GUJARAT TECHNOLOGICAL UNIVERSITY

Bachelor of Engineering
Subject Code: 3154501

Semester – VI
Subject Name: Cryptography and Network security

Type of course: core

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

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 network security issues. 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)	
4	0	2	5	70	30	30	20	150

Content:

Sr. No.	Content	Total HRS	% Weightage
1	Introduction & Classical Encryption Techniques : Security trends - Legal, Ethical and Professional Aspects of Security, Need for Security at Multiple levels, Security Policies - Model of network security – Security attacks, services and mechanisms – OSI security architecture – Symmetric cipher Model, Classical encryption techniques: substitution techniques, transposition techniques, steganography).- Foundations of modern cryptography: perfect security – information theory – product cryptosystem – cryptanalysis.	9	15%
2	Block Ciphers & Symmetric Key Cryptography : 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	7	10%
3	Block Cipher Operations : Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback	5	7%

	mode, Counter mode		
4	Number Theory & Asymmetric Key Cryptography : Finite fields – group, ring, fields, , The Euclidean algorithm, Fermat's and Euler's Theorems, Public Key Cryptosystems with Applications, Requirements and Cryptanalysis, RSA algorithm, its computational aspects and security, Diffie - Hillman Key Exchange algorithm, Man-in-Middle attack	9	15%
5	Cryptographic Hash Functions : Application of Cryptographic Hash Functions, Simple hash functions, its requirements and security, Hash functions based on Cipher Block Chaining, Secure Hash Algorithm (SHA)	4	7%
6	Message Authentication Codes : Requirements and security of Message Authentication Codes , MACs based on Hash Functions, MACs based on Block Ciphers	4	7%
7	Digital Signatures : Digital Signature, its properties, requirements and security, various digital signature schemes (Elgamal and Schnorr), NIST digital Signature algorithm	6	8%
8	Key Management and 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	8	10%
9	Transport Level Security : Web Security threats and approaches, SSL architecture and Protocol, Transport layer security, HTTPS and SSH.	4	7%
10	Electronic Mail Security : Internet Mail Architecture, Email Formats, Email threats and comprehensive email security, S/MIME, Pretty good privacy	4	7%
11	IP Security : IP Security Overview, IP security policy, Encapsulating Security Payload, Combining Security Associations and Key Management, Intrusion detection system IP Security.	4	7%

Suggested Specification table with Marks (Theory): (For BE only)

Distribution of Theory Marks					
R Level	U Level	A Level	N Level	E Level	C Level
7	**28**	**21**	**07**	**07**	**--**

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

GUJARAT TECHNOLOGICAL UNIVERSITY

Bachelor of Engineering
Subject Code:

Course Outcomes: Students will be able to

CO-No	CO statement	Marks % weightage
CO- 1	Explain basic terminology of information security and conventional techniques of cryptography.	15%
CO- 2	Apply standard symmetric key and asymmetric key algorithms used to provide confidentiality, integrity and authenticity.	25%
CO- 3	Analyze algorithms of message integrity , message authentication and digital signature	25%
CO- 4	Select proper key distribution and management schemes to solve security problems	10%
CO- 5	Explore different web security mechanisms and apply different network security concepts based on email security and IP security.	15%
CO- 6	Design secure applications using cryptographic mechanisms.	10%

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

List of open source software/website:

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**

8. **http://www.dvwa.co.uk/**
9. **https://www.tutorialspoint.com/cryptography/**

GUJARAT TECHNOLOGICAL UNIVERSITY

Bachelor of Engineering
Subject Code:

List of Practical:

1	Implement Ceasar and Hill cipher. Both are substitution cipher. Analyze the strength of the cipher in terms of brute force attack and cryptanalysis attack. Suggest one way to improve and strengthen the cipher and analyze with respect to cryptanalysis attack.
2	Implement Monoalphabetic Cipher. Mono alphabetic cipher is a substitution cipher in which for a given key od size 26 letter, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if 'A' is encrypted as 'D', for any number of occurrence in that plaintext, 'A' will always get encrypted to 'D'.
3	Implement playfair cipher. The plaintext is paired in two characters. Discuss the advantage of polyalphabetic cipher over monoalphabetic cipher. Key = MONARCHY Plaintext = ar mu hs ea Ciphertext = RM CM BP IM
4	Implement Vegenere Cipher. Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. The alphabet used at each point depends on a repeating keyword. • Input : Plaintext : GEEKSFORGEEKS • Keyword : AYUSH • Output : Ciphertext : GCYCZFMLYLEIM For generating key, the given keyword is repeated in a circular manner until it matches the length of the plain text.The keyword "AYUSH" generates the key "AYUSHAYUSHAYU"
5	Generate random number of 32 bits. Use different random number generation algorithms. Which method gives the best ? Random number must pass 3 tests 1. Uniformity 2. Scalabilty 3. Consistency First method: Linear congruential generator $X_{n+1} = (aX_n + c) \bmod m$ (m,a,c,X_0 are integers.) Second method : Blum Blum shub generator
6	Implement rail Fence and transposition cipher. Both are permutation cipher. Analyze the strength of the cipher in terms of crypt analysis. (For Transposition Key : 4312567, for rail fence consider depth 2) Plaintext: attackpostponeduntiltwoam
7	Implement DES algorithm.
8	Implement AES-128 algorithm.
9	Implement Euclid algorithm to find GCD.

10	Implement RSA algorithm. Take two prime numbers p,q such that n=pxq Initially take encryption key such that it is relatively prime with ϕ(n). Find out decryption key. Take plaintext message M, Ciphertext $C=M^e$ mod n. To get plaintect from ciphertext $M=C^d$ mod n. Test case : Two prime numbers 17,11 Encryption key = 7 Decryption key = 23 M=88 C=11
11	Implement Diffi-Hellmen Key exchange Method.
12	Write a program to generate SHA-1 hash.
13	Write a program that creates a shortcut of a file.(Virus program)
14	Implement a digital signature algorithm. To learn how to do file and email encryption using Gpg4win software (This software uses GnuPG public-key cryptography for data encryption and digital signatures.)
15	Demonstrate various encryption-decryption techniques with various Security tools/Cryptool.
16	Read traffic going on network. Analyze the traffic. Connect to internet and Read what is going on internet. Hint : Use Wireshark
17	Steps to ensure Security of any one web browser (Mozilla Firefox/Google Chrome)
18	Analysis the security vulnerabilities of E-Mail Application
19	Create your own website in cloud and perform security testing on it in order to find out web application vulnerabilities such as buffer overflow, credentials management, CRLF injection, cross-site request forgery, cross-site scripting, directory traversal, failure to restrict URL access, insecure cryptographic storage, LDAP injection, malicious code, OS command injection, race condition, SQL injection etc., and resolve and troubleshoot these problems