JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY: KAKINADA
KAKINADA – 533 003, Andhra Pradesh, India

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

IV Year –I Semester		L	T	P	C
		3	0	0	3
CRYPTOGRAPHY AND NETWORK SECURITY					

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, and SSL/TLS and email
- Concepts of cryptographic utilities and authentication mechanisms to design secure applications

Course Outcomes:
By the end of the course the student

- 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, analyze different attacks on networks and evaluate the performance of firewalls and security protocols like SSL, IPSec, and PGP
- Apply the knowledge of cryptographic utilities and authentication mechanisms to design secure applications

UNIT I
Classical Encryption Techniques: Security Attacks, Services & Mechanisms, Symmetric Cipher Model. Cyber Threats, Phishing Attack, Web Based Attacks, SQL Injection Attacks, Buffer Overflow& Format String Vulnerabilities, TCP session hijacking, UDP Session Hijacking.
Block Ciphers: Traditional Block Cipher Structure, Block Cipher Design Principles.

UNIT II
Symmetric Key Cryptography: Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish, IDEA, Block Cipher Modes of Operations.
Number Theory: Prime and Relatively Prime Numbers, Modular Arithmetic, Fermat's and Euler's Theorems, The Chinese Remainder Theorem, Discrete Logarithms.

UNIT III
Public Key Cryptography: Principles, Public Key Cryptography Algorithms, RSA Algorithm, Diffie Hellman Key Exchange, Elliptic Curve Cryptography.
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, Key Management and Distribution

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY: KAKINADA
KAKINADA – 533 003, Andhra Pradesh, India

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

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 Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management.

UNIT V

Transport Level Security: Web Security Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Shell (SSH)
Firewalls: Characteristics, Types of Firewalls, Placement of Firewalls, Firewall Configuration, Trusted Systems.

Text Books:

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

Reference Books:

1) Cryptography and Network Security- Behrouz A Forouzan, Debdeep Mukhopadhyaya, Mc-GrawHill, 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 by Dr. Debdeep MukhopadhyayIIT Kharagpur [Video Lecture]
2) https://nptel.ac.in/courses/106/105/106105162/ lecture by Dr. Sourav Mukhopadhyay IIT Kharagpur [Video Lecture]
3) https://www.mitel.com/articles/web-communication-cryptography-and-network-security web articles by Mitel Power Connections