

Stream Ciphers

Generadores pseudo-Aleatorios (PRG)

Un generador pseudo-Aleatorio es un algoritmo determinista para generar números aparentemente aleatorios. Estos números no son realmente aleatorios ya que siguen un algoritmo, pero parecen serlo.

$G: \{0,1\}^L \rightarrow \{0,1\}^L$ donde $L \leq L$ siendo L la longitud de la cadena.

Intuitivamente se dice que G es seguro si es computacionalmente difícil de distinguir entre $r=G(s)$ y un número verdaderamente aleatorio. Un desafiante selecciona un número y después genera un número aleatorio de forma desconocida para el atacante. Tras eso revela un número R de forma que el atacante debe saber si el número es verdaderamente aleatorio o no, si el atacante acierta el número entonces el sistema ha sido comprometido.

PRGs Seguros

G es un PRG seguro si: $|P(b=1|b=0) - p(b=1, b=1)| \leq \xi$ para un ξ extremadamente pequeño y todos los adversarios eficientes A .

G es seguro cuando no existe ninguna prueba estadística eficiente para decidir si $G(s)$ es aleatorio con una probabilidad que no sea extremadamente pequeña. Algunos test estadísticos pueden ser:

- Frecuencia empírica de 1s y 0s
- Frecuencia empírica de substrings
- Valores Extremos: mayor secuencia de 1s

Stream Ciphers

Stream Cipher es un cifrado basado en PRG. El Stream Cipher (E,D) definido de un PRG G es:

Encriptado: $E(s,m) = G(s) \oplus m$

Desencriptado: $D(s,c) = G(s) \oplus c$

Si G es un PRG seguro, entonces el Stream Cipher (E,D) construido a partir de G es semanticamente seguro.

From:
<http://www.knoppia.net/> - Knoppia

Permanent link:
<http://www.knoppia.net/doku.php?id=si:streamci&rev=1726587599>

Last update: **2024/09/17 15:39**



