Def $G: \{0,1\}^* \to \{0,1\}^*$ $p(n)$

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

G es generador pseudo-aleatorio:

(1) $\forall n: p(n) > n$

(2) Para todo algoritmo $D: \{0,1\}^* \to \{0,1\}$ de tiempo polinomial, existe una función despreciable $f(n)$:

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

$p(n)$ es el factor de expansión de G.

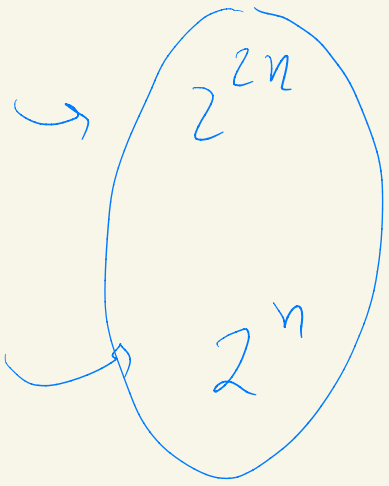
$p(n) = 2n$

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

$G(s) \in \{0,1\}^{2n}$

$r \leftarrow \{0,1\}^{2n}$

$D(r)$

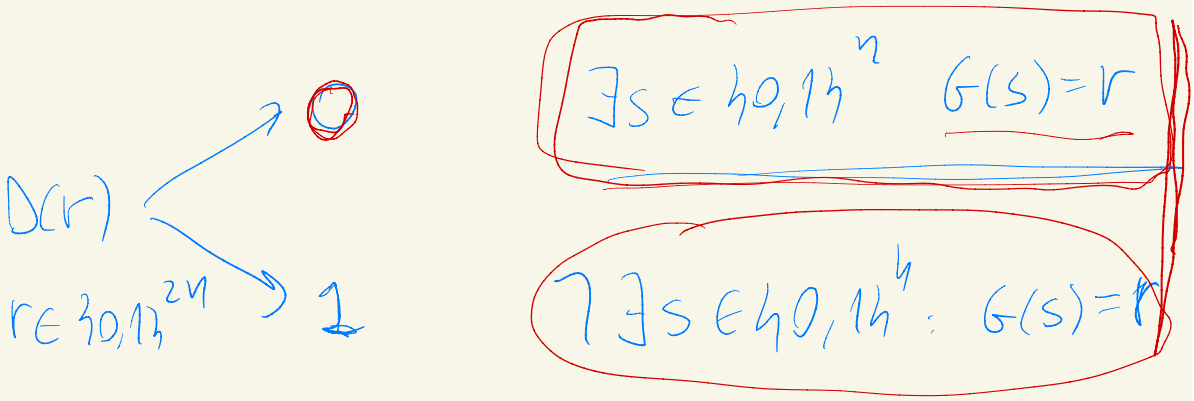


$s \leftarrow \{0,1\}^n$

$r = G(s)$

$D(r)$

$$Pr_{r \leftarrow \{0,1\}^{2n}}\left[\exists s \in \{0,1\}^n : G(s) = r\right] = \frac{2^n}{2^{2n}} = \frac{1}{2^n}$$



$$\Pr_{s \leftarrow \{0,1\}^n}[D(G(s)) = 1] = 0$$

2^n

$$\Pr_{r \leftarrow \{0,1\}^{2n}}[D(r) = 0] \leq \frac{2^n}{2^{2n}} = \frac{1}{2^n}$$

$$\Pr_{r \leftarrow \{0,1\}^{2n}}[D(r) = 1] - \Pr_{s \leftarrow \{0,1\}^n}[D(G(s)) = 1]$$

$$\geq 1 - \frac{1}{2^n} - 0 \geq 1 - \frac{1}{2^n}$$

$\leq f(n)$

$\exists n_0 \ \forall n \geq n_0 \quad 1 - \frac{1}{2^n} \leq \frac{1}{n}$

$S \in \{0,1\}^{10}$

Un sistema de cifrado de longa fijo $l(n)$

Suponemos que existe generador pseudo-aleatorio G con factor de expansión $l(n)$

(GEN, Enc, Dec)

- $GEN(1^n)$: $k \leftarrow \{0,1\}^n$

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

- $Enc(k, m) = G(k)$ XOR m
- $Dec(k, c) = G(k)$ XOR c

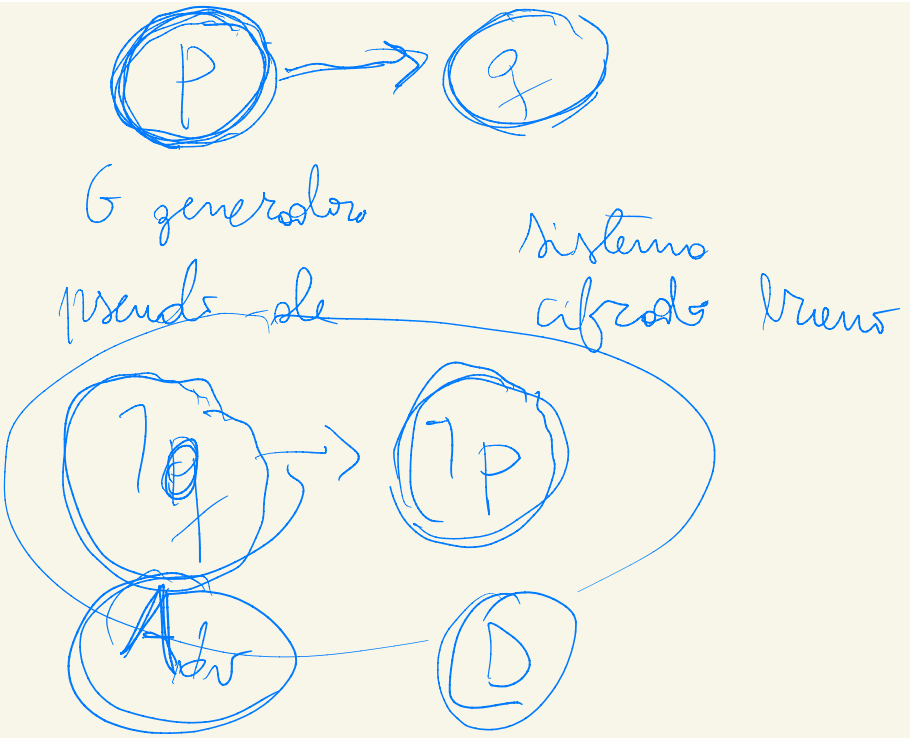
Teo: Si G es un generador pseudo-aleatorio, entonces el esquema anterior tiene "cifrado indistinguible ante un ataque de solo texto cifrado".

$|m_0| = |m_1|$

- Adv construye m_0 y m_1
- Ver $b \in \{0,1\}$ y $k \leftarrow \{0,1\}^n$, $c := Enc(k, m_b)$, y le pasa c a Adv
- Adv dice si $b=0$ o $b=1$

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

donde $f(n)$ es despreciable.


p
q
G gerador
pseudo-aleatório
sistema
cifrado Vernam
¬q
¬p
A ⊕
D

Un sistema de cifrado de longs arbitrarias (STREAM CYPHER)

$$G: \{0,1\}^* \times \{1\}^* \longrightarrow \{0,1\}^*$$

$s \in \{0,1\}^*$

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

$$G_p(s) = G(s, 1^{p(|s|)})$$

$|s| = k$

$\Rightarrow \quad G(s, 1^k) \in \{0,1\}^k$

(GEN, Enc, Dec)

$GEN(1^n) \qquad k \leftarrow \{0,1\}^n$

$Enc(k, m) = G(k, 1^{|m|}) \oplus m$

$Dec(k, c) = G(k, 1^{|m|}) \oplus c$

$G(k, 1^n)$

$G(k)$

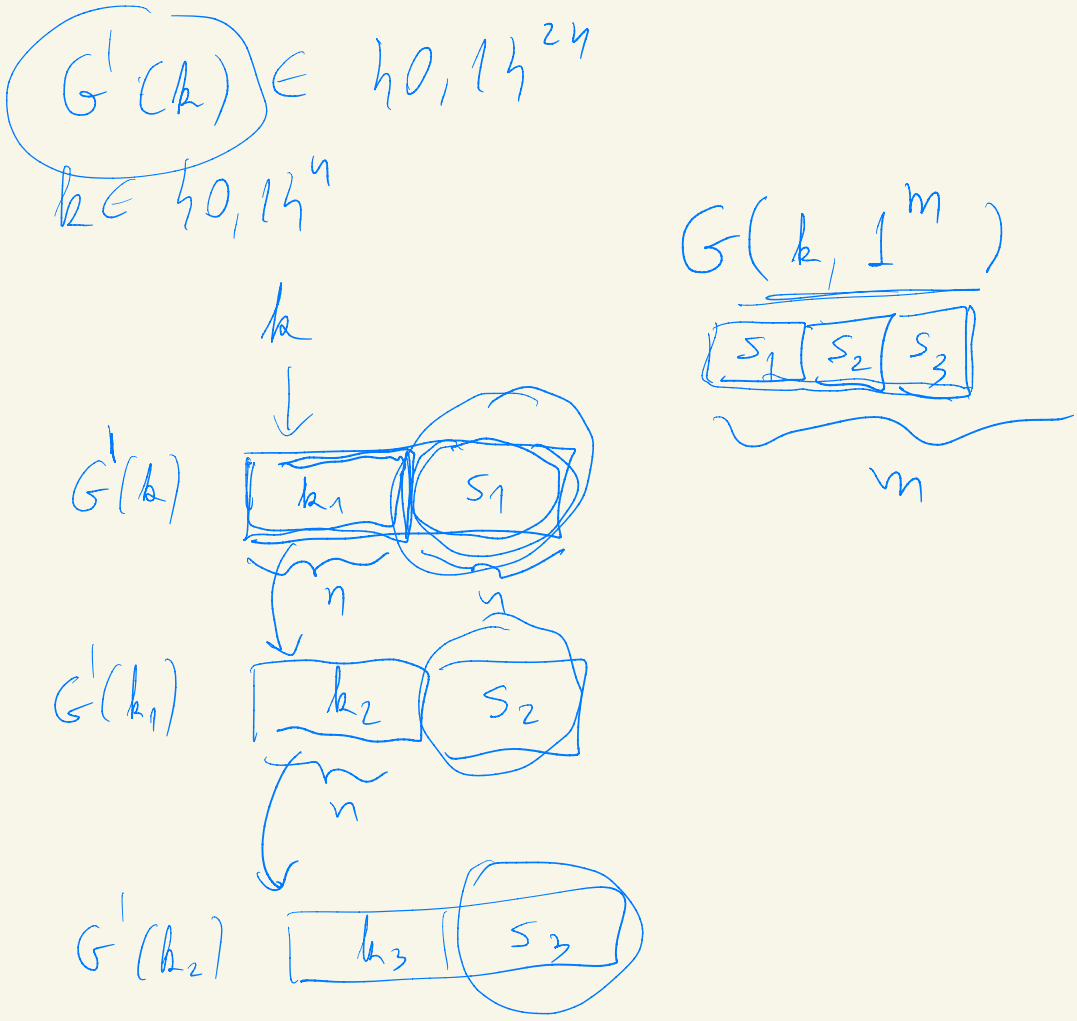
$G'(k) \in \{0,1\}^{2n}$

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

k

$|G(k)| = 2n$

$|G'(G(k))| = 4n$


$G'(k) \in \{0,1\}^{2n}$
$k \in \{0,1\}^n$
$G(k, 1^m)$
s_1 s_2 s_3
m
k
$G'(k)$
k_1 s_1
n n
$G'(k_1)$
k_2 s_2
n
$G'(k_2)$
k_3 s_3