Stream Ciphers

Generadores pseudo-Aleatorios

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 $l<=L$

Intuitivamente se dice que G es seguro si es computacionalmente difícil de distinguir entre $r=G(s)$ y un número verdaderamente aleatorio.