Tipos de cifragem em criptografia simétrica

Cifras de fluxo *(stream cipher)*
A cifragem é feita bit a bit (ou símbolo a símbolo).
Ex.: Substituição simples

Cifras de bloco *(block cipher)*
A cifragem é feita em blocos, cada um contendo vários símbolos.
Ex.: Transposição de colunas

Cifra de fluxo

- Cifra de chave simétrica que combina os bits de um fluxo de bits (*bitstream*) com os bits de uma chave (*keystream*)
- A encriptação geralmente é feita por meio de uma simples operação XOR:

$$c = E(k,m) = k \oplus m$$

One Time Pad

- Desenvolvido em 1917 por Gilbert Vernam nos laboratórios da Bell, para cifrar fluxos.
- A chave é uma string de bits aleatória do **mesmo tamanho da mensagem** a ser criptografada.
- É **inquebrável** (matematicamente comprovado), desde que a chave seja realmente aleatória e mantida em segredo.

One Time Pad

$c = E(k,m) = k \oplus m$

Mensagem: 1 0 0 0 1 1 0
Chave: 1 1 0 0 0 1 1
Texto cifrado: 0 1 0 0 1 0 1

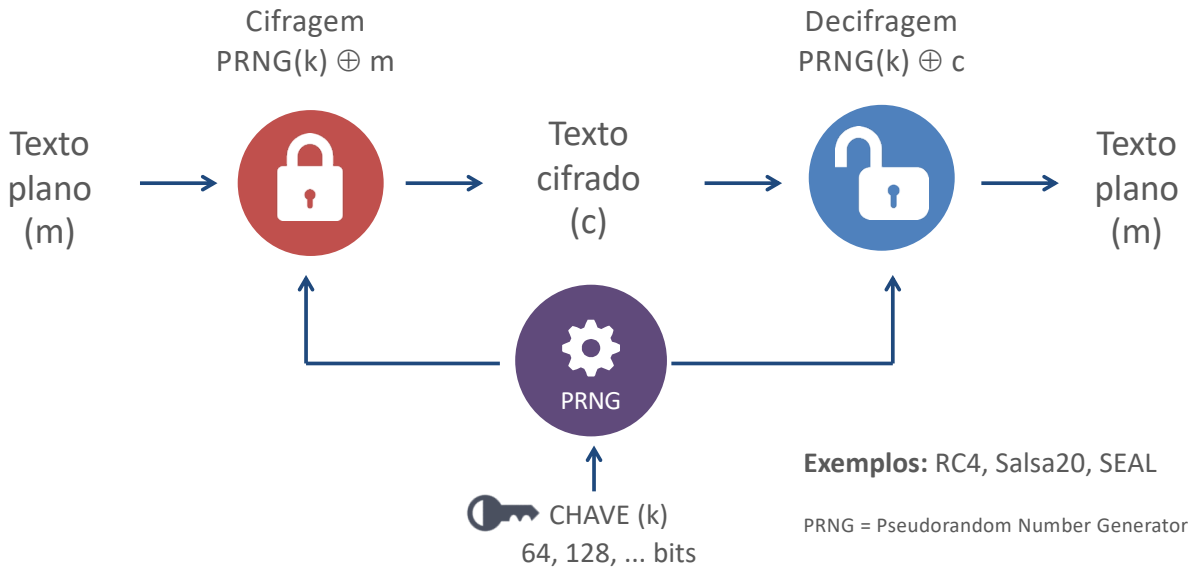
$m = D(k,m) = k \oplus c$

Texto cifrado: 0 1 0 0 1 0 1
Chave: 1 1 0 0 0 1 1
Mensagem: 1 0 0 0 1 1 0

One Time Pad

- O OTP requer chaves muito longas, difíceis de serem gerenciadas e mantidas em sigilo.
- Os algoritmos usam, portanto, um **gerador de chaves pseudoaleatórias** usando uma **chave semente** de 64, 128, 256 ou mais bits.

Chaves pseudoaleatórias



Cifras de fluxo

VANTAGENS

- **Alta velocidade**
  Os algoritmos são lineares no tempo e constantes no espaço.
- **Baixa propagação de erros**
  Um erro na cifragem de um símbolo dificilmente afetará os símbolos seguintes.

DESVANTAGENS

- **Baixa difusão**
  Toda a informação de um símbolo de texto simples é contido em um único símbolo de texto cifrado.
- **Suscetibilidade a inserções e modificações**
  Um intruso pode inserir texto falso que parece autêntico.