STREAM CIPHERS + ONE TIME PAD (OTP) 1

↳ CIFRAS DE FLUXO!

↳ PARTE SIMÉTRICA

* **DEF:** Uma cifra é definido como: $(\mathcal{K}, \mathcal{M}, \mathcal{C})$
"um par de algoritmos (E, D) eficientes onde: $D = (K, E(K,m)) = m$

$E = \mathcal{K} \times \mathcal{M} \to \mathcal{C}$, $D = \mathcal{K} \times \mathcal{C} \to \mathcal{M}$, ou seja,
$\forall m \in \mathcal{M}, K \in \mathcal{K} : D(K, E(K,m)) = m$

eficiência significa executar em X tempo.
↳ cifrar em X tempo.

* E: randomico
* D: determinístico

ONE TIME PAD (VERNAM 1917)

Exemplo: $\mathcal{M} = \mathcal{C} = \{0,1\}^n$ $\mathcal{K} = \{0,1\}^n$

↳ string de bits aleatória, não se sabe tamanho e nem a sequência.

$C := E(K,m) = K \oplus m$

$D(K,C) = K \oplus C$

$D(K, E(K,m)) = D(K, K \oplus m) = K \oplus (K \oplus m) =$
$= (K \oplus K) \oplus m = 0 \oplus m = m$

$$msg = 0\ 1\ 1\ 0\ 1\ 1\ 1 \oplus$$
$$K = 1\ 0\ 1\ 1\ 0\ 0\ 1$$
$$CT = 1\ 1\ 0\ 1\ 1\ 1\ 0$$

Questão: • Você recebe uma mensagem (m) e sua cifra (c) OTP.
• Você consegue computar a chave OTP a partir de m e c?

R:. Sim, a chave é $k = m \oplus c$

* OTP é rápido para cifrar e decifrar, mas tem chaves muito longas (tão longas quanto o texto da mensagem)

↳ mas, o que torna essa cifra segura então?

INFORMATION THEORETIC SECURITY

— SHANNON 1949

* CT: cipher text → texto cifrado
* PT: plain text → texto em claro

* Ideia básica: CT não deve revelar nenhuma informação sobre o PT

* DEF: Uma cifra (E, D) em $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ tem um segredo perfeito se:

$$\forall m_0, m_1 \in \mathcal{M} \quad (len(m_0) = len(m_1))$$

$$\forall c \in \mathcal{C} : \boxed{P_R[E(k, m_0) = c] = P_R[E(k, m) = c]}$$

onde k é uniforme em $\mathcal{K}$ $\quad (k \xleftarrow{R} \mathcal{K})$

se a mensagem for interceptada, o terceiro / atacante não poderá afirmar se é 0 ou 1, já que ambos podem ser o c cifrados.

Provando isso: "OTP tem um segredo perfeito"

$$\forall m, c = P_K[E(K,m)=c] = \frac{\#\text{chaves } K \in \mathcal{K} \text{ que } E(K,m)=c}{|\mathcal{K}|}$$

Então, $\forall m, c : \#\{K \in \mathcal{K} : E(K,m)=c\} = \underline{\text{const.}}$

↓

Tem um segredo perfeito!

Questão: Dado $m \in \mathcal{M}$ e $c \in \mathcal{C}$. Quantas chaves OTP mapeiam m para c?

R:. 1. Para OTP: $E(K,m)=c$

$\Rightarrow K \oplus m = c \Rightarrow K = m \oplus c$

$\Rightarrow \#\{K \in \mathcal{K} : E(K,m)=c\} = 1 \quad \forall m, c$

$\Rightarrow$ OTP tem um segredo perfeito

PORÉM, ... FALTA UMA PROPRIEDADE DO segredo PERFEITO:

* $|\mathcal{K}| \geq |\mathcal{M}|$