

(CMPSEGS)

# Segurança de Sistemas

Tecnologia em Análise e Desenvolvimento de Sistemas

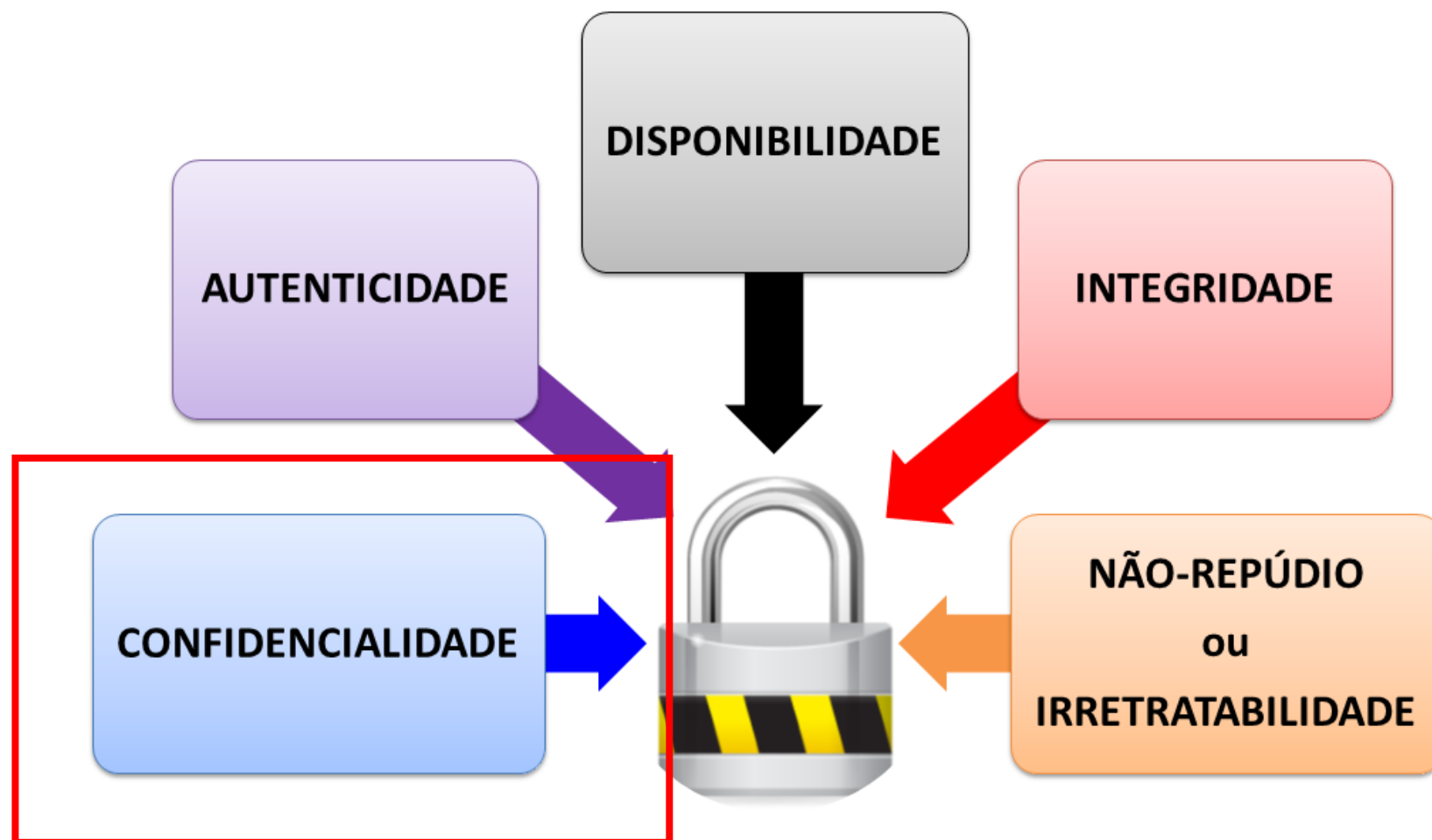
**Confidencialidade: princípios e práticas**  
**Cifragem simétrica**

**Prof. Me. Leonardo Arruda**

[leonardo.arruda@ifsp.edu.br](mailto:leonardo.arruda@ifsp.edu.br)



# Princípios da segurança de informação

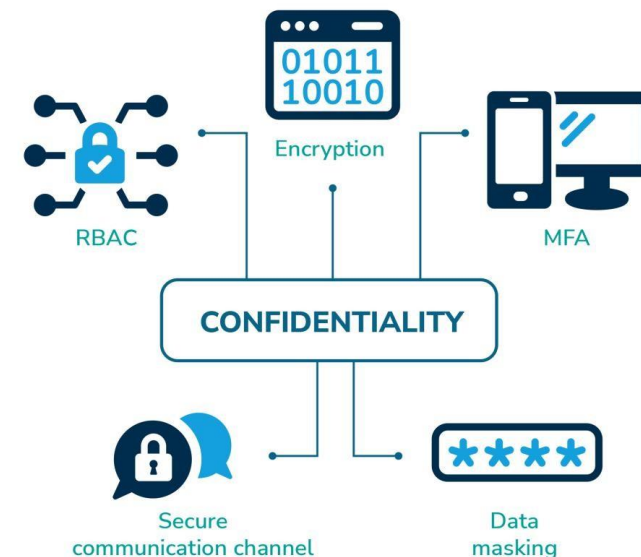


# Confidencialidade: conceito

A **confidencialidade** é o princípio de segurança que visa manter a informação secreta e protegida, assegurando que seu acesso e uso sejam restritos apenas às pessoas ou sistemas a quem ela é destinada.

Isso se aplica a todos os momentos do ciclo de vida dos dados: durante o armazenamento, a transmissão ou a utilização.

**Privacidade:** assegura que os indivíduos controlem ou influenciem quais informações relacionadas a eles podem ser obtidas e armazenadas, da mesma forma que como, por quem e para quem essas informações são passíveis de ser reveladas.



# Confidencialidade: conceito

A proteção é implementada de acordo com o grau de sigilo do conteúdo e é sustentada por três pilares:

- **Métodos Técnicos:** Como a criptografia (que transforma dados em código) e sistemas robustos de autenticação (para verificar a identidade do usuário).
- **Métodos Administrativos:** Incluem a criação de políticas internas, o estabelecimento de regras de acesso e a segregação de funções para prevenir conflitos de interesses.
- **Métodos Físicos:** Envolvem o controle de acesso a documentos físicos e a ambientes restritos.

O objetivo final é prevenir vazamentos e uso indevido de informações.

# Como garantir a Confidencialidade?

## Controle de Acesso e Autorização:

- **Define e impõe *quem* pode acessar o *quê*.** Baseia-se no princípio do privilégio mínimo e da “necessidade de conhecer”, garantindo que usuários e sistemas tenham acesso apenas aos recursos estritamente necessários para desempenhar suas funções.

## Autenticação Robusta:

- É o portão de entrada. Verifica a identidade de um usuário ou sistema antes de conceder qualquer acesso. Vai além do login e senha, incorporando fatores múltiplos como: ***Algo que você sabe*** (senha, PIN); ***Algo que você tem*** (token físico, aplicativo autenticador, etc.); e ***Algo que você é*** (biometria).

# Como garantir a Confidencialidade?

## Ofuscação de Tráfego (*Traffic Padding*):

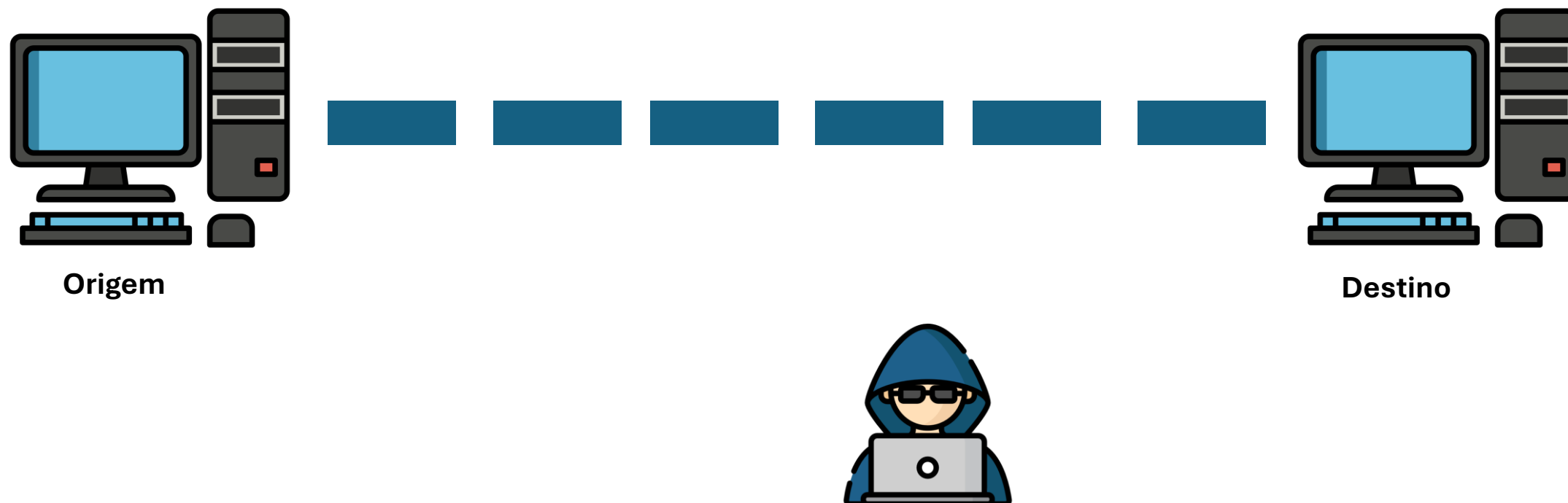
- Técnica de segurança de redes que insere **dados fictícios** e aleatórios no **fluxo de comunicação**. Isso mascara o volume real, o tempo e os padrões de tráfego, dificultando que um interceptador identifique quando e quais dados sensíveis estão sendo transmitidos.

## Criptografia:

- A espinhal dorsal da confidencialidade. Transforma dados legíveis em texto cifrado ilegível, protegendo informações **em repouso** (armazenadas em discos, bancos de dados), **em trânsito** (trafegando pela rede) e, em caso avançados, **em uso** (sendo processados na memória RAM). Somente portadores da chave correta podem reverter o processo e acessar a informação original.

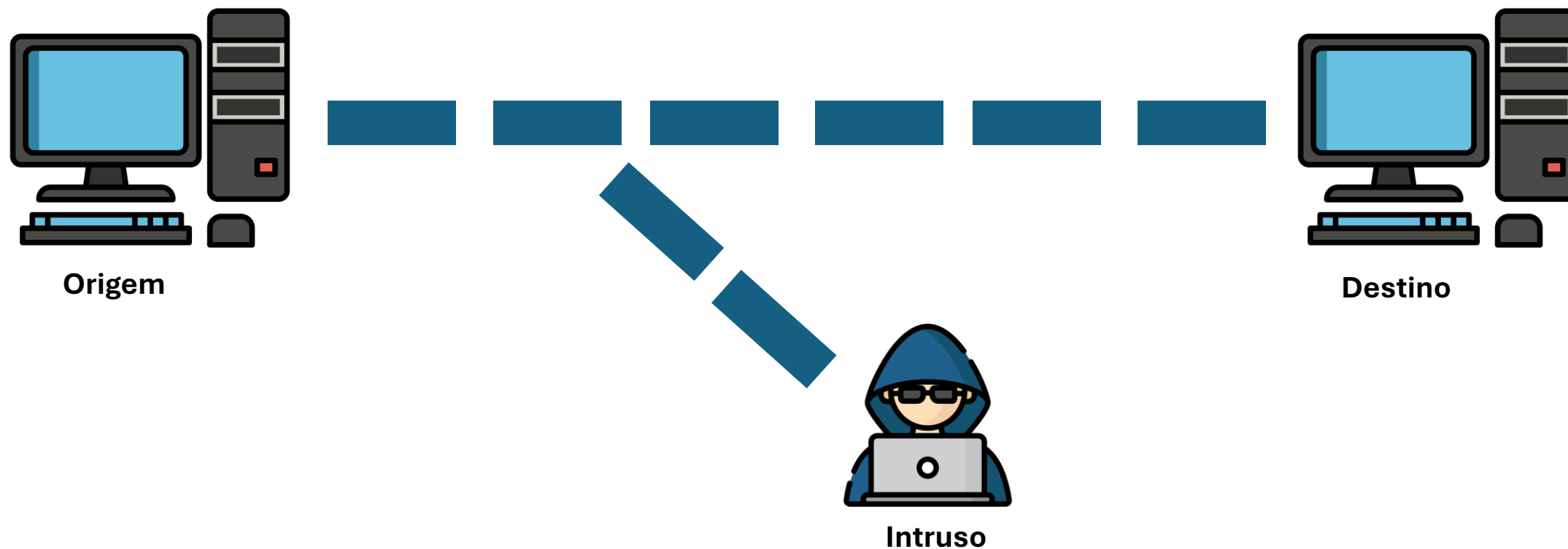
# Confidencialidade

- Prevenção do vazamento de informações



# Confidencialidade

- Prevenção do vazamento de informações

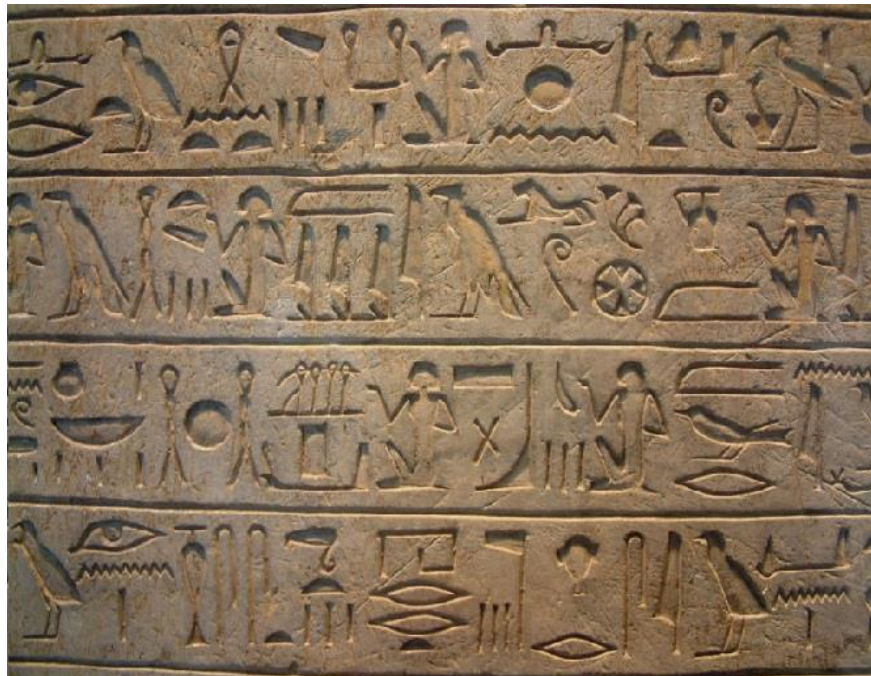




# Duas abordagens possíveis: esteganografia

## 1) Disfarçar os dados: esteganografia

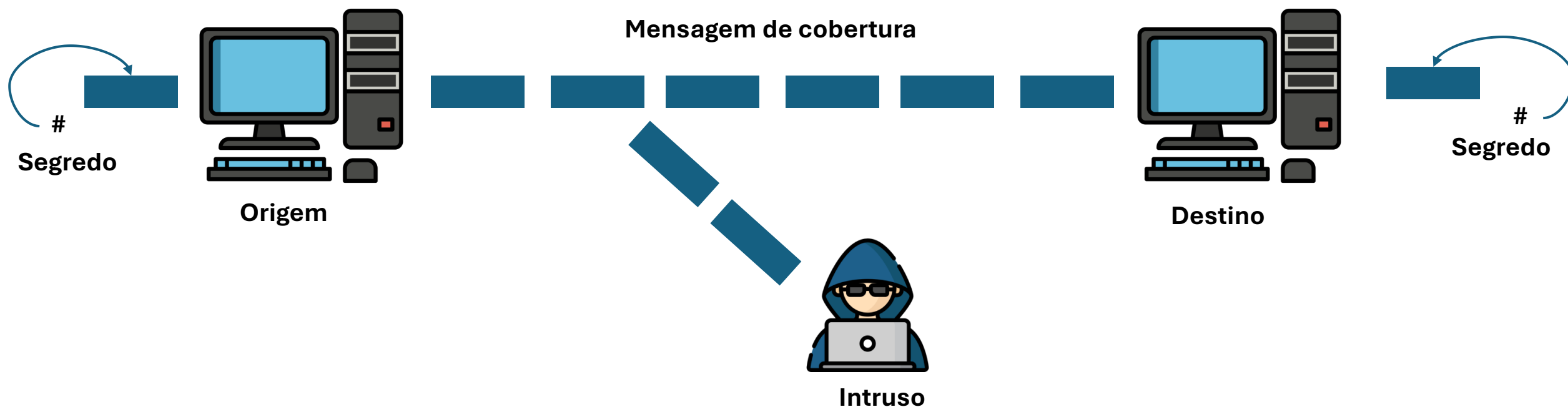
*Gregos e egípcios usavam esta técnica para esconder mensagens importantes*



a	ä	ā	y	u
b	p	f	m	n
n	r	r,l	h	h
kh	s	ś	sh	k
q	g	t	d	ta
t	dj	i	ch	m
				u

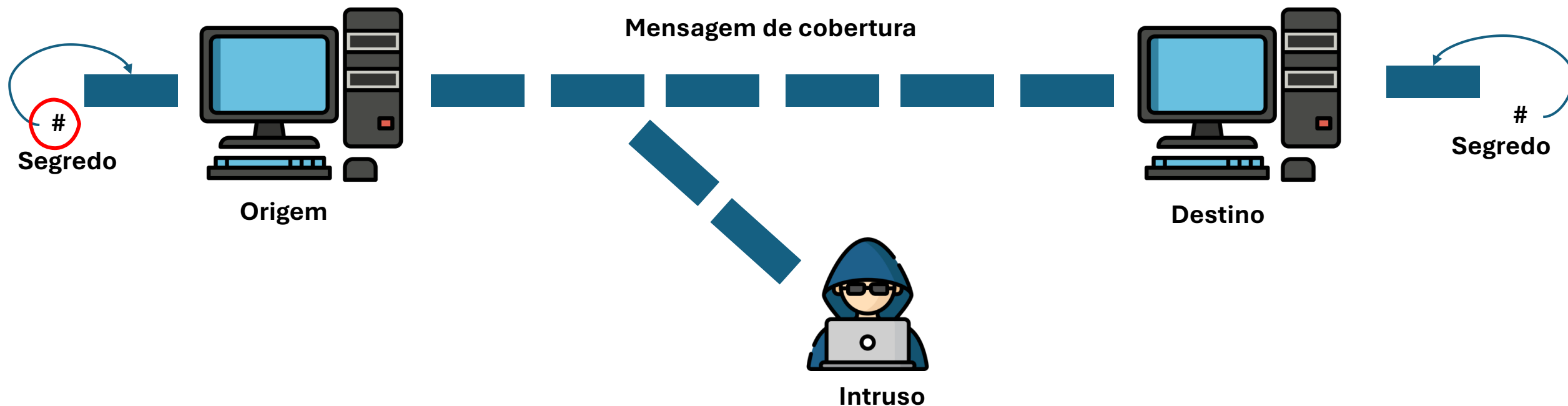
# Duas abordagens possíveis: esteganografia

## 1) Disfarçar os dados: esteganografia



# Duas abordagens possíveis: esteganografia

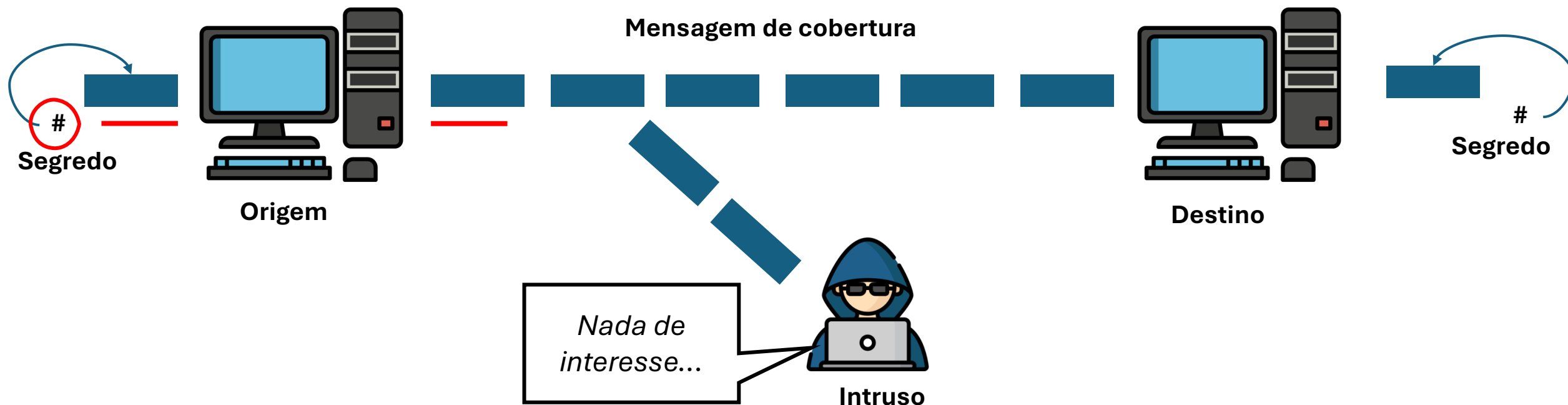
## 1) Disfarçar os dados: esteganografia



# Duas abordagens possíveis: esteganografia

## 1) Disfarçar os dados: esteganografia

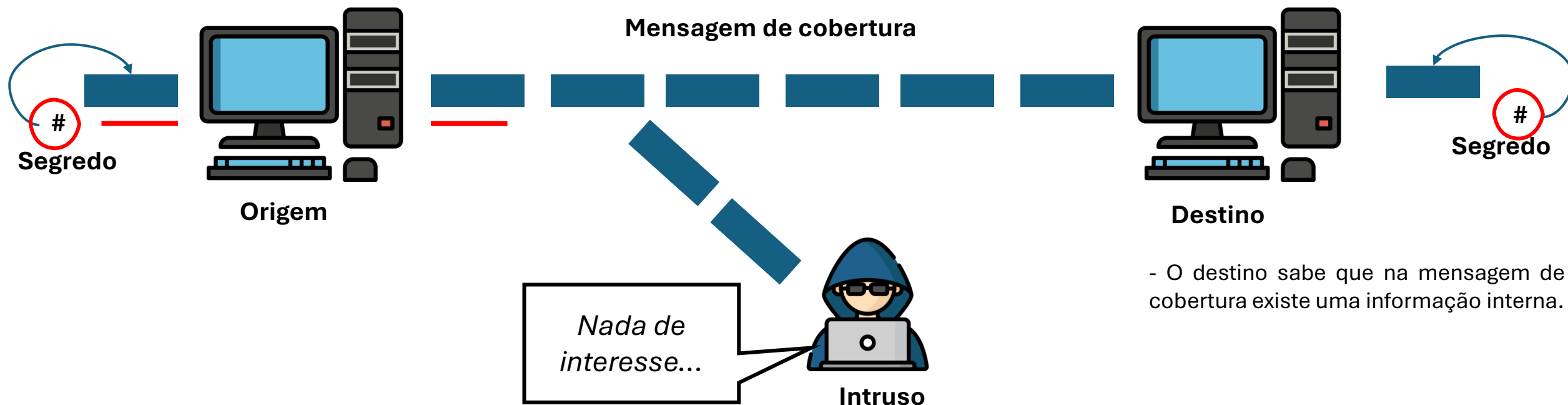
- A mensagem de cobertura pode ser uma imagem, áudio, vídeo, texto, entre outros.



# Duas abordagens possíveis: esteganografia

## 1) Disfarçar os dados: esteganografia

- A mensagem de cobertura pode ser uma imagem, áudio, vídeo, texto, entre outros.

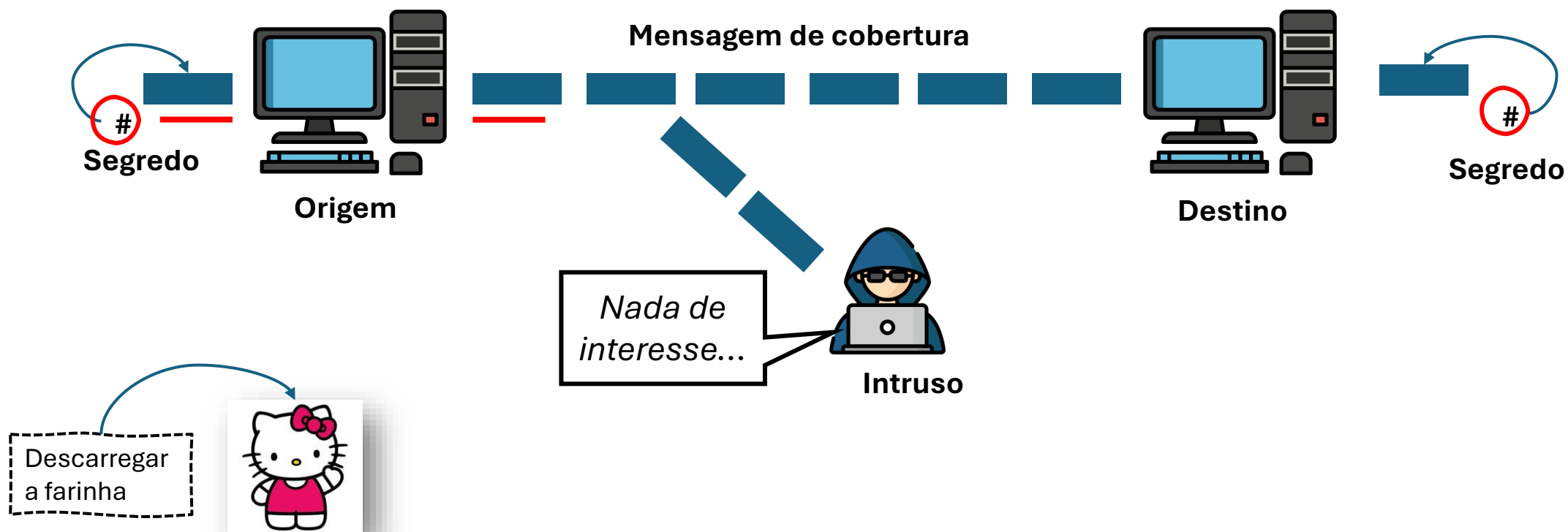


- O destino sabe que na mensagem de cobertura existe uma informação interna.

# Duas abordagens possíveis: esteganografia

## 1) Disfarçar os dados: esteganografia

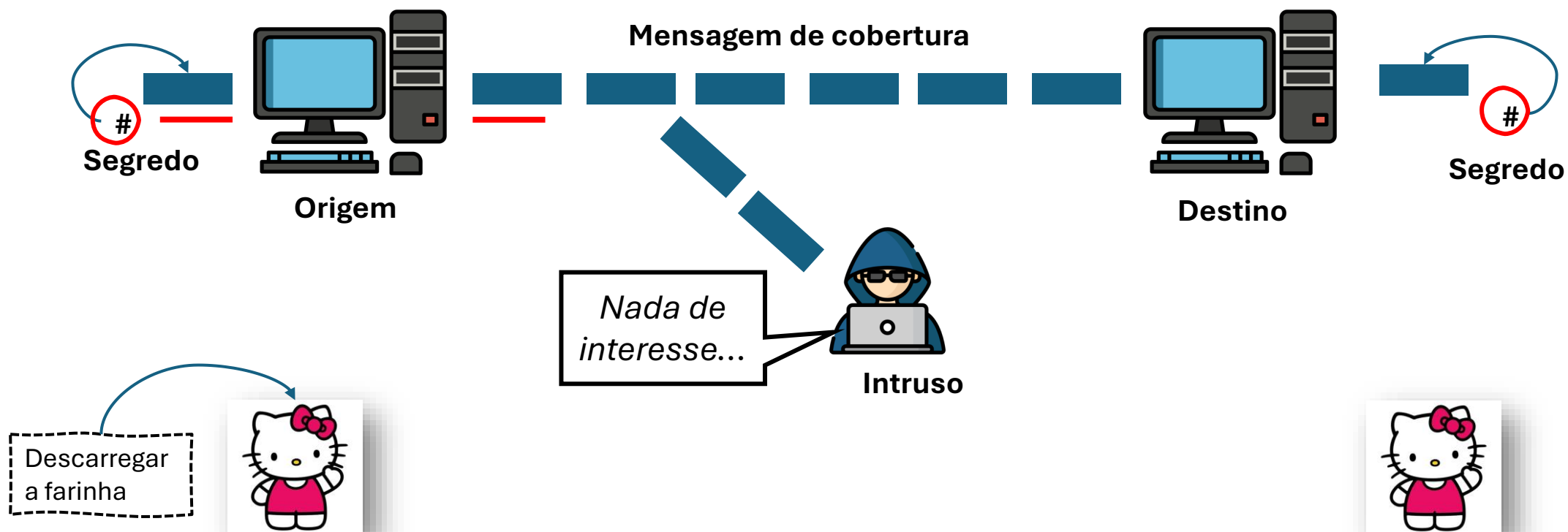
- A mensagem de cobertura pode ser uma imagem, áudio, vídeo, texto, entre outros.



# Duas abordagens possíveis: esteganografia

## 1) Disfarçar os dados: esteganografia

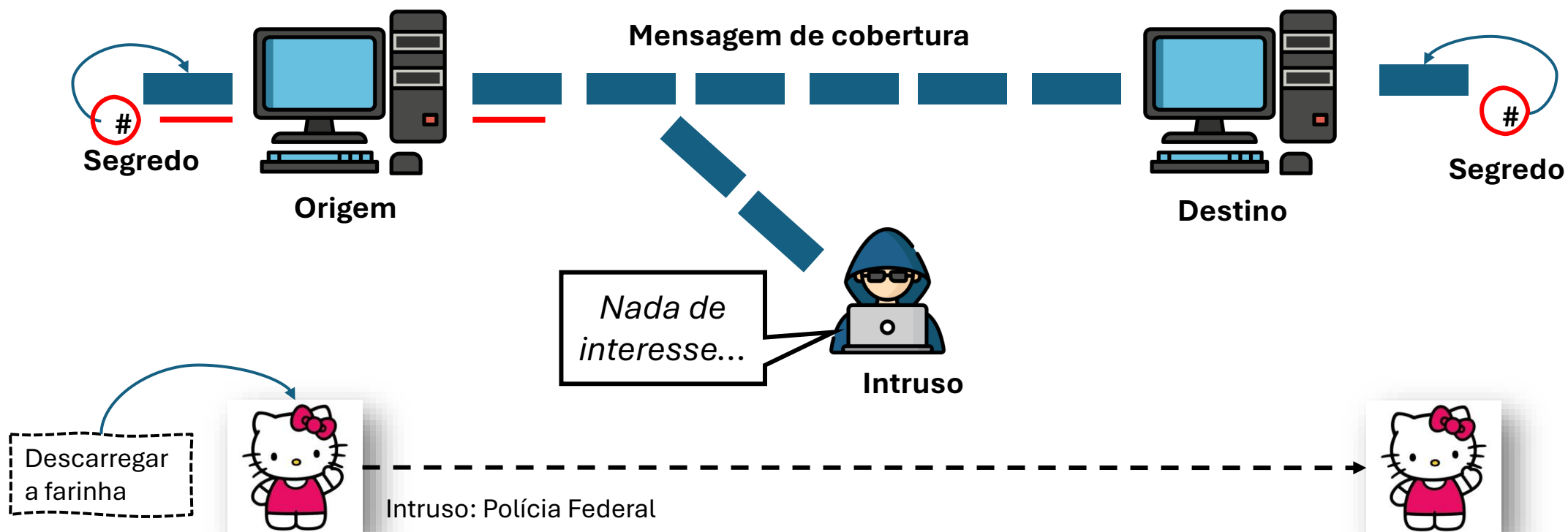
- A mensagem de cobertura pode ser uma imagem, áudio, vídeo, texto, entre outros.



# Duas abordagens possíveis: esteganografia

## 1) Disfarçar os dados: esteganografia

- A mensagem de cobertura pode ser uma imagem, áudio, vídeo, texto, entre outros.

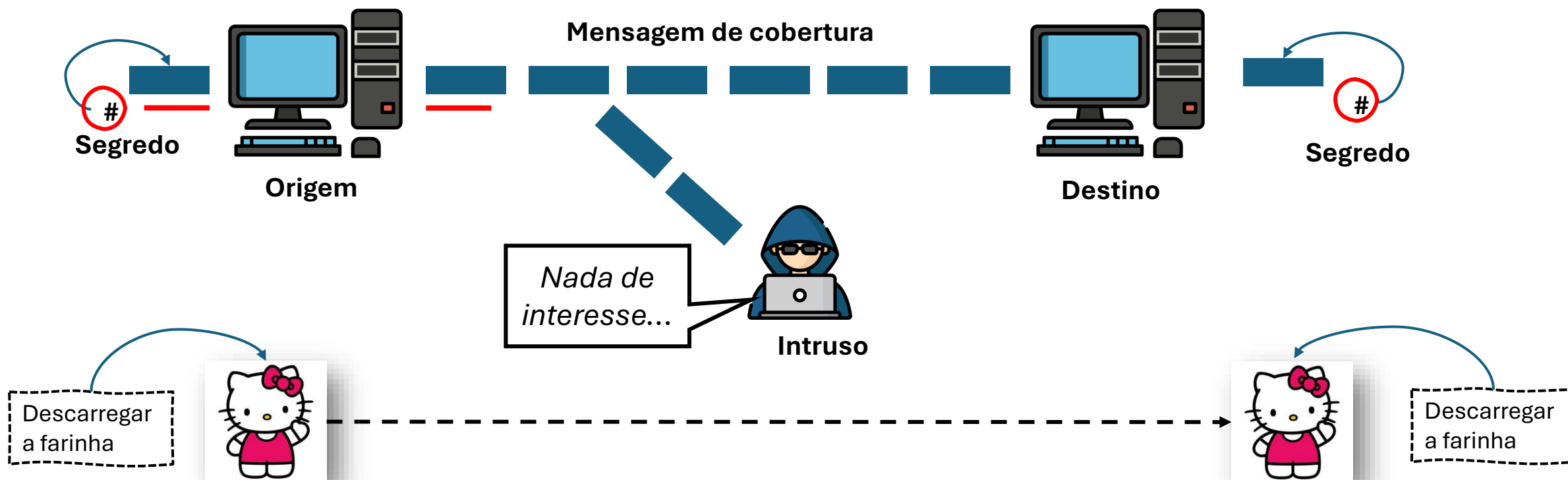




# Duas abordagens possíveis: esteganografia

## 1) Disfarçar os dados: esteganografia

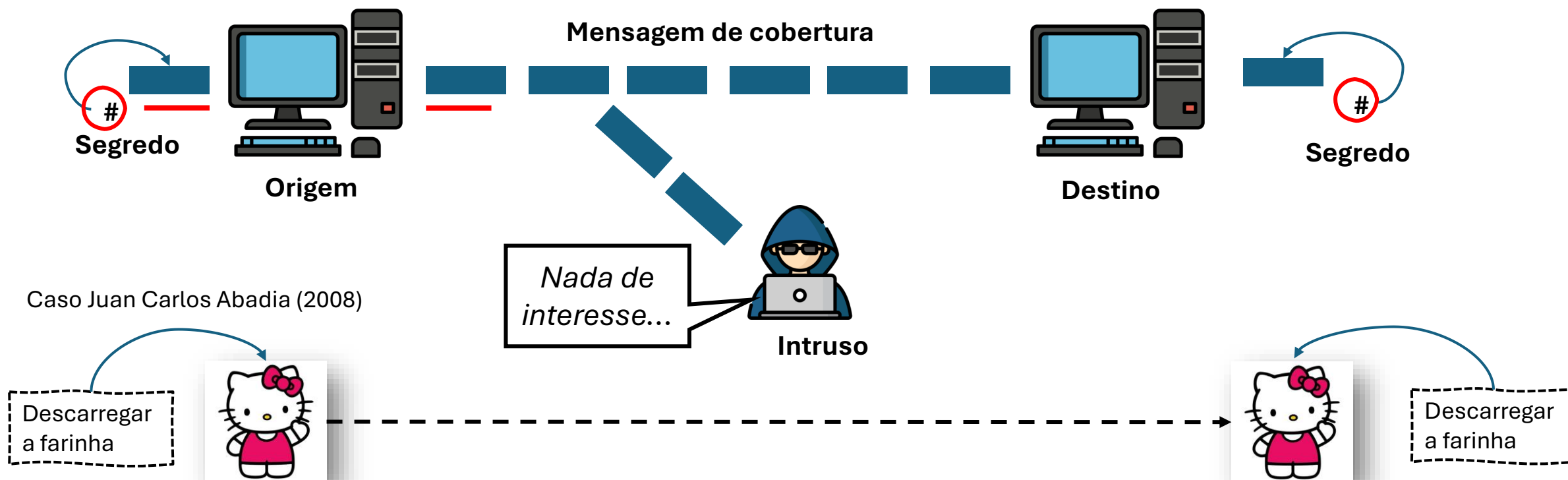
- A mensagem de cobertura pode ser uma imagem, áudio, vídeo, texto, entre outros.



# Duas abordagens possíveis: esteganografia

## 1) Disfarçar os dados: esteganografia

- A mensagem de cobertura pode ser uma imagem, áudio, vídeo, texto, entre outros.



# Duas abordagens possíveis: esteganografia

**Caso Juan Carlos Abadia (2008):**

**Para agência dos EUA, Abadía  
traficou no Brasil**

**Traficante enviaria e-mails com ordens escondidas em  
imagens da Hello Kitty**

**Eventual comprovação de que colombiano comandou  
tráfico a partir do Brasil poderá fazer que pedido de  
extradição seja negado**

**MARIO CESAR CARVALHO**  
DA REPORTAGEM LOCAL

<https://www1.folha.uol.com.br/fsp/cotidian/ff1003200801.htm>

[https://sbseg2016.ic.uff.br/pt/files/minicursos.pdf?utm\\_source](https://sbseg2016.ic.uff.br/pt/files/minicursos.pdf?utm_source) - pág. 46

# Esteganografia: exemplo

## Bit Menos Significativo (LSB):

- Alteração dos pixels da imagem;
- Um dos métodos mais utilizados na área da esteganografia;

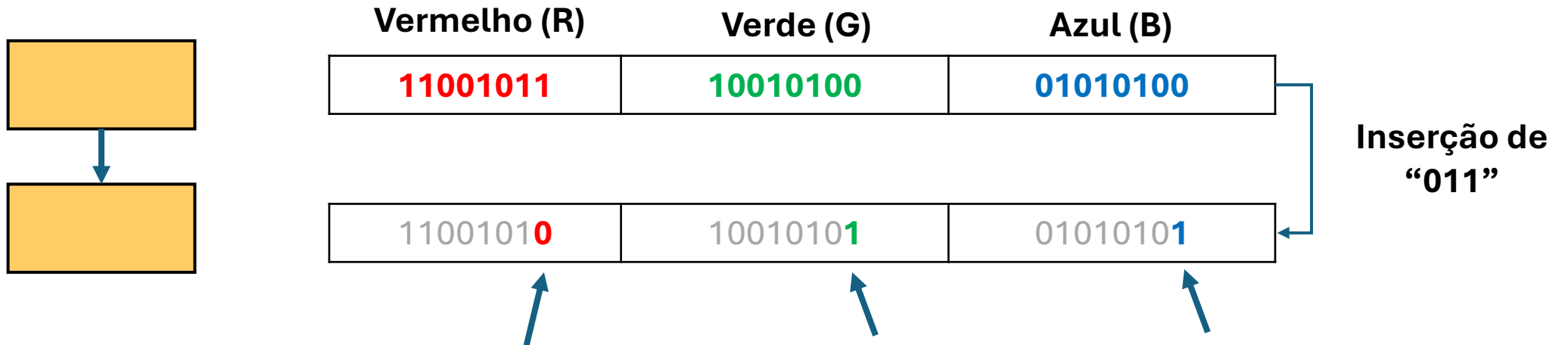


Vermelho (R)	Verde (G)	Azul (B)
11001011	10010100	01010100

# Esteganografia: exemplo

## Bit Menos Significativo (LSB):

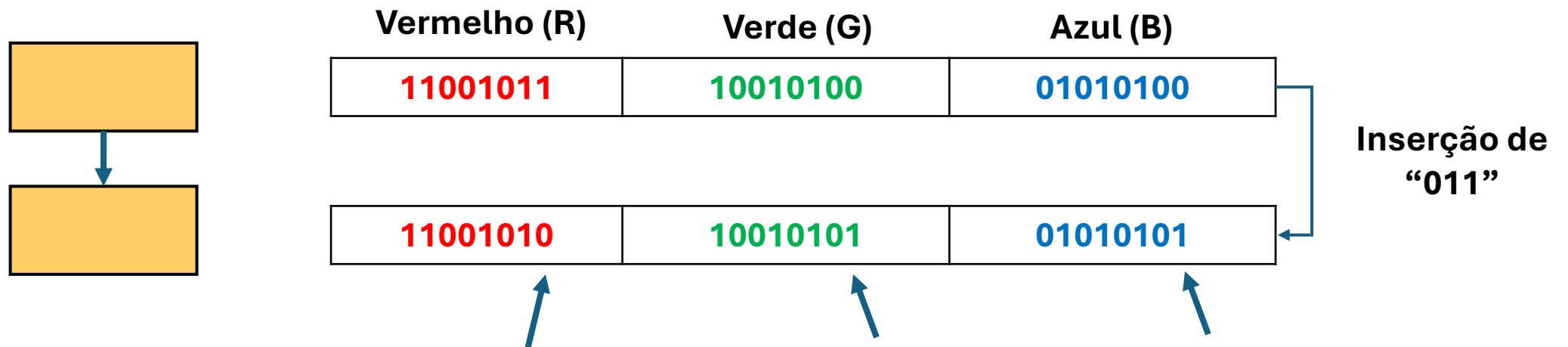
- Alteração dos pixels da imagem;
- Um dos métodos mais utilizados na área da esteganografia;
- Capacidade: segredo/cobertura  $\leq 1/8$



# Esteganografia: exemplo

## Bit Menos Significativo (LSB):

- Alteração dos pixels da imagem;
- Um dos métodos mais utilizados na área da esteganografia;
- Capacidade: segredo/cobertura  $\leq 1/8$



Em uma imagem de 8k é possível esconder 1k de informação sem distorcer (8bits = 1 bit de informação)

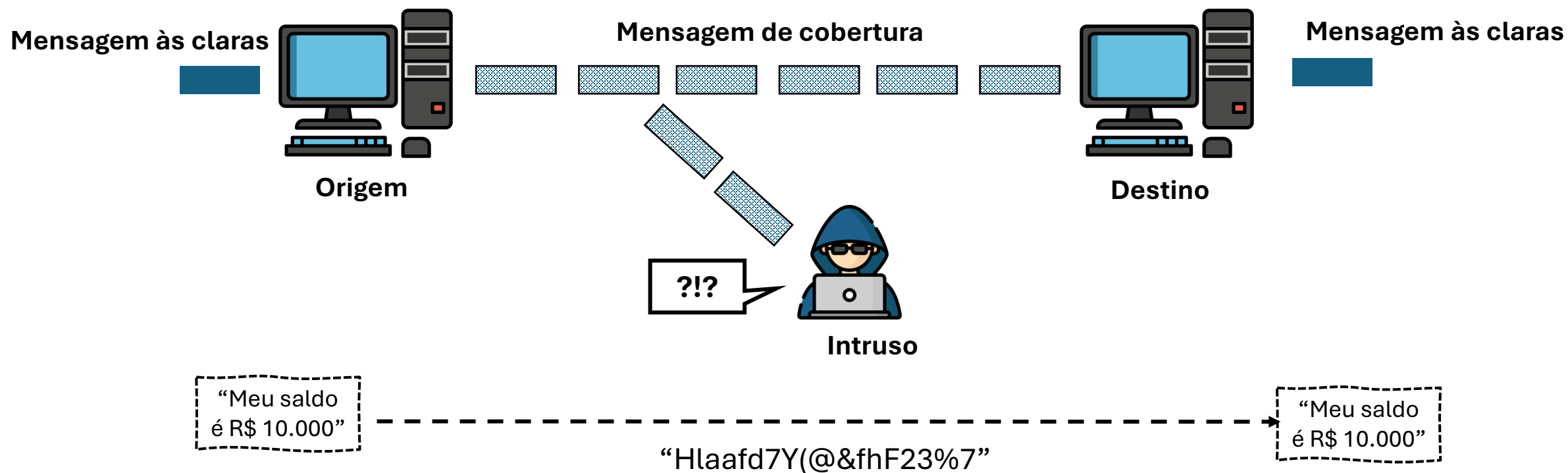
# Esteganografia: exemplo

## Bit Menos Significativo (LSB):

- Alteração dos pixels da imagem;
- Um dos métodos mais utilizados na área da esteganografia;
- Capacidade: segredo/cobertura  $\leq 1/8$ ;
- Não é utilizado na prática porque precisa de uma imagem de cobertura muito grande para conseguir colocar a informação dentro da imagem;

# Duas abordagens possíveis: cifras

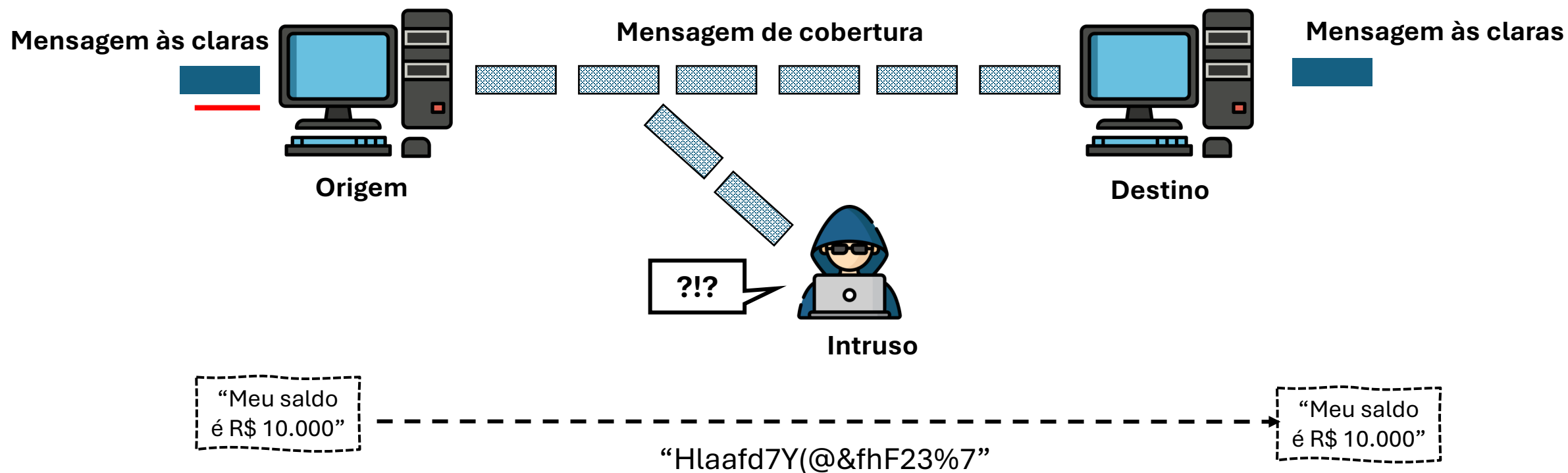
## 2) Embaralhar os dados: cifras





# Duas abordagens possíveis: cifras

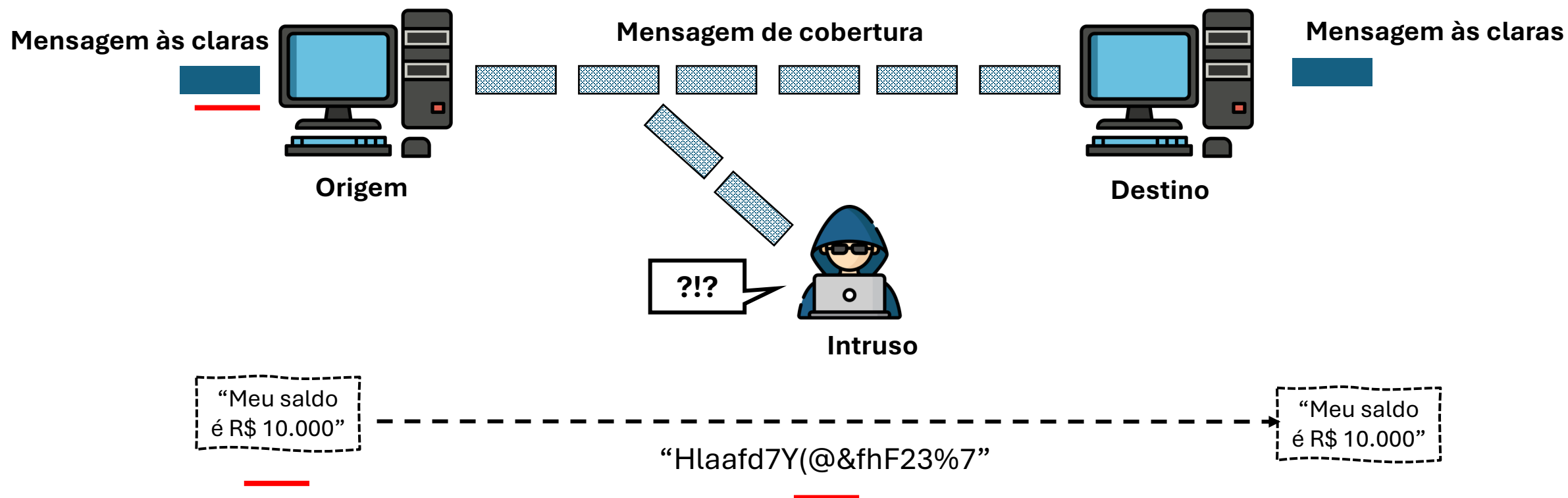
## 2) Embaralhar os dados: cifras



# Duas abordagens possíveis: cifras

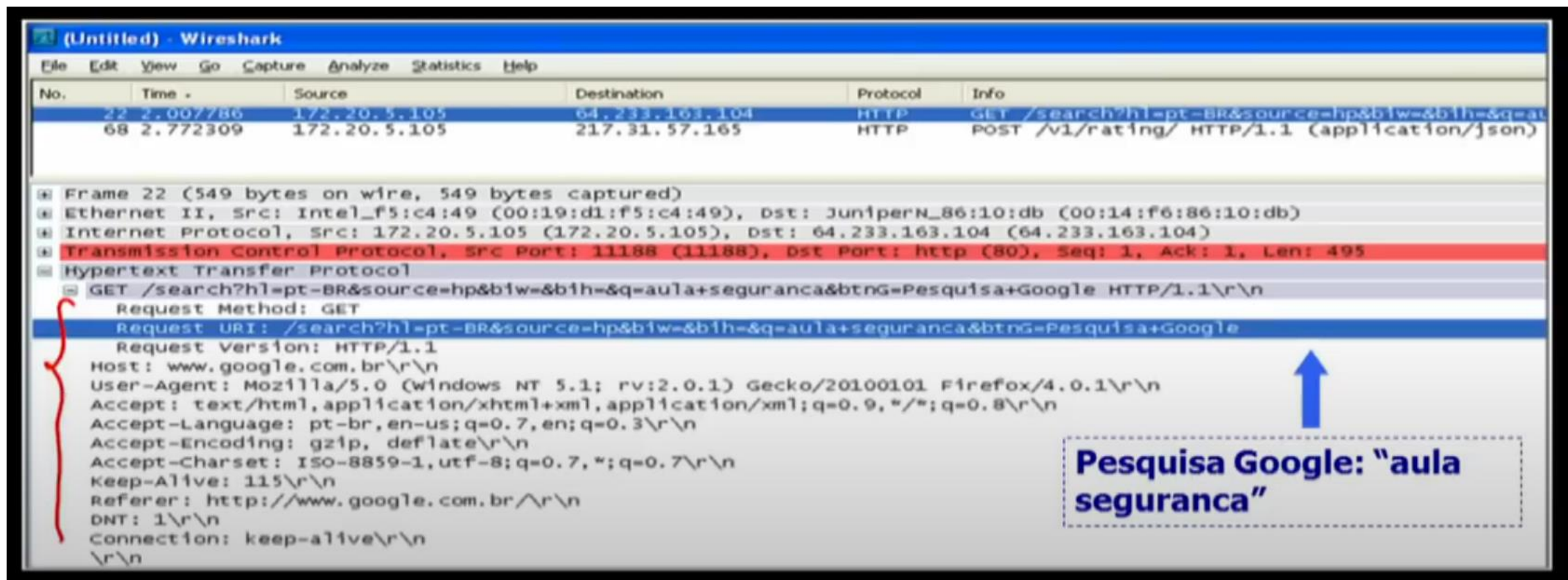
## 2) Embaralhar os dados: cifras

Intrusos não identificam o que está sendo enviado pela rede



# Exemplo prático: HTTP vs. HTTPS

HTTP: dados passam em aberto na rede



The image shows a Wireshark packet capture of an HTTP GET request. The packet list at the top shows two packets: packet 22 (GET) and packet 68 (POST). The packet details pane for packet 22 is expanded, showing the following information:

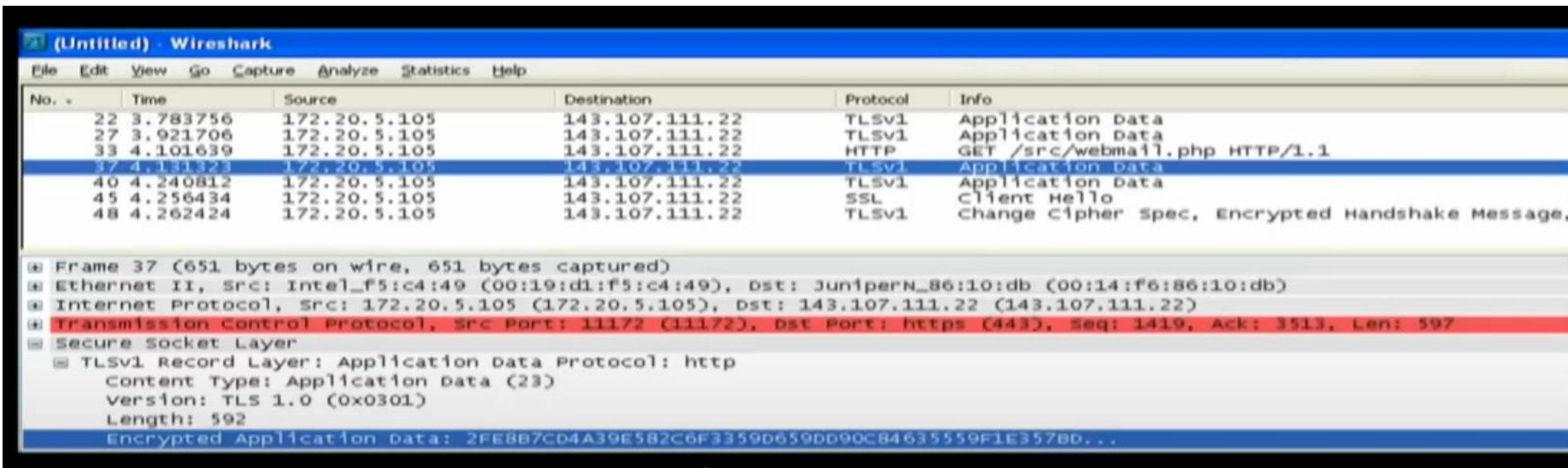
- Frame 22 (549 bytes on wire, 549 bytes captured)
- Ethernet II, Src: Intel\_f5:c4:49 (00:19:d1:f5:c4:49), Dst: JuniperN\_86:10:db (00:14:f6:86:10:db)
- Internet Protocol, Src: 172.20.5.105 (172.20.5.105), Dst: 64.233.163.104 (64.233.163.104)
- Transmission Control Protocol, Src Port: 11188 (11188), Dst Port: http (80), Seq: 1, Ack: 1, Len: 495
- Hypertext Transfer Protocol
  - GET /search?hl=pt-BR&source=hp&biw=&bih=&q=aula+seguranca&btnG=Pesquisa+Google HTTP/1.1\r\n
  - Request Method: GET
  - Request URI: /search?hl=pt-BR&source=hp&biw=&bih=&q=aula+seguranca&btnG=Pesquisa+Google
  - Request Version: HTTP/1.1
  - Host: www.google.com.br\r\n
  - User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1\r\n
  - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\r\n
  - Accept-Language: pt-br,en-us;q=0.7,en;q=0.3\r\n
  - Accept-Encoding: gzip, deflate\r\n
  - Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7\r\n
  - Keep-Alive: 115\r\n
  - Referer: http://www.google.com.br/\r\n
  - DNT: 1\r\n
  - Connection: keep-alive\r\n
  - \r\n

A red bracket on the left side of the packet details pane highlights the request information. A blue arrow points from the text box on the right to the Request URI field.

**Pesquisa Google: "aula seguranca"**

# Exemplo prático: HTTP vs. HTTPS

## HTTPS: dados cifrados (túnel TLS)



No.	Time	Source	Destination	Protocol	Info
22	3.783756	172.20.5.105	143.107.111.22	TLSv1	Application Data
27	3.921706	172.20.5.105	143.107.111.22	TLSv1	Application Data
33	4.101639	172.20.5.105	143.107.111.22	HTTP	GET /src/webmail.php HTTP/1.1
37	4.131323	172.20.5.105	143.107.111.22	TLSv1	Application Data
40	4.240812	172.20.5.105	143.107.111.22	TLSv1	Application Data
45	4.256434	172.20.5.105	143.107.111.22	SSL	Client Hello
48	4.262424	172.20.5.105	143.107.111.22	TLSv1	Change Cipher Spec, Encrypted Handshake Message,

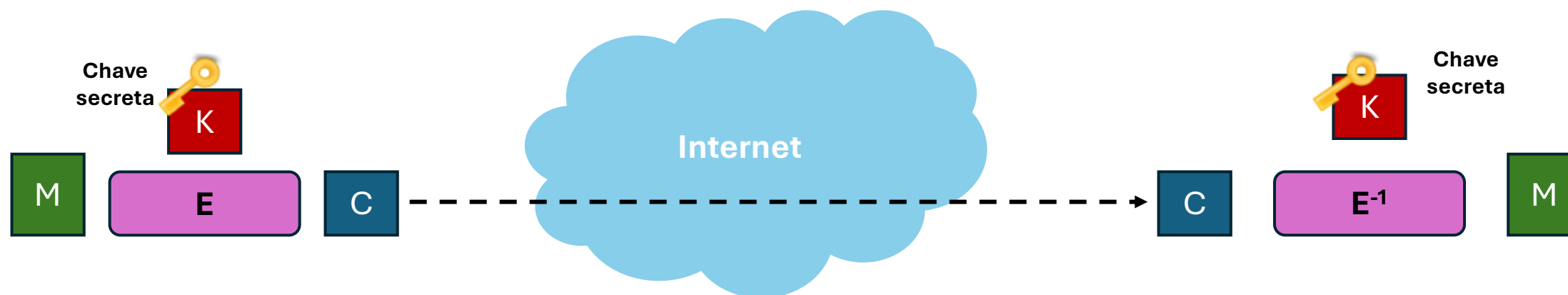
Frame 37 (651 bytes on wire, 651 bytes captured)
Ethernet II, Src: Intel_f5:c4:49 (00:19:d1:f5:c4:49), Dst: JuniperN_86:10:db (00:14:f6:86:10:db)
Internet Protocol, Src: 172.20.5.105 (172.20.5.105), Dst: 143.107.111.22 (143.107.111.22)
Transmission Control Protocol, Src Port: 11172 (11172), Dst Port: https (443), Seq: 1419, Ack: 3513, Len: 597
Secure Socket Layer
TLSv1 Record Layer: Application Data Protocol: http
Content Type: Application Data (23)
Version: TLS 1.0 (0x0301)
Length: 592
Encrypted Application Data: 2FE8B7CD4A39E582C6F3359D659DD90C84635559F1E357BD...

Dados enviados durante login em webmail 

# Cifragem simétrica: definição

Transformação matemática reversível: **cifração e decifração**

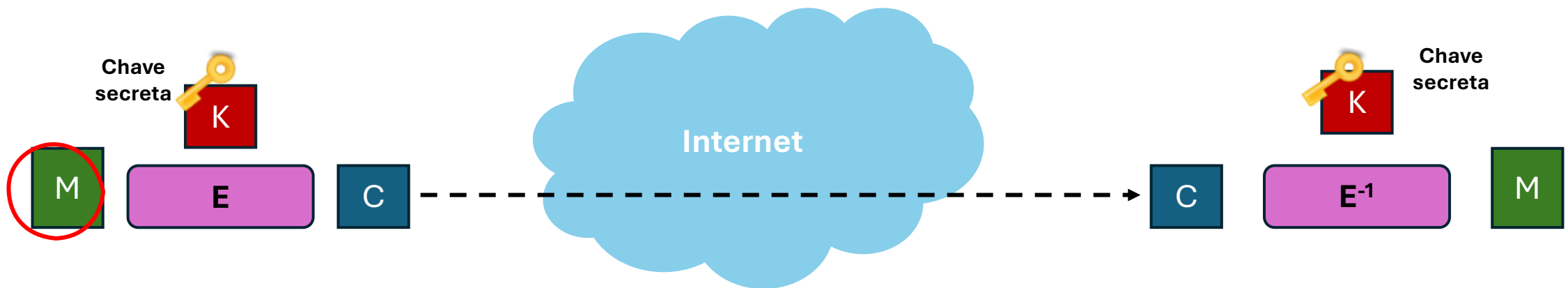
- Os dois processos dependem de uma **mesma informação secreta: a chave K**
- Se K for descoberta, então a confidencialidade é perdida;



# Cifragem simétrica: definição

Transformação matemática reversível: **cifração e decifração**

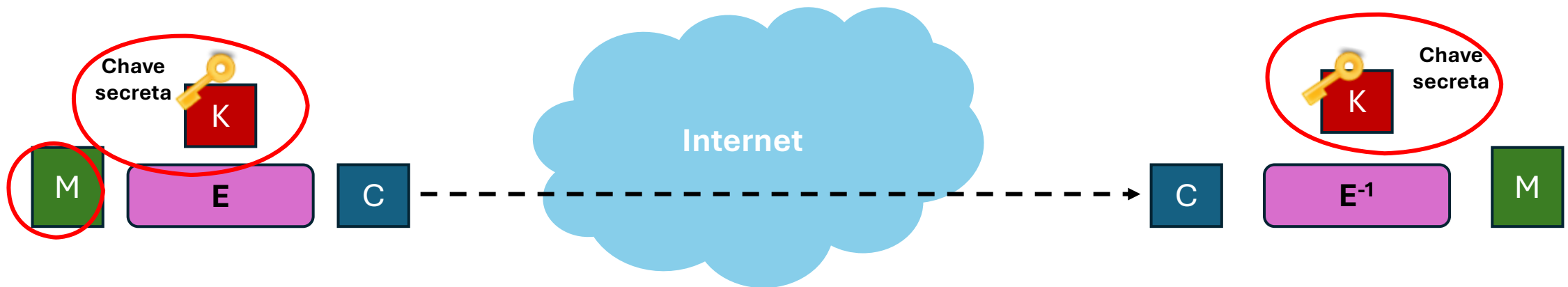
- Os dois processos dependem de uma **mesma informação secreta: a chave K**
- Se K for descoberta, então a confidencialidade é perdida;



# Cifragem simétrica: definição

Transformação matemática reversível: **cifração e decifração**

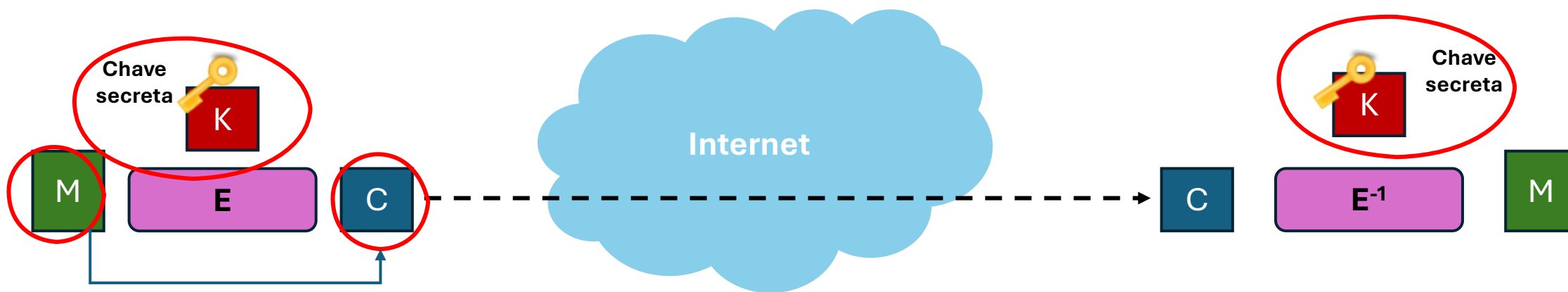
- Os dois processos dependem de uma **mesma informação secreta: a chave K**
- Se K for descoberta, então a confidencialidade é perdida;



# Cifragem simétrica: definição

Transformação matemática reversível: **cifração e decifração**

- Os dois processos dependem de uma **mesma informação secreta: a chave K**
- Se K for descoberta, então a confidencialidade é perdida;



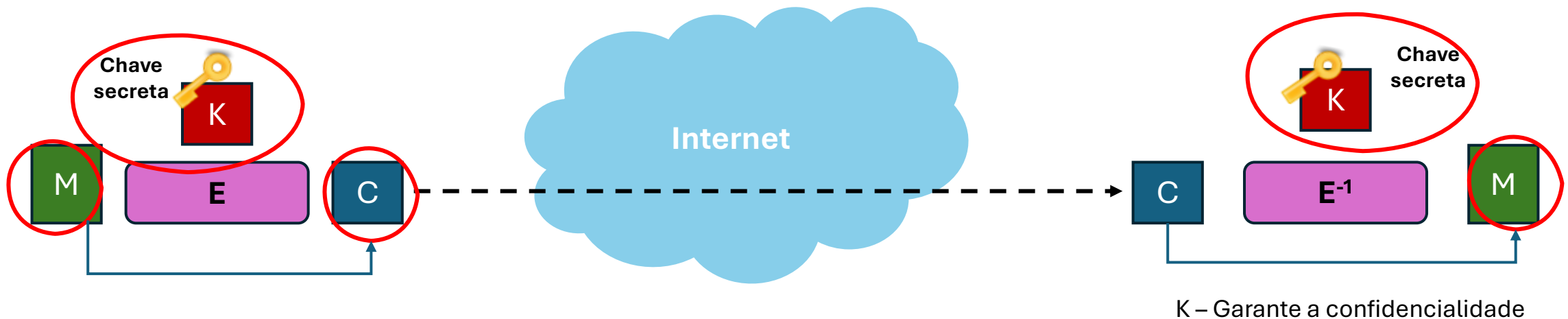
Usando algoritmos de cifração ou encriptação que transforma M em C (mensagem embaralhada)



# Cifragem simétrica: definição

Transformação matemática reversível: **cifração e decifração**

- Os dois processos dependem de uma **mesma informação secreta: a chave K**
- Se K for descoberta, então a confidencialidade é perdida;

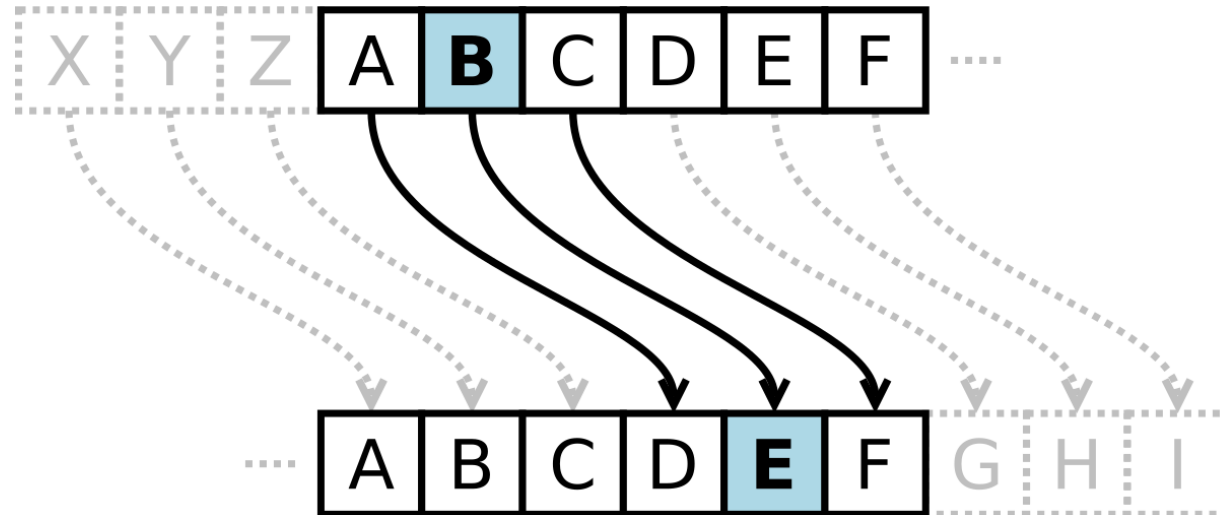


# Cifragem simétrica: exemplo



**Cifragem de César:** deslocar cada letra da mensagem de **k posições** no alfabeto latino (i.e., somar k posições);

- Decifrar equivale a subtrair a mesma chave k.
- Técnica usada por Júlio César para troca de mensagens com seus generais, com  $k = 3$ .

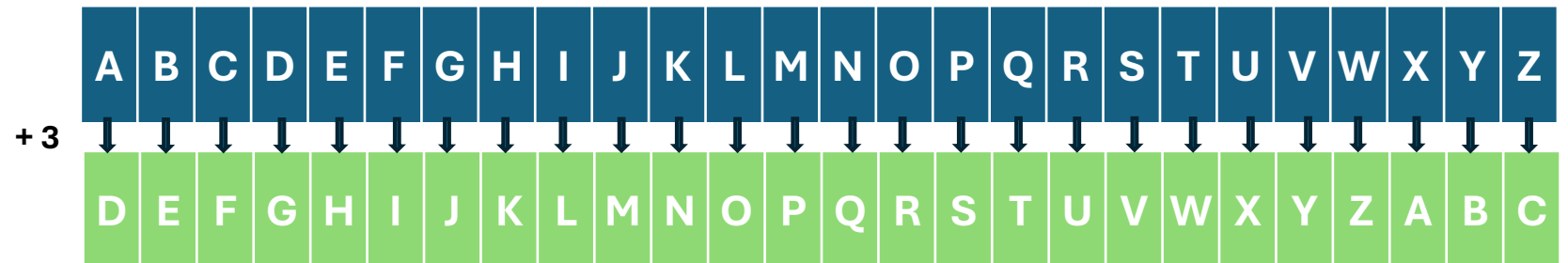


# Cifragem simétrica: exemplo



**Cifragem de César:** deslocar cada letra da mensagem de **k posições** no alfabeto latino (i.e., somar k posições);

- Decifrar equivale a subtrair a mesma chave k.
- Técnica usada por Júlio César para troca de mensagens com seus generais, com  $k = 3$ .

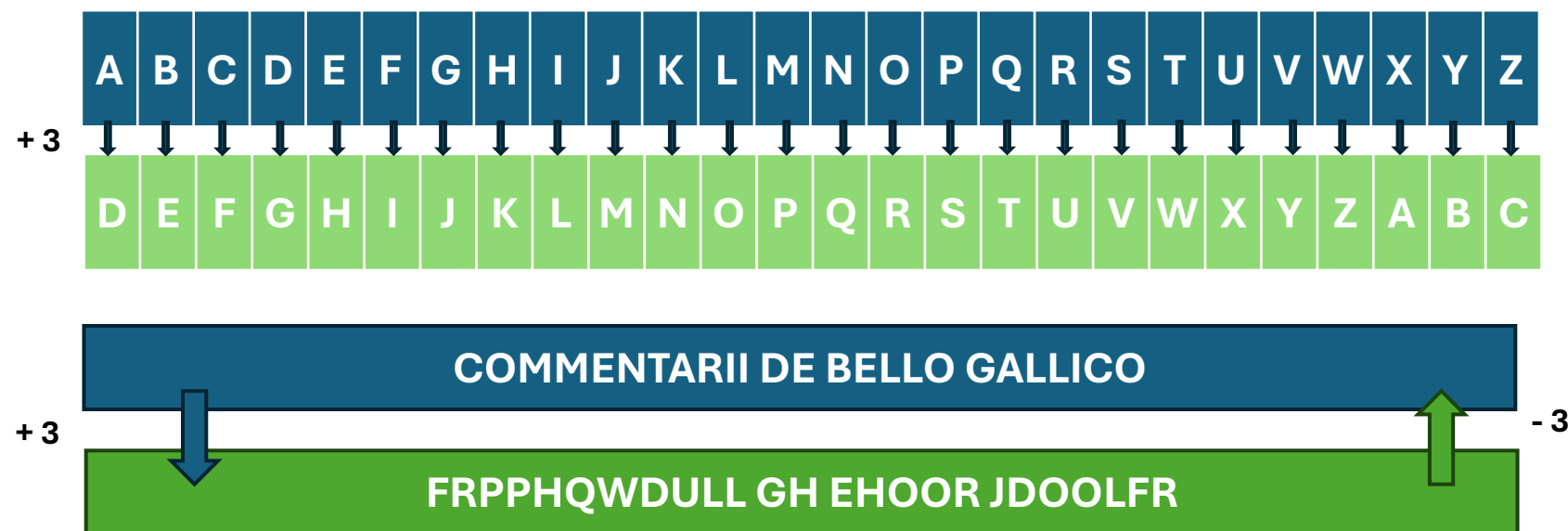


# Cifragem simétrica: exemplo



**Cifragem de César:** deslocar cada letra da mensagem de **k posições** no alfabeto latino (i.e., somar  $k$  posições);

- Decifrar equivale a subtrair a mesma chave  $k$ .
- Técnica usada por Júlio César para troca de mensagens com seus generais, com  $k = 3$ .



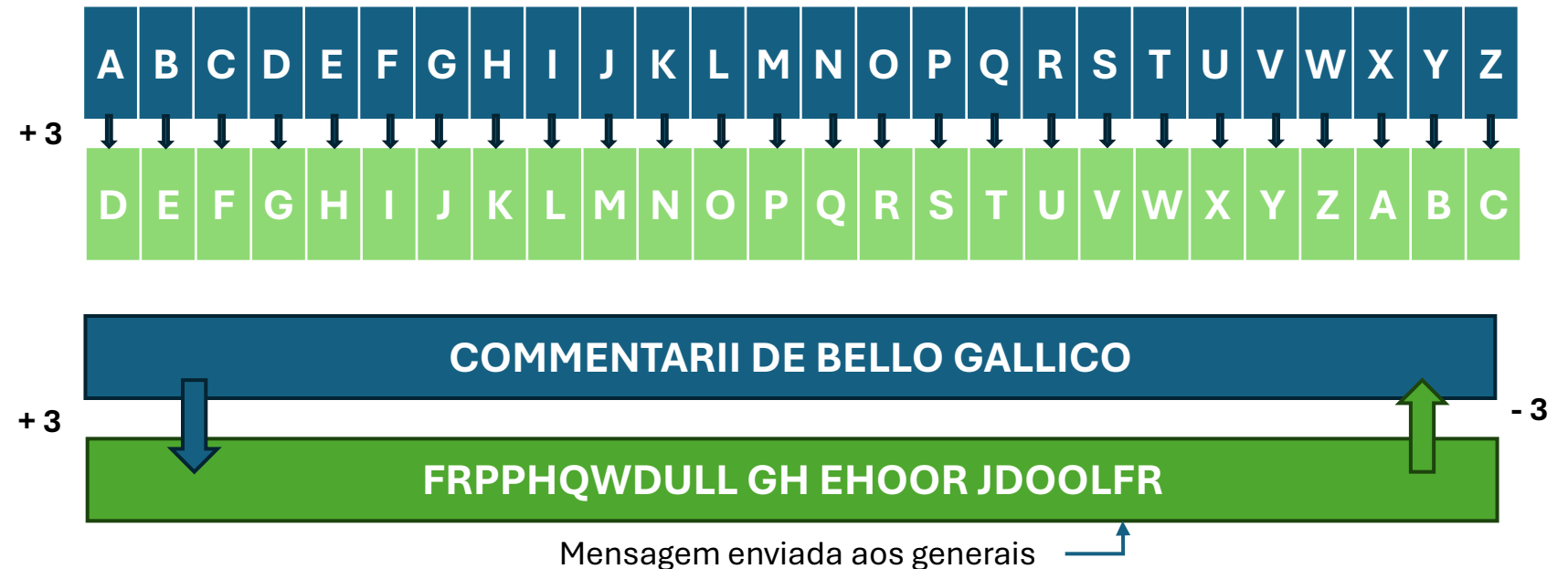


# Cifragem simétrica: exemplo



**Cifragem de César:** deslocar cada letra da mensagem de **k posições** no alfabeto latino (i.e., somar k posições);

- Decifrar equivale a subtrair a mesma chave k.
- Técnica usada por Júlio César para troca de mensagens com seus generais, com  $k = 3$ .



# Cifragem simétrica: exemplo

## Exercício:

- Decifrar a seguinte mensagem e identificar o valor de  $k$  usado
- Dica:  $k$  pode ter qualquer valor entre 1 e 25

NBBN ENAVNUQX MN VNDB XUQXB ENV MX ENAMN MJ WJCDANIJ

# Cifragem simétrica: exemplo

## Exercício:

- Decifrar a seguinte mensagem e identificar o valor de  $k$  usado
- Dica:  $k$  pode ter qualquer valor entre 1 e 25

Máx. de chaves

NBBN ENAVNUQX MN VNDB XUQXB ENV MX ENAMN MJ WJCDANIJ

# Cifragem simétrica: exemplo

## Exercício:

- Decifrar a seguinte mensagem e identificar o valor de  $k$  usado
- Dica:  $k$  pode ter qualquer valor entre 1 e 25
- Qualquer computador pode quebrar Máx. de chaves

NBBN ENAVNUQX MN VNDB XUQXB ENV MX ENAMN MJ WJCDANIJ



# Cifragem simétrica: exemplo

## Exercício:

- Decifrar a seguinte mensagem e identificar o valor de  $k$  usado
- Dica:  $k$  pode ter qualquer valor entre 1 e 25

Máx. de chaves



NBBN ENAVNUQX MN VNDB XUQXB ENV MX ENAMN MJ WJCDANIJ

# Cifragem simétrica: exemplo

## Resposta:

- Alguns facilitadores:
  - Conhecer a língua é importante;

NBBN ENAVNUQX MN VNDB XUQXB ENV MX ENAMN MJ WJCDANIJ

# Cifragem simétrica: exemplo

## Resposta:

- Alguns facilitadores:
  - Conhecer os padrões da língua

N **BB** N ENAVNUQX **MN** VNDB XUQXB ENV **MX** ENAMN **MJ** WJCDANIJ

# Cifragem simétrica: exemplo

## Resposta:

- Alguns facilitadores:
  - A letra que mais aparece no português é o **A**

N **BB** N ENAVNUQX **MN** VNDB XUQXB ENV **MX** ENAMN **MJ** WJCDANIJ

# Cifragem simétrica: exemplo

## Resposta: 9

- Alguns facilitadores:
  - A letra que mais aparece no português é o **A**

N **BB** N ENAVNUQX **MN** VNDB XUQXB ENV **MX** ENAMN **MJ** WJCDANIJ

*“Esse vermelho de meus olhos vem do verde da natureza.”*



# **Cifração moderna: AES e modos de operação**

# Cifras: algoritmos principais



## **DES (*Data Encryption Standard*):**

- Absoluto desde 2004 (chaves de 56 bits: muito curtas)

## **3DES (*DES Triplo*): aplicação tripla do DES**

- Legado: reaproveita implementação do DES simples
- Chaves:  $3 \times 56 = 168$  bits (mas segurança é de  $\sim 112$  bits)



## **RCA (*ArcFour*):**

- Chave: tamanho variável (múltiplo de 8 bits, até 2048 bits);
- Legado: uso seguro requer truques (descartar dados iniciais: `RCA_drop[n]`); não recomendado para aplicação futuras



## **AES (*Advanced Encryption Standard*):**

- Padrão atual (desde 2001): vencedor de concurso público iniciado em 1997
- Chaves de 128/192/256 bits.

# Cifras: algoritmos principais



DES (*Data Encryption Standard*):

- Absoluto desde 2004 (chaves de 56 bits: muito curtas)

3DES (*DES Triplo*): aplicação tripla do DES

- Legado: reaproveita implementação do DES simples
- Chaves:  $3 \times 56 = 168$  bits (mas segurança é de  $\sim 112$  bits)



RCA (*ArcFour*):

- Chave: tamanho variável (múltiplo de 8 bits, até 2048 bits);
- Legado: uso seguro requer truques (descartar dados iniciais: `RCA_drop[n]`); não recomendado para aplicação futuras



**AES (*Advanced Encryption Standard*):**

- Padrão atual (desde 2001): vencedor de concurso público iniciado em 1997
- Chaves de 128/192/256 bits.



# Cifras: algoritmos principais



## ***AES (Advanced Encryption Standard):***

- Padrão atual (desde 2001): vencedor de concurso público iniciado em 1997
- Chaves de 128/192/256 bits.
- Mais rápida entre os modelos apresentados anteriormente;
- Evita os problemas de análise estatísticas, letras próximas umas das outras, usando os princípios de **difusão e confusão**



# Difusão vs. Confusão

**Princípios básicos**, definidos por Claude Shannon, para o projeto de cifras seguras.

- **Difusão**: cada caractere da mensagem cifrada deve depender do **maior número possível** de caracteres da mensagem às claras e da chave.

ESSE  
↓  
NBBN

ESSA  
↓  
NBBJ

Cifra de César: baixa difusão

ESSE  
↓  
XKRP

ESSA  
↓  
QQTZ

Cifras modernas: alta difusão



# Difusão vs. Confusão

**Princípios básicos**, definidos por Claude Shannon, para o projeto de cifras seguras.

- **Difusão**: cada caractere da mensagem cifrada deve depender do **maior número possível** de caracteres da mensagem às claras e da chave.

ESSE  
↓  
NBBN

ESSA  
↓  
NBBJ

Cifra de César: baixa difusão

ESSE  
↓  
XKRP

ESSA  
↓  
QQTZ

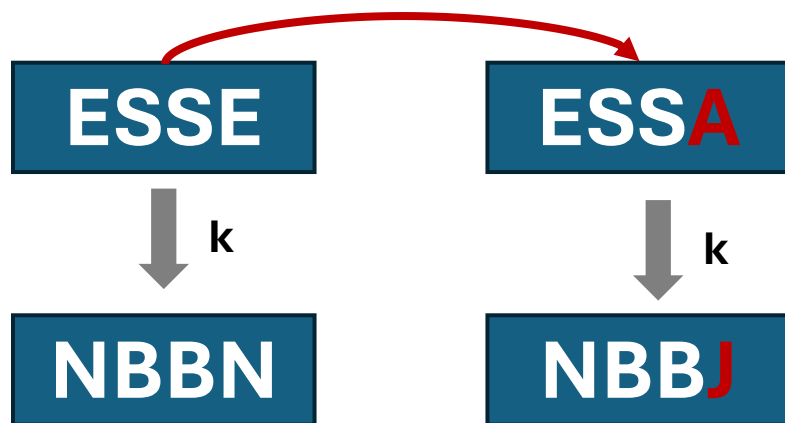
Cifras modernas: alta difusão



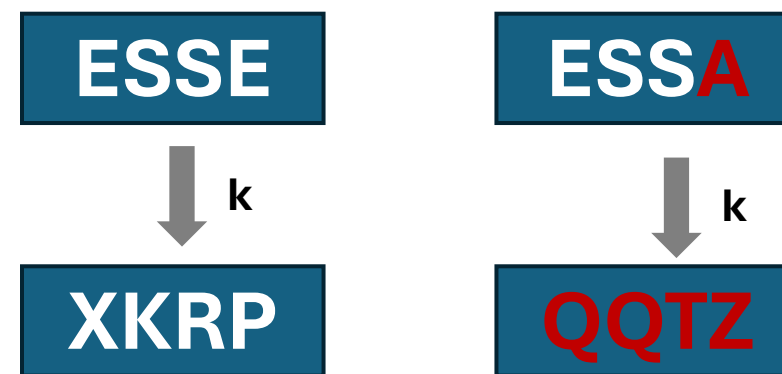
# Difusão vs. Confusão

**Princípios básicos**, definidos por Claude Shannon, para o projeto de cifras seguras.

- **Difusão**: cada caractere da mensagem cifrada deve depender do **maior número possível** de caracteres da mensagem às claras e da chave.



Cifra de César: baixa difusão



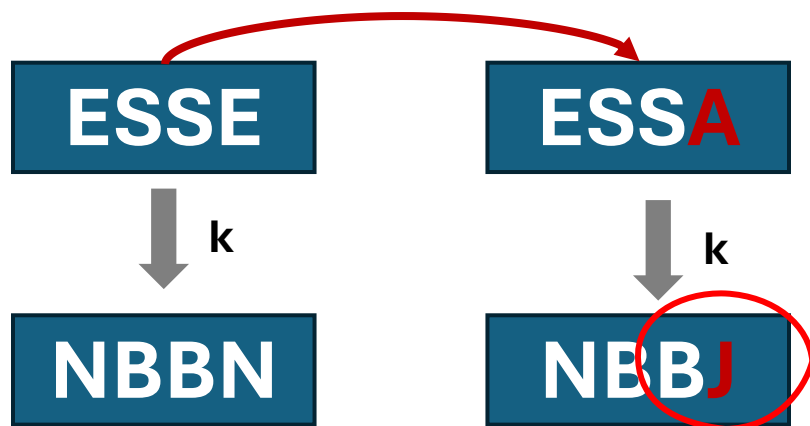
Cifras modernas: alta difusão



# Difusão vs. Confusão

**Princípios básicos**, definidos por Claude Shannon, para o projeto de cifras seguras.

- **Difusão**: cada caractere da mensagem cifrada deve depender do **maior número possível** de caracteres da mensagem às claras e da chave.



Cifra de César: baixa difusão



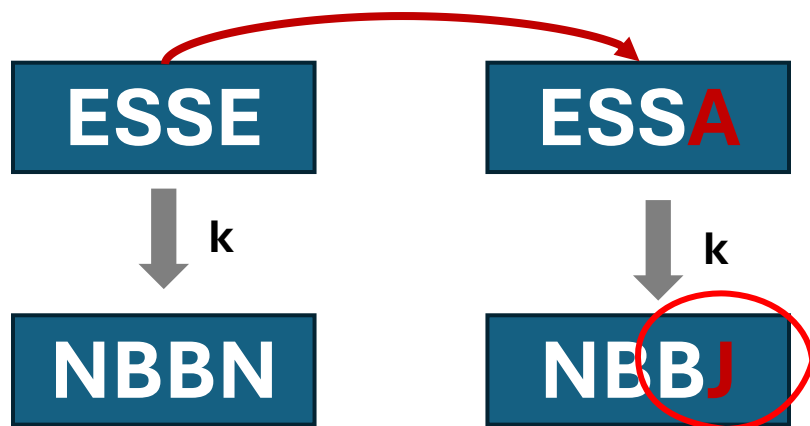
Cifras modernas: alta difusão



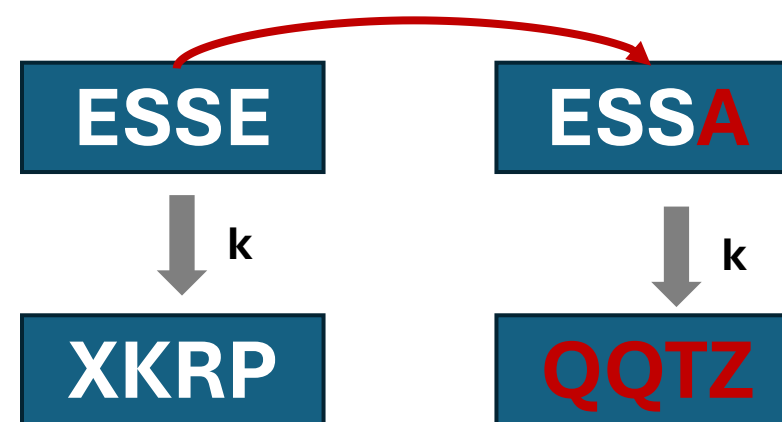
# Difusão vs. Confusão

**Princípios básicos**, definidos por Claude Shannon, para o projeto de cifras seguras.

- **Difusão**: cada caractere da mensagem cifrada deve depender do **maior número possível** de caracteres da mensagem às claras e da chave.



Cifra de César: baixa difusão



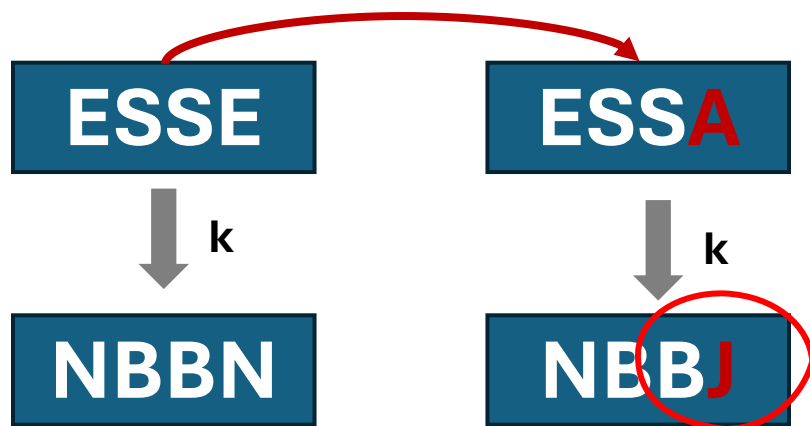
Cifras modernas: alta difusão



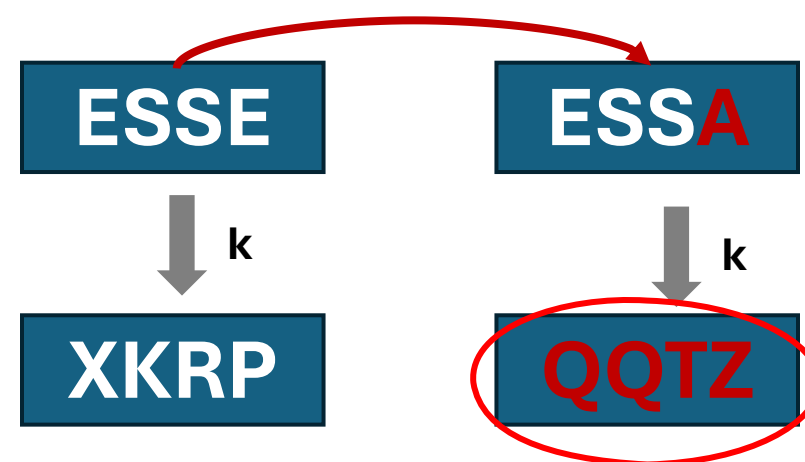
# Difusão vs. Confusão

**Princípios básicos**, definidos por Claude Shannon, para o projeto de cifras seguras.

- **Difusão**: cada caractere da mensagem cifrada deve depender do **maior número possível** de caracteres da mensagem às claras e da chave.



Cifra de César: baixa difusão



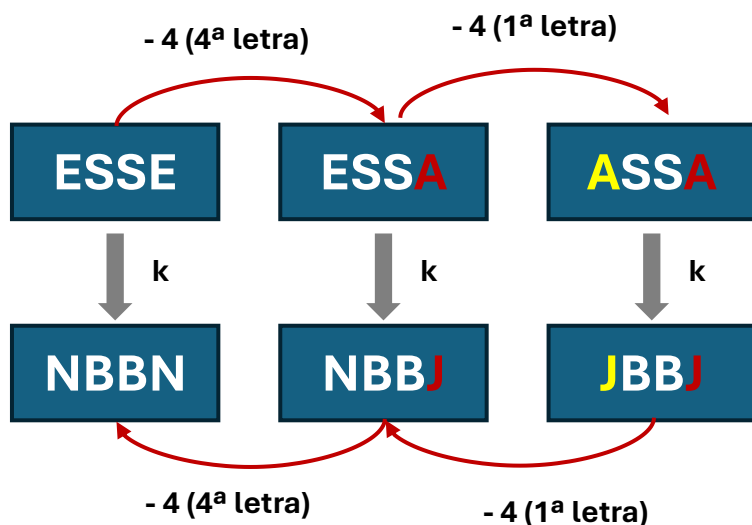
Cifras modernas: alta difusão



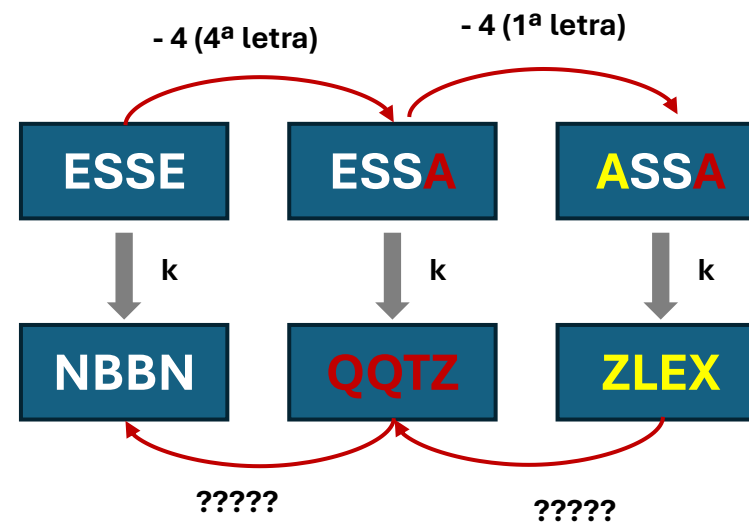
# Difusão vs. Confusão

**Princípios básicos**, definidos por Claude Shannon, para o projeto de cifras seguras.

- **Confusão**: relação entre a mensagem às claras, cifrada e a chave deve ter **alta complexidade**.



Cifra de César: baixa difusão



Cifras modernas: alta confusão

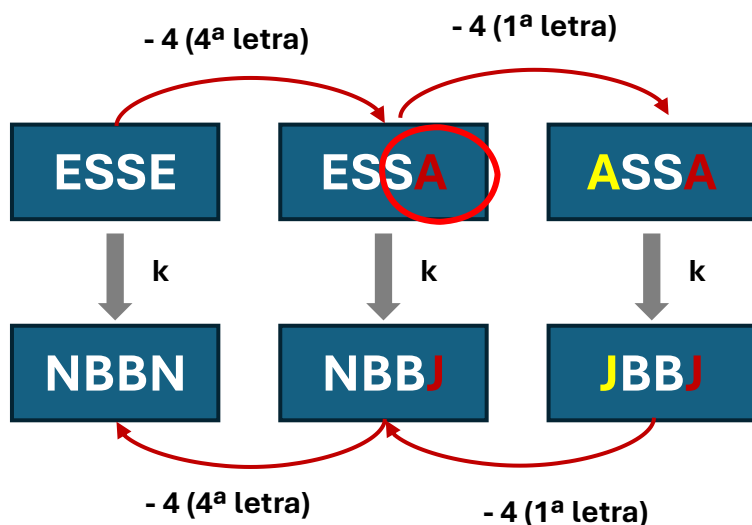




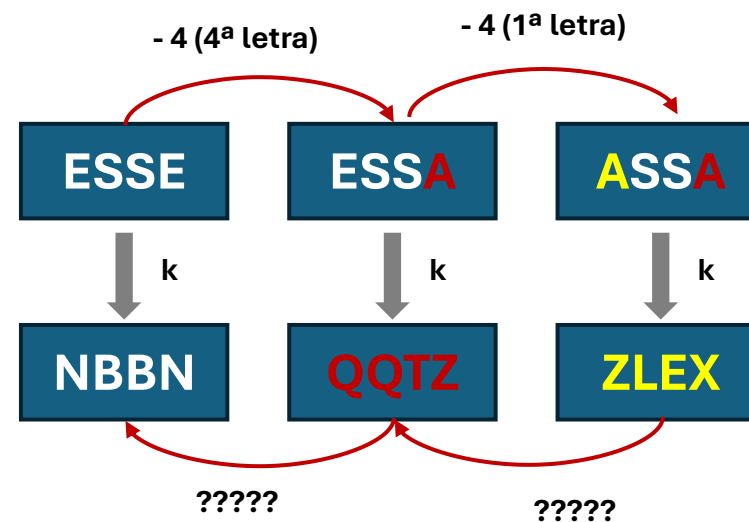
# Difusão vs. Confusão

**Princípios básicos**, definidos por Claude Shannon, para o projeto de cifras seguras.

- **Confusão**: relação entre a mensagem às claras, cifrada e a chave deve ter **alta complexidade**.



Cifra de César: baixa difusão



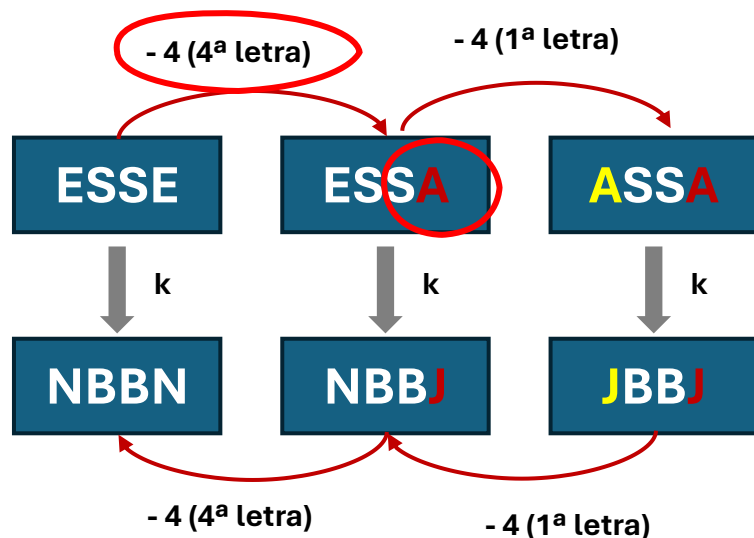
Cifras modernas: alta confusão



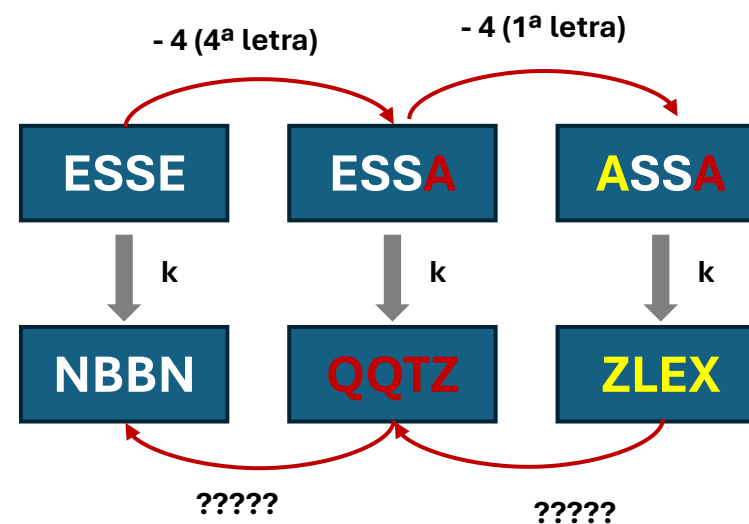
# Difusão vs. Confusão

**Princípios básicos**, definidos por Claude Shannon, para o projeto de cifras seguras.

- **Confusão**: relação entre a mensagem às claras, cifrada e a chave deve ter **alta complexidade**.



Cifra de César: baixa difusão



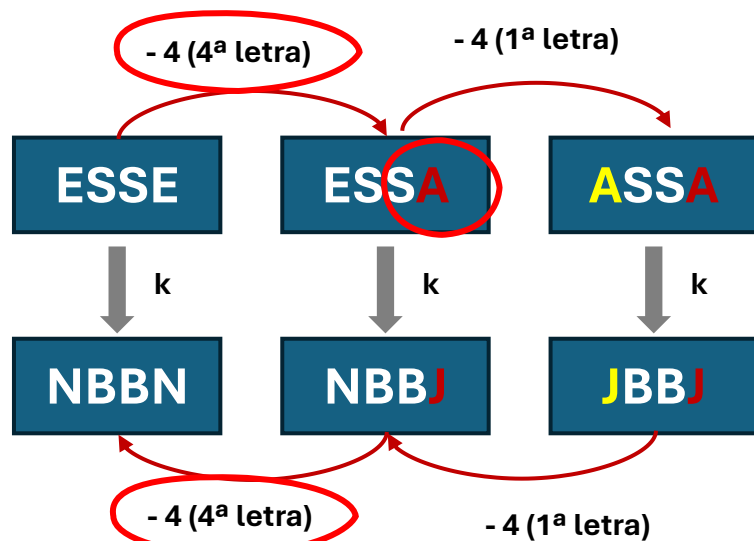
Cifras modernas: alta confusão



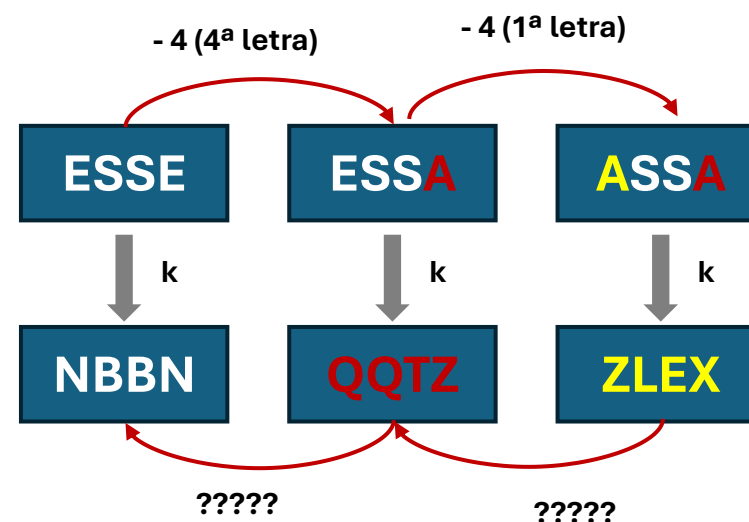
# Difusão vs. Confusão

**Princípios básicos**, definidos por Claude Shannon, para o projeto de cifras seguras.

- **Confusão**: relação entre a mensagem às claras, cifrada e a chave deve ter **alta complexidade**.



Cifra de César: baixa difusão



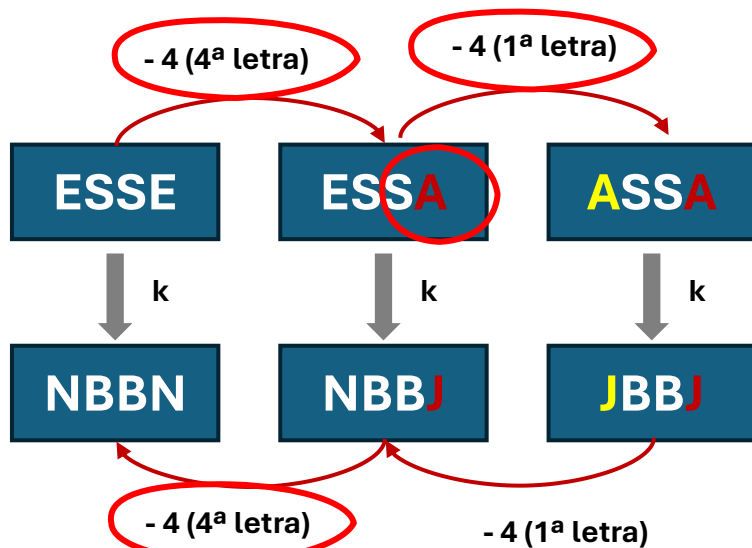
Cifras modernas: alta confusão



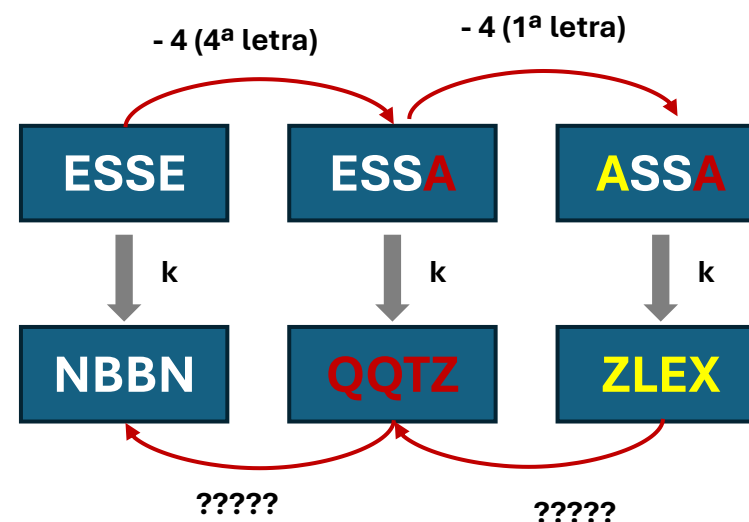
# Difusão vs. Confusão

**Princípios básicos**, definidos por Claude Shannon, para o projeto de cifras seguras.

- **Confusão**: relação entre a mensagem às claras, cifrada e a chave deve ter **alta complexidade**.



Cifra de César: baixa difusão



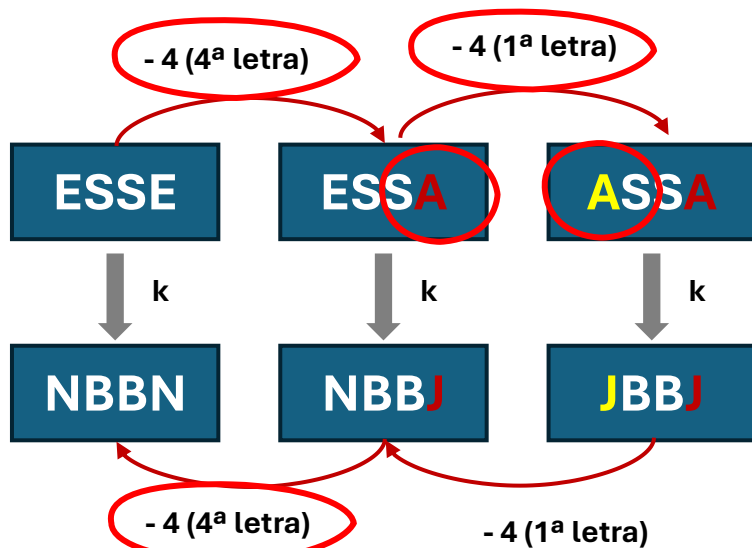
Cifras modernas: alta confusão



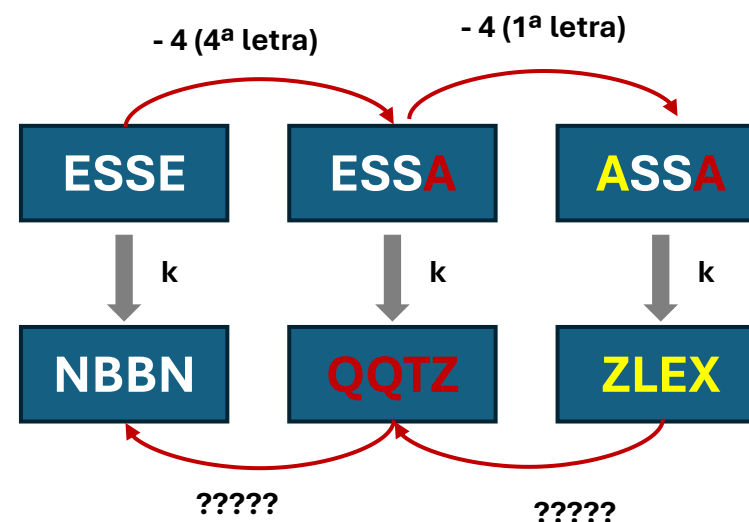
# Difusão vs. Confusão

**Princípios básicos**, definidos por Claude Shannon, para o projeto de cifras seguras.

- **Confusão**: relação entre a mensagem às claras, cifrada e a chave deve ter **alta complexidade**.



Cifra de César: baixa difusão



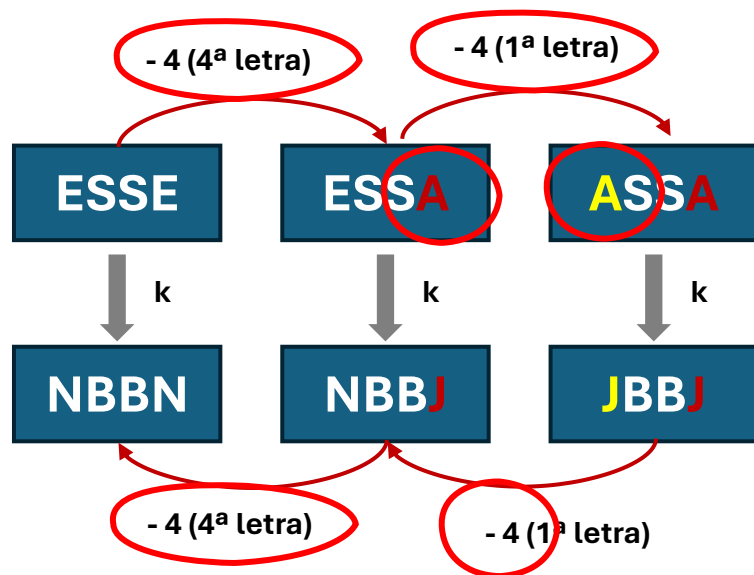
Cifras modernas: alta confusão



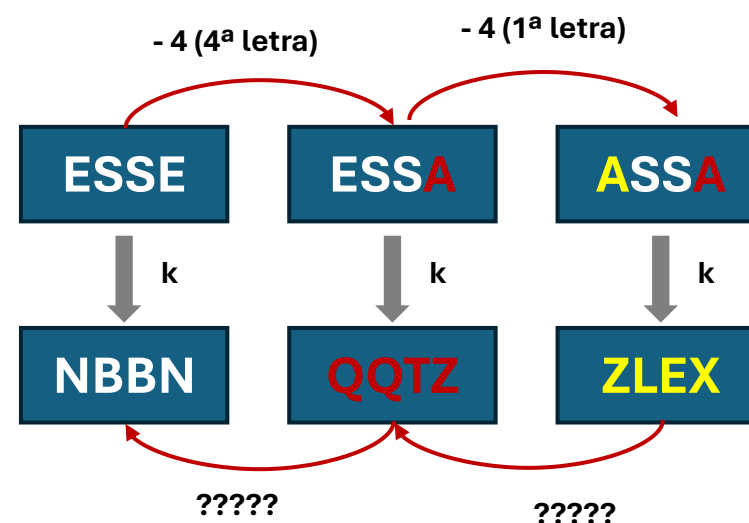
# Difusão vs. Confusão

**Princípios básicos**, definidos por Claude Shannon, para o projeto de cifras seguras.

- **Confusão**: relação entre a mensagem às claras, cifrada e a chave deve ter **alta complexidade**.



Cifra de César: baixa difusão



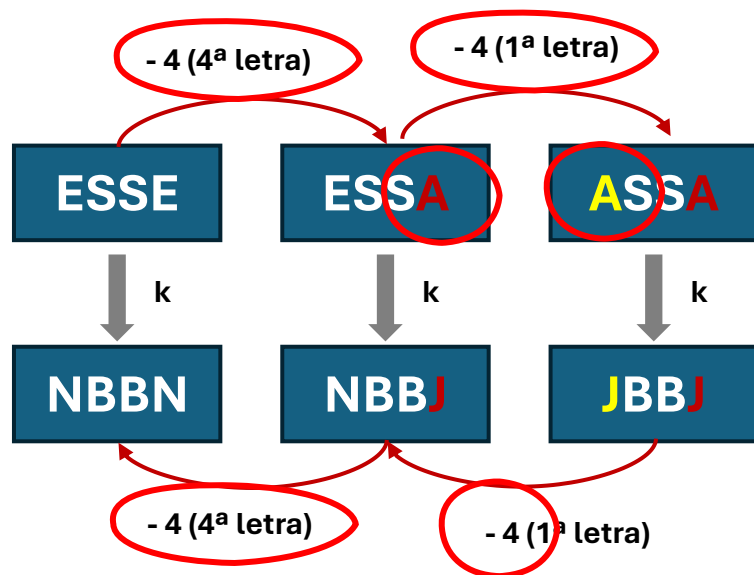
Cifras modernas: alta confusão



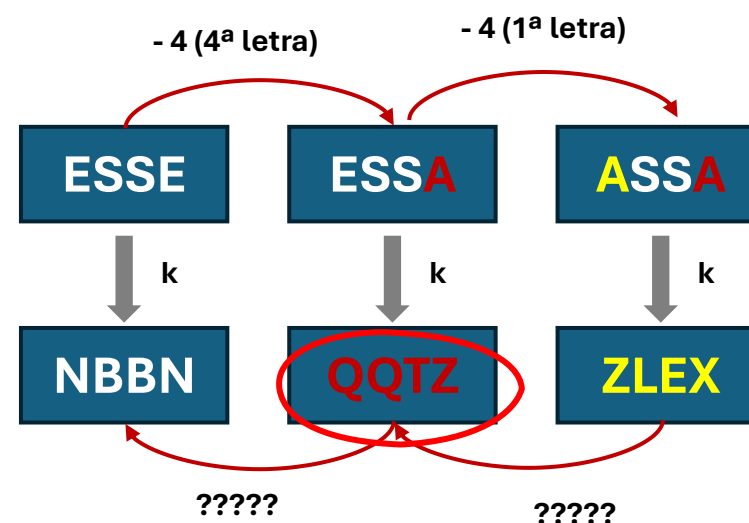
# Difusão vs. Confusão

**Princípios básicos**, definidos por Claude Shannon, para o projeto de cifras seguras.

- **Confusão**: relação entre a mensagem às claras, cifrada e a chave deve ter **alta complexidade**.



Cifra de César: baixa difusão



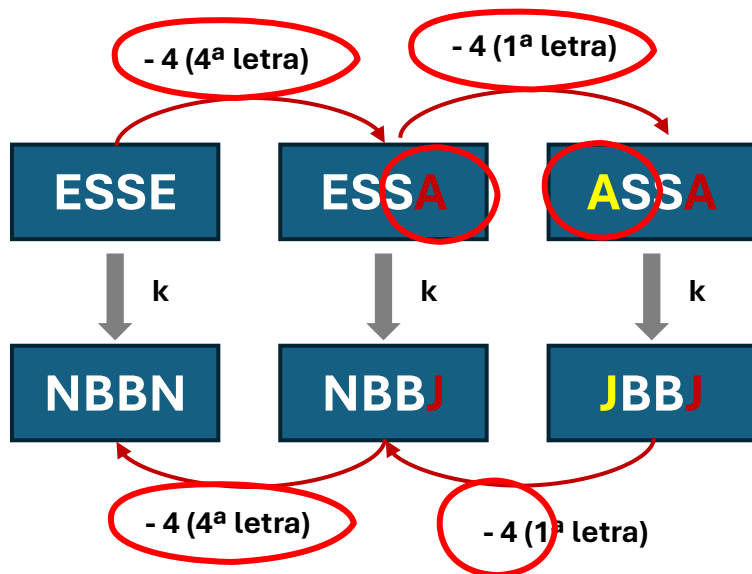
Cifras modernas: alta confusão



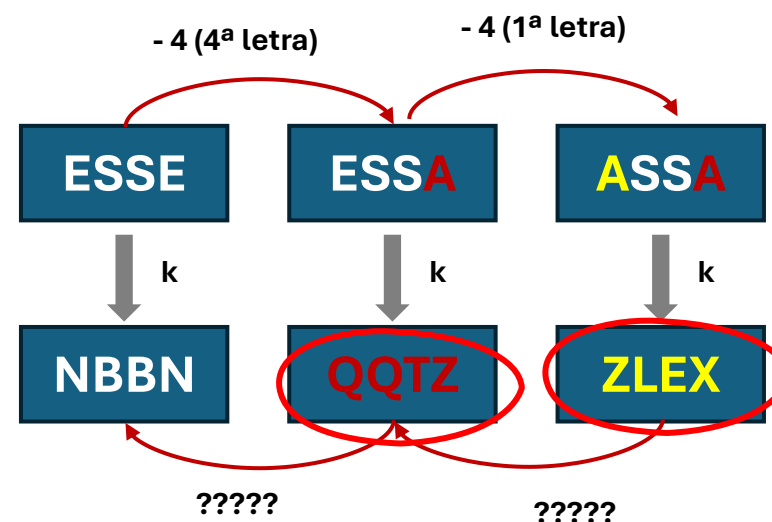
# Difusão vs. Confusão

**Princípios básicos**, definidos por Claude Shannon, para o projeto de cifras seguras.

- **Confusão**: relação entre a mensagem às claras, cifrada e a chave deve ter **alta complexidade**.



Cifra de César: baixa difusão



Cifras modernas: alta confusão

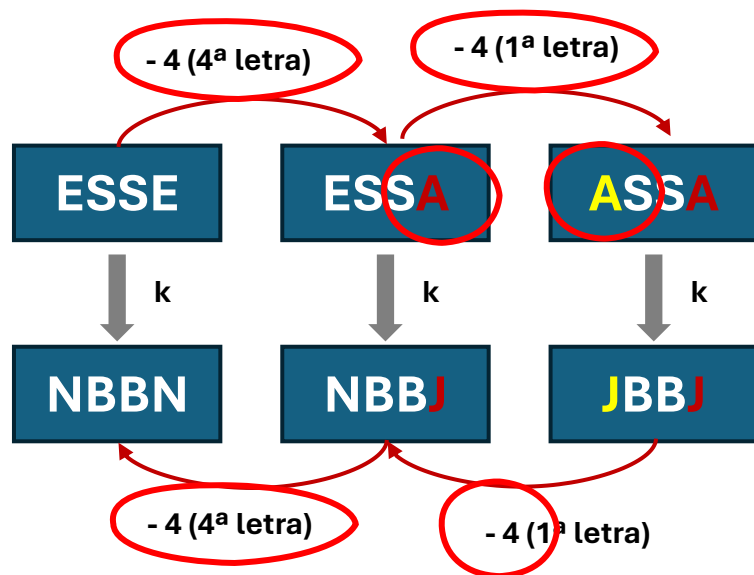




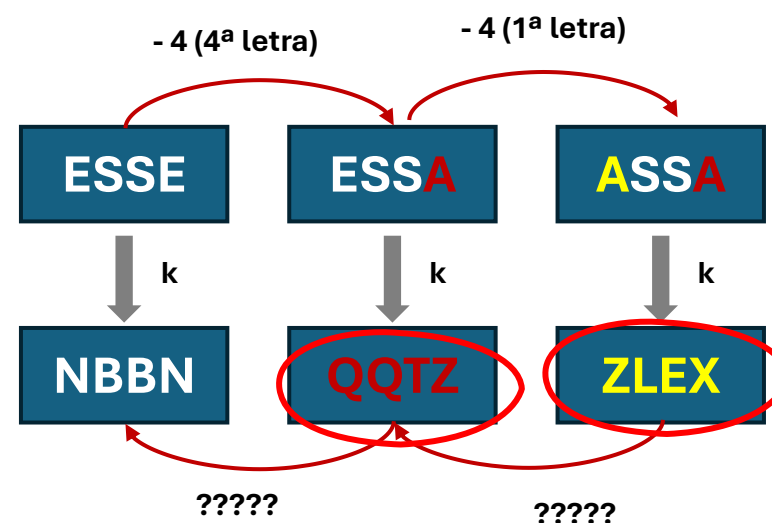
# Difusão vs. Confusão

**Princípios básicos**, definidos por Claude Shannon, para o projeto de cifras seguras.

- Não dá para ter uma relação clara entre mudanças das mensagens às claras com mudanças semelhantes a cifra moderna.



Cifra de César: baixa difusão



Cifras modernas: alta confusão



# Difusão vs. Confusão

- **“Efeitos de avalanche”**: pequenas mudanças levam a grandes impactos.
- **Cifras modernas** conseguem isso aplicando **operações simples de forma iterativa**, o que garante a difusão e confusão.

## Exemplo: AES

- Opera em mensagens de 128 bits (“bloco”);
- Rodadas: 10, 12 ou 14 para chaves de 128, 192 ou 256 bits;
- 4 operações por rodada: **ByteSub, ShiftRows, MixColumns e AddRoundKey**

# AES (visão geral)

**ByteSub:** substituição de bytes com tabela fixa (“S-Box”), independente da chave.

8bits

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

128 bits

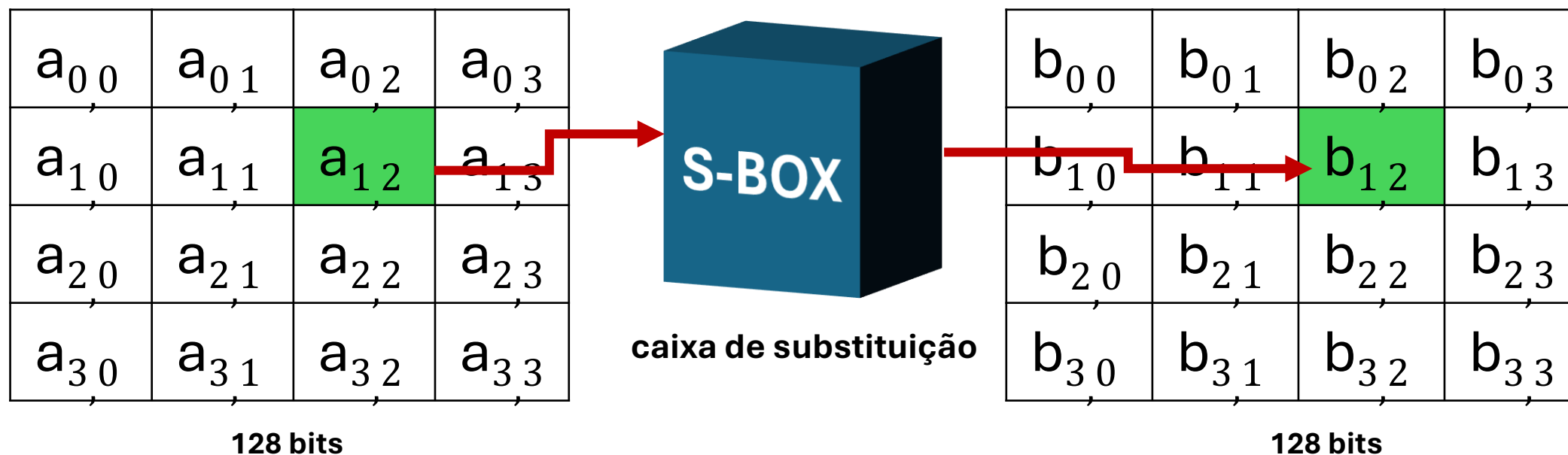


$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$

128 bits

# AES (visão geral)

**ByteSub:** substituição de bytes com tabela fixa (“S-Box”), independente da chave.

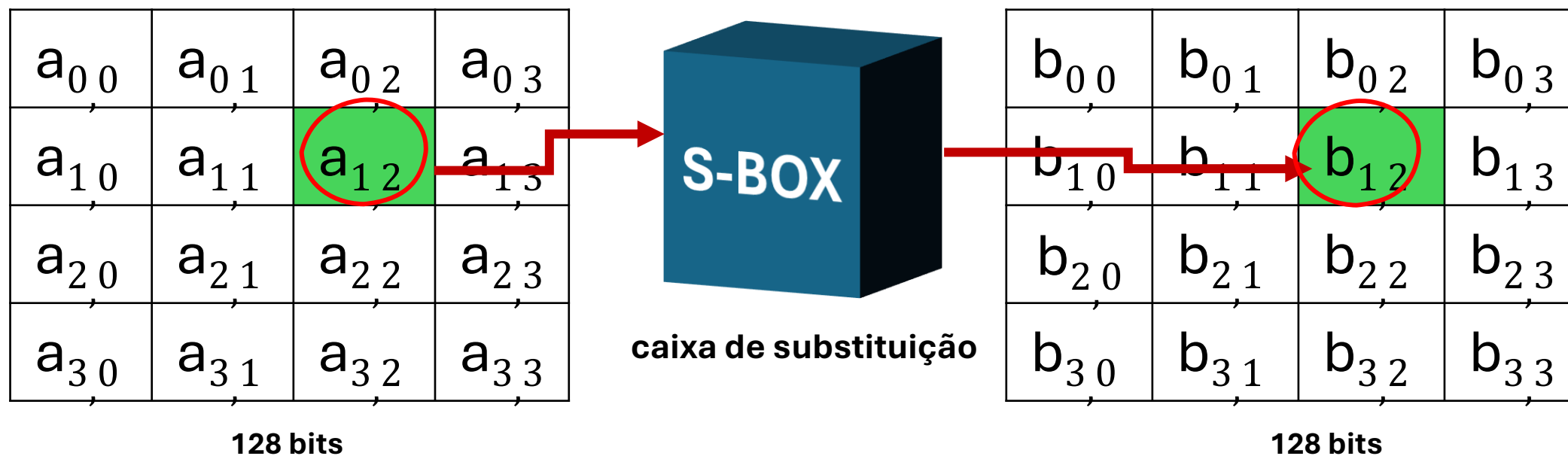


## Operações:

- Pega um bit e passa pela caixa de substituição e transforma um 1 em 17, 19 em 54, 4 em 98, entre outros;
- Tabela é pública e de fácil acesso;
- Documentação: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>

# AES (visão geral)

**ByteSub:** substituição de bytes com tabela fixa (“S-Box”), independente da chave.



## Operações:

- Pega um bit e passa pela caixa de substituição e transforma um 1 em 17, 19 em 54, 4 em 98, entre outros;
- Tabela é pública e de fácil acesso;
- Documentação: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>

# AES (visão geral)

**ShiftRows:** troca a posição de alguns bytes, rotacionando linhas (deslocamento é fixo) e não há tabela

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

128 bits

deslocamento

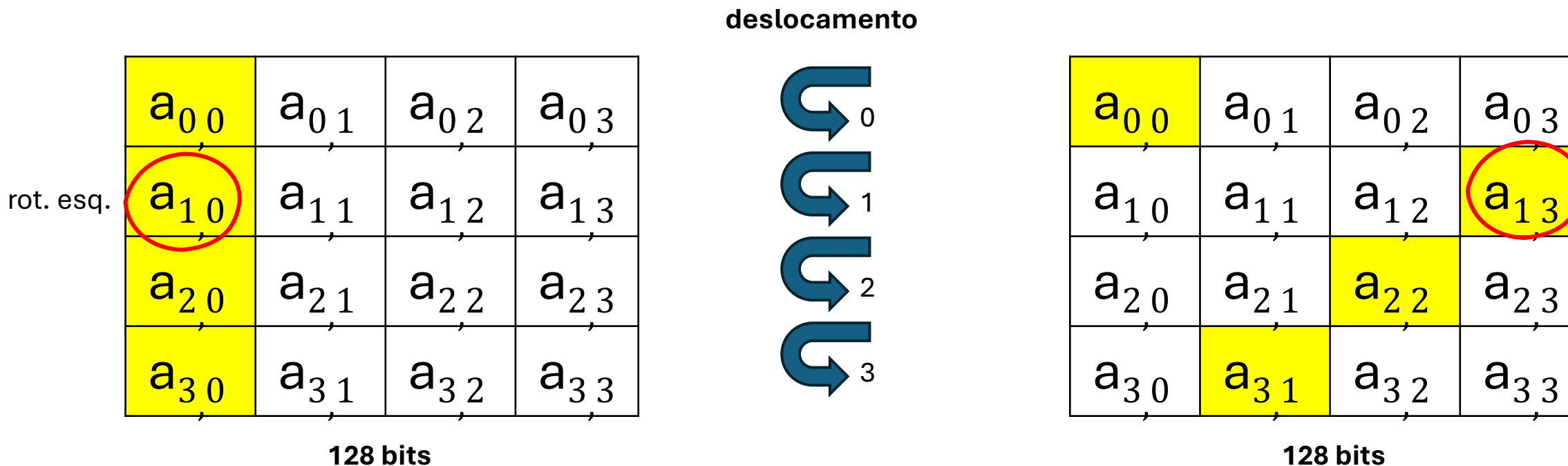


$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

128 bits

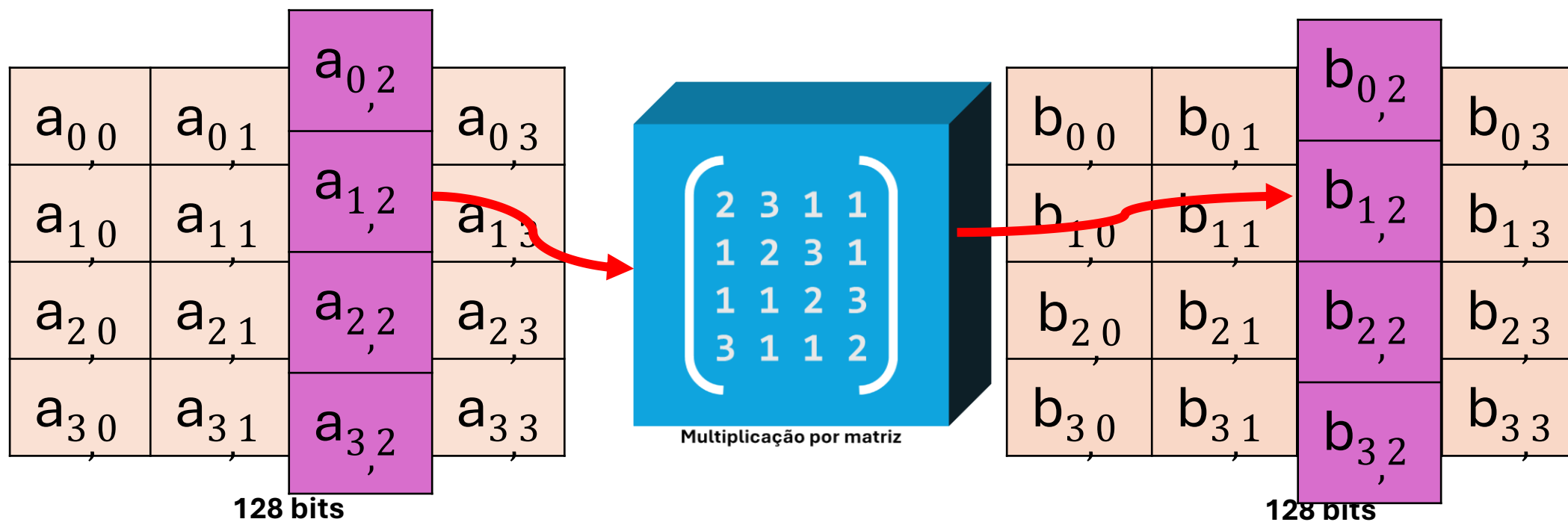
# AES (visão geral)

**ShiftRows:** troca a posição de alguns bytes, rotacionando linhas (deslocamento é fixo) e não há tabela



# AES (visão geral)

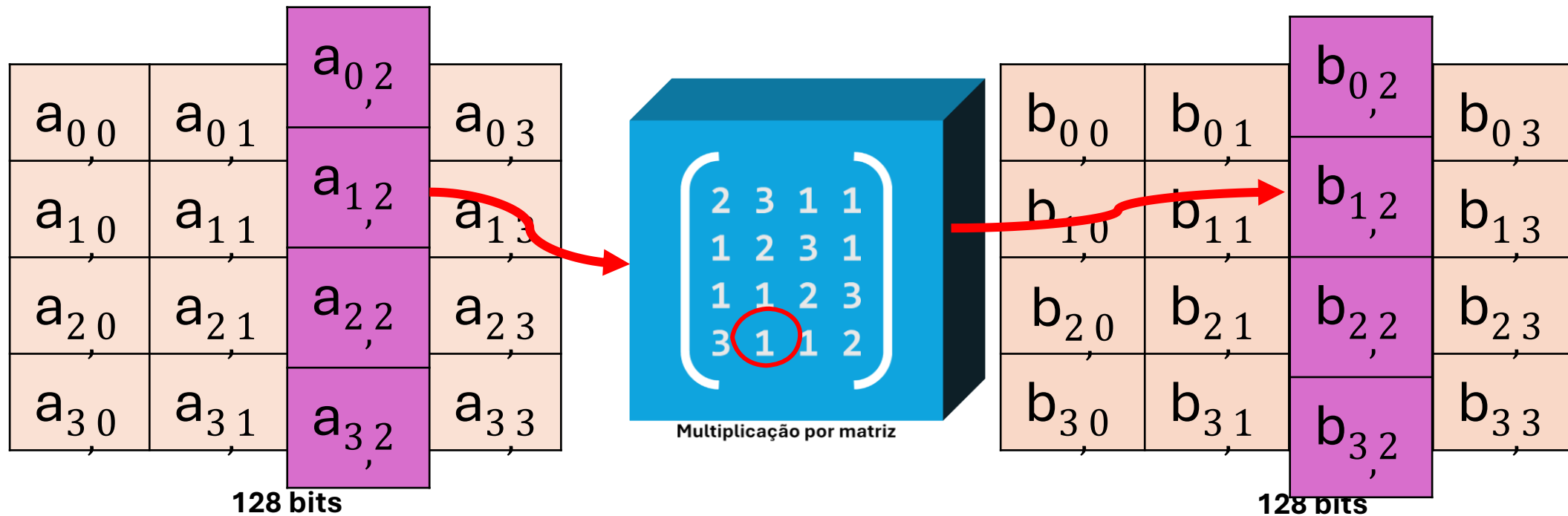
**MixColumns:** multiplicação por matriz, coluna a coluna.





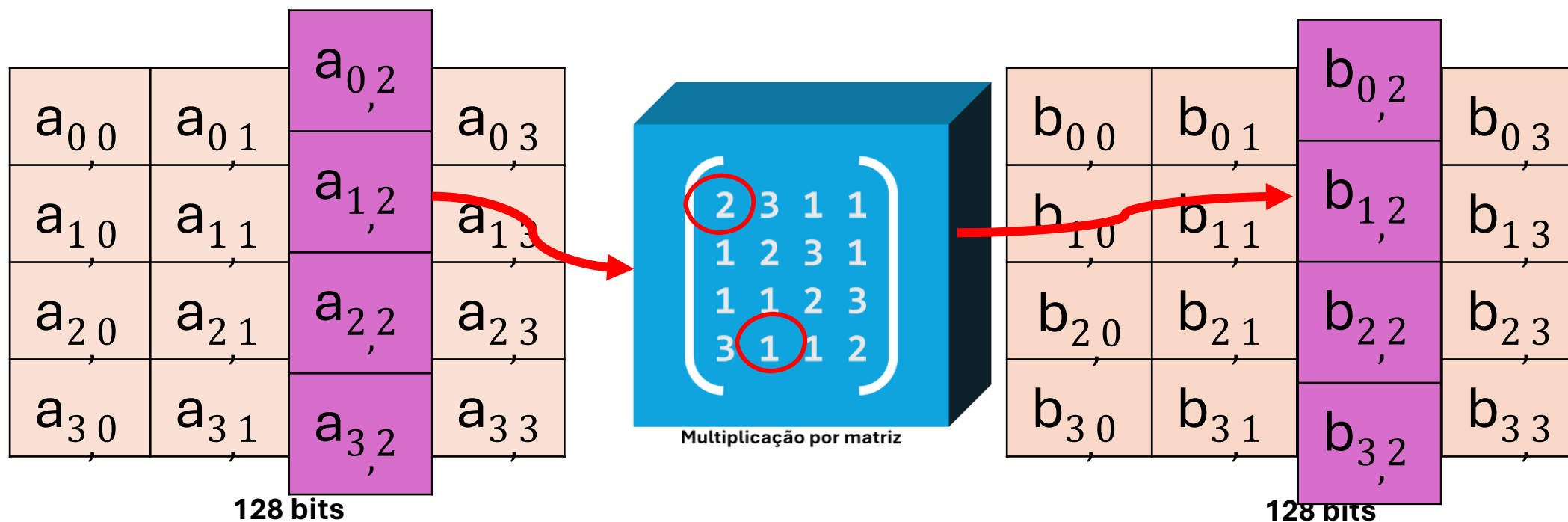
# AES (visão geral)

**MixColumns:** multiplicação por matriz, coluna a coluna.



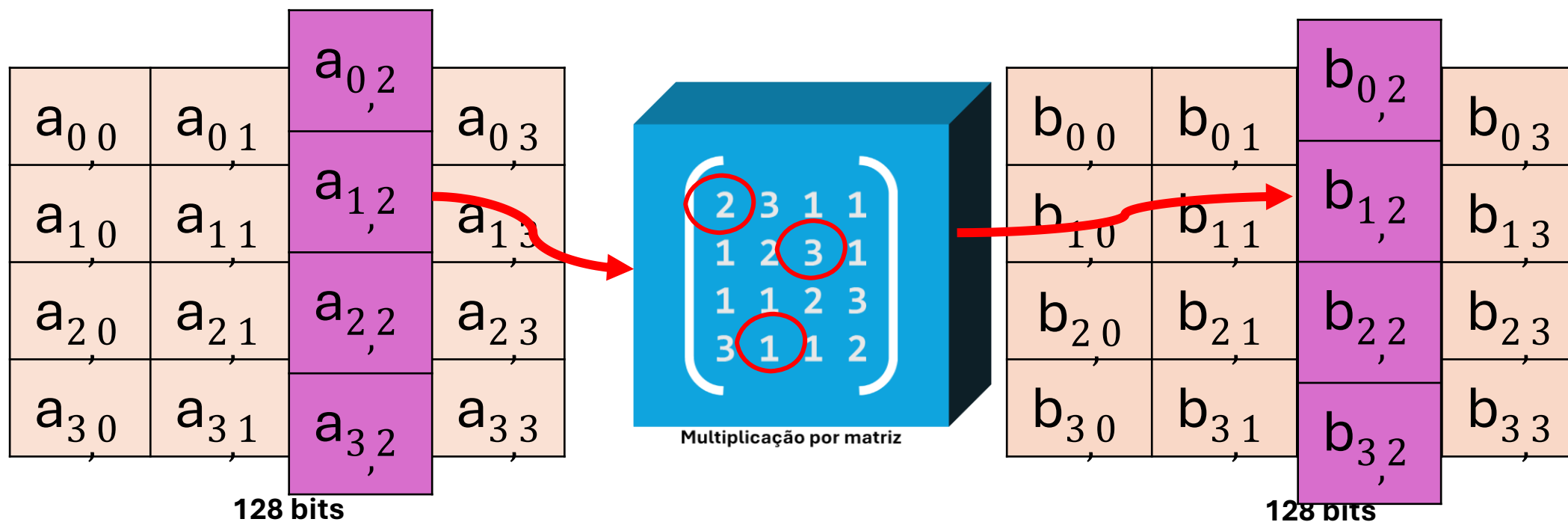
# AES (visão geral)

**MixColumns:** multiplicação por matriz, coluna a coluna.



# AES (visão geral)

**MixColumns:** multiplicação por matriz, coluna a coluna.



# AES (visão geral)

## AddRoundKey: aplicação da chave

- Operação de “ou-exclusivo”

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

 $\oplus$ 

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$

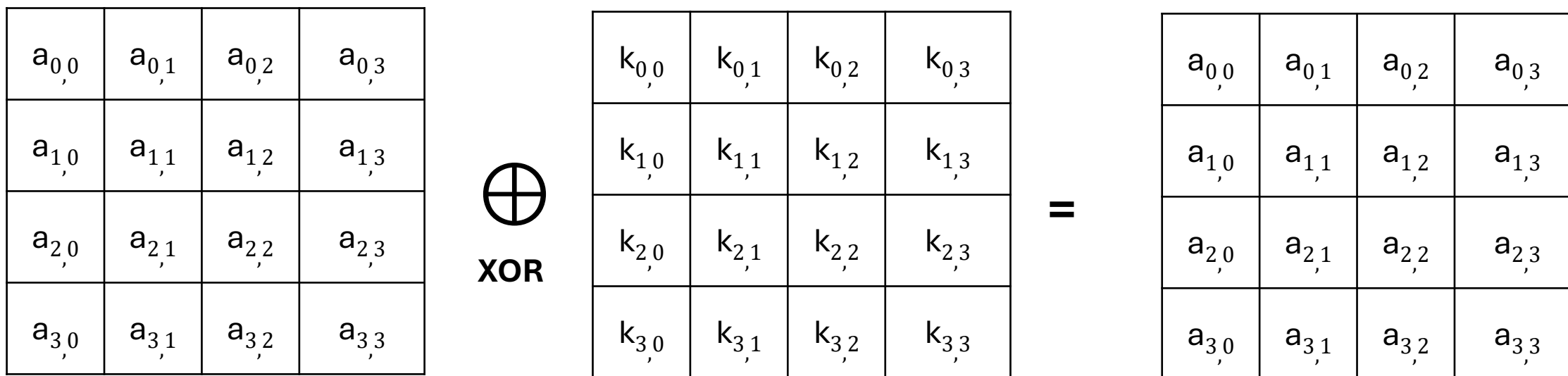
 $=$ 

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

# AES (visão geral)

## AddRoundKey: aplicação da chave

- Operação de “ou-exclusivo”

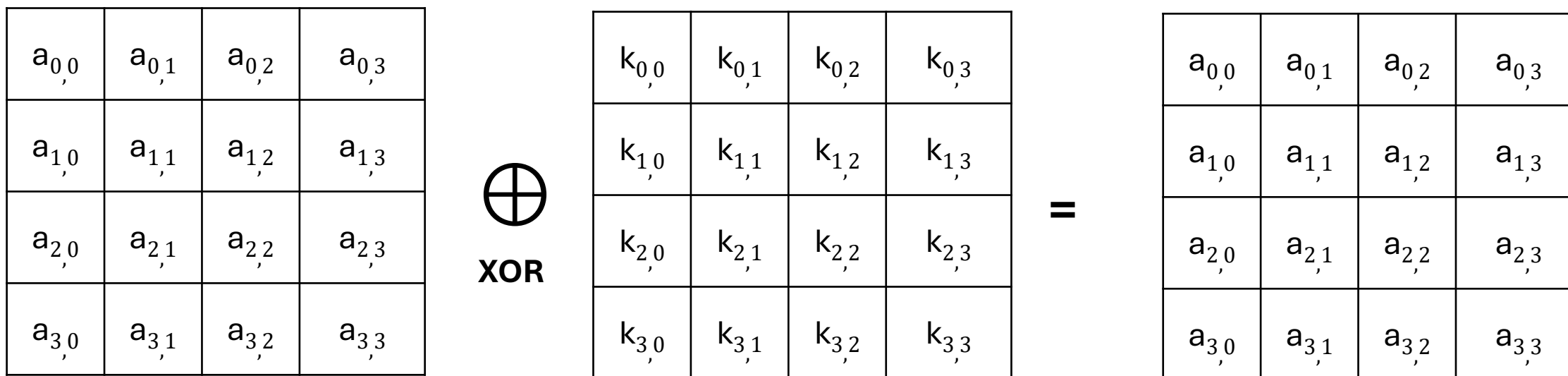


Usa a chave como máscaras  
para cada um byte

# AES (visão geral)

## AddRoundKey: aplicação da chave

- Operação de “ou-exclusivo”



**Detalhes: Cap. 2 – Técnicas básicas de encriptação.**

# Modo de operação

- Cifras de bloco apenas operam sobre mensagens de tamanho fixo (no AES: 128 bits).
- **Modo de operação:** permite cifração de **mensagens com tamanho diferente do bloco**.
- Alguns exemplos:
  - ECB, CBC, CFB, OFB, CTR (confidencialidade);
  - LRW, XEX, EME (cifração setorial para disco);
  - OCB, CCM, EAX, GCM (confidencialidade, integridade e também autenticidade)

# Modo de operação

- Cifras de bloco apenas operam sobre mensagens de tamanho fixo (no AES: 128 bits).
- **Modo de operação:** permite cifração de mensagens com tamanho diferente do bloco.
- Alguns exemplos:
  - ECB, CBC, CFB, OFB, CTR (confidencialidade);
  - LRW, XEX, EME (cifração setorial para disco);
  - OCB, CCM, EAX, GCM (confidencialidade, integridade e também autenticidade)



# Modo de operação

- Cifras de bloco apenas operam sobre mensagens de tamanho fixo (no AES: 128 bits).
- **Modo de operação:** permite cifração de mensagens com tamanho diferente do bloco.
  - Basicamente, adiciona alguns bits extras nas mensagens com menos de 128 bits.
- Alguns exemplos:
  - ECB, CBC, CFB, OFB, CTR (confidencialidade);
  - LRW, XEX, EME (cifração setorial para disco);
  - OCB, CCM, EAX, GCM (confidencialidade, integridade e também autenticidade)

# Modo de operação

**Quadro 6.1** Modos de operação de cifra de bloco.

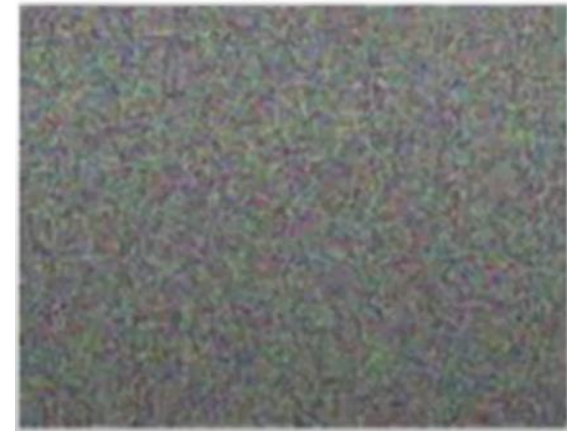
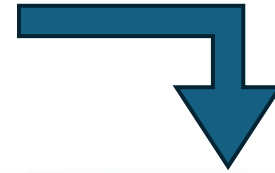
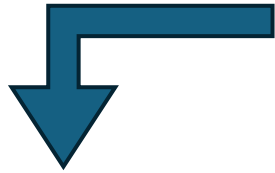
Modo	Descrição	Aplicação típica
Electronic codebook (ECB)	Cada bloco de bits de texto claro é codificado independentemente usando a mesma chave.	<ul style="list-style-type: none"><li>■ Transmissão segura de valores isolados (por exemplo, uma chave de encriptação)</li></ul>
Cipher block chaining (CBC)	A entrada do algoritmo de encriptação é o XOR dos próximos 64 bits de texto claro e os 64 bits anteriores de texto cifrado.	<ul style="list-style-type: none"><li>■ Transmissão de uso geral orientada a bloco</li><li>■ Autenticação</li></ul>
Cipher feedback (CFB)	A entrada é processada s bits de cada vez. O texto cifrado anterior é usado como entrada para o algoritmo de encriptação a fim de produzir saída pseudoaleatória, que é aplicada a um XOR com o texto claro para criar a próxima unidade de texto cifrado.	<ul style="list-style-type: none"><li>■ Transmissão de uso geral orientada a fluxo</li><li>■ Autenticação</li></ul>
Output feedback (OFB)	Semelhante ao CFB, exceto que a entrada do algoritmo de encriptação é a saída DES anterior, e são usados blocos completos.	<ul style="list-style-type: none"><li>■ Transmissão orientada a fluxo por canal com ruído (por exemplo, comunicação por satélite)</li></ul>
Counter (CTR)	Cada bloco de texto claro é aplicado a um XOR com um contador encriptado. O contador é incrementado para cada bloco subsequente.	<ul style="list-style-type: none"><li>■ Transmissão orientada a bloco de uso geral</li><li>■ Útil para requisitos de alta velocidade</li></ul>

**Detalhes: Cap. 6 – Operação de cifra de bloco**

**STALLINGS, William.** *Criptografia e segurança de redes: princípios e práticas*. Tradução de Daniel Vieira; revisão técnica de Paulo Sérgio Licciardi Messeder Barreto e Rafael Misoczki. 6. ed. São Paulo: Pearson Education do Brasil, 2015. ISBN 978-85-430-1450-0.

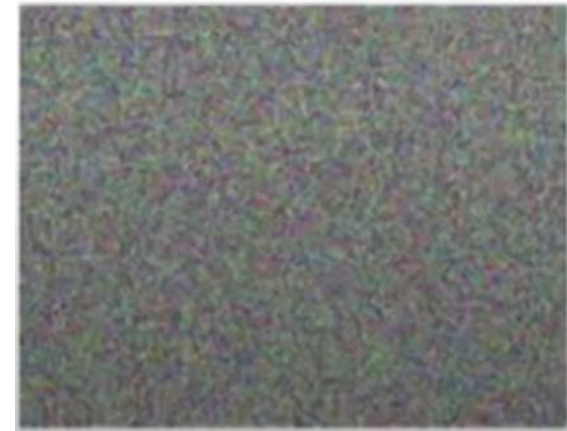
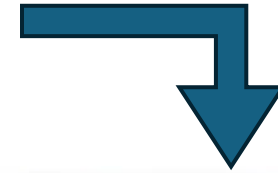
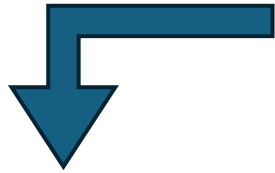
# Modo de operação: cuidados

É importante conhecer o modo operação para evitar problema de segurança, como o seguinte...



# Modo de operação: cuidados

É importante conhecer o modo operação para evitar problema de segurança, como o seguinte...



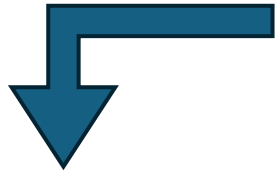
**Imagem cifrada usando:**

CTR

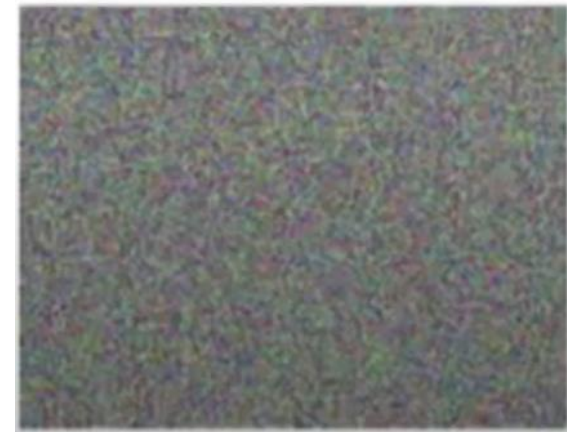
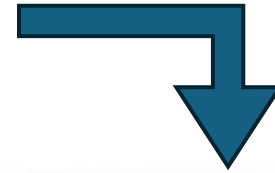
CBC

# Modo de operação: cuidados

É importante conhecer o modo operação para evitar problema de segurança, como o seguinte...



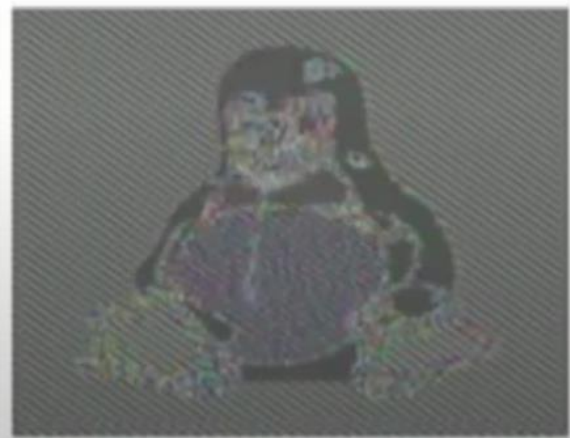
**Modo operando:**  
ECB



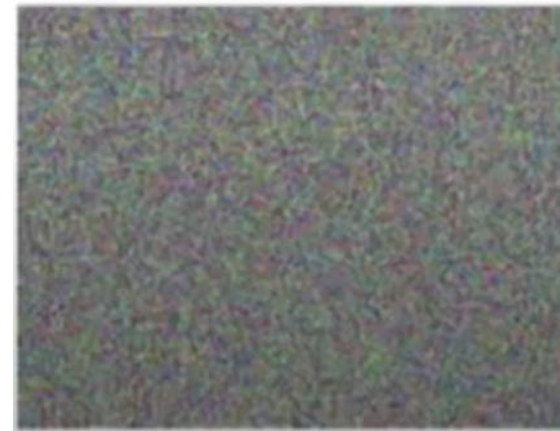
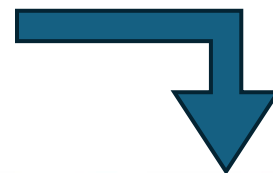
**Imagem cifrada usando:**  
CTR  
CBC

# Modo de operação: cuidados

É importante conhecer o modo operação para evitar problema de segurança, como o seguinte...



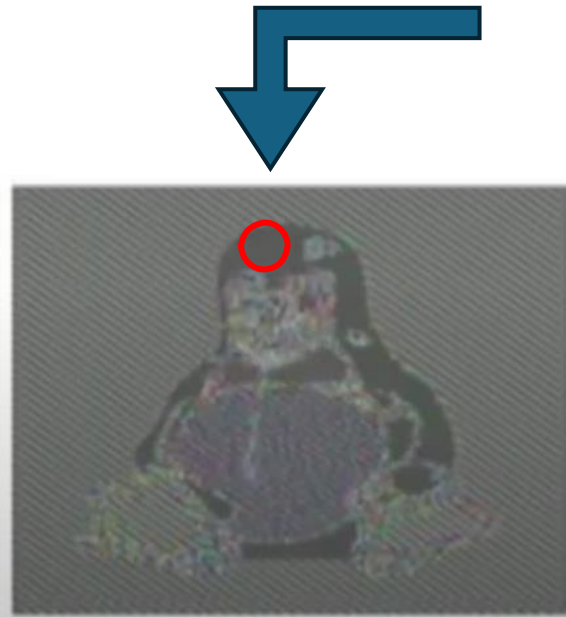
**Modo operando:**  
ECB



**Imagem cifrada usando:**  
CTR  
CBC

# Modo de operação: cuidados

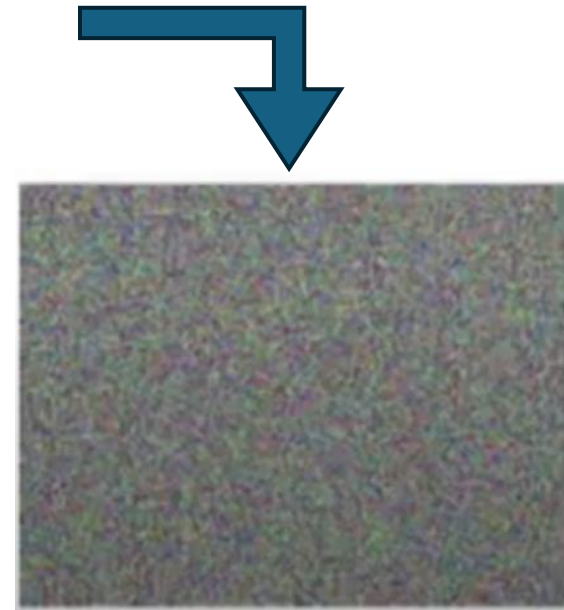
É importante conhecer o modo operação para evitar problema de segurança, como o seguinte...



**Modo operando:**

ECB

- Ele não protege tão bem as várias mensagens. O problema é que blocos iguais de entrada levam blocos iguais de saída. Pixels não alteram tanto, assim permite ver silhueta.



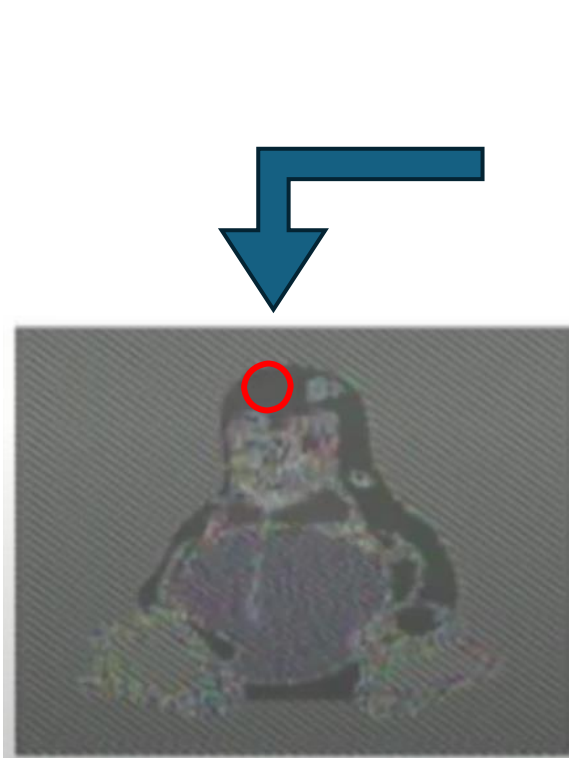
**Imagem cifrada usando:**

CTR

CBC

# Modo de operação: cuidados

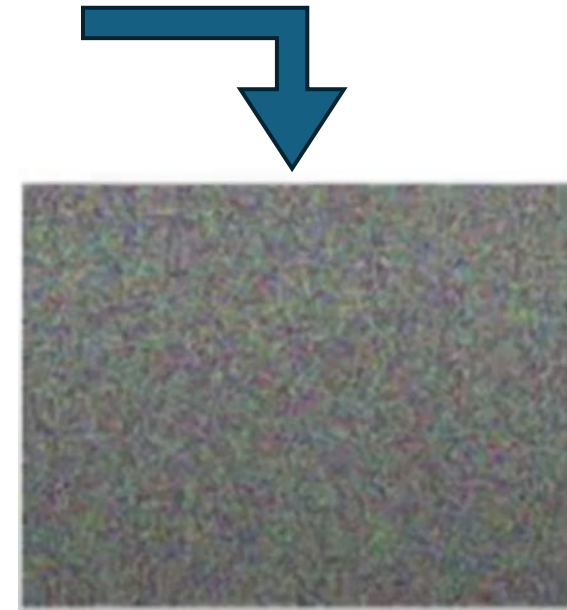
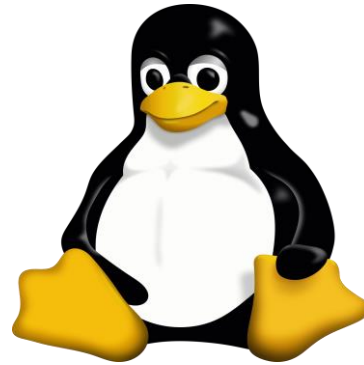
É importante conhecer o modo operação para evitar problema de segurança, como o seguinte...



**Modo operando:**

ECB

- Ele não protege tão bem as várias mensagens. O problema é que blocos iguais de entrada levam blocos iguais de saída. Pixels não alteram tanto, assim permite ver silhueta.



**Imagem cifrada usando:**

CTR

CBC



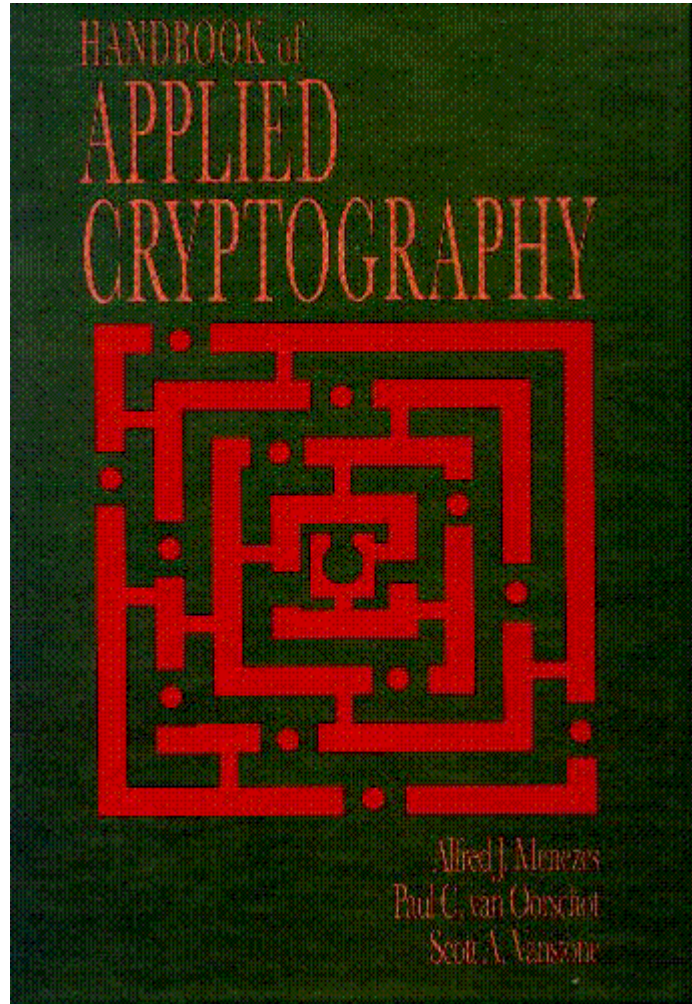
# Considerações práticas

- Há pacotes de algoritmos para as mais diversas linguagens de programação.
  - Java:
    - Java.Security
    - BouncyCastle
    - Java Cryptography Architecture (JCA) / Java Cryptography Extension (JCE);
    - Apache Shiro;
    - Jasypt (Java Simplified Encryption);
  - Python:
    - PyCryptodome;
    - Cryptography;
    - M2Crypto;
  - CyberChef: <https://gchq.github.io/CyberChef/>

# Considerações práticas

- Uso de cifras também em **várias aplicações**:
  - Cifração de disco: TrueCrypt, Veracrypt, CipherShed, BitLocker e afins;
  - Servidores Web: HTTPS (usa TLS);
  - Envio de e-mails seguros: extensões S/MIME;
  - Conexão remota: aplicativos de SSH;
  - Roteamento seguro: túnel IPSec, rede Tor;
  - Proteção de rede sem fio (WiFi): WPA2;

# Considerações práticas



MENEZES, Alfred J.; VAN OORSCHOT, Paul C.; VANSTONE, Scott A. *Handbook of applied cryptography*. 1. ed. Boca Raton: CRC Press, 2001.

Link: <https://cacr.uwaterloo.ca/hac/>

# Dúvidas?



# Referências Bibliográficas

SÊMOLA, Marcos. *Gestão da segurança da informação: uma visão executiva*. 2. ed., 8. tiragem. Rio de Janeiro: [s.n.], 2018.

SILVA, Pedro Tavares; CARVALHO, Hugo; TORRES, Catarina Botelho. *Segurança dos sistemas de informação: gestão estratégica da segurança empresarial*. 1. ed. Lisboa; V. N. Famalicão: Centro Atlântico, 2003. ISBN 972-8426-66-6.

STALLINGS, William; BROWN, Lawrie. *Segurança de computadores: princípios e práticas*. 2. ed. Tradução Arlete Simille Marques. Rio de Janeiro: Elsevier, 2014. ISBN 978-85-352-6449-4.

STALLINGS, William. *Criptografia e segurança de redes: princípios e práticas*. Tradução de Daniel Vieira; revisão técnica de Paulo Sérgio Licciardi Messeder Barreto e Rafael Misoczki. 6. ed. São Paulo: Pearson Education do Brasil, 2015. ISBN 978-85-430-1450-0.