GUJARAT TECHNOLOGICAL UNIVERSITY

Syllabus for Integrated M.Sc. (Computer Science)
(With Specialization: AI and Data Science/IoT/ Cyber Security)

With effective from academic year 2022-23

Subject Code: 1340305
Semester- IV
Subject Name: Cryptography

Teaching and Examination Scheme

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE(E)	PA (M)	PA (V)	PA (I)	
3	0	2	4	70	30	30	20	150

Content:

Sr. No.	Content	Teaching Hours	Module Weightage (%)
1	Symmetric Cipher Model, Cryptography, Cryptanalysis and Attacks; Substitution and Transposition techniques	4	10%
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	10	20%
3	Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode	8	20%
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	8	20%
5	Key management and distribution, symmetric key distribution using symmetric and asymmetric encryptions, distribution of public keys, X.509 certificates, Public key infrastructure	5	20%
6	Web Security threats and approaches, SSL architecture and protocol, Transport layer security, HTTPS and SSH	5	10%

Reference Books:

1. Cryptography And Network Security: Principles And Practice, 6th Edition, William Stallings, Pearson.
2. Information Security Principles and Practice, 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.

Course Outcome:

Subject Code: 1340305
Semester- IV
Subject Name: Cryptography

After learning the course, the students should be able to:

No.	CO statement
CO-1	Describe the principles of symmetric and asymmetric cryptography.
CO-2	Understand and apply the various symmetric, asymmetric key algorithms.
CO-3	Understand various key management and remote authentication mechanisms.
CO-4	Understand the concept transport layer security.
CO-5	Apply cryptographic techniques for preventive measures.