Course Type	Course Code	Name of Course	L	T	P	Credit
DP	NCSC512	**Cryptography and Network Security Lab**	0	0	3	1.5

Course Objective
The Lab provides hands-on experience in implementing cryptographic algorithms, protocols, and security mechanisms.
Learning Outcomes
Upon successful completion of this course, students will: ● Basic understanding of cryptography and network security concepts ● Capable to develop new security algorithms/protocols

Unit No.	Topics to be Covered	Lecture Hours	Learning Outcome
1	A) Implementation of classical encryption techniques (e.g., Caesar cipher, Affine cipher) and perform their cryptaanalysis. B) Implementation of symmetric cryptosystem DES and AES	9	To learn implementation of symmetric cryptosystem
2	A) To implement the Euclidean Algorithm B) To Implement algorithms related to prime numbers and factorization.	9	To understand number theory based algorithms
3	A) To RSA encryption and decryption B) To Implement Diffie-Hellman key exchange C) To implement ECC based key exchange protocol	9	To understand public key cryptosystem
4	A) Hash function implementation B) To implement Digital Signature Algorithm	9	To understand Digital Signature
5	A) Analysis of network vulnerabilities	6	To understand network analysis process
	Total	42	

Text Books:

1. "Cryptography and Network Security: Principles and Practice" by William Stallings