SWE3002	Information & Systems Security	L	T	P	J	C
		3	0	0	4	4
Pre-requisite	SWE2002	Syllabus version				
		v.1.0				

Course Objectives:

1. To learn principles of cryptography, network and information security.
2. To comprehend mathematical foundations of cryptography
3. To introduce the practices of cryptography and network security along with its applications
4. To use the information sources

Expected Course Outcomes:

1. Identify the challenges of security attacks
2. Understand the elementary cryptography based on symmetric and public-key encryption techniques
3. Understand public Key Crypto Systems models, RSA algorithm, Diffie-Hellman key exchange
4. Apply Cryptographic hash functions SHA-512, MAC requirements, security, HMAC, Digital signatures
5. To generate the key distributions using symmetric and asymmetric encryptions
6. Enumerate malicious software, viruses and counter measures
7. Understand Operating Systems & Data base Security issues and control methods
8. Study Applications of Information & Systems Security in industry

Student Learning Outcomes (SLO)	1, 2,17

Module:1	Fundamentals of Security	6 hours

Definitions & challenges of security, OSI security architecture, Attacks & services, Security policies, Access control structures.

Module:2	Elementary Cryptography	6 hours

Cryptography & cryptanalysis. Classical encryption techniques, Substitution techniques, Transposition techniques. Block ciphers, DES, AES structure.

Module:3	Public Key Crypto Systems	6 hours

Number theory fundamentals, Principles of pubic key crypto systems, RSA algorithm, Diffie-Hellman key exchange.

Module:4	Authentication Protocols	6 hours

Cryptographic hash functions, applications, requirements, SHA-512, MAC requirements, security, HMAC, Digital signatures.

Module:5	Key Management & Distribution	6 hours

Symmetric key distribution using symmetric and asymmetric encryptions, Distribution of public keys, PKI.

Module:6	Program Security	6 hours

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.		
Module:7	**Operating Systems & Database Security**	**7 hours**
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.		
Module:8	**Contemporary Issues**	**2 hours**
Applications of Information & Systems Security in Industry.		
	Total Lecture hours:	**45 hours**

Text Book(s)	
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.

Recommended by Board of Studies	12.06.2015		
Approved by Academic Council	No. 37	Date	16.06.2015