




# Segurança da Informação



A photograph of a server room with blue ambient lighting. Rows of server racks are visible, with some racks having glass doors that show internal components. The room has a high ceiling with exposed metal beams and cables.

# **Introdução a Segurança da Informação (cont.)**


→

Letra	Número	Letra	Número
A	00	N	13
B	01	O	14
C	02	P	15
D	03	Q	16
E	04	R	17
F	05	S	18
G	06	T	19
H	07	U	20
I	08	V	21
J	09	W	22
K	10	X	23
L	11	Y	24
M	12	Z	25



The background image shows a server room with rows of server racks. The lighting is a deep blue, creating a high-tech atmosphere. A semi-transparent white rectangular box is centered over the image, containing the title text. The server racks have glass doors, some of which are slightly ajar, revealing internal components. Cables are visible running along the top of the racks.

# Criptografia de Cesar

- 
- Criptografia de César
  - Consiste na **transposição** de letras que eram substituídas por letras seguintes do alfabeto exatamente em três casas posteriores.

Ou seja, considerando  $k=3$ , a letra A se torna a letra D

$$0 \leq k < 26$$



→ Usando a Criptografia de César ( $k = 22$ ) codificar a palavra DEUS.

- 1) Inicialmente, vamos Pré-codificar a mensagem de acordo com a tabela:
- 2) Adicione o valor da chave a cada número da pré-codificação:
- 3) Resultado (em texto):

Letra	Número	Letra	Número
A	00	N	13
B	01	O	14
C	02	P	15
D	03	Q	16
E	04	R	17
F	05	S	18
G	06	T	19
H	07	U	20
I	08	V	21
J	09	W	22
K	10	X	23
L	11	Y	24
M	12	Z	25



→ Usando a Criptografia de César ( $k = 22$ ) codificar a palavra DEUS.

$$03 + 22 = 25 \equiv 25 \pmod{26},$$

$$04 + 22 = 26 \equiv 00 \pmod{26},$$

$$20 + 22 = 42 \equiv 16 \pmod{26},$$

$$18 + 22 = 40 \equiv 14 \pmod{26}.$$





→ Usando a Criptografia de César ( $k = 22$ ) codificar a palavra DEUS.

Temos 26 correspondências de letras e números pertencentes ao intervalo de 0 a 25.

Portanto:

25 – 00 – 16 – 14.






→

$k \in \mathbb{Z}$ ,

tal que  $0 \leq k < 26$  da seguinte forma:

$$C(t) \equiv t + k \pmod{26}$$

- $C(t)$  → número codificado.
- $t$  → número pré-codificado.
- $k$  → chave da criptografia.




Qual é a mensagem secreta produzida pela mensagem?

– MEET YOU IN THE PARK

Primeiro passo

– Trocar letras por números

–



Qual é a mensagem secreta produzida pela mensagem?

– MEET YOU IN THE PARK

Primeiro passo

– Trocar letras por números


–

Segundo passo

– Trocar cada número  $p$  por  $f(p) = (p+3) \bmod 26$

–





Qual é a mensagem secreta produzida pela mensagem?

– MEET YOU IN THE PARK

Primeiro passo

– Trocar letras por números

–

Segundo passo

– Trocar cada número  $p$  por  $f(p) = (p+3) \bmod 26$

–

Terceiro passo

– Trocar cada número  $p$  por uma letra

–



Como fazer o processo inverso?

A photograph of a server room with blue ambient lighting. Several server racks are visible, some with glass doors open, revealing internal components. A semi-transparent white rectangular box is overlaid in the center of the image, containing text.

**Dúvidas?**  
**[henrique.mohr@sertao.ifrs.edu.br](mailto:henrique.mohr@sertao.ifrs.edu.br)**