GUJARAT TECHNOLOGICAL UNIVERSITY

SUBJECT NAME: Information and Network Security
SUBJECT CODE: 2170709
B.E. Semester VII

Type of course: Core course

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
L	T	P	C	Theory Marks			Practical Marks			
				ESE (E)	PA (M)		ESE (V)		PA (I)	
					PA	ALA	ESE	OEP		
4	0	2	6	70	20	10	20	10	20	150

L- Lectures; T- Tutorial/Teacher Guided Student Activity; P- Practical; C- Credit; ESE- End Semester Examination; PA- Progressive Assessment;

Contents:

Sr. No.	**Content**	**Total HRS**	**% Weightage**
1	Symmetric Cipher Model, Cryptography, Cryptanalysis and Attacks; Substitution and Transposition techniques	3	5%
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	10	25%
3	Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode	4	5%
4	Public Key Cryptosystems with Applications, Requirements and Cryptanalysis, RSA algorithm, its computational aspects and	7	15%

	security, Diffie-Hillman Key Exchange algorithm, Man-in-Middle attack		
5	Cryptographic Hash Functions, their applications, Simple hash functions, its requirements and security, Hash functions based on Cipher Block Chaining, Secure Hash Algorithm (SHA)	4	10%
6	Message Authentication Codes, its requirements and security, MACs based on Hash Functions, Macs based on Block Ciphers	3	10%
7	Digital Signature, its properties, requirements and security, various digital signature schemes (Elgamal and Schnorr), NIST digital Signature algorithm	4	8%
8	Key management and distribution, symmetric key distribution using symmetric and asymmetric encryptions, distribution of public keys, X.509 certificates, Public key infrastructure	4	7%
9	Remote user authentication with symmetric and asymmetric encryption, Kerberos	4	5%
10	Web Security threats and approaches, SSL architecture and protocol, Transport layer security, HTTPS and SSH	5	10%

Suggested Specification table with Marks (Theory):

Distribution of Theory Marks					
R Level	U Level	A Level	N Level	E Level	C Level
15	**20**	**20**	**5**	**5**	**5**

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

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

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 Outcome:

After learning the course the students should be able to:

- Define the concepts of Information security and their use.
- Describe the principles of symmetric and asymmetric cryptography.
- Understand and apply the various symmetric key algorithms.
- Understand and apply the various asymmetric key algorithms.
- Understand the concepts of hashing with algorithms and apply them.
- Understand and use the message authentication and its requirement.
- Understand the concepts of digital signature and digital certificates.
- List and explain various digital signature algorithms.
- Understand and use the various key management and remote authentication mechanisms.
- Understand the concept transport layer security.

List of Experiments:

1. Implement Caesar cipher encryption-decryption.
2. Implement Monoalphabetic cipher encryption-decryption.
3. Implement Playfair cipher encryption-decryption.
4. Implement Polyalphabetic cipher encryption-decryption.
5. Implement Hill cipher encryption-decryption.
6. To implement Simple DES or AES.
7. Implement Diffi-Hellmen Key exchange Method.
8. Implement RSA encryption-decryption algorithm.
9. Write a program to generate SHA-1 hash.
10. Implement a digital signature algorithm.
11. Perform various encryption-decryption techniques with cryptool.
12. Study and use the Wireshark for the various network protocols.

Design based Problems (DP)/Open Ended Problem:

1. Study the standard document for the security policy for an organization and prepare the detailed security policy document for managing information security for your institute.
2. Study the keytool provided by the Java to generate key pairs for public key cryptography. Design and develop your own such tool to generate the key pair and test the pair with RSA implementation for encyprion-decyprion.
3. Study how the browsers manage the digital certificates for various secured websites for making secured communication.

Major Equipments:

- Latest PCs with related software

List of Open Source Software/learning website:

- Software: cryptool (www.cryptool.org)
- Software: Wireshark (**www.wireshark.org**)
- http://www.cryptix.org/
- http://www.cryptocd.org/
- http://www.cryptopp.com/

ACTIVE LEARNING ASSIGNMENTS: Preparation of power-point slides, which include videos, animations, pictures, graphics for better understanding theory and practical work – The faculty will allocate chapters/ parts of chapters to groups of students so that the entire syllabus to be covered. The power-point slides should be put up on the web-site of the College/ Institute, along with the names of the students of the group, the name of the faculty, Department and College on the first slide. The best three works should submit to GTU.