GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Engineering
Level: Diploma
Branch: Information Technology
Course / Subject Code: DI03016021
Course / Subject Name: Cryptography and Web Security

w. e. f. Academic Year:	2024-25
Semester:	3rd
Category	PCC

Prerequisite:	Basic knowledge of computer networks, website and Internet, Basic mathematical concepts and modular arithmetic.
Rationale:	Understanding cryptography and web security is essential in today's digital landscape, where the protection of sensitive information is the main goal. It is the backbone of secure communication, financial transactions and data integrity across the internet. Incorporating cryptography fosters a culture of security awareness, essential for protecting information in our increasingly connected world. The subject **Cryptography and Web Security** aims to equip students with the foundational knowledge and practical skills required to understand and apply key security principles. The students will explore essential cryptographic algorithms: symmetric and asymmetric, and study their applications in real-world scenarios. The course also covers critical web security protocols including SSL, HTTPS, and firewall mechanisms, enabling students to understand vulnerabilities and secure online systems. Through Python-based programming implementations, students will gain hands-on experience in developing simple cryptographic solutions, thereby enhancing their analytical, problem-solving, and technical skills. This subject lays a strong foundation for advanced studies and careers in cyber security, ethical hacking, and secure software development.

Course Outcome:

After the completion of the course, the student will be able to:

No	Course Outcomes	RBT Level
01	Explain the concept of information security in network communication.	Understand
02	Use number theory to solve problems related to cryptographic computations.	Apply
03	Implement various cryptographic techniques.	Apply
04	Use web security principles and protocols to ensure secure communication.	Apply
05	Classify various types of firewalls based on their characteristics.	Understand

**Revised Bloom's Taxonomy (RBT)*

Teaching and Examination Scheme:

Teaching Scheme (in Hours)			Total Credits L+ T+ (PR/2)	Assessment Pattern and Marks				Total Marks
				Theory		Tutorial/Practical		
L	T	PR	C	ESE (E)	PA(M)	PA(I)	ESE (V)	
3	0	2	4	70	30	20	30	150

Course Content:

Unit No.	Content	No. of Hours	% of Weightage
1.	**Introduction of Information & Network Security** 1.1 Computer Security, Cyber Security, Information Security and Network Security 1.2 Essential network and computer security requirements 1.2.1 Confidentiality 1.2.2 Integrity 1.2.3 Availability 1.2.4 Authenticity 1.2.5 Accountability 1.3 The OSI Security Architecture 1.4 Security Attacks: Passive Attacks, Active Attacks 1.5 Security Services 1.5.1 Authentication 1.5.2 Access control 1.5.3 Data confidentiality 1.5.4 Data integrity 1.5.5 Nonrepudiation 1.5.6 Availability Service 1.6 Security Mechanisms 1.6.1 Specific Security Mechanism 1.6.2 Pervasive Security Mechanism 1.7 Model for Network Security 1.8 Cryptography: Concept & Classification 1.8.1 Key-less 1.8.2 Single-key and Two-key algorithms	9	18
2.	**Number theory in Cryptography** 2.1 Divisibility and Division algorithm 2.2 Modulo operator 2.2.1 Modular arithmetic properties over addition, subtraction and multiplication operations. 2.3 Set of residues: Z_n 2.3.1 Inverse: additive & multiplicative 2.3.2 Set of multiplicative inverse Z_n^*	8	16

	2.3.3 Calculation of addition – multiplication tables with its inverse 2.4 Calculation of GCD and Multiplicative inverse 2.4.1 Euclidean algorithm for GCD 2.4.2 Extended Euclidean algorithm for multiplicative inverse		
3.	**Classical Encryption Techniques** 3.1 Symmetric-key Encryption 3.1.1 Symmetric cipher model 3.1.2 Cryptanalysis and types of attacks 3.1.3 Brute-Force attack 3.2 Substitution ciphers 3.2.1 Mono alphabetic ciphers: Additive, Multiplicative, Affine and Mono alphabetic substitution cipher. 3.2.2 Poly alphabetic ciphers: Autokey, Vigenère, Playfair, Hill, One-time pad cipher. 3.3 Transposition ciphers 3.3.1 Keyless transposition: Rail fence, rectangular (columnar) 3.3.2 Keyed transposition method, keyed columnar transposition, its key inversion 3.3.3 Stream and Block ciphers 3.4 Asymmetric-key Cryptosystem 3.4.1 Ingredients of public-key encryption 3.4.2 Confidentiality in public-key cryptography, Authentication in public-key cryptography, 3.4.3 Basic working of RSA algorithm and its key-generation.	**12**	**26**
4.	**Web Security** 4.1 Web Security Considerations 4.1.1 Web security threats 4.1.2 Web traffic security approaches 4.2 Secure Socket Layer and Transport Layer Security 4.2.1 Overview of SSL Protocol Stack 4.2.2 Overview of TLS Protocol Stack 4.3 HTTPS 4.3.1 Connection initiation 4.3.2 Connection closure 4.4 Basic Concept of Secure Electronic Transactions 4.5 SSL versus SET	**10**	**24**
5.	**System Security** 5.1 Intrusion detection 5.1.1 Intrusion and classification of intruders: Masquerador, Misfeasor, and Clandestine users 5.1.2 Intrusion detection system and approaches to intrusion detection: Misuse detection, Anomaly detection 5.2 Firewall (Definition and Need) 5.2.1 Characteristics of Firewall 5.3 Types of Firewall	**6**	**16**

	5.3.1 Packet filtering firewall 5.3.2 Application-Level gateway 5.3.3 Circuit-Level gateway		
	Total	**45**	**100**

Suggested Specification Table with Marks (Theory):

Distribution of Theory Marks (in %)					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
25	**35**	**40**	**-**	**-**	**-**

Where R: Remember; U: Understanding; A: Application, N: Analyse and E: Evaluate C: Create (as per Revised Bloom's Taxonomy)

References/Suggested Learning Resources:

(A) Books:

Sr. No.	Title of Book	Author	Publication with Place, Year and ISBN
1	Cryptography and Network Security Principles and Practice	William Stallings	Pearson Publication, 2023 ISBN:9781292437484
2	Cryptography And Network Security	Behrouz A. Forouzan	McGraw Hill Education, 2015, ISBN: 9789339220945
3	Cryptography and Network Security	Atul Kahate	McGraw Hill Education, 2017, ISBN: 9781259029882
4	Cryptography Theory and Practice	Douglas Robert Stinson, Maura Paterson	CRC Press, 2018 ISBN: 9781138197015

(B) Open source software and website:

1. https://nptel.ac.in/courses/106105031
2. https://cse29-iiith.vlabs.ac.in/
3. https:// www.youtube.com/c/NesoAcademy
4. https://www.tpointtech.com/firewall
5. https://www.learnpython.org/

Suggested Course Practical List:

The following practical outcomes (PrOs) are the subcomponents of the COs. These PrOs need to be attained to achieve the COs.

Sr. No.	Practical Outcomes (PrOs)	Unit No.	Approx. Hrs. required
1	Prepare a study report on recent cyber-attacks in India and its impact.	1	2
2	Calculate Greatest Common Divisor using Euclidean algorithm. Display each step in tabular format.	2	2

3	Implement Extended Euclidean algorithm to check whether the multiplicative inverse exists or not in Z_n. If exist calculate positive inverse.	2	2
4	Prepare a module for Additive cipher. Implement encryption and decryption algorithms in two separate user-defined functions in it. Write an interactive program that inputs plain text, key and performs encryption-decryption.	3	2
5	Write a program to apply Brute-force attack on cipher text and find the key as well as plain text which is encrypted by Additive cipher.	3	2
6	Prepare a module for Multiplicative cipher. Define two separate functions for encryption and decryption algorithms in the module. Write an interactive program that inputs plain text, key and performs encryption-decryption using this module.	3	2
7	Prepare a module for Mon alphabetic substitution cipher. Define two separate functions for encryption and decryption algorithms in it. Write an interactive program that inputs key (mapping of 26 characters to each other), plain text and performs encryption-decryption using this module.	3	4
8	Prepare a module for Autokey cipher. Define two separate functions for encryption and decryption algorithms in it. Write an interactive program that inputs plain text, key and performs encryption-decryption using this module.	3	2
9	Prepare a module for Vigenère cipher. Define two separate functions for encryption and decryption algorithms in the module. Write an interactive program that inputs plain text, key and performs encryption-decryption using this module.	3	2
10	Prepare a module for matrix multiplication. Write an interactive program that inputs plain text, perform necessary calculation and then call matrix multiplication( ) to perform encryption and decryption using Hill cipher (3×3 matrix i.e. maximum plain text length = 9 characters). If less characters input then pad with character 'z'. Key matrix (K) is given with its inverse (K^{-1}). One of the key pair **K** =[5 7 10 13 0 17 7 5 4]and $K^{-1} =$ [21 14 1 0 13 8 25 3 8]	3	4
11	Prepare a module for keyless rectangular(columnar) cipher. Define two separate functions for encryption and decryption algorithms in the module. Write an interactive program that inputs plain text and performs encryption-decryption using this module. No of columns = 4.	3	2
12	Prepare a module for keyed transposition cipher. Define two separate functions for encryption and decryption algorithms in the module. Write an interactive program that inputs plain text, permutation key and performs encryption-decryption using this module.	3	2
13	Prepare a module for keyed columnar transposition cipher. Define two separate functions for encryption and decryption algorithms in the module. Write an interactive program that inputs plain text, permutation key and performs encryption-decryption using this module.	3	2

	Total		**30**

Note:-

More Practical Exercises can be designed and offered by the respective course teacher to develop the industry relevant skills/outcomes to match the COs. The above table is only a suggestive list.

List of Laboratory/Learning Resources Required:

Sr. No.	Laboratory/Learning Resources/Equipment Name with Broad Specifications	PrO. No.
1	Computer system with operating system: Windows 7 or higher version or MacOS or Linux, RAM 4GB or higher, Python version: 3.6.X or higher version.	All
2	Python IDEs and Code Editors: Open Source : IDLE, Visual Studio Code (VS Code), Jupyter, Spyder	All

Suggested Activities for Students:

Other than the classroom and laboratory learning, following are the suggested student- related co-curricular activities which can be undertaken to accelerate the attainment of the various outcomes in this course: Students should perform following activities in group and prepare reports of about 5 pages for each activity. They should also collect/record physical evidences for their (student's) portfolio which may be useful for their placement interviews:

a) Organize or attend workshops and training sessions on topics like ethical hacking, penetration testing.
b) Assign any tool for website vulnerability testing like Nessus, Nmap etc. and generate report on it.
c) Study any password cracking tool and try it on sample document. For example, John the ripper
d) Check the strength of your windows system password using L0phtCrack tool.
e) Use Cryptool 2.1 tool for various cryptographic techniques.

****