ABOUT THE BOOK
Many engineers consider cryptography to be a sort of magic security dust that they can sprinkle over their hardware or software, and which will imbue those products with the mythical property of “security.” Security is only as strong as the weakest link, and the mathematics of cryptography is almost never the weakest link. The fundamentals of cryptography are important, but far more important are, how those fundamentals are implemented and used. You can argue whether the stake should be a mile or a mile-and-a-half high, but the attacker is simply going to walk around the stake. Security is a broad stockade—it’s the things around the cryptography that make the cryptography effective.

This book is intended for use in Graduate and Post Graduate courses, and for the professional cryptographers, presenting the techniques and algorithms of the greatest interest to the current practitioner, along with the supporting motivation and background material. It also provides a comprehensive source from which cryptography can be learnt, serving both students and instructors. Throughout each chapter, emphasis has been laid on the relationship between various aspects of cryptography. We believe this style of presentation allows a better understanding of how algorithms actually work. Each chapter has been written to provide a self-contained treatment of one major topic. Collectively, however, the chapters have been designed and carefully integrated to be entirely complementary with respect to definitions, terminology, and notation. Furthermore, there is essentially no duplication of material across chapters; instead, appropriate cross-chapter references are provided where relevant.

ABOUT THE AUTHORS
Ajay Raj Parashar is an Assistant Professor, Department of Information Technology, Hindustan College of Science & Technology [SGI], Mathura (UP) since 2006. With a B.Tech. degree in Information Technology & an M.Tech. degree in Computer Science & Engineering, he has published several research papers in International & National Conferences. He has also attended and organized several Workshops as well as Value Added Courses, such as:
- Certification in Software Quality Testing from IIT, Roorkee,
- Certification in Rational Application Development (RAD) from IBM,
- Certification in JAVA from Oracle.

Deepti Mittal is an Assistant Professor, Department of Information Technology, Hindustan College of Science & Technology [SGI], Mathura (UP) since 2006. With a B.Tech. degree in Information Technology & an M.Tech. degree in Computer Science & Engineering, she has published several research papers in International & National Conferences. She is also an MBA in International Business. She has attended and organized several Workshops as well as Value Added Courses such as:
- Certification in Rational Application Development (RAD) from IBM,
- Certification in JAVA from Oracle.
Cryptography and Network Security
CRYPTOGRAPHY
AND
NETWORK SECURITY

By

AJAY RAJ PARASHAR
Assistant Professor, Department of IT
Hindustan College of Science & Technology,
Mathura (UP)

DEEPTI MITTAL
Assistant Professor, Department of IT
Hindustan College of Science & Technology,
Mathura (UP)

UNIVERSITY SCIENCE PRESS
(An Imprint of Laxmi Publications Pvt. Ltd.)
An ISO 9001:2008 Company
BENGALURU • CHENNAI • COCHIN • GUWAHATI • HYDERABAD
JALANDHAR • KOLKATA • LUCKNOW • MUMBAI • RANCHI • NEW DELHI
BOSTON (USA) • ACCRA (GHANA) • NAIROBI (KENYA)
CRYPTOGRAPHY AND NETWORK SECURITY

© by Laxmi Publications (P) Ltd.
All rights reserved including those of translation into other languages. In accordance with the Copyright (Amendment) Act, 2012, no part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise. Any such act or scanning, uploading, and or electronic sharing of any part of this book without the permission of the publisher constitutes unlawful piracy and theft of the copyright holder’s intellectual property. If you would like to use material from the book (other than for review purposes), prior written permission must be obtained from the publishers.

Printed and bound in India
Typeset at J.R. Enterprises, Delhi
First Edition: 2015

Limits of Liability/Disclaimer of Warranty: The publisher and the author make no representation or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties. The advice, strategies, and activities contained herein may not be suitable for every situation. In performing activities adult supervision must be sought. Likewise, common sense and care are essential to the conduct of any and all activities, whether described in this book or otherwise. Neither the publisher nor the author shall be liable or assumes any responsibility for any injuries or damages arising here from. The fact that an organization or Website if referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Website may provide or recommendations it may make. Further, readers must be aware that the Internet Websites listed in this work may have changed or disappeared between when this work was written and when it is read.

All trademarks, logos or any other mark such as Vibgyor, USP, Amanda, Golden Bells, Firewall Media, Mercury, Trinity, Laxmi appearing in this work are trademarks and intellectual property owned by or licensed to Laxmi Publications, its subsidiaries or affiliates. Notwithstanding this disclaimer, all other names and marks mentioned in this work are the trade names, trademarks or service marks of their respective owners.
This book is dedicated to our
Mata Kaila Devi, Mata Chamunda Devi
&
Lord Shiva
&
Loving Parents and Family,
Only because of their love and blessings we make this goal possible.
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to Symmetric Encryption</td>
<td>1-35</td>
</tr>
<tr>
<td>Security Attacks, Mechanisms and Services</td>
<td>1</td>
</tr>
<tr>
<td>Cryptography</td>
<td>2</td>
</tr>
<tr>
<td>Cryptanalysis</td>
<td>3</td>
</tr>
<tr>
<td>Substitution Techniques</td>
<td>3</td>
</tr>
<tr>
<td>Caesar Cipher</td>
<td>3</td>
</tr>
<tr>
<td>Mono-alphabetic Ciphers</td>
<td>4</td>
</tr>
<tr>
<td>Playfair Cipher</td>
<td>4</td>
</tr>
<tr>
<td>Hill Cipher</td>
<td>5</td>
</tr>
<tr>
<td>Polyalphabetic Ciphers</td>
<td>6</td>
</tr>
<tr>
<td>One-Time Pad</td>
<td>7</td>
</tr>
<tr>
<td>Transposition Techniques</td>
<td>7</td>
</tr>
<tr>
<td>Steganography</td>
<td>8</td>
</tr>
<tr>
<td>Block Cipher Principles</td>
<td>8</td>
</tr>
<tr>
<td>The Feistel Cipher</td>
<td>11</td>
</tr>
<tr>
<td>Feistel Cipher Structure</td>
<td>11</td>
</tr>
<tr>
<td>Feistel Decryption Algorithm</td>
<td>12</td>
</tr>
<tr>
<td>Data Encryption Standard (DES)</td>
<td>14</td>
</tr>
<tr>
<td>Initial Permutation</td>
<td>15</td>
</tr>
<tr>
<td>The Strength of DES</td>
<td>16</td>
</tr>
<tr>
<td>Double DES</td>
<td>17</td>
</tr>
<tr>
<td>Reduction to a Single Stage</td>
<td>17</td>
</tr>
<tr>
<td>Meet-in-the-Middle Attack</td>
<td>17</td>
</tr>
<tr>
<td>Triple DES with Two Keys</td>
<td>17</td>
</tr>
<tr>
<td>Block Cipher Modes of Operation</td>
<td>18</td>
</tr>
<tr>
<td>Electronic Codebook Mode</td>
<td>18</td>
</tr>
<tr>
<td>Cipher Block Chaining Mode</td>
<td>19</td>
</tr>
<tr>
<td>Cipher Feedback Mode</td>
<td>19</td>
</tr>
<tr>
<td>Output Feedback Mode</td>
<td>20</td>
</tr>
<tr>
<td>Counter Mode</td>
<td>21</td>
</tr>
<tr>
<td>Traffic Confidentiality</td>
<td>22</td>
</tr>
<tr>
<td>Link Encryption Approach</td>
<td>22</td>
</tr>
</tbody>
</table>

(vii)
End-to-End Encryption Approach 23
Key Distribution 23
Hierarchical Key Control 25
Session Key Lifetime 25
A Transparent Key Control Scheme 25
Decentralized Key Control 26
Controlling Key Usage 27
Random Number Generation 28
The Use of Random Numbers 28
Pseudorandom Number Generators (PRNGs) 28
Linear Congruential Generators 28
Cryptographically Generated Random Numbers 29
Blum Blum Shub Generator 31
*Solved Exercise* 31
*Unsolved Exercise* 34

**Groups, Rings and Fields** 36–73

Groups 36
Fields 37
Modular Arithmetic 38
Divisors 39
The Euclidean Algorithm 41
The RSA Algorithm 51
The Security of RSA 52
Key Management 53
Diffie-Hellman Key Exchange 57
Testing for Primality 60
Finding Primitive Roots 61
Elliptic Curves 62
ElGamal Encryption 63
Blowfish 64
International Data Encryption Standard [IDEA] 66
*Solved Exercise* 68
*Unsolved Exercise* 72

**Message Authentication and Hash Functions** 74–100

Authentication Requirements 74
Authentication Functions 74
Message Encryption 74
Message Authentication Code 75
Hash Function 77
Simple Hash Functions 79
Security of Hash Functions and Macs 80
Cryptanalysis 80
Preface

Too many engineers consider cryptography to be a sort of magic security dust that they can sprinkle over their hardware or software, and which will imbue those products with the mythical property of “security.” Security is only as strong as the weakest link, and the mathematics of cryptography is almost never the weakest link. The fundamentals of cryptography are important, but far more important are, how those fundamentals are implemented and used. You can argue whether the stake should be a mile or a mile-and-a-half high, but the attacker is simply going to walk around the stake. Security is a broad stockade: it’s the things around the cryptography that make the cryptography effective.

This book is intended for Professional cryptographers, presenting the techniques and algorithms of greatest interest to the current practitioner, along with the supporting motivation and background material. It also provides a comprehensive source from which to learn cryptography, serving both students and instructors.

Throughout each chapter, we emphasize the relationship between various aspects of cryptography. We believe this style of presentation allows a better understanding of how algorithms actually work. Each chapter was written to provide a self-contained treatment of one major topic. Collectively, however, the chapters have been designed and carefully integrated to be entirely complementary with respect to definitions, terminology, and notation. Furthermore, there is essentially no duplication of material across chapters; instead, appropriate cross-chapter references are provided where relevant.

—Authors
Acknowledgement

This book would not have been possible without the tremendous efforts put forth by our peers who have taken the time to read endless drafts and provide us with technical corrections, constructive feedback, and countless suggestions. In particular, the advice of our seniors has been invaluable, and it is impossible to attribute individual credit for their many suggestions throughout this book. Among our seniors, we would particularly like to thank:

Mr. Shankar Z. Thawkar (HOD-IT) & Mr. Munish Khanna (HOD-CSE).

In addition, we gratefully acknowledge the exceptionally large number of additional individuals who have helped improve the quality of this volume, by providing highly appreciated guidance on various matters. These individuals include:

Mr. Abhishek Bhardwaj & Mr. Vijay S. Katta, Asst. Professor (IT & CSE Deptt.).

We apologize to those whose names have inadvertently escaped this list. Special thanks are due to Dr. Rajan Mishra & Dr. Hema Mishra, who encouraged us to write this book. Their hard work contributed greatly to the quality of this book, and it was truly a pleasure working with them.

Any errors that remain are, of course, entirely our own. We would be grateful if readers who spot errors, missing references or credits, or incorrectly attributed results would contact us with details. It is our hope that this volume facilitates further advancement of the field, and that we have helped play a small part in this.

—Authors
CRYPTOGRAPHY AND NETWORK SECURITY
(As per Syllabus of Gautam Buddha Technical University, Lucknow)

(STRICTLY AS PER NEW SYLLABUS)

For B.Tech. [EIT-701 & ECS-084]

UNIT-I
Introduction to security attacks, services and mechanism, introduction to cryptography.
Conventional Encryption: Conventional encryption model, classical encryption techniques-substitution ciphers and transposition ciphers, cryptanalysis, stereography, stream and block ciphers.
Modern Block Ciphers: Block ciphers principals, Shannon’s theory of confusion and diffusion, fiestal structure, Data Encryption Standard(DES), strength of DES, differential and linear crypt analysis of DES, block cipher modes of operations, triple DES, IDEA encryption and decryption, strength of IDEA, confidentiality using conventional encryption, traffic confidentiality, key distribution, random number generation.

UNIT-II
Introduction to graph, ring and field, prime and relative prime numbers, modular arithmetic, Fermat’s and Euler’s theorem, primality testing, Euclid’s Algorithm, Chinese Remainder theorem, discrete logarithms.
Principals of public key crypto systems, RSA algorithm, security of RSA, key management, Diffie-Hellman key exchange algorithm, introductory idea of Elliptic curve cryptography, Elganel encryption.

UNIT-III
Message Authentication and Hash Function: Authentication requirements, authentication functions, message authentication code, hash functions, birthday attacks, security of hash functions and MACS, MD5 message digest algorithm, Secure hash algorithm(SHA).
Digital Signatures: Digital Signatures, authentication protocols, Digital Signature Standards (DSS), proof of digital signature algorithm.

UNIT-IV
Authentication Applications: Kerberos and X.509, directory authentication service, electronic mail security-pretty good privacy (PGP), S/MIME.
UNIT-V

System Security: Intruders, Viruses and related threads, firewall design principals, trusted systems.

For MCA [MCA-404]

UNIT-I


UNIT-II


UNIT-III


UNIT-IV


UNIT-V

Cryptography And Network Security

Publisher: Laxmi Publications
ISBN: 9789351382669
Author: Ajay Raj Parashar And Deepti Mittal

Type the URL: http://www.kopykitab.com/product/10354

Get this eBook