Course: BTech **Semester:** 6

Prerequisite: Basic knowledge of computer networks, cryptography, operating systems, programming, data structures, and cybersecurity fundamentals is required.

Course Objective: This course introduces the fundamental principles of cryptography and its applications on the network security domain as well as software development domain. This subject covers various important topics concerning information security like symmetric and asymmetric cryptography, hashing, message and user authentication, digital signatures, key distribution and overview of the malware technologies. The subject also covers the applications of all of these in real life situations

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Seminar Hrs/Week	Credit	Internal Marks			External Marks		
					T	CE	P	T	P	
3	0	0	0	3	20	20	-	60	-	100

SEE - Semester End Examination, **T** - Theory, **P** - Practical

Course Content

W - Weightage (%) , **T** - Teaching hours

Sr.	Topics	W	T
1	**Introduction:**Computer Security Concept, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanism, A Model for Network Security.	6	2
2	**Classical Encryption Techniques:**Symmetric Cipher Model, Cryptanalysis, Cryptanalysis Attacks, Substitution Techniques: Caesar Cipher, Monoalphabetic Cipher, Hill Cipher, Play fair Cipher, Polyalphabetic Cipher, OTP, Transposition Techniques, Steganography.	12	6
3	**Block Ciphers and the Data Encryption Standard**Stream ciphers and block ciphers, Block Cipher Principles, Data Stream ciphers and block ciphers, Confusion & Diffusion, Block Cipher Principles, Data Encryption Standard (DES), Deferential and Linear Cryptanalysis, Avalanche Effect, strength of DES, Design principles of block cipher. **Multiple Encryption and Triple DES** Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode.	20	14
4	**Number theory and Advance Encryption Standard**The Euclidean Algorithm, Modular Arithmetic, Finite Fields of the Form GF (p), Polynomial Arithmetic, Advance Encryption Standard (AES): structure, key expansion.	15	6
5	**Asymmetric Ciphers**Prime Numbers, Principles of Public-Key Cryptosystems, The RSA Algorithm, Diffie-Hellman Key Exchange, Man in the Middle attack.	15	4
6	**Cryptographic Data Integrity Algorithms**Hash Function: Hash Function and its Application, Security Requirements for Cryptographic Hash Functions, Hash Functions Based on Cipher Block Chaining, Secure Hash Algorithm (SHA), and MAC: Message Authentication Requirements, Message Authentication Functions, Requirements for Message Authentication Codes, Security of MACs, HMAC, Digital Signature: Introduction to Digital Signatures, Digital Signature Standard.	20	8
7	**Key Management and Distribution**Symmetric Key Distribution: Symmetric Key Distribution Using Symmetric Encryption, Symmetric Key Distribution Using Asymmetric Encryption, Asymmetric Key Distribution: Distribution of Public Keys, X.509 certificates, Advanced Topics: Firewall, Intruders, Virus, Trojans, Malware, and Ransomware.	12	5

Reference Books

1.	**Cryptography and Network Security** By William Stallings | Pearson Education
2.	**Cryptography & Network Security** By Behrouz A. Forouzan | Tata McGraw-Hill
3.	**Information Security Principles and Practice** By Deven Shah, | Wiley-India
4.	**Information Security Principles and Practice** By Mark Stamp, Willy India Edition
5.	**Information systems security** By Nina Godbole | Wiley Publications,2008

Course Outcome

After Learning the Course the students shall be able to:

1. Understand the need for information security, its importance, and applications.
2. Compare symmetric and asymmetric cryptography with the use of hashing algorithms for secure data processing.
3. Implementation of authentication mechanisms for secure communication.
4. Explain the digital signatures and certificates, their role in authentication and integrity, key management techniques, and remote authentication for secure access.
5. Analyze the software vulnerabilities and malware threats, and secure coding practices to mitigate risks.