Course code: Course Title	Course Structure			Pre-Requisite
SE406: Information and Network Security	L	T	P	NIL
	3	1	0	

Course Objective: To study various cryptographic algorithms and network security protocols.

S. NO	Course Outcomes (CO)
CO1	Understand security threats, cryptographic techniques, and encryption methods.
CO2	Analyze and understand modern block cipher principles, encryption techniques, and cryptanalysis methods.
CO3	Apply number theory concepts and cryptographic algorithms, including RSA, Diffie-Hellman, and elliptic curve cryptography.
CO4	Analyze message authentication techniques, hash functions, and digital signature protocols.
CO5	Analyze authentication mechanisms, IP security protocols, and web security technologies.

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, Elganel 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

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1.	William Stallings, "Cryptography and Network Security: Principals and Practice", Prentice Hall, New Jersy.	**2005**
2.	Atul Kahate, "Cryptography and Network Security", TMH.	**2006**
3.	Behrouz A. Forouzan, "Cryptography and Network Security", TMH.	**2008**
4.	Johannes A. Buchmann, "Introduction to Cryptography", Springer-Verlag.	**2004**
5.	BruceSchiener, "Applied Cryptography".	**1996**