GUJARAT TECHNOLOGICAL UNIVERSITY
Syllabus for Integrated MSc, 8th Semester
Branch: Computer Science
Subject Name: Information and Network Security
Subject Code: 1380302

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
				Theory Marks		Practical Marks		
L	T	P	C	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	**Introduction to Computer and Network Security:** Foundations of Computer Security: Definition and Need of Computer Security; Security Basis: Confidentiality, Integrity, Availability, Accountability, Non-Repudiation and Reliability, Risk and Threat Analysis, Types of Attacks, Introduction to Information Security, Basics principles of Information Security	03	05
2	**Cryptography Techniques and Cryptographic Algorithms:** Symmetric Cipher Model, Cryptography, Cryptanalysis and Attacks; Substitution and Transposition techniques, 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, Public Key Cryptosystems with Applications, Requirements and Cryptanalysis, RSA algorithm, its computational aspects and security, Diffie-Hillman Key Exchange algorithm	10	25
3	**Public Key Infrastructure:** Digital Signature, its properties, requirements and security, various digital signature schemes (Elgamal and Schnorr), NIST digital Signature algorithm Key management and distribution, symmetric key distribution using symmetric and asymmetric encryptions, distribution of public keys, X.509 certificates, Public key infrastructure	07	15
4	**Cryptographic Hash Functions:** Cryptographic Hash Functions, their applications, Simple hash functions, its requirements and security, Hash functions based on Cipher Block Chaining, Secure Hash Algorithm (SHA)	04	10

5	**Message Authentication Codes:** Message Authentication Codes, its requirements and security, MACs based on Hash Functions, MACs based on Block Ciphers, Key Wrapping 408	03	06
6	**User Authentication and Access Control** Remote user authentication principles, Remote user authentication using symmetric and asymmetric encryption, Kerberos	03	12
7	**Network Security:** Web Security threats and approaches, SSL architecture and protocol, Transport layer security, HTTPS and SSH	04	12
8	**Software Flaws and Malware:** Introduction, Software Flaws, Buffer overflow, Incomplete Mediation, Race Conditions Malware, Brain, Morris Worm, Code red, SQL Slammer, Trojan Example, Malware Detection, The Future of Malware, Cyber Disease versus Biological diseases, Miscellaneous software-based Attacks, Salami Attacks, Linearization, Time bombs, Trusting Software Insecurity in software: Software Reverse Engineering, Anti-disassembly Techniques, Anti-Debugging Techniques Software Tamper Resistance: Guards, Obfuscation, Metamorphism Revisited	06	15

Reference Books:

1. Cryptography And Network Security, Principles And Practice Sixth Edition, William Stallings, Pearson "Fundamentals of Database Systems", 7th Edition by R. Elmasri and S. Navathe, Pearson
2. Information Security Principles and Practice By Mark Stamp, Willy India Edition
3. Cryptography & Network Security, Forouzan, Mukhopadhyay, McGrawHill
4. Cryptography and Security, C K Shyamala, N Harini, T R Padmanabhan, Wiley-India
5. Build Your Own Security Lab : A Field Guide for network testing, Michael Gregg, Wiley India

Course Outcome:

1. Explore the basic principles of the symmetric cryptography and techniques with their strengths and weaknesses from perspective of cryptanalysis
2. Implement and analyze various symmetric and asymmetric key cryptography algorithms and their application in different context.
3. Explore the concept of hashing and implement various hashing algorithms for message integrity and also compare public key cryptography with private key cryptography
4. Explore and use the techniques and standards of digital signature, key management and authentication
5. Understand the concept of malware technology and its impacts.