PET6J009 CRYPTOGRAPHY AND NETWORK SECURITY

MODULE-I

Security Problems- Security problem in computing; Security Attacks; Security Services; Security Mechanisms; OSI security attack-Standards and standard setting organizations.

MODULE-II

Data Security- Basic encryption and decryption; Substitution, Transposition, Block ciphers, Data encryption, standard encryption and decryption; Differential and linear crypto analysis; Advanced encryption; Block cipher models-Triple DES with two keys-Stream cipher, RC4- RSA algorithm, Diffie-Hellman key exchange algorithm.

MODULE- III

Network Security- IP security overview, IP security architecture, Authentication header, Encapsulating security pay load, combining security association, Key management-Web security considerations, Secure socket layer, Secure electronic transaction.

MODULE- IV

Message Authentication- Hash Functions, MD5-Hash algorithm, SHA 512 logic; Authentication Protocols, Digital signature standards.

ADDITIONAL MODULE (TERMINAL EXAMINATION-INTERNAL)

System Security: Intruders and intrusion detection-Malicious software, Viruses and related threats, virus counter measures, distributed denial of services attack-Firewalls design principles-Trusted systems.

TEXT BOOKS

1. Cryptography and Network Security – Principles & Practice, William Stallings, Pearson Education, 3rd edition, 2002.
2. Everyday Cryptography- Fundamental Principles and Applications, Keith M. Martin, Oxford University Press

REFERENCE BOOKS

1. Security in Computing, Charles P. Pleeger, PHI Learning, 1998.
2. Cryptography and Network Security, Behrouz Forouzan, Tata McGraw-Hill, 1st edition, 2007.
3. Cryptography & Network Security, Atul Kahate, TMH, 2nd edition, 2008.