

# System Security [SS]

B.E. Sem. VII [CMPN]

---

---

## EVALUATION SYSTEM

	Time	Marks
Theory Exam	3 Hrs.	100
Practical Exam	–	–
Oral Exam	–	25
Term Work	–	25

## SYLLABUS

### 1. Introduction to Information Security

Security Goals.

### 2. Cryptography

Crypto Basic, Classic Cryptography; Symmetric Key Cryptography: Stream Ciphers, A5/1, RC4, Block Ciphers, Feistel Cipher, DES, Triple DES, AES; Public Key Cryptography: Knapsack, RSA, Diffie-Hellman, use of public key crypto- Signature and Non-repudiation, Confidentiality and Non-repudiation, Public Key Infrastructure; Hash Function: The Birthday Problem, MD5, SHA-1, Tiger Hash, Use of Hash Function.

### 3. Access Control - Authentication and Authorization

Authentication Methods, Passwords, Biometric, Single –sign on, Authentication Protocol, Kerberos; Access control Matrix, ACLs, Multiple level security model, Multilateral security, Covert channel, CAPTCHA.

### 4. Software Security

Software Flaws, Buffer Overflow, Incomplete Mediation, Race conditions. Malware, Salami attack, Linearization Attacks, Trusting Software; Software reverse engineering, Digital Rights management; Operating System and Security.

### 5. Network Security

Network security basics; TCP/IP Model and Port No., Protocol flaws; Enterprise wide network Design and Vulnerabilities; Reconnaissance of network; Packet sniffing, Session Hijacking, ARP Spoofing; Web site and web server vulnerabilities; Denial of Service; SSL and IPSec protocol; Firewall. Intrusion Detection System, and Honey pots.

### Reference :

1. Cryptography and Network Security (*Behrouz A. Forouzan*) Tata McGraw hill.
2. Security in Computing (*Charles P. Pfleeger*) Pearson Education.
3. Information security Principles and Practice (*Mark Stamp*) Wiley publication.
4. Cryptography and Network Security (*William Stalling*) Prentice Hall
5. Principles of Information Security (*Michael E.*) Cengage learning
6. Information Systems Security (*Nina Godbole*) Wiley
7. Network security bible 2<sup>nd</sup> edition, Eric Cole.

