II Year MCA II Semester	L	T	P	To	C
	3	1	-	4	4

MC202 CRYPTOGRAPHY AND NETWORK SECURITY

Objectives of the Course:

On completion of this course

- *Students will be able to identify the need of security in computer and information.*
- *Students will have an understanding of a variety of cryptographic algorithms and protocols underlying network security applications*

UNIT - I **(10 Hrs)**

Introduction: Security Trends – 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 **(12 Hrs)**

Block Ciphers and Data Encryption Standards: 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 **(15 Hrs)**

Public-Key Encryption And Hash Functions: Principles of Public –Key Cryptosystems – RSA Algorithm – Key Management – Diffie Hellman Key Exchange - 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 **(10 Hrs)**

Authentication Applications and Email Security: Kerberos – X.509 Authentication Service – Public Key Infrastructure – Pretty Good Privacy – S/MIME.

UNIT - V **(13 Hrs)**

IP Security and System Security: IP Security Overview – IP Security architecture- Authentication Header – Introduction to Ethical Hacking, General Introduction to Hacking-Vulnerabilities-Functionality and Easy of Use Triangle-Maintaining access-Covering Tracks-Types of Hacker Attacks-Collecting Information on Old and New Vulnerabilities-Computer Crimes and Implications.

Text Books:

1. Cryptography and Network security by William Stallings, Pearson Education, Fourth Edition
2. Cryptography and Network security by Behrouz. A. Forouzan TMH.
3. Ethical Hacking by Ankit Fadia.

Reference Books:

1. Fundamentals of Network Security by Eric Malwald(Dreamtech press)
2. Network Security – Private Communication in a Public World by Charlie Kaufman,Radis Perlman and Mike Speciner,Pearson Education
3. Introduction to Cryptography Buchmann, Springer
4. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education,Second Edition