

## Coding and Information Theory

Code: EC 703

**Credit: 4**

### Module 1. Introduction:

Coding for reliable digital transmission and storage, Types of codes, Types of errors encountered, Error Control Strategies.

### Module 2. Linear block codes:

Definition, Syndrome and Error detection, Minimum distance, Error detecting and Error-correcting capabilities, Standard Array and Syndrome decoding, Probability of an undetected error for linear codes over BSC, Hamming code.

### Module 3. Cyclic codes:

Description, Generator & parity-check matrices of cyclic codes, Encoding of cyclic codes, Syndrome computation and error detection, Decoding, Cyclic Hamming Codes, Shortened cyclic codes.

### Module 4. BCH codes:

Description, Decoding BCH codes, Implementation of error correction, Non binary BCH codes and Reed-Solomon codes, Weight distribution and Error detection of Binary BCH codes.

### Module 5. Convolution codes:

Encoding, Structural properties, Distance properties, Maximum likelihood decoding of convolution codes, Viterbi algorithm, Performance bound for convolution codes, Application of Viterbi decoding.

### Module 6. Information Theory

Basic Definition, Information & Entropy, Shannon's Channel Capacity Theorem, Source encoding, Channel capacity of a discrete memoryless channel, Channel capacity of a continuous channel.

### Module 7. Cryptography & Cryptosystems

Encryption & decryption, Public & private key cryptography, DES algorithm, RSA algorithm, Diffie-Hellman key exchange, Introduction of quantum cryptography, Applications of cryptography in network security.