CRYPTOGRAPHY AND NETWORK SECURITY

Dr. H. Shaheen
(*Associate Professor, CSE Department*)
St. Peter's Engineering College, Hyderabad, (Telangana), INDIA

Dr. T. Sreenivasulu
(*Professor, CSE Department*)
St. Peter's Engineering College, Hyderabad, (Telangana), INDIA

Ms. V. Soniya
(*Assistant Professor, CSE Department*)
St. Peter's Engineering College, Hyderabad, (Telangana), INDIA

CRYPTOGRAPHY AND NETWORK SECURITY

Copyright © : Dr. H. Shaheen
Publishing Right ℗ : VSRD Academic Publishing
A Division of Visual Soft India Private Limited

ISBN-13: 978-93-87610-31-6

FIRST EDITION, JANUARY 2019, INDIA

Printed & Published by:

VSRD Academic Publishing

A Division of Visual Soft India Private Limited

Disclaimer: The author(s) are solely responsible for the contents compiled in this book. The publishers or its staff do not take any responsibility for the same in any manner. Errors, if any, are purely unintentional and readers are requested to communicate such errors to the Authors or Publishers to avoid discrepancies in future.

Printed & Bound in India

VSRD ACADEMIC PUBLISHING
A Division of Visual Soft (India) Pvt. Ltd.

REGISTERED OFFICE
154, Tezabmill Campus, Anwarganj, KANPUR – 208 003 (UP) (INDIA)
Mob.: +91 9899936803 ||Web.: www.vsrdpublishing.com || Email: vsrdpublishing@gmail.com

MARKETING OFFICE
340, First Floor, Adarsh Nagar, Oshiwara, Andheri(W), MUMBAI – 400 053 (MH) (INDIA)
Mob.: +91 9956127040 || Web.: www.vsrdpublishing.com || Email: vsrdpublishing@gmail.com

PREFACE

This book entitled **"Cryptography and Network Security"** has been written in accordance with the syllabus prescribed by the 'JNTUH R2016' for the Third Year, B.Tech students of Engineering Colleges affiliated to JNTUH.

This book comprises of five chapters which covers Jawaharlal Nehru Technological University, Hyderabad syllabus. The main emphasis of the book is to explain in a simple manner, the logical concepts that will enable even the beginners to understand them without difficulty.

Systematic care has been taken to support the topics with necessary illustrations and relevant diagrams to make learning much easier. It is believed that this book shall serve all the requirements of Final Year Engineering students.

It covers all the important questions that have appeared in the previous years of Jawaharlal Nehru Technological University, Hyderabad Examinations. University questions for regulations R2016 are given at the end.

Your suggestions are most welcome.

✍ *Authors*

ACKNOWLEDGEMENT

We sincerely thank the Almighty for being with us through all stages of the preparation of this book.

Firstly, we would like to express our sincere gratitude to **The Chairman T.Bala Reddy, St.Peters Engineering College** for the continuous support motivation, and immense knowledge.

Special Acknowledgement is due to our **Secretary Mr. T.V. Reddy, St.Peters Engineering College** for his continuous support for the successful completion of this book.

We thank **Dr. M. Narendra Kumar, Principal, St.Peters Engineering College** for his source of inspiration.

We thank **Dr.M.Sharada Varalakshmi, Head of the Department** who have always supported and motivated us to accomplish this incredible work.

We thank our Friends and Colleagues for their encouragement and support in various stages of writing this book.

We express our sincere thanks to our publisher **VSRD Academic Publishing (A Division of Visual Soft India Private Limited)**, for their help and co-operation in publishing this book.

✍ *Authors*

CONTENTS

CHAPTER 1 : SECURITY CONCEPTS, CRYPTOGRAPHY CONCEPTS AND TECHNIQUES

1.1. INTRODUCTION 2

1.2. WHY WE NEED INFORMATION SECURITY? BECAUSE THERE ARE THREATS. 2

1.3. SECURITY ATTACK 4

1.4. ACTIVE ATTACK 5

1.5. SECURITY SERVICES 6

1.6. SECURITY MECHANISMS 7

1.7. MODEL FOR NETWORK SECURITY 9

1.8. CRYPTOGRAPHY CONCEPTS AND TECHNIQUES 10

1.9. CRYPTANALYSIS 10

1.10. CLASSICAL ENCRYPTION TECHNIQUES 11

1.11. HILL CIPHER 13

1.12. TRANSPOSITION TECHNIQUES 15

1.13. ENCRYPTION AND DECRYPTION 16

1.14. SYMMETRIC AND ASYMMETRIC KEY CRYPTOGRAPHY 16

1.15. STEGANOGRAPHY 17

1.16. KEY TYPES AND KEY SIZE 17

1.17. POSSIBLE TYPES OF ATTACKS BRUTE FORCE ATTACK 18

1.18. REPLAY ATTACK 18

1.19. MAN IN THE MIDDLE ATTACK 18

1.20. IMPLEMENTATION ATTACK 18

1.21. STATISTICAL ATTACK 19

1.22. FREQUENCY ANALYSIS AND THE CIPHERTEXT ONLY ATTACK 19

1.23. KNOWN PLAINTEXT 19

CHAPTER 2 : SYMMETRIC AND ASYMMETRIC KEY CIPHERS

2.1. BLOCK CIPHER PRINCIPLES AND ALGORITHM 20

2.2. DATA ENCRYPTION STANDARD (DES) 23

2.3. ADVANCED ENCRYPTION STANDARD ALGORITHM (AES) 27

2.4. BLOWFISH ALGORITHM 31

2.5. RC5 33

2.6. IDEA(INTERNATIONAL DATA ENCRYPTION ALGORITHM) 34

2.7. BLOCK CIPHER MODES OF OPERATIONS 37

2.8. STREAM CIPHERS 41

2.9. RC4 41

2.10. PUBLIC KEY CRYPTOGRAPHY 43

2.11. RSA ALGORITHM 46
2.12. ELGAMAL CRYPTOGRAPHY 49
2.13. DIFFIE-HELLMAN KEY EXCHANGE 50
2.14. KNAPSACK ALGORITHM 52

CHAPTER 3 : CRYPTOGRAPHIC HASH FUNCTIONS, MESSAGE AUTHENTICATION CODES, KEY MANAGEMENT AND DISTRIBUTION

3.1. CRYPTOGRAPHIC HASH FUNCTIONS: MESSAGE AUTHENTICATION 56
3.2. SECURE HASH ALGORITHM 56
3.3. MESSAGE AUTHENTICATION CODE 60
3.4. HMAC 62
3.5. CMAC 66
3.6. DIGITAL SIGNATURE 67
3.7. ELGAMAL DIGITAL SIGNATURES 69
3.8. SYMMETRIC KEY DISTRIBUTION USING SYMMETRIC ENCRYPTION 69
3.9. SYMMETRIC KEY DISTRIBUTION USING ASYMMETRIC ENCRYPTION 76
3.10. DISTRIBUTION OF PUBLIC KEYS 77
3.11. KERBEROS 79
3.12. X.509 AUTHENTICATION SERVICE 85
3.13. PUBLIC KEY INFRASTRUCTURE 87

CHAPTER 4 : TRANSPORT LEVEL SECURITY AND WIRELESS NETWORK SECURITY

4.1. WEB SECURITY CONSIDERATIONS 89
4.2. SECURE SOCKET LAYER/TRANSPORT LAYER SECURITY 91
4.3. TRANSPORT LAYER SECURITY 97
4.4. HTTPS 98
4.5. WIRELESS NETWORK SECURITY 101
4.6. MOBILE DEVICE SECURITY 102
4.7. WIFI OPERATION 102
4.8. IEEE 802.11 WIRELESS LAN 102

CHAPTER 5 : EMAIL SECURITY, CASE STUDIES ON CRYPTOGRAPHY AND SECURITY

5.1. E-MAIL SECURITY 106
5.2. S/MIME 113
5.3. RFC 822 113
5.4. IP SECURITY 117
5.5. IP SECURITY ARCHITECTURE 119

5.7. ENCAPSULATING SECURITY PAYLOAD 124
5.8. COMBINING SECURITY ASSOCIATIONS 127
5.9. INTERNET KEY EXCHANGE (IKE)........ 129
5.10. KEY MANAGEMENT 129
5.11. ISAKMP........ 131
5.12. CASE STUDIES ON CRYPTOGRAPHY AND SECURITY 134

CHAPTER 6 : QUESTION BANK
6.1. QUESTION PAPER NOVEMBER / DECEMBER 2016 143
6.2. QUESTION PAPER NOVEMBER / DECEMBER 2017 144