SARDAR VALLABHBHAI PATEL INSTITUTE OF TECHNOLOGY, VASAD

INFORMATION TECHNOLOGY DEPARTMENT

Syllabus for Mid semester examination

SUBJECT CODE:**2170709**

SUBJECT NAME: **Information And Network Security**

1. Symmetric Cipher Model , Cryptography, Cryptanalysis And Attacks, Substitution And Transposition Techniques
2. Stream Cipher 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 Function, Key Expansion , Example And Implementation.
3. Multiple Encryption And Triple DES , Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback Mode, Output Feedback Mode, Counter Mode
4. Public Key Cryptosystem With Applications, Requirements And Cryptanalysis, RSA Algorithm , Its Computational Aspects And Security, Diffie-Hellman Key Exchange Algorithm , Man-In-The-Middle Attack
5. Cryptographic Hash Functions, Their Applications, Simple Hash Function, Its Requirements And Security, Hash Functions Based On Cipher Block Chaining, Secure Hash Algorithm
6. Message Authentication Code, Its Requirements And Security, MAC Based On Hash Functions, MAC Based On Block Ciphers