III B.Tech II Semester

		L	T	P	C
23A05601T	**CRYPTOGRAPHY & NETWORK SECURITY**	**3**	**0**	**0**	**3**

Course Objectives:

This course aim sat training students to master the:

- 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, PKIstandards
- Various secure communication standards including Kerberos, I Psec, TLS and email
- Concepts of crypto graphic utilitiesand authentication mechanismsto design secure applications

Course Out comes:

After completion of the course, students will beable to

- Identify information security goals, classical encryption techniques and acquire fundamental knowledge on the concepts offin it fields and number theory
- Compare and apply different encryption and decryption techniques to solve problems related to confidentiality and authentication
- Apply the knowledge of cryptographic check sums and evaluate the performance of different message digestalgorithms for verifying the integrity of varying message sizes.
- Demonstrate the ability to apply **user authentication principles** including **Kerberos** for secure authentication
- Gain proficiency in securing web communications using **TLS** and **HTTPS**, manage secure remote access with **SSH**, and design **firewall policies**

UNIT-I **Lecture9Hrs**

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 metricCip 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

UNIT II **Lecture 9Hrs**

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(2^n) .**Public Key Cryptography**: Principles, Public Key Cryptography Algorithms, RSA Algorithm, Diffie Hellman Key Exchange, Elliptic Curve Cryptography.

UNIT-III **Lecture9Hrs**

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

UNITIV **Lecture9Hrs**

UserAuthentication:RemoteUserAuthenticationPrinciples,Kerberos.ElectronicMailSecurity:PrettyGodPrivacy(PGP)AndS/MIME.
IPSecurity:IPSecurityOverview, IP SecurityPolicy, Encapsulating SecurityPayload,CombiningSecurityAssociations,InternetKeyExchange.

UNIT V **Lecture8Hrs**

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:
1) Cryp tography and Network Security – William Stallings, Pearson Education, 8th 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, 3rdEdition, 2015.
2) Network Security Illustrated, Jason Albanese and Wes Sonnenreich, MGH Publishers, 2003.

Online Learning Resources:
1) https://nptel.ac.in/courses/106/105/106105031/lecture
2) https://nptel.ac.in/courses/106/105/106105162/lecturebyDr.SouravMukhopadhyayIIT Kharagpur[VideoLecture]
3) https://www.mitel.com/articles/web-communication-cryptography-and-network-security web articles by Mitel Power Connections