UFRJ - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 07 de Março de 2017

CRIPTO / GRAFIA

SECRETO / ESCRITA

ESCONDIDO

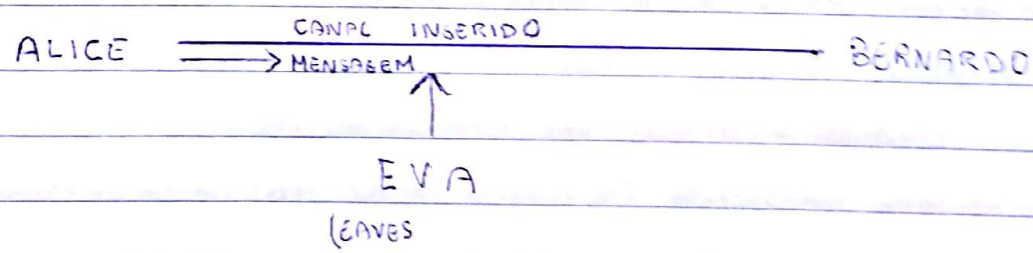
OCULTO

- OBJETIVO DA CRIPTOGRAFIA

-> Esconder o conteúdo original de uma mensagem

-> Codificar uma mensagem de forma que ela seja legível (e compreensível) apenas para seu remetente e destinatário

- MODELO PADRÃO



- CIFRA DE CÉSAR

↳ IMPERADOR ROMANO

-> Usava para se comunicar com os generais

-> Funcionamento:

-> Codifica a mensagem letra a letra

-> Uma letra é codificada como a letra que está K posições à frente no alfabeto.

/ /

- EXEMPLO:

M A T H E U S → MENSAGEM

↓ ↓ ↓ ↓ ↓ ↓ ↓

T H A O L B Z → MENSAGEM CODIFICADA

K=7 → Fruto de um acordo entre o remetente e o destinatário e tem que ser secreto

A informação necessária para codificar e decodificar mensagens é chamada de chave de criptografia. No caso da Cifra de César, a chave é o valor de K.

- CIFRA ENIGMA

→ Utilizada pelos militares alemães durante a 2ª Guerra Mundial para transmitir as ordens as tropas

→ Cifra feita pela máquina Enigma

→ Teclado (1 tecla por letra)

→ Painel de Lâmpadas (1 lâmpada por letra)

→ 3 rodas denteadas (26 dentes por roda)

→ A cada tecla apertada no teclado, uma lâmpada ascende

→ A letra da lâmpada que acende é a codificação da letra que foi apertada

→ A cada letra apertada, a 1ª roda gira uma posição

→ Quando a 1ª roda completa uma volta, a 2ª roda gira uma posição

→ Quando a 2ª roda completa uma volta, a 3ª roda gira uma posição

→ A codificação de uma letra depende, além da letra que foi apertada, da posição atual das 3 rodas

→ A cifra Enigma foi quebrada pelos britânicos com participação do matemático inglês Alan Turing.