Sem.	Course Code	Elective III (C): Cryptography and Network Security	Total Marks: 100		Hours Per Week	Credits
VI	19UAKET608		CIA: 25	ESE: 75	6	4

OBJECTIVE:

To impart knowledge regarding cryptography and network security.

COURSE OUTCOMES:

On successful completion of the course the students will able to:

CO1: Classify the symmetric encryption techniques (Understand)

CO2: Illustrate various Public key cryptographic techniques (Analyze)

CO3: Evaluate and authentication algorithms. (Evaluate)

CO4: Classify and Discuss hash Functions (Apply)

CO5: Summarize the concepts of digital signature algorithms (Create)

UNIT - I

Cryptography Techniques: Introduction – PlainText and CipherText - Symmetric Cipher model – Substitution techniques – transposition techniques – ROTOR machines – Steganography – The DES – The strength of DES - block chipper design principles.

UNIT - II

Multiple Encryption and Triple DES - Electronic Code Book – Cipher Block Chaining Mode - Cipher Feedback Mode – Output Feedback Mode – Counter Mode.

UNIT - III

Public Key Cryptography and RSA: Principles of Public-Key Cryptosystems - The RSA Algorithm- Other Public-Key Cryptosystems: Diffie-Hellman Key Exchange- Elgamal Cryptograpic System – Elliptic Curve Arithmetic: Abelian Groups - Pseudorandom number generation based on an asymmetric Cipher.

UNIT - IV

Cryptographic Hash Functions: Applications of Cryptographic Hash functions - Two Simple Hash Functions - Requirements and Security - Hash Functions based on Cipher Block Chaining.

UNIT - V

Digital Signatures – Elgamal Digital Signature Scheme – Schnorr Digital Signature Scheme – NIST Digital Signature Algorithm – Elliptic Curve Digital Signature Algorithm- RSA-PSS Digital Signature Algorithm.

TEXT BOOK:

William Stallings, "Cryptography and Network Security Principles and Practice", Sixth Edition, Pearson Education Inc., 2016

REFERENCE BOOKS:

1. Atulkahate, "Cryptography and Network Security", Second Edition, Third Edition,TMH, 2013

2. Behrouz A.forouzan, "Cryptography and Network Security", Second Edition, TMH 2013

Question Paper Pattern					
Section A	10 x 1 = 10 Marks (Multiple Choice, Four options) Two questions from each unit	**Section B**	5 x 7 = 35 Marks (Either or choice) Two questions From each unit	**Section C**	3 x 10 = 30 Marks (Answer any three questions) One question from each unit