804 : Computer Security

Unit : 1 **[20%]**

Introduction to computer security (book no-1)

What Is Computer Security?

A Broader Definition of Security

Security Policy

- Introduction
- Corporate Policy
- Information Security Policy
  - · Concepts, Classification of information
- Personnel Security policy
  - · Ethics ,Password Policy ,General Software Policy ,Networks , Internet, Laptops and portable computers
- Computer & Network Policy
  - · System administration policy
    - o Physical security, Access Control, Logon Policy, Assurance , Accountability and Audit , Reliability of Service
  - · Network Policy
    - o Network / Distributed Systems Policy , Dial-in access , Dial-out , Internet Firewall , Interfaces to other networks , Incident Response Procedure
  - · Software Development Policy
    - o General Guidelines, Production Guidelines
- Business Continuity Planning
- Enforcement

Physical Security

- Buildings
- Transport of Data
- Backups
- Disks
- Laptops / mobile computers
- Printers
- Computers
- "Clean desk"

Unit : 2 **[20%]**

System Security(book no-2)

- Intruders
  - o Intruders, Intruders detection, Password management.
- Malicious Software
  - o Viruses and Related Threats
- Firewalls
  - o Firewalls Design principle, established systems.

Unit : 3 **[25%]**

Cryptography(book no 2)

- Foundations of cryptography and computer security
    - o Mathematical foundations, Randomness
- Symmetric key cryptography
    - o Classical Encryption Techniques
    - o Block Ciphers And The Data Encryption Standard
    - o Advance Encryption Standard
    - o Confidentiality Using Symmetric Encryption
- Public key cryptography
    - o Public Key Cryptography And RSA
    - o Message Authentication And Hash Function

Unit : 4 **[35%]**

Network Security(book no-2)

- Protocols :- Digital Signature standards.
- Electronics Mail Security - PGP (Pretty Good Privacy) MIME, data Compression technique.
- IP Security:- Architecture, Authentication Leader, Encapsulating security Payload - Key Management.
- Web security: -Secure Socket Layer & Transport Layer security, secure electronics transactions.

book no 3

- Local and Metropolitan Area Network Security Environment.
- Wide Area Network Security.
- Virtual Networks Security.
- Distributed Systems Security.
- Wireless Networking Security

Textbooks:

1. IT Security Cook Book(http://www.boran.com/security)
2. Cryptography and Network Security (2nd edition) William Stallings(Pearson Education)
3. Enterprise Security, 1/e Robert C. Newman(Pearson Education)

Reference books:

1. Computer Security Basics By Debby Russell, G.T. Gangemi, Sr.(Oreilly)
2. Network Security private communication in a PUBLIC world By Charlie Kaufman, Radia Perlman , Mike Speciner
3. Security in Computing, 3/e Charless P. Pfleeger, Shari Lawrence Pfleeger.

804 : Computer Security [Practical List]

1. Write a 'c' program to encrypt the plaintext and display the cipher text using Ceaser Cipher.
2. Write a 'c' program to decrypt the ciphetext and display the plain text using Ceaser Cipher.
3. Write a 'c' program to encrypt the plaintext and display the cipher text using Monoalphabetic Substitution Cipher.
4. Write a 'c' program to Decrypt the cipher text and display the plain text using Monoalphabetic Substitution Cipher.
5. Write a 'c' program to Encrypt the plaintext and display the cipher text using playfair Cipher.
6. Write a 'c' program to Decrypt the Ciphertext and display the plaintext using playfair Cipher.
7. Write a 'c' program to Encrypt the plaintext and display the cipher text using Hill Cipher.
8. Write a 'c' program to Decrypt the Ciphertext and display the plaintext using Hill Cipher.
9. Write a 'c' program to Encrypt the plaintext and display the cipher text using Vigenere Cipher.
10. Write a 'c' program to Decrypt the cipher text and display the plain text using Vigenere Cipher.
11. Write a 'c' program to Encrypt the plaintext and display the cipher text using Autokey Vigenere Cipher.
12. Write a 'c' program to Decrypt the ciphertext and display the plain text using Autokey Vigenere Cipher.
13. Write a 'c' program to Encrypt the plaintext and display the cipher text using One-Time Pad Vigenere Cipher.
14. Write a 'c' program to Decrypt the ciphertext and display the plaintext using One-Time Pad Vigenere Cipher.
15. Write a 'c' program to Encrypt the plaintext and display the cipher text using Rail Fence Transposition Cipher.
16. Write a 'c' program to Decrypt the cipher text and display the plaintext using Rail Fence Transposition Cipher.
17. Write a 'c' program to Encrypt the plaintext and display the cipher text using Columnar Transposition Cipher.
18. Write a 'c' program to Decrypt the cipher text and display the plain text using Columnar Transposition Cipher.
19. Write a 'c' program to Encrypt the plaintext and display the cipher text using Three-Rotor machine.
20. Write a 'c' program to Decrypt the cipher text and display the plain text using Three-Rotor Machine.