INSTITUTO FEDERAL
MINAS GERAIS
Campus Ouro Preto

MATRIZES E CRIPTOGRAFIA

MATEMÁTICA – Prof. VIDIGAL

Lembra quando duas colegas suas, na época do ensino fundamental, trocava mensagens codificadas onde cada letra era um símbolo e cada símbolo representava uma letra? Isso já era uma forma rudimentar de criptografia.

A necessidade de guardar mensagens secretas, consideradas importantes, de forma que somente pessoas certas possam decifrá-las, vem acompanhando a sociedade a milênios, desde a época do antigo Egito, passando pelas guerras até os tempos atuais. A criptografia – do grego *kryptós* significa secreto, oculto, e *gráphein*, escrever - é um conjunto de técnicas que permite escrever em código uma mensagem, de modo que somente aquele que envia a mensagem original e o destinatário legítimo sejam capazes de interpretá-la. Atualmente, a criptografia é utilizada em transações eletrônicas, como movimentações bancárias executados na Internet e entre outras situações da vida cotidiana, os quais necessitam de uma comunicação confidencial para o tráfego de dados.

Muitas técnicas para codificar e decodificar mensagens secretas fazem uso de álgebra linear. Neste texto, está descrito um método bastante simples que envolve apenas um par de matrizes inversas, A e B = A^{-1}, cujos elementos são todos inteiros.

Vamos, em princípio, conhecer este método por meio de um exemplo, para isto, utilizaremos as matrizes A = $\begin{bmatrix} 5 & 7 \\ 2 & 3 \end{bmatrix}$ e B = $\begin{bmatrix} 3 & -7 \\ -2 & 5 \end{bmatrix}$. Pode observar que $A \cdot B = B \cdot A = I$ (faça as contas para confirmar), ou seja, a matriz B é inversa da matriz A. Neste método de criptografia, o remetente vai usar a matriz A para criptografar a mensagem e o destinatário vai usar a matriz B para decodificar. O objetivo deste método é que a mensagem seja codificada utilizando pares de caracteres, de modo que, se for interceptada, não possa der decodificada utilizando, por exemplo, uma tabela de frequência de letras e coisas do tipo que ajudem a um decodificador não-amigável.

O próximo passo é criar uma tabela de correspondência transformando o alfabeto em números para podermos operar. Utilizaremos a seguinte tabela de conversão:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

P	Q	R	S	T	U	V	W	X	Y	Z	.	,	_	¬
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Note que a tabela tem todas as letras além de dois sinais de pontuação (. e ,). Além destes ainda estão o símbolo "_" que será utilizado entre duas palavras (espaço) e o símbolo ¬ indica parágrafo. Qualquer outra numeração dos 30 símbolos também seria possível, mas o remetente e o destinatário teriam que combinar uma específica.

Vamos agora codificar a mensagem "OS NÚMEROS GOVERNAM O MUNDO.". De acordo com a tabela acima, transformaremos as letras e pontuação em números

O	S	_	N	U	M	E	R	O	S	_	G	O	V	E	R	N	A	M	_	O	_	M	U	N	D	O	.
15	19	29	14	21	13	5	18	15	19	29	7	15	22	5	18	14	1	13	29	15	29	13	21	14	4	15	27

Como a matriz codificadora tem Duas linhas e duas colunas, devemos arranjar a sequência de números em uma matriz com duas linhas. Assim, a matriz mensagem será:

$$M = \begin{bmatrix} 15 & 19 & 29 & 14 & 21 & 13 & 5 & 18 & 15 & 19 & 29 & 7 & 15 & 22 \\ 5 & 18 & 14 & 1 & 13 & 29 & 15 & 29 & 13 & 21 & 14 & 4 & 15 & 27 \end{bmatrix}$$

Se a mensagem tivesse uma quantidade ímpar de símbolos, você poderia acrescentar um espaço (_ - 29) ou um número qualquer maior que 30, no final.

Agora, para codificar a mensagem, multiplicamos a matriz M à esquerda pela matriz codificada A:

$$N = A \cdot M$$

$$N = \begin{bmatrix} 5 & 7 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 15 & 19 & 29 & 14 & 21 & 13 & 5 & 18 & 15 & 19 & 29 & 7 & 15 & 22 \\ 5 & 18 & 14 & 1 & 13 & 29 & 15 & 29 & 13 & 21 & 14 & 4 & 15 & 27 \end{bmatrix}$$

$$N = \begin{bmatrix} 110 & 221 & 243 & 77 & 196 & 268 & 130 & 293 & 166 & 242 & 243 & 63 & 180 & 299 \\ 45 & 92 & 100 & 31 & 81 & 113 & 55 & 123 & 69 & 101 & 100 & 26 & 75 & 125 \end{bmatrix}$$

E, em seguida, alinhamos os elementos de $N = A \cdot M$ para formarmos a mensagem codificada. Utilizamos vírgula entre os números para facilitar a leitura na hora da decodificação. A mensagem codificada é: 110, 221, 243, 77, 196, 268, 130, 293, 166, 242, 243, 63, 180, 299, 45, 92, 100, 31, 81, 113, 55, 123, 69, 101, 100, 26, 75, 125.

Uma importante característica deste tipo de criptografia é que enquanto havia repetições representando letras repetidas na mensagem original, essas repetições não se preservam na mensagem codificada. Os decifradores de códigos mais simples começam sempre pelas repetições. Aqui, estes decodificadores não têm por onde começar.

Quando esta mensagem codificada chega, o destinatário realiza os passos contrários e a sua primeira ação é transformar a sequência numérica em uma matriz N de duas linhas:

$$N = \begin{bmatrix} 110 & 221 & 243 & 77 & 196 & 268 & 130 & 293 & 166 & 242 & 243 & 63 & 180 & 299 \\ 45 & 92 & 100 & 31 & 81 & 113 & 55 & 123 & 69 & 101 & 100 & 26 & 75 & 125 \end{bmatrix}$$

Em seguida, ele utiliza a matriz decodificadora B para reverter os passos acima. Para tal, ele aplica a seguinte propriedade da multiplicação de matrizes:

$$B \cdot N = B \cdot A \cdot M = I \cdot M = M$$

Portanto, se o decodificador usar a mensagem codificada para construir uma matriz com duas linhas e depois multiplicar esta matriz à esquerda por B, ele obterá a matriz M do remetente.

$$B \cdot N = M$$

$$\begin{bmatrix} 3 & -7 \\ -2 & 5 \end{bmatrix} \cdot \begin{bmatrix} 110 & 221 & 243 & 77 & 196 & 268 & 130 & 293 & 166 & 242 & 243 & 63 & 180 & 299 \\ 45 & 92 & 100 & 31 & 81 & 113 & 55 & 123 & 69 & 101 & 100 & 26 & 75 & 125 \end{bmatrix} = M$$

$$\begin{bmatrix} 15 & 19 & 29 & 14 & 21 & 13 & 5 & 18 & 15 & 19 & 29 & 7 & 15 & 22 \\ 5 & 18 & 14 & 1 & 13 & 29 & 15 & 29 & 13 & 21 & 14 & 4 & 15 & 27 \end{bmatrix} = M$$

Agora, transforma-se a matriz em uma sequência numérica e transforma cada número para a letra correspondente:

15	19	29	14	21	13	5	18	15	19	29	7	15	22	5	18	14	1	13	29	15	29	13	21	14	4	15	27
O	S	_	N	U	M	E	R	O	S	_	G	O	V	E	R	N	A	M	_	O	_	M	U	N	D	O	.

E daí sai a mensagem que queria passar: Os números governam o mundo.

Agora, vamos praticar um pouquinho em duas tarefas:

Tarefa 01) A sequência abaixo é uma mensagem codificada como a regra mostrada acima. Cada letra foi substituída por um número de acordo com a seguinte tabela de conversão:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

P	Q	R	S	T	U	V	W	X	Y	Z	.	,	_	¬
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

A Matriz A, utilizada para criptografar a mensagem foi $A = \begin{bmatrix} 2 & 3 \\ 5 & 8 \end{bmatrix}$ e a sequência passada ao destinatário foi: 33, 83, 145, 59, 27, 87, 115, 75, 95, 145, 47, 17, 94, 50, 63, 82, 25, 93, 83, 93, 83, 215, 377, 157, 68, 225, 302, 195, 247, 377, 124, 45, 241, 129, 165, 214, 65, 242, 221, 247. Decodifique a mensagem.

Tarefa 02) Crie uma mensagem, codifique-a utilizando a matriz $A = \begin{bmatrix} 3 & 5 \\ 4 & 7 \end{bmatrix}$ e passe pra um colega. Pegue a mensagem de outro colega que fez a mesma coisa e decodifique-a. A seguir verifique se conseguiram chegar às mensagens originais.

"Quer ver mais?" Neste vídeo, você pode obter mais informações básicas sobre criptografia.

Existe um livro, intitulado Fortaleza Digital, de Dan Brow (o mesmo autor de O Código Da Vinci) que trata de criptografia e quebra de mensagens por criptoanálise. Veja mais informações sobre o livro na "Sugestão de leitura" a seguir

Podemos criar um aplicativo para criptografar/descriptografar mensagens de acordo com o algoritmo proposto aqui. Aceita o desafio?