Course Name: Network Security and Cryptography

Course Type: Core Course Credits: 3+1 credits

Objectives:

To make the student learn different encryption techniques along with hash functions, MAC, digital signatures and their use in various protocols for network security and system security.

Learning Outcomes:

The student after successfully completing this course will be able to:

1. Analyze and design classical encryption techniques and block ciphers.
2. Understand and analyze data encryption standard.
3. Understand and analyze public-key cryptography, RSA and other public-key cryptosystems
4. Understand key management and distribution schemes and design User Authentication
5. Protocols.
6. Know about Intruders and Intruder Detection mechanisms, Types of Malicious software.

Unit 1:

Introduction, The need for security, Security approaches, Principles of security-Confidentiality, Authentication, Integrity, Non-repudiation, Access control, Availability, Types of network Attacks, Cryptographic Techniques-Plain text and Cipher text, Substitution Techniques, Transposition Techniques, Encryption and Decryption, Symmetric and Asymmetric Key cryptography-Diffie-Hellman Key Exchange Algorithm. Steganography-Key Range and Key Size, Possible type of attacks

Unit 2:

Symmetric Key Cryptography-Algorithm types and Modes-Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Concept of RC4 and Blowfish

Unit 3:

Asymmetric Key Cryptography-Overview, The RSA Algorithm, ElGamal cryptography, Digital Signatures, Concept of Message Digests, Message Authentication Code (MAC), HMAC, Knapsack Algorithm, ElGamal Digital Signature, Attacks on Digital Signatures

Unit 4:

Internet Protocol Security (IPsec)- Email security, User Authentication Mechanisms- Authentication Basics, Passwords, Authentication Tokens, Certificate based authentication, Biometric authentication, Kerberos, Key Distribution center (KDC), Single sign on approaches

Recommended Books

1) “Cryptography and Network Security”, William Stallings, Pearson Education
2) “Cryptography and Network Security”, Atul Kahate, Mc Graw Hill Education
3) “Network security and Cryptography”, Bernard Menezes, Cengage Publication