GUJARAT TECHNOLOGICAL UNIVERSITY

M.E. Semester: II

M.E. Information Technology

Subject Name: **Advance Cryptography and Information Security**

Sr.No	Course content
1.	Cryptography and Data Security Information assurance issues -Threats to authentication, privacy and integrity, Generating MD5 hash collisions -Approaches to cryptography -Symmetric vs. asymmetric ciphers, Issues for secret key encryption, Public key fixes to secret key problems, Hashing and digital signatures, Generating and exchanging keys -Authentication via key ownership, Non-repudiation using digital signatures, Digital signatures in the real world, Key distribution and management, E-voting.
2.	Intrusion Detection Overview, Host based intrusion detection systems, Network based intrusion detection systems, IDS as part of the overall Security System, IDS Signatures and Analysis Schemes for Intrusion Detection Systems, Anomaly detection, Expert Systems, Tools for packet analysis and intrusion detection, Some intrusion detection tools(Snort,Windump,Ethereal etc.), Case Reports of various attack strategies, Implementation Issues ,Future directions.

Reference Books:

1. Intrusion Detection & Prevention by Carl Endorf, Eugene Schultz, Jim Mellander, Jack Kozio. Mcgraw Hill publication
2. Network Intrusion Detection (3Edition) by Stephen Northcutt and Judy Novak ISBN 0735712654
3. Snort 2.1 Intrusion Detection (Book with CD-ROM) by Jay Beale, Caswell syngress.
4. William Stallings; Cryptography and Network Security, Pearson publication, 4 edition, 2004
5. William Stallings; Network Secuirty Essentials, Pearson publication, 2005.
6. A. Menezes, P. van Oorschot, and S. Vanstone; Handbook of Applied Cryptography,
   CRC Press, 1996 -www.cacr.math.uwaterloo.ca/hac