

INFORMATION AND NETWORK SECURITY				
CLASS T.E. ( INFORMATION TECHNOLOGY)			SEMESTER VI	
HOURS PER WEEK	LECTURES	:	04	
	TUTORIALS	:	--	
	PRACTICALS	:	02	
			<b>HOURS</b>	<b>MARKS</b>
EVALUATION SYSTEM:	THEORY		3	100
	PRACTICAL		--	-
	ORAL		--	25
	TERM WORK		--	25

### 1. Introduction

What is 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, Email Security.

### 6. Administered Security

Planning, Risk Analysis, Organizational Policies, Physical Security

### Text Books

1. Mark Stamp, "Information security Principles and Practice" Wiley
2. Charles P. Pfleeger, "Security in Computing", Pearson Education

## **References**

1. Behrouz A. Forouzan, "Cryptography and Network Security", Tata McGraw Hill
2. William Stallings, "Cryptography and Network Security", Prentice Hall
3. Nina Godbole, "Information Systems Security", Wiley
4. Matt Bishop, "Computer Security: Art and Science", Pearson Education
5. Kaufman, Perlman, Speciner, "Network Security"
6. Mark Merkow, Jim Breithaupt, "IS Principles and Practices", Person Education

## **Term Work**

Term work shall consist of at least 10 assignments/programming assignments and one written test.

## **Marks**

- |  |          |
|--|----------|
| 1. Attendance (Theory and Practical)         | 05 Marks |
| 2. Laboratory work (Experiments and Journal) | 10 Marks |
| 3. Test (at least one)                       | 10 Marks |

The final certification and acceptance of Term Work ensures the satisfactory performance of laboratory Work and Minimum Passing in the term work.

## **Suggested Experiment List**

1. Block Cipher such as Feistel, DES or AES
2. Public Key Cryptography (RSA)
3. Conventional Cryptography
4. Authentication Methods such as passwords or Kerberos
5. Software Flaw Frauding tools such as flaw finders, ITS, PScan, RATS
6. Analysis of Network port scanner tool such as NMAP
7. Analysis of Sniffer program such as Ethernet
8. Transport Security using firewall
9. Application level security such as email by using PHP
10. Implementation of IDS