SUBJECT NO-CS60088, SUBJECT NAME- FOUNDATIONS OF CRYPTOGRAPHY

LTP- 3-1-0,CRD- 4

SYLLABUS :-

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

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 IND-CCA2), Attacks under Message Non-malleability: NM-CPA and NM-CCA2, Inter-relations among the attack model

Random Oracles: Provable Security and asymmetric cryptography, hash functions

One-way functions: Weak and Strong one way functions

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

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

Left or Right Security (LOR)

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

Shamirs Secret Sharing Scheme

Formally Analyzing Cryptographic Protocols

Zero Knowledge Proofs and Protocols

References

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

2. Wenbo Mao, Modern Cryptography, Theory and Practice, Pearson Education (Low Priced Edition)

3. Shaffi Goldwasser and Mihir Bellare, Lecture Notes on Cryptography, Available at http://citeseerx.ist.psu.edu/.

4. Oded Goldreich, Foundations of Cryptography, CRC Press (Low Priced Edition Available), Part 1 and Part 2