Prasad V. Potluri Siddhartha Institute of Technology:: Vijayawada.
Department of Computer Science and Engineering

I/II M.Tech. (CSE) (Second Semester)

17CSCS2T6A CRYPTOGRAPHY and NETWORK SECURITY Credits: 4

Elective - IV

Lecture: 4 Periods/week **Internal Assessment: 40 Marks**
Semester end examination: 60 Marks

Course Description

This course focuses towards the principles and practice of cryptography and network security: classical systems, symmetric block ciphers (DES, AES, other contemporary symmetric ciphers), linear and differential cryptanalysis, perfect secrecy, public-key cryptography (RSA, discrete logarithms), algorithms for factoring and discrete logarithms, cryptographic protocols, hash functions, authentication, key management, key exchange, signature schemes, email and web security, viruses, firewalls, and other topics

Course Outcomes:

At the end of the course, students should be able to:

CO1: Identify common network security vulnerabilities/attacks

CO2: Explain the foundations of Cryptography and network security

CO3: Critically evaluate the risks and threats to networked computers.

CO4: Demonstrate detailed knowledge of the role of encryption to protect data.

CO5: Analyze security issues arising from the use of certain types of technologies.

CO6: Identify the appropriate procedures required to secure networks.

CO7: Identify the appropriate procedures required for system security testing and procedures of Backup and recovery.

Unit-1

Introduction: Security Attacks, Security Services, Security Mechanisms and A model for Network Security. Basics of cryptography – Symmetric chipper model, Classical Encryption Techniques-Transposition and substitution techniques and other cipher properties-confusion, diffusion, block and stream cipher.

Unit-2

Secret Key Cryptography: Data Encryption Standard (DES), Strength Of DES, Block cipher design principles and modes of operations. Triple DES, IDEA, Blowfish and Advance Encryption Standard (AES). **Number Theory:** Prime and relatively prime numbers, Modular Arithmetic, Fermat's and Euler's theorem, the Chinese remainder theorem and discrete logarithms

Unit-3

Public Key Cryptography: Principles of Public key Cryptosystems, RSA algorithm, Diffie-Hellman Key Exchange, Introduction to Elliptic curve Cryptography. **Cryptographic Hash Functions:** Secure Hash Algorithim, Message Authentication Codes-Message Authentication requirements and functions, HMAC, Digital Signatures and Digital Signature Standards. **Authentication Applications:** Kerberos, X.509 Directory Authentication service. **Electronic Mail Security:** PGP and S/MIME

Unit-4

IP Security: Overview, Architecture, Authentication Header, Encapsulation Payload Header, Combining Security Associations, Internet Key exchange.**WebSecurity:** Web security considerations, Secure Socket Layer, TLS and SET. **System Security:** Intruders, Intrusion techniques, Intruder Detection. Malicious Software-Types of viruses, virus counter measures, worms. Firewalls: Characteristic of firewalls, Types of firewalls, Firewall Configuration and Trusted Systems

Text Book:

1. Cryptography and Network Security: Principles and Practise, 5th Edition, William Stallings, Pearson Education, 2011.

Reference Books:

1. Fundamentals of Network Security by Eric Maiwald (Dreamtech press).
2. Introduction to Cryptography, Buchmann, Springer.