23CS32T3 –CRYPTOGRAPHY & NETWORK SECURITY

Course Category:	Professional Core	**Credits:**	3
Course Type:	Theory	**Lecture-Tutorial-Practical:**	3-0-0
Prerequisite:	• Knowledge in Cryptography & Network Security	**Sessional Evaluation:** **Univ. Exam Evaluation:** **Total Marks:**	30 70 100
Course Objectives:	**Students undergoing this course are expected:**		
	• The concepts of classical encryption techniques and concepts of finite fields and number theory • Working principles and utilities of various crypto graphic algorithms including secret key crypto graphy, hashes, and message digests, and public key algorithms • Design issues and working principles of various authentication protocols, PKI standards • Various secure communication standards including Kerberos, I Psec, TLS and email • Concepts of crypto graphic utilities and authentication mechanisms to design secure applications		

Course Outcomes:	**Upon successful completion of the course, the students will be able to:**	
	CO1	Identify information security goals, classical encryption techniques and acquire fundamental knowledge on the concepts off in it fields and number theory
	CO2	Compare and apply different encryption and decryption techniques to solve problems related to confidentiality and authentication.
	CO3	Apply the knowledge of crypto graphic check sums and evaluate the performance of different message digest algorithms for verifying the integrity of varying message sizes.
	CO4	Demonstrate the ability to apply user authentication principles including Kerberos for secure authentication
	CO5	Gain proficiency in securing web communications using TLS and HTTPS, manage secure remote access with SSH, and design firewall policies.
	UNIT-I **Computer and Network Security Concepts:** Computer Security Concepts, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A Model for Network Security, Classical Encryption Techniques: Sym metric Cip her Model, Substitution Techniques, Transposition Techniques, Steganography, Block Ciphers: Traditional Block Cipher Structure, The Data Encryption Standard, Advanced Encryption Standard: AES Structure, AES Transformation Functions	

Course Content:	**UNIT-II** **Number Theory:** The Euclidean Algorithm, Modular Arithmetic, Fermat‘s and Euler‘s Theorems, The Chinese Remainder Theorem, Discrete Logarithms, Finite Fields: Finite Fields of the Form GF(p), Finite Fields of the Form GF(2n) . **Public Key Cryptography: Principles**: Public Key Cryptography Algorithms, RSA Algorithm, Diffie Hellman Key Exchange, Elliptic Curve Cryptography. . **UNIT-III** **Cryptographic Hash Functions:** Application of Cryp to graphic Hash Functions, Requirements & Security, Secure Hash Algorithm, Message Authentication Functions, Requirements & Security, HMAC &CMAC. **Digital Signatures**: NIST Digital Signature Algorithm, Distribution of Public Keys, X.509 Certificates, Public- Key Infrastructure. . **UNIT-IV** **User Authentication:** Remote User Authentication Principles, Kerberos. Electronic Mail Security: Pretty Good Privacy (PGP) And S/MIME. **IP Security**: IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange. **UNIT-V** **Transport Level Security:** Web Security Requirements, Transport Layer Security (TLS), HTTPS, Secure Shell (SSH) **Fire walls:** Fire wall Character is tics and Access Policy, Types of Fire walls, Fire wall Location and Configurations.
Text Books & References Books:	**TEXTBOOKS:** 1, Cryp tography and Network Security – William Stallings, Pearson Education, th Edition. 2. Cryp tography, Network Security and Cyber Laws–Bernard Menezes, Cengage Learning, 2010 edition **REFERENCE BOOKS:** 1 Cryptography and Network Security-BehrouzA Forouzan, Debdeep Mukhopadhyaya, Mc- Graw Hill, 3rd Edition, 2015. 2 Network Security Illustrated, Jason Albanese and Wes Sonnenreich, MGH Publishers, 2003..
E-Resources:	1. https://nptel.ac.in/courses/106/105/106105031/lecture 2.https://nptel.ac.in/courses/106/105/106105162/lecturebyDr.SouravMukhopadhyayIITKharagpur[VideoLecture] 3 https://www.mitel.com/articles/web-communication-cryptography-and-network-security web articles by Mitel Power Connections