Salahoddin Shokranian

CRIPTOGRAFIA PARA INICIANTES

2ª EDIÇÃO

EDITORA CIÊNCIA MODERNA

Resumo de Criptografia Para Iniciantes

A tecnologia moderna de comunicação e armazenamento de informações é uma ciência do século XX cujos pilares são criptografia e teoria de códigos. Este livro trata, particularmente, de uma introdução à criptografia, a ciência de comunicação secreta entre várias fontes autorizadas.

Os objetivos da criptografia são a criação de cifras para comunicação de mensagens entre fontes autorizadas, para que as fontes não autorizadas não tenham acesso ao conteúdo das mensagens, bem como o estudo de métodos para descobrir as mensagens interceptadas.

O presente livro é elementar, acessível aos alunos das universidades com conhecimento mínimo em matemática e em teoria dos números. O autor teve a oportunidade de utilizar algumas partes desta obra como aplicação da teoria dos números em suas aulas sobre esse assunto na Universidade de Brasília (UnB), e os alunos gostaram e mostraram motivação para aprofundar seus estudos nessa direção.

No final do livro, existem três apêndices. Os objetivos destes são a apresentação de alguns temas da teoria dos números com aplicação direta na criptografia e a criação de chaves públicas para comunicação no sistema de chave pública, como RSA.

Certamente os alunos de graduação e pós-graduação dos Departamentos de Matemática, Ciência da Computação, Engenharia Eletrônica e demais departamentos da área de tecnologia, poderão aproveitar bem esta Segunda Edição do livro em seus estudos sobre tecnologia digital.

Acesse aqui a versão completa deste livro