

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.

$G: \{0,1\}^I \rightarrow \{0,1\}^L$ donde $I \leq L$

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

From:

<https://knoppia.net/> - **Knoppia**

Permanent link:

<https://knoppia.net/doku.php?id=si:streamci&rev=1726586850>

Last update: **2024/09/17 15:27**

