CRPTOGRAPHY & NETWORK SECURITY
(PROFESSION ELECTIVES - V)

IV B. TECH- II SEMESTER

Course Code	Category	Hours / Week			Credits	Maximum Marks		
		L	T	P	C	CIE	SEE	Total
A5CS25	PEC	3	-	-	3	30	70	100

COURSE OBJECTIVES

The course should enable the students to:

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

COURSE OUTCOMES

At the end of the course, student 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 with Message Authentication Codes and Hash Functions .

UNIT- I	INTRODUCTION TO SECURITY AND CRYPTO GRAPHY:	CLASSES: 14

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, Stenography

UNIT - II	ENCRPTION STANDARDS AND SYMMETRIC CIPHERING	CLASSES: 14

Block Cipher and Data Encryption Standards: Block Cipher Principles, Data Encryption Standards, the Strength of DES, Block Cipher Design Principles.
Advanced Encryption Standards: Evaluation Criteria for AES, the AES Cipher.
Symmetric Ciphers: Multiple Encryption, Triple DES, Block Cipher Modes of Operation, Stream Cipher and RC4.

UNIT - III	PUBLIC KEY CRPTOGRAPHY AND AUTHENTICATION USING HASH FUNCTIONS	CLASSES: 16

Public Key Cryptography And Rsa: Principles Public key crypto Systems the RSA algorithm, Key Management, Diffie Hellman Key Exchange.
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	IP SECURITY	CLASSES: 12

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	CLASSES: 12
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, 2 nd edition, Tata Mc Grawhill, India. 3. Robert Bragg, Mark Rhodes (2004), Network Security: The complete reference, Tata Mc Grawhill, India.		