SWE3002 Information and Systems Security

L T P J C
3 0 0 4 4

Pre-Req: SWE2002

Objectives:

To learn principles of cryptography, network and information security.

To introduce the practices of cryptography and network security technology along with its practical use and applications

Expected Outcomes:

On completion of this course, students will be able to

Understand the principles of cryptography, network and information security and apply it in suitable security application.

Apply cryptography and network security technology into its practical applications.

Secure the data transferred over computer networks and devise practical solutions to network security requirements.

Provide multi-level security for data and databases

Module	Topics	L Hrs	SLO
1	**Fundamentals of Security:** Definitions & challenges of security, OSI security architecture, attacks & services, Security policies, access control structures.	6	1,2
2	**Elementary Cryptography:** Cryptography & cryptanalysis. Classical encryption techniques, substitution techniques, transposition techniques. Block ciphers, DES, AES structure,.	6	1,2
3	**Public Key Crypto Systems**. Number theory fundamentals, principles of pubic key crypto systems, RSA algorithm, Diffie-Hellman key exchange.	6	1
4	**Hash Functions & MAC** Cryptographic hash functions, applications, requirements, SHA-512, MAC requirements, security, HMAC, Digital signatures	6	1,2
5	**Key Management & Distribution**. Symmetric key distribution using symmetric and asymmetric encryptions, distribution of public keys, PKI	6	2
6	**Program Security** Secure programs, Non malicious program errors, types of malicious software, viruses and counter measures, Bots, Rootkits, Targeted malicious code, Controls against program threats, software security issues	6	2
7	**Operating Systems & Data base Security** Protected Objects and Methods of protection, Memory and Address Protection, Control of Access to General Objects, Kernel flaws, File protection Mechanisms. Security requirements of databases, Sensitive data, Inference, Multilevel secure databases, concurrency control and multilevel security.	6	2
8	Applications of Information & Systems Security in industry	3	2,17
	Total Lecture Hours	**45**	

 # Mode: Flipped Class Room,online quizzes,assignments,CAT ,FAT

Text Books

1. **William Stallings, Cryptography & Network Security- Principles and Practices, 6th Edition by Pearson Publishers, 2014.**

Reference Books

1. **William Stallings , Lawrie Brown, Computer Security: Principles and Practice, 3rd edition, 2014.**
2. **Christof Paar & Jan Pelzl, Understanding cryptography, Springer, 2010.**
3. **Charles P. Pfleeger, Security in computing, 4th Edition, Pearson, 2009.**

Compiled by Dr.Ch.Aswani Kumar

Date of Approval by the Academic Council on: 18.3.2016