

# STREAM CIPHERS 1 + ONE TIME PAD (OTP)

↳ CIFRAS DE FLUXO!

↳ PARTE SIMÉTRICA

\* DEF: Uma cifra é definida como:  $(\mathcal{K}, \mathcal{M}, \mathcal{C})$

"um par de algoritmos  $(E, D)$  eficientes onde:

$$D(K, E(K, m)) = m$$

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

↳ eficiência significa executar em X tempo.

↳ cifrar em X tempo.

\* E: randômico

\* 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 como é nem a sequência.

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

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

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

$$\begin{array}{rcccccccc} \text{msg} & = & 0 & 1 & 1 & 0 & 1 & 1 & 1 & \oplus \\ \text{K} & = & 1 & 0 & 1 & 1 & 0 & 0 & 1 & \\ \hline \text{CT} & = & 1 & 1 & 0 & 1 & 1 & 1 & 0 & \end{array}$$

- 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  $\rightarrow$  texto cifrado
- \* PT: plain text  $\rightarrow$  texto em claro
- \* Ideia básica: CT não deve revelar nenhuma informação sobre o PT
- \* DEF: Um cifr (E, D) em  $(\mathcal{K}, \mathcal{M}, \mathcal{C})$  tem um segredo perfeito se:

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

$$\forall c \in \mathcal{C} : P_K [E(K, m_0) = c] = P_K [E(K, m_1) = c]$$

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

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"

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

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



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: se  $E(k, m) = c$   
 $\Rightarrow k \oplus m = c \Rightarrow k = m \oplus c$   
 $\Rightarrow \#\{k \in \mathcal{K} : E(k, m) = c\} = 1 \quad \forall m, c$   
 $\Rightarrow$  OTP tem um segredo perfeito

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

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



### Vernam Cipher (One-Time Pad)

The Vernam cipher (aka the one-time pad, or Vigenere OTP) is the only encryption alg...

[youtube.com](https://www.youtube.com)



### One-Time Pad Cipher (Perfect Security)

One-Time Pad Cipher (Perfect Security) Index: - What is the one-time cipher? - How doe...

[youtu.be](https://youtu.be)