GUJARAT TECHNOLOGICAL UNIVERSITY

Bachelor of Engineering
Subject Code: 3161606
Semester – VI
Subject Name: Cryptography and Network security

Type of course: core

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)	
3	0	2	4	70	30	30	20	150

Content:

Sr. No.	**Content**	**Total HRS**	**% Weightage**
1	Introduction – Security services, security services, security mechanisms Finite fields – group, ring, fields, modular arithmetic, The Euclidean algorithm.	5	15%
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	5	10%
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 security, Diffie-Hillman Key Exchange algorithm, Man-in-Middle attack	7	15%
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): (For BE only)

Distribution of Theory Marks					
R Level	U Level	A Level	N Level	E Level	C Level
10	**40**	**20**	**--**	**--**	**--**

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

Course Outcomes: Students will be able to

Sr. No.	CO statement	Marks % weightage
CO-1	Define terms related to cryptography, hashing, message authentication code, digital signature.	20
CO-2	Describe and discuss symmetric key cryptography algorithms, public key cryptography algorithms, hashing algorithms, Message authentication code generation algorithms, digital signature algorithms, key generation and key management, issues in web security and solution, issues in Transport layer security and solution.	30
CO-3	Demonstrate the generation of keys and execution of symmetric and public key algorithms from given data.	40
CO-4	Implement cryptography solution for given security problem by identifying strength and weaknesses of algorithms based on	10

	cryptanalytic and brute force attack.	

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 opensource software/website:

https://www.wireshark.org/

List of Practical:

1.	Implement RSA algorithm. Take two prime numbers p,q n=pxq Initially take encryption key such that it is relatively prime with $\phi(n)$. 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

2.	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

3.	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. Ceasar cipher - You are given plaintext Hello, Welcome. The key used is 3. How Ceaser cipher will work? Test case :

	A B C D E F Hill Cipher - Key K = $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$ Plaintext = pay Ciphertext = RRL
5.	Implement Euclid algorithm to find GCD. GCD(16,12) = 4 GCD(12,4) = 0 Then 4 is the GCD(16,12)
6.	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 $X_{n+1} = (aX_n + c) \text{ mod } m$ m,a,c,X_0 are integers. Second method : Blum Blum shub generator

7.	Implement Euler's totient function $\phi(n)$ .It is defined as the number of positive integers less than n and relatively prime to n. Find $\phi(35)$ and $\phi(37)$. Observe the value and analyze the behavior of totient function.
8.	Write a program that creates a shortcut of a file.(Virus program)
9.	Write a program that increases file size by 10.
10.	Implement rail Fence and transposition cipher. Both are permutation cipher. Analyze the strength of the cipher in terms of cryptanalysis. Rail fence. Test case : Meetme Ciphertext : MEMETE Transposition Key : 4312567 Plaintext: attackpostponeduntiltwoam Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ
11.	Read traffic going on network. Analyze the traffic. Connect to internet and Read what is going on internet. Hint : Use Wireshark