GANDHINAGAR INSTITUTE OF TECHNOLOGY

Computer Engineering Department / Information Technology Department

CT1 Syllabus

Subject Name: Information and Network Security

Subject Code : 2170709

Unit	Topics
1	Symmetric Cipher Model, Cryptography, Cryptanalysis and Attacks; Substitution and Transposition techniques
2	Stream ciphers and block ciphers, Block Cipher structure, Data Encryption standard (DES) with example, strength of DES, Design principles of block cipher,
3	Multiple encryption and triple DES
4	Cryptographic Hash Functions, their applications, Simple hash functions, its requirements and security, Hash functions based on Cipher Block Chaining, Secure Hash Algorithm (SHA)
5	Message Authentication Codes, its requirements and security, MACs based on Hash Functions, Macs based on Block Ciphers