Flávio Ornellas Loureiro

Tópicos de criptografia para o ensino médio

Universidade Estadual do Norte Fluminense Darcy Ribeiro
Campos dos Goytacazes - RJ

Agosto, 2014

Flávio Ornellas Loureiro

Tópicos de criptografia para o ensino médio

Dissertação apresentada ao Centro de Ciências e Tecnologia da Universidade Estadual do Norte Fluminense Darcy Ribeiro, como parte das exigências para obtenção do título de Mestre em Matemática.

Universidade Estadual do Norte Fluminense Darcy Ribeiro - UENF

Orientador: Prof. Oscar Alfredo Paz la Torre

Universidade Estadual do Norte Fluminense Darcy Ribeiro
Campos dos Goytacazes - RJ

Agosto, 2014

Flávio Ornellas Loureiro
Tópicos de criptografia
para o ensino médio/ Flávio Ornellas Loureiro. – Universidade Estadual do Norte Fluminense Darcy Ribeiro
Campos dos Goytacazes - RJ, Agosto, 2014-
43 p. : il. (algumas color.) ; 30 cm.

Orientador: Prof. Oscar Alfredo Paz la Torre

Dissertação – Universidade Estadual do Norte Fluminense Darcy Ribeiro - UENF , Agosto, 2014.

1. Criptografia. 2. Função. I. Oscar Alfredo Paz la Torre. II. Universidade Estadual do Norte Fluminense Darcy Ribeiro. III. Laboratório de Ciências Matemáticas. IV. Tópicos de Criptografia para o Ensino Médio

CDU 02:141:005.7

Flávio Ornellas Loureiro

Tópicos de criptografia para o ensino médio

Dissertação apresentada ao Centro de Ciências e Tecnologia da Universidade Estadual do Norte Fluminense Darcy Ribeiro, como parte das exigências para obtenção do título de Mestre em Matemática.

Aprovado em 29 de agosto de 2014 pela Comissão Examinadora

Profª. Liliana Angelina León Mescua, D.Sc.
UENF

Prof. Paulo Sérgio Dias da SIlva, D.Sc.
UENF

Profª. Arilise Moraes de Almeida Lopes, D.Sc.
IFF

Prof. Oscar Alfredo Paz la Torre, D.Sc.
UENF
Orientador

Universidade Estadual do Norte Fluminense Darcy Ribeiro
Campos dos Goytacazes - RJ
Agosto, 2014

Este trabalho é dedicado a minha esposa Marília.

Agradecimentos

A Marília, minha esposa, pelo incentivo, pelo apoio durante toda elaboração do trabalho e por estar presente em minha vida.

Aos colegas do curso PROFMAT da UENF pelos dois anos maravilhosos, em especial ao amigo Flávio Miranda, pela parceria nas viagens.

Ao Professor Oscar pelas aulas ministradas e pela orientação no trabalho.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pela bolsa concedida.

"Não há ramo da Matemática, por mais abstrato que seja,
que não possa um dia vir a ser aplicado aos fenômenos do mundo real".
(Lobachevsky)

Resumo

Este trabalho tem como objetivo mostrar, como podemos usar certos tópicos de criptografia, incluindo sua história, para trabalharmos alguns temas de matemática abordados em turmas do ensino médio. De maneira mais específica, usamos a criptografia de substituição para contextualizarmos o uso de funções bijetoras; o conceito de matrizes para trabalharmos a cifra de Hill e análise combinatória para o cálculo da quantidade de chaves de uma cifra. Também apresentamos uma sequência de cinco atividades que relacionam criptografia com os temas citados.

Palavras-chaves: Criptografia. Função. Matriz. Análise Combinatória.

Abstract

This work aims to show how we can use certain topics of encryption, including its history, to work some math topics covered in high school classes. More specifically we use encryption to replacement contextualize the use of bijetoras functions; we use the concept of arrays to work the Hill's cipher and combinatorial analysis for calculating the amount of a cipher keys. We also present a sequence of five activities that relate to the topics mentioned encryption above.

Key-words: Cryptography. Function. Matrices. Combinatorial Analysis.

Lista de ilustrações

Lista de tabelas

Sumário

Introdução

A criptografia é a arte e ciência de fabricar códigos secretos. De maneira mais precisa, é o estudo das técnicas pelas quais uma informação pode ser modificada de forma a ficar oculta, ininteligível, salvo para o destinatário de direito da mensagem. Portanto a função da criptografia é de proteger uma informação. A palavra deriva do grego *Kryptós*,"escondido", e *gráphein*, "escrita".(FIGUEIREDO, 2012b)

A necessidade de se proteger uma informação é antiga. No início, a criptografia era uma ferramenta usada exclusivamente por governos em situações de guerra ou quando desejassem manter uma comunicação segura ou proteger alguma informação vital, que poderia causar danos se caísse em mãos inimigas. E, assim foi por milhares de anos, até a invenção dos computadores e da internet. Hoje a criptografia não é mais uma ciência de uso quase que exclusivamente militar. Não só os governos que precisam proteger informações; empresas e pessoas necessitam da criptografia para proteger suas informações.

A internet é uma grande rede que conecta diversos computadores e isso faz com que diversas informações sejam transmitidas por ela. Mas, essas informações estão suscetíveis a interceptação de terceiros podendo causar danos. Por exemplo: um banco precisa informar a um outro banco de um país diferente sobre uma movimentação financeira. Essa informação será enviada através da rede SWIFT, que é uma rede que conecta os bancos de todos os países. Se essa informação não estiver protegida (cifrada), ela pode ser interceptada por um hacker que poderá modificar os dados da transação. Mas não são apenas as transações financeiras que precisam ser protegidas. Empresas possuem informações que precisam ser protegidas, tais como: detalhes técnicos de um novo produto; previsões de venda; informações estratégicas, etc. Além das empresas, pessoas físicas possuem senhas; dados pessoais que podem ser usados de maneira fraudulenta; dados de cartões de crédito que são usados para transações comercias via internet entre pessoas e lojas, etc. Todos esses exemplos, são situações do cotidiano que podem gerar danos caso suas informações não estejam protegidas.

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

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

A criptografia utiliza diversos ramos da matemática, dentre os quais podemos citar: a cifra de César que está relacionada a aritmética modular; as cifras de substituição com as funções bijetoras; a cifra de Hill com as matrizes invertíveis; o RSA com o problema da fatoração de números inteiros; o Elgamal com o problema dos logaritmos discretos; as curvas elípticas ao problema do logaritmo discreto em corpos finitos e diversos outros casos. Por causa dessa intensa relação entre matemática e criptografia, e seu imprescindível uso nos temas atuais, propomos apresentar a relação existente entre o tema criptografia e conteúdos de matemática para o ensino médio, mais especificamente pesquisar, selecionar e desenvolver atividades didáticas de conteúdos matemáticos do ensino médio abordando o tema de criptografia.

O tema de criptografia abordada nas turmas de ensino médio

> Permite interligar os conteúdos matemáticos à situações do mundo real e ajuda a desenvolver habilidades e competências na resolução de problemas, a criar estratégias de resolução, a ter autonomia durante o processo de aprendizagem, com isso, tornando-os mais autoconfiantes e concentrados na realização das atividades.(GROENWALD E FRANKLE, 2008, *apud* (OLGIN; GROENWALD, 2011, p.12))

Além de ajudar a criar estratégias para resolução de problemas,

> Acredita-se que a inclusão de atividades que envolvam conceitos de criptografia pode ajudar a diminuir a existência de aulas mecânicas, onde o professor, através de atividades práticas, poderá mostrar a aplicabilidade dos conceitos trabalhados em sala de aula, relacionando-os a fatos importantes ocorridos na atualidade.(OLIVEIRA; KRIPKA, 2011, p.12)

Afim de apresentar uma visão geral do trabalho, fornecemos uma breve descrição dos temas abordados em cada capítulo.

No primeiro capítulo abordaremos a história da criptografia, as suas primeiras ocorrências e os seus avanços ao longo dos anos, com a intenção de motivar o aprendizado .No capítulo seguinte, mostraremos como utilizar as funções bijetoras para se montar uma cifra de substituição e as funções de várias sentenças para criarmos a cifra de César. Também usaremos o conceito de matrizes para detalharmos o funcionamento da Cifra de Hill e por fim, utilizaremos algumas ferramentas de análise combinatória para calcularmos a quantidade de chaves de uma cifra. O capítulo 3 é dedicado a discutir como os dois principais criptossistemas atuais, o RSA e o ECC, estão fundamentados na matemática. No último capítulo apresentamos algumas propostas de atividades envolvendo o tema, para serem usadas em salas de aula com a intenção de reforçar conteúdos já mencionados.

1 História da Criptografia

1.1 Origens da Criptografia

Segundo Singh (2011), os primeiros relatos de técnicas para proteger uma informação foram narradas por Hérodoto, "o pai da história". Ao narrar o conflito entre Grécia e Pérsia, em 480 a.C., Heródoto nos conta que Xerxes, rei dos Persas, havia planejado durante 5 anos um ataque surpresa a Grécia. Contudo um grego chamado Demarato, que morava na cidade persa de Susa, ao saber dos planos para o ataque, resolveu alertar ao seus conterrâneos sobre a invasão de Xerxes. Porém Demarato sabia que deveria transmitir a informação do ataque com segurança pois, o perigo de ser descoberto era grande, então para garantir que a mensagem chegasse com êxito, ele raspou a cera de um par de tabuletas de madeira, e escreveu o que Xerxes pretendia fazer, depois a mensagem foi coberta com cera novamente. Assim se um guarda interceptasse a mensagem, a tabuleta estaria em branco. A mensagem chegou ao destinatário e quando Xerxes resolveu atacar os gregos, eles já estavam preparados e com isso não conseguiu realizar o seu objetivo de conquistar o povo grego.

A história narrada por Heródoto mostra uma das primeiras técnicas para trazer privacidade a uma troca de informações, a esteganografia. A esteganografia consiste em esconder a mensagem. A segurança da informação vem da tática de simplesmente esconder a informação. É uma ciência considerada irmã da criptografia. Diversas técnicas esteganográficas surgiram ao longo dos anos. Um exemplo é o microponto, que consiste em reduzir uma foto de um texto até transformá-la em um ponto. O microponto era então oculto sobre o ponto final de uma carta aparentemente inofensiva. Tal técnica foi praticada pelos alemães durante a 2ª guerra mundial (SINGH, 2011). Mas a esteganografia sofre de uma fraqueza fundamental. Se a mensagem for descoberta, então o conteúdo da comunicação secreta é imediatamente revelado. A diferença entre esteganografia e a criptografia é que, o objetivo do primeiro é de esconder a mensagem, enquanto a do segundo é de ocultar o significado da mensagem. A vantagem da criptografia sobre a esteganografia é que, se o inimigo interceptar a mensagem ela estara codificada, logo será ininteligível e seu conteúdo não será revelado. Atualmente, em alguns casos, se usa uma combinação das duas afim de oferecer mais segurança (STALLINGS, 2004).

1.2 Citale Espartano e a Cifra de César

Um dos primeiros aparelhos criptográficos a que se tem conhecimento é o citale espartano, que data do século V antes de Cristo (FIGUEIREDO, 2012b). O citale consiste

num bastão de madeira em volta do qual é enrolada uma tira de couro ou pergaminho (Figura 1). O remetente escreve a mensagem ao longo do comprimento do citale e depois desenrola a tira, que agora parece conter uma série de letras sem sentido. O mensageiro então leva a tira de couro, e às vezes pode escondê-la usando-a como cinto, com as letras ocultas na face de dentro. Para decodificar a mensagem, o destinatário simplesmente enrola a tira de couro em torno de um citale de mesmo diâmetro do que foi usado pelo remetente. A técnica do citale consiste em uma cifra de transposição, isto é, as letras do texto claro são embaralhadas formando um anagrama, que é o texto cifrado.

Figura 1 – Citale Espartano

. Disponível em:<http://pt.wikipedia.org/wiki/C%C3%ADtala>. Acesso em jan.2014

Já o primeiro relato sobre uma cifra de substituição, onde as letras do texto claro são substituídas por outra, aparece no *Kama-sutra*. O Kama-sutra é um texto que data do século IV escrito pelo estudioso brâmane Vatsyayana, baseado em manuscritos que datam do século IV a.C. O texto recomenda que as mulheres devem estudar 64 artes, incluindo culinária, vestuário etc. O número 45 da lista é a *mlecchita-vikalpa*, a arte da escrita secreta, justificada de modo a ajudar as mulheres a esconderem os detalhes de seus relacionamentos (SINGH, 2011). A técnica consistia em um aparelhamento ao acaso das letras do alfabeto, substituindo-se cada letra na mensagem original por seu par.

O primeiro documento que usou uma cifra de substituição para propósito militar foi feito Imperador Julio César. A cifra de César, como ficou conhecida, consiste em deslocar as letras do texto claro em 3 casa para direita, sendo portanto uma cifra de substituição.

Exemplo 1 *Utilizando a cifra de César, vamos cifrar a mensagem "atacar amanha", deslocando o alfabeto em 3 casas. Na primeira linha da tabela temos o alfabeto normal, e na segunda linha o alfabeto deslocado em 3 casas para a direita.*

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*
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*

A primeira letra do texto claro é A e está será substituída pela letra D. Em seguida, a letra T pela letra W. Portanto, o texto cifrado fica assim: DWDFDUDPDQKD.

1.3 Origens da Criptoanálise e a Análise de Frequência

Paralelamente ao desenvolvimento da criptografia, ocorre o desenvolvimento da criptoanálise que é a ciência que estuda as técnicas para obtenção da informação sobre a mensagem original, a partir do texto cifrado. São as técnicas usadas para se "quebrar" a mensagem cifrada.

No século IX, o cientista al-Kindi, conhecido como o filósofo dos árabes, publica um trabalho intitulado "Um manuscrito sobre a decifração de mensagens criptográficas", onde nos apresenta a técnica de análise de frequência (SINGH, 2011).

Cifras de substituição como a do Kama-sutra e a de César, são cifras de substituição monoalfabética. Cifras de substituição monoalfabéticas, são cifras em que cada letra do texto claro é substituída sempre pela mesma letra no texto cifrado. Esse comportamento revela certos padrões no texto cifrado. Observa-se no exemplo 1 que a letra A é sempre trocada pela letra T no texto cifrado.

Se pensarmos em termos da língua portuguesa, percebe-se que algumas letras ocorrem com mais frequências que outras. As vogais ocorrem com mais frequência do que as consoantes. Com isso, é possível analisar a frequência de ocorrência de cada letra do alfabeto e construir uma tabela de frequência (Tabela 1). A tabela abaixo mostra a frequência de cada letra da língua portuguesa (FIGUEIREDO, 2012b).

A	B	C	D	E	F	G	H	I	J	K	L	M
14.63%	1.04%	3.88%	4.99%	12.57%	1.02%	1.30%	1.28%	6.18%	0.40%	0.02%	2.78%	4.74%

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
5.05%	10.73%	2.52%	1.20%	6.53%	7.81%	4.74%	4.63%	1.67%	0.01%	0.21%	0.01%	0.47%

Tabela 1 – Frequência do Alfabeto Português

Essa forma de comportamento das letras permitiu elaborar uma forte ferramenta para a criptoanálise, a análise de frequência. O que o ataque de análise de frequência faz é identificar em um texto cifrado, a porcentagem de ocorrência de cada letra e montar as associações. Por exemplo, se em um texto cifrado identificarmos que as maiores ocorrências são das letra W, M e P então as substituiremos pelas letras A, E e O respectivamente,

pois são as que possuem a maior frequência na língua portuguesa, conforme mostra a tabela. Essa técnica combinada com outras informações estatísticas referente a frequência de ocorrência de letras em um texto permite decifrar um texto onde a cifragem foi feita utilizando uma cifra de substituição monoalfabética.

O surgimento do ataque de análise de frequência fez com que as cifras de substituição monoalfabética se tornassem obsoletas. Coube nesse momento aos criptógrafos desenvolverem uma nova cifra que se prove imune ao ataque de análise de frequência.

O surgimento da criptoanálise foi um grande avanço na história da criptografia. O próximo passo ocorre na Europa durante a renascença, onde o italiano Leon Battista Alberti cria a cifra poliafabética.

1.4 Cifra de Vigenère

Leon Battista Alberti (1404 - 1472) foi um pintor, músico, escultor, arquiteto e humanista italiano. Alberti era amigo de um secretário do Papa chamado Leonardo Datto. Um dia, por volta de 1460, em uma conversa nos jardins do vaticano, Dato levantou a questão das cifras. Dato em sua função tinha que lidar com textos cifrados enviados pelo vaticano ou interceptado por espiões e confiar em outros para decifrá-los. O resultado das conversas com Alberti, resulta no tratado *De Cifris*, de 1467, em que Alberti escreveu e constitui o primeiro texto sobre cifras polialfabéticas (SINGH, 2011).

As cifras polialfabéticas são cifras que trabalham com vários alfabetos cifrados, sendo cada letra do texto claro substituída pela referente no alfabeto cifrado, porém sempre alternando o alfabeto cifrado.

O que Alberti propôs foi o uso de dois alfabetos cifrados, usados alternadamente, de modo a confundir os criptoanalistas em potencial.

Exemplo 2 *Vamos cifrar a mensagem "CARRO" com os dois alfabetos cifrados abaixo.*

$Original:$	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
$Cifrado1:$	R	X	B	G	I	L	N	M	C	S	A	E	Q	T	D	K	H	O	Z	W	V	F	Y	U	P	J
$Cifrado2:$	G	L	K	J	H	G	F	D	Z	A	P	O	I	U	Y	T	R	S	E	W	Q	B	N	M	C	V

A primeira letra C será substituída pela letra correspondente no alfabeto cifrado 1, no caso a letra B. Já a segunda letra da mensagem, A, será substituída pela correspondente no segundo alfabeto, no caso a letra G. A terceira letra do texto original será substituída pela letra correspondente no alfabeto cifrado 1. E assim segue o algoritmo de cifragem. O resultado obtido é BGOSD.

A vantagem crucial do sistema de Alberti é que a mesma letra do texto original não aparece necessariamente como uma única letra no texto cifrado. No caso do exemplo anterior, em um momento a letra R foi substituída pela letra O e em outro momento pela letra S.

Alberti também foi um dos primeiros a projetar e usar um dispositivo que facilitava o processo criptográfico. Este dispositivo ficou conhecido como Disco de Alberti (Figura 2).

Figura 2 – Disco de Alberti

Disponível em:<http://webdehistoria.blogspot.com.br/2014/05/leon-battista-alberti.html> Acesso em fev.2014

De acordo com Singh (2011), através do trabalho de Alberti e de outros que contribuiram, como Johannes Tritheminus e Giovanni Porta, o diplomata francês Blaise Vigenère desenvolve a cifra polialfabética mais conhecida, a cifra de Vigenère. A cifra é similar a cifra de Alberti, mas em vez de trabalhar com apenas 2 alfabetos cifrados, Vigenère trabalha com uma tabela que consiste no alfabeto escrito 26 vezes em diferentes linhas, cada um deslocado ciclicamente do anterior por uma posição e uma chave para cifrar e decifrar a mensagem (Figura 3).

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

Figura 3 – Imagem da Tabela de Vigenère

Disponível em:<http://pt.wikipedia.org/wiki/Cifra_de_Vigen%C3%A8re>. Acesso em fev.2014

Exemplo 3 *Vamos cifrar a palavra AMERICA usando a chave ROMA. O primeiro passo é montar o quadro de Vigenère, conforme a tabela acima.*

A primeira letra do texto cifrado será a interseção da coluna A com a linha R (primeira letra do texto claro com a primeira letra do texto cifrado). Obtemos R. O segundo passo é a interseção da coluna M com a linha O, resultando na letra A. prosseguimos dessa maneira temos:

texto claro: a m e r i c a
chave: R O M A R O M
texto cifrado: R A Q R Z Q M

A grande vantagem da cifra de Vigenère é que ela é imune à análise de frequência e possui um número grande de possíveis chaves.Isso fez com que a cifra ficasse conhecida como *le chiffre indechiffrable* (a cifra indecifravél).

Com uma cifra imune ao principal ataque criptoanalítico conhecido, o ataque de análise de frequência, coube aos criptoanalistas darem o próximo passo no desenvolvimento da história da criptografia. Esse passo veio quase 300 anos depois da invenção da Cifra de Vigenère e foi dado pelo oficial prussiano Friedrich Kasiski (1805-1881), um oficial de infantaria. Em 1863, Kasiski publica o livro "Die Geheimschriften und die Dechiffrierkunst"(Escrita secreta e a arte da decifragem) que relata o primeiro método para quebrar as cifras polialfabéticas (SINGH, 2011). O método ficou conhecido como Exame de Kasiski.

Kasiski percebeu uma fraqueza na cifra de Vigenère. Essa fraqueza vinha do fato de que a chave se repete. Por exemplo , uma palavra chave como SOL, de 3 letras, faria com que a primeira letra, e daí a cada 3 letras do texto, seja cifrado pela letra S, a segunda letra e daí a cada 3 letras, pela letra O, e a terceira e todas as 3 letras daí em diante pela letra L. São então, três cifras de César usadas em sequência. Percebe-se então que, se for possível descobrir o comprimento da palavra chave, então pode-se usar a análise de frequência em cada conjunto de letras cifradas com o mesmo alfabeto.

De forma independente, o matemático inglês Charles Babbage, também conseguiu quebrar a cifra de Vigenère, inclusive antes de Kasiski mas foi forçado a manter silêncio pelo governo inglês e não pode publicar a sua descoberta. Só foi revelado pelo governo inglês a descoberta de Babbage em 1887, 24 anos depois da descoberta de Kasiski (SINGH, 2011).

Graças a descobertas feitas por Kasiski e Babbage, a cifra de Vigenère não era mais segura. Embora os criptógrafos tenham criados novas cifras, nada de grande importância surgiu durante a segunda metade do século XIX. O próximo grande evento da criptografia, seria uma reencarnação do disco de Alberti que criou uma geração nova de cifras mais difíceis de serem quebradas do que qualquer outra usada anteriormente.

1.5 A Máquina Enigma

O próximo grande marco na história da criptografia é decorrente da 2ª guerra mundial: a máquina de cifragem Enigma. Esta máquina representa um divisor de águas entre a criptografia clássica e a moderna - a criptografia antes e depois da existência do computador.

Em 1918 o inventor alemão Arthur Scherbius (Figura 4) e seu amigo Richard Ritter fundaram uma empresa, a Scherbius & Ritter. Era uma firma de engenharia inovadora que trabalhava com tudo, de turbinas a travesseiros aquecidos. Scherbius estava encarregado da área de pesquisa e desenvolvimento e buscava sempre novas oportunidades. Um de seus projetos era substituir os sistemas de criptografia inadequados, usados na Primeira Guerra Mundial, trocando-se as cifras de papel e lápis por uma forma de cifragem que usasse a tecnologia do século XX. Tendo estudado engenharia elétrica em Hanover e Munique, ele desenvolveu uma máquina criptográfica que era, basicamente, uma versão elétrica do disco de cifras de Alberti. Chamada de Enigma, a invenção de Scherbius se tornaria uma peça fundamental para o surgimento dos primeiros computadores (SINGH, 2011).

Figura 4 – Arthur Scherbius

Disponível em:<http://enigma.umww.pl/index.php?page=Scherbius>. Acesso em abr.2014

Com aparência de uma máquina de escrever, a mensagem era cifrada e decifrada usando este mesmo modelo de máquina. A máquina Enigma era composta de um teclado usado para digitar as letras do texto claro, uma unidade misturadora, que cifra cada letra, transformando-a na letra correspondente da mensagem cifrada, e um mostrador consistindo em várias lâmpadas para identificar as letras do texto cifrado (Figura 5). O coração da enigma era os misturadores. A máquina Enigma tradicional usava três misturadores, tendo cada misturador 26 posições possíveis. A posição inicial dos misturadores dentro da câmara formavam a chave da cifra.

A utilização da Enigma era muito simples. Depois que a configuração da chave era

Figura 5 – Máquina Enigma

Disponível em:<http://www.ieeeghn.org/wiki/index.php/The_encryption_war_of_WWII:_the_Enigma_encryption_machine>. Acesso em jun.2014

acertada pelo operador, o que significava determinar a ordem dos misturadores, o operador teclava uma letra, o comando estimulava o circuito elétrico que percorria os misturadores passando pelo refletor, voltava pelos misturadores e finalmente iluminava a letra cifrada no painel luminoso. O operador escrevia em um papel a letra cifrada. Após a composição, a mensagem cifrada era, em seguida, transmitida principalmente pelo rádio.

A máquina enigma era usada em todos os níveis do governo e os alemães estavam seguros de que haviam criado uma máquina indecifrável. O esforço para decifrar as mensagens geradas pela Enigma, necessitou de um esforço realizado primeiro pelos poloneses e franceses e mais tarde pelos ingleses.

Ainda de acordo com Singh (2011), 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 Rejewki foram muito importante apesar de não conclusivas. Seu trabalho continuou e foi concluído com sucesso pela equipe inglesa liderada por Alan Turing e outros, em Bletchey Park, na Inglaterra.

Para realizar o trabalho como uma resposta a alta mecanização da Enigma, Alain Turing e seus colaboradores desenvolveram dois tipos de máquina para manipular as cifras interceptadas: a primeira foi denominada Bomba e a segunda Colossus. Esta última por ser programável, é considerada precursora dos modernos computadores.

A grande dificuldade encontrada pela equipe de Bletchey Park 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 máquina Enigma foi um grande avanço para o mundo da criptografia. O próximo grande passo ocorrerá nos anos 70 com o desenvolvimento da criptografia de chave pública e do RSA. Esse tema será abordado quando tratarmos de criptografia e atualidades.

2 Tópicos de Criptografia aplicados na Matemática do Ensino Médio

Conforme citamos na introdução, a criptografia faz uso de diversos áreas da matemática. Abaixo apresentamos um quadro, contendo alguns exemplos dessa conexão entre criptografia e matemática (Tabela 2):

Criptogramas	Conteúdos de Aritmética
Código ISBS	Aritmética Modular
Cifra de Substituição	Função Linear; quadrática Imagem de Função; Cálculo da função inversa
Cifra de Substituição	Potenciação; Equações exponenciais; Logaritmo
Cifra de Hill	Matrizes; Multiplicação de Matrizes; Operações com Matrizes; Matriz Inversa
RSA	Aritmética Modular; Números Primos
ECC	Curvas Elípticas; Corpos Finitos

Tabela 2 – Atividades didáticas envolvendo criptografia

Neste segundo capítulo temos como objetivo mostrar, como podemos trabalhar temas de matemática ensinados em turmas de ensino médio, utilizando algumas ferramentas criptográficas. De maneira mais detalhada, iremos relembrar no primeiro momento como podemos usar as funções bijetoras para criarmos cifras de substituição. Na segunda parte usaremos a Cifra de Hill para trabalharmos com as operações matriciais e por último, as ferramentas de análise combinatória para calcularmos o número de chaves de uma cifra. O critério utilizado para escolha do sistema criptográfico citados acima, é devido a sua fácil compreensão e também por estar ligado diretamente a conteúdos trabalhados no ensino médio.

A criptografia é a ciência responsável por desenvolver técnicas que permitem proteger uma informação, isto é, tornar o texto ininteligível de modo que apenas o receptor de direito da mensagem possa ler. Também é responsável pela operação oposta, a de "quebrar" uma mensagem protegida, ramo da criptografia chamado de criptoanálise.

Uma mensagem aberta legível para todos é chamado de texto normal ou texto claro. O processo de converter uma texto normal em algo ininteligível é chamado cifragem. A decifragem é a tarefa oposta, ou seja, converter o texto cifrado em texto normal. Os processos utilizados para cifragem são chamados de cifras ou criptossistemas.

Toda cifra depende de uma chave e de um algoritmo de cifragem. A determinação da chave é que dá início ao algoritmo de cifragem (Figura 6). Se a chave usada para cifrar é

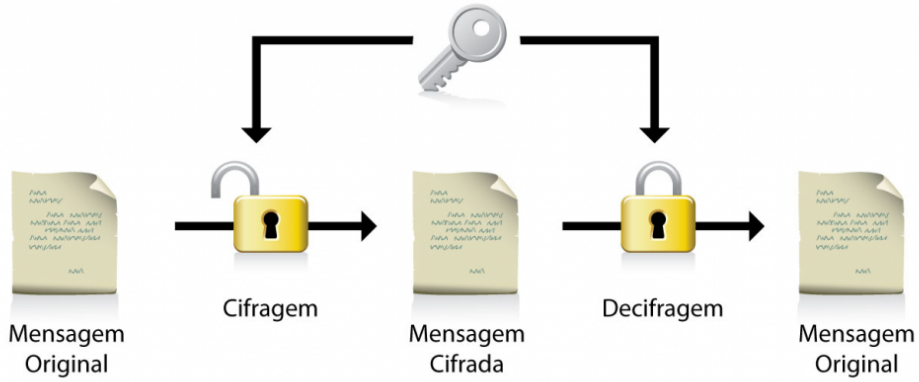


Figura 6 – Esquema de cifragem e decifragem

Disponível em:<http://www.di.ufpe.br/ flash/ais98/cripto/criptografia.htm>. Acesso em fev.2014

a mesma usada para decifrar então a cifra é dita simétrica. Mas se a chave usada para cifrar for diferente da usada para decifrar então, a cifra é dita assimétrica. As cifras simétricas podem ser classificadas em transposição ou substituição. As cifras de transposição são anagramas do texto claro, isto é, consiste em embaralhar as letras do texto claro. Já nas cifras de substituição, as letras do texto claro são substituídas por outras letras.

2.1 Cifra de Substituição

As cifras de substituição são aquelas em que a cifragem é feita pela substituição de cada letra por outra letra na língua utilizada. Para criarmos uma cifra de substituição precisamos estabelecer uma regra para cifrarmos e uma regra oposta para decifrarmos. Nesse momento, é que utilizamos as funções.

As funções são regras que dizem como associar dois elementos de maneira ordenada. Dentro desse universo temos as funções bijetoras, que são funções com uma via para ir e uma via para voltar. A cifragem do texto corresponde a ida e a decifragem à volta.

Vamos fazer então um breve resumo do conceito de função e as condições necessárias para que a função seja bijetora.

Definição 1 (Função) *Sejam A e B conjuntos diferentes do vazio. Uma relação f de A em B é uma função, se e somente se, todo elemento de A estiver associado, por meio de f, a um único elemento de B. O conjunto A é chamado domínio da função e o conjunto B contra-domínio.*

É importante nesse momento relembrar os conceitos de função injetora e sobrejetora,

pois são condições necessárias para que possamos estabelecer a função inversa, responsável pela decifragem do texto.

Definição 2 (Função Injetora) *Uma função f é dita injetora se para dois elementos distintos x_1 e x_2 do domínio, temos $f(x_1) \neq f(x_2)$.*

Uma boa maneira de determinarmos se certa função é injetora, é traçar linhas horizontais pelo seu gráfico. Se alguma linha intercepta o gráfico em mais de um ponto então, a função não é injetora.

Definição 3 (Função Sobrejetora) *Uma função f é sobrejetora, se cada ponto do contra-domínio é a imagem de pelo menos um ponto no domínio, isto é, se para cada $y \in B$ existe ao menos um $x \in A$ tal que $f(x) = y$.*

Definição 4 (Função Bijetora) *Se uma função f é injetora e sobrejetora, então dizemos que f é uma função bijetora.*

Uma condição necessária e suficiente para que uma função possua inversa, está estabelecida no teorema abaixo.

Teorema 1 *Uma função f admite função inversa, se e somente se, f for uma função bijetora.*

O importante de garantirmos que a função possua uma inversa é para fazermos a decifragem do texto. Veja que uma f associa um elemento de A há um elemento de B. Já a função inversa, f^{-1}, associa cada elemento de B há um elemento de A.

Vamos agora há um exemplo onde usaremos uma função bijetora para montarmos uma cifra de substituição.

Exemplo 4 *Vamos considerar o seguinte exemplo: Alice e Bob desejam trocar uma mensagem em sigilo. Eles decidem secretamente, antes de começar a troca de mensagem, que irão usar a função $f(x) = 2x + 1$ para cifrar a mensagem. Essa função será o nosso algoritmo de cifragem. Antes de começar a cifrar, Alice constrói uma tabela, da qual Bob tem conhecimento, para associar cada letra a um número. Digamos que Alice tenha construído a seguinte 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

O valor das letras nessa tabela corresponde ao domínio da função.

A mensagem que Alice deseja cifrar é "VAMOS NOS ENCONTRAR AMANHA". Primeiro ela deverá transformar cada letra da mensagem em um número de acordo com a tabela. Por exemplo, a letra V se transforma no número 21. A letra A no número 0. A letra M no número 12 e assim sucessivamente.

A mensagem então se transforma na seguinte sequência de dígitos:

21 - 0 - 12 - 14 - 18 - 13 - 14 - 18 - 4 - 13 - 2 - 14 - 13 - 19 - 17 - 0 - 17 - 0 - 12 - 0 - 13 - 7 - 0

Agora Alice deve usar a função $f(x) = 2x + 1$ para codificar a mensagem. Para isso, ela deverá calcular os valores numéricos dos números que substituem a mensagem.

$$\begin{aligned} f(21) &= 2.21 + 1 = 43 \\ f(0) &= 2.0 + 1 = 1 \\ f(12) &= 2.12 + 1 = 25 \\ &\vdots \end{aligned}$$

Quando Alice terminar os cálculos, irá encontrar os seguintes valores:

43 - 1 - 25 - 29 - 37 - 27 - 29 - 37 - 9 - 27 - 5 - 29 - 27 - 39 - 35 - 1 - 35 - 1 - 25 - 1 - 27 - 15 - 1

Essa sequência de números é que será enviado para Bob.

Ao receber a mensagem, Bob deverá usar a função inversa da função usada para cifrar a mensagem para determinar o conteúdo real da mensagem. Como ele sabe que foi usada a função $f(x) = 2x + 1$, então ele deverá ser capaz de determinar a função inversa.

$$\begin{aligned} x &= 2f^{-1}(x) + 1 \\ x - 1 &= 2f^{-1}(x) \\ f^{-1}(x) &= \frac{x-1}{2} \end{aligned}$$

Temos que $f^{-1}(x) = \dfrac{x-1}{2}$ é a função inversa da função usada para cifrar a mensagem.

Agora o que Bob precisa é usar a função inversa em cada valor recebido por Alice para determinar os valores originais e juntamente com a tabela determinar a mensagem original.

Aplicando a função inversa em alguns valores, temos:

$$f^{-1}(43) = \frac{43-1}{2} = 21$$
$$f^{-1}(1) = \frac{3-1}{2} = 0$$
$$f^{-1}(25) = \frac{25-1}{2} = 12$$
$$\vdots$$

Observe que estamos obtendo os valores iniciais, antes da função de cifragem. Ao procurar os valores na tabela, Bob consegue ler a mensagem.

Nesse exemplo, vimos como podemos trabalhar o conceito de função no tema de criptografia. No caso do exemplo optamos por uma função do 1° grau, onde facilmente podemos mostrar ser injetora e como o contra-domínio será a sequência de valores obtida por Alice, então temos uma função bijetora. Mas o professor tem a liberdade de utilizar qualquer função. Por exemplo, pode utilizar uma função exponencial e sua inversa que é o logaritmo. Poderá usar uma função com a operação de módulo e verificar com os alunos se é uma boa escolha.

Exemplo 5 *Digamos agora que a função escolhida para a cifragem seja $f(x) = x^2$. Como a função é do 2º grau o seu gráfico é uma parábola, se considerarmos o seu domínio como sendo os reais, o que nos permite concluir que a função não é injetora. Mas veja que como estamos falando do processo de cifragem, o nosso domínio se restringe aos 26 valores da tabela. Como os pontos ficam à direita do vértice da parábola, a função é injetora e podemos usar a inversa $f^{-1}(x) = \sqrt{x}$.*

O fato dos pontos do domínio ficarem à direita do vértice é que nos permitiu utilizar a função, mas se tivéssemos usado a função $f(x) = x^2 - 12x + 36$ então teríamos pontos à esquerda e à direita do vértice, $(6, 0)$, o que faz com que a função não seja uma boa escolha, pois no cálculo da inversa teríamos alguns número no contra-dominio sendo associado a dois valores no domínio, isto é, estaríamos associando a duas letras, o que poderia causar problemas durante a tradução.

Exemplo 6 *Cálculo do vértice da função $f(x) = x^2 - 12x + 36$.*

$$X_v = \frac{-b}{2a} = \frac{12}{2} = 6$$
$$Y_v = \frac{-(b^2 - 4ac)}{4a} = \frac{0}{4} = 0$$

Os pontos 0,1,2,3,4 e 5, que estão a esquerda do vértice tem o mesmo valor numérico que os pontos 12,11,10,9,8 e 7, respectivamente, que estão a direita do vértice. A função não é injetora, logo também não é bijetora.

A maneira de contornarmos o ocorrido acima seria redefinir os valores da tabela, adicionando 6 unidades a cada valor da tabela de associação do alfabeto aos números, dessa maneira estamos deslocando os pontos para a direita do vértice.

Veja que o professor tem a oportunidade de fazer o aluno explorar e compreender melhor o comportamento das funções.

Exemplo 7 *Digamos agora que Alice deseja usar a função $f(x) = x^2 - 4x + 4$. Essa função para montar a cifra de substituição é uma boa escolha? A resposta é não, pois como no exemplo anterior, não é uma função bijetora se considerarmos os valores da tabela do exemplo como domínio. Veja que $f(1) = f(3) = 1$, logo não é injetora e nem bijetora.*

2.2 Cifra de César

Conforme mencionado no primeiro capítulo, a Cifra de César foi usada pelo imperador Júlio César para se comunicar em segurança com seus subordinados. A cifragem, no caso específico do imperador, consistia em reescrever o texto claro deslocando cada letra do texto em 3 casas para direita. Podemos pensar na chave com sendo o número 3 e o algoritmo de cifragem como o processo de deslocar para a direita. Para decifrar a mensagem e obter o texto claro, o receptor da mensagem precisa fazer a operação inversa, isto é, deve deslocar cada letra do texto cifrado em 3 casas para a esquerda.

Toda essa operação envolvendo a cifra de César pode ser escrita em termos matemáticos, usando o conceito de aritmética modular. Mas como o conteúdo não é trabalhado nas turmas de ensino médio, propõe-se o uso de função com várias sentenças.

Para montarmos a cifra de César usando o conceito de função com várias sentenças, precisamos novamente criar uma tabela para associarmos as letras do alfabetos há números inteiros. Usaremos novamente a tabela abaixo.

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

Para fazermos a cifragem usando o método de César, trabalharmos com a seguinte expressão:

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

onde x representa a posição da letra e L a quantidade de casa que será deslocada. O termo L da expressão é a chave da cifra. No caso específico do imperador César, o

valor de L é 3. O motivo de se trabalhar com uma função duas sentenças, é que se o valor numérico da função passar de 25, é necessário associar ao início da tabela. Percebe-se que a função é bijetora, que é a condição estabelecida para criarmos uma cifra de substituição.

Exemplo 8 *Alice deseja enviar uma mensagem confidencial para o seu amigo Bob. Ela combina antes que irá usar a Cifra de César e que chave será $L = 15$. A mensagem é ME ENCONTRE AMANHA.*

A expressão que iremos usar para cifrar é:

$$f(x) = \begin{cases} x + 15, \text{ se } 0 \leq x \leq 10 \\ x - 11, \text{ se } 10 < x \leq 25 \end{cases}$$

A letra M corresponde, segundo a tabela, o número 12. Como o número 12 está no segundo intervalo usa-se a segunda sentença.

$$f(12) = 12 - 11$$
$$f(12) = 1$$

Portanto a letra M será substituída pela letra B. Prosseguindo dessa maneira para as demais letras do texto claro, temos a seguinte mensagem cifrada: BTTCRDCIGTPBPCWA.

Veja que esse tipo de cifra contém poucas opções de chaves, apenas 25. Pois como o intervalo do domínio é de $0 \leq x \leq 25$, temos que $0 \leq L \leq 25$. Esse modelo de cifra pode ser facilmente quebrada se tentarmos um ataque de força bruta, que consiste em testa todas as opções de chaves até determinarmos um texto que tenha sentido.

Para se fazer a decifragem, utiliza-se a função inversa da função cifradora.

Exemplo 9 *Bob recebeu de Alice a seguinte mensagem:BTTCRDCIGTPBPCWA. Ele sabe que foi usado a Cifra de César e que chave é $L = 15$. Para decifrar a mensagem, Bob trabalhara com a expressão:*

$$f(x) = \begin{cases} x - 15, \text{ se } 10 < x \leq 25 \\ x + 11, \text{ se } 0 \leq x \leq 10 \end{cases}$$

que é a função inversa da cifragem. Ao ver que a primeira letra do texto cifrado é B e que segundo a maneira de associar, temos $B = 1$, logo Bob começara usando a segunda sentença. Portanto

$$f(1) = 1 + 11$$
$$f(1) = 12$$

Logo a letra B equivale a M no texto claro. Prosseguindo dessa maneira, tem-se o texto claro MEENCONTREAMANHA, que significa ME ENCONTRE AMANHA.

É interessante observar como os intervalos que definem a sentença mudam de posição.

Agora vamos trabalhar com o conceito de matriz e matriz inversa para entendermos o funcionamento da Cifra de Hill.

2.3 Cifra de Hill

A cifra de Hill foi inventada em 1929 pelo matemático americano Lester Hill (1891-1961) (FIGUEIREDO,). É uma cifra de substituição que torna difícil um ataque de análise de frequência. Outro aspecto interessante da cifra de Hill é que ela é uma cifra de bloco. Isto significa que a mensagem clara é quebrada em blocos de tamanhos fixados e o bloco é cifrado como um todo, ou seja, a cifragem não é letra a letra, como a cifra que acabamos de analisar.

O uso da cifra de Hill depende do conhecimento de matrizes, multiplicação de matrizes, matriz inversa e aritmética modular. Os conteúdos de matrizes são comumente ensinados em turmas de 2º ano do ensino médio.

Como no exemplo anterior a cifra de Hill depende da associação de cada letra do alfabeto há um número. Vamos trabalhar com a mesma tabela do exemplo anterior. O algoritmo atua em blocos de n letras. Cada bloco forma uma matriz coluna P com n elementos. Uma matriz invertível, que admite inversa, K será utilizada como chave e a cifragem consiste na multiplicação da matriz K pelo vetor P. Assim a mensagem cifrada C será:

$$C = K.P$$

A inversa K^{-1} da matriz K será utilizada para decifrar a mensagem. Para obter o texto claro P a partir da mensagem cifrada, multiplicamos por K^{-1}.

$$K^{-1}.C = K^{-1}(K.P) = (K^{-1}.K).P = I_n.P = P$$

portanto $P = K^{-1}.C$ O termo I_n representa a matriz identidade de ordem n.

Exemplo 10 *Vamos cifrar a palavra ATACAR usando a matriz*

$$K = \begin{bmatrix} 1 & 3 & 3 \\ 1 & 4 & 3 \\ 1 & 3 & 4 \end{bmatrix}$$

como chave.

Como a matriz é de ordem 3*, devemos quebrar a mensagem em blocos de tamanho 3, formando um total de 2 blocos, que são: ATA - CAR. Usando a tabela para associar cada letra a um número, temos as seguintes matrizes colunas:*

$$K_1 = \begin{bmatrix} 0 \\ 19 \\ 0 \end{bmatrix} \text{ e } K_2 = \begin{bmatrix} 2 \\ 0 \\ 17 \end{bmatrix}$$

Nesse momento devemos multiplicar cada matriz coluna pela matriz K*, assim estaremos cifrando a mensagem.*

Vamos efetuar as multiplicações.

$$\begin{bmatrix} 1 & 3 & 3 \\ 1 & 4 & 3 \\ 1 & 3 & 4 \end{bmatrix} . \begin{bmatrix} 0 \\ 19 \\ 0 \end{bmatrix} = \begin{bmatrix} 57 \\ 76 \\ 57 \end{bmatrix} = \begin{bmatrix} 5 \\ 24 \\ 5 \end{bmatrix} (mod 26) \ ^{1} = \begin{bmatrix} F \\ Y \\ F \end{bmatrix}$$

$$\begin{bmatrix} 1 & 3 & 3 \\ 1 & 4 & 3 \\ 1 & 3 & 4 \end{bmatrix} . \begin{bmatrix} 2 \\ 0 \\ 17 \end{bmatrix} = \begin{bmatrix} 53 \\ 53 \\ 70 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 18 \end{bmatrix} (mod 26) = \begin{bmatrix} B \\ B \\ S \end{bmatrix}$$

Observe que ao final da operação, foi realizada a operação $mod 26$*. Essa operação foi realizada para que os valores fiquem no intervalo de* 0 *à* 25 *e possam ser substituídos por letras. A cifra de Hill é uma cifra de substituição.*

Com os resultados obtidos, formamos o texto cifrado FYFBBS, que será enviada por Alice para Bob.

De posse da mensagem cifrada e da matriz usada na cifragem, Bob deverá ser capaz de calcular a matriz inversa para ler a mensagem original. Temos que a matriz inversa é dada por

$$K^{-1} = \begin{bmatrix} 7 & -3 & -3 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix}$$

De posse da matriz inversa, Bob irá dividir os códigos recebidos em matrizes colunas de 3 elementos e multiplicar.

Fazendo os cálculos temos:

[1] A operação *mod26* corresponde a uma operação de aritmética modular. Para mais detalhes da operação de congruência, consultar Domingues e Iezzi (2003).

$$\begin{bmatrix} 7 & -3 & -3 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} . \begin{bmatrix} 5 \\ 24 \\ 5 \end{bmatrix} = \begin{bmatrix} -52 \\ 19 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 19 \\ 0 \end{bmatrix} (mod 26) = \begin{bmatrix} A \\ T \\ A \end{bmatrix}$$

$$\begin{bmatrix} 7 & -3 & -3 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} . \begin{bmatrix} 1 \\ 1 \\ 18 \end{bmatrix} = \begin{bmatrix} -50 \\ 0 \\ 17 \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \\ 17 \end{bmatrix} (mod 26) = \begin{bmatrix} C \\ A \\ R \end{bmatrix}$$

Juntando as duas matrizes colunas, temos o texto claro ATACAR.

Com esse exemplo o professor tem a oportunidade de relembrar a operação de multiplicação de matriz e também o cálculo da matriz inversa. Apesar do exemplo ter sido realizado com uma matriz de ordem 3×3, também poderia ser realizado com uma matriz de ordem 2, já que são os modelos de matrizes mais trabalhados no ensino médio. Uma pergunta que pode surgir é: o que fazer quando o tamanho da mensagem não é divisível pelo comprimento do bloco? De acordo com Stallings (2004), quando isso ocorre, o emissor deve inserir no final da mensagem, sequências de letra X até deixar a mensagem com um tamanho que possa ser dividido pelo comprimento do bloco. O receptor da mensagem sabe que deve ignorar as letras X no final do texto. Digamos que queiramos cifrar a palavra FOGO usando a matriz de ordem 3 do exemplo anterior. No caso a mensagem deve ser divida em blocos de tamanho 3, mas como só temos 4 letras, então a mensagem a ser cifrada passa a ser FOGOXX para que a divisão de exata.

Outro conceito que podemos utilizar dentro dessa temática, é a definição e cálculo de determinante para testarmos a "qualidade" da matriz escolhida para cifragem. Veja que para decifrarmos a mensagem é necessário que a matriz tenha inversa, caso contrário não poderemos usar o método praticado anteriormente, e o conceito de determinante nos permite justamente investigarmos de antemão se uma matriz possui inversa ou não.

Teorema 2 *Seja K uma matriz quadrada. A inversa de K existe, se e somente se, o seu determinante não é nulo, det(K)≠0.*

Caso o professor queira, poderá fazer a demonstração do teorema para relembrar os alunos e também revisar como calcular o determinante de matrizes quadradas.

Exemplo 11 *Novamente nossos amigos Alice e Bob desejam trocar uma mensagem em segurança. Para isso desejam usar a Cifra de Hill. Alice sugere usar a matriz*

$$K = \begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix}$$

Seria essa matriz uma boa escolha?

A resposta é não. Se usarmos o resultado do teorema 2, veremos que o determinante da matriz em questão:

$$det(K) = 1.2 - 2.1 = 0$$

possui valor 0*, com isso Bob não será capaz de montar a matriz inversa para realizar a decifragem da mensagem.*

2.4 Análise Combinatória e Quantidade de Chaves

A criptografia também é responsável pelo estudos das técnicas para se decifrar uma mensagem sem o uso da chave. Entre as várias formas de ataque conhecido, está o ataque por força bruta. Nessa forma de ataque, o atacante, isto é, a pessoa responsável por decifrar a mensagem, tenta quebrar o código testando sistematicamente todas as chaves possíveis.

O que a análise combinatória permite é, calcular a quantidade de chaves para uma cifra. Se a quantidade de opções de chave for pequena, um ataque de força bruta pode decifrar a mensagem. Um bom criptossistema precisa ser imune ao ataque de força bruta.

Exemplo 12 *A Cifra de César consiste em deslocar as letras do texto claro uma quantidade específica. No caso só existem 25 possibilidades de chaves. Pois se deslocarmos 26 posições teremos o alfabeto original e se deslocarmos 27 corresponde a deslocar 1 unidade para direita. Um ataque de força bruta não levaria muito tempo para se determinar o texto claro*

Podemos usar o conceito de permutação de elementos para calcular a quantidade de chaves possíveis para uma cifra de substituição monoalfabética.

Definição 5 (Permutação) *Dado um conjunto A tal que* $\#A = n$ *,o número de modos distintos de ordenar todos os n elementos do conjunto A chama-se permutação.*

Pelo princípio multiplicativo, o total de permutação de n elementos é $n!$.

Exemplo 13 *Como em uma cifra substituição monoalfabética, cada letra é substituída sempre pela mesma letra ao longo do texto, então temos uma permutação das 26 letras. Para criarmos o alfabeto cifrado, a primeira letra pode ser associada a qualquer uma das 26. Já a segunda letra a qualquer uma das 25 restantes e assim sucessivamente. Logo, temos* $26!$*. Mas é preciso subtrair 1 unidade que é o alfabeto original, portanto o total de chaves é* $26! - 1 = 403.291.461.126.605.635.583.999.999$*.*

Isso mostra que o ataque de força bruta é impraticável para uma cifra monoalfabética, mas outras formas de ataque como o de análise de frequência decifram a mensagem.

3 Criptografia e Atualidades

3.1 Surgimento da Criptografia de Chave Pública

No capítulo 1, relatamos a evolução da ciência criptográfica, dos primórdios até o fim da 2ª guerra mundial. A proposta deste capítulo é mostrar onde a criptografia está inserida atualmente, e como é fundamental para o nosso cotidiano.

Até o período da 2ª guerra mundial, a criptografia usava de cifras simétricas. As cifras simétricas são cifras que trabalham com uma única chave. A chave usada para cifrar a mensagem é a mesma usada para decifrar a mensagem. Essa restrição, de trabalhar com uma única chave, trazia um grande desafio para o emissor e o receptor da mensagem, que era a de combinar a chave com segurança. Tínhamos então um problema de distribuição de chaves. Afinal, como duas pessoas poderiam combinar a chave com segurança? Em muitos casos, as pessoas envolvidas na troca de mensagens deveriam se encontrar para combinar as chaves ou confiar a chave, a um terceiro para que levasse do emissor ao receptor, o que era um enorme problema pois toda a segurança da mensagem está na mão dessa terceira pessoa (FIGUEIREDO, 2012a).

Para se ter uma ideia de como a distribuição de chaves tornou-se um desafio para criptografia, Singh (2011) relata que na década de 70, os bancos tentaram distribuir chaves usando viajantes que estavam entre os empregados de maior confiança da empresa. Esses servidores percorriam o mundo com valises trancadas, distribuindo pessoalmente as chaves para todos os que receberiam mensagens do banco na semana seguinte. Mas a medida que a rede de negócios aumentavam de tamanho, mais mensagens eram enviadas e mais chaves tinham que ser entregues. Os bancos logo descobriram que esses processos de distribuição tornara-se um horrível pesadelo logístico, e os custos ficaram proibitivos.

Durante a segunda guerra mundial, a distribuição de chaves era um pesadelo para os países envolvidos. O alto comando alemão precisava distribuir o livro mensal de chaves diárias para todos os operadores da máquina enigma e ainda tinham o desafio de que muitos submarinos costumavam passar longos períodos longe de suas bases e, de algum modo, precisavam obter um suprimento regular de chaves.

Além do desafio de se combinar a chave com segurança, na década de 80 foi quando a internet começou a ser usada por não-acadêmicos e não governamentais. Essa adesão a internet gerou o seguinte cenário: Imagine uma pessoa querendo encomendar um produto pela internet. Como essa pessoa poderia mandar um e-mail contendo informações cifrada sobre seu cartão de crédito, de modo que apenas o vendedor da internet pudesse decifrá-la? Como essas pessoas, que não se conhecem, poderiam combinar uma chave? O número de

contatos casuais e a quantidade de e-mails espontâneos entre o público seria enorme e isto significaria que a distribuição de chaves seria impraticável. Com isso tinha-se o temor de que o público jamais teria acesso a privacidade digital.

Motivado por esse problema da distribuição de chaves e pensando nele é que os cientistas Whitfield Diffie (Figura 8) e Martin Hellman (Figura 9), desenvolveram o conceito de criptografia de chave pública, sem dúvida um marco na história da criptografia. Na criptografia de chave pública usam-se duas chaves distintas: uma chave chamada de pública e outra chave chamada de secreta (ou privada). A chave pública é usada para cifrar a mensagem enquanto a chave secreta é usada para decifrar a mensagem, conforme o esquema abaixo (Figura 7).

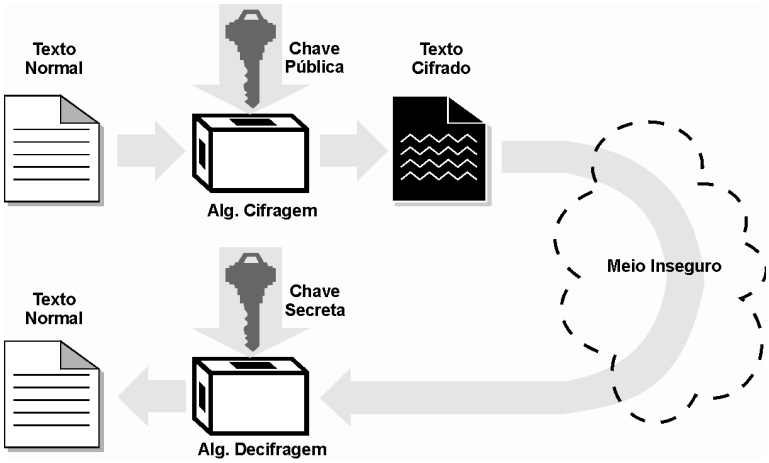


Figura 7 – Esquema da Criptografia de Chave Pública

. Disponível em:<http://www.di.ufpe.br/ flash/ais98/cripto/criptografia.htm>. Acesso em mai.2014.

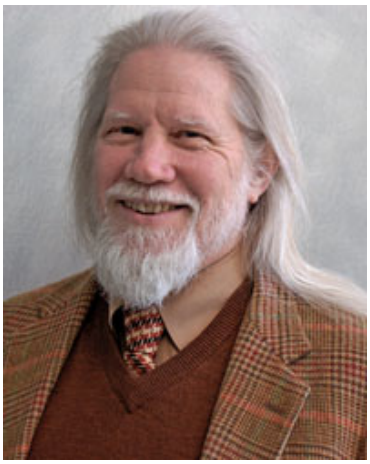


Figura 8 – Whitfield Diffie

Disponível em:<http://www.computerhistory.org/fellowawards/hall/bios/Whitfield,Diffie/>. Acesso em mai.2014

Figura 9 – Martin Hellman

Disponível em:<http://en.wikipedia.org/wiki/Martin_Hellman>. Acesso em mai.2014.

O mais interessante é que a chave pública não precisa ser mantida em segredo, por isso é pública. A única que precisa ser mantida em segredo é a chave secreta. Assim por exemplo, digamos que Bob queira enviar uma mensagem C para Alice. Então Bob consulta Alice para saber qual é a sua chave pública. Essa consulta não precisa ser feita em segredo, não tem problema se ela for interceptada. Alice então responde que a chave pública é K_a. De posse da chave pública de Alice, Bob cifra a mensagem obtendo $K_a(C)$ e envia para Alice. Alice então usando a chave privada P_a decifra a mensagem $P_a(K_a(C)) = C$. A chave pública e a secreta são operações opostas, mas é importante ressaltar que a chave pública é construída de modo que não se pode determinar a chave privada a partir dela.

Desse modo Diffie e Hilman conseguiram brilhantemente resolver o problema da distribuição de chaves. O que eles conseguiram foi idealizar a ideia mas não tinham nenhum exemplo de uma cifra de chave pública desenvolvido. A primeira cifra de chave pública apareceria um ano depois.

3.2 Números primos e RSA

Em 1977, no MIT (Massachusetts Institute of Technology), tem-se o surgimento da primeira cifra de chave pública (COUTINHO, 2000). Proposta por Ron Rivest, Adi Shamir e Len Adleman, o RSA (usa-se as inicias dos nomes dos criadores) faz uso dos números primos e da operação de fatoração. Primeiro vamos relembrar alguns conceitos importantes.

Definição 6 *Chamamos de números primos, números naturais maiores que 1, divisíveis apenas por 1 e por ele mesmo.*

Os primeiros números primos são: 2,3,5,7,11,13 .... Dois importantes resultados envolvendo números primos são: o teorema fundamental da aritmética e a infinitude dos números primos. Vamos fazer aqui a demonstração desses dois resultados.

Para demonstrarmos o Teorema Fundamental da Aritmética é necessário o seguinte resultado.

Lema 1 *Todo número inteiro $a \geq 2$ possui pelo menos um divisor primo*

Teorema 3 (Fundamental da Aritmética) *Todo número natural pode ser decomposto em fatores primos de maneira única.*

Demonstração 1 *Dado um número inteiro n, vamos mostrar por indução que $n = p_1.p_2...p_r$, com cada p_j sendo um número primo.*

De fato, para $n = 2$ o teorema é válido.

Se $n > 2$ e n for primo, o teorema também é válido pois basta tomarmos $p_1 = n$.

Considere então que $n > 2$ é composto, e que a hipótese de indução é que todo número menor que n admite decomposição em fatores primos. Por causa do lema anterior, existe um número primo p_1 tal que p_1 divide n, ou seja, existe um $q \in \mathbf{Z}$ tal que $n = p_1 q$. Se q for primo então o resultado está provado, mas se q for composto então pelo princípio de indução existem números primos tais que q é o produto desses primos. Portanto n é a junção dos fatores primos de q com p_1.

Vamos demonstrar agora a unicidade do teorema.

Suponhamos que

$$n = p_1 p_2 p_3 \dots p_r \text{ e } n = q_1 q_2 q_3 \dots q_s,$$

Com p_i, q_j primos maiores que 0 e $1 \leq i \leq r, 1 \leq j \leq s$. Como p_1 divide $q_1 q_2 q_3 \dots q_s$ então p_1 divide q_i para algum i. Sem perda de generalidade podemos supor $i = 1$. Daí p_1 divide q_1 e como ambos são primos, logo $p_1 = q_1$. Com isso temos que

$$p_1 p_2 p_3 \dots p_r = p_1 q_2 q_3 \dots q_s$$

Como $p_1 \neq 0$, simplificando, obtemos $p_2 p_3 \dots p_r = q_2 q_3 \dots q_s$.Repetindo este processo, chegaremos que $r = s$ e após um rearranjo dos índices q_j, encontramos $p_1 = q_1$,$p_2 = q_2$,$p_3 = q_3$,...,$p_r = q_r$.

Teorema 4 *Existem infinitos números primos*

Demonstração 2 *Suponha por absurdo que existem n números primos, denotados por $p_1, p_2, \ldots, p_n$, tais que $p_1 < p_2 < p_3 \ldots < p_n$. Considere o número natural $x = p_1.p_2...p_n + 1$. O número x não é divisível por nenhum dos números $p_1, p_2, \ldots, p_n$, pois sempre deixa resto 1. Esse resultado contradiz o teorema fundamental da aritmética citado acima, logo existem infinitos números primos.*

Neste momento apresentaremos em linhas gerais como funciona o RSA e explicar porque ele é difícil de ser decifrado. O funcionamento preciso do RSA requer muitas ferramentas matemáticas, mas podemos entender como se dá o seu funcionamento, pois sua base está montada em cima da dificuldade de se decompor um número em fatores primos.

O RSA faz uso dois números primos que vamos chamar de p e q. Para codificar uma mensagem usando o RSA é suficiente conhecermos o produto desses dois primos, que vamos chamar de N, isto é, $N = p.q$. Já para decifrar a mensagem, precisamos conhecer os valores de p e q. A chave de codificação do RSA é portando, constituída essencialmente pelo número N. Essa chave é tornada pública. Já a chave de decodificação é constituída pelos números primos p e q. Essa é a chave secreta que deve ser mantida em segredo, pois quem souber o valor de p e q poderá decifrar a mensagem.(COUTINHO, 2000)

Digamos que Bob queira enviar uma mensagem para Alice. Então, Bob verifica com Alice, qual é a sua chave pública e Alice informa o valor N, mas em hipótese alguma deve revelar quais números primos ela usou para formar N. De posse do valor N, Bob cifra a mensagem usando N como chave cifradora e envia a mensagem cifrada para Alice. Ao receber o texto cifrado, Alice utiliza os números primos p e q que formaram o número composto N para decifrar o texto.

Pode-se imaginar que é fácil quebrar o RSA, basta fatorar N que obteremos a chave secreta p e q. Isto está correto. Digamos que, uma pessoa mal intencionada, Eva, esteja ouvindo a conversa entre Bob e Alice. Eva irá ouvir Alice informando a Bob a chave N e sabendo que irá ser cifrada usando o RSA, esta deverá apenas decompor o valor de N para obter a chave secreta p e q e assim conseguirá ler a mensagem. Decifrar um texto cifrado pelo RSA teoricamente é fácil, basta usar a fatoração. O desafio é que não existe nenhum algoritmo prático de fatoração. Para se ter uma ideia de como o processo de decomposição é extremamente trabalhoso, Coutinho (2000) relata que pouco depois do RSA ser inventado, uma mensagem desafio foi codificada usando uma chave pública de 129 algarismos, que ficou conhecida como RSA-129. Em 1994, 17 anos depois e com o uso de 600 computadores espalhados por 25 países e um supercomputador foi possível fatorar a chave e decifrar a mensagem. Veja que o RSA-129 foi proposto na década de 80. Se para quebrar uma chave pública de 129 algarismos demorou-se todo esse tempo, imagina então decompor números com milhares de casas decimais. Essas são as chaves

públicas usadas atualmente. Veja que, conhecer a chave cifradora não te permitir descobrir a chave secreta.

A tarefa de se decompor números primos ainda é um desafio. Tanto que até o ano de 2007, o site oficial do RSA propunha desafios com prêmios em dinheiro para quem conseguisse decompor certos números. Os prêmios foram cancelados, mas os desafios ainda existem e poucos foram resolvidos.

O professor poderá consultar o artigo de Almeida e Giudice (2008) ontem contém, de maneira bem simples uma explicação mais detalhada do RSA e inclusive um exemplo de atividade para ser realizada em sala de aula.

3.3 Logaritmos Discreto e ECC

Além do RSA, existe atualmente um segundo criptossistema de chave pública ganhando destaque, o ECC (Elliptic Curve Cryptography). O ECC, conhecido como criptografia de curvas elípticas, foi desenvolvido em 1985, de maneiras independentes, por Victor Miller e Neal Koblitz.(MAGALHAES; QUEIROZ, 2011) Assim como o RSA tem sua segurança baseada na dificuldade de se fatorar um número composto, o ECC tem sua segurança baseado no problema de se calcular o logaritmo discreto em um corpo finito. O ECC é fundamentalmente mais difícil de explicar que o RSA, pois necessita de um conhecimento sobre corpos finitos e equações cúbicas.

A criptografia de curva elíptica tem ganhado bastante destaque atualmente pois, consegue oferecer uma segurança igual ao RSA, porém com chaves de tamanhos menor. Com isso, torna-se a exigência computacional menor. Segundo MAGALHES&QUEIROZ(2010), enquanto o RSA precisa de uma chave de 15360 bits para fornecer um certo nível de segurança, o ECC trabalha com uma de 512 bits. Com o avanço da troca de dados em dispositivos móveis, a tendência é que o ECC ganhe mais popularidade.

Atualmente o ECC é usado para transações envolvendo a primeira moeda digital descentralizada, o bitcoin. Bitcoin é uma criptomoeda cuja criação e transferência é baseada em protocolos de código fonte aberto de criptografia que é independente de qualquer autoridade central. Os bitcoins são comercializados e trocados diretamente por pessoas, sem interferência de nenhuma instituição financeira, e armazenados em computadores ou pendrives. Nos EUA já se usa bitcoins para compra de produtos, tais como livros, jogos e até carros. Toda essa transação precisa estar protegida e é nesse momento que se usa o ECC.

4 Atividades para o Ensino Médio

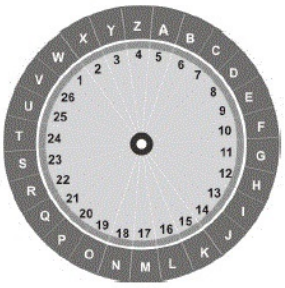
Este trabalho apresenta uma pesquisa, com o propósito de investigar o tema de criptografia, sua história e aplicação na matemática. Nesta pesquisa propõ-se o desenvolvimento de cinco atividades com enunciado e resolução. Essas atividades foram desenvolvidas a partir de pesquisa em livros acadêmicos e artigos científicos. Em cada atividade indicaremos o objetivo geral, objetivo específico, público-alvo, pré-requisitos, recursos metodológicos e a metodologia.

Conforme indicam os Parâmetros Curriculares Nacionais, "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"BRASIL (1997).

4.1 Atividade 1 - Utilizando o Disco de Alberti

Conforme citado na introdução, o Disco de Alberti foi desenvolvido por Leon Alberti e representou um avanço na criptografia. Nessa atividade iremos trabalhar com um modelo similar ao Disco de Alberti e cifrar um texto usando o disco.

Nesse modelo similar, a chave consiste em escolher um número e girar o disco até o número corresponde a letra A. Depois disso, as letras das palavras são substituídas pelos números correspondentes, separados por traços. Por exemplo, na figura abaixo, a chave é 5, e a palavra PAI é codificada como 20-5-13.



- Objetivo Geral: Mostrar o funcionamento do disco de Alberti.
- Objetivo específico: Usar o disco de Alberti para cifrar e decifrar uma palavra.
- Público-alvo: Estudantes do ensino médio, a partir do 1º ano.
- Recursos Metodológicos: Lápis, borracha, e folha contendo a atividade.
- Pré-requisito: Não há nenhum pré-requisito para realização da atividade.
- Metodologia: Essa atividade pode ser realizada individualmente ou em grupo. Caso seja realizado a atividade em grupo, sugerimos trabalhar com 3 grupos: O grupo 1 é o remetente da mensagem, isto é, deve criar uma mensagem cifrada e enviar para o grupo destinatário; O grupo 2 é o destinatário, recebe a mensagem cifrada e a decifra. O grupo 1 e 2 devem combinar a chave. O grupo 3 é o interceptador, recebe a mensagem cifrada e tenta decifrar sem conhecer a chave

Atividade: Utilizando o disco acima e a explicação sobre o seu funcionamento, responda as questões abaixo.

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

b) Codifique PROFMAT usando a chave 20

c) Quantas chaves são possíveis para o disco?

Solução:

a) Correspondendo cada número a uma letra segundo o disco, temos a palavra SUCURI.

b) Construindo um disco similar porém com o número 20 na letra A, a sequência fica 9-11-8-25-6-20-13

c) São possíveis apenas 26 chaves. O disco é uma mecanização da cifra de César

4.2 Atividade 2 - Utilizando funções na Criptografia

No capítulo 2 observamos como podemos usar as funções bijetoras para criarmos uma cifra de substituição. Nessa atividade, listaremos algumas funções a serem analisadas. Mais modelos de funções com algumas variações podem ser vistos em Santos (2013) e Marques (2013).

- Objetivo Geral: Mostrar como podemos usar as funções para criarmos cifras de substituição.
- Objetivo específico: Trabalhar a operação de valor numérico, cálculo da função inversa; reconhecer quando uma função é bijetora.
- Público-alvo: Estudantes do ensino médio, a partir do 1º ano.
- Recursos Metodológicos: Lápis, borracha, calculadora e folha contendo a atividade.
- Pré-requisito: Se faz necessário para realização dessa atividade conhecimento prévio de valor numérico de funções e o procedimento para determinação da função inversa.
- Metodologia: Essa atividade pode ser realizada individualmente ou em grupo. Caso seja realizado a atividade em grupo, sugerimos trabalhar com 3 grupos: O grupo 1 é o remetente da mensagem, isto é, deve criar uma mensagem cifrada e enviar para o grupo destinatário; O grupo 2 é o destinatário, recebe a mensagem cifrada e a decifra. O grupo 1 e 2 devem combinar a chave. O grupo 3 é o interceptador, recebe a mensagem cifrada e tenta decifrar sem conhecer a chave.

Atividade: Para cada uma das funções abaixo, verifique se dada a relação

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

é possível ser feita a cifragem. Caso seja, cifre a palavra PROFMAT e monte a função decifradora.

a) $f(x) = 2x + 5$

b) $f_2(x) = x^2 - 8x + 17$

c) $f_3(x) = 2^x$

Solução:

a) O texto claro PROFMAT, segundo a tabela construída, se refere a sequência 15-17-14-5-12-0-19. É preciso calcular o valor numérico da função para cada um desses valores.

$$\begin{aligned} f(15) &= 2.15 + 5 = 35 \\ f(17) &= 2.17 + 5 = 39 \\ f(14) &= 2.14 + 5 = 33 \\ f(5) &= 2.5 + 5 = 15 \\ f(12) &= 2.12 + 5 = 29 \\ f(0) &= 2.0 + 5 = 5 \\ f(19) &= 2.19 + 5 = 43 \end{aligned}$$

A função inversa para realizar o processo de decifrar é dada pela inversa:
$f^{-1}(x) = \dfrac{x-5}{2}$

b) Antes de começar o cálculo do valor numérico para cada pontos, é importante observarmos a posição do vértice com relação ao eixo x.

$$X_v = \frac{-b}{2a} = \frac{8}{2} = 4$$

Como $X_v = 4$, isso significa que existem, segundo a nossa maneira de associar letras a números, 4 valores a esquerda e a direita do parábola com o mesmo valor numérico, logo a função não é bijetora e não terá inversa.

c) Como f_3 é uma função exponencial, a intenção do exercício não é cobrar os cálculos numéricos, pois estes seriam exaustivos, mas sim fazer os alunos compreenderem que a inversa é a função logarítmica $f(x) = \log_2 x$.

4.3 Atividade 3 - Utilização da Cifra de César

Nessa terceira atividade, vamos relembrar o funcionamento da cifra de César para cifrarmos uma mensagem.

- Objetivo Geral: Utilizar a cifra de César para o ensino funções com várias sentenças.
- Objetivo específico: Compreender o funcionamendo da cifra de césar; trabalhar a com funções de várias sentenças.
- Público-alvo: Estudantes do ensino médio, a partir do 1º ano.
- Recursos Metodológicos: Lápis, borracha e folha contendo a atividade.
- Pré-requisito: Se faz necessário para realização dessa atividade um conhecimento prévio sobre função.
- Metodologia: Essa atividade pode ser realizada individualmente ou em grupo. Caso seja realizado a atividade em grupo, sugerimos trabalhar com 3 grupos: O grupo 1 é o remetente da mensagem, isto é, deve criar uma mensagem cifrada e enviar para o grupo destinatário; O grupo 2 é o destinatário, recebe a mensagem cifrada e a decifra. O grupo 1 e 2 devem combinar a chave. O grupo 3 é o interceptador, recebe a mensagem cifrada e tenta decifrar sem conhecer a chave.

Atividade: Usando o princípio da cifra de César, cifre a mensagem O INIMIGO ATACA AMANHA, deslocando 12 casas para a direita. Após ter cifrado a mensagem, descreva qual a função que o receptor deverá usar para obter o texto claro.

Solução: Para cifrar a mensagem deslocando 12 casas para a direta, deve-se utilizar a função:

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

A mensagem O INIMIGO ATACA AMANHA é transformado na sequência 14-8-13-8-12-8-6-14-0-19-0-2-0-0-12-0-13-7-0.

Utilizando a função acima para $x = 14$, tem-se $f(14) = 14 - 14 = 0$ que significa a letra A.

Utilizando a função acima para $x = 8$, tem-se $f(14) = 8 + 12 = 20$ que significa a letra U.

Portanto o texto cifrado fica assim: AUZUYUSAMFMOMMYMZTM.

Para que o receptor possa decifrar a mensagem, utiliza-se a função inversa da usada para cifrar:

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

4.4 Atividade 4 - Utilizando Matrizes na Criptografia

Nessa quarta atividade, faremos uso da cifra de Hill para cifrarmos e decifrarmos uma mensagem. Mais modelos de matrizes podem ser vistos em Santos (2013) e Marques (2013).

- Objetivo Geral: Mostrar como podemos usar as matrizes para criarmos cifrarmos uma mensagem.
- Objetivo específico: Trabalhar a operação de multiplicação de matrizes, cálculo da matriz inversa; cálculo do determinante.
- Público-alvo: Estudantes do ensino médio, a partir do 2º ano.
- Recursos Metodológicos: Lápis, borracha, calculadora e folha contendo a atividade.
- Pré-requisito: Faz-se necessário para realização dessa atividade, o conhecimento prévio de operações matriciais, incluindo o cálculo da inversa e cálculo do determinante.
- Metodologia: Essa atividade pode ser realizada individualmente ou em grupo. Caso seja realizado a atividade em grupo, sugerimos trabalhar com 3 grupos: O grupo 1 é o remetente da mensagem, isto é, deve criar uma mensagem cifrada e enviar para o grupo destinatário; O grupo 2 é o destinatário, recebe a mensagem cifrada e a decifra. O grupo 1 e 2 devem combinar a chave. O grupo 3 é o interceptador, recebe a mensagem cifrada e tenta decifrar sem conhecer a chave.

Atividade: Utilizando a cifra de Hill e a chave $K = \begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix}$ pede-se:

a) Cifre a palavra MATEMATICA

b) Decifre a palavra IIEM sabendo que foi cifrada com a mesma chave K.

c) Se as pessoas envolvidas na troca de mensagens tivessem usado a matriz

$$K = \begin{pmatrix} 2 & -3 \\ 6 & -9 \end{pmatrix}$$

como chave, teriam feito uma boa escolha?

Solução:

a) Por causa da matriz K ser de ordem 2, o texto claro deve ser dividido em blocos de 2 letras. Cada bloco terá como elementos, a posição da letra no alfabeto, sendo a letra $A = 0$. Portanto os vetores coluna são:

$$P_1 = \begin{pmatrix} 12 \\ 0 \end{pmatrix},\ P_2 = \begin{pmatrix} 19 \\ 4 \end{pmatrix},\ P_3 = \begin{pmatrix} 12 \\ 0 \end{pmatrix},\ P_4 = \begin{pmatrix} 19 \\ 8 \end{pmatrix} \text{ e } P_5 = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$$

Cada vetor coluna será multiplicado pela chave $K = \begin{pmatrix} 2 & -3 \\ 6 & -9 \end{pmatrix}$.

$$\begin{pmatrix} 2 & -3 \\ 6 & -9 \end{pmatrix}\begin{pmatrix} 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 60 \\ 38 \end{pmatrix} mod26 = \begin{pmatrix} 8 \\ 10 \end{pmatrix} = \begin{pmatrix} I \\ K \end{pmatrix}$$
$$\begin{pmatrix} 2 & -3 \\ 6 & -9 \end{pmatrix}\begin{pmatrix} 19 \\ 4 \end{pmatrix} = \begin{pmatrix} 119 \\ 50 \end{pmatrix} mod26 = \begin{pmatrix} 15 \\ 24 \end{pmatrix} = \begin{pmatrix} P \\ Y \end{pmatrix}$$
$$\begin{pmatrix} 2 & -3 \\ 6 & -9 \end{pmatrix}\begin{pmatrix} 19 \\ 8 \end{pmatrix} = \begin{pmatrix} 143 \\ 62 \end{pmatrix} mod26 = \begin{pmatrix} 13 \\ 10 \end{pmatrix} = \begin{pmatrix} N \\ K \end{pmatrix}$$
$$\begin{pmatrix} 2 & -3 \\ 6 & -9 \end{pmatrix}\begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 10 \\ 4 \end{pmatrix} = \begin{pmatrix} K \\ E \end{pmatrix}$$

Observe que não foi necessário efetuar o cálculo de P_3, pois $P_3 = P_1$.

Portanto, a mensagem cifrada é IKPYIKNKKE.

b) Para decifrarmos a mensagem IIEM é necessário utilizar a matriz inversa da chave $K = \begin{pmatrix} 2 & -3 \\ 6 & -9 \end{pmatrix}$. A matriz inversa é $K^{-1} = \begin{pmatrix} 1 & -2 \\ -\frac{2}{3} & \frac{5}{3} \end{pmatrix}$.

A mensagem é dividida em dois blocos II-EM que são as matrizes coluna $P_1 = \begin{pmatrix} 8 \\ 8 \end{pmatrix}$ e $P_2 = \begin{pmatrix} 4 \\ 12 \end{pmatrix}$. Fazendo a multiplicação da matriz inversa pelas matrizes coluna P_1 e P_2 tem-se:

$$\begin{pmatrix} 1 & -2 \\ -\frac{2}{3} & \frac{5}{3} \end{pmatrix}\begin{pmatrix} 8 \\ 8 \end{pmatrix} = \begin{pmatrix} -8 \\ 8 \end{pmatrix} mod26 = \begin{pmatrix} 18 \\ 8 \end{pmatrix} = \begin{pmatrix} S \\ I \end{pmatrix}$$
$$\begin{pmatrix} 1 & -2 \\ -\frac{2}{3} & \frac{5}{3} \end{pmatrix}\begin{pmatrix} 4 \\ 12 \end{pmatrix} = \begin{pmatrix} -20 \\ \frac{52}{3} \end{pmatrix} mod26 = \begin{pmatrix} 6 \\ 0 \end{pmatrix} = \begin{pmatrix} G \\ A \end{pmatrix}$$

Portanto o texto claro era SIGA.

c) A resposta é não, pois o $det(K) = 0$, logo não temos uma matriz inversa para fazer a decifragem.

4.5 Atividade 5 - Utilizando Análise Combinatória na Criptografia

No final da 1ª Guerra Mundial, começou o uso da cifra ADFGVX por parte da Alemanha, idealizada por um coronel alemão . Faremos a explicação de uma versão mais simples da cifra(SINGH, 2011).

A cifra utiliza de uma grade 6×6 e enchendo-a com 36 quadrados onde distribuímos um conjunto de 26 letras e 10 digitos. Cada fileira e coluna da grade é identificada por uma das 6 letras A,D,F,G,V e X. O arranjo dos elementos na grade são a chave da cifra. Uma possível chave, utilizando o alfabeto de 26 letras e os digitos de 0 a 9, é :

	A	D	F	G	V	X
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

A cifragem se faz, pegando cada letra do texto claro e substituindo pelas letras que estão na linha e coluna. Usando a grade acima, a mensagem AVANCEM DIA 10 ficaria assim:

$$\begin{array}{cccccccccccc} A & V & A & N & C & E & M & D & I & A & 1 & 0 \\ DV & VF & DV & AX & FG & XD & GX & AG & VG & DV & AV & XG \end{array}$$

Observe na grade que a letra A, está na fileira D com coluna V. A letra V está na interseção da linha V com a coluna F. Seguindo dessa maneira a mensagem cifrada é DVVFDVAXFGXDGXAGVGDVAVXG.

Para essa atividade temos como:

- Objetivo Geral: Mostrar como podemos usar análise combinatória na criptografia.
- Objetivo específico: Utilizar a ferramenta de permutação para o cálculo da quantidade de chave.
- Público-alvo: Estudantes do ensino médio, a partir do 2º ano.
- Recursos Metodológicos: Lápis, borracha, calculadora e folha contendo a atividade.
- Pré-requisito: Faz-se necessário para realização dessa atividade, o conhecimento prévio das ferramentas de análise combinatória.
- Metodologia: Essa atividade foi pensada para ser realizada individualmente.

Atividade: Usando os conceitos de análise combinatória e a explicação dada sobre a cifra, determine qual a quantidade de chaves da cifra ADFGVX.

Solução: Temos 36 símbolos distintos (26 lembras mais 10 números) para dispormos em 36 espaços. Para o primeiro espaço temos 36 opções de elementos, para o 2 segundo espaço 35 elementos, para o terceiro espaço 34 elementos e assim sucessivamente. Ao final teremos um total de:

$$36.35.34.33.\ldots.1 = 36!$$

Portanto são $36!$ chaves possíveis.

Conclusão

O professor tem a responsabilidade de preparar os alunos para a convivência em sociedade, e para se viver em sociedade é necessário conhecê-la. A criptografia é um importante alicerce para a sociedade atual, e essa foi a motivação para a realização deste trabalho.

Este trabalho teve como meta mostrar as várias oportunidades que se tem para introduzir, e explorar o tema de criptografia junto as disciplinas de matemática que já fazem parte da grade curricular das turmas de ensino médio. As atividades propostas ao final são exemplos de recursos didáticos que o professor pode utilizar na sala de aula para fixar, exercitar e revisar conteúdos.

Além da matemática na criptografia , o professor tem a oportunidade de juntamente com a aula promover um debate social: Um indivíduo comum deve ter acesso a software de criptografia forte? Deveria ter a possibilidade de cifrar uma mensagem de e-mail, de tal forma que as agências de segurança dos governos não pudessem interceptar a comunicação?. É um debate complexo porque, se por um lado, a privacidade pode ser vista como um direito individual e, sendo assim, a criptografia como forma de protegê-la deveria ser acessível a todos, por outro lado, também significa que terroristas e outros bandidos teriam formas bastantes seguras de proteger e comunicar informações que podem causar grande dano a outros indivíduos.

Enfim, pudemos perceber que a criptografia é um tema bem abrangente e atual. A sua história é bem rica e interessante, o que ajuda a atrair a atenção do aluno. Por isso, consideramos este trabalho como uma boa oportunidade para o professor se familiarizar com o tema e assim conseguir enriquecer a sua aula.

Referências

ALMEIDA, M. F. L. B. P.; GIUDICE, M. D. Criptografia rsa, dízimas periódicas, e o ensino de álgebra. *In: Seminário de Pesquisa em Educação Matemática do Estado do Rio de Janeiro, VI*, 2008. Acesso em: 10 Jul. de 2014. Disponível em: <http://www.sbemrj.com.br/sbemrjvi/artigos/c6.pdf>. Citado na página 29.

BRASIL. *Parâmetros Curriculares Nacionais: Matemática*. [S.l.], 1997. Acesso em: 12 Fev. de 2014. Disponível em: <http://portal.mec.gov.br/seb/arquivos/pdf/livro03.pdf>. Citado na página 30.

COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. Rio de Janeiro, RJ: SBM, 2000. 213 p. Citado 2 vezes nas páginas 26 e 28.

DOMINGUES, H. H.; IEZZI, G. *Álgebra Moderna*. São Paulo, SP: Atual Editora, 2003. 368 p. Citado na página 20.

FIGUEIREDO, L. M. Introdução a criptografia. Acesso em: 20 de Jan. de 2013. Disponível em: <www.labcas.uff.br/criptografia>. Citado na página 19.

FIGUEIREDO, L. M. Números primos e criptografia de chave publica. Acesso em: 10 de Mar. de 2013. 2012. Disponível em: <www.labcas.uff.br/criptografia>. Citado na página 24.

FIGUEIREDO, L. M. O que é criptografia. Acesso em: 23 de Jan. de 2013. 2012. Disponível em: <www.labcas.uff.br/criptografia>. Citado 3 vezes nas páginas 1, 3 e 5.

MAGALHAES, D. K. S.; QUEIROZ, R. J. G. B. Curvas elípticas aplicadas à criptografia. *In: ERCEMAPI*, p. 8, 2011. Acesso em: 24 de Jul. de 2013. Disponível em: <http://www.die.ufpi.br/ercemapi2011/artigos/ST2_07.pdf>. Citado na página 29.

MARQUES, T. V. *Criptografia: abordagem histórica, Protocolo Diffie-Hellman e Aplicações em sala de aula*. Dissertação (Mestrado) — Universidade Federal da Paraiba (UFPB), Joã Pessoa, 2013. Acessado em: 15 de Nov. de 2013. Disponível em: <www.bit.profmat-sbm.org.br/Xmlui/bitstream/handle/123456789/281/2001_00133_THIAGO_VALENTIM_MARQUES.pdf?sequence=1>. Citado 2 vezes nas páginas 33 e 37.

OLGIN, C. A.; GROENWALD, C. L. O. Criptografia e conteúdos de matemática do ensino médio. *In: Congresso Nacional de Educação Matemática, II*, Junho 2011. Acesso em: 9 de Dez. de 2013. Disponível em: <http://www.projetos.unijui.edu.br/matematica/cnem/cnem/principal/cc/PDF/CC9.pdf>. Citado na página 2.

OLIVEIRA, D.; KRIPKA, R. M. L. O uso da criptografia no ensino de matemática. *In: Conferência Interamericana de Educação Matemática, XIII*, 2011. Acesso em: 23 de Abr. de 2014. Disponível em: <http://www.lematec.net/CDS/XIIICIAEM/artigos/1817.pdf>. Citado na página 2.

SANTOS, J. L. *A Arte de Cifrar, Criptografar, Esconder e Salvaguardar como Fontes Motivadores para Atividades de Matemática Básica*. Dissertação (Mestrado) —

Universidade Federal da Bahia (UFBA), Salvador, 2013. Acessado em: 15 de Nov. de 2013. Disponível em: <www.bit.profmat-sbm.org.br/Xmlui/bitstream/handle/123456789/281/2011_0046_JOSE_LUIS_DOS_SANTOS.pdf?sequence=1>. Citado 2 vezes nas páginas 33 e 37.

SINGH, S. *O Livro dos Codigos*. São Paulo, SP: Editora Record, 2011. 446 p. Citado 10 vezes nas páginas 3, 4, 5, 6, 7, 8, 9, 10, 24 e 39.

STALLINGS, W. *Criptografia e Segurança de Redes*. São Paulo, SP: Editora Pearson, 2004. 492 p. Citado 3 vezes nas páginas 1, 3 e 21.