(GEN, ENC, DEC)

$M, K, C \subseteq \{0,1\}^*$

$GEN: \{1\}^* \longrightarrow K$

$GEN(1^n) \rightarrow k \qquad k \in K$

$k \leftarrow \{0,1\}^n$

$k \leftarrow GEN(1^n)$

largo fijo $\ell(n)$

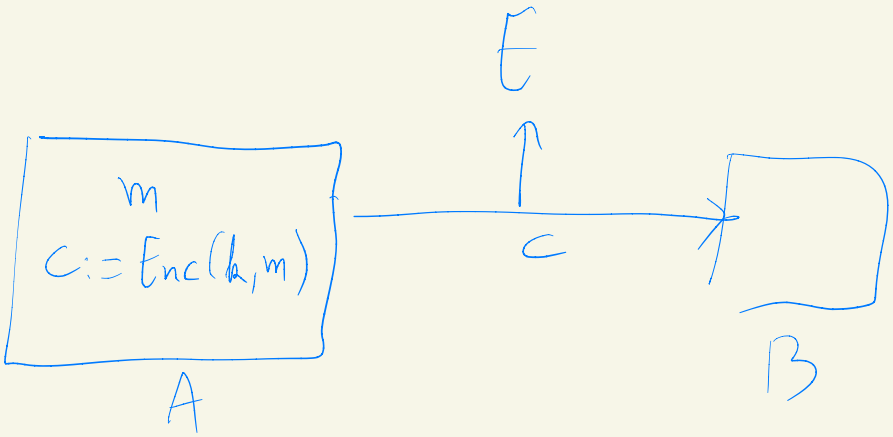
$\hookrightarrow Enc(k, m) \qquad |m| = \ell(n)$

Un sistema criptográfico es seguro si cada adversario corriendo en tiempo polinomial en n tiene éxito en quebrar el sistema con una probabilidad despreciable

↪ $f(n) \leq \frac{1}{P(n)}$

$f(n) = \frac{2^{100}}{2^n} \leq$

$\forall P(n)\ \exists n_0\ \forall n \geq n_0 \quad \frac{2^{100}}{2^n} \leq \frac{1}{P(n)}$



"Ataque de solo texto cifrado"

(1) Adv recibe 1^n, y construye un par de mensajes m_0 y m_1 del mismo largo

(2) Verificador genera $k \leftarrow GEN(1^n)$ y $b \in \{0,1\}$, calcula $c := Enc(k, m_b)$, y entrega c a Adv

(3) Adv indica si $b=0$ o $b=1$, y gana si la respuesta es correcta

Def: (GEN, Enc, Dec) tiene "cifrado indistinguible ante un ataque de solo texto cifrado" si para cada Adv que funciona en tiempo polinomial en n:

$$Pr(\text{Adv acierta el valor de } b) \leq \frac{1}{2} + \frac{1}{p(n)}$$

$$Pr(\text{Adv gana el juego}) \leq \frac{1}{2} + f(n)$$

donde $f(n)$ es una función despreciable.

$\frac{1}{2} + \frac{1}{2^n}$

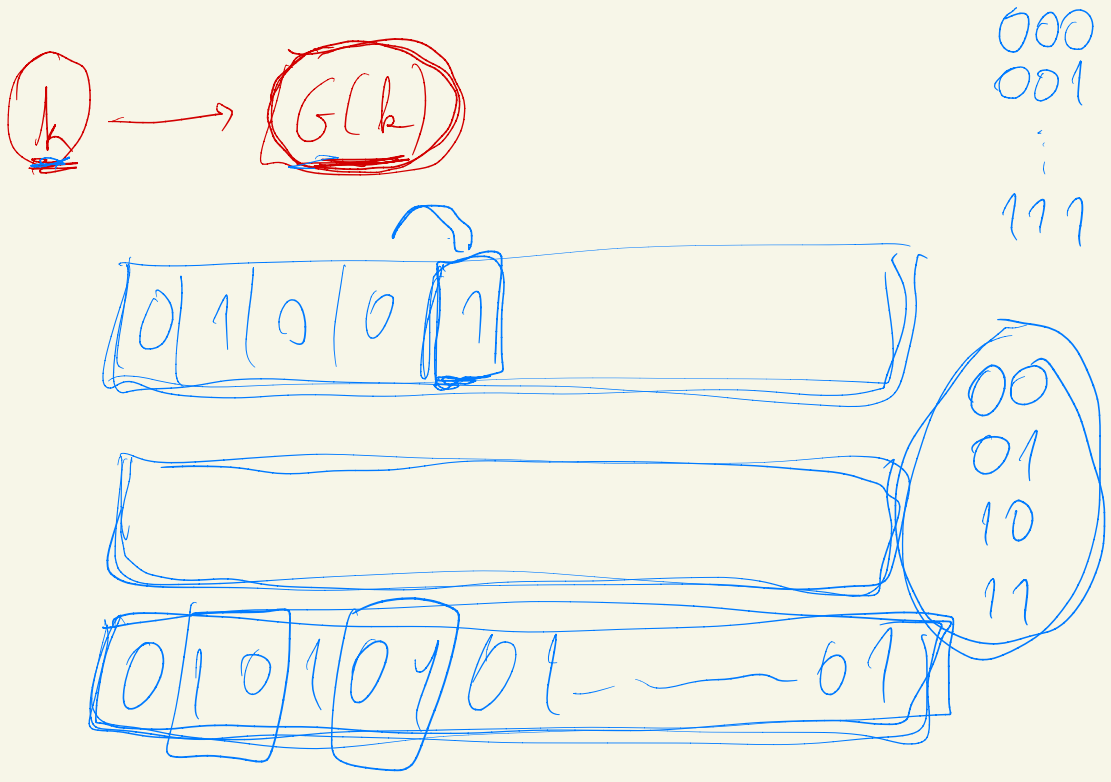
OTP

$c = k \oplus m$

$\forall m_1, m_2$

$Pr[k \leftarrow \{0,1\}^n : k \oplus m_1 = c] = Pr[k \leftarrow \{0,1\}^n : k \oplus m_2 = c]$

$G(k) \oplus m$ (GEN, Enc, Dec)



Def: Sea $G: \{0,1\}^* \to \{0,1\}^*$ un algoritmo de tiempo polinomial que dado $s \in \{0,1\}^n$, construye $G(s) \in \{0,1\}^{p(n)}$, donde $p(n)$ es un polinomio fijo. G es un <u>generador pseudo-aleatorio</u> si:

1. Expansión $\forall n: p(n) > n$
2. Pseudo-aleatoriedad: para todo algoritmo $D: \{0,1\}^* \to \{0,1\}$ de tiempo polinomial, existe una función despreciable $f(n)$:

$$\left| \Pr_{r \leftarrow \{0,1\}^{p(n)}}[D(r)=1] - \Pr_{s \leftarrow \{0,1\}^n}[D(G(s))=1] \right| \leq f(n)$$

$g(n)$

$$\Pr[D(r)=1] \qquad p(n)>n$$

$r \leftarrow \{0,1\}^{p(n)}$

$$\equiv$$

$$\Pr[D(G(s))=1]$$

$s \leftarrow \{0,1\}^{n}$

$$G(s) \in \{0,1\}^{p(n)}$$

$\|-n-1$	$\|-$
$0 \cdots 0$ (n)	$01\{0,1\}^{p(n)-1} = G(s)$
!	