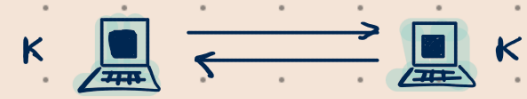
OVERVIEW

APLICAÇÕES DA CRIPTOGRAFIA

* COMUNICAÇÃO SEGURA: • HTTPS (WEB), Bluetooth, GSM e 802.11i WPA2 (WIRELESS, para Wi-Fi)
* CRIPTOGRAFIA DE ARQUIVOS em disco: EFS e TrueCrypt.
* PROTEÇÃO de conteúdo: CSS e AACS → Blu-Ray
* AUTENTICAÇÃO DE USUÁRIOS

CSS → DVD → "Content Scrambling System"

I) COMUNICAÇÃO SEGURA:

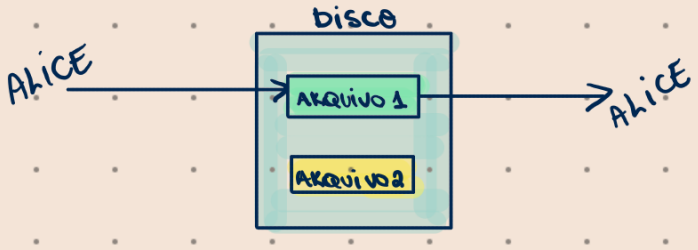


HTTPS → HTTP

SSL/TLS → 2 etapas: 1. Handshake (estabelecer uma chave secreta utilizando criptografia de chave pública)

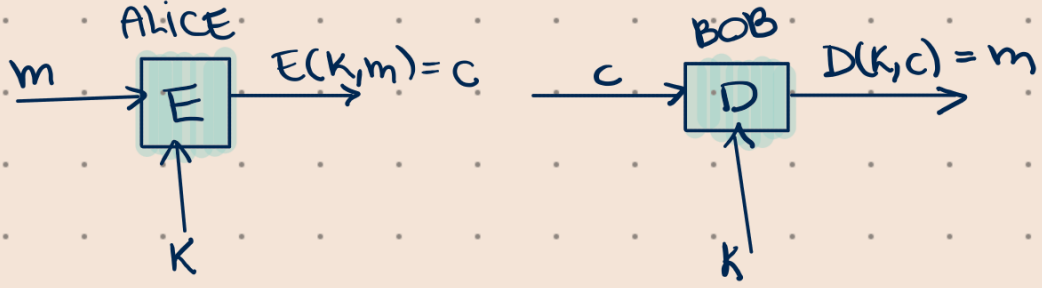
2. Modo de registro → transmitir dados utilizando a chave secreta compartilhada

II) CRIPTOGRAFIA de ARQUIVOS em disco:



é necessário garantir integridade (não pode ter adulteração do arquivo) e confidencialidade (não pode haver escuta 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.

tem dois tipos de uso → chave de uso único
- cifra somente 1 mensagem
- email criptografado (p/ cada email, uma nova chave é gerado)

→ chave de múltiplos usos
- cifra múltiplas mensagens
- criptografia de múltiplos arquivos (1 chave para muitos arquivos).

CRIPTOGRAFIA NÃO RESOLVE TUDO!

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