GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Engineering

Level: PG

Branch: Cyber Security

Subject Code : ME02059071

Subject Name : Advanced Cryptography Techniques

w. e. f. Academic Year:	2024-25
Semester:	2
Category of the Course:	Professional Elective Course

Prerequisite:	• Basic of cryptography, introduction to encryption/decryption and hashing algorithms.
Rationale:	• The subject covers fundamental topics related to Key management and its distribution with various user authentication techniques. • The subject also focuses on classic as well as modern techniques of cryptanalysis and their use. • The course also put some light on the history of steganography, modern methods, algorithms and tools for steganography.

Course Outcome:

After Completion of the Course, Student will able to:

No	Course Outcomes	RBT Level
01	Understand the key management and distribution techniques with types.	UN
02	Differentiate between authentication using symmetric encryption and asymmetric encryption techniques.	AN
03	Apply and test classic and modern techniques for cryptanalysis.	AP
04	Apply cryptographic backdoors for its merits and demerits.	AP
05	Evaluate various algorithms and open source tools for steganography and applications.	EL

**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 / CA (M)	PA/CA (I)	ESE (V)	
03	00	02	04	70	30	20	30	150

GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Engineering

Level: PG

Branch: Cyber Security

Subject Code : ME02059071

Subject Name : Advanced Cryptography Techniques

Course Content:

Unit No.	Content	No. of Hours	% of Weightage
1.	**UNIT-I: Introduction to Key Management and Distribution** Symmetric Key Distribution based on Symmetric Encryption, Symmetric Key Distribution based on Asymmetric Encryption, Distribution of Public Keys.	08	10
2.	**UNIT-II: User Authentication** Remote user authentication principles and techniques, Remote user authentication based on Symmetric Encryption, Kerberos, Remote user authentication based on Asymmetric Encryption, Federated Identity Management, Personal Identity Verification.	08	20
3.	**UNIT-III: Cryptanalysis** Classic techniques of cryptanalysis, Modern methods of cryptanalysis, The birthday paradox, Various other techniques for breaching cryptography.	06	20
4.	**UNIT-IV: Cryptographic Backdoors** General concepts of cryptographic backdoors, Specific use case of cryptographic backdoors, Dominance of cryptographic backdoors, Countermeasures and standard producers.	07	20
5.	**UNIT-V: Steganography** Concept of Steganography, The history behind steganography, Modern methods and algorithms, Open source tools for steganography, Steganalysis, Distributed steganography.	08	20
6	**UNIT-VI: Future of Cryptography** Cryptography and the cloud, Homomorphic cryptography, The anatomy of ransomeware attack, Modern Hardware Design Practices, Quantum cryptography, AI for Cryptography.	08	10
	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**
10	**20**	**20**	**20**	**20**	**10**

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

References/Suggested Learning Resources:

(a) Books:

1. Cryptography and Network Security, Principles and Practice Sixth Edition, William Stallings, Pearson
2. Modern Cryptography: Applied Mathematics for Encryption and Information Security, Chuck Easttom, McGraw-Hill Education
3. Cryptography & Network Security, Forouzan, Mukhopadhyay, McGraw-Hill
4. Cryptography and Network Security Atul Kahate, TMH
5. Cryptography and Security, C K Shyamala, N Harini, T R Padmanabhan, Wiley-India.

(b) Open source software and website:

1. Course-related online MOOC on SWAYAM NPTEL/Coursera Platform.
2. Recently published papers/articles of reputed journals/conferences.s

Suggested Course Practical List:

- List of Laboratory/Learning Resources Required: The practical work will be carried out based on the content covered during the academic sessions.

List of Laboratory/Learning Resources Required: Open source tools for cryptography.

Suggested Project List: Creation of local network and its security projects.

* * * * * * *