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.

$G:[{0,1}]^l -> [{0,1}]^L$ donde $l<=L$ 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: $|P(b=1|b=0)-p(b=1,b=1)|<=ξ$ 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 estdísticos pueden ser:

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

Stream Ciphers

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

Encriptado: $E(s,m) = G(s)⊕m$

Desencriptado: $D(s,c)=G(s)⊕C$

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