AMHE19 CRYPTOGRAPHY AND NETWORK SECURITY

UNIT-1 INTRODUCTION TO THE CONCEPT OF SECURITY

1.1 Introduction, The Need of Security,
1.2 Security Approaches,
1.3 Principal of Security, Types of Attacks

UNIT-2 CRYPTOGRAPHIC TECHNIQUES

2.1 Plain Text and Cipher Text, Substitution Techniques, Transposition Techniques,
2.2 Encryption and decryption, Symmetric and Asymmetric Key Cryptography,
2.3 Steganography, Key Range and Key Size, Possible Types of Attacks

UNIT-3 COMPUTER-BASED SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHMS

3.1 Algorithm Types and Models, An Overview of Symmetric Key Cryptography,
3.2 Data Encryption Standard(DES), International Data Encryption Algorithm(IDEA),
3.3 RC5, Blowfish, Advanced Encryption Standard(AES), Differential and Linear Cryptanalysis

UNIT-4 COMPUTER-BASED ASYMMETRIC KEY CRYPTOGRAPHIC ALGORITHMS

4.1 Brief History of Asymmetric Key Cryptography,
4.2 An Overview of Asymmetric Key Cryptography,
4.3 The RSA Algorithm, Symmetric and Asymmetric Key Cryptography Together,
4.4 Digital Signatures, Knapsack Algorithm, Some Other Algorithms

UNIT-5 PUBLIC KEY INFRASTRUCTURE (PKI)

5.1 Digital Certificates, Private Key Management, The PKIX Model,
5.2 Public Key Cryptography standard(PKCS), XML, PKI and Security

UNIT-6 INTERNET SECURITY PROTOCOLS

6.1 Basic Concepts, Security Socket Layer(SSL),
6.2 Secure Hyper Text Transfer Protocol(SHTTP), Time stamping Protocol(TSP),
6.3 Secure Electronic Transaction(SET),SSL Versus SET, 3-D Secure Protocol,
6.4 Electronic Money, Email Security,
6.5 Wireless Application Protocol(WAP) Security, Security in GSM

UNIT-7 NETWORK SECURITY

3.1 Brief Introduction to TCP/IP, Firewalls, IP Security,
3.2 Virtual Private Networks (VPN)

Reference Book:

1. Behrouz A. Forouzan and D. Mukhopadhyay- Cryptography & Network Security, 2nd Edition - 1st reprint 2010, McGraw Hill, New Delhi.
2. Wade Trapple, Lawrence C. Washington- Introduction to Cryptography with coding Theory, 2nd Edition pearson Education