# Segurança da informação

Criptografia por chave

&

Certificado digital

# Criptografia por chave

# Chave assimétrica

- Assimétrica
- Simétrica

- Chave privada
  Assinatura - criptografia
- Chave pública
  verificação de autenticidade

- Assimétrica
- Simétrica

Chave única privada

- Conhecimento prévio da chave
- Como transferir a chave?

# Chave simétrica

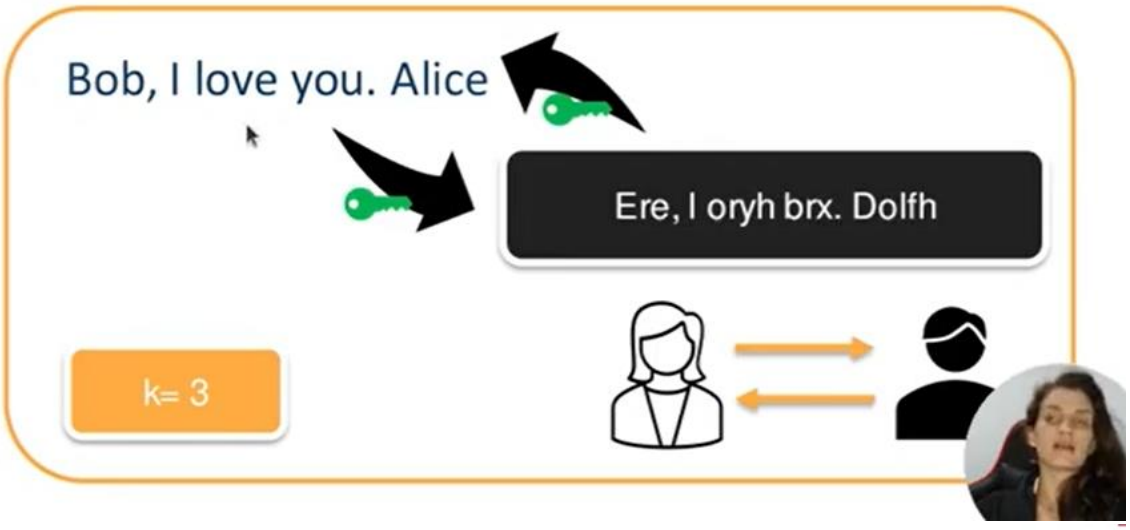
Cifra de César

Criptografia por Chave

Funcionamento

Substituição da letra pela k-ésima do alfabeto
Rotatividade do alfabeto

k= [1,26]

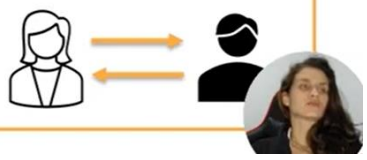



# Chave simétrica

101010100
010100101

## Cifra de fluxo


- Sequência de bits pseudo-aleatório
- Mapeamento 1 para 1

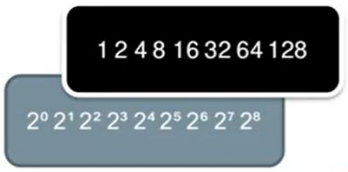


## Cifra de bloco

Blocos de bits

- k= número de bits
- Ex:

k = 64





## Cifra de bloco

k= 3

010110001111

101000111001

| Entrada | Saída | Entrada | Saída |
|---|---|---|---|
| 000 | 110 | 100 | 011 |
| 001 | 111 | 101 | 010 |
| 010 | 101 | 110 | 000 |
| 011 | 100 | 111 | 001 |

Fonte: kurose - 5° ed

## Cifra de bloco

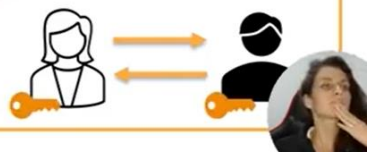
Possibilidades?

- Mapeamento por permutação
- 8!

40.320

1 2 4 8 16 32 64 128

$2^0$ $2^1$ $2^2$ $2^3$ $2^4$ $2^5$ $2^6$ $2^7$ $2^8$



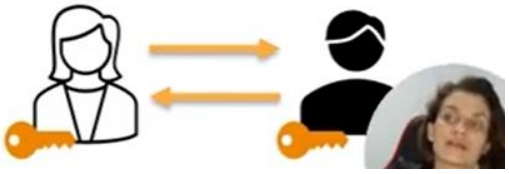
## Cifra de bloco

K>64

$1{,}844674407 \times 10^{19}$!

Mapeamento por funções

Permutação



# Chave simétrica

DES
AES
3DES

Cifra de bloco

E na prática?

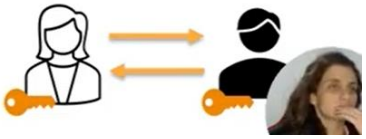
K>64

$1,844674407 \times 10^{19}$!

Mapeamento por funções

Encadeamento de cifras

Permutação



# Certificado digital

IPSec
SSL
TSL

Certificação de chave pública

- O que é certificar uma chave?

Sou bob

Sou bob

???

- O que é certificar uma chave?
  Comprovar autenticidade

- Entidade certificadora
  *Certification Authority - CA*

# Certificado digital

Alta confiabilidade

Entidade Certificadora


- Verificação de identidade
- Emissão de certificados

Vínculo entre chave e entidade


Padrões de autoridades certificadoras

- IETF - recomendação ITUX.509

Especificação de um serviço de autenticação e sintaxe de certificados

- RFC 1422

Gerenciamento de chaves baseado em CA em emails seguros