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

DEPARTMENT OF INFORMATION TECHNOLOGY

III Year – II Semester		L	T	P	C
		3	0	0	3
CRYPTOGRAPHY AND NETWORK SECURITY					

Course Objectives:
The main objectives of this course are to explore the working principles and utilities of various cryptographic algorithms including secret key cryptography, hashes and message digests, public key algorithms, design issues and working principles of various authentication protocols and various secure communication standards including Kerberos, IPsec, and SSL/TLS.

Course Outcomes : At the end of the course, student will be able to
- Explain different security threats and countermeasures and foundation course of cryptography mathematics.
- Classify the basic principles of symmetric key algorithms and operations of some symmetric key algorithms and asymmetric key cryptography
- Revise the basic principles of Public key algorithms and Working operations of some Asymmetric key algorithms such as RSA, ECC and some more
- Design applications of hash algorithms, digital signatures and key management techniques
- Determine the knowledge of Application layer, Transport layer and Network layer security Protocols such as PGP, S/MIME, SSL,TSL, and IPsec .

UNIT I:
Basic Principles : Security Goals, Cryptographic Attacks, Services and Mechanisms, Mathematics of Cryptography.

UNIT II:
Symmetric Encryption: Mathematics of Symmetric Key Cryptography, Introduction to Modern Symmetric Key Ciphers, Data Encryption Standard, Advanced Encryption Standard.

UNIT III:
Asymmetric Encryption: Mathematics of Asymmetric Key Cryptography, Asymmetric Key Cryptography

UNIT IV:
Data Integrity, Digital Signature Schemes & Key Management : Message Integrity and Message Authentication, Cryptographic Hash Functions, Digital Signature, Key Management.

UNIT V:
Network Security-I: Security at application layer: PGP and S/MIME, Security at the Transport Layer: SSL and TLS, **Network Security-II :** Security at the Network Layer: IPSec, System Security

Text Books:
1. Cryptography and Network Security, 3rd Edition Behrouz A Forouzan, Deb deep Mukhopadhyay, McGraw Hill,2015
2. Cryptography and Network Security,4th Edition, William Stallings, (6e) Pearson,2006
3. Everyday Cryptography, 1st Edition, Keith M.Martin, Oxford,2016

Reference Books:
1. Network Security and Cryptography, 1st Edition, Bernard Meneges, Cengage Learning,2018