Lista de exercícios 4
Funções e permutações aleatórias
Segurança da Informação

1. Defina um algoritmo de geração de números aleatórios a partir de uma função aleatória chaveada.

2. Explique o cenário de segurança de um atacante capaz de escolher textos em claro para a vítima encriptá-los.

3. Obtenha, explicando passo a passo, a equação que provê o número de funções existentes que mapeiam dois conjunto de n elementos.

4. O que é uma cifra de blocos?

5. Seja $X = \{0, 1\}$. Seja o espaço de chaves $K = \{0, 1\}$, o espaço de mensagens $X = \{0, 1\}$ e a função aleatória chaveada $E(k, x) = x \oplus k$. Essa função é segura?

6. Seja $X = \{0, 1\}$. Seja o espaço de chaves $K = \{0, 1\}$, o espaço de mensagens $X = \{0, 1\}$ e a função de permutações aleatórias $E(k, x) = x \oplus k$. Essa função é segura?