****

**Assignment Answer**

**CSE432, Computer Security**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name: | Mai suody abd elghany | ID: | 1601501 |  |

Assignment No: ( AES )

Date: 3 / 2 /2021

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

I was programming this algorithm using python 3.9.1, the algorithm is Advanced Encryption Standard (AES)

Let’s start discussing function this algorithm:

All incoming function don’t return but using in the inverse, shift rows an dinverse them, add rounds, mixing columns and inverse them, and take the text and make them n matrix, and take matrix to binary.

subBytes(sub)

inverseSubBytes(sub)

shiftRows(sub)

inverseShiftRows(sub)

add\_round\_key(sub, key)

mixingOneColumn(sin)

mixingColumns(sub)

inverseMixingColumns(sub)

bytesToMatrix(text)

matrixToBytes(matrix)

xor(a, b)

class AES(object):

have function and return values

\_\_init\_\_(self, master\_key)

\_expand\_key(self, master\_key)

encrypt\_block(self, plaintext)

function takes the plaintext and convert it

decrypt\_block(self, ciphertext)

function takes the ciphertext and convert it

snpshots of output

