

Disciplina: Tópicos Avançados em Ciência da Computação VI

Tema: Introdução à Criptografia

1. Introdução

- 1.1. Importância
- 1.2. Aplicações: Comerciais e Governamentais
- 1.3. Fundamentos da Segurança

2. Criptologia

- 2.1. Conceito
- 2.2. Criptografia Clássica
- 2.3. Criptoanálise

3. Teoria de Shannon

- 3.1. Segredo perfeito
- 3.2. Entropia
- 3.3. Aplicações a Sistemas Criptográficos

4. Sistema Criptográfico AES

- 4.1. Descrição
- 4.2. AES na prática: modos de operação
- 4.3. Criptoanálise Linear
- 4.4. Criptoanálise Diferencial

5. Sistemas de Chave Pública

- 5.1. Importância e Fundamentos
- 5.2. Teoria dos Números
- 5.3. Algoritmo de Euclides
- 5.4. Teorema Chinês dos Restos

6. Sistema Criptográfico RSA

- 6.1. Implementação
- 6.2. Teste de Primalidade Probabilístico
- 6.3. Ataques ao RSA

7. Sistema Criptográfico El Gamal

- 7.1. Algoritmos para o Logaritmo Discreto
- 7.2. A segurança dos Logaritmos Discretos

8. Esquemas de Assinaturas Digitais

- 8.1. Esquema El Gamal
- 8.2. Padrão de Assinatura Digital

9. Distribuição de Chaves

- 9.1. Pré-distribuição de Chaves
- 9.2. Troca de Chaves

10. Geração de Números Pseudo-Aleatórios

10.1. Introdução e Exemplos

10.2. Medindo a qualidade de um Gerador Pseudo-Aleatório

11. Criptografia Quântica

11.1. Fundamentos

11.2. Implementação

12. Criptografia Pós-quântica

12.1 Fundamentos

12.2 Métodos

Bibliografia:

STALLINGS, William. Criptografia e segurança de redes: princípios e práticas. 6. ed. São Paulo: Pearson, 2014.

MENEZES, Alfred J.; VAN OORSCHOT, Paul C.; VANSTONE, Scott A. Handbook of applied cryptography. Boca Raton: CRC Press, 1996.

KATZ, Jonathan; LINDELL, Yehuda. Introduction to modern cryptography. 2. ed. Boca Raton: Chapman & Hall/CRC, 2015.

SCHNEIER, Bruce. Applied cryptography: protocols, algorithms, and source code in C. 2. ed. New York: John Wiley & Sons, 1996.

BERNSTEIN, Daniel J.; BUCHMANN, Johannes; DAHMEN, Erik (org.). Post-quantum cryptography. Berlin: Springer, 2009.