Assignment Answer

CSE432, Computer Security

Name: Mai suody abd elghany ID: 1601501

Assignment No: (DES)

Date: 3 / 2 /2021

I was programming this algorithm using python 3.9.1, the algorithm is Data Encryption Standard (DES).

Let's start discussing function this algorithm:

```
#give size of binary and return the value as a string
binaryAsString(val, bitsize)

#give size of hexa and return binary number
hexaToBinary(hexa_D, numOfBits)

"""
using Substitute box to Substitute byte
then, usnig SplitToN function to sublist the array that have 6 bits
to get the row with the first and last bit and columns is the 2,3,4,5th bits
"""
substitute(data)

#start Permutation using the given table
permutation(giv_Bloc, giv_table)
```

Apply xor and return the resulting list

```
xor(A, B)


#start shifting a list of the given value
moveList(g_, d_, num)


#generate the key
generation(key)

#take the list and split it into sublists
SplitToN(sub, size)

"""
In this function starting using all of the previous function
"""
DES(key, hexStr):
```

The file name is DES.py

The out put:

```
Enter Key in 16 hexa: 0000000000000000
Enter Plaintext in 16 hexa: FFFFFFFFFFFFFFFF
Enter number of runs: 1
355550B2150E2451
```

```
Enter 16 hex digit Key: 0000000000000000
Enter 16 hex digit Plaintext: FFFFFFFFFFFFFFFF
Enter number of runs: 2
FFFFFFFFFFFFFFFF
```