CRYPTOGRAPHY AND INFORMATION SECURITY
(Common to CSE&IT)

	L	T	P	C
IV B. Tech. - I Semester	L	T	P	C
Course Code: A3CS30	3	1	-	3

COURSE OVERVIEW:

This course will emphasise on 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 algorithms for factoring and discrete logarithms, cryptographic protocols, hash functions, authentication, key management, key exchange, signature schemes, email and web security, viruses, firewalls, digital right management, and other topics. In this course students will learn as aspects of network security and cryptography.

COURSE OBJECTIVES:

1. To provide deeper understanding into cryptography, its application to network security, threats/vulnerabilities to networks and countermeasures.
2. To explain various approaches to Encryption techniques, strengths of Traffic Confidentiality, Message Authentication Codes.
3. To familiarize Digital Signature Standard and provide solutions for their issues.
4. To familiarize with cryptographic techniques for secure (confidential) communication of two parties over an insecure (public) channel; verification of the authenticity of the source of a message.

COURSE OUTCOMES:

At the end of this course students will be able to:

1. Identify basic security attacks and services
2. Use symmetric and asymmetric key algorithms for cryptography
3. Design a security solution for a given application
4. Analyze Key Management techniques and importance of number Theory.
5. Understanding of Authentication functions the manner in which Message Authentication Codes and Hash Functions works.
6. To examine the issues and structure of Authentication Service and Electronic Mail Security

SYLLABUS

UNIT - I

INTRODUCTION: Security trends, The OSI Security Architecture, Security Attacks, Security Services and Security Mechanisms, A model for Network security.

CLASSICAL ENCRYPTION TECHNIQUES: Symmetric Cipher Modes, Substitute Techniques, Transposition Techniques, Rotor Machines, Stenography.

UNIT - II

BLOCK CIPHER AND DATA ENCRYPTION STANDARDS: Block Cipher Principles, Data Encryption Standards, the Strength of DES, Differential and Linear Crypt Analysis, Block Cipher Design Principles.

ADVANCED ENCRYPTION STANDARDS: Evaluation Criteria for AES, the AES Cipher.

MORE ON SYMMETRIC CIPHERS: Multiple Encryption, Triple DES, Block Cipher Modes of Operation, Stream Cipher and RC4.

INTRODUCTION TO NUMBER THEORY: Prime Numbers, Fermat’s and Euler’s Theorem, Testing for Primality, The Chinese Remainder Theorem, Discrete logarithms,

UNIT - III

PUBLIC KEY CRYPTOGRAPHY AND RSA: Principles Public key crypto Systems, Diffie Hellman Key Exchange, the RSA algorithm, Key Management, , Elliptic Curve Arithmetic, Elliptic Curve Cryptography.

MESSAGE AUTHENTICATION AND HASH FUNCTIONS: Authentication Requirement, Authentication Function, Message Authentication Code, Hash Function, Security of Hash Function and MACs.

HASH AND MAC ALGORITHM: Secure Hash Algorithm, Whirlpool, HMAC, CMAC.
DIGITAL SIGNATURE: Digital Signature, Authentication Protocol, Digital Signature Standard.

UNIT - IV
AUTHENTICATION APPLICATION: Kerberos, X.509 Authentication Service, Public Key Infrastructure.
EMAIL SECURITY: Pretty Good Privacy (PGP) and S/MIME.
IP SECURITY: Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management.

UNIT - V
WEB SECURITY: Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET), Intruders, Viruses and related threats.
FIREWALL: Firewall Design principles, Trusted Systems.

TEXT BOOKS:

1. William Stallings (2006), Cryptography and Network Security: Principles and Practice, 4th edition, Pearson Education, India.
2. William Stallings (2000), Network Security Essentials (Applications and Standards), Pearson Education, India.

REFERENCE BOOKS:

1. Charlie Kaufman (2002), Network Security: Private Communication in a Public World, 2nd edition, Prentice Hall of India, New Delhi.
2. Atul Kahate (2008), Cryptography and Network Security, 2nd edition, Tata Mc Grawhill, India.
3. Robert Bragg, Mark Rhodes (2004), Network Security: The complete reference, Tata Mc Grawhill, India.