Course code	Course Title	L	T	P	C
BITE401L	Network and Information Security	3	0	0	3
Pre-requisite	BITE305L, BITE305P	Syllabus version			
		1.0			

Course Objectives:

1. To introduce principles of network and information security
2. To develop workable knowledge on various cryptographic algorithms
3. To analyse Web and Internet security protocols.

Course Outcomes:

1. Understand the security principles and mechanisms.
2. Analyze and evaluate cryptographic primitives
3. Evaluate security issues in web applications
4. Design and develop security solutions.
5. Understand Web security concepts and information security mechanisms.

Module:1	Network Security Concepts	7 hours

Challenges of Network Security - OSI Security Architecture - Security Attacks - Security Services - Model for Network Security – Security Standards – Cryptography - Classical Encryption Techniques - Substitution Techniques - Transposition Techniques – Block Ciphers - Traditional Block Cipher Structure – DES – AES – Triple DES - Stream Ciphers.

Module:2	Public Key Cryptography	6 hours

Need and Principles of Public Key Cryptosystems - RSA Algorithm - El Gamal Cryptographic System - Elliptic Curve Cryptography - Public Key Distribution and Management - Diffie-Hellman Key Exchange.

Module:3	Cryptographic Hash Functions	6 hours

Applications of Cryptographic Hash Functions - Security Requirements for Cryptographic Hash Functions - Hash Functions Based on Cipher Block Chaining - Secure Hash Algorithm (SHA) – SHA3.

Module:4	MAC & Digital Signatures	6 hours

Message Authentication Requirements - Security of MACs - MACs Based on Hash Functions: HMAC - MACs Based on Block Ciphers: DAA and CMAC - Authenticated Encryption: Key Wrapping - Pseudorandom Number Generation using Hash Functions and MACs - Digital Signatures

Module:5	User Authentication	6 hours

Remote user authentication - symmetric and asymmetric encryptions for user authentications - Kerberos, identity management & verification.

Module:6	Wireless Network Security	6 hours

Wireless Network Threats - Wireless Security Measures - IEEE 802.11i Wireless LAN Security - Wireless Intrusion Detection and Prevention - Wireless Network Positioning and Secure Gateways.

Module:7	Web Security	6 hours

Web Security Considerations - Web Security Threats - Web Traffic Security Approaches - Transport Layer Security – HTTPS - Secure Shell (SSH) - Email Threats - Electronic Mail Security - IP Security - Internet Key Exchange

Module:8	Contemporary Issues	2 hours

	Total Lecture hours:	**45 hours**

Text Books	
1.	William Stallings, "Cryptography and Network Security- Principles and Practice", 2020, 8th Edition, Pearson Publishers.
2.	Michael E Whitman and Herbert J Mattord, "Principles of Information Security", 2017, 6th Edition, Course Technology Inc.
Reference Books	
1.	Jason Andress, "Foundations of Information Security: A Straightforward Introduction",2019, 1st Edition, No Starch Press.
2.	Charles P. Pfleeger, Shari Lawrence Pfleeger and Jonathan Margulies, "Security in Computing", 2015, 5th Edition, Pearson Publishers.
Mode of Evaluation: Continuous Assessment Tests, Assignment, Quiz, Final Assessment Test	

Recommended by Board of Studies	20-05-2022		
Approved by Academic Council	No. 66	Date	16-06-2022