GUJARAT TECHNOLOGICAL UNIVERSITY
Syllabus for Integrated MSc, 6th Semester
Branch: Computer Science
Subject Name: IT security and Audit
Subject Code: 1360305

Teaching and Examination Scheme:

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

Content:

Sr. No.	Content	Teaching Hours	Module(%) Weightage
1	Symmetric Cipher Model, Cryptography, Cryptanalysis and Attacks; Substitution and Transposition techniques	03	12
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	08	16
3	Web Security Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET). Firewalls: Firewall Design principles, Trusted Systems, Intrusion Detection Systems	05	16
4	**Auditing For Security:** Introduction, Basic Terms Related to Audits, Security audits, The Need for Security Audits in Organization, Organizational Roles and Responsibilities for Security Audit, Auditors Responsibility In Security Audits, Types Of Security Audits.	05	14
5	Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode	05	16
6	Public Key Cryptosystems with Applications, Requirements and Cryptanalysis, RSA algorithm, its computational aspects and security, Diffie-Hillman Key Exchange algorithm, Man-in-Middle attack	08	14
7	Cryptographic Hash Functions, their applications, Simple hash functions, its requirements and security, Hash functions based on Cipher Block Chaining, Secure Hash Algorithm (SHA)	05	12

Reference Books:

1. Cryptography And Network Security, Principles And Practice Sixth Edition, William Stallings, Pearson
2. Information Security Principles and Practice By 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

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 key cryptography algorithms and their application in different context.
3. Compare public key cryptography with private key cryptography and Implement various asymmetric key cryptography algorithms.
4. Explore the concept of hashing and implement various hashing algorithms for message integrity.
5. Explore and use the techniques and standards of digital signature, key management and authentication.