Cryptography & Network Security

(2 Edition)

By Atul Kahate
Tata McGraw Hill Education Private Limited

Cryptography & network security is proposed for anyone interested knowing about security. Security is used today in every field. It introduces the concept of security.

This book has been structured to serve as an ideal text book for various introductory courses of cryptography & network security, fundamentals of cryptography for courses Engineering. The layout, organization and contents of the books are designed to project the fundamental concepts of cryptography and network security in an interesting, logical and informative manner. In general, the book provides insights on the functions and usage principal applicable to all types of network security system. The concepts are well illustrated with suitable examples and numerous diagrams for better illustrations. The book has attempted to avoid overloading to a reader who is interested in introductory concepts.

The book has been authorized by Atul Kahate. Atul kahate has 12 years of experience in Information Technology in India and abroad in various capacities. He has done his Bachelor of Science degree in Statistics and his Master of Business.

This book is divided into 10 chapters. Chapter 1 introduces the basic concept and need of security. It describes the security models, principles of security with practical example. It discusses ethical issues and different types of attacks with theoretical concept and example. It also discusses different programs of attacks, viruses and security management practices.

Chapter 2 introduces the concept of cryptography, basic terminologies of cryptography. It discusses cryptography algorithm based on substitution method and transposition method. This chapter introduces the concept of encryption and decryption. This chapter explains symmetric key cryptography and problems related to key distribution with practical example and also explain the concept of asymmetric key cryptography. This chapter also introduces the possible types of attacks in cryptography.

Chapter 3 discuss the various aspect related to symmetric key cryptography. It discusses stream and block cipher and the various chaining modes. It discusses algorithm modes, their limitations and comparison among them based on their features. This chapter also discusses major symmetric key cryptography algorithm in detail such as DES, Double DES, IDEA, RC4, RC5 and Blowfish.

Chapter 4 examines the concepts, issues in asymmetric key cryptography with history. This chapter discusses major asymmetric key cryptography algorithm in detail such as RSA, SHA and HMAC. This chapter introduce concept of digital envelop, digital signature and message digest. This chapter describes the MD5 algorithm with its strength and attacks launched against MD5.

Chapter 5 provides information of upcoming popular technology of Public Key Infrastructure (PKI). This chapter discuss about digital certificates, how they can be created, distributed, maintained and used. This chapter discusses the role of Certificate Authorities (CA) and Registration Authorities (RA) and also introduces the Public Key Cryptography Standards (PKCS).

Chapter 6 deals with the important security protocols for the internet. Different internet protocols are SSL, SHTTP, TSP, SET and 3-D secure. This chapter also discusses working of electronic money, dangers involved in it and how best we can make use of it. This chapter covers email security, detailed discussion of the key email security protocols such as PGP, PEM and S/MIME. This chapter also discusses wireless security.

Chapter 7 deals with the authentication of a user. There are various ways to do this. This chapter examines each one of them in detail with their pros and cons. This chapter discuss password-based authentication, authentication based on something derived from the password, authentication tokens, certificate based authentication. This chapter also discusses popular Kerberos protocol.

Chapter 8 deals with the practical issues related to cryptography. Currently there are three main ways to achieve this is to use the cryptographic mechanism provided by Sun (In Java Programming Language), Microsoft and third party toolkits. This chapter also discusses security mechanism in different operating system such as windows 2000 and UNIX and also covers database security.

Chapter 9 deals with network layer security. Here we studied firewall, their types and configuration. This chapter discusses on IP security, Virtual Private Networks (VPN).

Chapter 10 contains a number of case studies in the area of cryptography and network security. This chapter discusses how the concepts learnt in earlier chapter can be put into actual practice. It also covers some real-life security attacks that have happened. This chapter also presents the viewpoints of the attackers as well as those of the attacked party.

The book provides lot of information coverage and knowledge in the field of cryptography and network security. The faculty members would be able to prepare their lectures using this handbook. At the same time the students would be able to- (i) Acquire knowledge about the various topics. (ii) Make notes for their study purpose. (iii) Prepare for the examination.

Book Reviewed by

Radheshyam Acholiya
Assistant Professor
Pioneer Institute of Professional Studies, Indore

Dr. Mona Tawar
Director,
Pioneer Institute of Professional Studies, Indore