GUJARAT TECHNOLOGICAL UNIVERSITY

M.E Semester: 2

Computer Engineering

Subject Name Cryptography & Network Security

Sr.No	Course content
1.	Introduction: Threats, Vulnerabilities, Attacks, Integrity, Confidentiality, Anonymity, Authentication, Authorization, Non-repudiation, Data Security and Database Security
2.	Secret Key Cryptography: DES, Triple DES, AES, Key Distribution, Attacks
3.	Public Key Cryptography: RSA, ECC, Key Exchange, Attacks.
4.	Integrity, Authentication an Non-Repudiation: Hash Functions, Message Authentication Code, Digital Signature
5.	Public Key Infrastructure: Digital Certificates, Certification Authorities.
6.	Protocols: Basic Authentication Protocols, Attacks, Needham Schroeder Protocol, Kerberos, Network Security with IP Security, Web Security using SSL, E-cash and Secure Electronic Transaction
7.	System Security using Firewalls and VPNs
8.	Worms and Viruses
9.	Miscellaneous: Smart Cards and security, Zero knowledge protocols, Enterprise Application Security, Biometric Authentication, Database Access Control, Security and Privacy Issues in RFIDs

Reference Books:

1. Cryptography and Network Security by William Stallings
2. Security in Computing by Pfleeger and Pfleeger, 3rd Edition, PHI,
3. Computer Security: Art and Science by Bishop, Pearson Edition
4. Computer Security by Gollmall, Willey Publication
5. Network Security by Kaufman, Pearson Edition