JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY ANANTAPUR

B.Tech (CSE)– IV-I Sem	L	T	P	C
	3	0	0	3

(20A05702b) CRYPTOGRAPHY & NETWORK SECURITY
(Professional Elective Course – IV)

Course Objectives:

This course aims at 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 cryptographic algorithms including secret key cryptography, 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, IPsec, TLS and email
- Concepts of cryptographic utilities and authentication mechanisms to design secure applications

Course Outcomes:

- After completion of the course, students will be able to
- Identify information security goals, classical encryption techniques and acquire fundamental knowledge on the concepts of finite 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 checksums and evaluate the performance of different message digest algorithms for verifying the integrity of varying message sizes.
- Apply different digital signature algorithms to achieve authentication and create secure applications
- Apply network security basics, analyse different attacks on networks and evaluate the performance of firewalls and security protocols like TLS, IPSec, and PGP
- Apply the knowledge of cryptographic utilities and authentication mechanisms to design secure applications

UNIT I Lecture 9Hrs

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 : Symmetric Cipher 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 Lecture 9Hrs

Cryptographic Hash Functions: Application of Cryptographic 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 Lecture 9Hrs

User Authentication: Remote User Authentication Principles, Kerberos. Electronic Mail Security: Pretty Good Privacy (PGP) And S/MIME.

IPSecurity: IP Security Overview,IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange.

UNIT V Lecture 8Hrs

Transport Level Security: Web Security Requirements, Transport Layer Security (TLS), HTTPS, Secure Shell(SSH)

Firewalls: Firewall Characteristics and Access Policy, Types of Firewalls, Firewall Location and Configurations.

Textbooks:

1) Cryptography and Network Security- William Stallings, Pearson Education, 7thEdition.
2) Cryptography, Network Security and Cyber Laws – Bernard Menezes, Cengage Learning, 2010 edition.

Reference Books:

1) Cryptography and Network Security- Behrouz A Forouzan, DebdeepMukhopadhyaya, Mc-GrawHill, 3rd Edition,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/lecture by Dr.SouravMukhopadhyay IIT Kharagpur [VideoLecture]
3) https://www.mitel.com/articles/web-communication-cryptography-and-network-securityweb articles by Mitel PowerConnections