BCSE309L	Cryptography and Network Security	L	T	P	C
		3	0	0	3
Pre-requisite	NIL	Syllabus version			
		1.0			

Course Objectives

1. To explore the concepts of basic number theory and cryptographic techniques.
2. To impart concept of Hash and Message Authentication, Digital Signatures and authentication protocols.
3. To reveal the basics of transport layer security, Web Security and various types of System Security.

Course Outcomes

On completion of this course, students should be able to:

1. To know the fundamental mathematical concepts related to security.
2. To understand concept of various cryptographic techniques.
3. To apprehend the authentication and integrity process of data for various applications
4. To know fundamentals of Transport layer security, web security, E-Mail Security and IP Security

Module:1	Fundamentals of Number Theory	5 hours

Finite Fields and Number Theory: Modular arithmetic, Euclidian Algorithm, Primality Testing: Fermats and Eulers theorem, Chinese Reminder theorem, Discrete Logarithms.

Module:2	Symmetric Encryption Algorithms	7 hours

Symmetric key cryptographic techniques: Introduction to Stream cipher, Block cipher: DES, AES,IDEA, Block Cipher Operation, Random Bit Generation and RC4

Module:3	Asymmetric Encryption Algorithm and Key Exchange	8 hours

Asymmetric key cryptographic techniques: principles, RSA, ElGamal, Elliptic Curve cryptography, Homomorphic Encryption and Secret Sharing, Key distribution and Key exchange protocols, Diffie-Hellman Key Exchange, Man-in-the-Meddle Attack

P

Module:4	Message Digest and Hash Functions	5 hours

Requirements for Hash Functions, Security of Hash Functions, Message Digest (MD5), Secure Hash Function (SHA),Birthday Attack, HMAC

Module:5	Digital Signature and Authentication Protocols	7 hours

Authentication Requirements, Authentication Functions, Message Authentication Codes, Digital Signature Authentication, Authentication Protocols, Digital Signature Standards, RSA Digital Signature, Elgamal based Digital Signature, Authentication Applications: Kerberos, X.509 Authentication Service, Public Key Infrastructure (PKI)

Module:6	Transport Layer Security and IP Security	4 hours

Transport-Layer Security, Secure Socket Layer(SSL),TLS, IP Security: Overview: IP Security Architecture, Encapsulating Payload Security

Module:7	E-mail, Web and System Security	7 hours

Electronic Mail Security, Pretty Good Privacy (PGP), S/MIME, Web Security: Web Security Considerations, Secure Electronic Transaction Protocol

Intruders, Intrusion Detection, Password Management, Firewalls: Firewall Design Principles, Trusted Systems.

Module:8	Contemporary Issues	2 hours
	Total Lecture hours:	45 hours

Text Book

1. Cryptography and Network Security-Principles and Practice, 8th Edition, by Stallings

	William, published by Pearson, 2020		
Reference Books			
1.	Cryptography and Network Security, 3rd Edition, by Behrouz A Forouzan and Depdeep Mukhopadhyay, published by McGrawHill, 2015		
Mode of Evaluation: CAT, written assignment, Quiz, and FAT			
Recommended by Board of Studies	04-03-2022		
Approved by Academic Council	No. 65	Date	17-03-2022