CA9185 CRYPTOGRAPHY AND NETWORK SECURITY

L T P C
3 0 0 3

UNIT I SYMMETRIC CIPHERS 9

Overview - Classical Encryption Techniques – Block Ciphers and the Data Encryption Standard – Introduction to Finite Fields – Advanced Encryption Standard – More on Symmetric Ciphers – Confidentiality using Symmetric Encryption.

UNIT II PUBLIC-KEY ENCRYPTION AND HASH FUNCTIONS 9

Introduction to Number Theory – Public-Key Cryptography and RSA – Key Management - Diffie-Hellman Key Exchange – Elliptic Curve Cryptography – Message Authentication and Hash Functions – Hash and MAC Algorithms – Digital Signatures and Authentication Protocols.

UNIT III NETWORK SECURITY PRACTICE 9

Authentication Applications – Kerberos – X.509 Authentication Service – Electronic mail Security – Pretty Good Privacy – S/MIME – IP Security – Web Security.

UNIT IV SYSTEM SECURITY 9

Intruders – Intrusion Detection – Password Management – Malicious Software – Viruses and Related Threats - Viruses Countermeasures – Distributed Denial of Service Attacks - Firewalls – Firewall Design Principles – Trusted Systems.

UNIT V WIRELESS SECURITY 9

Introduction to Wireless LAN Security Standards – Technology Comparisons - Wireless LAN Security Factors – Issues in Wireless Security.

Total = 45

REFERENCES

1. William Stallings, “Cryptography And Network Security – Principles and Practices”, Pearson Education, Fourth Edition, 2006.
2. Atul Kahate, “Cryptography and Network Security”, Tata McGraw Hill, 2003.
3. Bruce Schneier, “Applied Cryptography”, John Wiley & Sons Inc, 2001.
4. Stewart S. Miller, “Wi-Fi Security”, McGraw-Hill 2003.
5. Charles B. Pfleeger, Shari Lawrence Pfleeger, “Security in Computing”, Fourth Edition, Pearson Education, 2007.