Cryptography and Information Security

Second Edition

V.K. Pachghare
Cryptography and Information Security
Second Edition

V.K. PACHGHARE
Associate Professor
Department of Computer Engineering and Information Technology
College of Engineering, Pune
(An Autonomous Institute of Government of Maharashtra)

PHI Learning Private Limited
Delhi-110092
2015
CRYPTOGRAPHY AND INFORMATION SECURITY, Second Edition
V.K. Pachghare

© 2015 by PHI Learning Private Limited, Delhi. All rights reserved. No part of this book may be reproduced in any form, by mimeograph or any other means, without permission in writing from the publisher.


The export rights of this book are vested solely with the publisher.

Fifth Printing (Second Edition) ... ... January, 2015

Published by Asoke K. Ghosh, PHI Learning Private Limited, Rimjhim House, 111, Patparganj Industrial Estate, Delhi-110092 and Printed by Mudrak, 30-A, Patparganj, Delhi-110091.
To
my parents,
my wife Archana
and
my daughter Samiksha
# Contents

Preface ........................................................................................................................................... xv
Acknowledgements ......................................................................................................................... xix

1. Introduction .................................................................................................................................. 1
   1.1 Security ......................................................................................................................... 1
   1.2 Elements of Information Security .............................................................................. 2
      1.2.1 Confidentiality ........................................................................................................ 2
      1.2.2 Integrity ................................................................................................................ 2
      1.2.3 Availability ............................................................................................................ 2
   1.3 Security Policy ................................................................................................................. 3
   1.4 Security Techniques ....................................................................................................... 3
   1.5 Steps for Better Security .............................................................................................. 4
   1.6 Category of Computer Security ................................................................................... 5
   1.7 The Operational Model of Network Security ............................................................. 6
   1.8 Security Services .......................................................................................................... 6
   1.9 Basic Network Security Terminology .......................................................................... 7
      1.9.1 Cryptography ......................................................................................................... 7
      1.9.2 Hacking ................................................................................................................ 8
      1.9.3 Encryption ............................................................................................................ 8
      1.9.4 Decryption ............................................................................................................ 8
      1.9.5 Cryptanalysis ....................................................................................................... 9
   1.10 Security Attacks ......................................................................................................... 9
      1.10.1 Passive Attack ..................................................................................................... 9
      1.10.2 Active Attack ................................................................................................... 10

Summary ...................................................................................................................................... 12
Exercises ...................................................................................................................................... 12
Multiple Choice Questions ......................................................................................................... 13
2. Data Encryption Techniques ................................................................. 14
  2.1 Introduction 14
  2.2 Encryption Methods 15
    2.2.1 Symmetric Encryption 15
    2.2.2 Asymmetric Encryption 16
  2.3 Cryptography 17
  2.4 Substitution Ciphers 17
    2.4.1 The Caesar Cipher 17
    2.4.2 Monoalphabetic Ciphers 18
    2.4.3 Playfair Cipher 19
    2.4.4 The Hill Cipher 22
    2.4.5 Polyalphabetic Ciphers 26
    2.4.6 One-time Pad or Vernam Cipher 28
  2.5 Transposition Ciphers 29
    2.5.1 Single Columnar Transposition 30
    2.5.2 Double Columnar Transposition 31
  2.6 Cryptanalysis 32
    2.6.1 Enumerate All Short Keywords 32
    2.6.2 Dictionary Attacks 33
  2.7 Steganography 34
    2.7.1 Applications 34
    2.7.2 Limitations 35

Solved Problems 35
Summary 44
Exercises 44
Multiple Choice Questions 45

3. Data Encryption Standards ................................................................. 47
  3.1 Introduction 47
  3.2 Block Ciphers 47
  3.3 Block Cipher Modes of Operation 48
    3.3.1 Electronic Code Book (ECB) Mode 48
    3.3.2 Cipher Block Chaining (CBC) Mode 49
    3.3.3 Feedback Mode 51
    3.3.4 Counter Mode 54
  3.4 Feistel Ciphers 56
  3.5 Data Encryption Standard 57
    3.5.1 Working of DES 58
    3.5.2 Cracking DES 64
  3.6 Triple DES 64
    3.6.1 Working of Triple DES 64
    3.6.2 Modes of Operation 65
  3.7 DES Design Criteria 65
    3.7.1 Design of S-box 65
  3.8 Other Block Ciphers 66
  3.9 Differential Cryptanalysis 66
3.10 Linear cryptanalysis 67
3.11 Weak Keys in DES Algorithms 67
Summary 70
Exercises 70
Multiple Choice Questions 71

4. Advanced Encryption Standard.......................................................................................... 72
4.1 Introduction 72
4.2 Advanced Encryption Standard (AES) 73
4.3 Overview of Rijndael 73
4.4 Key Generation 74
  4.4.1 Round Constant 76
4.5 Encryption 77
  4.5.1 Initial Round 78
  4.5.2 Round 1 79
4.6 Decryption 84
  4.6.1 Initial Round 84
  4.6.2 Round 1 84
4.7 Galois Field of Multiplication 86
4.8 Advantages of AES 88
4.9 Comparison of AES with Other Ciphers 89
Solved Problems 89
Summary 95
Exercises 95
Multiple Choice Questions 96

5. Symmetric Ciphers ................................................................................................................. 97
5.1 Introduction 97
5.2 Blowfish Encryption Algorithm 97
  5.2.1 Key Expansion 98
  5.2.2 Encryption 99
  5.2.3 Blowfish Architecture 101
  5.2.4 Cryptanalysis of Blowfish 102
5.3 RC5 102
  5.3.1 Characteristics of RC5 103
  5.3.2 Parameters 104
  5.3.3 Cipher Modes in RC5 105
5.4 RC4 106
  5.4.1 Design 106
  5.4.2 Characteristics 106
  5.4.3 Algorithms 106
5.5 RC6 107
  5.5.1 Parameters of RC6 108
  5.5.2 Basic Operations 108
  5.5.3 Working of RC6 109
5.6 Comparison between RC6 and RC5 109
5.7 IDEA 110
   5.7.1 Working of IDEA 111
   5.7.2 Decryption 114
   5.7.3 Security 115

Solved Problems 115
Summary 128
Exercises 128
Multiple Choice Questions 129

6. Number Theory................................................................................................................. 130
   6.1 Introduction 130
   6.2 Prime Numbers 130
      6.2.1 Relative Prime Numbers 131
   6.3 Modular Arithmetic 131
      6.3.1 Properties 132
   6.4 Fermat’s Theorem 134
      6.4.1 An Application of Fermat’s Little Theorem and Congruence 136
   6.5 Euler’s Theorem 138
      6.5.1 The General Formula to Compute $\phi(n)$ 139
   6.6 Euclidean Algorithm 143
      6.6.1 Extended Euclidean Algorithm 145
   6.7 Primality Test 151
      6.7.1 Naïve Methods 151
      6.7.2 Probabilistic Tests 152
      6.7.3 Fermat Primality Test 152
      6.7.4 Miller–Rabin Primality Test 153
      6.7.5 Agrawal, Kayal and Saxena Primality Test (AKS Test) 153
   6.8 Chinese Remainder Theorem 154
   6.9 Discrete Logarithms 158
      6.9.1 Index Calculus Algorithm 159

Summary 160
Exercises 160
Multiple Choice Questions 161

7. Public Key Cryptosystems........................................................................................................ 162
   7.1 Introduction 162
   7.2 Public Key Cryptography 163
      7.2.1 Authentication, Secrecy and Confidentiality 165
      7.2.2 Key Length and Encryption Strength 168
      7.2.3 Applications of Public Key Cryptography 168
      7.2.4 Strength and Weakness of Public Key 169
      7.2.5 Comparison of Asymmetric Encryption and Symmetric Encryption 169
   7.3 RSA Algorithm 169
      7.3.1 Working of RSA 169
      7.3.2 Key Length 172
      7.3.3 Security 172
8. **Key Management** .................................................................................................................. 178

8.1 Introduction 178
8.2 Key Distribution 178
  8.2.1 Public Announcement 179
  8.2.2 Publicly Available Directory 179
  8.2.3 Public Key Authority 180
  8.2.4 Public Key Certificates 181
8.3 Diffie–Hellman Key Exchange 182
  8.3.1 Description 183
  8.3.2 Security 185
  8.3.3 Man-in-the-Middle Attack 185
  8.3.4 Authentication 186
8.4 Elliptic Curve Arithmetic 186
  8.4.1 Elliptic Curve Groups Over Real Numbers 187
  8.4.2 Elliptic Curve Addition: A Geometric Approach 187
  8.4.3 Elliptic Curve Addition: An Algebraic Approach 190
  8.4.4 Elliptic Curve Groups over $F_p$ 190
  8.4.5 Arithmetic in an Elliptic Curve Group over $F_p$ 191
  8.4.6 Elliptic Curve Groups over $F_{2^n}$ 192
  8.4.7 Arithmetic in an Elliptic Curve Group over $F_{2^m}$ 192
8.5 Elliptic Curve Cryptography (ECC) 193
  8.5.1 Elliptic Curve Diffie–Hellman 193
  8.5.2 Key Establishment Protocol 193
8.6 Elliptic Curve Security and Efficiency 194
8.7 Zero-Knowledge Proof 195
  8.7.1 Cave Story 196

9. **Authentication** ...................................................................................................................... 202

9.1 Introduction 202
  9.1.1 Objectives 202
  9.1.2 Measurements 203
9.2 Authentication Methods 204
  9.2.1 Password-based Authentication Method 204
  9.2.2 Two-factor Authentication Method 206
  9.2.3 Biometric Authentication Method 206
  9.2.4 Extensible Authentication Protocol (EAP) 208
9.3 Message Digest 210
  9.3.1 MD2 210