Lista de exercícios 3
Números aleatórios
Segurança da Informação

1. Descreva um método para diferenciar números provenientes de uma distribuição uniforme aleatória e de números provientes de um gerador de números pseudo-aleatórios. Calcule o número máximo de bits que esses números podem ter para um computador rodando em 4GHz conseguir identificar se os números são provenientes de um gerador pseudo-aleatório com probabilidade pelo menos 0.5 em até um ano. Considere que o computador executa uma operação lógico-aritmética por ciclo de clock.

2. Porque números aleatórios são importantes para criptografia?

3. Porque usar um conjunto de testes de hipóteses para verificar se números são aleatórios não é suficiente para garantir a segurança de seu uso?

4. Considere um algoritmo de geração de números aleatórios $G : K \to \{0,1\}^n$ tal que $XOR(G(k)) = 1$. É possível afirmar que G é seguro? Porque?

5. Seja G um gerador pseudo-aleatório tal que $|G(s)| \geq 2 \cdot |s|$. Defina $G'(s) = G(s0^{|s|})$. É verdade que G' é obrigatoriamente um gerador de números pseudo-aleatórios?

6. Seja $F : K \times X \to \{0,1\}^{128}$ uma função pseudo-aleatória segura. Defina a função $G(k,x) = 0^{128}$ se $x = 0$ e $G(k,x) = F(k,x)$ caso contrário. Prove se G é seguro ou não.

7. Seja $G : K \to \{0,1\}^n$ um gerador de números pseudo-aleatórios tal que a partir dos últimos $n/2$ de $K(k)$ é possível computar os primeiros $n/2$ bits. É possível predizer G para algum $i \in \{0,\ldots,n-1\}$? Porque?