**CS6008 CRYPTOGRAPHY AND NETWORK SECURITY ASSIGNMENT – 5**

**EXTERNAL LEARNING MODULE 7 AND 8**

**BLOCK CIPHER**

**18.12.2021**

**Done by**

**SABHARI P**

**2018103582**

***1.Implement block ciphers using openssl in C/C++***

A block cipher is an encryption method that applies a deterministic algorithm along with a symmetric key to encrypt a block of text, rather than encrypting one bit at a time as in stream ciphers.

For example, a common block cipher, AES, encrypts 128 bit blocks with a key of predetermined length: 128, 192, or 256 bits. Block ciphers are pseudorandom permutation (PRP) families that operate on the fixed size block of bits. PRPs are functions that cannot be differentiated from completely random permutations and thus, are considered reliable, Block cipher modes of operation have been developed to eliminate the chance of encrypting identical blocks of text the same way, the ciphertext formed from the previous encrypted block is applied to the next block.

A block of bits called an initialization vector (IV) is also used by modes of operation to ensure ciphertexts remain distinct even when the same plaintext message is encrypted a number of times. Where an IV is crossed with the initial plaintext block and the encryption algorithm is completed with a given key and the ciphertext is then outputted. This resultant cipher text is then used in place of the IV in subsequent plaintext blocks.

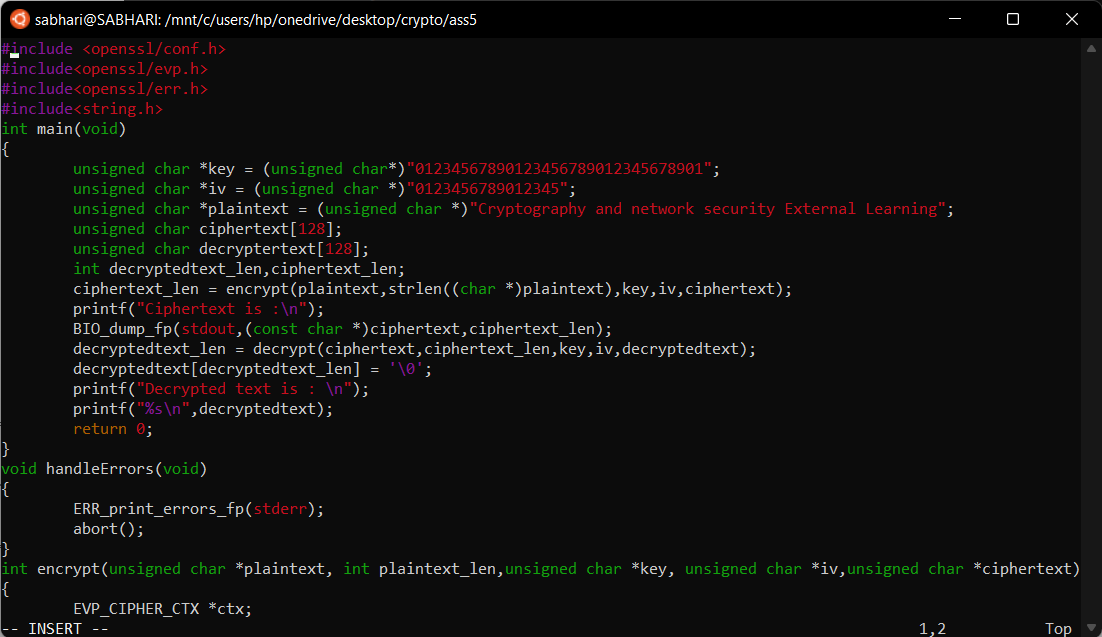
A block cipher takes in a block of plain text as input and produces a block of cipher text which is the same size as that of the plain text. The size of the input or cipher block can decided by the specific algorithm.

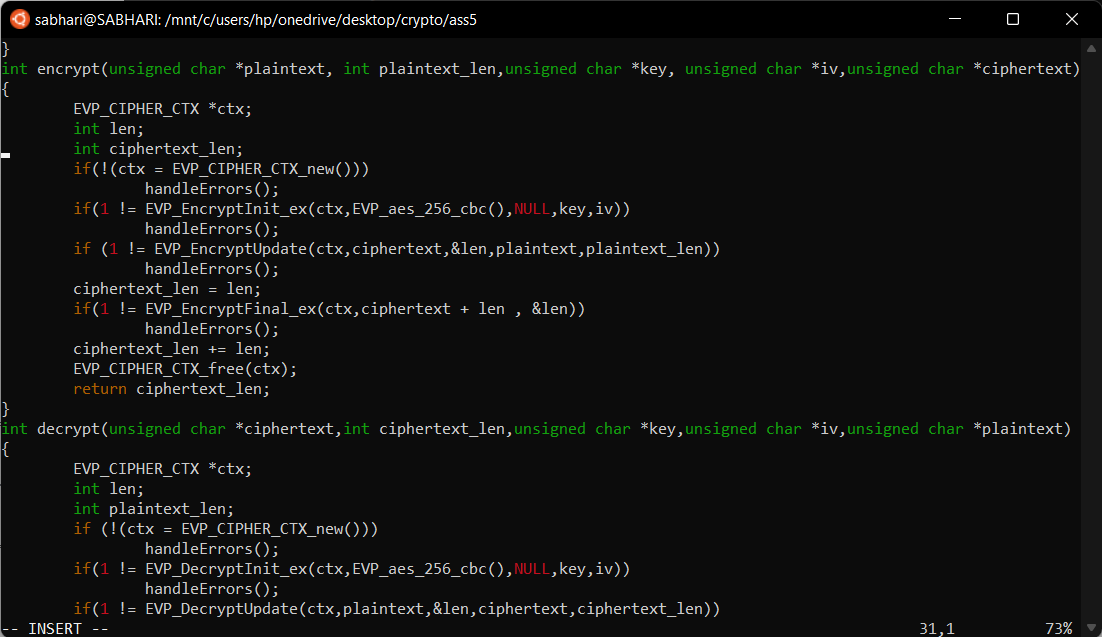
An encryption key is generally used to generate the cipher text. The size of the encryption key usually determines the strength of encryption. Although a block of any size is acceptable, multiples of eight are preferred. This is because a computer system usually addresses eight bits collectively as a unit(byte).

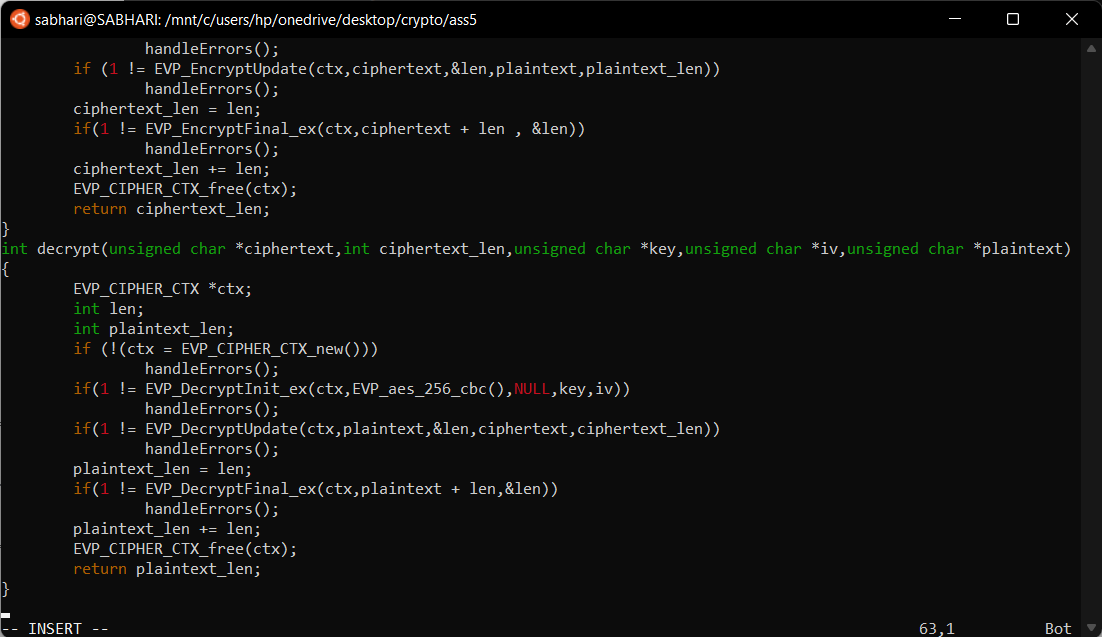
Input sizes aren’t exactly divisible by the predefined block size. Hence we pad the input until it occupies a block.

Very large block sizes aren’t usually preferred since we have to pad the input text before encryption. Some examples of block ciphers are Digital Encryption Standard(DES), Triple DES and Advanced Encryption Standard(AES).

***Code :***

******





In the above example we are demonstrating a classical example of block ciphers popularly known as 256 bit Advanced Encryption Standard (AES). Here the key must be known to the receiver to decrypt the message. In a 256 bit AES algorithm, the key’s length should be 256 bits.

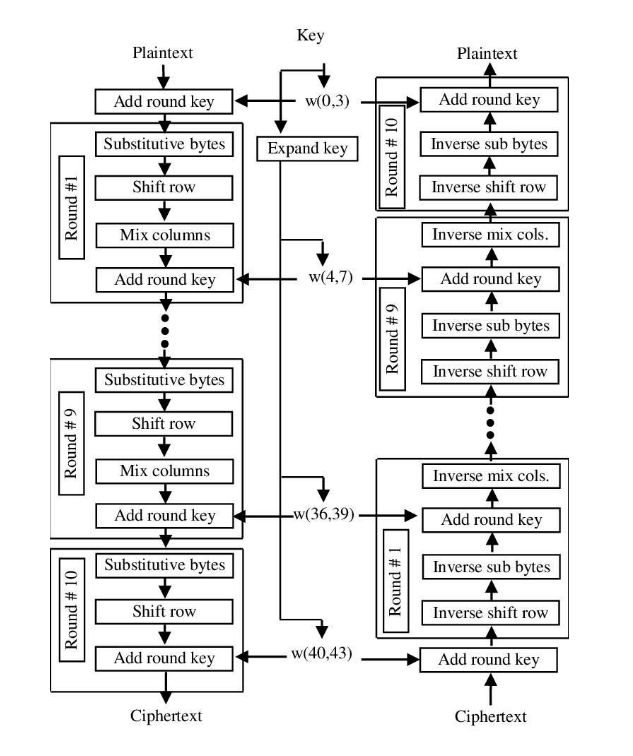
Initially a secret key is chosen. The secret key must be known both to the sender and receiver. In block ciphers, encryption is carried out as an iterative process. Each module requires encrypted text from the previous block or module as input. Hence for the first module a randomly chosen initialisation vector is given as input. Encryption and decryption are carried out with the help of openssl libraries.

***The plain text is :"Cryptography and network security External Learning"***

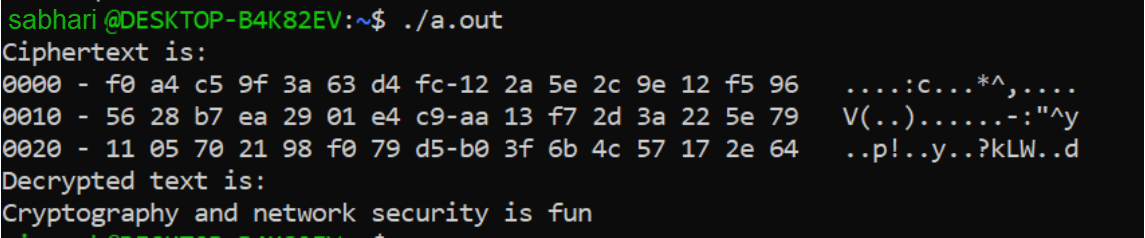
***The key is : "01234567890123456789012345678901"***

***The IV is : "0123456789012345"***

The block diagram for AES256 bit encryption is shown below. Encryption is carried out as a series of ten rounds. The key is expanded and each round uses four subkeys. The left hand part of the diagram encrypts plaintext while the right hand part decrypts ciphertext.



***Output:***

******

***The code is submitted for reference.***