Cryptography -> Encryption-> symmetric &Asymmetric ->Algorithms

**Stream Cipher** is generalization of one-time Pad and is initialized with short key. XOR is used to encrypt and decrypt. Advantages- speed and low error progation. Disadvantages are low diffusion and susceptibility and insertion/modification

**Block cipher** encryption advantages are high diffusion and immunity to tampering. Disadvantages are slowness and error propagation

**Substitution cipher** means every character of plain text is replaced by another character in the cipher text. **Caesar cipher is substitution cipher**

**Transposition** cipher means order of the characters is rearranged but doesn’t change the actual characters. Number key is used in the table to change the location.

**Symmetric Encryption**- It is called as “Secret key or private key encryption. One key is shared between sender and receiver to encrypt and decrypt the message. Sender encrypts the message with private key and receiver decrypts the message with the same private key. Faster, but sharing key is an important to avoid attack. It uses substitution and transposition. **Vulnerable to frequency analysis attack**

Data encryption standard(DES) is a popular symmetric encryption. IBM first created LUCIFIER and then it became DES. It uses 64-bit block cipher and 56 bit key. It uses 16 rounds. It provides confusion and diffusion. It converts into 48 bits during the rounds and then it again converts into 32 bit in S BOX. S box does real confusion(mixing). DES uses 8 s boxes with each 6 bit input and a 4 bit output. Other **symmetric algorithms are DES, AES,3DES, RC4, QUAD ,Blowfish &Skipjack.** AES uses 128 bit block cipher. Keys are 128/192/256 and rounds are 10/12/14 respectively. AES is non feistal structure whereas DES is feistal. ..

**Asymmetric Encryption** – Two keys used. Private key and public key. Also called as public key encryption. Sender encrypts the message with receiver public key and receiver decrypts the message with receiver’s private key. Slower but better than symmetric.

**Asymmetric algorithms are RSA, Differ-hellman, ECC,DSA and egamal.**

**Digital signature** uses hashing algorithm. It is used for non-repudiation. Sender encrypts the content with sender’s private key and receiver decrypts with sender’s public key. Once the content is encrypted. The sender can encrypt the Key with receiver’s public key and receiver will decrypt it with his private key first and then decrypt the content.

When trusted center(CA) in place. Sender encrypts with sender’s private key and trusted center will decrypt with sender’s public key and then trusted center will encrypt with trusted center’s private key and the final receiver will decrypt with trusted center’s public key.

**Digital certificate** contains public key of the owner and owner identity information and signed by CA’s private key. When sender sends the file, receiver checks the sender’s public key and decrypt using CA’s private key.

**Important note- data encrypted with public key can be decrypted only with the corresponding private key. Provides encryption operation. Data encrypted with private key can be decrypted only with the public key which provides non-repudiation/ integrity..**