Course Code	Course Title	L	T	P	C
BACSE319	Cryptography and Network Security	3	0	2	4
Pre-requisite	NIL	**Syllabus Version**			
		1			

Course Objectives

To explore the concepts of security, number theory and types of cryptosystems.
To impart the concepts of digital signatures, authentication and hashing.
To apply the concepts of internet security and Network Endpoint.

Course Outcomes

Realize the fundamentals of security services and number theory.
Explore the different types of cryptosystems.
Comprehend the concepts of data integrity algorithms.
Analyze mutual trust models and user authentication.
Deduce the various network and Internet security mechanisms.

Module:1	**Cryptography Concepts**	**8 hours**

Information and Network Security Concepts - Security attacks - Security Services - Security Mechanisms - Elementary Number Theory - Euclidean Algorithm – Modular Arithmetic – Prime Numbers – Fermat's and Eulers Theorems – Testing for Primality – Discrete Logarithms - Pseudo Random Bit Generation.

Module:2	**Cryptographic Algorithms**	**9 hours**

Symmetric Key Cryptography - Stream Cipher – RC4 algorithm - Block Cipher - DES, Triple – DES, AES, Block Cipher Modes of Operation - Asymmetric Key Cryptography - RSA Algorithm, Elgamal Algorithm, Diffie-Hellman Key Exchange - Elliptic Curve Cryptography.

Module:3	**Data Integrity Algorithms**	**9 hours**

Message Authentication Code - Secure Hash Algorithm: SHA 256 – SHA 512- Hash based Message Authentication Code –Entity Authentication-Digital Signatures– Standards - RSA Digital Signature - ElGamal based Digital Signature.

Module:4	**Mutual Trust**	**7 hours**

Cryptographic Key Management and Distribution – Distribution of public keys – X.509 Certificates – Public Key Infrastructure – User Authentication – Remote User Authentication Principles – Kerberos – Federated Identity Management.

Module:5	**Network Security and Post Quantum Cryptography**	**10 hours**
Electronic Mail Security – PGP,S/MIME - Transport Level Security – IP Security - Intrusion Detection System - Wireless Network Security -Introduction to Post Quantum Cryptography – Overview of NIST PQC standardization - PQC Algorithms - Lattice Based Cryptography.		
Module:6	**Contemporary Issues**	**2 hours**
	Total Lecture Hours:	**45 hours**

Text Book(s)

William Stallings, "**Cryptography and Network Security Principles and Practice**", Pearson Education, 8th Edition, **2023**

Reference Books

Behrouz A Forouzan and Debdeep Mukhopadhyay, "**Cryptography and Network Security**", McGraw Hill, 3rd Edition, **2015**

Christof Paar, Jan Pelzl, Tim Güneysu, "**Understanding Cryptography From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms**", Springer, 2nd Edition, **2024**

Indicative Experiments

1. Consider a sender and receiver who need to exchange data confidentially using symmetric encryption. Write program that implements DES encryption and decryption.	3 hours
2. Consider a sender and receiver who need to exchange data confidentially using symmetric encryption. Write program that implements AES-128/192/256 cryptosystem.	3 hours
3. (i) Implement RSA algorithm to verify the user transmitted messages. (ii) Implement Elliptic Curve Cryptography	2 hours
4. Implement hashing algorithm that generates hash-based Message Authentication Code.	2 hours
5. Find a Message Authentication Code for given variable size message by using SHA-128 and SHA-256 Hash algorithm. Measure the time consumptions for varying message size for both SHA-128 and SHA-256.	4 hours
6. Apply Digital Signature Standard for verifying the legal communication parties.	4 hours

7. Verify the keys shared by implementing Diffie Hellman multiparty key exchange protocol while performing Man-in-the- Middle Attack.	2 hours
8. Write a simple client and server application using SSL socket communication.	2 hours
9. Write a simple client server model and capture the packets using packet capturing tools. Analyze the PCAP file and get the transmitted data (plain text) using any packet capturing tool. Implement the above scenario using SSH and observe the data.	2 hours
10. Construct Intrusion Detection System rules to notify attack traffic flows.	2 hours
11. Send and receive an encrypted email message using S/MIME.	2 hours
12. Construct IP tables for incoming network traffic flows.	2 hours
Total Laboratory Hours:	**30 hours**
Mode of Evaluation : Continuous Assessment Test, Digital Assignment, Quiz, Final Assessment Test, Lab Continuous Assessment, Lab Final Assessment, Oral Examination, Seminar, Group Discussion, Presentation	
Recommended by Board of Studies :	02-06-2025
Approved by Academic Council : No. 78	12-06-2025