# Usando matrizes em criptografia

# Vídeos

1) O Átila

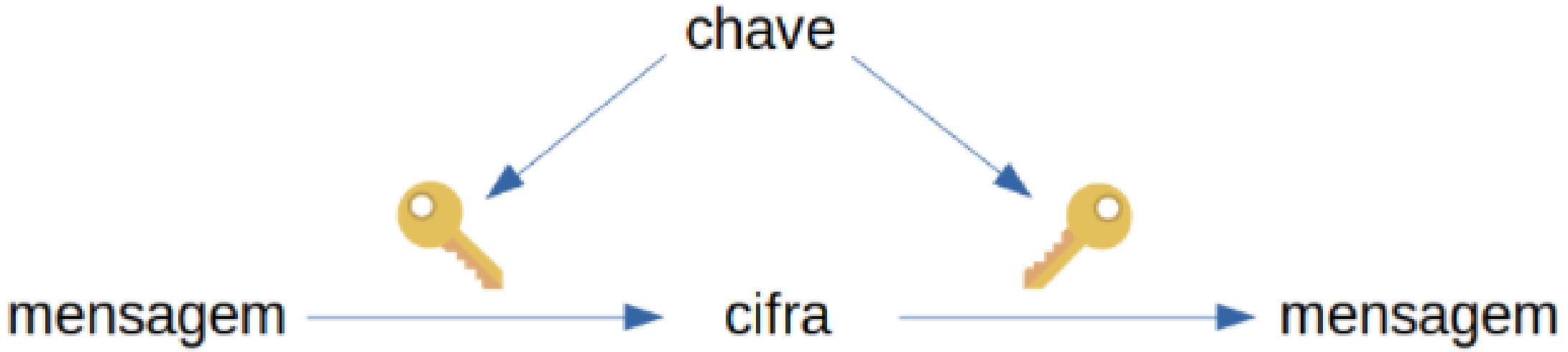
https://www.youtube.com/watch?v=_Eeg1LxVWa8

2) Chaves públicas e privadas

https://www.youtube.com/watch?v=8JEC-QKEGrw

3) Criptografia usando matriz inversa

https://www.youtube.com/watch?v=rEKjkrIdYH0


chave
mensagem
cifra
mensagem

# CIFRA DE HILL e Matriz Inversa

Dada uma matriz quadrada A de ordem n , chamamos de inversa de A uma matriz B tal que

$$\mathbf{A \cdot B = B \cdot A = I_n}$$

onde $I_n$ é a matriz identidade de ordem n.

Podemos também representar a matriz inversa de A como $A^{-1}$

(sendo -1 apenas uma notação, não sendo um expoente a ser aplicado!)

# Exemplos:

## Matriz Inversa 2x2

- inversa de $\mathbf{A} = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix}$ é $\mathbf{A^{-1}} = \begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix}$

$$\mathbf{A} \cdot \mathbf{A^{-1}} = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} \cdot \begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \mathbf{I_2}$$

$$\mathbf{A^{-1}} \cdot \mathbf{A} = \begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \mathbf{I_2}$$

## Matriz Inversa 3x3

- inversa de $\mathbf{B} = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix}$ é $\mathbf{B^{-1}} = \begin{bmatrix} 1 & -2 & 5 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{bmatrix}$

$$\mathbf{B} \cdot \mathbf{B^{-1}} = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -2 & 5 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \mathbf{I_3}$$

$$\mathbf{B^{-1}} \cdot \mathbf{B} = \begin{bmatrix} 1 & -2 & 5 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \mathbf{I_3}$$

# Como calcular a matriz inversa?

$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 3 & 1 \\ 1 & 2 & 0 \end{bmatrix} \cdot \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} a & b & c \\ a+3d+g & b+3e+h & c+3f+i \\ a+2d & b+2e & c+2f \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 3 & 1 \\ 1 & 2 & 0 \end{bmatrix}$$

$$\mathbf{A}^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ -1/2 & 0 & 1/2 \\ 1/2 & 1 & -3/2 \end{bmatrix}$$

# Outra técnica utilizando determinante:

Sendo $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, matriz quadrada de ordem 2, temos que a matriz inversa $A^{-1}$ será dada por

$$A^{-1} = \frac{1}{\det A} \cdot \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Sendo $\det A = \mathrm{ad} - \mathrm{bc}$ e $\det A \neq 0$.

# Extras:

Cifras de Hill

https://www.youtube.com/watch?v=manRQNeRTCs

Diferença entre hacker e cracker

https://www.educamaisbrasil.com.br/educacao/dicas/diferenca-entre-hacker-e-cracker

Criptografia e números primos

https://www.youtube.com/watch?v=Uf7nd8sz5yQ&t=44s

https://www.youtube.com/watch?v=glGrlf5mWcY