




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.

**Sepejampam bempem vinpindospos
aopaoespestrapanhopo munpundopo
dospos
cópódipigospos epe daspas
cipifraspas!**



Enviar mensagens secretas é uma tarefa muito antiga.

O homem sentiu, desde muito cedo, a necessidade de guardar informações em segredo; ela nasceu com a diplomacia e com as transações militares.





Ou seja...

→ A Criptologia é a arte ou a ciência de escrever em cifra ou em código

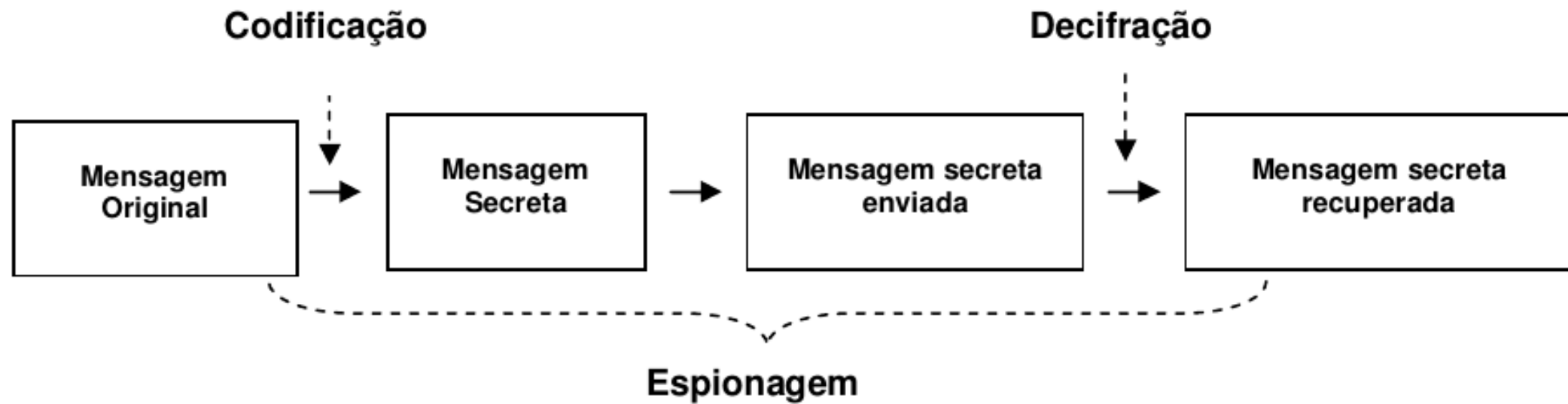



Ou seja...

→ comunicação eletrônica, a Criptografia deixou de ser unicamente segredo de estado, pois muitas atividades essenciais dependem do sigilo na troca de mensagens, principalmente aquelas que envolvem transações financeiras e uso seguro da Internet.

A photograph of a server room with blue ambient lighting. Several server racks are visible, with some doors open, revealing internal components. The room has a high ceiling with exposed metal beams and cables.

**Você consegue identificar um serviço
que necessita de criptografia?**





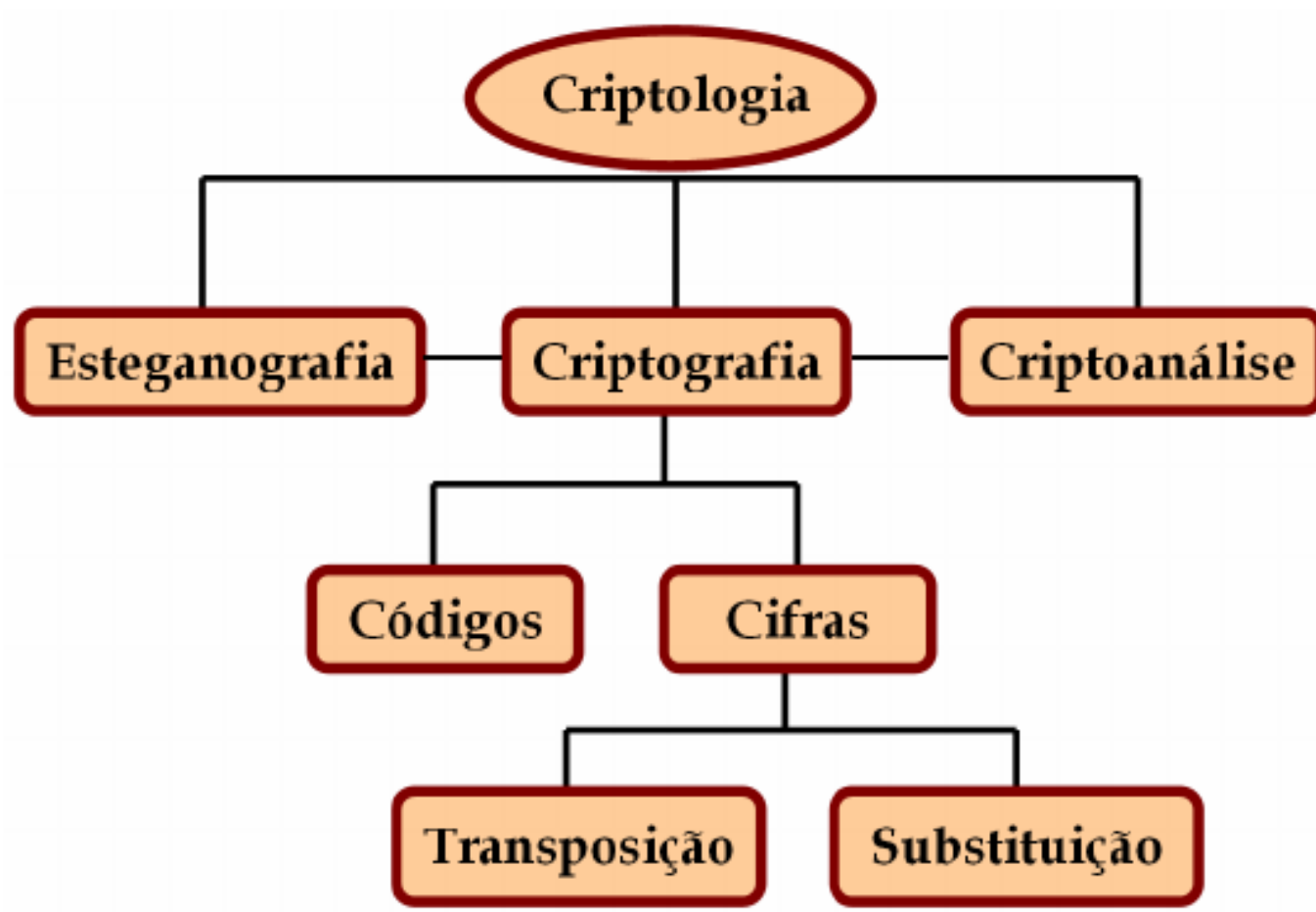
→ criptologia: ciência que se ocupa das ocultações de informações e da **quebra das informações ocultadas**.

→ Podemos esconder as informações de duas maneiras:

- Ocultando a existência da mensagem (esteganografia)

- Ocultando o significado do conteúdo da mensagem (criptografia)

→ criptologia



Áreas da Criptologia

→ Esteganografia

→ É bastante utilizada na área de segurança monetária, na autenticação de documentos, em imagens e nas gravações em geral (música, filmes, etc).

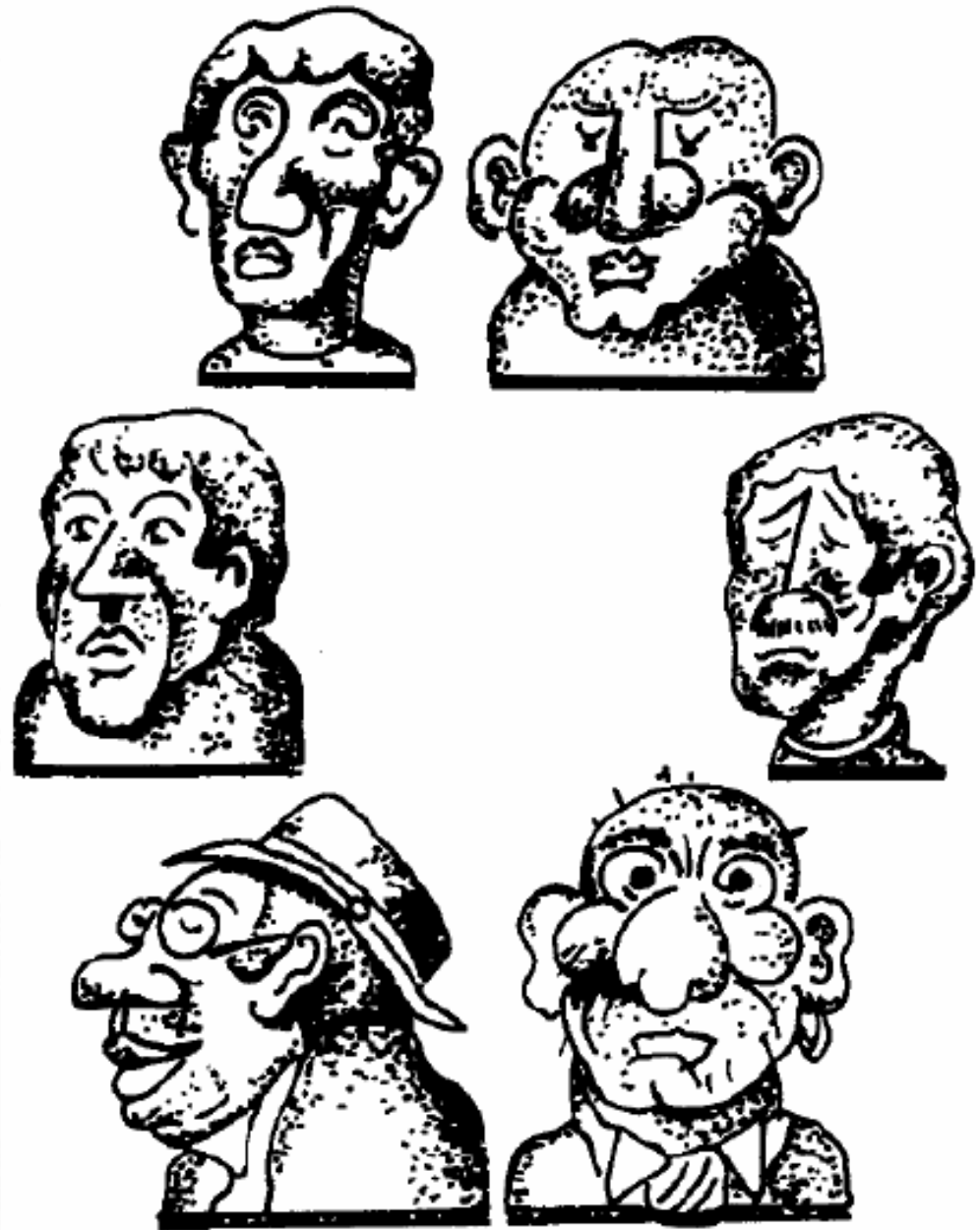


A marca d'água (na figura, a bandeira nacional) é um recurso esteganográfico presente nas notas de dinheiro que ajuda a combater a falsificação.

→ Esteganografia

Estas cabeças formam uma série, podendo ordenar-se da primeira à sexta segundo uma regra lógica.

Qual é essa regra?





→ Esteganografia

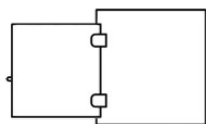
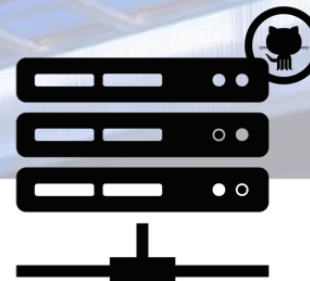
A esteganografia em imagens digitais visa inserir dados dentro de uma imagem, através da manipulação dos bits (um bit é a menor parcela de informação processada por um computador; um bit comporta uma informação binária que somente pode assumir os valores 0 ou 1), de forma que ninguém note a existência de dados nesta imagem.



→ Criptografia

Para codificarmos ou decodificarmos uma mensagem necessitamos de informações confidenciais denominadas **chave**.

A criptoanálise estuda formas de decodificar uma mensagem sem se conhecer, de antemão, a chave.



Private Key
~/.ssh/id_rsa



Public Key
~/.ssh/id_rsa.pub

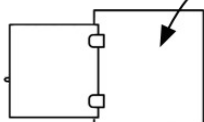


Public Key

1 - Client initiates SSH connection



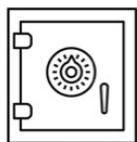
Private Key



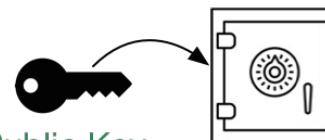
2 - Server sends random message



3 - Client **encrypts** message
with private key



4 - Client sends encrypted message



Public Key

5 - Server **decrypts** message
with public key



6 - If messages match, client is authenticated





→ Termos utilizados:

Codificar

Decodificar

Decifrar



→ Termos utilizados:

Codificar uma mensagem é transformá-la em um código secreto. O destinatário legal, usuário do código, decodifica, isto é, interpreta a mensagem recebida, que é um processo mais complexo do que o simples fato de codificar.

Enquanto, decifrar uma mensagem significa “quebrar” o código secreto quando este não é um usuário lícito do código.



- Nesse sentido, criptografar uma mensagem baseia-se na ideia de transformar uma mensagem em um determinado código para que apenas os seus usuários legais consigam interpretá-la.
- Precisamos estabelecer uma tabela de conversão!

→

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




→ Utilizando a tabela de conversão, faça a seguinte *pré-codificação* da seguinte frase:

A matematica e bela.

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.

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 chave original da Criptografia de César ($k = 3$) codificar a palavra CONGRUENCIA.

- 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

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