

# OVERVIEW

## APLICAÇÕES DA CRIPTOGRAFIA

\* COMUNICAÇÃO SEGURA: • HTTPS, Bluetooth, GSM e 802.11i WPA2.

\* CRIPTOGRAFIA DE ARQUIVOS em disco: EFS e TrueCrypt.

\* PROTEÇÃO de conteúdo: CSS e AACS → Blu-Ray

\* AUTENTICAÇÃO DE USUÁRIOS → "Content Scrambling System" DVD

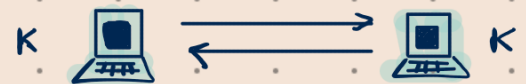
## I) COMUNICAÇÃO SEGURA:

HTTPS → HTTP  
SSL/TLS

2 etapas: 1. Handshake

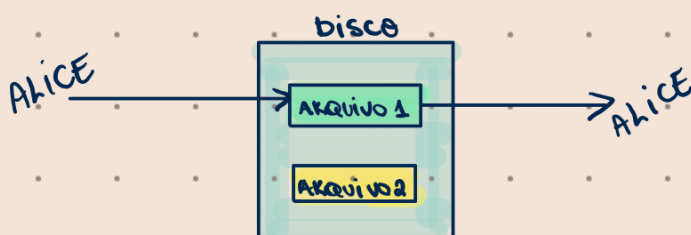
2. modo de registro

transmitem dados utilizando a chave secreta compartilhada



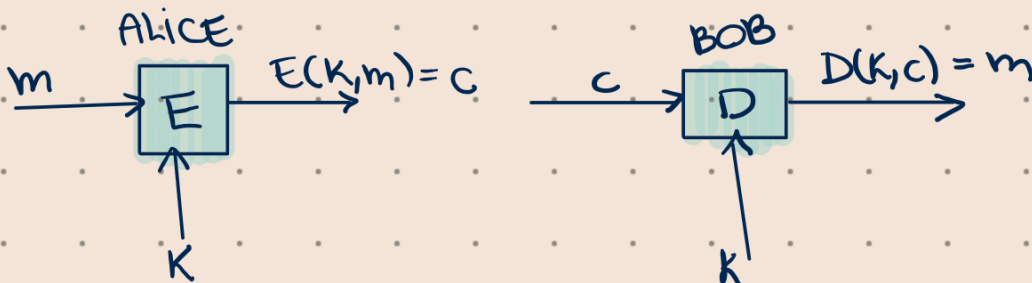
estabelecer uma chave secreta utilizando criptografia de chave pública

## II) CRIPTOGRAFIA de ARQUIVOS em disco:



é necessário garantir integridade (não pode ter adulteração do arquivo) e confidencialidade (não pode haver acesso de terceiros)

## CRIPTOGRAFIA Simétrica

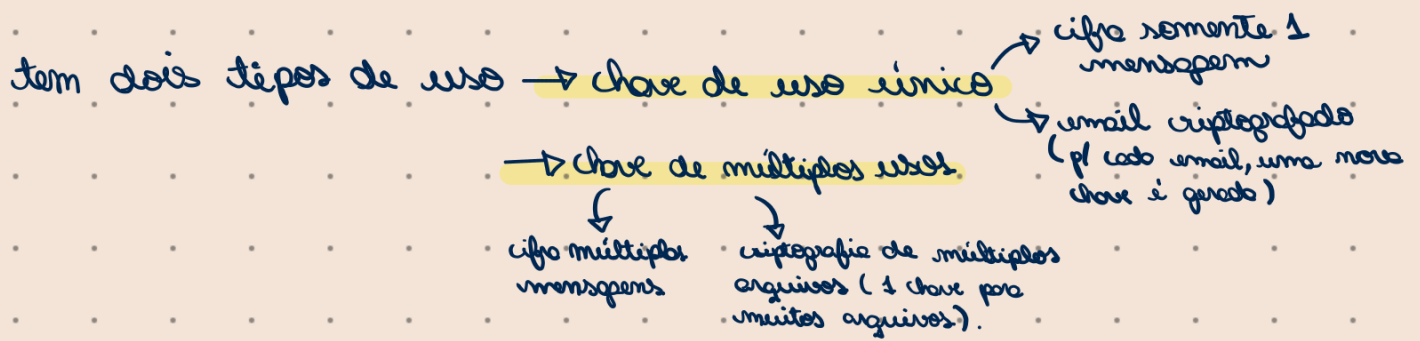


$E, D$ : cifrar e decifrar

$m, c$ : texto claro e texto cifrado

$K$ : chave secreta

algoritmos de criptografia são conhecidos, somente sua chave ( $K$ ) não.



## CRIPTOGRAFIA NÃO RESOLVE tudo!

- ↳ problemas de software.
- ↳ engenharia social (phishing)
- ↳ se não implementada corretamente
- ↳ não inventa! existem padrões funcionais.