(IT614) NETWORK MANAGEMENT & SECURITY

(ELECTIVE - III)

Objective of the course :

After completion of this course the student will become familiar with different encryption and decryption techniques that will enable him to design Secure software for network management.

UNIT - I

Introduction : Classical security Techniques and Computer Network Security Concepts. Confidentiality and Security, Security Policy and Operations Life Cycle, Security System Development and Operations.

Secure Networking Threats : The Attack Process, Attacker Types. Vulnerability Types. Attack Results. Attack Taxonomy. Threats to Security: Physical security, Biometric systems, monitoring controls, and Data security and intrusion and detection systems.

UNIT - II

Encryption Techniques : Conventional techniques, Modern techniques, DES, DES chaining, Triple DES, RSA algorithm, Key management. Message Authentication and Hash Algorithm, Authentication requirements and functions secure Hash Algorithm, Message digest algorithm, digital signatures. AES Algorithms.

UNIT - III

Designing Secure Networks : Components of a Hardening Strategy. Network Devices. Host Operating Systems. Applications. Appliance-Based Network Services. Rogue Device Detection, Network Security Technologies The Difficulties of Secure Networking. Security Technologies. Emerging Security Technologies, General Design Considerations, Layer 2 Security Considerations. IP Addressing Design Considerations. ICMP Design Considerations. Routing Considerations. Transport Protocol Design Considerations

UNIT - IV

Network Security Platform Options : Network Security Platform Options. Network Security Device Best Practices, Common Application Design Considerations. E-Mail. DNS. HTTP/HTTPS. FTP. Instant Messaging.

IPsec VPN Design Considerations : VPN Basics. Types of IPsec VPNs. IPsec Modes of Operation and Security Options. Topology Considerations. Design Considerations. Site-to-Site Deployment Examples.

UNIT - V

Secure Network Management and Network Security Management: Organizational Realities. Protocol Capabilities. Tool Capabilities. Secure Management Design Options. Network Security Management, Firewalls, Trusted systems, IT act and cyber laws.

TEXT BOOKS :

1. Sean Convery, " Network Security Architectures, Published by Cisco Press, 1st ed., 2004.
2. William Stalling "Cryptography and Network Security" 4th ed., Prentice Hall, 2006.

REFERENCE BOOKS :

1. Charles P. Pfleeger, Shari Lawrence Pfleeger, "Security in Computing" 3rd ed., Prentice Hall, 2003.
2. Jeff Crume "Inside Internet Security" Addison Wesley, 2003.