

INFORMATION SECURITY

Dr. H. Shaheen

(Associate Professor)

Department of Computer Science & Engineering
ST. PETER'S ENGINEERING COLLEGE
Hyderabad, Telangana, INDIA.

Ms. Deepthi Reddy

(Assistant Professor)

Department of Computer Science & Engineering
ST. PETER'S ENGINEERING COLLEGE
Hyderabad, Telangana, INDIA.

INFORMATION SECURITY

Copyright © : Dr. H. Shaheen
Publishing Rights © : VSRD Academic Publishing
A Division of Visual Soft India Pvt. Ltd.

ISBN-13: 978-93-86258-96-0
FIRST EDITION, MARCH 2018, INDIA

Printed & Published by:
VSRD Academic Publishing
(A Division of Visual Soft India Pvt. Ltd.)

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.

All rights reserved. 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, without the prior permission of the Publishers & Author.

Printed & Bound in India

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

REGISTERED OFFICE

154, Tezabmill Campus, Anwarganj, KANPUR – 208003 (UP) (IN)
Mb: 98999 36803, Web: www.vsrdpublishing.com, Email: vsrdpublishing@gmail.com

MARKETING OFFICE

340, FF, Adarsh Nagar, Oshiwara, Andheri(W), MUMBAI–400053 (MH)(IN)
Mb: 99561 27040, Web: www.vsrdpublishing.com, Email: vsrdpublishing@gmail.com

P R E F A C E

This book entitled “**Information Security**” has been written in accordance with the syllabus prescribed by the ‘JNTUH R2013’ 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 Third 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 R2013 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 **The Chairman T.BalaReddy, St.Peters Engineering College** for the continuous support motivation, and immense knowledge.

Special Acknowledgements are 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.

Our thanks to the **Head of the Department, Dr. M. Raja** for his constant source of encouragement 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 ONE

COMPUTER SECURITY AND CRYPTOGRAPHY 1

1.1	INTRODUCTION.....	3
1.2	WHY WE NEED INFORMATION SECURITY?	3
1.3	ASPECTS OF SECURITY.....	4
1.3.1	SECURITY ATTACK	5
1.3.2	SECURITY SERVICES.....	6
1.3.3	SECURITY MECHANISMS	8
1.4	MODEL FOR NETWORK SECURITY.....	9
1.4.1	CRYPTOGRAPHY.....	11
1.4.2	CRYPTANALYSIS	11
1.5	CLASSICAL ENCRYPTION TECHNIQUES.....	11
1.7	STEGANOGRAPHY	17
1.8	KEY TYPES AND KEY SIZE	18

CHAPTER TWO

SYMMETRIC & ASYMMETRIC KEY CIPHERS 19

2.1	BLOCK CIPHER PRINCIPLES AND ALGORITHM.....	21
2.1.1	BLOCK CIPHER SCHEMES.....	21
2.1.2	BLOCK VS STREAM CIPHERS	21
2.2	FEISTEL CIPHER STRUCTURE	22
2.3	CONVENTIONAL ENCRYPTION PRINCIPLES	24
2.4	DEFINITIONS.....	25
2.4.1	SIMPLIFIED DATA ENCRYPTION STANDARD (S-DES)	26
2.4.2	DATA ENCRYPTION STANDARD (DES)	30
2.4.3	WORKING OF DES	31
2.5	STRUCTURE OF DES	32
2.6	DETAILS OF INDIVIDUAL ROUNDS	34
2.6.1	S-BOX DESCRIPTION.....	35
2.6.2	ADVANCED ENCRYPTION STANDARD ALGORITHM (AES).....	36

2.6.3	BLOWFISH ALGORITHM	40
2.8	LINEAR CRYPTANALYSIS	44
2.9	BLOCK CIPHER MODES OF OPERATIONS.....	44
2.10	STREAM CIPHERS	48
2.10.1	RC4.....	49
2.11	PLACEMENT OF ENCRYPTION.....	51
2.12	PUBLIC KEY CRYPTOGRAPHY	52
2.12.1	RSA ALGORITHM.....	56
2.12.2	DIFFIE-HELLMAN KEY EXCHANGE	59
2.12.3	ELLIPTIC CURVE CRYPTOGRAPHY (ECC).....	61
2.13	KEY MANAGEMENT.....	64

CHAPTER THREE

MESSAGE AUTHENTICATION ALGORITHMS AND

HASH FUNCTION..... 69

3.1	MESSAGE AUTHENTICATION	71
3.2	MESSAGE ENCRYPTION	72
3.3	MESSAGE AUTHENTICATION CODE	73
3.3.1	MESSAGE AUTHENTICATION CODE BASED ON DES.....	74
3.4	HASH FUNCTION	75
3.5	MD5 - MESSAGE DIGEST ALGORITHM	77
3.6	SECURE HASH ALGORITHM	81
3.6.1	WHIRLPOOL HASH FUNCTION	83
3.7	WHIRLPOOL OVERVIEW	84
3.8	HMAC.....	85
3.9	CMAC.....	89
3.10	DIGITAL SIGNATURE.....	90
3.10.1	DIGITAL SIGNATURE STANDARD (DSS).....	91
3.11	KNAPSACK ALGORITHM	92
3.12	AUTHENTICATION APPLICATIONS	95
3.12.1	KERBEROS.....	95
3.13	KERBEROS VERSION 4	96
3.15	X.509 AUTHENTICATION SERVICE.....	100

3.16	AUTHENTICATION PROCEDURES	103
3.17	PUBLIC KEY INFRASTRUCTURE.....	104
3.18	BIOMETRIC AUTHENTICATION	106

CHAPTER FOUR

EMAIL PRIVACY AND IP SECURITY..... 109

4.1	PRETTY GOOD PRIVACY.....	111
4.4	IP SECURITY OVERVIEW.....	122
	4.4.1 IP SECURITY ARCHITECTURE.....	124
4.5	SECURITY ASSOCIATIONS	126
4.6	AUTHENTICATION HEADER	127
4.7	ENCAPSULATING SECURITY PAYLOAD	131
4.8	KEY MANAGEMENT.....	134
	4.8.1 OAKLEY KEY DETERMINATION PROTOCOL.....	135
	4.8.2 ISAKMP.....	137

CHAPTER FIVE

WEB SECURITY, VIRUS, FIREWALLS,

CRYPTOGRAPHY AND SECURITY..... 141

5.1	WEB SECURITY CONSIDERATIONS	143
5.2	SECURE SOCKET LAYER.....	144
5.3	TRANSPORT LAYER SECURITY	151
5.4	SET (SECURE ELECTRONIC TRANSACTION).....	153
	5.4.1 DUAL SIGNATURE.....	155
5.5	INTRUDERS.....	157
5.6	INTRUSION DETECTION	158
5.7	VIRUSES AND RELATED THREATS.....	159
	5.7.1 VIRUS COUNTERMEASURES	164
5.8	PASSWORD MANAGEMENT	167
5.9	FIREWALLS	169
5.10	CASE STUDIES ON CRYPTOGRAPHY AND SECURITY	176
	5.10.1 SECURE INTER-BRANCH PAYMENT TRANSACTIONS.....	176

5.10.2 CROSS SITE SCRIPTING VULNERABILITY (CSSV)	180
5.10.3 VIRTUAL ELECTIONS.....	183