# Encryption

Encryption is the process by which a readable or understandable message is converted to an unreadable form to prevent unauthorized parties from reading it. It is the process of encrypting plain text to cipher text. It is done at sender’s side. It helps in protecting consumer information, emails and other sensitive data from unauthorized access to it as well as secures communication networks.

# Decryption

Decryption is the reverse process of encryption. It is the process of converting encrypted message (cipher text) back to its original format. It is done at receiver side. The recipients must have the right decryption or decoding tools to access the original details. The only single algorithm is used for encryption-decryption with a pair of keys where each use for encryption and decryption.

# Data Encryption Standard

DES stands for data encryption standard. There are certain machines that can be used to crack the DES algorithm. The DES algorithm uses a key of 56 bit size. Using this key, the DES takes a block of 64 bit plain text as input and generates a block of 64-bit cipher text.

The DES process has several steps involved in it, where each step is called a round. Depending upon the size of the key being used, the number of rounds varies. For example, a 128-bit key requires 10 rounds, a 192-bit key requires 12 rounds and so on.

# Advanced Encryption Standard

The AES encryption algorithm (also known as Rijndael algorithm) is a symmetric block cipher algorithm with a block size of 128 bits. It converts these individual blocks using keys of 128, 192, and 256 bits. Once it encrypts these blocks, it joins them together to form the cipher text.

That mean, it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data.

# International Data Encryption algorithm

IDEA is a block cipher and it operates on 64 bit plain text and 128 bit key. IDEA is reversible like DES that is, the equivalent algorithm can be used for encryption and decryption. IDEA needs both diffusion and confusion for encryption.

The 64 bit plain text is divided into four portions of 16 bits plain text (p1 to p4 ). These are input to the first round. There are 8 such rounds. The key includes 128 bits. In each round, six sub-keys are produced from the original key, each of these sub-key includes 16 bits.