III Year B.Tech. ECM II - Semester	L	T	P	To	C
	4	-	-	4	4

CS427 CRYPTOGRAPHY AND NETWORK SECURITY (Elective – II)

Course Description and Objectives:

This Course focuses towards the introduction of network security using various cryptographic algorithms and understanding network security applications. It also focuses on the practical applications that have been implemented and are in use to provide email and web security.

Course Outcomes:

On successful completion of this course, the students

- *Will have knowledge and understanding of: Classical encryption techniques, Block ciphers and the Data Encryption Standard, Basics of finite fields, Advanced Encryption Standard, Contemporary symmetric ciphers, Confidentiality using symmetric encryption, Basics of number theory, Key management, Public key cryptosystems, Message authentication, Hash functions and algorithms, Digital signatures and authentication protocols, Network security practice, Applications, E-Mail, IP and web security, System security, Intruders, Malicious software, Firewalls.*
- *Will develop their skills in: the programming of symmetric and/or asymmetric ciphers and their use in the networks.*
- *Will learn protocols used in Web Security and Transport layer Security*

UNIT I - NETWORK SECURITY INTRODUCTION

Security attacks – Security services – Security Mechanisms – A Model for Network Security Model Classical Encryption Techniques – Symmetric Cipher Model – Substitution Techniques – Transposition Techniques – Rotor Machines – Steganography

UNIT II - BLOCK CIPHERS AND DATA ENCRYPTION STANDARD

Block Cipher Principles – Data Encryption Standard – Strength of DES – Differential and Linear Cryptanalysis - Block Cipher Design Principles.- Advanced Encryption Standard – Evaluation Criteria of AES – AES Cipher – More on Symmetric Ciphers – Multiple encryption and Triple DES – Block Cipher Modes of Operation – RC4.

UNIT III - PUBLIC-KEY ENCRYPTION AND HASH FUNCITONS

Principles of Public –Key Cryptosystems – RSA Algorithm – Key Management – Message Authentication and Hash Functions – Authentication Requirements – Authentication Functions – Message Authentication – Hash Functions – Security of Hash Functions and MACs- Digital Signatures - Authentication Protocols – Digital Signature Standard.

UNIT IV - NETWORK SECURITY APPLICATIONS

Kerberos – X.509 Authentication Service – Public Key Infrastructure – Pretty Good Privacy – S/MIME- IP Security Overview – IP Security architecture- Authentication Header – Encapsulating Security Payload – Combining Security associations – Key Management

UNIT V - Web Security

Secure Socket Layer and Transport Layer Security – Secure Electronic Transaction. SYSTEM SECURITY Intruders – Intrusion Detection – Password Management – Malicious Software - Firewalls – Trusted Systems.

TEXT BOOKS :

1. William Stallings, “Cryptography and Network security”, 4th ed., Pearson Education, 2010.
2. William Stallings “Network Security Essentials Applications and Standards”, 2nd ed.,Pearson Education, 2009.

REFERENCE BOOKS :

1. Eric Malwald, “Fundamentals of Network Security “, 4th ed., Pearson Education, 2010.
2. Charlie Kaufman, “Radis Perlman and Mike Speciner ,Network Security – Private Communication in a Public World”, 1st ed., Pearson Education,2009 .
3. Buchmann, Springer ,”Introduction to Cryptography”, 2nd ed., Pearson Education, 2009.
4. William Stallings,”Cryptography and Network security”, 1st ed., Pearson Education, 2008.
5. Lorrie Faith Cranor, Simson Garfinkel, “Security & Usability”, 2nd ed., SPD OREILLY Publications, 2005.
6. Chris Frj & Martin Nystrom “Security Monitoring”, 1st ed., SPD OREILLY Publications, 2009.