SARVAJANIK UNIVERSITY
INCLUSIVE | INTEGRATED | INNOVATIVE

SARVAJANIK UNIVERSITY
Sarvajanik College of Engineering and Technology
Bachelor of Technology

Year: B. Tech IV (Semester VII)

Subject Name: Information Security **Subject Code:** BTAI14701
Type of course: Professional Elective Course
Prerequisite (if any): - -

Rationale: The use of the Internet for various purpose including social, business, communication and other day to day activities has been in common place. The information exchanged through Internet plays vital role for their owners and the security of such information/data is of prime importance. Knowing the concepts, principles and mechanisms for providing security to the information/data is very important for the students of Computer Engineering/Information technology. The subject covers various important topics concern to information security like symmetric and asymmetric cryptography, hashing, message and user authentication, digital signatures, as well as Law and Ethics in Information Security.

Teaching and Examination Scheme:

Teaching Scheme				Theory Marks			Practical Marks		Total
L	T	P	C	TEE	CA1	CA2	TEP	CA3	
3	0	0	3	60	25	15	0	0	100

CA1: Continuous Assessment (assignments / projects / open book tests / closed book tests) CA2: Sincerity in attending classes / class tests / timely submissions of assignments / self-learning attitude / solving advanced problems TEE: Term End Examination TEP: Term End Practical Exam (Performance and viva on practical skills learned in course) CA3: Regular submission of Lab work / Quality of work submitted / Active participation in lab sessions / viva on practical skills learned in course.

Contents:

Sr. No.	Contents	Total Hours
1.	**Introduction** Computer Security Concepts, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A Model for Network Security	04
2.	**Number Theory and Finite Fields** Divisibility and the Division Algorithm, Euclidean Algorithm, Modular Arithmetic, Groups, Rings and Fields, Finite Fields of the Form GF(p)	07
3.	**Symmetric Ciphers** Classical Encryption Techniques, Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Block Ciphers and the Data Encryption Standard,	08

	Traditional Block Cipher Structure, The Data Encryption Standard with Example, Advance Encryption Standard with Example	
4.	**Asymmetric Ciphers** Principles of Public-Key Cryptosystems, RSA Algorithm, Diffie-Hellman Key Exchange, Elgamal Cryptographic System	06
5.	**Cryptographic Data Integrity Algorithms** Applications of Cryptographic Hash Functions, Two Simple Hash Functions, Requirements and Security, Hash Functions Based on Cipher Block Chaining, Secure Hash Algorithm (SHA), Message Authentication Requirements, Message Authentication Functions, Requirements for Message Authentication Codes, Security of MACs, MACs Based on Hash Functions, MACs based on Block Ciphers	08
6.	**Digital Signature** Introduction, Digital Signature properties, Requirements and Security, Elgamal Digital Signature Scheme	06
7.	**Legal Issues in Security and Risk Management** Law and Ethics in Information Security, International Laws and Legal Bodies, Ethics and Information Security, Overview of Risk Management, Risk Identification and Risk Assessment, Risk Control Strategies	06

Suggested Specification table with Marks (Theory): (For B. Tech only)

Distribution of Theory Marks					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
15	20	10	15	-	-

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (Revised Bloom's Taxonomy)

Reference Books:

Sr no	**Title of book /article**	**Author(s)**	**Publisher and details like ISBN**	**Year of publication**	**Publication Edition**
1	Cryptography And Network Security, Principles And Practice	William Stallings	Pearson	2014	5th Edition
2	Information Security Principles and Practice	Mark Stamp	Willy India Edition	2011	2nd Edition
3	Cryptography &	Behrouz A.	McGraw Hill	2007	3rd Edition

	Network Security	Forouzan, Debdeep Mukhopadhyay			
4	Principles of Information Security	Michael E Whitman and Herbert J Mattord	Vikas Publishing House	2003	6th Edition

Course Outcomes (CO):

Sr. No.	CO statements	Marks % weightage
CO-1	Comprehend the fundamental concepts of security viz. OSI security architecture, security services, security mechanisms, security model.	15%
CO-2	Apply the mathematical operations on to the problems related to cryptography.	25%
CO-3	Discuss the algorithms for data encryption using symmetric key ciphers, asymmetric key ciphers and for data integrity using digital signature, hashing.	50%
CO-4	Comprehend the legal and ethical issues in Security and Risk management.	10%