III YEAR SEM-1 B.Tech CSE	ELECTIVE	L	T	P	C
CODE: CS3505	Cryptography & Network Security	2	2	0	4

COURSE OBJECTIVES	
1.	To understand basics of Cryptography and Network Security.
2.	To be able to secure a message over insecure channel by various means.
3.	To learn about how to maintain the Confidentiality, Integrity and Availability of a data.
4.	To understand various protocols for network security to protect against the threats in the networks.

SYLLABUS:

UNITI(Introduction to Cryptography and Block Ciphers)

Introduction to security attacks - services and mechanism - introduction to cryptography - Conventional Encryption: Conventional encryption model - classical encryption techniques - substitution ciphers and transposition ciphers – cryptanalysis – steganography - stream and blockciphers - Modern Block Ciphers: Block ciphers principals - Shannon’s theory of confusion anddiffusion - fiestal structure - data encryption standard(DES) - strength of DES - differential and linearcrypt analysis of DES - block cipher modes of operations - triple DES – AES.

Unit II (Confidentiality and Modular Arithmetic)

Confidentiality using conventional encryption - traffic confidentiality - key distribution - random number generation - Introduction to graph - ring and field - prime and relative prime numbers - modular arithmetic - Fermat’s and Euler’s theorem - primality testing - Euclid’s Algorithm - Chinese Remainder theorem - discrete algorithms.

Unit III (Public key cryptography and Authentication requirements)

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 IV (Integrity checks and Authentication algorithms)

MD5 message digest algorithm - Secure hash algorithm (SHA) Digital Signatures: Digital Signatures - authentication protocols - digital signature standards (DSS) - proof of digital signature algorithm - Authentication Applications: Kerberos and X.509 - directory authentication service - electronic mail security-pretty good privacy (PGP) - S/MIME.

Unit V (IP Security and Key Management)

IP Security: Architecture - Authentication header - Encapsulating security payloads - combining security associations - key management.

Unit VI (Web and System Security)

Web Security: Secure socket layer and transport layer security - secure electronic transaction (SET) - System Security: Intruders - Viruses and related threads - firewall design principals – trusted systems.

RESOURCES:

Video Lectures

1. http://nptel.ac.in/courses/106105031/**lecture by** Dr. Debdeep MukhopadhyayIIT Kharagpur
2. https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-033-computer-system-engineering-spring-2009/video-lectures/ **lecture by** Prof. Robert Morris and Prof. Samuel Madden MIT.

Text Books

1. William Stallings, "Crpyptography and Network security Principles and Practices", Pearson/PHI.
2. Wade Trappe, Lawrence C Washington, " Introduction to Cryptography with coding theory", Pearson.

Reference Books

1. W. Mao, "Modern Cryptography – Theory and Practice", Pearson Education.
2. Charles P. Pfleeger, Shari Lawrence Pfleeger – Security in computing – Prentice Hall of India.

OUTCOMES:

After successful completion of the course, the learners would be able to

1. Provide security of the data over the network.
2. Do research in the emerging areas of cryptography and network security.
3. Implement various networking protocols.
4. Protect any network from the threats in the world.