CRYPTOGRAPHY AND NETWORK SECURITY

—A Practical Approach

CRYPTOGRAPHY AND NETWORK SECURITY
—A Practical Approach

By

K. Haribaskar

M.E., Assistant Professor
Department of Computer Science & Engg.,
Mount Zion College of Engg. & Tech.,
Pudukkottai
Tamil Nadu

UNIVERSITY SCIENCE PRESS

(An Imprint of Laxmi Publications Pvt. Ltd.)

BANGALORE • CHENNAI • COCHIN • GUWAHATI • HYDERABAD
JALANDHAR • KOLKATA • LUCKNOW • MUMBAI • RANCHI

NEW DELHI • BOSTON, USA

CRYPTOGRAPHY AND NETWORK SECURITY—A PRACTICAL APPROACH

Printed and bound in India
Typeset at ABRO Enterprises
First Edition: 2014
UCN-9679-195-CRYPTOGRAPHY NET SEC-ANA
ISBN 978-93-81159-63-7

Price: ₹ 195.00

PUBLISHED IN INDIA BY

UNIVERSITY SCIENCE PRESS
(An Imprint of Laxmi Publications Pvt.Ltd.)
113, GOLDEN HOUSE, DARYAGANJ,
NEW DELHI - 110002, INDIA
Telephone : 91-11-4353 2500, 4353 2501
Fax : 91-11-2325 2572, 4353 2528
www.laxmipublications.com info@laxmipublications.com

Branches

Bangalore	080-26 75 69 30	
Chennai	044-24 34 47 26,	24 35 95 07
Cochin	0484-237 70 04,	405 13 03
Guwahati	0361-254 36 69,	251 38 81
Hyderabad	040-27 55 53 83,	27 55 53 93
Jalandhar	0181-222 12 72	
Kolkata	033-22 27 43 84	
Lucknow	0522-220 99 16	
Mumbai	022-24 91 54 15,	24 92 78 69
Ranchi	0651-220 44 64	

C—
Printed at:

CONTENTS

APPENDICES

(Pages 223–232)

PREFACE

The explosive growth in computer systems and their interconnections via network has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. The internet as a world wide communication network has changed our daily life in many ways. The internet, as an open forum, has created some security problems.

Network security is a set of protocols that allows us to use the internet comfortably without worrying about security attacks. The most common tool for providing network security is cryptography, an old technique that has been revived and adopted to network security. In this Universal electronic connectivity, virus and hackers, electronic eavesdropping, and electronic fraud, security is paramount. This book provides a practical survey of the principles of cryptography and network security.

This book is organized with the following styles:

- **Symmetric Ciphers:** A detailed examination of Classical Encryption Techniques, Block Ciphers, Data Encryption Standard and Advanced Encryption Standard.
- **Asymmetric Ciphers:** A detailed covers of Number Theory, Public Key encryption algorithms and principles, including a discussion of Key Management Techniques.
- **Cryptographic Data Integrity Algorithms:** A detailed examination of Authentication Requirements, Elliptic Curve functions, Hash Functions and its algorithm and Digital Signature.
- **Mutual Trust:** Looks at network security tools and applications including Kerberos, X.509 certificates, PGP, S/MIME, IP Security and SET. Looks at system-level security issues.

Suggestions for the improvement of the book will be gracefully acknowledged.

—Author

ACKNOWLEDGEMENTS

My sincere thanks to the Chairman of Mount Zion Christian Educational Trust Mr. Jayabarathan Chelliah and Mount Zion College of Engineering and Technology Director Prof. Jayson Keerthy Jayabarathan.

I would like to thank the following mentors who provided detailed technical reviews of many chapters: Dr. R. Krishnamoorty Dean, Anna University of Technology Tiruchirappalli India. Dr. S. Palani Dean, Sudharsan Engineering College, Pudukkottai, India; Dr. R. Raghavan Director, Sethu Institute of Technology, Virudhunagar, India.

The following people contributed for syllabus and course content: Mrs. S. Malarvizhi and Ms Seema Dev Akshtha.

My heartful gratitude to my parents and family members for their passionate support throughout the preparation of the book.

—Author

PART 1
SYMMETRIC CIPHERS

Chapters

1. Introduction to Networking
2. Classical Encryption Techniques
3. Block Ciphers and the Data Encryption Standard
4. Advanced Encryption Standard

CHAPTER 1 INTRODUCTION TO NETWORKING

1.1 STEP TO INFORMATION SECURITY

The network security and information security are often used interchangeably. Network security is generally taken as providing protection at the boundaries of an organization by keeping out intruders. Information security, however, explicitly focuses on protecting data resources from malware attack or simple mistakes by people within an organization by use of data loss prevention (DLP) techniques. One of these techniques is to compartmentalize large networks with internal boundaries.

Comparison with Computer Security

Securing network infrastructure is like securing possible entry points of attacks on a country by deploying appropriate defense. Computer security is more like providing means to protect a single PC against outside intrusion. The former is better and practical to protect the civilians from getting exposed to the attacks. The preventive measures attempt to secure the access to individual computers—the network itself—thereby protecting the computers and other shared resources such as printers, network-attached storage connected by the network. Attacks could be stopped at their entry points before they spread. As opposed to this, in

computer security the measures taken are focused on securing individual computer hosts. A computer host whose security is compromised is likely to infect other hosts connected to a potentially unsecured network. A computer host's security is vulnerable to users with higher access privileges to those hosts.

1.2 NETWORK SECURITY CONCEPTS

Network Security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together. Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them.

Network security starts from authenticating the user, commonly with a username and a password. Since this requires just one thing besides the user name, *i.e.,* the password which is something you 'know', this is sometimes termed one factor authentication. With two factor authentication something you 'have' is also used (*e.g.,* a security token or 'dongle', an ATM card, or your mobile phone), or with three factor authentication something you 'are' is also used (*e.g.,* a fingerprint or retinal scan).

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network and traffic for unexpected (*i.e.,* suspicious) content or behaviour and other anomalies to protect resources, *e.g.,* from denial of service attacks or an employee accessing files at strange times. Individual events occurring on the network may be logged for audit purposes and for later high level analysis.

Communication between two hosts using the network could be encrypted to maintain privacy.

1.3 ELEMENTS OF COMPUTER SECURITY

This general approach to computer security is based on eight major elements:

1. Computer security should support the mission of the organization.
2. Computer security is an integral element of sound management.
3. Computer security should be cost-effective.
4. Computer security responsibilities and accountability should be made explicit.
5. System owners have computer security responsibilities outside their own organizations.

6. Computer security requires a comprehensive and integrated approach.
7. Computer security should be periodically reassessed.
8. Computer security is constrained by societal factors.

1.4 SECURITY MANAGEMENT

Security Management for networks is different for all kinds of situations. A small home or an office would only require basic security while large businesses will require high maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

Small Homes

- A basic firewall.
- For windows users, basic Antivirus software like McAfee, Norton AntiVirus or AVG Antivirus. An anti-spyware program such as Windows Defender or Spybot would also be a good idea. There are many other types of antivirus or antispyware programs out there to be considered.
- When using a wireless connection, use a robust password. Also try and use the strongest security supported by your wireless devices, such as WPA or WPA2.

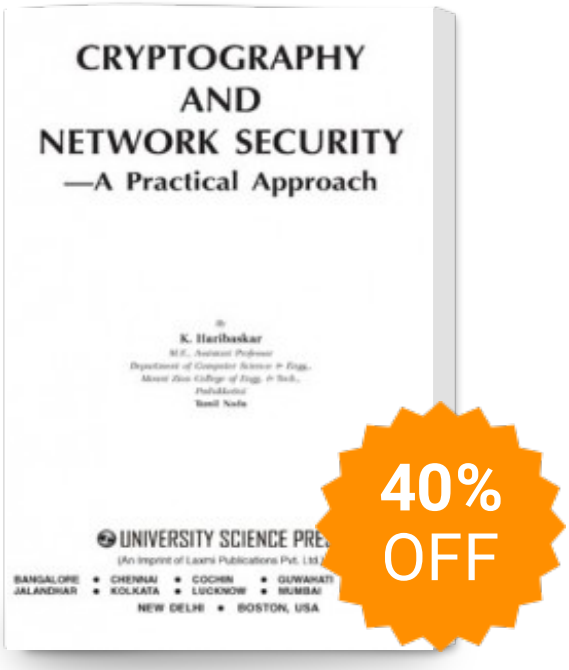
Medium Businesses

- A fairly strong firewall.
- Strong Antivirus software and Internet Security Software.
- For authentication, use strong passwords and change it on a bi-weekly/monthly basis.
- When using a wireless connection, use a robust password.
- Raise awareness about physical security to employees.
- Use an optional network analyzer or network monitor.

Large Businesses

- A strong firewall and proxy to keep unwanted people out.
- A strong Antivirus software package and Internet Security Software package.
- For authentication, use strong passwords and change it on a weekly/bi-weekly basis.
- When using a wireless connection, use a robust password.
- Exercise physical security precautions to employees.
- Prepare a network analyzer or network monitor and use it when needed.
- Implement physical security management like closed circuit television for entry areas and restricted zones.
- Security fencing to mark the company's perimeter.
- Fire extinguishers for fire-sensitive areas like server rooms and security rooms.
- Security guards can help to maximize security.

Cryptography and Network Security - A Practical Approach By K.Haribaskar



Publisher : Laxmi Publications ISBN : 9789381159637 Author : K.Haribaskar