Cryptography

Theory L/T (Hours per week): 4/0, Credit: 4

MODULE-I

Introduction to Cryptography: Basics of Symmetric Key Cryptography, Basics of Assymetric Key Cryptography, Hardness of Functions

Notions of Semantic Security (SS) and Message Indistinguishability (MI): Proof of Equivalence of SS and MI, Hard Core Predicate, Trap-door permutation, Goldwasser-Micali Encryption.

MODULE-II

Goldreich-Levin Theorem: Relation between Hardcore Predicates and Trap-door permutations

Formal Notions of Attacks: Attacks under Message Indistinguishability: Chosen Plaintext Attack(IND-CPA), Chosen Ciphertext Attacks (IND-CCA1 and INDCCA2), Attacks under Message Non-malleability: NM-CPA and NM-CCA2, Interrelations among the attack model

Random Oracles: Provable Security and asymmetric cryptography, hash functions

One-way functions: Weak and Strong one way functions

MODULE-III

Pseudo-random Generators (PRG): Blum-Micali-Yao Construction, Construction of more powerful PRG, Relation between One-way functions and PRG, Pseudorandom Functions (PRF)

Building a Pseudorandom Permutation: The LubyRackoff Construction: Formal Definition, Application of the LubyRackoff Construction to the construction of Block Ciphers, The DES in the light of LubyRackoff Construction

Left or Right Security (LOR)

MODULE-IV

Message Authentication Codes (MACs): Formal Definition of Weak and Strong MACs, Using a PRF as a MAC, Variable length MAC

Public Key Signature Schemes: Formal Definitions, Signing and Verification, Formal Proofs of Security of Full Domain Hashing

Assumptions for Public Key Signature Schemes: One way functions Imply Secure One-time Signatures Shamir's Secret Sharing Scheme Formally Analyzing Cryptographic Protocols Zero Knowledge Proofs and Protocols

REFERENCE BOOKS:

1. Y. Daniel Liang**:** Introduction to JAVA Programming, 6th Edition, Pearson, 2007.

2. Chris Bates: Web Programming Building Internet Applications, 3rd Edition, Wiley India, 2006.

3. XueBai et al: The Web Warrior Guide to Web Programming, Thomson, 2003.

4. Hans Delfs and Helmut Knebl, Introduction to Cryptography: Principles and Applications, Springer Verlag.