Program	Bachelor of Technology (BTech)	**Semester - 6**
Type of Course	Professional Core	
Prerequisite	Fundamental concepts of programming and Mathematics	
Course Objective	The subject covers various important topics concern to 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 applications.	

Teaching Scheme (Contact Hours)				Examination Scheme				
				Theory Marks		Practical Marks		
Lecture	Tutorial	Practical	Credit	SEE (T)	CIA (T)	SEE (P)	CIA (P)	Total Marks
3	0	2	4	70	30	25	25	150

***SEE** - Semester End Examination, **CIA** - Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)*

Course Content

T - Teaching Hours | **W** - Weightage

Sr.	Topics	T	W
1	**Introduction to Symmetric Cipher, Stream Ciphers, and Block Ciphers** Symmetric Cipher Model, Cryptography, Cryptanalysis and Attacks, Substitution and Transposition techniques, Stream ciphers and block ciphers, Block Cipher structure.	7	20
2	**DES, AES, and Modes of operation** Data Encryption standard (DES) with example, strength of DES, Design principles of block cipher, AES with structure, its transformation functions, key expansion, example and implementation, Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode.	10	20
3	**Public Key Encryption and Hash Algorithms** Public Key Cryptosystems with Applications, Requirements and Cryptanalysis, RSA algorithm, its computational aspects and security, Diffie-Hillman Key Exchange algorithm, Man-in-Middle attack, Cryptographic Hash Functions, their applications, Simple hash functions, its requirements and security, Hash functions based on Cipher Block Chaining, Secure Hash Algorithm (SHA).	10	20
4	**MAC and Digital Signature** Message Authentication Codes, its requirements and security, MACs based on Hash Functions, MACs based on Block Ciphers, Digital Signature, its properties, requirements and security, various digital signature schemes (Elgamal and Schnorr), NIST digital Signature algorithm.	9	20
5	**Key Management and Remote User Authentication** Key management and distribution, symmetric key distribution using symmetric and asymmetric encryptions, distribution of public keys, X.509 certificates, Public key infrastructure, Remote user authentication with symmetric and asymmetric encryption, Kerberos.	9	20
	Total	**45**	**100**

Suggested Distribution Of Theory Marks Using Bloom's Taxonomy

Level	Remembrance	Understanding	Application	Analyze	Evaluate	Create
Weightage	10	40	50	0	0	0

NOTE : This specification table shall be treated as a general guideline for the students and the teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Course Outcomes

At the end of this course, students will be able to:	
CO1	**demonstrate** symmetric ciphers, stream ciphers and block ciphers.
CO2	**implement** DES, AES and modes of operations.
CO3	**execute** public key encryption and hash algorithm.
CO4	**perform** techniques of MAC and digital signature.
CO5	**expremient** key management and remote user authentication.

Reference Books

1.	**Cryptography & Network Security: Principles and Practice (TextBook)** By W. Stallings | Prentice Hall
2.	**Cryptography & Network Security** By Behrouz A. Forouzan and Debdeep Mukhopadhyay | Tata Mcgraw Hill Education Private Limited | Second Edition, Pub. Year 2011
3.	**Information Security Principles and Practice** By Deven Shah | Wiley | 2nd
4.	**Cryptography and Network Security** By Atul Kahate | Tata McGraw-Hill | 2nd

List of Practical

1.	**Study of passive and active attacks on computer systems.**
2.	**Implementation of caesar cipher techniques**
3.	**Implementation monoalphabetic substitution cipher technique**
4.	**Demonstration of polyalphabetic cipher technique**
5.	**Implementation of playfair cipher technique**
6.	**Implementation of hill cipher technique**
7.	**Implementation of vermin cipher technique**
8.	**Implementation of rail fence cipher technique**
9.	**Implementation of RSA Algorithm technique**
10.	**Implementation of Diffie Hellman Key exchange technique**