Course Type	Course Code	Name of the Course	L	T	P	Credits
DC	NCSC509	Cryptography and Network Security	3	1	0	4

Course Objective

- To understand basics of Cryptography and Network Security and to learn how to maintain the Confidentiali Integrity, and Availability (CIA) of the data.
- To be able to secure a message over insecure channel by various the cryptographic techniques and understanding the various protocols for network security to protect the data against the threats in the networks.

Learning Outcomes

- To understand the both theoretical and practical knowledge in information security aspects and provide the security of the data over the public network.
- To do research in the new emerging areas of cryptography and network security and implement the various networking protocols.
- To protect any network from the threats in the real scenario.

Unit No.	Topics to be Covered	Lecture Hours	Learning Outcome
1.	Cryptography: Introduction, Security requirements, Attacks, Security techniques, modes of operation	6+2	Learning the basics of cryptography and security
2.	Mathematical backgrounds: Modular Arithmetic, Group, Ring, Field, elliptic curve	5+3	Understanding the basics of mathematics used in cryptography
3.	Classical encryption techniques, Block ciphers, Public-key ciphers, Elliptic curve cryptography	6+2	Learning about the classical as well as public ciphers techniques, elliptic curve cryptography
4.	Message authentication, Cryptographic hash algorithms, Digital Signatures	6+2	learning about message authentication, hash algorithms and digital signatures
5.	Network Security: Network layer security (IPSec)- Authentication header (AH), Encapsulated security payload (ESP), Security association (SA), Internet security protocol (IKE).	7+2	Understanding the network layer security and the protocols
6.	Transport layer security: Secure socket layer (SSL)- SSL architecture, Four protocols, SSL message formats, TLS	6+2	Understanding the transport layer security and the protocols
7.	E-mail security: Introduction to E-mail architecture, PGP (Pretty Good Privacy), S/MIME	6+1	Understanding the application layer security and the protocols
	TOTAL	**42L+14T**	

Text Books:

1. William Stallings, ‘Cryptography and Network Security-Principles and Applications’ Pearson Education.

Reference Books:

1. B.A. Forouzan, ‘Cryptography and Network Security’ Tata McGraw-Hil