EMENTA

Introdução a Teoria da Informação e Complexidade Computacional. Cripto-Sistemas de Chave Privada e Cripto-Sistemas de Chave Pública. Assinaturas Digitais. Criptoanálise. Técnicas de Implementação e Aplicações.

CONTEÚDO PROGRAMÁTICO

01. Complexidade de Algoritmos em Criptografia. As classes P e NP.
02. Entropia e Ambiguidade. Sigilo Perfeito. Distância de Unicidade.
03. Cripto-Sistemas de Chave Privada. Cifras de Transposição e de Substituição.
04. Os Padrões de Cifragem de Dados DES, IDEA, SAFER e AES.
05. Técnicas de Criptoanálise. Ataques por Texto Cifrado, por Texto Claro Conhecido e por Texto Claro Escolhido.
06. Os Algoritmos da Mochila, El Gamal e RSA. Assinaturas Digitais.
07. Testes de Composição e de Primalidade.
08. Algoritmos de Fatoração de Números Inteiros.
09. Técnicas de Implementação. Cifragem de Bloco e Bit a Bit.
10. Cifragem com Encadeamento e Realimentação.
11. Aplicações.

BIBLIOGRAFIA

01. J. L. Massey, Cryptography: Fundamentals and Applications, Editores: V. C. da Rocha Jr. and R. D. Lins, 1999. Disponível em CD.
02. B. Schneier, Applied Cryptography - Protocols, Algorithms, and Source Code in C, John Wiley, Segunda Edição, 1996.