolução de problemas do cotidiano e para modelar fenômenos das distintas aéreas 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.

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 um cabedal de exemplos contextualizados, ao mesmo tempo em que promovem uma interessante ligação com as ciências sociais. A seguir, exemplos da correlação entre matemática e criptografia, ressaltando que a forma de abordagem dos conteúdos não são, necessariamente, a mais adequada para aplicação com estudantes do Ensino Médio, mas servem para embasar o conhecimento dos professores que se propuserem a ensinar este assunto em sala de aula. Conforme o mandamento número 2, proposto por George Polya em seus dez

mandamentos para o professor de matemática: *"Conheça sua Matéria"*.

O capítulo 4 possui vários exemplos de atividades para aplicação com estudantes do Ensino Médio.

3.1 O Ensino de Funções Aplicado a Cifras de Substituição e Transposição

.

3.1.1 Preliminares

Um conceito que é absolutamente fundamental para a Criptografia é o de *Função* no sentido matemático de uma Transformação. Neste contexto, abordaremos algumas definições preliminares que servirão como base para a aplicação em técnicas de cifragem por substituição e transposição.

Definição 1 *Uma relação f entre os conjuntos X e Y é dita uma função quando $(x, y) \in f$ e $(x, y') \in f$ implicam em $y = y'$, ou seja, uma* função *é definida por dois conjuntos X e Y e uma regra f que atribui a cada elemento de X precisamente um elemento de Y. O conjunto X é chamado o Domínio da função e o conjunto Y o Contra-Domínio.*

Se x é um elemento de X, usualmente escrito $x \in X$, a imagem de x é o elemento em Y cujo a regra f associa com x. A imagem y de x é denotada por $y = f(x)$. A notação padrão para uma função f do conjunto X para o conjunto Y é $f : X \to Y$. Se $y \in Y$ então uma *preimagem* de y é um elemento $x \in X$ tal que $f(x) = y$. O conjunto de todos os elementos de Y que tem pelo menos uma *preimagem* é chamado de imagem de f, denotado por $Im(f)$.

Definição 2 *Uma Função é* injetora *se cada elemento do contradomínio Y é a imagem de no máximo um elemento do domínio X.*

Definição 3 *Uma função é* sobrejetora *se cada elemento do contradomínio Y é a imagem de pelo menos um elemento do domínio. Equivalentemente, uma função f é sobrejetora se $Im(f) = Y$.*

Definição 4 *Se uma função $f : X \to Y$ é injetora e sobrejetora então f é dita uma* bijeção.

Se $f : X \to Y$ é *injetora* então $f : X \to Im(f)$ é uma *bijeção*. Em particular, Se $f : X \to Y$ é *injetora* e X e Y são conjuntos finitos com o mesmo número de elementos, então f é uma *bijeção*.

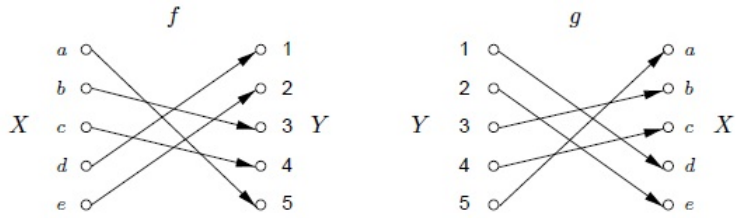


Figura 3.1: Uma bijeção f e sua inversa $g = f^{-1}$

Definição 5 *Se f é uma bijeção de X para Y então podemos definir de forma óbvia uma bijeção g de Y para X, bastando para cada $y \in Y$ definir $g(y) = x$ onde $x \in X$ e $f(x) = y$. A função g obtida de f é chamada a* função inversa *de f e é denotada por $g = f^{-1}$.*

Note que se f é uma *bijeção* então temos sua inversa f^{-1}. Em criptografia bijeções são utilizadas como ferramentas para encriptar mensagens e sua inversa para decriptar.

Permutações são funções que são utilizadas frequentemente em várias construções criptográficas.

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

Exemplo: Seja $S = \{1, 2, 3, 4, 5\}$. Uma *permutação* $p : S \to S$ definida por $p(1) = 3$; $p(2) = 5$; $p(3) = 4$; $p(4) = 2$; $p(5) = 1$ pode ser representada pela seguinte forma matricial.

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$$

A primeira linha da matriz representa o Domínio e a segunda linha a Imagem de p.

Como *permutações* são bijeções então elas possuem inversa. Se uma permutação for escrita na forma matricial, sua inversa é facimente encontrada, bastando trocar a posição das linhas da matriz. No exemplo acima, a inversa de p é

$$p^{-1} = \begin{pmatrix} 3 & 5 & 4 & 2 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

Exemplo: Seja $X = \{0,\ 1,\ 2,\ 3,\ ...,\ pq-1\}$ onde p e q são números primos com mais de 100 algarismos e suponha que 3 não divide $p-1$ e nem $q-1$. Então, pode-se mostrar que a função $p(x) = r_x$, onde r_x é o resto da divisão de x^3 por pq, é uma *permutação*. Porém, determinar a permutação inversa p^{-1} é computacionalmente inviável para os padrões tecnológicos atuais, a menos que p e q sejam conhecidos. Esta é uma ideia básica para a criptografia assimétrica.

Alguns tipos de função tem a propriedade de serem a sua própria inversa.

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

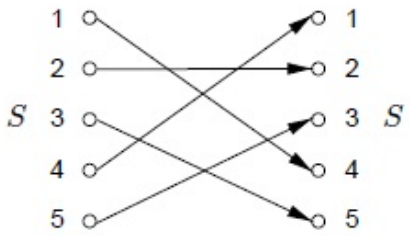


Figura 3.2: Uma involução sobre um conjunto S com 5 elementos

3.1.2 Cifras de Substituição Monoalfabética

Cifras de substituição são cifras de bloco que substituem símbolos por outros símbolos ou grupo de símbolos.

Definição 8 *Seja A um alfabeto com q símbolos e seja M o conjunto de todas as sequências de comprimento t sobre A. Seja K o conjunto de todas as permutações do cojunto A. Definimos para cada $e \in K$ uma função criptográfica E_e como:*

$$E_e(m) = (e(m_1)e(m_2)\dots e(m_t)) = (c_1c_2\dots c_t) = c$$

onde $m = (m_1m_2\dots m_t) \in M$. Em outras palavras, para cada símbolo em uma t-upla, deve-se substituí-lo por outro símbolo de A conforme cada permutação fixada e.

Para decriptar $c = (c_1c_2\dots c_t)$ determine a permutação inversa $d = e^{-1}$ e faça

$$D_d(c) = (d(c_1)d(c_2)\dots d(c_t)) = (m_1m_2\dots m_t) = m.$$

E_e é chamada de Cifra de Substituição Monoalfabética.

A quantidade de cifras distintas (chaves) será discutida e calculada na seção 3.2.

Exemplo: Utilizando nosso alfabeto com 26 letras e definindo uma permutação $e = x + 3$, teremos exatamente a *cifra de Cesar*, a qual transforma a mensagem m=MESTRADO PROFISSIONAL EM MATEMATICA na mensagem cifrada $E_e(m)$ = PHVXUDGR SURILVVLRQDO HP PDXHPDXLFD. Para decriptar, utiliza-se a permutação inversa $d = e^{-1} = x - 3$.

3.1.3 Cifras de Substituição Homofônica

Definição 9 *Para cada símbolo $a \in A$, associa-se o conjunto $H(a)$ de sequências de t símbolos, com a restrição que conjuntos $H(a)$, $a \in A$, sejam separados em pares disjuntos. Uma* cifra de substituição homofônica *substitui cada símbolo a em um bloco de mensagem de texto simples com uma escolha aleatória de sequências para $H(a)$. Para decifrar uma sequência c de t símbolos, basta determinar um $a \in A$ tal que $c \in H(a)$. A chave da cifra é o conjunto $H(a)$.*

Exemplo: Considere $A = \{a,\ b\}, H(a) = \{00,\ 10\}$ e $H(b) = \{01,\ 11\}$. o bloco de mensagem de texto simples ab é encriptado em uma das seguintes formas: 0001, 0011, 1001, 1011. Observe que o contradomínio da função criptográfica, para mensagens de comprimento 2, consiste dos seguintes conjuntos de pares disjuntos de sequências de 4 elementos:

$$\begin{array}{l} aa \to \{0000,\ 0010,\ 1000,\ 1010\} \\ ab \to \{0001,\ 0011,\ 1001,\ 1011\} \\ ba \to \{0100,\ 0110,\ 1100,\ 1110\} \\ bb \to \{0101,\ 0111,\ 1101,\ 1111\} \end{array}$$

Qualquer seqüência de 4 elementos identifica um elemento do contradomínio e, portanto, uma mensagem de texto simples.

3.1.4 Cifras de Substituição Polialfabética

Definição 10 *Uma* cifra de substituição polialfabética *é uma cifra de bloco com comprimento do bloco t sobre um alfabeto A, com as seguintes propriedades:*
(i) O conjunto das chaves K consiste de todos os conjuntos ordenados de t permutações $(p_1, p_2, \ldots, p_t)$*, onde cada permutação* p_i *é definida no conjunto A;*
(ii) A encriptação da mensagem $m = (m_1 m_2 \ldots m_t)$ *sob a chave* $e = (p_1, p_2, \ldots, p_t)$ *é dada por* $E_e(m) = (p_1(m_1)p_2(m_2)\ldots p_t(m_t))$*; e*
(iii) a chave de decriptação associada a $e = (p_1, p_2, \ldots, p_t)$ *é* $d = (p_1^{-1}, p_2^{-1}, \ldots, p_t^{-1})$.

Exemplo: *(Cifra de Vigenere)* Seja $A = \{A,\ B,\ C,\ \ldots\ X,\ Y,\ Z\}$ e $t = 3$. Escolha $e = (p_1, p_2, p_3)$, onde p_1 leva cada letra para uma letra a três posições a direita no alfabeto, p_2 para uma letra a sete posições a direita e p_3 a dez posições a direita. Se

$$m = \text{MES TRA DOP ROF ISS ION ALE MAT EMA TIC A}$$

Então

$$c = E_e(m) = \text{PLD XZK GVZ UVP LZC LVX DSO PHD HTK XPM D}$$

Cifras Polialfabéticas tem a vantagem sobre as cifras de substituição monoalfabéticas pois a frequência dos símbolos não são preservadas. No exemplo acima, a letra E é encriptada primeiramente pela letra L, depois

pela letra O e finalmente pela letra H. No entanto, *Cifras Polialfabéticas* não apresentam muita dificuldade para a criptoanálise pois é similar a várias cifras monoalfabéticas. De fato, dado um determinado bloco de comprimento t, a mensagem pode ser dividida em t grupos, onde o grupo i, $1 \leq$i$\leq$t, consiste das letras da mensagem derivadas da permutação p_i, e a análise de frequência pode ser feita em cada grupo. (Ataque de Babbage à cifra de Vigenere).

3.1.5 Cifras de Transposição

Outra classe de cifras de chave simétrica é a *cifra de transposição simples* que simplesmente permuta os símbolos em um bloco.

Definição 11 *Considere uma chave simétrica em um esquema de encriptação em bloco, com bloco de comprimento t. Seja K o conjunto de todas as permutações do conjunto $\{1, \ 2, \ \ldots \ t\}$. Para cada $e \in K$ define-se a função de encriptação por*

$$E_e(m) = (m_{e(1)} m_{e(2)} \ldots m_{e(t)})$$

onde $m = (m_1 m_2 \ldots m_t) \in M$ é o espaço de mensagem. O conjunto de todas essas transformações é chamado de cifra de transposição simples.

A chave de decriptação correspondente a e é a permutação inversa $d = e^{-1}$. Para decriptar $c = (c_1 c_2 \ldots c_t)$, calcule $D_d(c) = (c_{d(1)} c_{d(2)} \ldots c_{d(t)})$.

Exemplo: Cifrando a mensagem m

$$(MEST - RADO - PROF - ISSI - ONAL - EMMA - TEMA - TICA)$$

com $t = 4$ e $e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 8 & 7 & 4 & 1 & 6 & 2 \end{pmatrix}$, temos

$$\begin{array}{ll} m_{e(1)} = m_3 = PROF & m_{e(2)} = m_5 = ONAL \\ m_{e(3)} = m_8 = TICA & m_{e(4)} = m_7 = TEMA \\ m_{e(5)} = m_4 = ISSI & m_{e(6)} = m_1 = MEST \\ m_{e(7)} = m_6 = EMMA & m_{e(8)} = m_2 = RADO \end{array}$$

Portanto,

$E_e(m) = (PROF - ONAL - TICA - TEMA - ISSI - MEST - EMMA - RADO)$.

3.1.6 Composição de Cifras

Com a finalidade de dificultar a criptoanálise de um texto, podemos utilizar uma cifra híbrida, ou seja, compor uma cifra de transposição com uma cifra de substituição, embora, na prática, isso não ocorra.

Definição 12 *Seja S, T e U conjuntos finitos e seja $f : S \to T$ e $g : T \to U$ funções. A composição de g com f, denotada por $g \circ f$, é a função de S para U como ilustrado na figura abaixo e definida por $(g \circ f)(x) = g(f(x))$, para todo $x \in S$.*

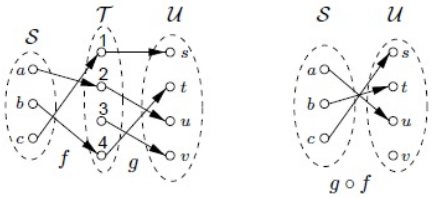


Figura 3.3: A composição $g \circ f$ das funções g e f

A *composição* pode ser extendida para mais que duas funções. Para funções $f_1, f_2, \ldots, f_t$ define-se $f_t \circ \cdots \circ f_2 \circ f_1$, onde o domínio de f_t equivale ao contradomínio de f_{t-1} e assim por diante.

3.2 A Utilização de Técnicas de Contagem na Determinação do Número de Chaves Criptogáficas

.

Nesta Seção serão analisadas diversas situações acerca da quantidade de chaves criptográficas de uma cifra de substituição monoalfabética e, para isso, serão utilizadas algumas técnicas de contagem, geralmente estudadas dentro do assunto análise combinatória ministrado para estudantes do ensino médio.

Análise combinatória é a parte da matemática que analisa estruturas e relações discretas, como a contagem dos subconjuntos de um conjunto finito, sem a necessidade de enumerá-los. Um dos primeiros problemas que está

ligado à *análise combinatória* é o do desenvolvimento do binômio $(1+x)^n$, onde o caso $n = 2$ está nos *Elementos de Euclides*, em torno de 300 a.C.

Portanto, antes da abordargem do problema da contagem das chaves, alguns assuntos preliminares serão introduzidos.

3.2.1 Preliminares

Os principais conceitos que serão utilizados como base para o desenvolvimento do que iremos abordar, são:

Definição 13 *(Princípio Aditivo) Dados os conjuntos $A_1, A_2, \ldots, A_n$, disjuntos 2 a 2, se cada A_i tem a_i elementos, $\#(A_i) = a_i$, então a união desses conjuntos é igual à soma de seus elementos, ou seja, $\cup_{i=1}^{n} A_i = \sum_{i=1}^{n} a_i$.*

Exemplo: Considere a *cifra de Cesar*, onde cada letra da mensagem é substituída por uma letra do alfabeto após um certo deslocamento linear, em um alfabeto com 26 letras, definimos cada conjunto A_i como uma forma diferente de se processar tal deslocamento. Desta forma, $\#(A_i) = a_i = 1$ para todo $i = 1, 2, \ldots, 25$. Portanto, a quantidade de chaves possíveis em uma *cifra de Cesar* é igual a $\sum_{i=1}^{25} a_i = 25$.

Definição 14 *(Princípio Multiplicativo) Se um evento A_i pode ocorrer de a_i formas distintas, onde $i = 1, 2, 3, \ldots, n$, então a quantidade de formas distintas de ocorrer, consecutivamente, os eventos $A_1, A_2, \ldots, A_n$ é igual ao produto do número de ocorrências de cada evento, ou seja, é igual a $\prod_{i=1}^{n} a_i$.*

Exemplo: Considere uma *cifra polialfabética* onde foram utilizados 3 alfabetos distintos e com deslocamento como na cifra de Cesar. Para o primeiro evento (alfabeto) A_1, como vimos acima tem-se 25 possibilidades, ou seja, $a_1 = 25$. Para o segundo alfabeto, tirando apenas o alfabeto A_1, teremos $A_2 = 24$ e, consequentemente, $A_3 = 23$. Desta forma, a quantidade de chaves possíveis nesta situação é $\prod_{i=1}^{3} a_i = 25.24.23 = 13800$.

Definição 15 *(Permutação Simples) Dado um conjunto A tal que* $\#(A) = n$*, o número de modos distintos de ordenar todos os n elementos do conjunto A chama-se permutação e, utilizando o princípio multiplicativo, temos que o número de permutações desses n elementos é* $P_n = \prod_{i=1}^{n} i = n!$.

Definição 16 *(Combinação Simples) Dado um conjunto A tal que* $\#(A) = n$*, o total de escolhas não ordenadas de p elementos do conjunto A,* $p \leq n$*, é chamada de combinação de n elementos escolhidos p a p, cuja notação é* C_n^p*. Utilizando o princípio multiplicativo e considerando que as escolhas são não ordenadas, temos* $C_n^p = \frac{\prod_{i=n-p+1}^{n} i}{p!}, p \leq n$.

Exemplo: Considerando todas as possíveis chaves de uma cifra monoalfabética em um alfabeto com 26 letras, tem-se que cada chave é uma *Permutação* do alfabeto original. Portanto, o número de chaves será $P_{26} - 1 = 26! - 1 = 403.291.461.126.605.635.583.999.999$. Se cada chave gastasse 1 segundo para ser verificada, o tempo total para que todas as chaves fossem verificadas seria de quase 1 bilhão de vezes a idade do universo.

No entanto, se considerarmos que ao escolher uma chave para uma cifra monoalfabética deseja-se preservar a ordem usual das letras, ou seja, não escolher a própria letra para substitui-la na mensagem, quantas serão essas chaves ? Isso é o que será visto a seguir.

3.2.2 O Problema da Contagem de Chaves em uma Cifra Monoalfabética

.

O Problema da quantidade de chaves de uma cifra monoalfabética considerando que uma letra não pode ser substituída por ela própria, é um típico exemplo de *permutação caótica* ou *desordenamento*.

Definição 17 *Uma permutação dos termos da sequência* $a_1, a_2, a_3, \ldots, a_n$ *é dita caótica se cada termo* a_i *da sequência não ocupar a posição de número i, com* $i = 1, 2, 3, \ldots, n$.

Para se calcular a quantidade de *permutações caóticas* de uma sequência, denotado por D_n, tem-se que, dado um conjunto com n elementos $A = \{a_1, a_2, \ldots, a_n\}$ e definindo A_i como sendo o conjunto das permutações em que o elemento a_i está na posição de número i, D_n é o complementar da união dos A_i, ou seja, $D_n = \overline{\cup_{i=1}^{n} A_i}$.

Portanto,

$$D_n = n! - \sum_{i=1}^{n} \#(A_i) + \sum_{1 \leq i < j} \#(A_i \cap A_j) - \sum_{1 \leq i < j < k} \#(A_i \cap A_j \cap A_k) + \cdots + \\ + (-1)^n \#(A_1 \cap A_2 \cap \cdots \cap A_n).$$

Como

$$\#(A_i) = (n-1)!$$

$$\#(A_i \cap A_j) = (n-2)!$$

$$\#(A_i \cap A_j \cap A_k) = (n-3)!$$

$$\vdots$$

$$\#(A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n) = 1$$

temos

$$D_n = n! - n(n-1)! + C_n^2(n-2)! - C_n^3(n-3)! + \cdots + (-1)^n.1.$$

Logo,

$$D_n = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}\right)$$

Retomando o problema da quantidade de chaves de uma cifra monoalfabética, em um alfabeto com 26 letras e considerando que cada letra da mensagem não pode ser substituída por ela própria, aplica-se o resultado acima para obter:

$$D_{26} = 26! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{1}{26!}\right)$$

donde calcula-se que $D_{26} = 148.362.637.348.470.135.821.287.825$

3.3 Aplicação de Matriz e Aritmética Modular na Utilização da Cifra de Hill

.

Criada por Lester S. Hill em 1929, a Cifra de Hill é um tipo de cifra de substituição, em bloco, baseada em álgebra linear e aritmética modular, que não é vulnerável à análise de frequência das letras do alfabeto, porém pode ser quebrada utilizando recursos da própria álgebra linear. Para uma melhor compreensão dos processos de cifragem e decifragem, alguns conceitos básicos devem ser entendidos preliminarmente.

3.3.1 Preliminares

.

O primeiro conceito que será necessário para a compreenção dos processos de cifragem e decifragem de uma mensagem utilizando a cifra de Hill é o de aritmética modular.

Definição 18 *Dado um número inteiro positivo m, dois números interios a e b são ditos congruentes módulo m se os restos da divisão euclidiana de a e b por m são iguais. Denota-se $a \equiv b \pmod{m}$.Desta forma, m divide $a - b$.*

O conjunto formado pelos possíveis restos da divisão euclidiana de um inteiro a por m é dito o *conjunto dos resíduos de a módulo m* e é denotado por Z_m, isto é, $Z_m = \{0, 1, 2, \ldots, m-1\}$.

Proposição 1 *Qualquer inteiro a é congruente módulo m a um dos inteiros $0, 1, 2, \ldots, m-1$.*

Demonstração: Qualquer que seja $a \in Z$, pode-se expressar $a = mq + r$, com $0 \leq r < m$ e $q \in Z$. Portanto, $mq = a - r$ significa que m divide $a - r$. Logo, $a \equiv r \pmod{m}, r \in \{0, 1, 2, \ldots, m-1\}$.

Exemplo: $35 \equiv 11 \pmod{12}$, pois $35 = 12 \times 2 + 11$;

$-38 \equiv 14 \pmod{26}$, pois $-38 = 26 \times (-2) + 14$.

$$111911 \equiv 0 \pmod{17}, \text{ pois } 111911 = 17 \times 6583 + 0.$$

3.3.2 Cifração

Definição 19 *(Cifra de Hill) É uma cifra em blocos de comprimento n sobre um alfabeto com q símbolos, cuja mensagem aberta* $M = (m_1, m_2, \ldots, m_n)$ *é transformada pela chave* $A = (a_{ij})_n, a_{ij} \in Z_q$, *na mensagem cifrada* $C = (c_1, c_2, \ldots, c_n)$, *onde cada* c_i *é uma combinação linear dos blocos* m_i, $1 \leq i \leq n$, *isto é,*

$$c_1 = a_{11}m_1 + a_{12}m_2 + \cdots + a_{1n}m_n(modq)$$

$$c_2 = a_{21}m_1 + a_{22}m_2 + \cdots + a_{2n}m_n(modq)$$

$$\vdots$$

$$c_n = a_{n1}m_1 + a_{n2}m_2 + \cdots + a_{nn}m_n(modq)$$

Em notação matricial temos $C = A.M$, onde

$$C = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} ; A = \begin{bmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{bmatrix} \text{ e } M = \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix}$$

são matrizes cujos elementos pertencem a Z_q.

Originalmente a cifra de Hill trabalha com um alfabeto de 26 letras. Portanto, daqui em diante será considerado $q = 26$.

Exemplo: Considerando o alfabeto com 26 letras, como na 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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

e utilizando a chave $k = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$ onde $n = 2$, para cifrar a mensagem **CIFRAR É UMA ARTE**, procede-se da seguinte forma:

Utiliza-se a tabela para transformar as letras em números e efetua-se o produto matricial.

C	I	F	R	A	R	E	U	M	A	A	R	T	E
2	8	5	17	0	17	4	20	12	0	0	17	19	4

$$\begin{bmatrix}5 & 6\\ 2 & 3\end{bmatrix}\cdot\begin{bmatrix}2 & 5 & 0 & 4 & 12 & 0 & 19\\ 8 & 17 & 17 & 20 & 0 & 17 & 4\end{bmatrix}=\begin{bmatrix}58 & 127 & 102 & 140 & 60 & 102 & 119\\ 28 & 61 & 51 & 68 & 24 & 51 & 50\end{bmatrix}=$$

$$=\begin{bmatrix}6 & 23 & 24 & 10 & 8 & 24 & 15\\ 2 & 9 & 25 & 16 & 24 & 25 & 24\end{bmatrix}(mod 26).$$

Recorrendo à tabela, obtém-se o texto cifrado **GCXJYZKQIYYZPY**.

3.3.3 Decifração

No processo de cifração de uma mensagem aberta M, efetua-se o produto matricial $C = A \times M$ para obter a mensagem cifrada C. É fácil verificar que para obter a mensagem aberta M a partir da mensagem cifrada C basta multiplicar à esquerda da equação a matriz A^{-1}, inversa da matriz A, ou seja, $A^{-1} \times C = A^{-1} \times A \times M$, fornecendo $M = A^{-1} \times C$.

No entanto, para garantir a existência da inversa da matriz A, será necessária a aplicação de alguns resultados, enunciados a seguir, cuja demonstração de alguns deles será omitida pois foge ao objetivo deste trabalho.

Definição 20 *Dado um número $a \in Z_m$, o seu inverso multiplicativo é o número $a^{-1} \in Z_m$ tal que $aa^{-1} = a^{-1}a = 1(mod\ m)$, que é a solução da congruência $aX \equiv 1 \pmod{m}$, com $(a, m) = 1$.*

Em [8], prova-se que se $(a, m) \neq 1$ então a não possui inverso multiplicativo em Z_m.

Exemplo: Analisando os inversos multiplicativos em Z_{26}, observa-se que os números pares (2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24) e o 13 não possuem inverso multiplicativo pois não são co-primos com 26. Para os demais elementos de Z_{26}, calcula-se o inverso multiplicativo resolvendo a congruência

$aX \equiv 1 \pmod{26}$.

Portanto, o inverso multiplicativo de 3 é a solução de $3X \equiv 1 \pmod{26}$, que é 9. A tabela abaixo fornece os inversos multiplicativos de Z_{26}. Em [8] pode-se verificar com detalhes a técnica para a resolução de congruências, no entanto, para números pequenos como 26 é viável fazer tentativas.

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

Na teoria sobre matrizes e determinantes, comprova-se que dada uma matriz quadrada M, com $det(M) \neq 0$, a sua inversa é $M^{-1} = \frac{1}{det(M)}.\overline{M}$, onde $\overline{M}$ é a matriz transposta da matriz dos cofatores de M, chamada *Matriz Adjunta*.

Proposição 2 *Seja M uma matriz quadrada. A inversa de M existe, se e somente se, $det(M) \neq 0$.*

Demonstração:
Se $det(M) \neq 0$, temos que existe a inversa $M^{-1} = \frac{1}{det(M)}.\overline{M}$;
Se a inversa M^{-1} existe então $M.M^{-1} = I$ e, pelo teorema de Binet, $det(M) \times det(M^{-1}) = 1 \neq 0$, portanto $det(M) \neq 0$.

Considerando que se esteja trabalhando em Z_m, a matriz codificadora A terá inversa módulo m se $det(A)(\text{mod m}) \times det(A^{-1})(\text{mod m}) = 1(\text{mod m})$. Pode-se então concluir que:

Uma matriz quadrada A com entradas em Z_m é invertível módulo m se e somente se, o resíduo de $det(A)$ módulo m possui um inverso multiplicativo em Z_m.

No caso específico da cifra de Hill, onde trabalha-se em Z_{26}, pode-se afirmar que a matriz codificadora A possui inversa módulo 26 se, e somente se, o resíduo do $det(A)$ módulo 26 não é múltiplo de 2 ou de 13.

Exemplo: Decifrando a mensagem utilizada no exemplo da cifração, onde a mensagem cifrada é **GCXJYZKQIYYZPY** e a matriz codificadora

é $A = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$, tem-se:

$det(A) = 3$ e $3^{-1} = 9 \pmod{26}$.

Então, $A^{-1} = 9.\begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix} = \begin{bmatrix} 27 & -54 \\ -18 & 45 \end{bmatrix} = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \pmod{26}$.

Portanto,

$$M = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \times \begin{bmatrix} 6 & 23 & 24 & 10 & 8 & 24 & 15 \\ 2 & 9 & 25 & 16 & 24 & 25 & 24 \end{bmatrix} = \begin{bmatrix} 54 & 239 & 624 & 394 & 584 & 624 & 591 \\ 86 & 355 & 667 & 384 & 520 & 667 & 576 \end{bmatrix} =$$

$$= \begin{bmatrix} 2 & 5 & 0 & 4 & 12 & 0 & 19 \\ 8 & 17 & 17 & 20 & 0 & 17 & 4 \end{bmatrix} \pmod{26}.$$

Recorrendo à tabela, obtém-se o texto aberto **CIFRAR É UMA ARTE**.

Capítulo 4

Atividades de Matemática Básica Motivadas pela Arte de Cifrar, Criptografar, Esconder e Salvaguardar.

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 pueris ou não condizentes com a realidade. Também é comum achar que contextualização e aplicação são sinônimos. Contextualizar a matemática é 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 teorias 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 estudan-

tes, como já declarado pelo Filósofo Francês, Auguste Comte:

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

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

Em [20], 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 [21, 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 [22], 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 corroborar 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.

4.1 Atividades de Criptografia para o Ensino de Funções

.

O conceito de função, no sentido matemático de transformação, é um dos assuntos mais importantes do Ensino Médio. É o momento em que o estudante começa a ter a noção da utilização da matemática para modelar

situações do cotidiano. Os livros didáticos estão repletos desses exemplos.

Cada atividade proposta abaixo, explora uma determinada característica do ensino de funções, possibilitando a confecção de uma família de atividades similares aos exemplos.

ATIVIDADE 1: Explora o conceito básico de função no sentido de transformação, o cálculo da imagem de um elemento do domínio da função, a determinação da inversa de uma função bijetora e o cálculo da pré-imagem de um elemento da imagem.

Competências e Habilidades:
Competência de área 5 - Modelar e resolver problemas que envolvem variáveis socioeconômicas ou técnico-científicas, usando representações algébricas.
Habilidade 19 - Identificar representações algébricas que expressem a relação entre grandezas.
Habilidade 20 - Interpretar gráfico cartesiano que represente relações entre grandezas.
Habilidade 21 - Resolver situação-problema cuja modelagem envolva conhecimentos algébricos.
Habilidade 22 - Utilizar conhecimentos algébricos/geométricos como recurso para a construção de argumentação.
Habilidade 23 - Avaliar propostas de intervenção na realidade utilizando conhecimentos algébricos.

Ações Didáticas:
Os estudantes devem trabalhar em pequenos grupos, de até 4 componentes, onde cada um terá uma função específica, que são: Líder: Coordena o trabalho da equipe, imputando aos membros do grupo a realização de tarefas não especificadas em cada função; Executor: Organiza a execução do problema e escreve a solução do mesmo; Relator: Responsável por relatar como a equipe trabalhou na resolução do problema, mencionando também as dificuldades encontradas. É também responsável por relatar as dúvidas ao professor, durante a resolução do problema; Verificador: Responsável pela verificação dos resultados encontrados. No caso de um grupo com 3 componentes, a função de verificador se acumula com a do líder. Todos os membros devem trabalhar na solução do problema e se ajudarem mutuamente para a realização de cada tarefa do grupo. Durante a execução da atividade, o professor deve percorrer os grupos para tirar possíveis dúvidas, enfatizar questões importantes e observar a ação individual dos membros de cada equipe. Ao final da atividade, o executor entrega a parte escrita ao professor, o relator expõe

a solução de um determinado item para toda a turma e o professor distribui uma ficha de avaliação de cada membro da equipe, que deverá ser preenchida pelos próprios alunos e complementada pelo professor, fruto de sua observação durante a atividade. É aconselhável a utilização de calculadora para a realização da atividade. O tempo mínimo para a realização de todas as etapas da atividade é de 1 hora e 30 minutos.

Atividade:

Luiz deseja enviar uma mensagem sigilosa para José, a qual deverá ser cifrada substituindo-se cada letra por um número, conforme a tabela abaixo, aplicando o número correspondente na função $f(x) = 3x - 2$, obtendo a mensagem cifrada. Por exemplo, a letra m corresponde ao número 13, que é transformado pela função em $f(13) = 3 \times 13 - 2 = 37$, ou seja, a letra m é 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

RESPONDA:

1) CIFRE a mensagem aberta: *O dólar 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 decifração.

3) Complete os espaços abaixo:

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

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																					

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

6) Se a função CIFRADORA fosse modificada para $g(x) = 3x + 1$, qual a modificação que deveríamos fazer na tabela para não alterarmos o código de cada letra ?

7) Considerando a possibilidade de modificação 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 , $f(15) = 43$, $o \mapsto 43$.

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

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

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

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

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

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

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

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

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

A mensagem codificada fica: $43 - 10 - 43 - 34 - 1 - 52 - 64 - 1 - 25 - 55 - 61 - 4 - 25 - 52$.

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 de tornar a função bijetora para obter a sua inversa será abordada na atividade 2. Novamente fica explícita a idéia de transformação.

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

$1 \mapsto a \quad ; \quad 58 \mapsto t \quad ; \quad 49 \mapsto q \quad ; \quad 61 \mapsto u \quad ; \quad 13 \mapsto e \quad ; \quad 43 \mapsto o$

$37 \mapsto m \quad ; \quad 40 \mapsto n \quad ; \quad 22 \mapsto h \quad ; \quad 7 \mapsto c \quad ; \quad 52 \mapsto r$

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

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, é 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

5) Neste item, num primeiro momento peça apenas que os estudantes identifiquem o domínio da função cifradora, $\{1, 2, 3, \ldots, 26\}$, a sua imagem, $\{1, 4, 7, 10, \ldots, 76\}$ 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 $\{1, 2, 3, \ldots, 26\} = \{x | 1 \leq x \leq 26\}$ como exemplo. Ao representarem o conjunto imagem, geralmente por $\{3x - 2 | 1 \leq x \leq 26\}$, mostre que existem outras possibilidades, como $\{3x + 1 | 0 \leq x \leq 25\}$, o que já indicará o que fazer no item 6). Também é interessante mostrar aos estudantes a representação formal das funções, $f : A \longrightarrow B$, $f(x) = 3x - 2$, enfatizando que ao mudar o domínio e o contradomínio, pode representar a criação de uma nova função (transformação).

6) Neste item, o estudante naturalmente irá recorrer ao item 5 e responderá com suas palavras, que nem sempre é a mais precisa, 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 naturalmente 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 $B \equiv 1 \pmod 3$.

ATIVIDADE 2: *Explora o conceito de bijeção como condição necessária e suficiente para a inversão de uma função. Mostra a importância do domínio e do contra-domínio na obtenção de bijeções. Explora a análise de gráficos de funções, mostrando a diferença entre o gráfico de funções com domínio contínuo e com domínio discreto.*

Competências e Habilidades:
Competência de área 5 - Modelar e resolver problemas que envolvem variáveis socioeconômicas ou técnico-científicas, usando representações algébricas.
Habilidade 19 - Identificar representações algébricas que expressem a relação entre grandezas.
Habilidade 20 - Interpretar gráfico cartesiano que represente relações entre grandezas.
Habilidade 21 - Resolver situação-problema cuja modelagem envolva conhecimentos algébricos.
Habilidade 22 - Utilizar conhecimentos algébricos/geométricos como recurso para a construção de argumentação.
Habilidade 23 - Avaliar propostas de intervenção na realidade utilizando conhecimentos algébricos.

Ações Didáticas:
Esta atividade pressupõe que os estudantes já tenham realizado a atividade 1. Caso isto não tenha ocorrido, será necessário detalhar melhor o enunciado. Os estudantes devem trabalhar em pequenos grupos, de até 4 componentes, onde cada um terá uma função específica, que são: Líder: Coordena o trabalho da equipe, imputando aos membros do grupo a realização de tarefas não especificadas em cada função; Executor: Organiza a execução do problema e escreve a solução do mesmo; Relator: Responsável por relatar como a equipe trabalhou na resolução do problema, mencionando também as dificuldades encontradas. É também responsável por relatar as dúvidas ao professor, durante a resolução do problema; Verificador: Responsável pela verificação dos resultados encontrados. No caso de um grupo com 3 componentes, a função de verificador se acumula com a do líder. Todos os membros devem trabalhar na solução do problema e se ajudarem mutuamente para a realização de cada tarefa do grupo. Durante a execução da atividade, o professor deve percorrer os grupos para tirar possíveis dúvidas, enfatizar questões importantes e observar a ação individual dos membros de cada equipe. Ao final da atividade, o executor entrega a parte escrita ao professor, o relator expõe a solução de um determinado item para toda a turma e o professor distribui uma ficha de avaliação de cada membro da equipe, que deverá ser preenchida pelos próprios alunos e complementada pelo professor, fruto de sua

observação durante a atividade. É fundamental a utilização de calculadora e desejável a utilização de software de plotar gráficos (Geogebra ou Winplot) para a realização da atividade. O tempo mínimo para a realização de todas as etapas da atividade é de 1 hora e 30 minutos.

Atividade:
Para enviar uma mensagem sigilosa, José substitui as letras da mensagem aberta por números, conforme a tabela abaixo 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

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

5) Crie uma função quadrática f, preencha na tabela abaixo os números que substituem as letras do alfabeto (Domínio de f) e determine a função de cifradora. Faça um teste cifrando e decifrando alguma palavra.

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

6) Construa o gráfico de sua função cifradora localize o x do vértice. Com base em suas observações, elabore uma conjectura sobre funções quadráticas

cifradoras.

7) Utilize a tabela abaixo e a função codificadora $y = 3x^2 - 5x + 3$ para codificar a palavra MATEMÁTICA. Porque a função codificadora f é bijetora, apesar da letra a não ser substituída por um número igual ou maior que o x do vértice ?

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

8) Analise o gráfico da função cifradora $y = 3x^2 - 5x + 3$ e estipule condições sobre um polinômio quadrático do tipo $f(x) = Ax^2 + Bx + C$, com A, B e C inteiros, $A \neq 0$, tal que ele possa ser uma função cifradora, independente da numeração imposta às letras do alfabeto.

9) Determine uma função quadrática onde as letras equidistantes do centro do alfabeto (a e z ; b e y ; c e x ; . . . ; m e n) tenham o mesmo código.

SOLUÇÕES E COMENTÁRIOS

1) De forma análoga ao item 1 da atividade 1, 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 corresponde ao 3 , $f(3) = 3$, $C \mapsto 3$.

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.

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

Temos então que a função decodificadora é $f^{-1} = 4 \pm \sqrt{x-1}$, onde $x \geq 1$.

Apesar da importância em observar que $x \geq 1$, ressalta-se que esta condição se cumpre naturalmente.

Ao aplicar a mensagem cifrada na função de cifradora, obtém-se o seguinte:

$$5 \begin{array}{llll} \mapsto & 6 & \mapsto & F \\ \mapsto & 2 & \mapsto & B \end{array} \quad ; \quad 10 \begin{array}{llll} \mapsto & 7 & \mapsto & G \\ \mapsto & 1 & \mapsto & A \end{array} \quad ; \quad 197 \begin{array}{llll} \mapsto & 18 & \mapsto & R \\ \mapsto & -10 & \mapsto & \notin D_{f^{-1}} \end{array}$$

$$26 \begin{array}{llll} \mapsto & 9 & \mapsto & I \\ \mapsto & -1 & \mapsto & \notin D_{f^{-1}} \end{array} \quad ; \quad 2 \begin{array}{llll} \mapsto & 5 & \mapsto & E \\ \mapsto & 3 & \mapsto & C \end{array} \quad ; \quad 1 \mapsto 4 \mapsto D$$

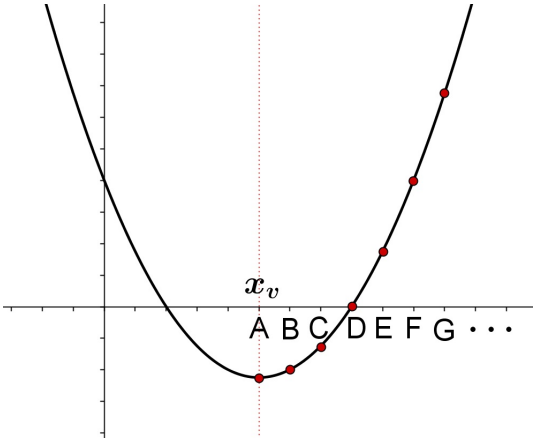
Nesta situação, o estudante terá que fazer algumas tentativas para chegar à mensagem *FÁBRICA DE FACA*.

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 idéia de bijeção como condição suficiente para a escolha da função cifradora.

4) 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.

5) Neste item os estudantes podem responder livremente, porém, na maioria dos casos, as funções serão polinômios quadráticos com coeficiente líder igual a 1, o que os levará à necessidade de escolher bem os números correspondentes das letras do alfabeto, ou seja, escolher bem o domínio da função



cifradora para torná-la bijetora, como será visto nos itens 7 e 8.

6) Para a construção do gráfico, é desejável que se utilize o software Geogebra ou Winplot. Após a exibição do gráfico do item 4, é natural que os estudantes procedam de forma similar e conjecturem que as letras do alfabeto devam ser substituídas por valores maiores ou iguais ao x do vértice. Cabe ao professor complementar observando que os polinômios quadráticos devem possuir coeficientes inteiros para que a imagem seja, necessariamente, um número inteiro, citando a propriedade do fechamento em relação as operações de adição e multiplicação de números inteiros.

7) M corresponde ao 13 , $f(13) = 445$, $M \mapsto 445$.

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

T corresponde ao 20 , $f(20) = 1103$, $T \mapsto 1103$.

E corresponde ao 5 , $f(5) = 53$, $E \mapsto 53$.

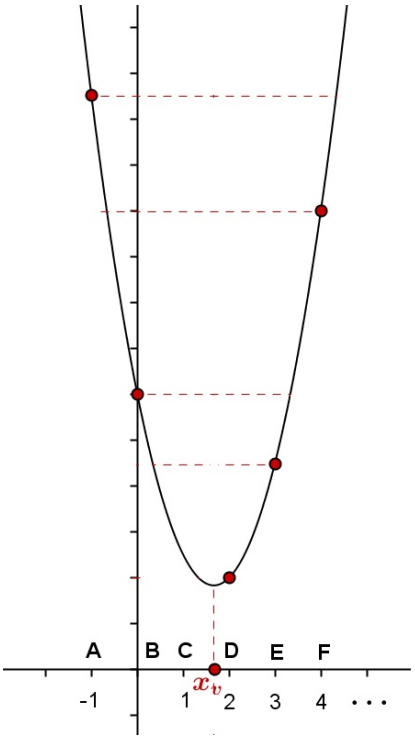
I corresponde ao 9 , $f(9) = 201$, $I \mapsto 201$.

C corresponde ao 3 , $f(3) = 15$, $C \mapsto 15$.

$$445 - 1 - 1103 - 53 - 445 - 1 - 1103 - 201 - 15 - 1$$

Para ajudar os estudantes a responder a segunda parte do item, sugere-se que esbocem o gráfico da função cifradora e observem que os pontos da

parábola referentes às letras do alfabeto não determinam imagens iguais, pois os números correspondentes as letras não são simétricos em relação ao x do vértice.



8) Um polinômio quadrático da forma $f(x) = Ax^2+Bx+C$ com coeficientes inteiros, $A \neq 0$ e entradas inteiras, gera imagens inteiras (propriedade do fechamento em relação as operações de adição e multiplicação dos números inteiros). Considerando o fato de que a parábola é uma curva simétrica em relação ao seu eixo de simetria $x = -\dfrac{B}{2A}$, se o x_v for o ponto médio de dois pontos consecutivos correspondentes às letras do alfabeto, ou seja, se for o ponto médio de dois números inteiros consecutivos, o que ocorre se $B = kA$ com k inteiro, então existe a possibilidade de obtermos cifras iguais para letras distintas, a menos que se estipule as letras do alfabeto por números inteiros maiores (menores) ou iguais ao x do vértice. Neste caso se estaria contrariando a condição de não impor a numeração das letras do alfabeto, ou seja, não escolher o Domínio da função cifradora. Particularmente, se $A = 1$ então $B = k \in Z$, ou seja, todo polinômio quadrático da forma acima, com coeficiente líder $A = 1$, não é uma boa escolha para a função cifradora.

Logo, para atender as condições do problema, basta escolher para função quadrática cifradora, um polinômio da forma $f(x) = Ax^2 + Bx + C$, com coeficientes inteiros, $A \neq 0$ e $B \neq kA$ onde $k \in Z$.

É importante comentar durante a discussão do problema, que este tipo de função quadrática é bijetora devido ao seu domínio ser um conjunto discreto com um número finito de elementos, neste caso, 26 elementos. O seu gráfico é um conjunto de 26 pontos sobre a parábola.

Também é importante comentar que criptografar mensagens utilizando esta técnica, permite determinar duas chaves: uma chave é a função escolhida e a outra a correlação entre as letras do alfabeto e a numeração correspondente, o que não torna esta técnica imune ao ataque por Análise de Frequência.

9) Neste item, existem infinitas soluções, pois temos a situação contrária do item 8). Devemos escolher uma função quadrática $f(x) = Ax^2 + Bx + C$ com A, B e C inteiros, $A \neq 0$ e $B = kA$, de forma que o $x_v = -\dfrac{B}{2A} = -\dfrac{kA}{2A} = -\dfrac{k}{2}$, $k \in Z$, ou seja, o x_v será a média de dois números inteiros. Em seguida, basta determinar valores equidistantes do x_v para as letras.

Por exemplo: Como mencionado no item 8), se escolhermos qualquer função quadrática com $A = 1$, recairemos nesta situação. Portanto, para $f(x) = x^2 - 7x + 13$, temos $x_v = \frac{7}{2} = 3,5$. Basta então, determinar para as letras equidistantes do centro do alfabeto, valores equidistantes do x_v. Uma possibilidade é $m = 3$ e $n = 4$; $l = 2$ e $o = 5$; $k = -1$ e $p = 8$; $j = 9$ e $q = -2$; e assim por diante, observando que para cada par de letras equidistantes do centro do alfabeto, basta determinar os valores resultantes de $\mid x_v - k_i \mid$, $k_i \in Z$, quando x_v for inteiro ou $\mid\mid x_v - 0,5 \mid -k_i \mid$, $k_i \in Z$, quando x_v não for inteiro , onde para cada $i \in \{1, 2, \ldots, 13\}$, k_i representa um valor inteiro distinto.

ATIVIDADE 3: *Explora o conceito de bijeção como condição necessária e suficiente para a inversão de uma função*

Competências e Habilidades:
Competência de área 5 - Modelar e resolver problemas que envolvem variáveis socioeconômicas ou técnico-científicas, usando representações algébricas.
Habilidade 19 - Identificar representações algébricas que expressem a relação entre grandezas.
Habilidade 20 - Interpretar gráfico cartesiano que represente relações entre grandezas.
Habilidade 21 - Resolver situação-problema cuja modelagem envolva conhecimentos algébricos.
Habilidade 22 - Utilizar conhecimentos algébricos/geométricos como recurso para a construção de argumentação.
Habilidade 23 - Avaliar propostas de intervenção na realidade utilizando conhecimentos algébricos.

Ações Didáticas:
Esta atividade pressupõe que os estudantes já tenham realizado a atividade 2. Pode ser trabalhada em grupos como proposto nas atividades anteriores ou de forma individual. É fundamental a utilização de calculadora e desejável a utilização de software de plotar gráficos (Geogebra ou Winplot) para a realização da atividade. O tempo mínimo para a realização de todas as etapas da atividade é de 45 minutos.

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

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

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

COMENTÁRIO: Neste item deve-se observar que $B \neq kA$, ou seja, como visto na Atividade 2, basta estipular qualquer valor distinto para as letras do alfabeto que se estabelecerá uma bijeção. A determinação da função de cifradora 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
$f_3(x) = x^2 + 6x - 2$																										
$f_3^{-1}(x) =$																										

COMENTÁRIO: Neste item deve-se observar que $A = 1$, ou seja, como visto na Atividade 2, é necessário estipular para as letras do alfabeto valores maiores (menores) ou iguais ao 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
$f_4(x) = \|x - 4\|$																										
$f_4^{-1}(x) =$																										

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.

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

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.

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

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, inclusive verificando que a sua inversa é 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
$f_7(x) = \log_5(x+3)$																										
$f_7^{-1}(x) =$																										

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, inclusive verificando que sua inversa é uma função exponencial.

4.2 Atividades de Criptografia para o Ensino de Análise Combinatória

.

O ato de quantificar elementos de um conjunto acompanha o homem desde seu surgimento e está presente em diversas áreas do conhecimento. Em criptografia, a determinação da quantidade de chaves criptográficas induziu pesquisadores a desenvolverem técnicas alternativas ao ataque por força bruta a textos cifrados, como o caso da técnica da análise de frequência e do ataque de Babbage à cifra de Vigenère.

O ensino da Análise Combinatória possibilita sua inserção em vários contextos, dentre eles o da criptografia, conforme proposto nas atividades seguintes.

ATIVIDADE 4: *Explora o conceito de Permutação com elementos repetidos.*

Competências e Habilidades:
Competência de área 1 - Construir significados para os números naturais, inteiros, racionais e reais.
Habilidade 1 - Reconhecer, no contexto social, diferentes significados e representações dos números e operações - naturais, inteiros, racionais ou reais.
Habilidade 2 - Identificar padrões numéricos ou princípios de contagem.
Habilidade 3 - Resolver situação-problema envolvendo conhecimentos numéricos.
Habilidade 4 - Avaliar a razoabilidade de um resultado numérico na construção de argumentos.
Habilidade 5 - Avaliar propostas de intervenção na realidade utilizando conhecimentos numéricos.

Ações Didáticas:
Esta atividade pressupõe que os estudantes já tenham visto o conceito de permutação, particularmente o caso de conjuntos com elementos repetidos. Pode ser incluída em uma lista com outros problemas com enredos em contextos diversos.

Atividade: Para dificultar a análise de frequência em textos cifrados, *Simeone de Crema*, em 1452, propôs a utilização de códigos de substituição homofônica.

Suponha que o conjunto de letras A, B, C, D, E serão substituídas por 10 símbolos distintos da seguinte forma:
Para as letras A e E serão atribuídos 3 símbolos diferentes; para a letra C, 2 símbolos diferentes; e para as letras B e D, um único símbolo.

Quantas são as possíveis correspondências entre essas letras e os símbolos?

SOLUÇÕES e COMENTÁRIOS:

Considerando os 10 símbolos como sendo 1, 2, 3, 4, 5, 6, 7, 8, 9, e 10, podemos dispor as letras e seus respectivos símbolos como exemplificado abaixo.

LETRAS	A			B	C		D	E		
SÍMBOLOS	1	2	3	4	5	6	7	8	9	10

Tem-se 10! permutações distintas dos símbolos, porém, a sequência
(1 2 3)(4)(5 6)(7)(8 9 10) representa a mesma correspondência que a sequência
(2 3 1)(4)(6 5)(7)(10 9 8).

Logo, a quantidade de correspondências entre as letras e seus símbolos é

$$\frac{10!}{3!2!3!} = 50.400.$$

Nesta atividade, utiliza-se a ideia de permutação com elementos repetidos sem utilizar exemplos com anagramas nem mencionar ou mostrar claramente que os elementos se repetem.

ATIVIDADE 5: *Explora o Princípio das gavetas de Dirichlet.*

Competências e Habilidades:
Competência de área 1 - Construir significados para os números naturais, inteiros, racionais e reais.
Habilidade 1 - Reconhecer, no contexto social, diferentes significados e representações dos números e operações - naturais, inteiros, racionais ou reais.

Habilidade 2 - Identificar padrões numéricos ou princípios de contagem.
Habilidade 3 - Resolver situação-problema envolvendo conhecimentos numéricos.
Habilidade 4 - Avaliar a razoabilidade de um resultado numérico na construção de argumentos.
Habilidade 5 - Avaliar propostas de intervenção na realidade utilizando conhecimentos numéricos.

Ações Didáticas:
Esta atividade utiliza o Princípio das gavetas de Dirichlet, assunto geralmente não abordado no ensino básico. Porém, devido a sua simplicidade, os estudantes quase sempre concluem corretamente a ideia da solução, cabendo ao professor comentar e expor aos estudantes o Princípio das gavetas de Dirichlet, que pode ser consultado em [13]. Pode ser incluída em uma lista com outros problemas com enredos em contextos diversos.

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:

Em [13], tem-se a seguinte definição:

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.

Portanto, 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 11 objetos colocados em 5 gavetas, pelo menos uma gaveta conterá pelo menos 3 objetos. Logo, no texto, a letra **e** será cifrada pelo menos 3 vezes pela mesma cifra.

4.3 Atividades de Criptografia para o Ensino de Matrizes

.

As abordagens sobre matrizes no ensino básico, geralmente são feitas de maneira excessivamente conceitual, da mesma forma como abordado em livros mais técnicos de àlgebra linear. Nos livros didáticos, encontramos bons exemplos contextualizados, mas apenas no início do capítulo sobre matrizes, ficando os textos conceituais meras paráfrases do que já existe há longas datas, se eximindo das correlações com a vida real.

As atividades abaixo, apesar de trabalhosas, utilizam conceitos básicos que podem ser apresentados aos estudantes de forma simples e direta.

ATIVIDADE 6: Explora o conceito de multiplicação de matrizes, conceitos básicos sobre matrizes invertíveis e cálculo da inversa de uma matriz 2×2.

Competências e Habilidades:
Competência de área 5 - Modelar e resolver problemas que envolvem variáveis socioeconômicas ou técnico-científicas, usando representações algébricas.
Habilidade 21 - Resolver situação-problema cuja modelagem envolva conhecimentos algébricos.
Habilidade 22 - Utilizar conhecimentos algébricos/geométricos como recurso para a construção de argumentação.
Habilidade 23 - Avaliar propostas de intervenção na realidade utilizando conhecimentos algébricos.

Ações Didáticas:
Esta atividade ilustra uma possível aplicação de conceitos básicos de matriz, possibilitando ao professor extrapolar o cálculo manual, utilizando recursos computacionais e trabalhando com matrizes de ordem maiores que 2, como uma atividade posterior a esta. É importante que o professor ressalte o cálculo da inversa de uma matriz de ordem 2, mecanizando os procedimentos na forma de um algoritmo, o que facilitará a compreensão da importância da utilização de recursos computacionais para o cálculo da inversa de matrizes com ordens maiores. Pode-se trabalhar individualmente ou em grupos, como proposto na atividade 1. É fundamental a utilização da calculadora. Pode ser incluída em uma lista com outros problemas com enredos em contextos diversos.

Atividade: Para cifrar uma mensagem evitando a análise de frequência sobre o texto cifrado, utiliza-se cifras em bloco. Uma forma simples desta técnica é implementada com matrizes representando a mensagem (M) e a chave da cifra (A) para obter o texto cifrado

$$C = A.M$$

Utilizando a tabela abaixo para substituir as letras por números, a chave $A = \begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix}$ e escrevendo a mensagem na matriz $M_{2\times n}$, completando as colunas de cima para baixo e da esquerda para a direita, faça o que se pede:

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

1) Cifre a palavra MATEMÁTICA.

2) Decifre o texto cifrado
$(38 - 53 - 46 - 53 - 66 - 61 - 46 - 57 - 10 - 15 - 16 - 8)$.

SOLUÇÕES e COMENTÁRIOS:

1) Como M corresponde ao 12 , A corresponde ao 0 , T corresponde ao 19 , E corresponde ao 4 , I corresponde ao 8 e C corresponde ao 2 , temos

$$C = \begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix} \times \begin{pmatrix} 12 & 19 & 12 & 19 & 2 \\ 0 & 4 & 0 & 8 & 0 \end{pmatrix} = \begin{pmatrix} 24 & 46 & 24 & 54 & 4 \\ 12 & 31 & 12 & 43 & 2 \end{pmatrix}.$$

Logo, o texto cifrado é $(24 - 12 - 46 - 31 - 24 - 12 - 54 - 43 - 4 - 2)$

2) Para decifrar o texto, fazemos

$$C = A \times M \ ; \ A^{-1} \times A \times M = A^{-1} \times C \ ; \ M = A^{-1} \times C \ ,$$

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

Para determinar a inversa de uma matriz de ordem 2, $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, faz-se

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

De fato,

Como $B \times B^{-1} = I$, temos que $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$;

que gera o seguinte sistema:

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

cuja solução é

$$x = \frac{d}{ad - bc} = \frac{1}{detB} \times d \quad ; \quad y = \frac{-b}{ad - bc} = \frac{1}{detB} \times (-b) \ ;$$
$$z = \frac{-c}{ad - bc} = \frac{1}{detB} \times (-c) \quad ; \quad w = \frac{a}{ad - bc} = \frac{1}{detB} \times a.$$

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

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

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

Logo,

$$M = \begin{pmatrix} \frac{3}{4} & -\frac{1}{2} \\ -\frac{1}{4} & \frac{1}{2} \end{pmatrix} \times \begin{pmatrix} 38 & 46 & 66 & 46 & 10 & 16 \\ 53 & 53 & 61 & 57 & 15 & 8 \end{pmatrix} = \begin{pmatrix} 2 & 8 & 19 & 6 & 0 & 8 \\ 17 & 15 & 14 & 17 & 5 & 0 \end{pmatrix}$$

que gera o texto aberto CRIPTOGRAFIA.

ATIVIDADE 7:

Competências e Habilidades:
Competência de área 5 - Modelar e resolver problemas que envolvem variáveis socioeconômicas ou técnico-científicas, usando representações algébricas.
Habilidade 21 - Resolver situação-problema cuja modelagem envolva conhecimentos algébricos.
Habilidade 22 - Utilizar conhecimentos algébricos/geométricos como recurso para a construção de argumentação.
Habilidade 23 - Avaliar propostas de intervenção na realidade utilizando conhecimentos algébricos.

Ações Didáticas:
Nesta atividade, é fundamental a utilização de calculadora. Trabalha-se conceitos básicos de matriz, principalmente o resultado do produto de uma matriz invertível por sua inversa, ou seja, $A \times A^{-1} = I$. Não há necessidade de se calcular a inversa de uma matriz, apenas efetuar o produto de matrizes. Para isso, seria bem interessante a utilização de algum software que opera matrizes, como o Geogebra por exemplo. Pode-se trabalhar individualmente ou em grupos, como proposto na atividade 1. Pode ser incluída em uma lista com outros problemas com enredos em contextos diversos.

Atividade: Para cifrar uma mensagem aberta M, cujas letras forma substituídas por números conforme a tabela abaixo e arrumadas em blocos (matrizes) $M_{2\times 2}$, completando as colunas de cima para baixo e da direita para a esquerda, opera-se da seguinte forma:

$$A^{-1} \times M \times B^{-t} = C \text{ , onde } A = \begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix} \text{ e } B = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}.$$

Decifre a mensagem cifrada

$$(147 - 72 - 257 - 126 - 192 - 83 - 338 - 147)$$

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

SOLUÇÕES e COMENTÁRIOS:

O principal objetivo desta atividade é que o estudante conclua que cada bloco $M = A \times C \times B^t$.

Depois, basta realizar os cálculos, que devem ser feitos, preferencialmente, utilizando o Geogebra ou, alternativamente, uma calculadora.

Então,

$$M_1 = \begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix} \times \begin{pmatrix} 147 & 257 \\ 72 & 126 \end{pmatrix} \times \begin{pmatrix} 2 & -5 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 17 & 18 \end{pmatrix} \text{ e}$$

$$M_2 = \begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix} \times \begin{pmatrix} 192 & 338 \\ 83 & 147 \end{pmatrix} \times \begin{pmatrix} 2 & -5 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} 8 & 2 \\ 11 & 24 \end{pmatrix}$$

gerando a mensagem aberta BRASILCY, onde as letras C e Y foram incluídas para completar o bloco M_2.

4.4 Atividades Diversas de Criptografia

.

A seguir, algumas atividades envolvendo o tema criptografia, que aparecem em vestibulares e em Olimpíadas de Matemática.

ATIVIDADE 8: Inspirado na questão 24 da primeira fase do Vestibular da Universidade Federal Fluminense de 2005.

Um dispositivo eletrônico usado em segurança modifica a senha escolhida por um usuário, de acordo com o procedimento descrito abaixo.

A senha escolhida deve conter quatro dígitos $S_1S_2S_3S_4$, representados por S_1 , S_2 , S_3 e S_4. Esses dígitos são, então, transformados nos dígitos M_1 , M_2 , M_3 e M_4 da seguinte forma:

$$\begin{pmatrix} M_1 \\ M_2 \end{pmatrix} - P \begin{pmatrix} S_1 \\ S_2 \end{pmatrix} = \begin{pmatrix} M_3 \\ M_4 \end{pmatrix} - P \begin{pmatrix} S_3 \\ S_4 \end{pmatrix}, \text{ onde } P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Se a senha de um usuário, já modificada, é 0110, isto é, $M_1 = 0$, $M_2 = 1$, $M_3 = 1$ e $M_4 = 0$ e sabendo-se que:
• O usuário nasceu no dia 17 de junho (17/06) e que esses dígitos foram utilizados na senha;
• O primeiro dígito da senha do usuário é o menor possível;

Determine a senha escolhida pelo usuário.

SOLUÇÕES e COMENTÁRIOS:

Nesta atividade, o estudante tende a resolver a equação antes de tentar escrevê-la de forma mais simplificada, como a seguir.

Reescrevendo a equação $\begin{pmatrix} M_1 \\ M_2 \end{pmatrix} - P \begin{pmatrix} S_1 \\ S_2 \end{pmatrix} = \begin{pmatrix} M_3 \\ M_4 \end{pmatrix} - P \begin{pmatrix} S_3 \\ S_4 \end{pmatrix}$,

como $A - PB = C - PD$, fazendo $S_1 = a$, $S_2 = b$, $S_3 = c$ e $S_4 = d$, aplica-se algumas propriedade operatórias de matrizes para chegar a

$P(D - B) = C - A$, ou seja,

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} c-a \\ d-b \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix} \quad ; \quad \begin{pmatrix} d-b \\ c-a \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Portanto, tem-se que $\begin{cases} d = b + 1 \\ c = a - 1 \end{cases}$, onde $\{a, b, c, d\} = \{0, 1, 6, 7\}$
.

Temos, então, duas possibilidades: $\begin{matrix} a = 1; & b = 6; & c = 0; & d = 7 \\ a = 7; & b = 0; & c = 6; & d = 1 \end{matrix}$.

Logo, como a é o menor possível, a senha escolhida pelo usuário é 1607.

ATIVIDADE 9: Problema 1 da XVII Olimpíada de Maio, Primeiro nível, 2011.

As quatro palavras codificadas

$$@*X \qquad +\#\& \qquad *@\& \qquad X\Delta+$$

são em alguma ordem

$$\text{AMO} \qquad \text{SUR} \qquad \text{REO} \qquad \text{MAS}$$

Decifrar $X\Delta@*+\#@\&X$.

SOLUÇÕES e COMENTÁRIOS:

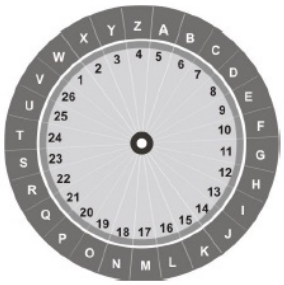
Nas palavras AMO e MAS, temos que as duas primeiras letras estão permutadas e que as terceiras letras são diferentes. Comparando com as palavras codificadas, observa-se que $@*X$ e $*@\&$ possuem esta mesma característica. Observa-se ainda que a letra O está na terceira posição da palavra REO, o que permite concluir que:

$$\begin{array}{ccc} @*X & \Longleftrightarrow & MAS \\ +\#\& & \Longleftrightarrow & REO \\ *@\& & \Longleftrightarrow & AMO \\ X\Delta+ & \Longleftrightarrow & SUR \end{array}$$

Logo, a palavra cifrada $X\Delta@*+\#@\&X$ é $SUMAREMOS$.

ATIVIDADE 10: Questão 2, do nível 1, da segunda fase, da 3ª Olimpíada Brasileira de Matemática das Escolas Públicas, 2007.

Um antigo método para codificar palavras consiste em escolher um número de 1 a 26, chamado chave do código, e girar o disco interno do aparelho ilustrado na figura 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.



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

(b) Codifique OBMEP usando a chave 20.

(c) Chicó codificou uma palavra de 4 letras com a chave 20, mas esqueceu-se de colocar os tracinhos e escreveu 2620138. Ajude o Chicó 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) $23 - 25 - 7 - 25 - 22 - 13$

S U C U R I

b) Existem várias formas de pensar a solução, uma sugestão é fazer

$o \mapsto a + 14$ posições à direita;

$b \mapsto a + 1$ posição à direita;

$m \mapsto a + 12$ posições à direita;

$e \mapsto a + 4$ posições à direita;

$p \mapsto a + 15$ posições à direita;

Como a chave é 20, o a estará na posição 20, onde conclui-se que

$$o \mapsto 8 \quad ; \quad b \mapsto 21 \quad ; \quad m \mapsto 6 \quad ; \quad e \mapsto 24 \quad ; \quad p \mapsto 9$$

Logo, a palavra OBMEP codificada com a chave 20 fica $8-21-6-24-9$.

c) Como a palavra de Chicó tem 4 letras e a palavra codificada tem 7 números, então existe uma única letra correspondente a um número de 1 algarismo.

Fazendo tentativas, temos:

$2 - 620138$ não é possível pois teríamos 62 como o segundo número e o disco vai até o úmero 26;

$26-20138$ é possível, desde que os demais tracinhos fiquem $26-20-13-8$, pois não existe correspondente no disco para os símbolos 01 e 38.

Logo, o texto cifrado é $26 - 20 - 13 - 8$ que, com a chave 20, corresponde à palavra GATO.

d) Normalmente os estudantes fariam algumas tentativas diretas para chegarem ao resultado, o que neste contexto não seria uma escolha ruim. Porém, cabe ressaltar que pode-se diminuir a quantidade de tentativas observando que 52 não é múltiplo de 3, ou seja, a soma de três números consecutivos não pode ser 52. Portanto, os três valores possíveis seriam $26 - 1 - 2$, cuja soma não dá 52, ou $25 - 26 - 1$ que é o único resultado correto.

Logo, a chave é 25.

Capítulo 5

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 desenvolvimentos 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 médio, retirando a matemática do isolamento didático que tradicionalmente se confina no contexto escolar.

No ensino de 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, a utilização de uma cifra homofônica produz um exemplo mais natural da utilização do conceito de permutação com elementos repetidos; e a utilização de

cifras em bloco para fugir da análise de frequência, enfatiza a importância do conceito de matrizes e suas propriedades.

A forma atual em que a criptografia está inserida, induz à 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.

Bibliografia

[1] Secretaria de Educação Básica **(2006)** *Orientações Curiculares para o Ensino Médio*. Brasília: Ministério da Educação, Secretaria da Educação Básica.

[2] MENEZES, A. J. et al. **(1997)** *Handbook of Applied Cryptography*. Boca Raton, FL. CRC Press.

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

[4] STALLINGS, William. **(1999)** *Cripytography and Network security: Principles and Practice*. 2.ed. Prentice Hall.

[5] KAHN, David. **(1967)** *The Codebreakers*. Nova York: Macmillan.

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

[7] COUTINHO, S. C. **(2000)** *Números Inteiros e Criptografia RSA*. 2.ed. SBM

[8] HEFEZ, Abramo. **(2005)** *Elementos de Aritmética*. SBM

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

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

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

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

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

[14] NOGUEIRA, Rio **(1972)** *Lições de Análise Combinatória*. Rio de Janeiro, Editora Fundo de Quintal.

[15] SANTOS, José Plínio de Oliveira **(2007)** *Introdução à Análise Combinatória*. 4.ed. Editora Ciência Moderna.

[16] ANTON, Howard et al. **(2002)** *Álgebra Linear com Aplicações*. Bookman

[17] COSTA, Celso José da, et al. **(2005)** *Criptografia Geral*. Rio de Janeiro, Centro de Estudos de Pessoal

[18] COSTA, Celso José da, et al. **(2005)** *Introdução à Criptografia*. Rio de Janeiro, Centro de Estudos de Pessoal

[19] TERADA, Routo **(1988)** *Criptografia e a Importância das suas Aplicaçõesl*. Revista do Professor de Matemática úmero 12, página 1, SBM.l

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

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

[22] ONUCHIC, Lourdes de La Rosa. **(1999)** *Ensino-Aprendizagem de Matemática Através da Resolução de Problemas.*. São Paulo, Editora UNESP