UCS1505 INTRODUCTION TO CRYPTOGRAPHIC TECHNIQUES 3 0 0 3

OBJECTIVES

• To understand the classical and symmetric cryptographic techniques

• To study about message authentication and hash functions

• To learn number theory fundamentals needed by cryptographic algorithms

• To understand the various key distribution and management schemes

• To understand the concepts of Public key cryptography and digital signatures.

UNIT I INTRODUCTION AND CLASSICAL CRYPTOGRAPHY AND SYMMENTRIC CRYPTOGRAPHY 10

Cryptography and Modern Cryptography -- Setting of Private-Key Encryption – Historical Ciphers -- Basic Principles; Perfectly Secret Encryption; Private-Key Encryption and Pseudo randomness.

UNIT II MESSAGE AUTHENTICATION CODES AND COLLISION-RESISTANT HASH FUNCTIONS 8

Secure Communication and Message Integrity -- Encryption vs. Message Authentication -- Message Authentication Codes -- Constructing Secure Message Authentication Codes – CBCMAC Collision-Resistant Hash Functions – NMAC and HMAC – Constructing CCA-Secure Encryption Schemes Obtaining Privacy and Message Authentication.

UNIT III BLOCK CIPHERS 10

Substitution-Permutation Networks -- Feistel Networks -- DES -- AES -- Differential and Linear Cryptanalysis; One-Way Functions -- From One-Way Functions to Pseudo randomness -- Constructing Pseudorandom Generators -- Constructing Pseudorandom Permutations -- Necessary Assumptions for Private-Key Cryptography.

UNIT IV NUMBER THEORY & KEY DISTRIBUTION 8

Number Theory: Preliminaries and Basic Group Theory -- Primes, Factoring, and RSA -- Cryptographic Applications of Number-Theoretic Assumptions; Private-Key Management and the Public-Key Revolution: Limitations of Private-Key Cryptography -- Key Distribution Centers -- The Public-Key Revolution -- Diffie-Hellman Key Exchange.

UNIT V PUBLIC-KEY ENCRYPTION & DIGITAL SIGNATURE 9

Public-Key Encryption – An Overview -- Definitions -- Hybrid encryption -- RSA encryption – The El Gamal Encryption Scheme -- Security Against Chosen-Ciphertext Attacks; DigitalSignatures Schemes: An Overview -- Definitions -- RSA Signatures -- The Hash-and-Sign Paradigm -- Lamport's One-Time Signature Scheme -- Signatures from Collision – Resistant Hashing -- The Digital Signature Standard -- Certificates and Public-Key Infrastructures; Authentication Protocol: SSL and TLS.

TOTAL PERIODS: 45

OUTCOMES

On successful completion of this course, the student will be able to:

• Describe and implement classical and symmetric ciphers (K2)

• Describe the authentication schemes and hash algorithms (K2)

• Understand the number theoretic foundations of cryptography (K3)

• Compare and contrast various Public key cryptographic techniques (K3)

• Illustrate various Public key cryptographic techniques (K3).

TEXTBOOKS

1. Jonathan Katz, YehudaLindell, “Introduction to Modern Cryptography”,2nd Edition

(Chapman & Hall/CRC Cryptography and Network Security Series), 2014.

2. Wenbo Mao, “Modern Cryptography – Theory and Practice”, Pearson Education, 2004.

REFERENCE BOOKS

1. Johannes A Buchmann, “Introduction to Cryptography”, 2nd edition, Pearson Education,

Springer, 2009.

2. Charles P Pfleeger, Shari Lawrence Pfleeger, “Security in computing”, 3rd Edition,Prentice Hall of India,2006.

3. Bruce Schneier,Neils Ferguson, “Practical Cryptography”,1st Edition, Wiley Dreamtech

India Pvt Ltd, 2003.

4. http://nptel.ac.in/courses/106105031/lecture by Dr Debdeep Mukhopadhyay, IIT

Kharagpur.