ITE4001	**Network and Information Security**	**L**	**T**	**P**	**J**	**C**
		3	**0**	**0**	**4**	**4**
Pre-requisite	**ITE3001**	**Syllabus version**				
		1.1				

Course Objectives:

- To learn principles of cryptography, network and information security
- To acquire knowledge on algorithms to provide confidentiality, integrity and authenticity.
- To understand how to deploy encryption techniques to secure data in transit across networks.

Expected Course Outcome:

1) Understand the fundamentals of security.
2) Have a theoretical understanding of the principles underlying cryptography and have a technical understanding of the main cryptographic concepts and technologies.
3) Provide data integrity using hashing algorithms.
4) Sign and verify messages using well known signature generation and verification algorithms.
5) Analyze user authentication techniques and provide identity management.
6) Analyze the cause for classical network attacks and describe the working of advanced security controls.
7) Analyze the IP and wireless security.
8) Apply cryptography and network security technology in practical applications.

Student Learning Outcomes (SLO): **1, 2, 17**

[1] Having an ability to apply knowledge of mathematics, science, and engineering

[2] Having a clear understanding of the subject related concepts and of contemporary issues

[17] Having an ability to use techniques, skills and modern engineering tools necessary for engineering practice.

Module:1	**Fundamentals of Security**	**8 hours**

Definitions & challenges of security, OSI security architecture, attacks & services. Cryptography & cryptanalysis. Classical encryption techniques, substitution techniques, transposition techniques. Block ciphers, DES, AES structure, multiple encryption-triple DES.

Module:2	**Public Key Crypto Systems, Key Management & Distribution**	**8 hours**

Number theory fundamentals, principles of pubic key crypto systems, RSA algorithm, Strength of RSA, Diffie-Hellman key exchange, Elliptic curve cryptography. Symmetric key distribution using symmetric and asymmetric encryptions, distribution of public keys, X.509 Certificates, PKI.

Module:3	**Hash Functions**	**5 hours3**	
Cryptographic hash functions, applications, security requirements, hash function based on block chaining, SHA-512			
Module:4	**MAC Codes & Digital Signatures**	**4 hours**	
MAC, security requirements, HMAC, CMAC, key wrapping, Digital signatures.			
Module:5	**User Authentication**	**5 hours**	
Remote user authentication, symmetric and asymmetric encryptions for user authentications, Kerberos, identity management & verification.			
Module:6	**Transport Level Security & E-mail Security**	**6 hours**	
Web security, Secure Socket Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH), HTTPS, E-mail security, PGP, S/MIME.			
Module:7	**IP & Wireless Security**	**6 hours**	
IP Security, Policy, encapsulating security payload, combining security association, internet key exchange. Wireless security, IEEE 802.11 overview & its security.			
Module:8	**Contemporary issues:**	**3 hours**	
	Total Lecture hours:	**45 hours**	
Text Book(s)			
1.	William Stallings, Cryptography & Network Security- Principles and Practices, Sixth Edition, Pearson Publishers, 2014.		
Reference Books			
1.	Christof Paar & Jan Pelzl, Understanding cryptography, **Heidelberg [u.a.] Springer 2014.**		
2.	Bragg et al., Network security – The complete reference, Tata Mc Graw Hill, 2012.		
Recommended by Board of Studies	12-08-2017		
Approved by Academic Council	No. 47	Date	05-10-2017