AES

We have chosen to carry out this coding project on c#.

1. Introduction on AES

AES, which stands for Advanced Encryption Standard, is a widely used symmetric encryption algorithm designed to secure sensitive information. It is a symmetric key algorithm, meaning that the same key is used for both encryption and decryption. AES was established as a standard by the U.S. National Institute of Standards and Technology (NIST) in 2001, replacing the older Data Encryption Standard (DES).

Here are key features and aspects of AES:

- **Key Lengths:**

AES supports key lengths of 128, 192, and 256 bits. The key length directly influences the strength of the encryption. For our code, we have of chosen a key of 128 bits.

- **Block Cipher:**

AES operates as a block cipher, meaning it processes data in fixed-size blocks. For AES, each block is 128 bits.

- **Rounds:**

The number of rounds (iterations) for the encryption process depends on the key length: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

- **Substitution-Permutation Network:**

AES employs a substitution-permutation network (SPN) structure. It consists of a series of substitution, permutation, and mixing operations that provide a high level of security.

- **Key Expansion:**

AES uses a key expansion algorithm to generate a set of round keys from the original secret key. These round keys are used in each round of the encryption process.

- **Confidentiality and Integrity:**

AES is primarily designed for confidentiality (encryption) but can be combined with other algorithms to provide data integrity and authentication.

- **Cryptographic Strength:**

AES has withstood extensive analysis and cryptanalysis, and it is considered highly secure when used with a properly chosen key. Its strength lies in the complexity of its operations and the large key space.

- **Versatility:**

AES is versatile and widely adopted, used in various applications such as securing communications over the internet, encrypting files and data at rest, and ensuring the confidentiality of sensitive information.

- **Standardization:**

AES was chosen through an open competition, inviting submissions from cryptographers worldwide. Rijndael, the algorithm that became AES, was selected for its security, efficiency, and suitability for different applications.

In summary, AES is a robust and efficient encryption algorithm that forms the backbone of secure communication and data protection in numerous systems and applications. Its widespread adoption and standardized nature contribute to its trustworthiness in the field of cryptography.

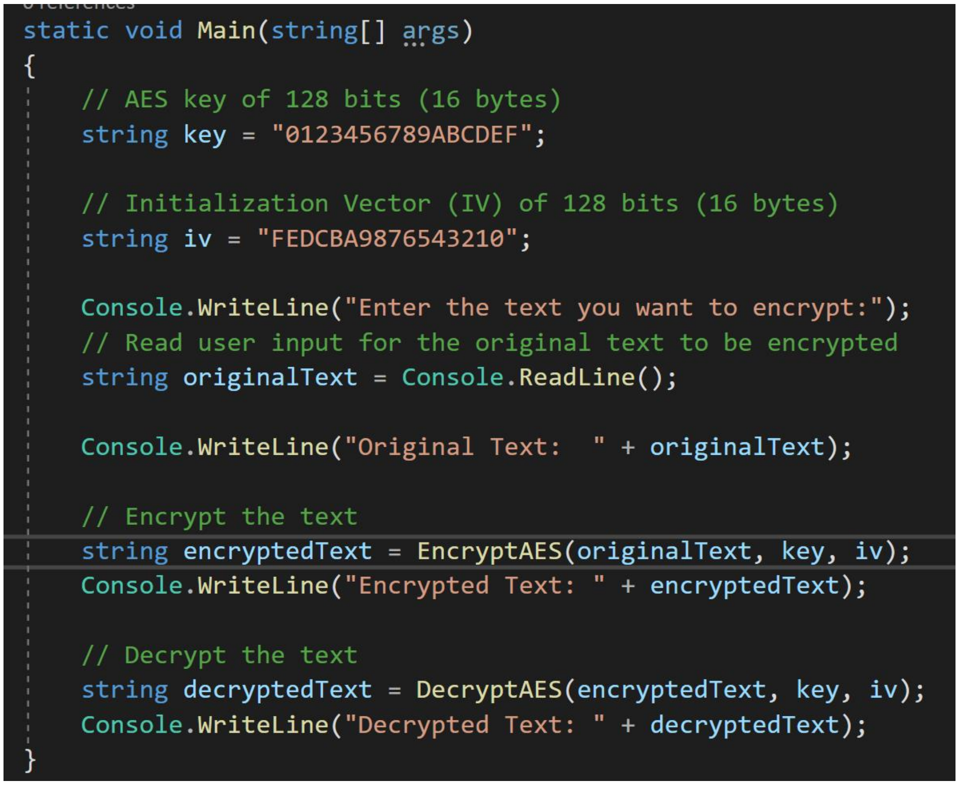
2. Main Method Overview:

The Main method is the entry point of the program.

An AES key (key) and an Initialization Vector (iv) are initialized for encryption and decryption.

The interface prompts the user to enter text for encryption.

It displays the original text, encrypted text, and decrypted text.



```
0 references
static void Main(string[] args)
{
    // AES key of 128 bits (16 bytes)
    string key = "0123456789ABCDEF";

    // Initialization Vector (IV) of 128 bits (16 bytes)
    string iv = "FEDCBA9876543210";

    Console.WriteLine("Enter the text you want to encrypt:");
    // Read user input for the original text to be encrypted
    string originalText = Console.ReadLine();

    Console.WriteLine("Original Text:  " + originalText);

    // Encrypt the text
    string encryptedText = EncryptAES(originalText, key, iv);
    Console.WriteLine("Encrypted Text: " + encryptedText);

    // Decrypt the text
    string decryptedText = DecryptAES(encryptedText, key, iv);
    Console.WriteLine("Decrypted Text: " + decryptedText);
}
```

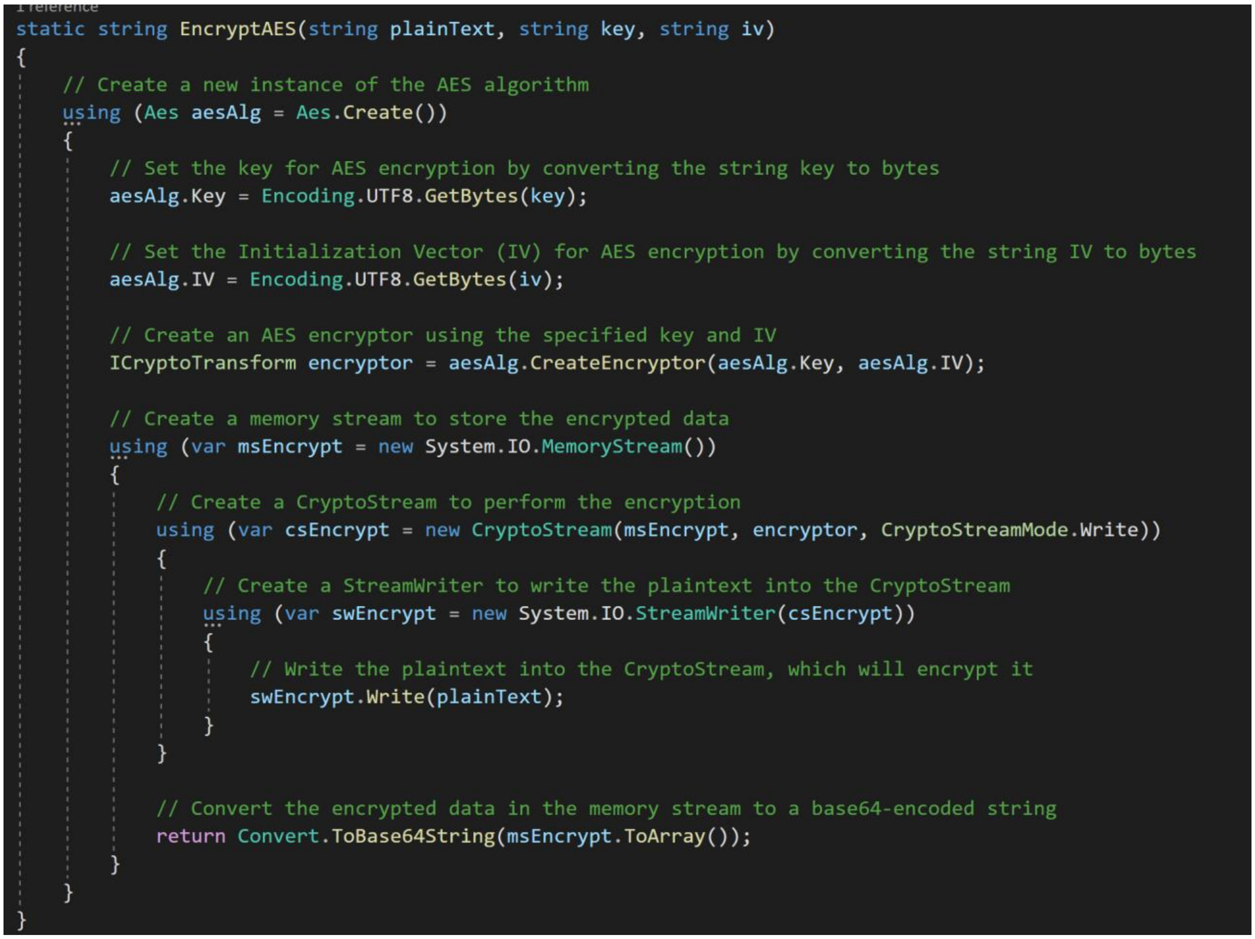
After, there are two functions : one for encrypting and the other one for decrypting.

3. EncryptAES Method Overview:

This method takes plaintext, an AES key, and an Initialization Vector (IV) as parameters.

It creates a new instance of the AES algorithm, sets the key and IV for AES encryption and creates an encryptor using the key and IV.

Then , it uses a memory stream to store the encrypted data, utilizes a CryptoStream to perform the encryption and converts the encrypted data to a base64-encoded string and returns it.



```
1 reference
static string EncryptAES(string plainText, string key, string iv)
{
    // Create a new instance of the AES algorithm
    using (Aes aesAlg = Aes.Create())
    {
        // Set the key for AES encryption by converting the string key to bytes
        aesAlg.Key = Encoding.UTF8.GetBytes(key);

        // Set the Initialization Vector (IV) for AES encryption by converting the string IV to bytes
        aesAlg.IV = Encoding.UTF8.GetBytes(iv);

        // Create an AES encryptor using the specified key and IV
        ICryptoTransform encryptor = aesAlg.CreateEncryptor(aesAlg.Key, aesAlg.IV);

        // Create a memory stream to store the encrypted data
        using (var msEncrypt = new System.IO.MemoryStream())
        {
            // Create a CryptoStream to perform the encryption
            using (var csEncrypt = new CryptoStream(msEncrypt, encryptor, CryptoStreamMode.Write))
            {
                // Create a StreamWriter to write the plaintext into the CryptoStream
                using (var swEncrypt = new System.IO.StreamWriter(csEncrypt))
                {
                    // Write the plaintext into the CryptoStream, which will encrypt it
                    swEncrypt.Write(plainText);
                }
            }

            // Convert the encrypted data in the memory stream to a base64-encoded string
            return Convert.ToBase64String(msEncrypt.ToArray());
        }
    }
}
```

4. DecryptAES Method Overview:

This method takes ciphertext, an AES key, and an Initialization Vector (IV) as parameters.

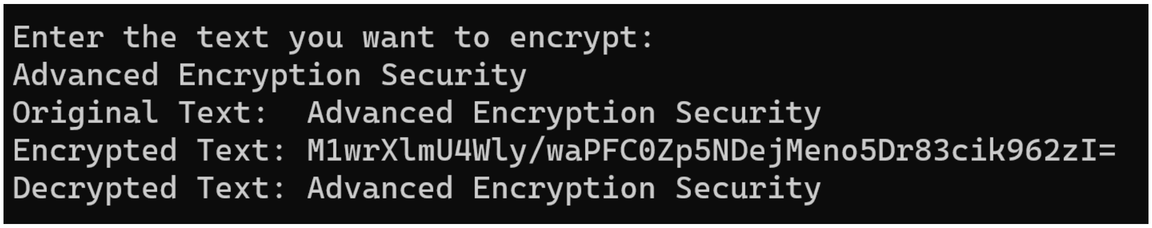
It Creates a new instance of the AES algorithm, sets the key and IV for AES decryption and creates a decryptor using the key and IV.

Moreover, it uses a memory stream to store the decrypted data, initializing it with the base64-decoded ciphertext and utilizes a CryptoStream to perform the decryption.

Finally , a StreamReader is used to read the decrypted data and the algorithm returns it as a string.

5. User Interface

First, users are prompted to enter the text they wish to be encrypted using the AES method. Then, once encrypted, the word is displayed to the user. Finally, the encrypted word is decrypted and displayed on the console.



```
Enter the text you want to encrypt:
Advanced Encryption Security
Original Text:  Advanced Encryption Security
Encrypted Text: M1wrXlmU4Wly/waPFC0Zp5NDejMeno5Dr83cik962zI=
Decrypted Text: Advanced Encryption Security
```