05 1x18 CRYPTOGRAPHY Credit : 3

1. Introduction : The OSI Security Architecture, Security attack, Security Services, Security Mechanism, A model for Network Security. Lecture : 4

2. Symmetric Cipher : Classical Encryption Techniques, Symmetric Cipher Model, Block Cipher Principles, DES,

Cryptanalysis, Block Cipher Design Principle, The Euclidean Algorithm, Finite field of Form GP(p), Advance

Encryption Standard (AES), AES Cipher, Multiple Encryption and Triple DES, Stream, Placement of Encryption

Function, Traffic Confidentiality, Key Distribution, Random number generation. Lecture
: 15

3. Public Key Encryption and Hash Function : Fermat's & Euler's Theorems, The Chinese Remainder Theorem,

RSA Algorithm, Diffe-Hellman Key Exchange, Elliptic Curve Cryptography, Massage authentication code, Security of

Hash Functions and MAACs, Secure Hash algorithm, Whirlpool, HMAC, CMAC, Digital Signature. Lecture : 12

4. Network Security Applications : Kerberos, X.509 Authentication Service, S/MIME, IP Security Architecture,

Encapsulating Security Payload, Secure Socket Layer (SSL), Transport layer security, Secure Electronic Transaction.

Lecture : 6

5. System Security : Intrusion detection, Password Management, Virus
countermeasure, Denial of Service Attack,

Firewall design principles, Trusted System. Lecture

: 6

Text Book :

1. Cryptography and Network Security : Principle and Practice, 4e by William Stalling, Pearson Education/PHI.

Reference Books :

1. Beginning Cryptography with Java by David Hook, Wiley Dreamtech.
2. Modern Cryptography Theory & Practices by Wenbo Mao, Pearson Education.
3. Cryptography for Database and Internet Application by Nick Galbreath, Wiley Dreamtech.
4. Network Security : Private Communication in a Public World, 2e, by Charlie Kaufman, Radia Perlman and

Mike Speciner, Pearson Education.