GUJARAT TECHNOLOGICAL UNIVERSITY

Bachelor of Engineering
Subject Code: 3170720
Semester – VII
Subject Name: Information Security

Type of course: Elective

Prerequisite: Mathematical concepts: Random numbers, Number theory, finite fields

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, key distribution and overview of the malware technologies. The subject also covers the applications of all of these in real life applications.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
				Theory Marks		Practical Marks		
L	T	P	C	ESE (E)	PA (M)	ESE (V)	PA (I)	
3	0	2	4	70	30	30	20	150

Content:

Sr. No.	Content	Total Hrs
1	Symmetric Cipher Model, Cryptography, Cryptanalysis and Attacks; Substitution and Transposition techniques	03
2	Stream ciphers and block ciphers, Block Cipher structure, 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	08
3	Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode	04
4	Public Key Cryptosystems with Applications, Requirements and Cryptanalysis, RSA algorithm, its computational aspects and security, Diffie-Hillman Key Exchange algorithm, Man-in-Middle attack	08
5	Cryptographic Hash Functions, their applications, Simple hash functions, its requirements and security, Hash functions based on Cipher Block Chaining, Secure Hash Algorithm (SHA)	05
6	Message Authentication Codes, its requirements and security, MACs based on Hash Functions, Macs based on Block Ciphers	05
7	Digital Signature, its properties, requirements and security, various digital signature schemes (Elgamal and Schnorr), NIST digital Signature algorithm	04
8	Key management and distribution, symmetric key distribution using symmetric and asymmetric encryptions, distribution of public keys, X.509 certificates, Public key	04

	infrastructure	
9	Remote user authentication with symmetric and asymmetric encryption, Kerberos	**04**

Suggested Specification table with Marks (Theory):

Distribution of Theory Marks					
R Level	U Level	A Level	N Level	E Level	C Level
7	14	21	14	7	7

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

Reference Books:

1. Cryptography And Network Security, Principles And Practice Sixth Edition, William Stallings, Pearson
2. Information Security Principles and Practice By Mark Stamp, Willy India Edition
3. Cryptography & Network Security, Forouzan, Mukhopadhyay, McGrawHill
4. Cryptography and Network Security Atul Kahate, TMH
5. Cryptography and Security, C K Shyamala, N Harini, T R Padmanabhan, Wiley-India
6. Information Systems Security, Godbole, Wiley-India
7. Information Security Principles and Practice, Deven Shah, Wiley-India
8. Security in Computing by Pfleeger and Pfleeger, PHI
9. Build Your Own Security Lab : A Field Guide for network testing, Michael Gregg, Wiley India

Course Outcomes:

Sr. No.	**CO statement**	**Marks % weightage**
CO-1	Explore the basic principles of the symmetric cryptography and techniques with their strengths and weaknesses from perspective of cryptanalysis	10
CO-2	Implement and analyze various symmetric key cryptography algorithms and their application in different context.	25
CO-3	Compare public key cryptography with private key cryptography and Implement various asymmetric key cryptography algorithms.	25
CO-4	Explore the concept of hashing and implement various hashing algorithms for message integrity.	20
CO-5	Explore and use the techniques and standards of digital signature, key management and authentication.	20

List of Experiments:

Minimum 10 practices are to be performed covering the contents of the syllabus. Use of the tools for performing practices is highly recommended.

GUJARAT TECHNOLOGICAL UNIVERSITY

Bachelor of Engineering
Subject Code:

List of e-Learning Resources:

1. Software: cryptool (www.cryptool.org)
2. Software: Wireshark (**www.wireshark.org**)
3. http://www.cryptix.org/
4. http://www.cryptocd.org/
5. http://www.cryptopp.com/
6. **https://nptel.ac.in/**
7. **https://www.coursera.org/**