PRG SECURITY DEFS.

STREAM CIPHERS 5

Considerando: $G: K \to \{0,1\}^n$ sendo PRG, o que torna um número pseudo aleatório indistinguível de um aleatório?

$[k \xleftarrow{R} \mathcal{K}, \text{output } G(k)]$

$[r \xleftarrow{R} \{0,1\}^n, \text{output } r]$

TESTE ESTATÍSTICO

↳ exemplo: em $\{0,1\}^n$: algoritmo A que A(x) tem saída "0" ou "1".

"ALEATÓRIO" ↑

↓ "NÃO ALEATÓRIO"

VANTAGEM

* Considerando $G: K \to \{0,1\}^n$ seja um PRG e A um teste estatístico em $\{0,1\}^n$, temos:

$$Adv_{PRG}[A,G] := \left| P_{k \xleftarrow{R} \mathcal{K}}[A(G(k))=1] - P_{k \xleftarrow{R} \{0,1\}^n}[A(r)=1] \right| \in [0,1]$$

↳ $\cong 1$: PRG ruim.

$\cong 0$: PRG seguro, saída indistinguível de números aleatórios para A.

Questão: $G: K \to \{0,1\}^n$ satisfaz $msb(G(k)) = 1$ para 2/3 das chaves de K em $\mathcal{K}$.

- defina um teste estatístico que: se [msb(x=1)] a saída é "1" caso contrário "0".

- qual a vantagem?

• R.

$$Adv_{PRG}[A,G] = |P_R[A(G(k))=1] - P_R[A(r)=1]| =$$
$$|\ 2/3 \quad - \quad 1/2\ | = 1/6$$

***DEf:** ∀ teste estatístico "eff." em A, $Adv_{PRG}[A,G]$ é neg.

***DEf:** se ∀ i ∈ {0,...,n-1} PRG G é imprevisível na posição i então G é um PRG seguro.