CS-702: Information Security

Introduction:

10L

History ,Critical Characteristics, Components , Approaches of Implementation, Security Systems Development Life Cycle, Security Professionals.

[1] Pages 1 - 30

Security Issues :

8 L

Need for Security, threat, risk, attack, legal and ethical issues.

[1] Pages 37-68

Error Detection / Correction: 8 L

Block Codes, Generator Matrix, Parity Check Matrix, Minimum distance of a Code, Error detection and correction, Standard Array and syndrome decoding. Hamming Codes.

[3] Pages 51-80

Cryptography:

Modular Arithmetic, Congruence.[2] Pages16-37 4L

Plain text, Cipher Text, Key, Encryption, Decryption, Kerckhoff's Principle. Substitution Ciphers, Transposition Ciphers, Types of Attacks on Ciphers. Cryptanalysis of Substitution Ciphers, Transposition Ciphers. Block Cipher, Stream Cipher, Data Encryption Standard,

[2] Pages 46 – 76. Pages 106 – 128 Pages 144-157

10L

Diffie- Hellma key exchange algorithm, Rabin Cipher.

[2]. Pages 283, Pages 410-411

4L

Public Key Infrastructure.

[2] Pages 415-422

Digital Signature

[2] Pages 358-362

E-mail Security .

[2] Pages 415-422.

Security tools : 4 L

Intrusion detection systems, Honey pots, Honey nets and padded cell systems, scanning and analysis tools

[1]. Pages 284- 317

Recommended Reading Material

Text Books

1. Michael E. Whitman , H J Mattord , 2nd edition *Principals of Information Security*, Thompson course technology, 2007.
2. Behrouz A Forouzan, Debdeep Mukhopadhyay, *Cryptography and Network Security*, 2nd edition, Tata McGraw Hill Education Private Limited , New Delhi, 2012.
3. Shu Lin , D.J. Costello,Jr *Error Control Coding: Fundamentals and applications*, Printice –Hall, New Jersey, 2003.

References Books:

4. Kaufman, Perlman , Speciner 'Network Security' PHI ,India, 2nd Ed. 2010

Online References :

5. http://www.cryptogram.org
6. http://www.math.niu.edu

PRACTICAL LIST BASED CS-702: INFORMATION SECURITY

Write Programs for the following

1. Additive Cipher

2. Multiplicative Cipher
3. Affine Cipher
4. Monoalphabetic substitution Cipher
5. Playcipher
6. Vigenere cipher
7. Hill cipher
8. One time pad cipher
9. Roter cipher
10. Enigma Machine
11. Transposition cipher
12. Double Transposition cipher
13. Stream cipher based on XOR operation
14. Data Encryption Algorithm
15. Rabin Cipher
16. For a given parity check matrix write a program to find
    a. the code words and minimum weight of the code
    b. Standard array of the code
    c. error patterns and syndromes