DISCIPLINE SPECIFIC ELECTIVE 1– Cryptography

Course title &Code	Credits	Credit distribution of the course			Eligibility criteria	Pre-requisite of the course (if any)
		Lecture	Tutorial	Practical/ Practice		
Cryptography	4	3	0	1	NA	NA

Learning Objectives

The course objectives of this paper are: to understand basics of Cryptography and Network Security, to be able to secure a message over insecure channel by various means, to learn about how to maintain the Confidentiality, Integrity and Availability of a data, to understand various protocols for network security to protect against the threats in the networks.

Learning Outcomes

On successful completion of the course, students will be able to:

1. Comprehend the fundamentals of Cryptography and Network Security
2. To be able to secure a message over an unsecured channel using a variety of methods.
3. To gain knowledge on how to preserve the Confidentiality, Integrity, and Availability of data
4. To comprehend various network security protocols for protection against network threats

SYLLABUS OF DSE 1

Unit 1 Overview of Security: (2 weeks)

Protection versus security; aspects of security–data integrity, data availability, privacy; security problems, user authentication, Orange Book.

Unit 2 Security Threats: (3 weeks)

Program threats, worms, viruses, Trojan horse, trap door, stack and buffer overflow; system threats-intruders; communication threats- tapping and piracy.

Unit 3 Cryptography: (4 weeks)

Substitution, transposition ciphers, symmetric-key algorithms-Data Encryption Standard, advanced encryption standards, public key encryption - RSA; Diffie-Hellman key exchange, ECC cryptography, Message Authentication- MAC, hash functions.

Unit 4 Public key cryptography and Authentication requirements: **(4 weeks)**

Principles of public key crypto systems - RSA algorithm - security of RSA - key management – Diffle-Hellman key exchange algorithm - introductory idea of Elliptic curve cryptography – Elgamel encryption - Message Authentication and Hash Function: Authentication requirements - authentication functions - message authentication code - hash functions - birthday attacks – security of hash functions and MACS.

Unit 5 Digital signatures: (2 weeks)

Symmetric key signatures, public key signatures, message digests, public key infrastructures.

Essential Readings

1. W. Stalling, Cryptography and Network Security Principles and Practices (4th ed.), Prentice-Hall of India, 2006
2. C. Pfleeger and SL Pfleeger, Security in Computing (3rd ed.), Prentice-Hall of India, 2007
3. D. Gollmann, Computer Security, John Wiley and Sons, NY, 2002
4. J. Piwprzyk, T. Hardjono and J. Seberry, Fundamentals of Computer Security, Springer-Verlag Berlin, 2003

Suggested Readings

(i) W. Mao, "Modern Cryptography – Theory and Practice", Pearson Education.

(ii) Charles P. Pfleeger, Shari Lawrence Pfleeger – Security in computing – Prentice Hall of India.

(iii) J.M. Kizza, Computer Network Security, Springer, 2007

(iv) M. Merkow and J. Breithaupt, Information Security: Principles and Practices, Pearson Education, 2006.