JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

IV Year B.Tech. Computer Science Engineering. I-Sem.

CRYPTOGRAPHY AND NETWORK SECURITY

UNIT-I:

Introduction: Security Attacks, Security Services, Security Mechanisms, and a Model for Network Security, Non-Cryptographic Protocol Vulnerabilities - DoS, DDoS, Session Hijacking and Spoofing, Software Vulnerabilities - Phishing, Buffer Overflow, Format String Attacks, SQL Injection, Basics of Cryptography - Symmetric Cipher Model, Substitution Techniques, Transportation Techniques, Other Cipher Properties - Confusion, Diffusion, Block and Stream Ciphers.

UNIT-II:

Secret Key Cryptography: Data Encryption Standard(DES), Strength of DES, Block Cipher Design Principles and Modes of Operations, Triple DES, International Data Encryption algorithm, Blowfish, CAST-128, AES

UNIT-III:

Number Theory: Prime and Relatively Prime Numbers, Modular Arithmetic, Fermat's and Euler's Theorems, the Chinese Remainder Theorem, Discrete Logarithms.

UNIT-IV:

Public Key Cryptography: Principles of Public Key Cryptosystems, RSA Algorithm, Diffie-Hellman Key Exchange, Introduction to Elliptic Curve Cryptography.

UNIT-V:

Cryptographic Hash Functions: Applications of Cryptographic Hash Functions, Secure Hash Algorithm, Message Authentication Codes - Message Authentication Requirements and Functions, HMAC, Digital signatures, Digital Signature Schemes, Authentication Protocols, Digital Signature Standards.

UNIT-VI:

Authentication Applications: Kerberos, Key Management and Distribution, X.509 Directory Authentication service, Public Key Infrastructure, Electronic Mail Security: Pretty Good Privacy, S/MIME.

UNIT-VII:

IP Security: Overview, Architecture, Authentication Header, Encapsulating Security Payload, Combining security Associations, Internet Key Exchange, Web Security: Web Security Considerations, Secure Sockets Layer and Transport Layer Security, Electronic Payment.

UNIT-VIII:

System Security: Intruders, Intrusion Detection, Password Management, Malicious Software - Types, Viruses, Virus Countermeasures, Worms, Firewalls - Characteristics, Types of Firewalls, Placement of Firewalls, Firewall Configuration, Trusted systems.

TEXT BOOKS:

1. Cryptography and Network Security: Principles and Practice, 5th Edition, William Stallings, Pearson Education, 2011.
2. Network Security and Cryptography, Bernard Menezes, Cengage Learning, 2011.
3. Cryptography and Network, 2nd Edition, Behrouz A. Fourouzan and Debdeep Mukhopadhyay, McGraw-Hill, 2010.

REFERENCE BOOKS:

1. Fundamentals of Network Security by Eric Maiwald (Dreamtech press)
2. Principles of Information Security, Whitman, Thomson.
3. Introduction to Cryptography, Buchmann, Springer.
4. Applied Cryptography, 2nd Edition, Bruce Schneier, Johnwiley & Sons.