Assignment Answer

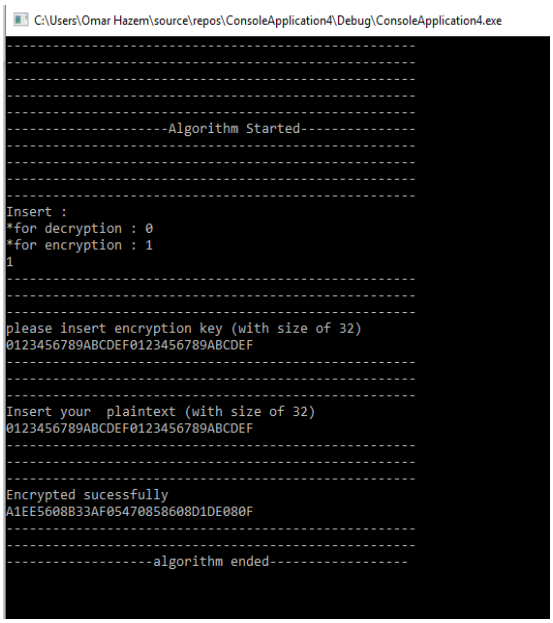
CSE436, Computer and Networks Security

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
Enc_Byts(curren_Stat);	Substitute bytes :- uses an S-box to perform a byte-by-byte substitution of the block for encryption	key_rou_add(curren_Stat, alg_K[MY_i]);	AddRoundKey: a simple bitwise XOR of the current block with a portion of the expanded key
rows_sh_enccryption(curren_Stat);	Shift Rows : permutation process for encryption	decyption_mixing_col(curren_Stat);	Mixing columns : Substitution process done for decryption
Encyption_mixing_col(curren_Stat);	Mixing columns : Substitution process done for encryption	rows_sh_decryption(curren_Stat);	Shift Rows: permutation process for decryption
key_rou_add(curren_Stat, alg_K[MY_i]);	AddRoundKey: a simple bitwise XOR of the current block with a portion of the expanded key	Dec_Byts(curren_Stat);	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