GUJARAT TECHNOLOGICAL UNIVERSITY

Master of Engineering

EF Academic Year	: 2021-22
Semester	: 2
Category of the Course	: Program Elective Course-IV
Course Name & Code	: Advanced Cryptography (4725907)

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 Scheme:

Teaching Scheme			Total Credits	Assessment Pattern and Marks				Total Marks
				Theory		Practical		
L	T	PR	C	ESE (E)	PA(M)	ESE (V)	PA (I)	
03	00	02	04	70	30	30	20	150

Course Content:

Sr. No	Course Content	No of Hours	%
1	**UNIT-I: Introduction to Key Management and Distribution** Symmetric Key Distribution Using Symmetric Encryption, Symmetric Key Distribution Using Asymmetric Encryption, Distribution of Public Keys.	08	20
2	**UNIT-II: User Authentication** Remote User-Authentication Principles , Remote User-Authentication Using Symmetric Encryption, Kerberos, Remote User Authentication Using Asymmetric Encryption, Federated Identity Management, Personal Identity Verification.	08	20

3	**UNIT-III: Cryptanalysis** Classic techniques of cryptanalysis, Modern methods, Rainbow tables, The birthday paradox, Other methods for breaching cryptography.	06	15
4	**UNIT-IV: Cryptographic Backdoors** General concepts of cryptographic backdoors, Specific examples of cryptographic backdoors, Prevalence of cryptographic backdoors, Countermeasures.	06	15
5	**UNIT-V: Steganography** Steganography basics, The history of steganography, Modern methods and algorithms, Tools for steganography, Steganalysis, Distributed steganography.	06	15
6	**UNIT-VI: The Future of Cryptography** Cryptography and the cloud, Homomorphic cryptography, The anatomy of ransomeware attack, Modern Hardware Design Practices, Quantum cryptography.	06	15

Textbooks/ Reference 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

Course Outcome:

After completion of the Course, Students will be able to:

No	Course Outcomes	RBT Level*
01	Understand the basic Key Management and distribution concepts with their various types.	UN
02	Differentiate between authentication using symmetric encryption and authentication using asymmetric encryption.	UN
03	Apply classic and modern techniques for cryptanalysis.	AP

04	Analyze various cryptographic backdoors for their merits and demerits.	AN
05	Evaluate various algorithms and tools for steganography with their applications.	EL

*RM: Remember, UN: Understand, AP: Apply, AN: Analyze, EL: Evaluate, CR: Create

Suggested Course Practical List:

- The practical work will be carried out based on the content covered during the academic sessions.

List of Laboratory/Learning Resources Required:

- Course-related online MOOCs on NPTEL/SWAYAM platform.
- Recently Published papers/articles in reputed peer-reviewed journals.
- White paper on topics covered during the syllabus.