17ES020 CRYPTOGRAPHY AND NETWORK SECURITY

Hours Per Week :

L	T	P	C
3	1	-	4

Total Hours :

L	T	P
45	15	-

WA/RA	SSH/HSH	CS	SA	S	BS
15	30	-	5	5	-

Course Objectives:

The objective of the course is to ensure that students have the necessary networking skills to design, implement, and analyze data communication networks.

Course Outcomes:

- To be able to understand the concepts of security in Networks
- To be able to understand different attacks
- To be able to analyze the given network and know its performance for various situations

SKILLS:

- Understand various Network attacks, Protocols
- Understand the Internet threats
- Analysation of the Different Protocols

ACTIVITIES:

- Smoothening of image using filters.
- To create basic Networks and configure them
- To check the robustness of networks on various attacks
- To implement basic cryptographic Algorithms using open source tools

Unit – I

Introduction : Introduction, Services, Attacks, Security model, OSI security architecture and mechanisms, Internet standards and RFC, Buffering.

Unit - II

Encryption algorithms : Principles, Conventional algorithms, Key distribution, AES ,Diffie Hellman, N-parity Deffie Hellman, Elliptic curve and Elliptic curve cryptography,X.509 directory ,Authentication services, Hash functions secure hash

Unit - III

IP security : IP security overview , Architecture,IPV6 authentication header ,Encapsulation Security payload, ESP, Web security requirements.

Unit – IV

Transport layer security : SNMP, SNMPv1, SNMPv3, Intruders, Viruses, Threats , Secure Socket Layer and Transport Layer Security – Secure Electronic Transaction. SYSTEM SECURITY Intruders – Intrusion Detection – Password Management – Malicious Software - Firewalls – Trusted Systems.

Unit-V

Public Key Infrastructure : Digital Certificates, Private Key Management, The PKIX Model, Public Key Cryptography Standards, XML, PKI and Security. Internet Security Protocols: Basic Concepts, Secure Socket Layer, SHTTP, Time Stamping Protocol, Secure Electronic Transaction, SSL versus SET, 3-D Secure Protocol, Electronic Money, E-mail Security, Wireless Application Protocol (WAP) Security, Security in GSM

TEXTBOOKS:

1. Cryptography and Network Security – by Atul Kahate – TMH.
2. Data Communications and Networking- by Behourz A Forouzan
3. William Stallings, “Cryptography and Network security”, 4th ed., Pearson Education, 2010.
4. William Stallings “Network Security Essentials Applications and Standards”, 2nd ed.,Pearson Education, 2009.

REFERENCEBOOKS:

1. James .F. Kurouse & W. Rouse, “Computer Networking: A Topdown.Approach Featuring”,3/e, Pearson Education.
2. Forouzan, “Data Communications and Networking”, 4th Edition,McGraw Hill
3. William Stallings, “Data and Computer Communication”, Eighth Edition, Pearson Education, 2000