

# Lista de exercícios 2

## Sigilo Perfeito

### Segurança da Informação

25 de Abril de 2017

1. Explique com um exemplo o teorema de Bayes.
2. Porque a operação XOR bit a bit é usada tanto em criptografia?
3. Seja  $x$  arbitrário e  $y$  uniformemente aleatório. Porque  $x$  XOR  $y$  é uniformemente aleatório? Porque isso é útil em criptografia?
4. Descreva as partes da cifra de Vernam.
5. Suponha que você tem uma mensagem  $m$  e o texto cifrado correspondente obtido com o OTP em arrays de `char`. Escreva um código em C para obter a chave usada.
6. Seja  $m \in \mathcal{M}$  e  $c \in \mathcal{C}$ . Quantas chaves  $k \in \mathcal{K}$  são capazes de mapear  $m$  em  $c$  no algoritmo One-Time Pad?
7. Explique com equações porque é necessário ter chaves de tamanho no mínimo igual à mensagem sendo transmitida para um método de encriptação ter sigilo perfeito.
8. Criptografia é a técnica de transformação da informação de sua forma original para outra ilegível. Esse processo prevê que somente a pessoa detentora do código de decifração, ou chave, possa restaurar e ter acesso à informação. O nome do processo criptográfico no qual são utilizadas duas chaves, uma no emissor e outra no receptor da informação, é
  - (A) criptografia de chave simétrica.
  - (B) cifra de César.
  - (C) criptografia de chave assimétrica.
  - (D) criptografia quântica.
  - (E) criptografia linear.
9. Escolha a alternativa que apresenta somente exemplos de algoritmos criptográficos de chave simétrica
  - (A) RSA, ElGamal, DES
  - (B) Diffie-Helman, RSA, RC4
  - (C) ElGamal, Diffie-Helman, Curvas Elípticas
  - (D) RC4, RC5, RSA
  - (E) DES, IDEA, AES
10. O que é um esquema criptográfico com sigilo perfeito? Use a definição formal. Prove que o One-Time Pad é desse tipo.
11. O que é a indiscernibilidade perfeita. Mostra a ligação desse conceito com sigilo perfeito.
12. Descreva e explique o experimento  $Priv_{\mathcal{A}, \Pi}^{eav}$ .

**13.** Escreva um algoritmo que decifra (sem usar a chave) múltiplos textos cifrados com o OTP com a mesma chave.

**14.** É verdade que para todo esquema criptográfico com sigilo perfeito vale que para toda distribuição sobre o espaço de mensagens  $\mathcal{M}$ , todo  $m, m'$  e todo  $c \in \mathcal{C}$ :

$$P(\mathcal{M} = m|C = c) = P(M = m'|C = c)$$

?

**15.** É verdade todo esquema de encriptação em que o tamanho do espaço de chaves é igual ao tamanho do espaço de mensagem e em que a chave é escolhida uniformemente do espaço de chaves é perfeitamente secreto?