GUJARAT TECHNOLOGICAL UNIVERSITY

B. E. SEMESTER: VI

Computer Engineering/Information Technology/Computer Science & Engineering

Subject Name: **Information Security**
Subject Code: **160702**

Teaching Scheme				Evaluation Scheme		
Theory	**Tutorial**	**Practical**	**Total**	**University Exam (Theory) (E)**	**Mid Sem Exam (Theory) (M)**	**Practical (I)**
4	0	2	6	70	30	50

Sr. No	Course Content	Total Hrs.
1.	**Conventional Encryption:** Conventional Encryption Model, Steganography, Classical Encryption Techniques	04
2.	**Conventional Encryption Techniques:** Simplified Des, Block Cipher Principles, Data Encryption Standards, Differential And Linear Cryptography Principles, Block Cipher Design Principles, Modes Of Operations, Algorithms Like Triple Des, International Data Encryption Algorithm, Blowfish, Rc5, Cast-128, Rc2, Characteristics Of Advanced Symmetrical Block Cipher, Issues Of Conventional Encryption Like Traffic Distribution, Random Number Generation, Key Distribution	14
3.	**Public Key Cryptography:**Principles Of Public-Key Cryptography, RSA Algorithm, Key Management, Elliptic Curve Cryptography, Diffie-Hellman Key Exchange	08
4.	**Number Theory:**Prime And Relative Prime Numbers, Modular Arithmetic, Euler's Theorem, Euclid's Algorithm, Discrete Logarithm Tics	04
5.	**Message Authentication And Hash Functions:**Authentication Requirement, Functions, Message Authentication Code, Hash Functions, Security Of Hash Functions And Macs, MD5 Message Digest Algorithm, Secure Hash Algorithm, Ripemd-160, Hmac	06
6.	**Introduction To E-Commerce:** Introduction To E-Commerce, Transactions On E-Commerce, Requirement Of Security On E-Commerce	04

7.	**Network Security:** Digital Signatures, Authentication Protocols, Digital Signature Standards, Application Authentication Techniques Like Kerberos, X.509 Directory Authentication Services, Active Directory Service Of Windows NT/Windows 2000	10
8.	**IP Security E-Mail Security:** IP Security Overview, Architecture, Authentication Header, Encapsulation Security Payload, Combining Security Association, Key Management, Pretty Good Privacy, S/Mime And Types	08
9.	**Web Security:** Web Security Requirement, SSL And Transport Layer Security, Secure Electronic Transactions, Firewall Design Principles, Trusted Systems	06

Text Book:

1. Cryptography And Network Principles And Practice Fourth Edition, William Stallings, Pearson

Reference Books:

1 Cryptography & Network Security, Forouzan, Mukhopadhyay, McGrawHill
2 Cryptography and Network Security (2nd Ed.), Atul Kahate, TMH
3 Information Systems Security, Godbole, Wiley-India
4 Information Security Principles and Practice, Deven Shah, Wiley-India