Course related to Professional Ethics

SEM	Course Code	Advanced Learners Course: Cryptography and Network Security	Total Marks: 100	Hours per Week	Credits
V	17UAJAL510		ESE: 100	-	2

Objective: To enable the students to understand the fundamentals of cryptography and network security.

UNIT – I: BLOCK CIPHERS & PUBLIC KEY CRYPTOGRAPHY: Cryptography: Introduction – Substitution ciphers – Transposition Ciphers – One Time Pad – Principles - Data Encryption Standard-Block cipher principles-block cipher modes of operation-Advanced Encryption Standard (AES)-Triple DES-Blowfish-RC5 algorithm.

UNIT – II: Public key cryptography: Principles of public key cryptosystems-The RSA algorithm-Key management – Diffie Hellman Key exchange-Elliptic curve arithmetic-Elliptic curve cryptography. Authentication applications – Kerberos – X.509 Authentication services

UNIT – III: SECURITY PRACTICE & SYSTEM SECURITY: Internet Firewalls for Trusted System: Roles of Firewalls – Firewall related terminology- Types of Firewalls – Firewall designs – SET for E-Commerce Transactions. Intruder – Intrusion detection system – Virus and related threats – Countermeasures – Firewalls design principles – Trusted systems – Practical implementation of cryptography and security.

UNIT – IV: E-MAIL, IP & WEB SECURITY: E-mail Security: Security Services for E-mail-attacks possible through E-mail – establishing keys privacy-authentication of the source-Message Integrity-Non-repudiation-Pretty Good Privacy-S/MIME.

UNIT – V: IPSecurity: Overview of IPSec – IP and IPv6-Authentication Header-Encapsulation Security Payload (ESP)-Internet Key Exchange (Phases of IKE, ISAKMP/IKE Encoding).Web Security: SSL/TLS Basic Protocol-computing the keys- client authentication-PKI as deployed by SSLAttacks fixed in v3- Exportability-Encoding-Secure Electronic Transaction (SET).

TEXT BOOKS:

1. William Stallings, "Cryptography and Network Security", 6th Edition, Pearson Education, March 2013. (UNIT I,II,III,IV).
2. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security", Prentice Hall of India, 2002. (UNIT V).
3. Andrew S. Tanenbaum, "Computer Networks", Fourth Edition, Pearson Education, 2003.

KONGU ARTS AND SCIENCE COLLEGE (AUTONOMOUS) ERODE 638 107

for HEAD OF THE DEPARTMENT
DEPARTMENT OF COMPUTER APPLICATIONS
KONGU ARTS AND SCIENCE COLLEGE
(AUTONOMOUS)
ERODE - 638 107.

Dr. N. RAMAN
PRINCIPAL,
KONGU ARTS AND SCIENCE COLLEGE
(AUTONOMOUS)
NANAPURAM, ERODE - 638 107.