

CRIPTOGRAFIA ELEMENTAR COM MATRIZES

A ideia é mostrar como criar um sistema de criptografia simples utilizando multiplicação de matrizes.

Num primeiro momento, vamos estabelecer uma correspondência numérica com as letras do nosso alfabeto, que será a seguinte:

LETRA	Nº	LETRA	Nº	LETRA	Nº
A	1	K	11	U	21
B	2	L	12	V	22
C	3	M	13	W	23
D	4	N	14	X	24
E	5	O	15	Y	25
F	6	P	16	Z	26
G	7	Q	17		
H	8	R	18		
I	9	S	19		
J	10	T	20	Espaço	0

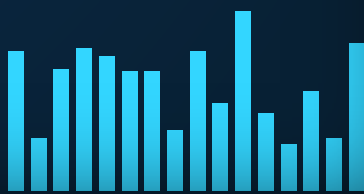
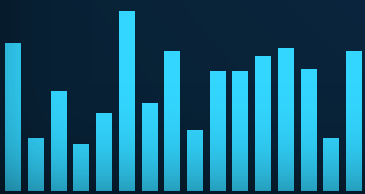
Assim, a palavra GATO pode ser escrita como:

G	A	T	O
7	1	20	15

O código, então, é 7 1 20 15.

Vamos organizar esse código numa matriz transformando a única linha que o código tem em colunas. Ficando assim:

$GATO = \begin{bmatrix} 7 & 20 \\ 1 & 15 \end{bmatrix}$



Um outro exemplo, agora com a palavra POETISA:

P	O	E	T	I	S	A
16	15	5	20	9	19	1

Organizando a matriz:

$$POETISA = \begin{bmatrix} 16 & 5 & 9 & 1 \\ 15 & 20 & 19 & 0 \end{bmatrix}$$

Observe que, como a referida palavra tem um número ímpar de letras e a matriz é organizada aos pares, então completei com zero no final.

Agora precisamos de uma matriz para transformar e embaralhar nossos números, gerando um código final não tão óbvio: é aí que entra a multiplicação de matrizes. Podemos utilizar milhões de matrizes para isso, mas vou escolher esta aqui:



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

Assim, começando pela palavra GATO cujo código é 7, 1, 20 e 15, vamos realizar a multiplicação:

$$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 7 & 20 \\ 1 & 15 \end{bmatrix}$$

Cujo resultado é a matriz:

$$\begin{bmatrix} 8 & 35 \\ 9 & 50 \end{bmatrix}$$

Assim, o código final para GATO é 8 9 35 50.



E quanto à decodificação? Isto é, quem receber o código, como fará para identificar a palavra? É aqui que entra o conceito de matriz inversa: ao multiplicar o código recebido pela inversa da matriz chave, o embaralhamento e as transformações são desfeitas.

Para o nosso caso específico, a matriz chave foi:

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

Escolhi essa matriz, pois sua inversa é bastante simples:

$$CHAVE^{-1} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix}$$

Note que, de fato, essa é a matriz inversa da nossa chave:

$$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Assim, o código da palavra GATO recebido foi 8, 9, 35 e 50, cuja matriz é:

$$\begin{bmatrix} 8 & 35 \\ 9 & 50 \end{bmatrix}$$

Multiplicando essa matriz pela nossa matriz decodificadora:

$$\begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 8 & 35 \\ 9 & 50 \end{bmatrix} = \begin{bmatrix} 7 & 20 \\ 1 & 15 \end{bmatrix}$$

Que é nossa palavra GATO:

G	A	T	O
7	1	20	15

Para fixar melhor, vamos realizar o mesmo procedimento com a palavra POETISA:

P	O	E	T	I	S	A
16	15	5	20	9	19	1

$$POETISA = \begin{bmatrix} 16 & 5 & 9 & 1 \\ 15 & 20 & 19 & 0 \end{bmatrix}$$

Embaralhando e transformando os números com nossa matriz chave:

$$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 16 & 5 & 9 & 1 \\ 15 & 20 & 19 & 0 \end{bmatrix} = \begin{bmatrix} 31 & 25 & 28 & 1 \\ 46 & 45 & 47 & 1 \end{bmatrix}$$

Assim, o código a ser enviado é 31 46 25 45 28 47 1 1.

Decodificando com a matriz inversa de nossa matriz chave:

$$\begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 31 & 25 & 28 & 1 \\ 46 & 45 & 47 & 1 \end{bmatrix} = \begin{bmatrix} 16 & 15 & 9 & 1 \\ 15 & 20 & 19 & 0 \end{bmatrix}$$

Que é nossa palavra POETISA.

0	1	0	0	0	1	1	0	0	1	0	1	1	0	0	1
0	1	0	0	0	1	0	0	0	1	1	1	0	1	0	1
0	1	1	0	1	1	1	0	1	0	1	0	0	0	1	1
1	1	0	0	1	0	0	0	0	1	0	1	0	0	1	1
1	1	1	0	1	1	1	1	1	1	1	0	0	0	0	0
0	0	1	1	1	1	1	0	0	0	0	0	0	0	1	1
0	0	0	1	1	0	1	0	1	0	1	0	0	1	0	1
0	1	0	1	1	1	0	1	1	1	1	0	1	0	1	0
1	1	1	0	0	1	1	0	0	1	0	1	1	1	1	0
1	0	0	1	0	0	0	1	1	0	1	0	1	1	1	1
1	1	1	0	1	0	0	1	0	1	1	1	0	1	0	1
1	1	1	0	1	1	1	0	1	0	1	0	1	1	1	1
0	1	0	0	1	1	0	0	1	0	1	1	0	0	1	1
0	0	1	0	1	1	1	0	0	0	1	0	0	1	1	1
1	0	0	1	1	0	0	1	0	0	0	0	0	1	0	0
1	1	0	0	1	1	1	0	1	0	1	0	1	1	0	0