

# TEXTO COMPLEMENTAR

**Disciplina:** Álgebra Linear

**Professor:** Hugo Gava Insua

Criptografia por Matrizes:

O método de criptografia por matrizes funciona da seguinte forma: a mensagem a ser criptografada é convertida em uma matriz na qual cada letra é transformada em um número conforme sua posição no alfabeto. As posições em que não houverem números são preenchidas por 0.

Em álgebra linear, uma matriz pode ser utilizada para criptografar uma mensagem de maneira simples. Seja A a matriz contendo a mensagem a ser criptografada e B a matriz com a chave de criptografia, basta transformarmos as duas matrizes, em matrizes numéricas e depois multiplicar seus elementos, gerando assim uma nova matriz contendo a mensagem criptografada. Utilizaremos como exemplo a frase : "Vamos pela manhã" e como chave de criptografia a palavra "Estrategistas".

$$\begin{bmatrix} v & a & m & o \\ s & p & e & l \\ a & m & a & n \\ h & a & - & - \end{bmatrix} \begin{bmatrix} e & s & t & r \\ a & t & e & - \\ g & i & s & t \\ a & s & - & - \end{bmatrix} \rightarrow \begin{bmatrix} 22 & 1 & 13 & 15 \\ 19 & 16 & 5 & 12 \\ 1 & 13 & 1 & 14 \\ 8 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 5 & 19 & 20 & 18 \\ 1 & 20 & 5 & 0 \\ 7 & 9 & 19 & 20 \\ 1 & 19 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 217 & 840 & 692 & 656 \\ 158 & 954 & 555 & 442 \\ 39 & 554 & 104 & 38 \\ 41 & 172 & 165 & 144 \end{bmatrix}$$

Para decodificar a mensagem, basta multiplicar a matriz codificada pela inversa da matriz que representa a chave de encriptação, assim:

MECATRONE

Vol. 2, nº 1 (2017)

Texto Livre 4, pág. 6

$$\begin{bmatrix} 217 & 840 & 692 & 656 \\ 158 & 954 & 555 & 442 \\ 39 & 554 & 104 & 38 \\ 41 & 172 & 165 & 144 \end{bmatrix} \times \begin{bmatrix} -950 & 551 & 855 & -35 \\ 1751 & 1751 & 1751 & 1751 \\ 50 & -29 & -45 & 94 \\ 1751 & 1751 & 1751 & 1751 \\ -10 & 356 & 9 & -369 \\ 1751 & 1751 & 1751 & 1751 \\ 639 & -518 & -200 & 641 \\ 1751 & 1751 & 1751 & 1751 \end{bmatrix} = \begin{bmatrix} 22 & 1 & 13 & 15 \\ 19 & 16 & 5 & 12 \\ 1 & 13 & 1 & 14 \\ 8 & 1 & 0 & 0 \end{bmatrix}$$

A partir disto, é necessário somente converter os números para letras de acordo com suas respectivas posições no alfabeto.

Fonte: PEREIRA, J. R. de S.; COSTA, R. B. Álgebra Linear Numérica: aplicações em métodos computacionais e a sua importância para a Engenharia. *Revista MECATRONE*, 2(1). 2017. Disponível em: <https://doi.org/10.11606/issn.2526-8260.mecatrone.2017.142042>