CS302: Information and Network Security	L	T	P	Nil
	3	0	2	

Course Objective: To study concepts of information and network security using cryptographic algorithms and network security protocols.

S. No	Course Outcomes (CO)
CO1	Identify and explain various security attacks and basic cryptographic techniques. [Understanding, Applying]
CO2	Analyze the principles and methods of modern block ciphers for e.g. DES, IDEA etc. [Remembering, Undrstanding]

CO3	Apply mathematical concepts such as modular arithmetic and discrete logarithms to understand and implement public key cryptography systems like RSA, Elgamal etc. [Applying, Evaluating]
CO4	Understand message authentication codes, hash functions, and digital signatures, emphasizing their role in securing communications. [Understanding]
CO5	Evaluate authentication applications and protocols, such as Kerberos and assess their effectiveness in securing electronic communications. [Understanding,Evaluate]

S. No	Contents	Contact Hours
UNIT 1	Introduction: Need for security, Introduction to security attacks, services and mechanism, introduction to cryptography, Conventional Encryption: Conventional encryption model, classical encryption techniques- substitution ciphers and transposition ciphers, cryptanalysis, stereography, stream and block ciphers, Intruders, Viruses and related threads.	**8**
UNIT 2	Modern Block Ciphers: Block ciphers principals, Shannon's theory of confusion and diffusion, Fiestal structure, data encryption standard(DES), strength of DES, crypt analysis of DES, block cipher modes of operations, triple DES, IDEA encryption and decryption, strength of IDEA, key distribution	**6**
UNIT 3	Introduction to graph, ring and field, prime and relative prime numbers, modular arithmetic, Fermat's and Euler's theorem, primarily testing, Euclid's Algorithm, Chinese Remainder theorem, discrete logarithms, Principals of public key crypto systems, RSA algorithm, security of RSA, key management, Diffle-Hellman key exchange algorithm, introductory idea of Elliptic curve cryptography, Elgamal encryption.	**10**
UNIT 4	Message Authentication and Hash Function: Authentication requirements, authentication functions, message authentication code (MAC), hash functions, security of hash functions and MACS, MD5 message digest algorithm, Secure hash algorithm(SHA), Public Key Infrastructure(PKI): Digital Certificate, private key management, Digital Signatures: Digital Signatures, authentication protocols, digital signature standards (DSS), proof of digital signature algorithm	**6**
UNIT 5	Authentication Applications: Kerberos and X.509, directory authentication service, password, challenge-response, biometric authentication, electronic mail security-pretty good privacy (PGP), S/ MIME.	**6**
UNIT 6	IP Security: Architecture, Authentication header, Encapsulating security payloads, combining security associations, key management. Web Security: Secure Socket Layer(SSL) and transport layer security, TSP, Secure Electronic Transaction (SET), Electronic money, WAP security, firewall design principals, Virtual Private Network (VPN) security.	**6**
	Total	**42**