"perfect secrecy"

K, M, C

$\forall c \in C \quad \forall m_0, m_1 \in M$

$$Pr_{k \leftarrow K}[Enc(k, m_0) = c] = Pr_{k \leftarrow K}[Enc(k, m_1) = c]$$

"Computacionalmente seguro"

- de capacidad computacional del adversario
- probabilidad de éxito del adversario

"Seguridad concreta"

Un sistema criptográfico es (t, ε)-seguro si un adv corriendo en tiempo t tiene una probabilidad de quebrar el sistema de a lo más ε.

Ejemplo: $K = \{0,1\}^{256}$

$$\frac{t}{2^{256}}$$

"Seguridad asintótica"

Un sistema criptográfico es seguro si cada adversario corriendo en tiempo polinomial en n tiene éxito en quebrar el sistema con una probabilidad despreciable (1)

(1) $f(n) = \frac{1}{e^n}$ $\frac{1}{k^n}$ $\frac{1}{n^{\log n}}$

$\frac{1}{2^{\sqrt{n}}}$ ~~$\frac{1}{2}$~~ ~~$\frac{1}{n}$~~

$\frac{1}{2^n}$ $n=10$ $n=20$

① Una función $f: \mathbb{N} \to [0,1)$ es despreciable si

$\forall$ polinomio $p(n)$

$\exists n_0 \in \mathbb{N}$

$\forall n \geq n_0 : \quad f(n) \leq \frac{1}{p(n)}$

$\exists n_0 \; \forall n \geq n_0 : f(n) \leq \frac{1}{n^2}$

$\frac{1}{2^n} \leq \frac{1}{n^k}$ $\qquad 0 \leq \frac{f(n)}{p(n)} \leq \frac{1}{p(n)^2} \to 0$

---

f, g son despreciables, $f+g$ es despreciable?

$\forall p(n)$ $\exists n_0$ $\forall n \geq n_0$ $f(n) \leq \frac{1}{p(n)}$ (A)

$\forall q(n)$ $\exists m_0$ $\forall m \geq m_0$ $g(m) \leq \frac{1}{q(m)}$ (B)

Sem $f+g$:

P.d. $\forall r(n)$ $\exists l_0$ $\forall l \geq l_0$ $f(l)+g(l) \leq \frac{1}{r(l)}$

$r(n)$

(A) $2r(n)$: $\exists n_0 \forall n \geq n_0 f(n) \leq \frac{1}{2r(n)}$

(B) $2r(n)$: $\exists m_0 \forall m \geq m_0 g(m) \leq \frac{1}{2r(m)}$

$l_0 = \max\{n_0, m_0\}$ $(l_0 = n_0 + m_0)$

$\forall l \geq l_0$: $f(l)+g(l) \leq \frac{1}{2r(l)} + \frac{1}{2r(l)}$

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

Sistema de cifrado simétrico o esquema de cifrado simétrico sobre M, K, C es una tupla (GEN, ENC, DEC)

① $GEN: \{1\}^* \longrightarrow K$

$\hookrightarrow \{\varepsilon, 1, 11, 111, \dots\}$

es un algoritmo aleatorizado de tiempo polinomial

$\rightarrow G(1^n)$ genera una clave k

$k \leftarrow G(1^n)$

n = 900.000

$\ell = 6$

k

$10^{\ell} \approx n$

$\log_{10}(n)$

$\log_2(n)$

111111

$n = 6$

$Enc : K \times M \longrightarrow C$ es un algoritmo de tiempo polinomial

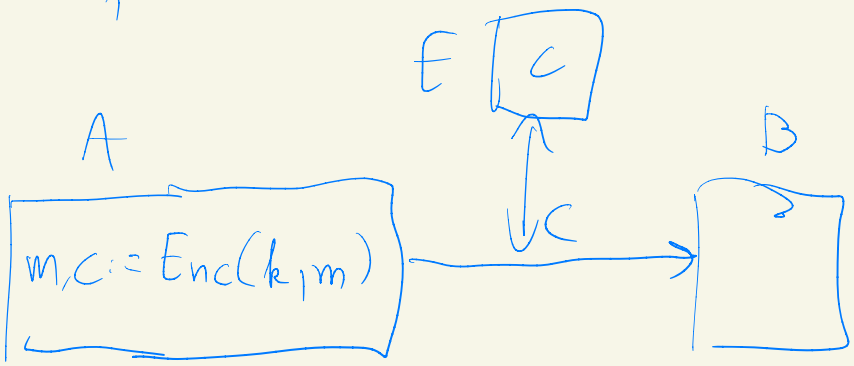
$Enc(k, m)$

$DEC : K \times C \to M$ es un algoritmo de tiempo polinomial

$DEC(k, Enc(k, m)) = m.$

Si para cada $k \leftarrow GEN(1^n)$, se tiene que $Enc(k, m)$ está definido solo para mensajes $m \in \{0,1\}^{\ell(n)}$, entonces (GEN, Enc, DEC) es un sistema de cifrado de largo fijo $\ell(n)$.

→ "Ataque de solo texto cifrado"



→ Adv recibe 1^n, construye $m_0, m_1 \in M$ del mismo largo → $m_0, m_1 \in \{0,1\}^{\ell(n)}$

→ Adv envía m_0 y m_1 a el verificador. El ver:

- toma $b \in \{0,1\}$ y $k \leftarrow GEN(1^n)$, calcula $c := Enc(k, m_b)$, y le pasa c a Adv.

→ Adv es decir si $b=0$ o $b=1$