



Assignment Answer

CSE436, Computer and Networks Security

Name: **Omar Hazem Mohamed**

ID: **16p6073**

Assignment No: (III)

Date: 27 / 06 / 2020

GENERAL NOTES

FUNCTIONS USED FOR AES ENCRYPTION Process	WHAT IT DOES	FUNCTIONS USED FOR AES DECRYPTION Process	WHAT IT DOES
<code>Enc_Byts(current_Stat);</code>	Substitute bytes :- uses an S-box to perform a byte-by-byte substitution of the block for encryption	<code>key_rou_add(current_Stat, alg_K[MY_i]);</code>	AddRoundKey: a simple bitwise XOR of the current block with a portion of the expanded key
<code>rows_sh_encryption(current_Stat);</code>	Shift Rows : permutation process for encryption	<code>decryption_mixing_col(current_Stat);</code>	Mixing columns : Substitution process done for decryption
<code>Encryption_mixing_col(current_Stat);</code>	Mixing columns : Substitution process done for encryption	<code>rows_sh_decryption(current_Stat);</code>	Shift Rows: permutation process for decryption
<code>key_rou_add(current_Stat, alg_K[MY_i]);</code>	AddRoundKey: a simple bitwise XOR of the current block with a portion of the expanded key	<code>Dec_Byts(current_Stat);</code>	Substitute bytes :- uses an S-box to perform a byte-by-byte substitution of the block for decryption

Screenshots

I used the example from the documentation file for encryption and decryption screenshots

```
C:\Users\Omar Hazem\source\repos\ConsoleApplication4\Debug\ConsoleApplication4.exe

-----Algorithm Started-----

Insert :
*for decryption : 0
*for encryption : 1
1

-----
please insert encryption key (with size of 32)
0123456789ABCDEF0123456789ABCDEF

-----
Insert your plaintext (with size of 32)
0123456789ABCDEF0123456789ABCDEF

-----
Encrypted successfully
A1EE5608B33AF05470858608D1DE080F

-----algorithm ended-----
```

```
9600] ConsoleApplication4.exe - Lifecycle Events - Thread: [20164] Main Thread

C:\Users\Omar Hazem\source\repos\ConsoleApplication4\Debug\ConsoleApplication4.exe

-----algorithm ended-----

Insert :
*for decryption : 0
*for encryption : 1
0

-----
Insert decryption key (with size of 32)
0123456789ABCDEF0123456789ABCDEF

-----
Insert your ciphertext (with size of 32)
A1EE5608B33AF05470858608D1DE080F

-----
Decrypted successfully
0123456789ABCDEF0123456789ABCDEF

-----algorithm ended-----
```