

Syllabus of the Course

PERIOD PER WEEK			CREDITS			MAXIMUM MARKS				
T	P	Tu.	T	P	Tu.	THEORY		PRACTICAL		TOTAL MARKS
						CW	END SEM	SW	END SEM	
3	2	0	3	1	0	30	70	40	60	200

PRE-REQUISITE: 1. CO34007: Computer Network

COURSE OUTCOMES:

After Completing the course student should be able to:

1. Understand meaning of information and secure system and need of information security.
2. Understand cryptography and various cryptographic techniques.
3. Understand threats and vulnerabilities in network protocols and attacks.
4. Understand security policies and security in software.

COURSE CONTENTS:

THEORY:

UNIT 1. Introduction to Information Security, Security threats – Vulnerabilities and Attacks, Security Goals, Security planning and Risk analysis, Legal and Ethical Issues in Computer Security.

UNIT 2. Cryptography – Classical Cryptography, Symmetric key Encryption: DES, Triple DES algorithm, Key Exchange; Public Key Cryptography: RSA algorithm; Hash Functions and Message Authentication: MD5, SHA-1, HMAC, PKI: Digital Signatures, Digital Certificates, X.509 standard, Authentication applications like Kerberos.

UNIT 3. Security in networks: Threats and Vulnerabilities, IP Security – Overview, Architecture etc., Email Security – PGP, S/MIME; Web Security – Requirements, Security Protocols like SSL, TLS, SET; Firewalls.

UNIT 4. Intruders, Intrusion Detection and Preventing techniques, Program Security- Threats against programs, Secure programs, Viruses and other malicious code; Introduction to Operating System Security: User Authentication mechanisms, Memory and Address protection, File system protection.

UNIT 5. Access Control Mechanisms, Security Policies: Definition, Types, various models of security; Introduction to Security in Distributed Systems, Introduction to Database security methods.