http://highered.mheducation.com/sites/0072967757/student\_view0/chapter29/index.html

http://highered.mheducation.com/sites/0072967757/student\_view0/chapter30/multiple\_choice\_quiz.html

**SYMMETRIC KEY ENCRYPTION**

Same key is used for both encryption and decryption. Limitations are

Requirement of large number of unique keys. For example for n users the number of keys required is n(n-1)/2.

Distribution of keys among the users in a secured manner is difficult.

**Monoalphabetic Substitution --**

the relationship between a character in the plaintext and a character in the ciphertext is always one-to-one

**Polyalphabetic Substitution --**

The relationship between a character in the plaintext and a character in the ciphertext is always one-to-many.

**Transpositional Cipher --**

The characters are arranged in two-dimensional matrix and columns are interchanged according to a key is shown in the middle portion of the diagram

**Block Ciphers --**

The mapping should be one-to-one.

**Public key Cryptography**

The sender uses the public key of the receiver for encryption and the receiver uses his private key for decryption