**DEPARTMENT OF INFORMATION TECHNOLOGY**

**COURSE CODE: DJ19ITL501 DATE: 5/11/22**

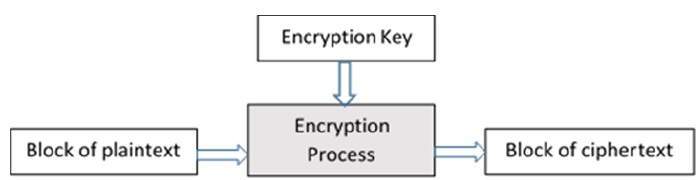
**COURSE NAME: Cryptography and Network Security Lab Class: A3**

**LAB EXPERIMENT NO. 4**

**AIM:** Design Analysis of Modern Block Ciphers (use crypt APIs)

**DESCRIPTION OF EXPERIMENT:**

A block cipher takes a block of plaintext bits and generates a block of ciphertext bits, generally of same size. The size of block is fixed in the given scheme. The choice of block size does not directly affect to the strength of encryption scheme. The strength of cipher depends up on the key length.



**Analysis:**

1. Use crypt API to encrypt/decrypt a plaintext block using AES, DES
2. Avalanche Effect: Change in Plaintext
3. Avalanche Effect: Change in key

**TECHNOLOGY STACK** : Python

**DESIGN AND IMPLEMENTATION CODE:**

**Aes:**

from Crypto.Cipher import AES

def encrypt(message,key):

    obj = AES.new(key, AES.MODE\_CBC, 'This is an IV456')

    #message = "The answer is no"

    ciphertext = obj.encrypt(message)

    print(ciphertext)

    return ciphertext

def decrypt(ciphertext,key):

    obj2 = AES.new(key, AES.MODE\_CBC, 'This is an IV456')

    pt=obj2.decrypt(ciphertext)

    print(pt)

    return pt

**des:**

from Crypto.Cipher import DES

def encrypt(message,key):

    obj = DES.new(key, DES.MODE\_OFB,'ThiIV456')

    #message = "The answer is no"

    ciphertext = obj.encrypt(message)

    print(ciphertext)

    return ciphertext

def decrypt(ciphertext,key):

    obj2 = DES.new(key, DES.MODE\_OFB,'ThiIV456')

    pt=obj2.decrypt(ciphertext)

    print(pt)

    return pt

**3-des:**

from Crypto.Cipher import DES3

def encrypt(message,key):

    obj = DES3.new(key, DES3.MODE\_OFB,'ThiIV456')

    #message = "The answer is no"

    ciphertext = obj.encrypt(message)

    print(ciphertext)

    return ciphertext

def decrypt(ciphertext,key):

    obj2 = DES3.new(key, DES3.MODE\_OFB,'ThiIV456')

    pt=obj2.decrypt(ciphertext)

    print(pt)

    return pt

**Avalanche Effect: Change in key**

import aes

import des

#avalanch key

keya='This is a key123'

bitchangedkey='This is a kfy123'

print("\n\navalanch in aes key changed from ",keya,"to ",bitchangedkey," : ")

message = "123456xxxxxxxxxx"

c1=aes.encrypt(message,keya)

c2=aes.encrypt(message,bitchangedkey)

keyd='key12345'

bitchangedkey='kfy12345'

print("\n\navalanch in des key changed from ",keyd,"to ",bitchangedkey," : ")

message = "123456xxxxxxxxxx"

c1=des.encrypt(message,keyd)

c2=des.encrypt(message,bitchangedkey)

**Avalanche Effect: Change in plaintext**

import aes

import des

#avalanch message

keya='This is a key123'

keyd='key12345'

message = "123456xxxxxxxxxx"

bitchangedmssg="223456xxxxxxxxxx"

print("\n\navalanch in aes message changed from ",message,"to ",bitchangedmssg," : ")

c1=aes.encrypt(message,keya)

c2=aes.encrypt(bitchangedmssg,keya)

message = "123456xxxxxxxxxx"

bitchangedmssg="223456xxxxxxxxxx"

print("\n\navalanch in des message changed from ",message,"to ",bitchangedmssg," : ")

c1=des.encrypt(message,keyd)

c2=des.encrypt(bitchangedmssg,keyd)

**Avalanche Effect: 3des**

import tdes

keya='This is a key123'

message = "123456xxxxxxxxxx"

bitchangedmssg="223456xxxxxxxxxx"

bitchangedkey='This is a kfy123'

print("\n\navalanch in 3-des message changed from ",message,"to ",bitchangedmssg," : ")

c1=tdes.encrypt(message,keya)

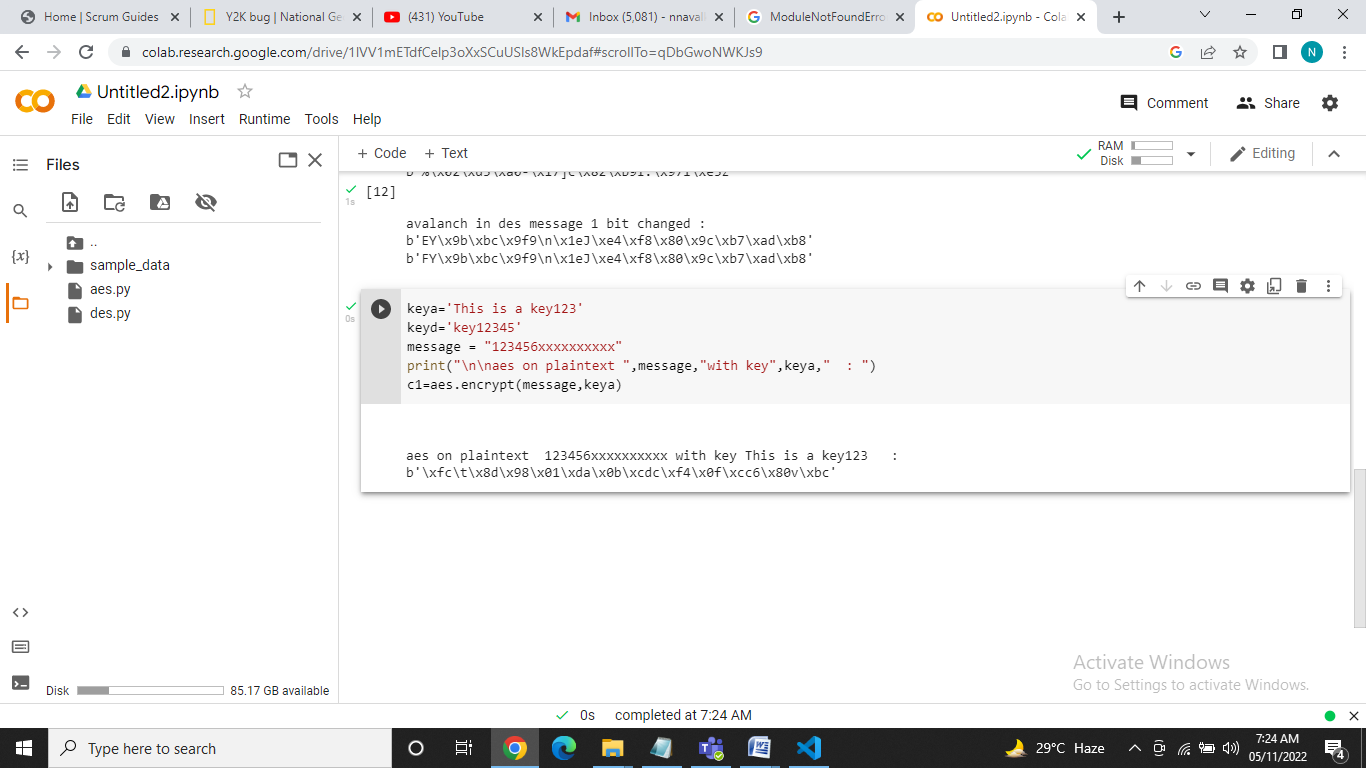
c2=tdes.encrypt(bitchangedmssg,keya)

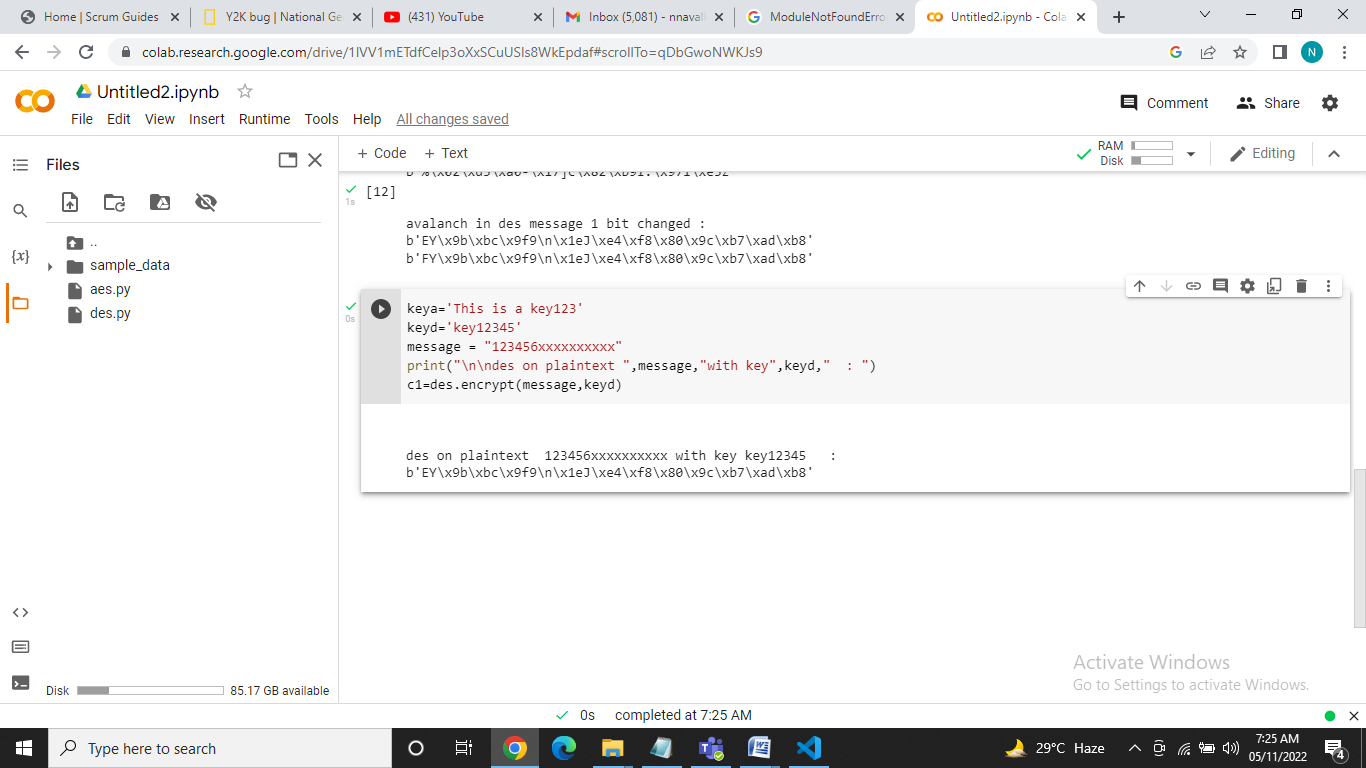
print("\n\navalanch in 3-des key changed from ",keya,"to ",bitchangedkey," : ")

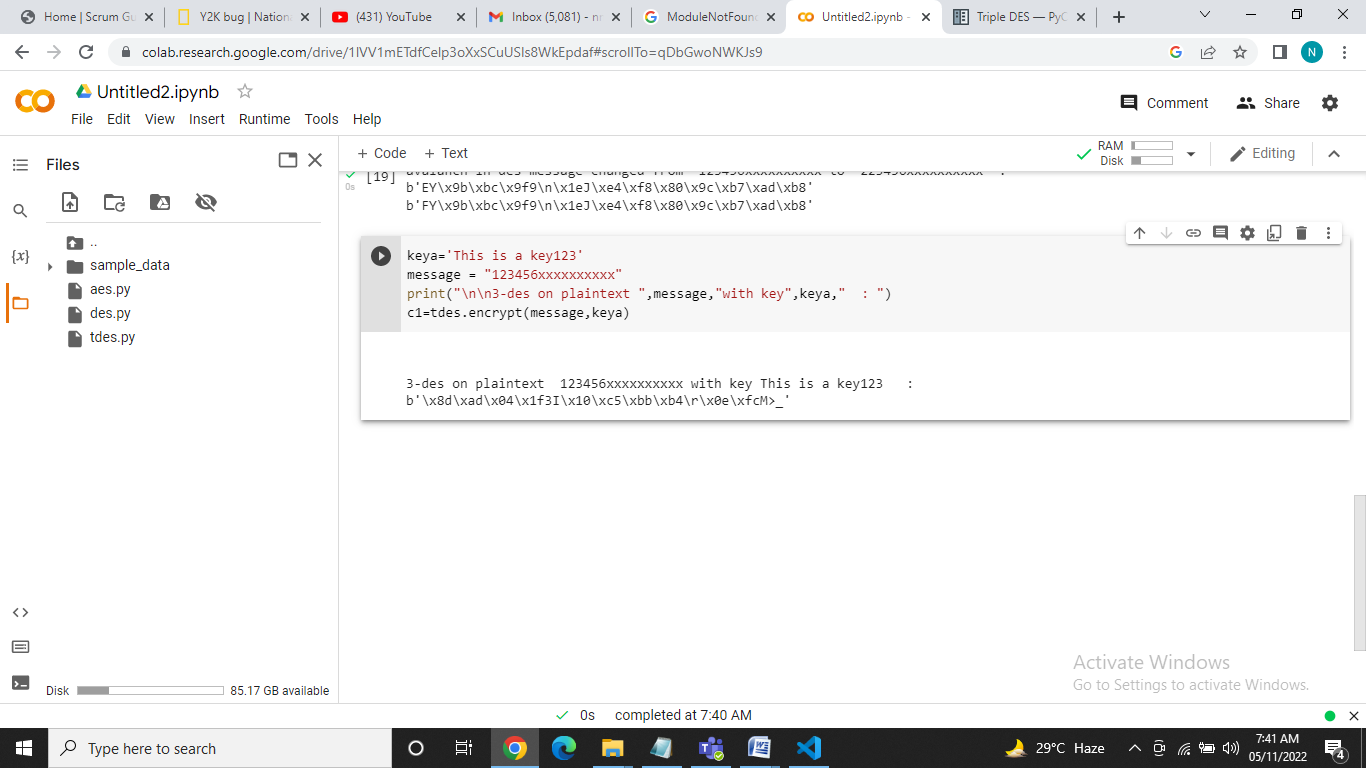
c1=tdes.encrypt(message,keya)

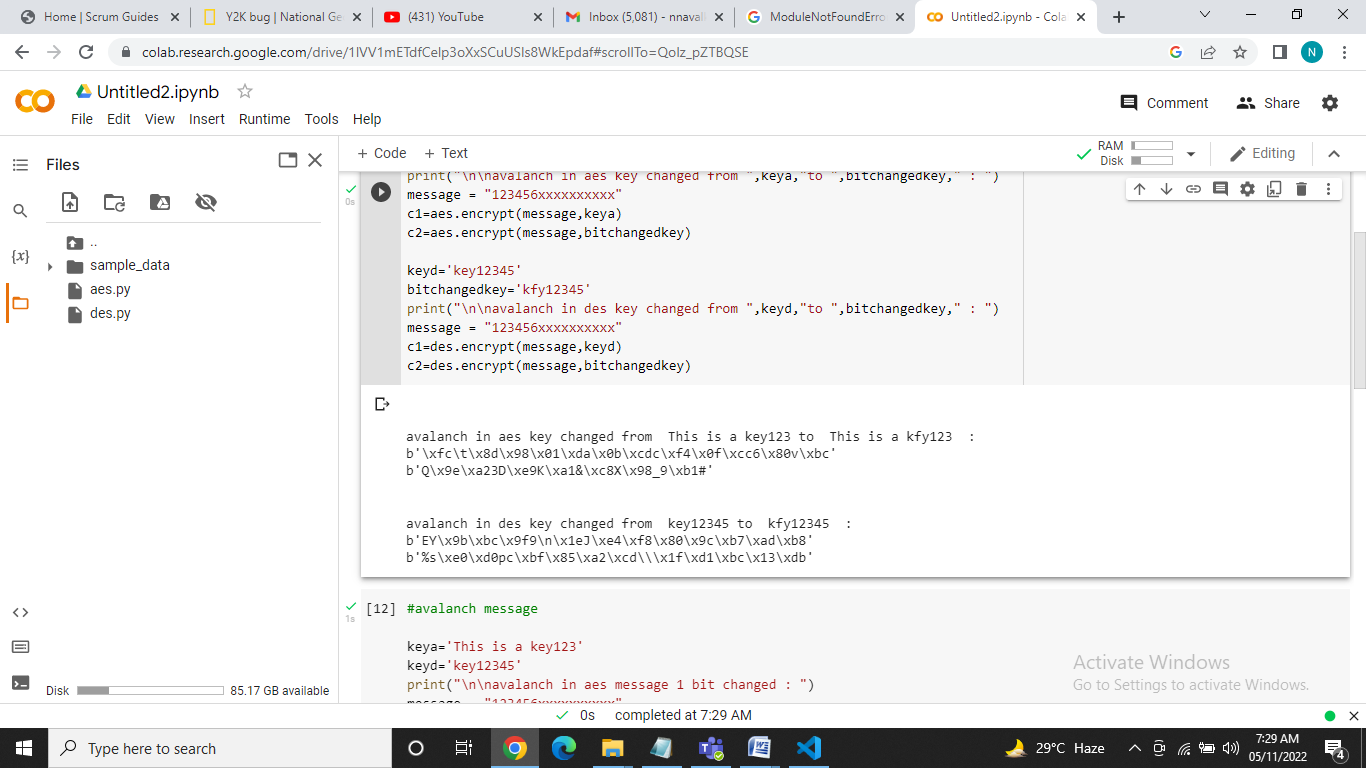
c2=tdes.encrypt(message,bitchangedkey)

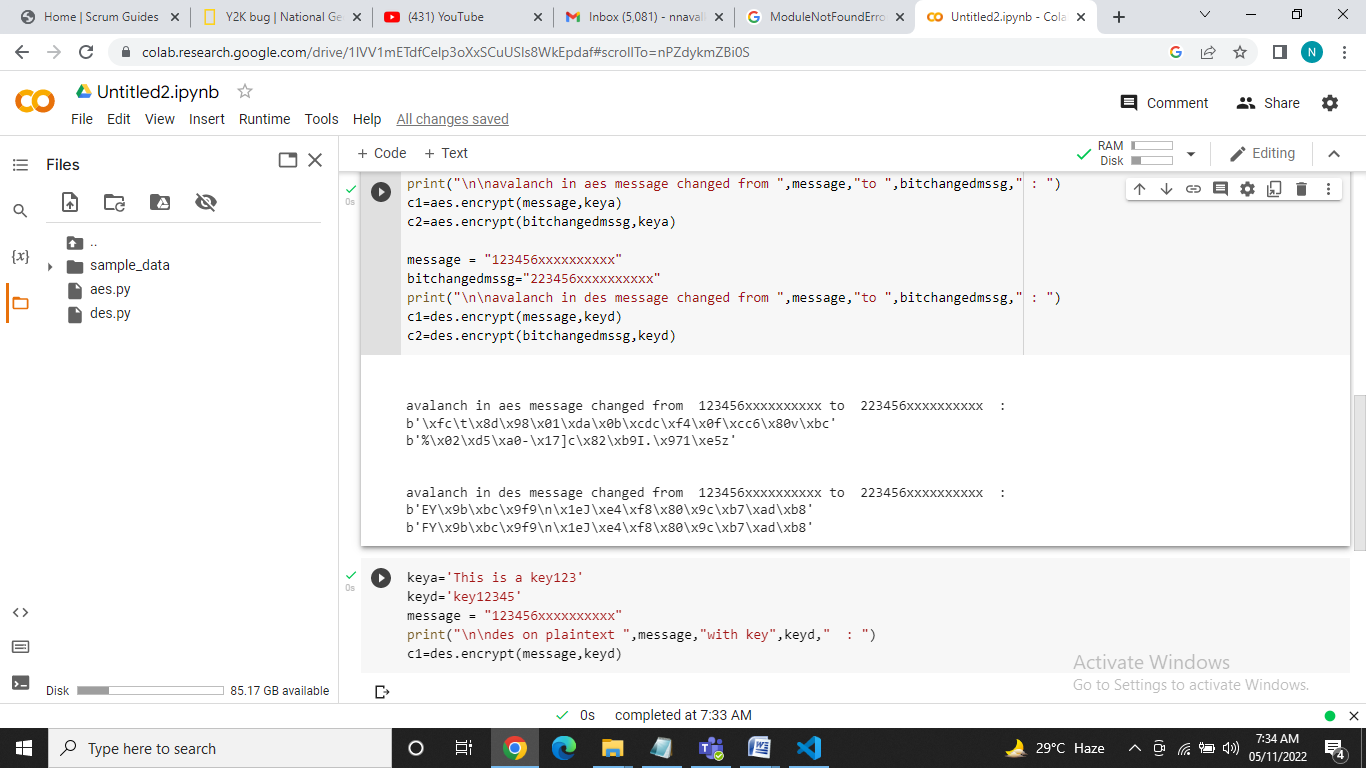
**OUTPUT:**

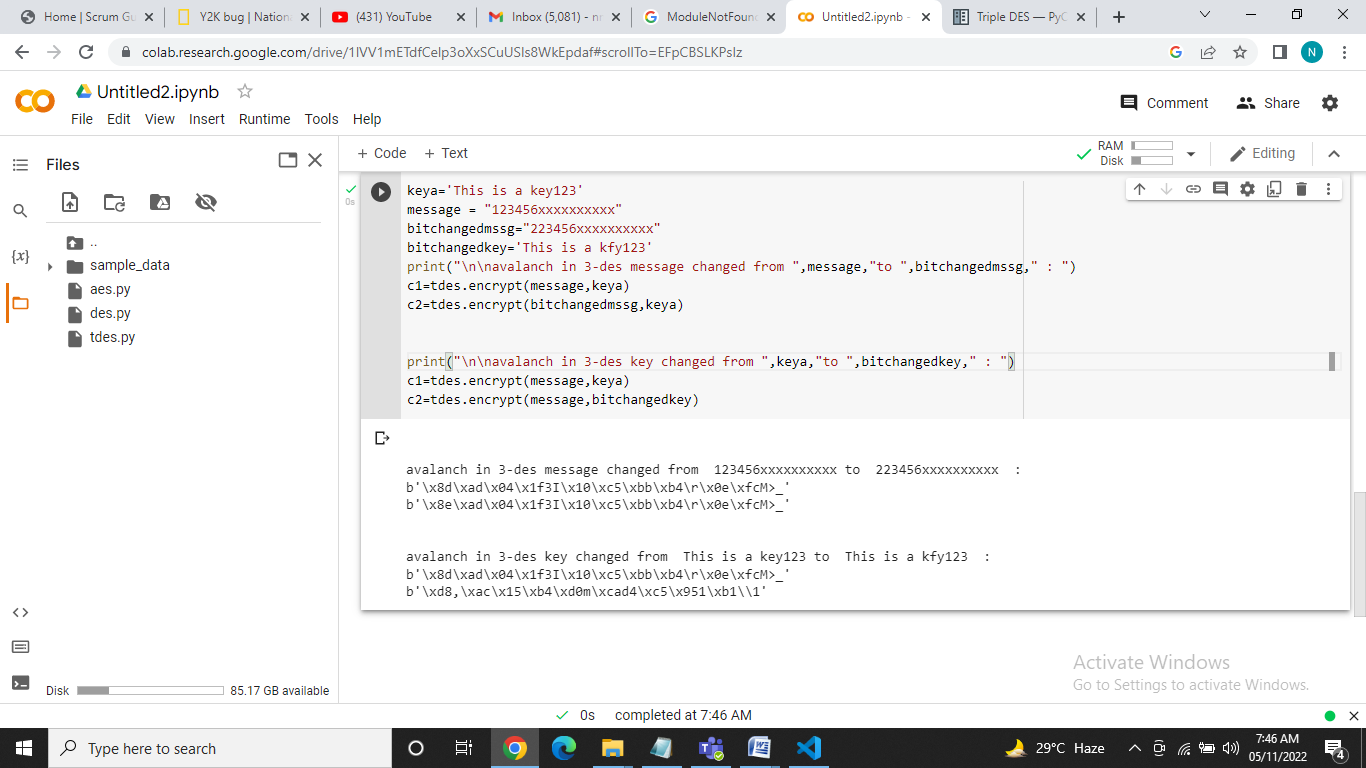
****

****

****

****

****

****

**OBSERVATIONS:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Avalanche effect (change in plaintext) | DES | Triple DES | AES-128 | AES-192 | AES-256 |
| key | key12345 | This is a key123 | This is a key123 | This is a key123 of aes2 | This is a key123 of aes2 1234567 |
| Original plaintext | 123456xxxxxxxxxx | | | | |
| ciphertext | 'EY\x9b\xbc\x9f9\n\x1eJ\xe4\xf8\x80\x9c\xb7\xad\xb8' | '\x8d\xad\x04\x1f3I\x10\xc5\xbb\xb4\r\x0e\xfcM>\_' | '\xfc\t\x8d\x98\x01\xda\x0b\xcdc\xf4\x0f\xcc6\x80v\xbc' | '\xcap\xa4\xd1\xe5\xa2\x93\x90\x9au\x8e\xf2\xf5\x0e\x08\xf8' | '\x15\xcfGT\xf5\x1f\xbd\xb90\xa4\x7f\x92Bt\x9f\x97' |
| Changed plaintext | 223456xxxxxxxxxx | | | | |
| New CT | 'FY\x9b\xbc\x9f9\n\x1eJ\xe4\xf8\x80\x9c\xb7\xad\xb8' | '\x8e\xad\x04\x1f3I\x10\xc5\xbb\xb4\r\x0e\xfcM>\_' | '%\x02\xd5\xa0-\x17]c\x82\xb9I.\x971\xe5z' | '\x12\x02\x052q\xeb>\n\xe4Aw\xf24\xc7\xc4\xb7' | '\xab\x01!\xf1\xda\xecJ\n\xedk\xe3\xed\xadV\xe5p' |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Avalanche effect (change in key) | DES | Triple DES | AES-128 | AES-192 | AES-256 |
| key | key12345 | This is a key123 | This is a key123 | This is a key123 of aes2 | This is a key123 of aes2 1234567 |
| Original plaintext | 123456xxxxxxxxxx | | | | |
| ciphertext | 'EY\x9b\xbc\x9f9\n\x1eJ\xe4\xf8\x80\x9c\xb7\xad\xb8' | '\x8d\xad\x04\x1f3I\x10\xc5\xbb\xb4\r\x0e\xfcM>\_' | '\xfc\t\x8d\x98\x01\xda\x0b\xcdc\xf4\x0f\xcc6\x80v\xbc' | '\xcap\xa4\xd1\xe5\xa2\x93\x90\x9au\x8e\xf2\xf5\x0e\x08\xf8' | '\x15\xcfGT\xf5\x1f\xbd\xb90\xa4\x7f\x92Bt\x9f\x97' |
| Changed key | kfy12345 | This is a kfy123 | This is a kfy123 | This is a kfy123 of aes2 | This is a kfy123 of aes2 1234567 |
| New CT | '%s\xe0\xd0pc\xbf\x85\xa2\xcd\\\x1f\xd1\xbc\x13\xdb' | '\xd8,\xac\x15\xb4\xd0m\xcad4\xc5\x951\xb1\\1' | 'Q\x9e\xa23D\xe9K\xa1&\xc8X\x98\_9\xb1#' | \x82\x9a=\xe6\xe3V\xb3\xb5\xb7!\xbb\xa8k\x1c\xfd\xa7' | '\x8a\xb0W\x00\x89F\xeb\xe0\xc2\xf6(\xeeH\xa5\xe3\xc1' |

**CONCLUSION:**

Thus it can observed thatAvalanche Effect with respect to change in message produces minimal change in cipher text for DES, 3DES but produces huge changes for AES

Avalanche Effect with respect to change in key produces noticeable change in cipher text for all block ciphers.

Therefore AES produces more Avalanche Effect because of having superior diffusion and confusion.

Thus, we have studied and implemented AES and DES, 3-DES block ciphers.