

CS6701 CRYPTOGRAPHY AND NETWORK SECURITY

DETAILED SYLLABUS

UNIT I INTRODUCTION & NUMBER THEORY

Services, Mechanisms and attacks-the OSI security architecture-Network security model-Classical Encryption techniques (Symmetric cipher model, substitution techniques, transposition techniques, steganography). FINITE FIELDS AND NUMBER THEORY: Groups, Rings, Fields-Modular arithmetic Euclid's algorithm-Finite fields- Polynomial Arithmetic –Prime numbers-Fermat's and Euler's theorem Testing for primality -The Chinese remainder theorem-Discrete logarithms.

UNIT II BLOCK CIPHERS & PUBLIC KEY CRYPTOGRAPHY 10

Data Encryption Standard-Block cipher principles-block cipher modes of operation-Advanced Encryption Standard (AES)-Triple DES-Blowfish-RC5 algorithm. Public key cryptography: Principles of public key cryptosystems-The RSA algorithm-Key management - Diffie Hellman Key exchange Elliptic curve arithmetic-Elliptic curve cryptography.

UNIT III HASH FUNCTIONS AND DIGITAL SIGNATURES

Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC –MD5 - SHA - HMAC – CMAC - Digital signature and authentication protocols – DSS – El Gamal – Schnorr.

UNIT IV SECURITY PRACTICE & SYSTEM SECURITY

Authentication applications – Kerberos – X.509 Authentication services - Internet Firewalls for Trusted System: Roles of Firewalls – Firewall related terminology- Types of Firewalls - Firewall designs – SET for E-Commerce Transactions. Intruder – Intrusion detection system – Virus and related threats – Countermeasures – Firewalls design principles – Trusted systems – Practical implementation of cryptography and security.

UNIT V E-MAIL, IP & WEB SECURITY

E-mail Security: Security Services for E-mail-attacks possible through E-mail - establishing keys privacy-authentication of the source-Message Integrity-Non - repudiation-Pretty Good Privacy-S/MIME. IP Security: Overview of IPsec - IP and IPv6-Authentication Header-Encapsulation Security Payload (ESP)-Internet Key Exchange (Phases of IKE, ISAKMP/IKE Encoding). Web Security: SSL/TLS Basic Protocol-computing the keys- client authentication-PKI as deployed by SSL Attacks fixed in v3- Exportability-Encoding-Secure Electronic Transaction (SET).

OBJECTIVES:

The student should be made to:

- Understand OSI security architecture and classical encryption techniques.
- Acquire fundamental knowledge on the concepts of finite fields and number theory.
- Understand various block cipher and stream cipher models.

- Describe the principles of public key cryptosystems, hash functions and digital signature.

TEXT BOOKS:

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013. (UNIT I, II, III, IV).
2. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security", Prentice Hall of India, 2002. (UNIT V).

REFERENCES:

1. Behrouz A. Ferouzan, "Cryptography & Network Security", Tata Mc Graw Hill, 2007.
2. Man Young Rhee, "Internet Security: Cryptographic Principles", "Algorithms and Protocols", Wiley Publications, 2003.
3. Charles Pfleeger, "Security in Computing", 4th Edition, Prentice Hall of India, 2006.
4. Ulysess Black, "Internet Security Protocols", Pearson Education Asia, 2000.
5. Charlie Kaufman and Radia Perlman, Mike Speciner, "Network Security, Second Edition, Private Communication in Public World", PHI 2002.
6. Bruce Schneier and Neils Ferguson, "Practical Cryptography", First Edition, Wiley Dreamtech India Pvt Ltd, 2003.
7. Douglas R Simson "Cryptography – Theory and practice", First Edition, CRC Press, 1995.
8. <http://nptel.ac.in/>.