INFORMATION SECURITY

ASSIGNMENT 01

Submitted by: Minam Faisal & Momenah Saif
Roll number: 21i-1901, 21i-1909.
Date: 24th March,2024

Table of Contents

- **Introduction** 2
- **Calculating Avalanche Effect** 2
- **Calculating Avalanche Effect (altered bit)** 10
- **Discussing statistics** 18
- **Summary** 19
- **References** 20

Introduction

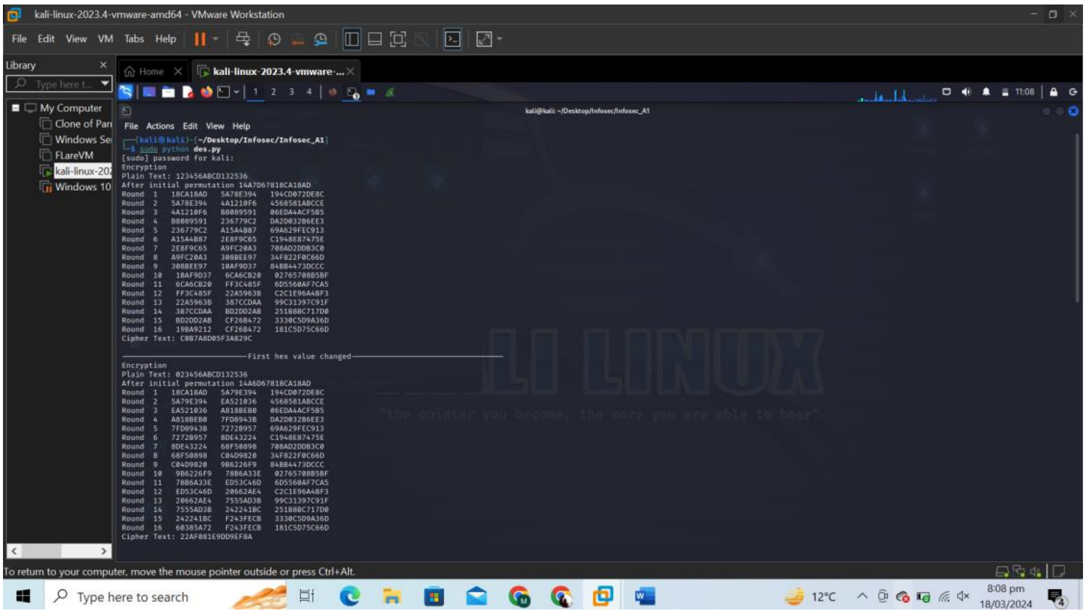
In this assignment, we explore the concept of the Avalanche Effect in various encryption algorithms, namely DES, 2-DES, 3-DES, AES-128, AES-192, and AES-256. The Avalanche Effect refers to the property of encryption algorithms where a small change in the input (plaintext) results in a significantly different output (ciphertext). We investigate the extent of this effect across different algorithms and analyze whether altering the position of a single bit affects the degree of avalanche. The assignment aims to provide insights into the cryptographic strength and behavior of these algorithms under different conditions.

For the code implementation, we used Python to develop scripts that simulate encryption operations and measure the avalanche effect.

Calculating Avalanche Effect

DES

In DES, there are total 16 rounds. Firstly, we do an encryption of a plaintext: "123456ABCD132536". Below screenshot shows after initial permuatation,16 rounds and final permutation our plaintext is converted to ciphertext: "C0B7A8D05F3A829C".

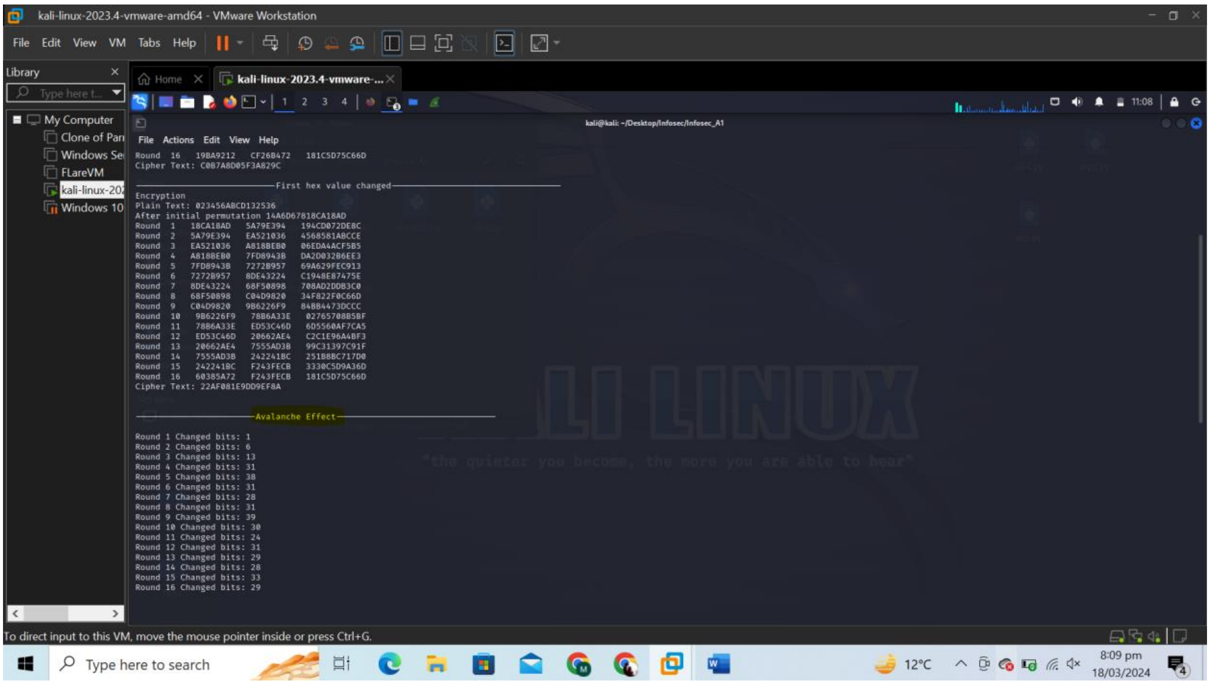


```
┌──(kali㉿kali)-[~/Desktop/Infosec/Infosec_A1]
└─$ sudo python des.py
[sudo] password for kali:
Encryption
Plain Text: 123456ABCD132536
After initial permutation 14A7D67818CA18AD
Round  1   18CA18AD   5A78E394   194CD072DE8C
Round  2   5A78E394   4A1210F6   4568581ABCCE
Round  3   4A1210F6   B8089591   06EDA4ACF5B5
Round  4   B8089591   236779C2   DA2D032B6EE3
Round  5   236779C2   A15A4B87   69A629FEC913
Round  6   A15A4B87   2E8F9C65   C1948E87475E
Round  7   2E8F9C65   A9FC20A3   708AD2DDB3C0
Round  8   A9FC20A3   308BEE97   34F822F0C66D
Round  9   308BEE97   10AF9D37   84BB4473DCCC
Round  10   10AF9D37   6CA6CB20   02765708B5BF
Round  11   6CA6CB20   FF3C485F   6D5560AF7CA5
Round  12   FF3C485F   22A5963B   C2C1E96A4BF3
Round  13   22A5963B   387CCDAA   99C31397C91F
Round  14   387CCDAA   BD2DD2AB   251B8BC717D0
Round  15   BD2DD2AB   CF26B472   3330C5D9A36D
Round  16   19BA9212   CF26B472   181C5D75C66D
Cipher Text: C0B7A8D05F3A829C

──────────────────────First hex value changed──────────────────────
Encryption
Plain Text: 023456ABCD132536
After initial permutation 14A6D67818CA18AD
Round  1   18CA18AD   5A79E394   194CD072DE8C
Round  2   5A79E394   EA521036   4568581ABCCE
Round  3   EA521036   A818BEB0   06EDA4ACF5B5
Round  4   A818BEB0   7FD8943B   DA2D032B6EE3
Round  5   7FD8943B   7272B957   69A629FEC913
Round  6   7272B957   8DE43224   C1948E87475E
Round  7   8DE43224   68F50898   708AD2DDB3C0
Round  8   68F50898   C04D9820   34F822F0C66D
Round  9   C04D9820   9B6226F9   84BB4473DCCC
Round  10   9B6226F9   78B6A33E   02765708B5BF
Round  11   78B6A33E   ED53C46D   6D5560AF7CA5
Round  12   ED53C46D   20662AE4   C2C1E96A4BF3
Round  13   20662AE4   7555AD3B   99C31397C91F
Round  14   7555AD3B   242241BC   251B8BC717D0
Round  15   242241BC   F243FECB   3330C5D9A36D
Round  16   60385A72   F243FECB   181C5D75C66D
Cipher Text: 22AF081E9DD9EF8A
```

kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Clone of Pari
Windows Se
FLareVM
kali-linux-202
Windows 10
Home
kali-linux-2023.4-vmware-...
File Actions Edit View Help
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
Type here to search
12°C
8:08 pm
18/03/2024

Now by changing fisrt bit of plaintext: "023456ABCD132536" , after completing DES whole process, my ciphertext is: "22AF081E9DD9EF8A".

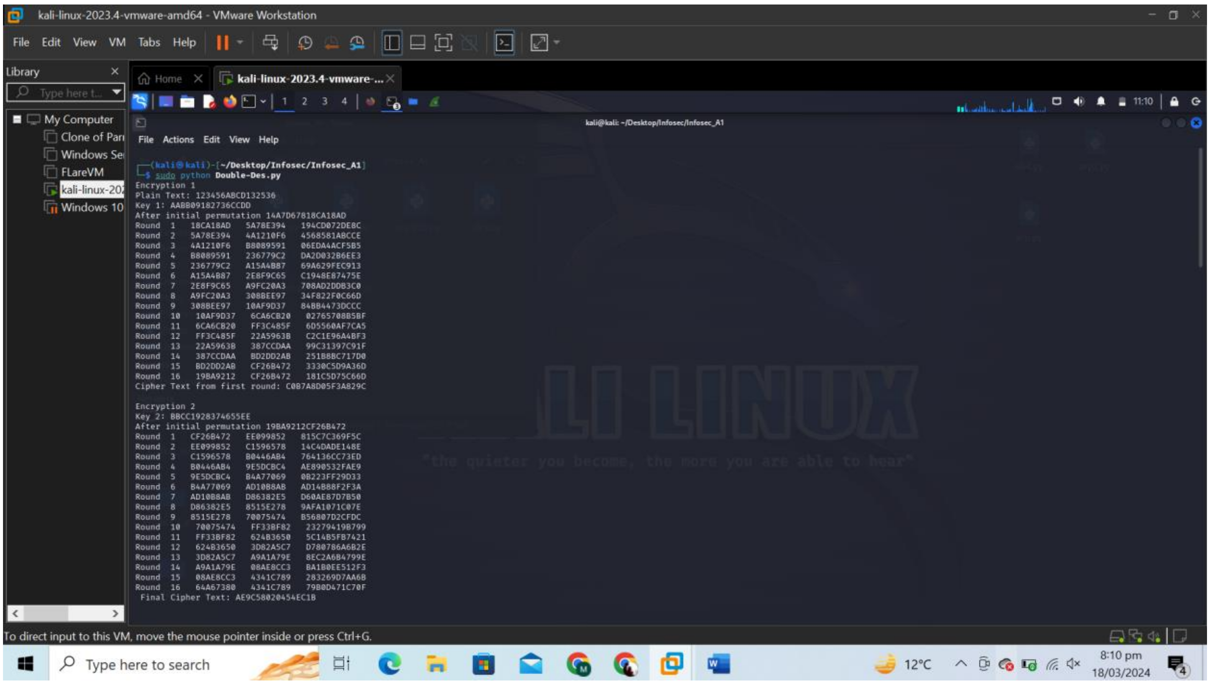
There is a calculation of change of bits in every round. (avalanche effect).


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Clone of Pari
Windows Se
FLareVM
kali-linux-202
Windows 10
Home
kali-linux-2023.4-vmware-...
kali@kali: ~/Desktop/Infosec/Infosec_A1
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
12°C
8:09 pm
18/03/2024

```
Round  16   19BA9212   CF26B472   181C5D75C66D
Cipher Text: C0B7A8D05F3A829C

────────────────────First hex value changed────────────────────
Encryption
Plain Text: 023456ABCD132536
After initial permutation 14A6D67818CA18AD
Round  1   18CA18AD   5A79E394   194CD072DE8C
Round  2   5A79E394   EA521036   4568581ABCCE
Round  3   EA521036   A818BEB0   06EDA4ACF5B5
Round  4   A818BEB0   7FD8943B   DA2D032B6EE3
Round  5   7FD8943B   7272B957   69A629FEC913
Round  6   7272B957   8DE43224   C1948E87475E
Round  7   8DE43224   68F50898   708AD2DDB3C0
Round  8   68F50898   C04D9820   34F822F0C66D
Round  9   C04D9820   9B6226F9   84BB4473DCCC
Round  10   9B6226F9   78B6A33E   02765708B5BF
Round  11   78B6A33E   ED53C46D   6D5560AF7CA5
Round  12   ED53C46D   20662AE4   C2C1E96A4BF3
Round  13   20662AE4   7555AD3B   99C31397C91F
Round  14   7555AD3B   242241BC   251B8BC717D0
Round  15   242241BC   F243FECB   3330C5D9A36D
Round  16   60385A72   F243FECB   181C5D75C66D
Cipher Text: 22AF081E9DD9EF8A

────────────────Avalanche Effect────────────────

Round 1 Changed bits: 1
Round 2 Changed bits: 6
Round 3 Changed bits: 13
Round 4 Changed bits: 31
Round 5 Changed bits: 38
Round 6 Changed bits: 31
Round 7 Changed bits: 28
Round 8 Changed bits: 31
Round 9 Changed bits: 39
Round 10 Changed bits: 30
Round 11 Changed bits: 24
Round 12 Changed bits: 31
Round 13 Changed bits: 29
Round 14 Changed bits: 28
Round 15 Changed bits: 33
Round 16 Changed bits: 29
```

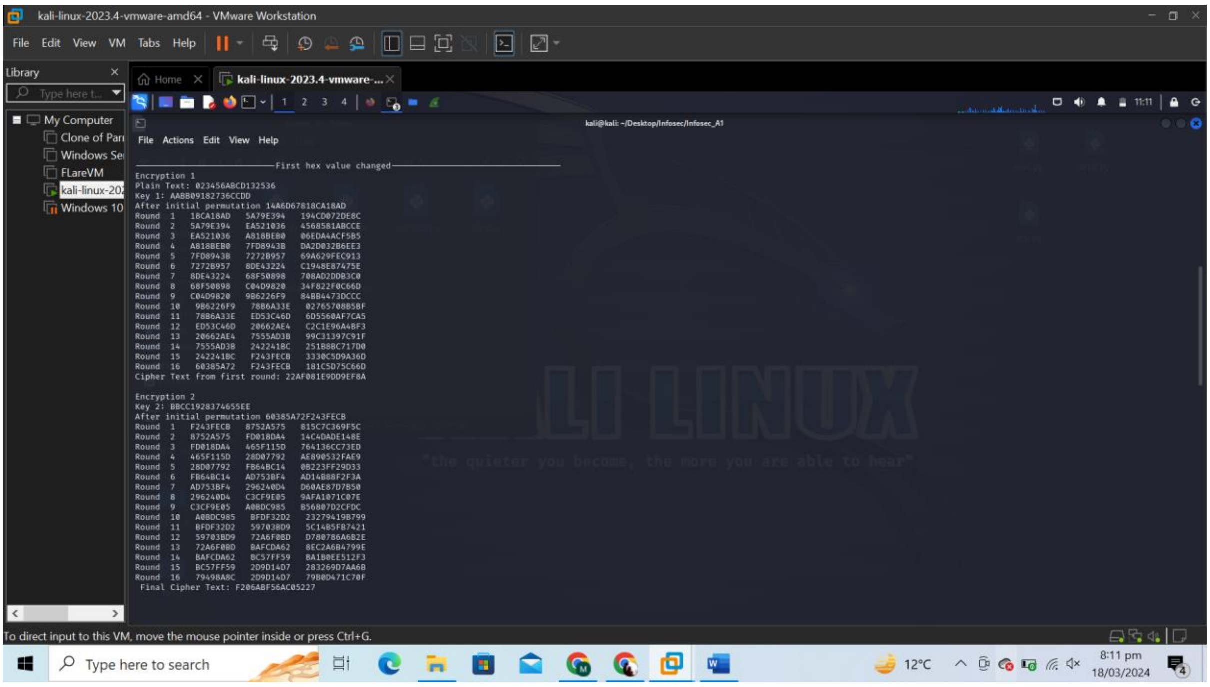
- ## 2-DES

  In Double DES, we call encryption function 2 times, which means there are total 32 rounds by which we get our cipher text. So, our plaintext is "123456ABCD132536", and after completing two times encryption we got our ciphertext: "AE9C58020454EC1B".


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Clone of Pari
Windows Se
FLareVM
kali-linux-202
Windows 10
Home
kali-linux-2023.4-vmware-...
kali@kali: ~/Desktop/Infosec/Infosec_A1
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
12°C
8:10 pm
18/03/2024

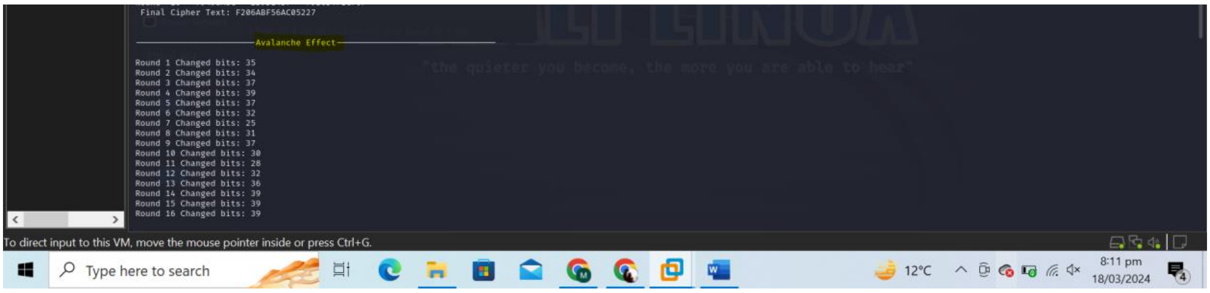
```
┌──(kali㉿kali)-[~/Desktop/Infosec/Infosec_A1]
└─$ sudo python Double-Des.py
Encryption 1
Plain Text: 123456ABCD132536
Key 1: AABB09182736CCDD
After initial permutation 14A7D67818CA18AD
Round  1   18CA18AD   5A78E394   194CD072DE8C
Round  2   5A78E394   4A1210F6   4568581ABCCE
Round  3   4A1210F6   B8089591   06EDA4ACF5B5
Round  4   B8089591   236779C2   DA2D032B6EE3
Round  5   236779C2   A15A4B87   69A629FEC913
Round  6   A15A4B87   2E8F9C65   C1948E87475E
Round  7   2E8F9C65   A9FC20A3   708AD2DDB3C0
Round  8   A9FC20A3   308BEE97   34F822F0C66D
Round  9   308BEE97   10AF9D37   84BB4473DCCC
Round  10   10AF9D37   6CA6CB20   02765708B5BF
Round  11   6CA6CB20   FF3C485F   6D5560AF7CA5
Round  12   FF3C485F   22A5963B   C2C1E96A4BF3
Round  13   22A5963B   387CCDAA   99C31397C91F
Round  14   387CCDAA   BD2DD2AB   251B8BC717D0
Round  15   BD2DD2AB   CF26B472   3330C5D9A36D
Round  16   19BA9212   CF26B472   181C5D75C66D
Cipher Text from first round: C0B7A8D05F3A829C

Encryption 2
Key 2: BBCC1928374655EE
After initial permutation 19BA9212CF26B472
Round  1   CF26B472   EE099852   815C7C369F5C
Round  2   EE099852   C1596578   14C4DADE148E
Round  3   C1596578   B0446AB4   764136CC73ED
Round  4   B0446AB4   9E5DCBC4   AE890532FAE9
Round  5   9E5DCBC4   B4A77069   0B223FF29D33
Round  6   B4A77069   AD10B8AB   AD14B88F2F3A
Round  7   AD10B8AB   D86382E5   D60AE87D7B50
Round  8   D86382E5   8515E278   9AFA1071C07E
Round  9   8515E278   70075474   B56807D2CFDC
Round  10   70075474   FF33BF82   23279419B799
Round  11   FF33BF82   624B3650   5C14B5FB7421
Round  12   624B3650   3D82A5C7   D780786A6B2E
Round  13   3D82A5C7   A9A1A79E   8EC2A6B4799E
Round  14   A9A1A79E   08AE8CC3   BA1B0EE512F3
Round  15   08AE8CC3   4341C789   283269D7AA6B
Round  16   64A67380   4341C789   79B0D471C70F
 Final Cipher Text: AE9C58020454EC1B
```

Now by changing first bit form plaintext, our plaintext become: “023456ABCD132536”. Ciphertext generated after completing 32 rounds is now: “F206ABF56AC05227”.



```
────────────────────────First hex value changed────────────────────────
Encryption 1
Plain Text: 023456ABCD132536
Key 1: AABB09182736CCDD
After initial permutation 14A6D67818CA18AD
Round  1   18CA18AD   5A79E394   194CD072DE8C
Round  2   5A79E394   EA521036   4568581ABCCE
Round  3   EA521036   A818BEB0   06EDA4ACF5B5
Round  4   A818BEB0   7FD8943B   DA2D032B6EE3
Round  5   7FD8943B   7272B957   69A629FEC913
Round  6   7272B957   8DE43224   C1948E87475E
Round  7   8DE43224   68F50898   708AD2DDB3C0
Round  8   68F50898   C04D9820   34F822F0C66D
Round  9   C04D9820   9B6226F9   84BB4473DCCC
Round  10   9B6226F9   78B6A33E   02765708B5BF
Round  11   78B6A33E   ED53C46D   6D5560AF7CA5
Round  12   ED53C46D   20662AE4   C2C1E96A4BF3
Round  13   20662AE4   7555AD3B   99C31397C91F
Round  14   7555AD3B   242241BC   251B8BC717D0
Round  15   242241BC   F243FECB   3330C5D9A36D
Round  16   60385A72   F243FECB   181C5D75C66D
Cipher Text from first round: 22AF081E9DD9EF8A

Encryption 2
Key 2: BBCC1928374655EE
After initial permutation 60385A72F243FECB
Round  1   F243FECB   8752A575   815C7C369F5C
Round  2   8752A575   FD018DA4   14C4DADE148E
Round  3   FD018DA4   465F115D   764136CC73ED
Round  4   465F115D   28D07792   AE890532FAE9
Round  5   28D07792   FB64BC14   0B223FF29D33
Round  6   FB64BC14   AD753BF4   AD14B88F2F3A
Round  7   AD753BF4   296240D4   D60AE87D7B50
Round  8   296240D4   C3CF9E05   9AFA1071C07E
Round  9   C3CF9E05   A0BDC985   B56807D2CFDC
Round  10   A0BDC985   BFDF32D2   23279419B799
Round  11   BFDF32D2   59703BD9   5C14B5FB7421
Round  12   59703BD9   72A6F0BD   D780786A6B2E
Round  13   72A6F0BD   BAFCDA62   8EC2A6B4799E
Round  14   BAFCDA62   BC57FF59   BA1B0EE512F3
Round  15   BC57FF59   2D9D14D7   283269D7AA6B
Round  16   79498A8C   2D9D14D7   79B0D471C70F
 Final Cipher Text: F206ABF56AC05227
```

Change in bits in every round is calculated.

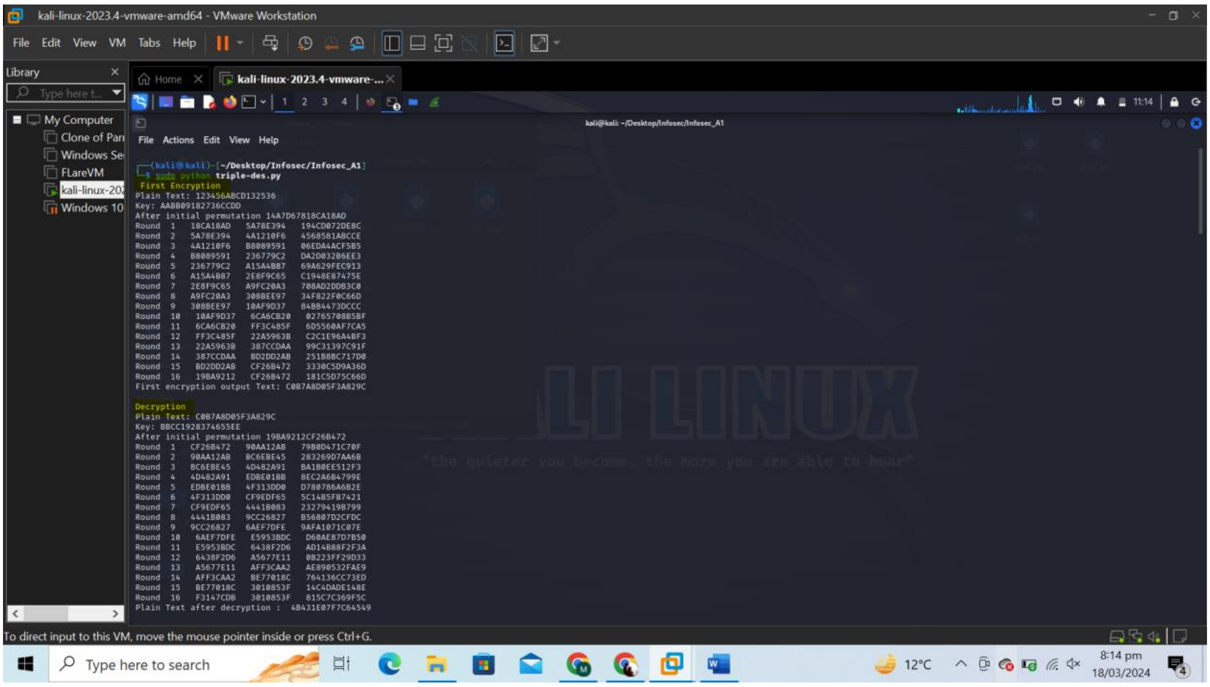


```
 Final Cipher Text: F206ABF56AC05227

──────────────────Avalanche Effect──────────────────

Round 1 Changed bits: 35
Round 2 Changed bits: 34
Round 3 Changed bits: 37
Round 4 Changed bits: 39
Round 5 Changed bits: 37
Round 6 Changed bits: 32
Round 7 Changed bits: 25
Round 8 Changed bits: 31
Round 9 Changed bits: 37
Round 10 Changed bits: 30
Round 11 Changed bits: 28
Round 12 Changed bits: 32
Round 13 Changed bits: 36
Round 14 Changed bits: 39
Round 15 Changed bits: 39
Round 16 Changed bits: 39
```

- ## 3-DES

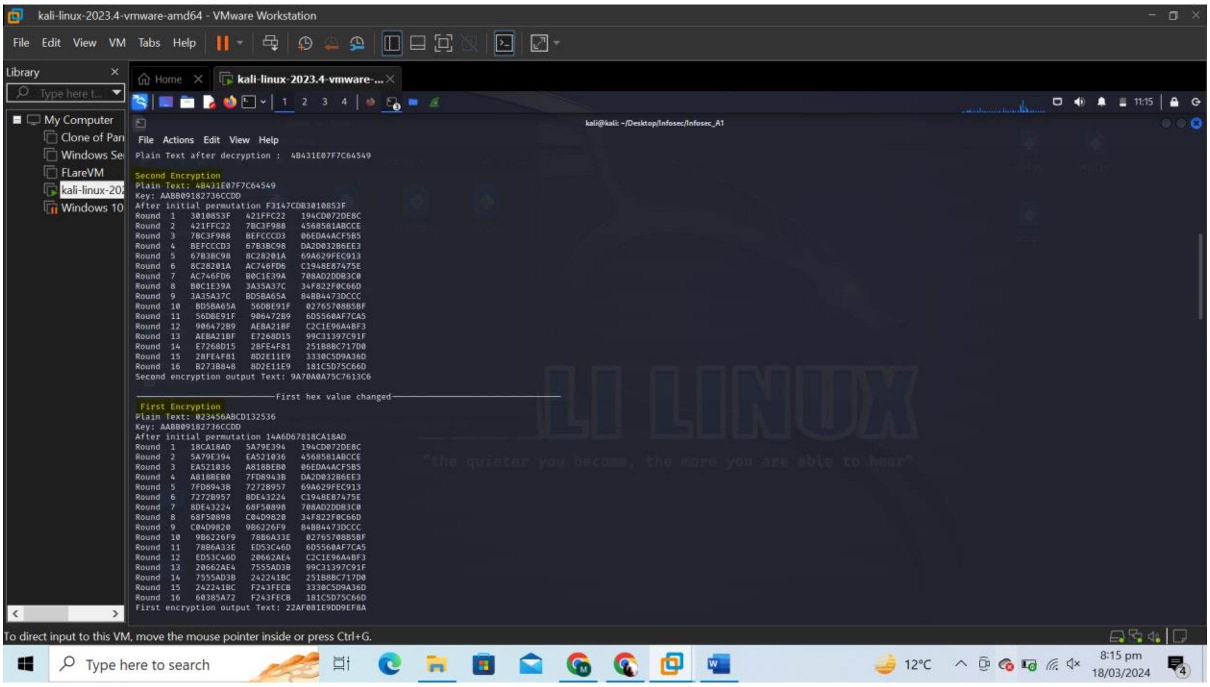
In triple DES, there are two modes. First is **[encryption, encryption, encryption]** and the second is **[encryption, decryption, encryption]**. We choose second one and implement in our code for performing tripes DES. We used two keys for this process. First key is used to encrypt the plaintext and pass it to the decryption function and then we used second key to decrypt it and again pass it to the encryption function, this time we again used first key to encrypt the plaintext we got from decryption function and convert it to final ciphertext.

In starting plaintext is: “123456ABCD132536” and we got our ciphertext by completing whole process of encryption, decryption, encryption. Ciphertext we got is: “9A70A0A75C7613C6”.

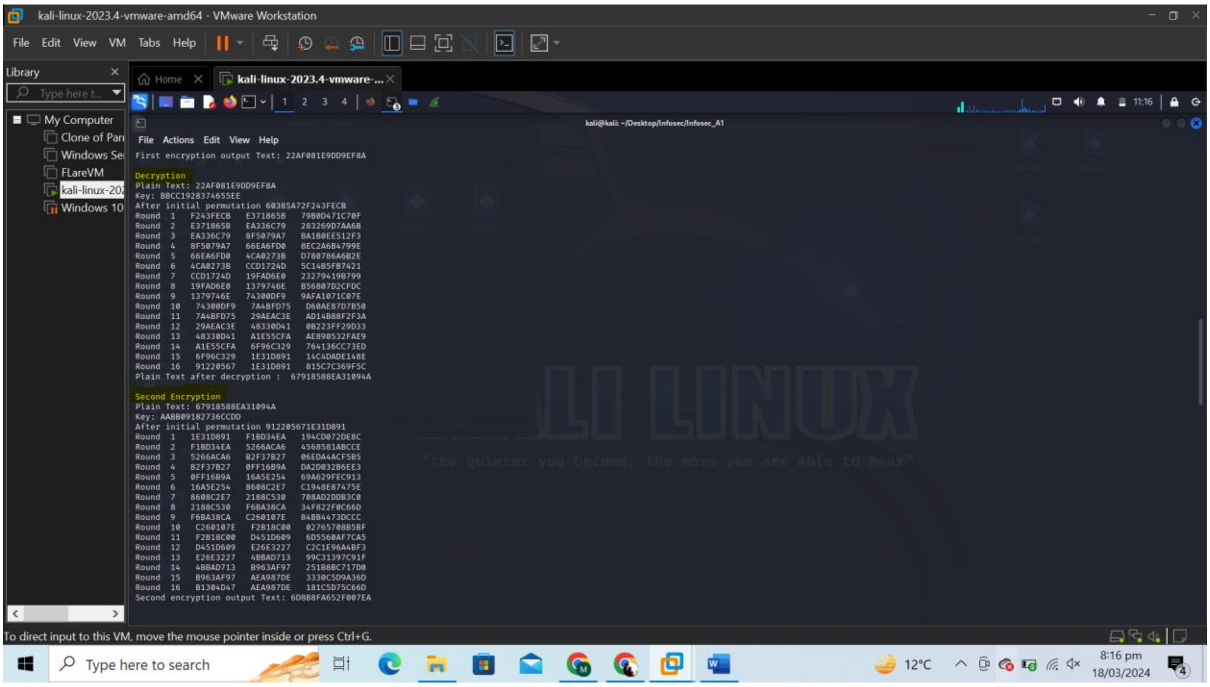


```
┌──(kali㉿kali)-[~/Desktop/Infosec/Infosec_A1]
└─$ sudo python triple-des.py
 First Encryption
Plain Text: 123456ABCD132536
Key: AABB09182736CCDD
After initial permutation 14A7D67818CA18AD
Round  1   18CA18AD   5A78E394   194CD072DE8C
Round  2   5A78E394   4A1210F6   4568581ABCCE
Round  3   4A1210F6   B8089591   06EDA4ACF5B5
Round  4   B8089591   236779C2   DA2D032B6EE3
Round  5   236779C2   A15A4B87   69A629FEC913
Round  6   A15A4B87   2E8F9C65   C1948E87475E
Round  7   2E8F9C65   A9FC20A3   708AD2DDB3C0
Round  8   A9FC20A3   308BEE97   34F822F0C66D
Round  9   308BEE97   10AF9D37   84BB4473DCCC
Round  10   10AF9D37   6CA6CB20   02765708B5BF
Round  11   6CA6CB20   FF3C485F   6D5560AF7CA5
Round  12   FF3C485F   22A5963B   C2C1E96A4BF3
Round  13   22A5963B   387CCDAA   99C31397C91F
Round  14   387CCDAA   BD2DD2AB   251B8BC717D0
Round  15   BD2DD2AB   CF26B472   3330C5D9A36D
Round  16   19BA9212   CF26B472   181C5D75C66D
First encryption output Text: C0B7A8D05F3A829C

Decryption
Plain Text: C0B7A8D05F3A829C
Key: BBCC1928374655EE
After initial permutation 19BA9212CF26B472
Round  1   CF26B472   90AA12AB   79B0D471C70F
Round  2   90AA12AB   BC6EBE45   283269D7AA6B
Round  3   BC6EBE45   4D482A91   BA1B0EE512F3
Round  4   4D482A91   EDBE01BB   8EC2A6B4799E
Round  5   EDBE01BB   4F313DD0   D780786A6B2E
Round  6   4F313DD0   CF9EDF65   5C14B5FB7421
Round  7   CF9EDF65   4441B083   232794198799
Round  8   4441B083   9CC26827   B56807D2CFDC
Round  9   9CC26827   6AEF7DFE   9AFA1071C07E
Round  10   6AEF7DFE   E5953BDC   D60AE87D7B50
Round  11   E5953BDC   6438F2D6   AD14B88F2F3A
Round  12   6438F2D6   A5677E11   0B223FF29D33
Round  13   A5677E11   AFF3CAA2   AE890532FAE9
Round  14   AFF3CAA2   BE77018C   764136CC73ED
Round  15   BE77018C   3010853F   14C4DADE148E
Round  16   F3147CDB   3010853F   815C7C369F5C
Plain Text after decryption :  4B431E07F7C64549
```

We changed first bit of our plaintext: "023456ABCD132536" and then performing triple DES on it. The ciphertext we got is: "6D8B8FA652F007EA".

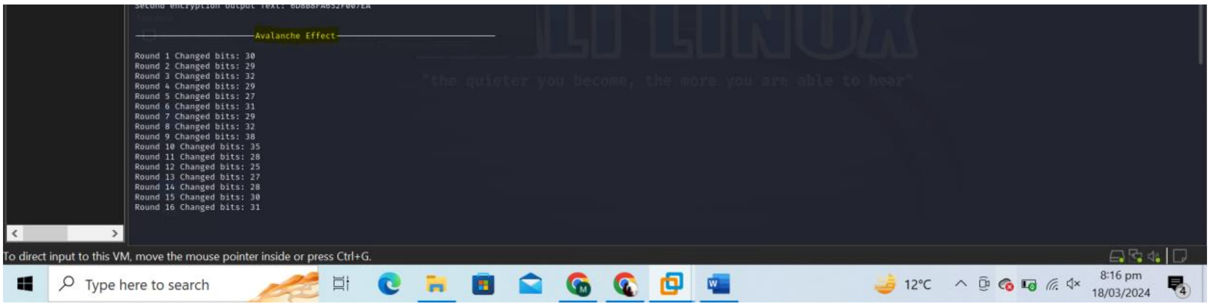


```
Plain Text after decryption :  4B431E07F7C64549

Second Encryption
Plain Text: 4B431E07F7C64549
Key: AABB09182736CCDD
After initial permutation F3147CDB3010853F
Round  1   3010853F   421FFC22   194CD072DE8C
Round  2   421FFC22   7BC3F988   4568581ABCCE
Round  3   7BC3F988   BEFCCCD3   06EDA4ACF5B5
Round  4   BEFCCCD3   67B3BC98   DA2D032B6EE3
Round  5   67B3BC98   8C28201A   69A629FEC913
Round  6   8C28201A   AC746FD6   C1948E87475E
Round  7   AC746FD6   B0C1E39A   708AD2DDB3C0
Round  8   B0C1E39A   3A35A37C   34F822F0C66D
Round  9   3A35A37C   BD5BA65A   84BB4473DCCC
Round  10   BD5BA65A   56DBE91F   02765708B5BF
Round  11   56DBE91F   906472B9   6D5560AF7CA5
Round  12   906472B9   AEBA21BF   C2C1E96A4BF3
Round  13   AEBA21BF   E7268D15   99C31397C91F
Round  14   E7268D15   28FE4F81   251B8BC717D0
Round  15   28FE4F81   8D2E11E9   3330C5D9A36D
Round  16   B273B848   8D2E11E9   181C5D75C66D
Second encryption output Text: 9A70A0A75C7613C6

────────────────────First hex value changed────────────────────
 First Encryption
Plain Text: 023456ABCD132536
Key: AABB09182736CCDD
After initial permutation 14A6D67818CA18AD
Round  1   18CA18AD   5A79E394   194CD072DE8C
Round  2   5A79E394   EA521036   4568581ABCCE
Round  3   EA521036   A818BEB0   06EDA4ACF5B5
Round  4   A818BEB0   7FD8943B   DA2D032B6EE3
Round  5   7FD8943B   7272B957   69A629FEC913
Round  6   7272B957   8DE43224   C1948E87475E
Round  7   8DE43224   68F50898   708AD2DDB3C0
Round  8   68F50898   C04D9820   34F822F0C66D
Round  9   C04D9820   9B6226F9   84BB4473DCCC
Round  10   9B6226F9   78B6A33E   02765708B5BF
Round  11   78B6A33E   ED53C46D   6D5560AF7CA5
Round  12   ED53C46D   20662AE4   C2C1E96A4BF3
Round  13   20662AE4   7555AD3B   99C31397C91F
Round  14   7555AD3B   242241BC   251B8BC717D0
Round  15   242241BC   F243FECB   3330C5D9A36D
Round  16   60385A72   F243FECB   181C5D75C66D
First encryption output Text: 22AF081E9DD9EF8A
```



```
First encryption output Text: 22AF081E9DD9EF8A

Decryption
Plain Text: 22AF081E9DD9EF8A
Key: BBCC1928374655EE
After initial permutation 60385A72F243FECB
Round  1   F243FECB   E371865B   79B0D471C70F
Round  2   E371865B   EA336C79   283269D7AA6B
Round  3   EA336C79   8F5079A7   BA1B0EE512F3
Round  4   8F5079A7   66EA6FD0   8EC2A6B4799E
Round  5   66EA6FD0   4CA0273B   D780786A6B2E
Round  6   4CA0273B   CCD1724D   5C14B5FB7421
Round  7   CCD1724D   19FAD6E0   23279419B799
Round  8   19FAD6E0   1379746E   B56807D2CFDC
Round  9   1379746E   74300DF9   9AFA1071C07E
Round  10   74300DF9   7A4BFD75   D60AE87D7B50
Round  11   7A4BFD75   29AEAC3E   AD14B88F2F3A
Round  12   29AEAC3E   48330D41   0B223FF29D33
Round  13   48330D41   A1E55CFA   AE890532FAE9
Round  14   A1E55CFA   6F96C329   764136CC73ED
Round  15   6F96C329   1E31D891   14C4DADE148E
Round  16   91220567   1E31D891   815C7C369F5C
Plain Text after decryption :  67918588EA31094A

Second Encryption
Plain Text: 67918588EA31094A
Key: AABB09182736CCDD
After initial permutation 912205671E31D891
Round  1   1E31D891   F1BD34EA   194CD072DE8C
Round  2   F1BD34EA   5266ACA6   4568581ABCCE
Round  3   5266ACA6   B2F37B27   06EDA4ACF5B5
Round  4   B2F37B27   0FF16B9A   DA2D032B6EE3
Round  5   0FF16B9A   16A5E254   69A629FEC913
Round  6   16A5E254   8608C2E7   C1948E87475E
Round  7   8608C2E7   2188C530   708AD2DDB3C0
Round  8   2188C530   F6BA38CA   34F822F0C66D
Round  9   F6BA38CA   C260107E   84BB4473DCCC
Round  10   C260107E   F2B18C00   02765708B5BF
Round  11   F2B18C00   D451D609   6D5560AF7CA5
Round  12   D451D609   E26E3227   C2C1E96A4BF3
Round  13   E26E3227   4BBAD713   99C31397C91F
Round  14   4BBAD713   B963AF97   251B8BC717D0
Round  15   B963AF97   AEA987DE   3330C5D9A36D
Round  16   B1304D47   AEA987DE   181C5D75C66D
Second encryption output Text: 6D8B8FA652F007EA
```

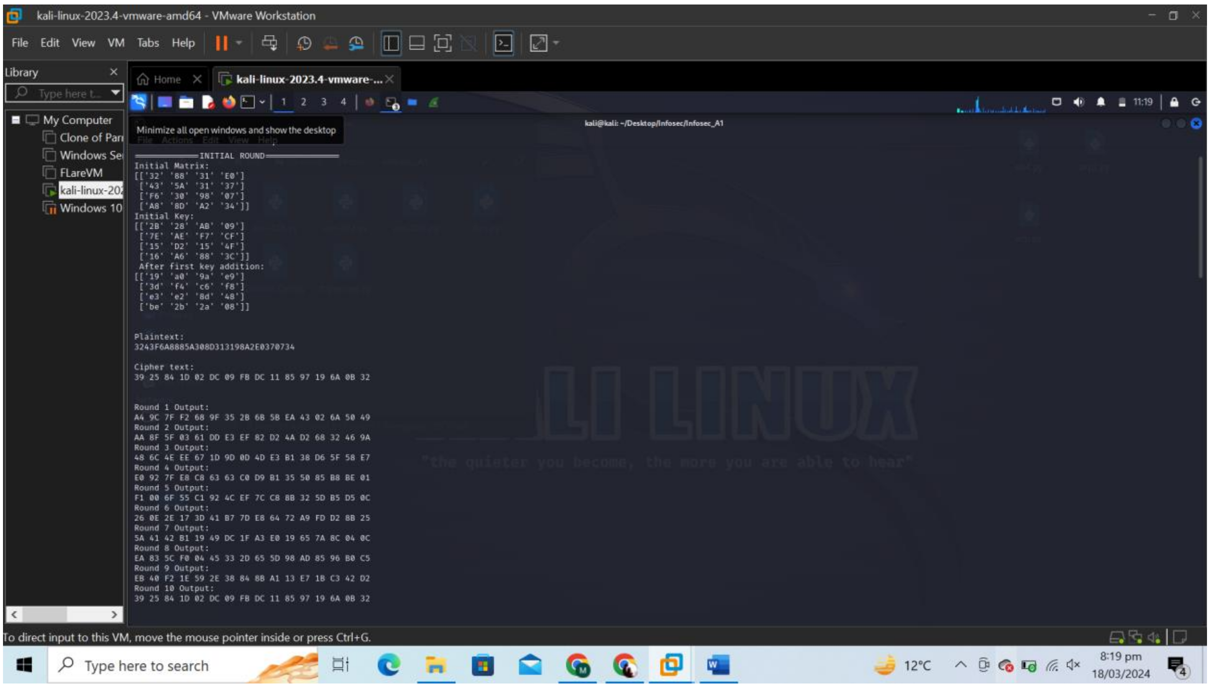
Change in bits in every round is shown below.



```
Second encryption output Text: 6D8B8FA652F007EA

────────────────────Avalanche Effect────────────────────

Round 1 Changed bits: 30
Round 2 Changed bits: 29
Round 3 Changed bits: 32
Round 4 Changed bits: 29
Round 5 Changed bits: 27
Round 6 Changed bits: 31
Round 7 Changed bits: 29
Round 8 Changed bits: 32
Round 9 Changed bits: 38
Round 10 Changed bits: 35
Round 11 Changed bits: 28
Round 12 Changed bits: 25
Round 13 Changed bits: 27
Round 14 Changed bits: 28
Round 15 Changed bits: 30
Round 16 Changed bits: 31
```

- ## AES-128

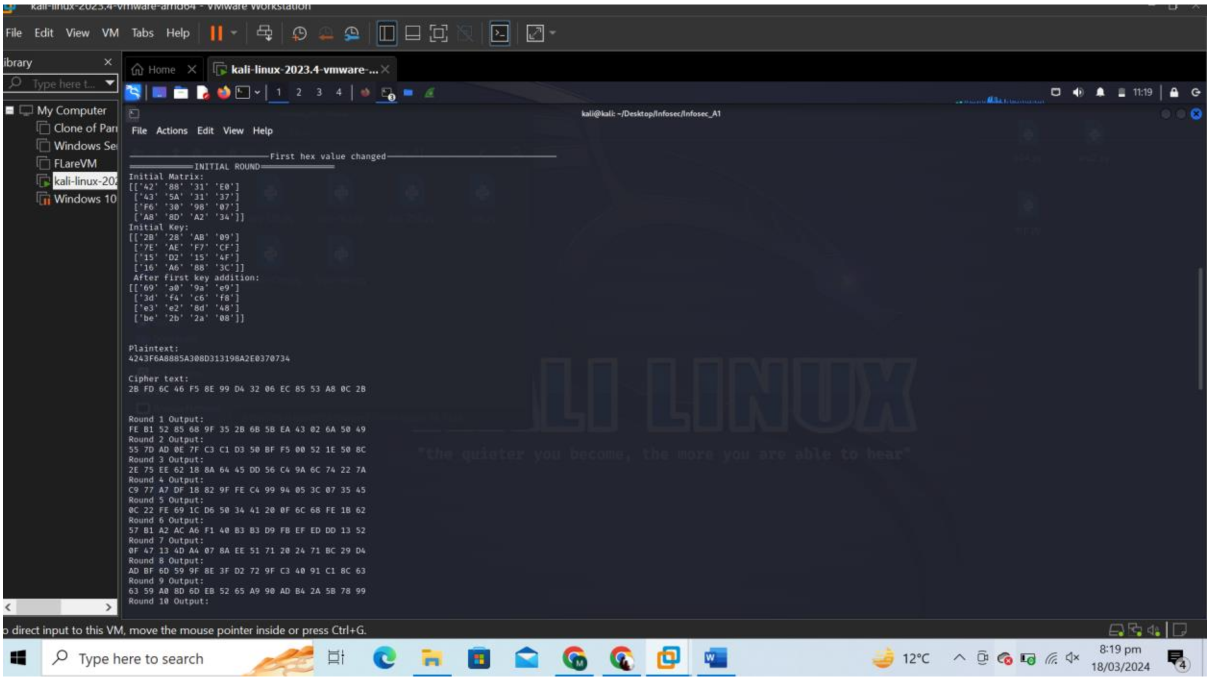
AES-128 completes in 10 rounds. We input our plaintext: “3243F6A8885A308D313198A2E0370734” to AES-128 script, and we got our cipher text: “3925841D02DC09FBDC118597196A0B32”.



kali-linux-2023.4-vmware-amd64 - VMware Workstation
Minimize all open windows and show the desktop
kali@kali: ~/Desktop/Infosec/Infosec_A1
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
8:19 pm
18/03/2024

```
════════════INITIAL ROUND════════════
Initial Matrix:
[['32' '88' '31' 'E0']
 ['43' '5A' '31' '37']
 ['F6' '30' '98' '07']
 ['A8' '8D' 'A2' '34']]
Initial Key:
[['2B' '28' 'AB' '09']
 ['7E' 'AE' 'F7' 'CF']
 ['15' 'D2' '15' '4F']
 ['16' 'A6' '88' '3C']]
 After first key addition:
[['19' 'a0' '9a' 'e9']
 ['3d' 'f4' 'c6' 'f8']
 ['e3' 'e2' '8d' '48']
 ['be' '2b' '2a' '08']]


Plaintext:
3243F6A8885A308D313198A2E0370734

Cipher text:
39 25 84 1D 02 DC 09 FB DC 11 85 97 19 6A 0B 32


Round 1 Output:
A4 9C 7F F2 68 9F 35 2B 6B 5B EA 43 02 6A 50 49
Round 2 Output:
AA 8F 5F 03 61 DD E3 EF 82 D2 4A D2 68 32 46 9A
Round 3 Output:
48 6C 4E EE 67 1D 9D 0D 4D E3 B1 38 D6 5F 58 E7
Round 4 Output:
E0 92 7F E8 C8 63 63 C0 D9 B1 35 50 85 B8 BE 01
Round 5 Output:
F1 00 6F 55 C1 92 4C EF 7C C8 8B 32 5D B5 D5 0C
Round 6 Output:
26 0E 2E 17 3D 41 B7 7D E8 64 72 A9 FD D2 8B 25
Round 7 Output:
5A 41 42 B1 19 49 DC 1F A3 E0 19 65 7A 8C 04 0C
Round 8 Output:
EA 83 5C F0 04 45 33 2D 65 5D 98 AD 85 96 B0 C5
Round 9 Output:
EB 40 F2 1E 59 2E 38 84 8B A1 13 E7 1B C3 42 D2
Round 10 Output:
39 25 84 1D 02 DC 09 FB DC 11 85 97 19 6A 0B 32
```

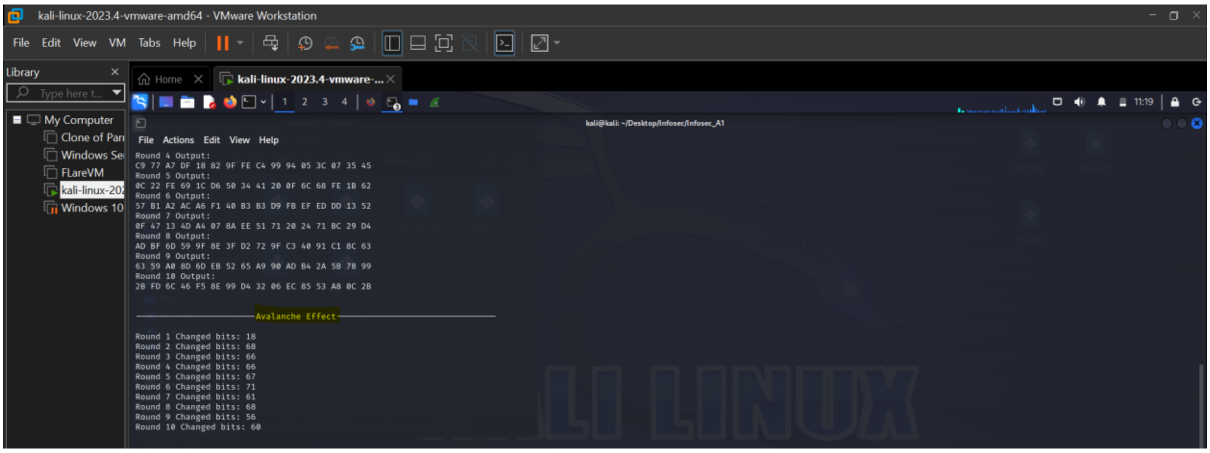
Then we changed first bit from our plaintext: "4243F6A8885A308D313198A2E0370734", and our ciphertext becomes: "2BFD6C46F58E99D43206EC8553AB0C2B".



kali-linux-2023.4-vmware-amd64 - VMware Workstation
kali@kali: ~/Desktop/Infosec/Infosec_A1
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
8:19 pm
18/03/2024

```
────────────────First hex value changed────────────────
════════════INITIAL ROUND════════════
Initial Matrix:
[['42' '88' '31' 'E0']
 ['43' '5A' '31' '37']
 ['F6' '30' '98' '07']
 ['A8' '8D' 'A2' '34']]
Initial Key:
[['2B' '28' 'AB' '09']
 ['7E' 'AE' 'F7' 'CF']
 ['15' 'D2' '15' '4F']
 ['16' 'A6' '88' '3C']]
 After first key addition:
[['69' 'a0' '9a' 'e9']
 ['3d' 'f4' 'c6' 'f8']
 ['e3' 'e2' '8d' '48']
 ['be' '2b' '2a' '08']]


Plaintext:
4243F6A8885A308D313198A2E0370734

Cipher text:
2B FD 6C 46 F5 8E 99 D4 32 06 EC 85 53 A8 0C 2B


Round 1 Output:
FE B1 52 85 68 9F 35 2B 6B 5B EA 43 02 6A 50 49
Round 2 Output:
55 7D AD 0E 7F C3 C1 D3 50 BF F5 00 52 1E 50 8C
Round 3 Output:
2E 75 EE 62 18 8A 64 45 DD 56 C4 9A 6C 74 22 7A
Round 4 Output:
C9 77 A7 DF 18 82 9F FE C4 99 94 05 3C 07 35 45
Round 5 Output:
0C 22 FE 69 1C D6 50 34 41 20 0F 6C 68 FE 1B 62
Round 6 Output:
57 B1 A2 AC A6 F1 40 B3 B3 D9 FB EF ED DD 13 52
Round 7 Output:
0F 47 13 4D A4 07 8A EE 51 71 20 24 71 BC 29 D4
Round 8 Output:
AD BF 6D 59 9F 8E 3F D2 72 9F C3 40 91 C1 8C 63
Round 9 Output:
63 59 A0 8D 6D EB 52 65 A9 90 AD B4 2A 5B 78 99
Round 10 Output:
```

Avalanche effect for each round is calculated and shown below.

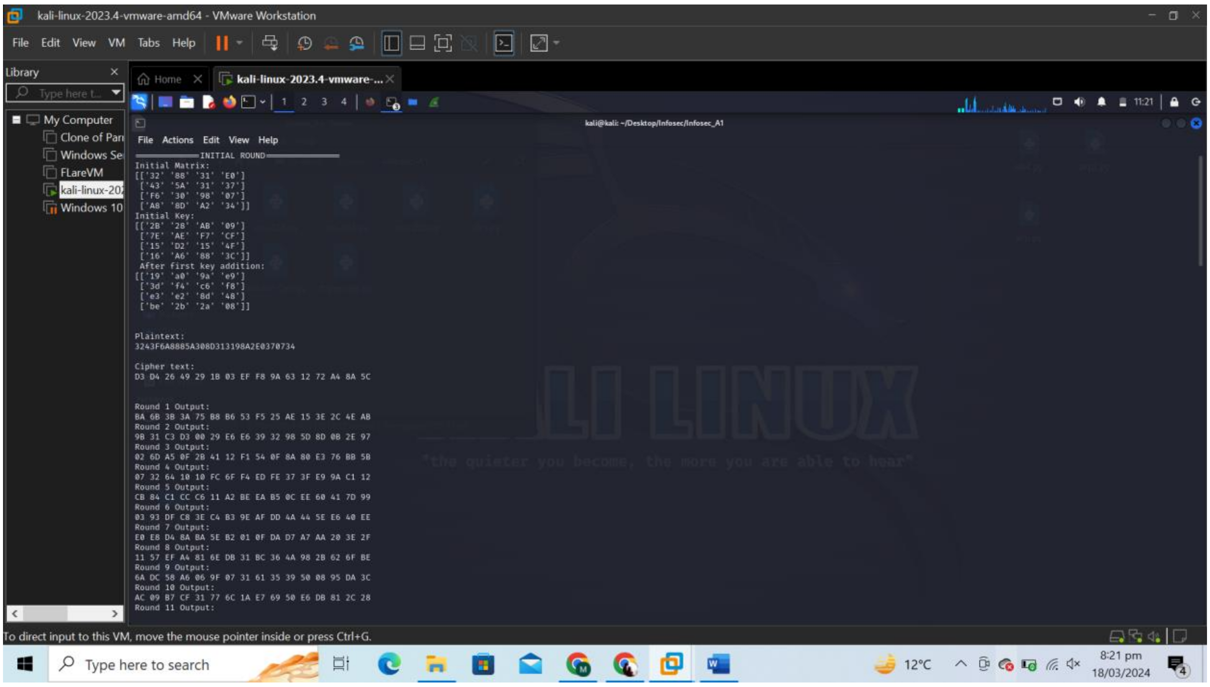


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Clone of Pari
Windows Se
FLareVM
kali-linux-202
Windows 10
Home
kali-linux-2023.4-vmware-...
kali@kali: ~/Desktop/Infosec/Infosec_A1
File Actions Edit View Help

```
Round 4 Output:
C9 77 A7 DF 18 82 9F FE C4 99 94 05 3C 07 35 45
Round 5 Output:
0C 22 FE 69 1C D6 50 34 41 20 0F 6C 68 FE 1B 62
Round 6 Output:
57 B1 A2 AC A6 F1 40 B3 B3 D9 FB EF ED DD 13 52
Round 7 Output:
0F 47 13 4D A4 07 8A EE 51 71 20 24 71 BC 29 D4
Round 8 Output:
AD BF 6D 59 9F 8E 3F D2 72 9F C3 40 91 C1 8C 63
Round 9 Output:
63 59 A0 8D 6D EB 52 65 A9 90 AD B4 2A 5B 78 99
Round 10 Output:
2B FD 6C 46 F5 8E 99 D4 32 06 EC 85 53 A8 0C 2B


────────────────────Avalanche Effect────────────────────

Round 1 Changed bits: 18
Round 2 Changed bits: 68
Round 3 Changed bits: 66
Round 4 Changed bits: 66
Round 5 Changed bits: 67
Round 6 Changed bits: 71
Round 7 Changed bits: 61
Round 8 Changed bits: 68
Round 9 Changed bits: 56
Round 10 Changed bits: 60
```

- ## AES-192

In AES-192, number of rounds are 12 now, functionality in the rounds is same as AES-128. Our plaintext is: "3243F6A8885A308D313198A2E0370734" and AES-192 convert it into the ciphertext: "D3D42649291B03EFF89A631272A48A5C".

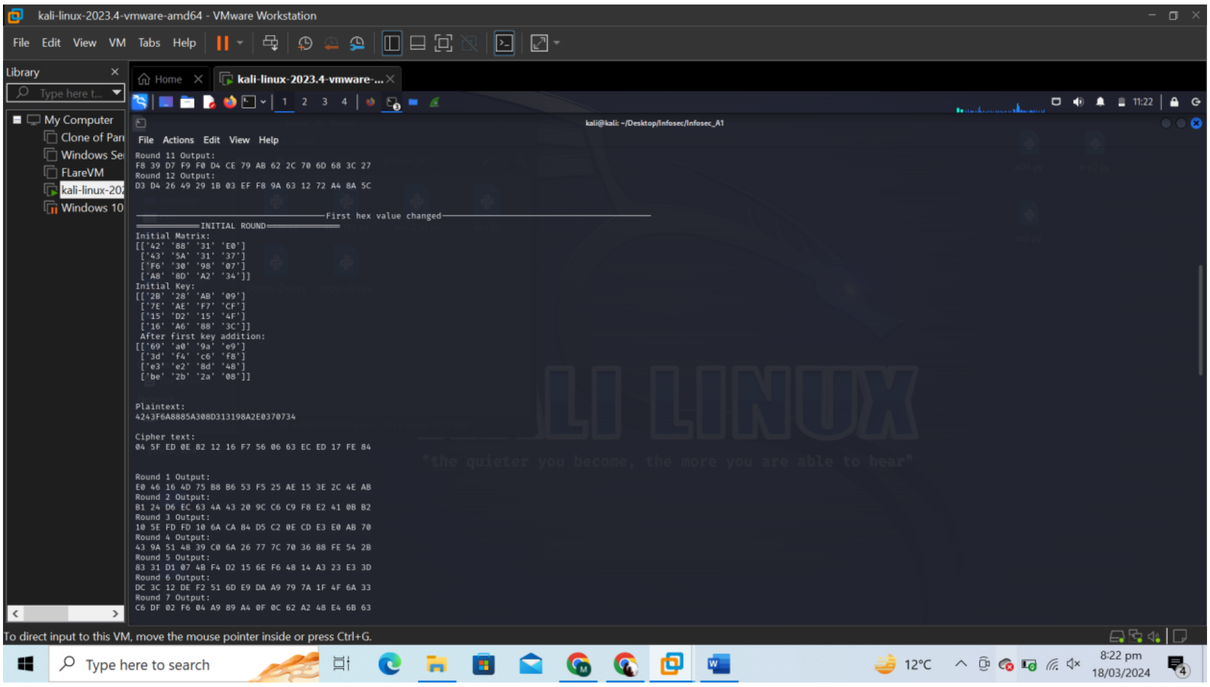


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Clone of Pari
Windows Se
FLareVM
kali-linux-202
Windows 10
Home
kali-linux-2023.4-vmware-...
kali@kali: ~/Desktop/Infosec/Infosec_A1
File Actions Edit View Help
Type here to search
12°C
8:21 pm
18/03/2024

```
═══════════════INITIAL ROUND═══════════════
Initial Matrix:
[['32' '88' '31' 'E0']
 ['43' '5A' '31' '37']
 ['F6' '30' '98' '07']
 ['A8' '8D' 'A2' '34']]
Initial Key:
[['2B' '28' 'AB' '09']
 ['7E' 'AE' 'F7' 'CF']
 ['15' 'D2' '15' '4F']
 ['16' 'A6' '88' '3C']]
 After first key addition:
[['19' 'a0' '9a' 'e9']
 ['3d' 'f4' 'c6' 'f8']
 ['e3' 'e2' '8d' '48']
 ['be' '2b' '2a' '08']]


Plaintext:
3243F6A8885A308D313198A2E0370734

Cipher text:
D3 D4 26 49 29 1B 03 EF F8 9A 63 12 72 A4 8A 5C


Round 1 Output:
BA 6B 3B 3A 75 B8 B6 53 F5 25 AE 15 3E 2C 4E AB
Round 2 Output:
9B 31 C3 D3 00 29 E6 E6 39 32 98 5D 8D 0B 2E 97
Round 3 Output:
02 6D A5 0F 2B 41 12 F1 54 0F 8A 80 E3 76 B8 5B
Round 4 Output:
07 32 64 10 10 FC 6F F4 ED FE 37 3F E9 9A C1 12
Round 5 Output:
CB 84 C1 CC C6 11 A2 BE EA B5 0C EE 60 41 7D 99
Round 6 Output:
03 93 DF C8 3E C4 B3 9E AF DD 4A 44 5E E6 40 EE
Round 7 Output:
E0 E8 D4 8A BA 5E B2 01 0F DA D7 A7 AA 20 3E 2F
Round 8 Output:
11 57 EF A4 81 6E DB 31 BC 36 4A 98 2B 62 6F BE
Round 9 Output:
6A DC 58 A6 06 9F 07 31 61 35 39 50 08 95 DA 3C
Round 10 Output:
AC 09 B7 CF 31 77 6C 1A E7 69 50 E6 DB 81 2C 28
Round 11 Output:
```

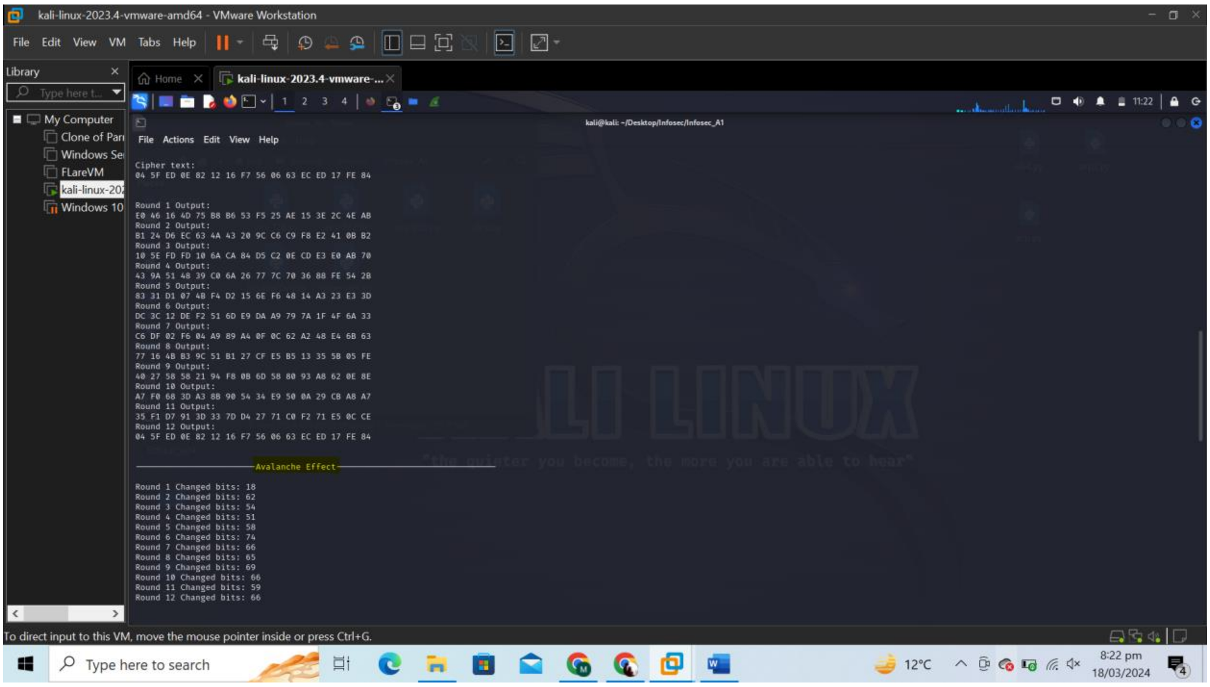
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

We changed one bit from the start of the plaintext to calculate the Avalanche effect. Our plaintext is now: "4243F6A8885A308D313198A2E0370734" and the ciphertext we got from AES-192 is now: "045FED0E821216F7560663ECED17Fe84".


kali-linux-2023.4-vmware-amd64 - VMware Workstation
kali@kali: ~/Desktop/Infosec/Infosec_A1
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
Round 11 Output:
F8 39 D7 F9 F0 D4 CE 79 AB 62 2C 70 6D 68 3C 27
Round 12 Output:
D3 D4 26 49 29 1B 03 EF F8 9A 63 12 72 A4 8A 5C

────────────────────────────────────First hex value changed──────────────
═════════════INITIAL ROUND═════════════
Initial Matrix:
[['42' '88' '31' 'E0']
 ['43' '5A' '31' '37']
 ['F6' '30' '98' '07']
 ['A8' '8D' 'A2' '34']]
Initial Key:
[['2B' '28' 'AB' '09']
 ['7E' 'AE' 'F7' 'CF']
 ['15' 'D2' '15' '4F']
 ['16' 'A6' '88' '3C']]
 After first key addition:
[['69' 'a0' '9a' 'e9']
 ['3d' 'f4' 'c6' 'f8']
 ['e3' 'e2' '8d' '48']
 ['be' '2b' '2a' '08']]


Plaintext:
4243F6A8885A308D313198A2E0370734

Cipher text:
04 5F ED 0E 82 12 16 F7 56 06 63 EC ED 17 FE 84


Round 1 Output:
E0 46 16 4D 75 B8 B6 53 F5 25 AE 15 3E 2C 4E AB
Round 2 Output:
B1 24 D6 EC 63 4A 43 20 9C C6 C9 F8 E2 41 0B B2
Round 3 Output:
10 5E FD FD 10 6A CA 84 D5 C2 0E CD E3 E0 AB 70
Round 4 Output:
43 9A 51 48 39 C0 6A 26 77 7C 70 36 88 FE 54 2B
Round 5 Output:
83 31 D1 07 4B F4 D2 15 6E F6 48 14 A3 23 E3 3D
Round 6 Output:
DC 3C 12 DE F2 51 6D E9 DA A9 79 7A 1F 4F 6A 33
Round 7 Output:
C6 DF 02 F6 04 A9 89 A4 0F 0C 62 A2 48 E4 6B 63
```

Change in bits by just changing one bit in the plaintext changes many bits in every round.

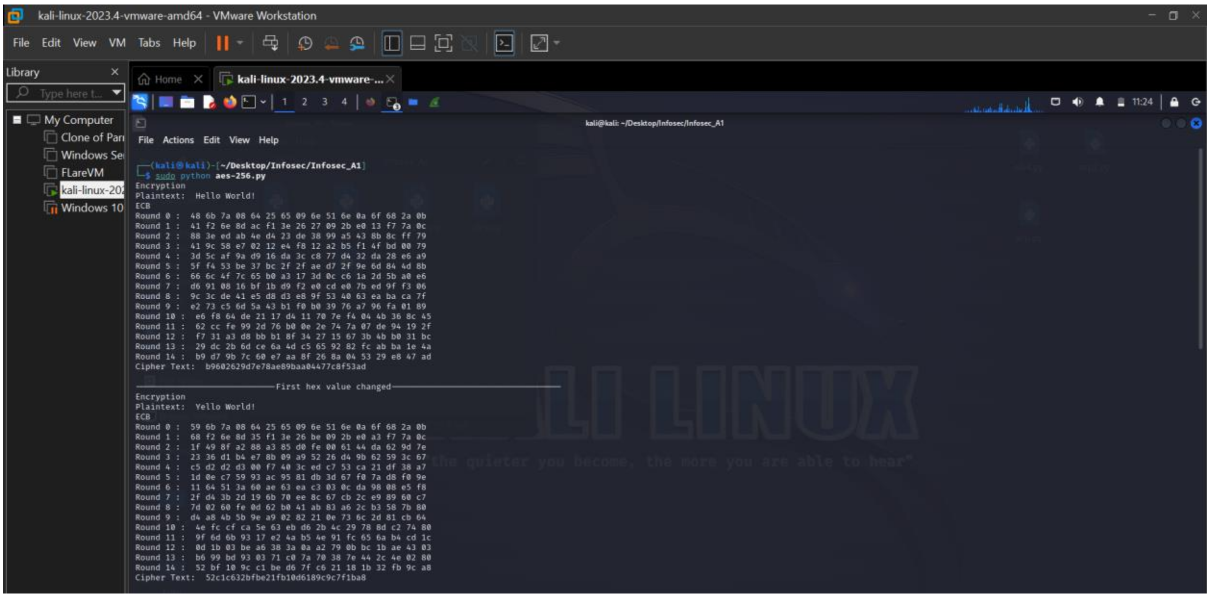

kali-linux-2023.4-vmware-amd64 - VMware Workstation
kali@kali: ~/Desktop/Infosec/Infosec_A1
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
Cipher text:
04 5F ED 0E 82 12 16 F7 56 06 63 EC ED 17 FE 84


Round 1 Output:
E0 46 16 4D 75 B8 B6 53 F5 25 AE 15 3E 2C 4E AB
Round 2 Output:
B1 24 D6 EC 63 4A 43 20 9C C6 C9 F8 E2 41 0B B2
Round 3 Output:
10 5E FD FD 10 6A CA 84 D5 C2 0E CD E3 E0 AB 70
Round 4 Output:
43 9A 51 48 39 C0 6A 26 77 7C 70 36 88 FE 54 2B
Round 5 Output:
83 31 D1 07 4B F4 D2 15 6E F6 48 14 A3 23 E3 3D
Round 6 Output:
DC 3C 12 DE F2 51 6D E9 DA A9 79 7A 1F 4F 6A 33
Round 7 Output:
C6 DF 02 F6 04 A9 89 A4 0F 0C 62 A2 48 E4 6B 63
Round 8 Output:
77 16 4B B3 9C 51 B1 27 CF E5 B5 13 35 5B 05 FE
Round 9 Output:
40 27 58 58 21 94 F8 0B 6D 58 80 93 A8 62 0E 8E
Round 10 Output:
A7 F0 68 3D A3 8B 90 54 34 E9 50 0A 29 CB A8 A7
Round 11 Output:
35 F1 D7 91 3D 33 7D D4 27 71 C0 F2 71 E5 0C CE
Round 12 Output:
04 5F ED 0E 82 12 16 F7 56 06 63 EC ED 17 FE 84

───────────────────────Avalanche Effect─────────────────────────

Round 1 Changed bits: 18
Round 2 Changed bits: 62
Round 3 Changed bits: 54
Round 4 Changed bits: 51
Round 5 Changed bits: 58
Round 6 Changed bits: 74
Round 7 Changed bits: 66
Round 8 Changed bits: 65
Round 9 Changed bits: 69
Round 10 Changed bits: 66
Round 11 Changed bits: 59
Round 12 Changed bits: 66
```

- ## AES-256

Number of rounds are 14 in AES-256. The mode we used is **ECB**. This time we used plaintext: "Hello World". After completing its 14 rounds it gives us the ciphertext in Hex form: "b9602629d7e78ae89baa04477c8f53ad".

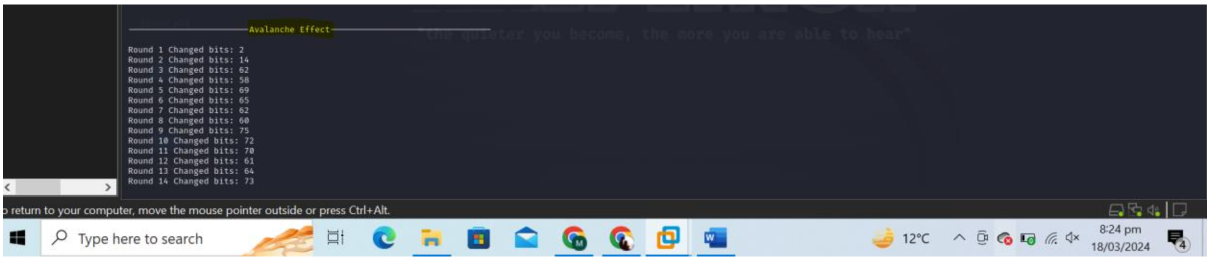
Then we changed first bit from our plaintext: "Yello World". And we got changed cipher text this time which is: "52c1c632bfbe21fb10d6189c9c7f1ba8".



kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Clone of Parr
Windows Se
FLareVM
kali-linux-202
Windows 10
Home
kali-linux-2023.4-vmware-...
kali@kali: ~/Desktop/Infosec/Infosec_A1
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/Infosec/Infosec_A1]
└─$ sudo python aes-256.py
Encryption
Plaintext:  Hello World!
ECB
Round 0 :  48 6b 7a 08 64 25 65 09 6e 51 6e 0a 6f 68 2a 0b
Round 1 :  41 f2 6e 8d ac f1 3e 26 27 09 2b e0 13 f7 7a 0c
Round 2 :  88 3e ed ab 4e d4 23 de 38 99 a5 43 8b 8c ff 79
Round 3 :  41 9c 58 e7 02 12 e4 f8 12 a2 b5 f1 4f bd 00 79
Round 4 :  3d 5c af 9a d9 16 da 3c c8 77 d4 32 da 28 e6 a9
Round 5 :  5f f4 53 be 37 bc 2f 2f ae d7 2f 9e 6d 84 4d 8b
Round 6 :  66 6c 4f 7c 65 b0 a3 17 3d 0c c6 1a 2d 5b a0 e6
Round 7 :  d6 91 08 16 bf 1b d9 f2 e0 cd e0 7b ed 9f f3 06
Round 8 :  9c 3c de 41 e5 d8 d3 e8 9f 53 40 63 ea ba ca 7f
Round 9 :  e2 73 c5 6d 5a 43 b1 f0 b0 39 76 a7 96 fa 01 89
Round 10 :  e6 f8 64 de 21 17 d4 11 70 7e f4 04 4b 36 8c 45
Round 11 :  62 cc fe 99 2d 76 b0 0e 2e 74 7a 07 de 94 19 2f
Round 12 :  f7 31 a3 d8 bb b1 8f 34 27 15 67 3b 4b b0 31 bc
Round 13 :  29 dc 2b 6d ce 6a 4d c5 65 92 82 fc ab ba 1e 4a
Round 14 :  b9 d7 9b 7c 60 e7 aa 8f 26 8a 04 53 29 e8 47 ad
Cipher Text:  b9602629d7e78ae89baa04477c8f53ad

────────────────────First hex value changed────────────────────
Encryption
Plaintext:  Yello World!
ECB
Round 0 :  59 6b 7a 08 64 25 65 09 6e 51 6e 0a 6f 68 2a 0b
Round 1 :  68 f2 6e 8d 35 f1 3e 26 be 09 2b e0 a3 f7 7a 0c
Round 2 :  1f 49 8f a2 88 a3 85 d0 fe 00 61 44 da 62 9d 7e
Round 3 :  23 36 d1 b4 e7 8b 09 a9 52 26 d4 9b 62 59 3c 67
Round 4 :  c5 d2 d2 d3 00 f7 40 3c ed c7 53 ca 21 df 38 a7
Round 5 :  1d 0e c7 59 93 ac 95 81 db 3d 67 f0 7a d8 f0 9e
Round 6 :  11 64 51 3a 60 ae 63 ea c3 03 0c da 98 08 e5 f8
Round 7 :  2f d4 3b 2d 19 6b 70 ee 8c 67 cb 2c e9 89 60 c7
Round 8 :  7d 02 60 fe 0d 62 b0 41 ab 83 a6 2c b3 58 7b 80
Round 9 :  d4 a8 4b 5b 9e a9 02 82 21 0e 73 6c 2d 81 cb 64
Round 10 :  4e fc cf ca 5e 63 eb d6 2b 4c 29 78 8d c2 74 80
Round 11 :  9f 6d 6b 93 17 e2 4a b5 4e 91 fc 65 6a b4 cd 1c
Round 12 :  0d 1b 03 be a6 38 3a 0a a2 79 0b bc 1b ae 43 03
Round 13 :  b6 99 bd 93 03 71 c0 7a 70 38 7e 44 2c 4e 02 80
Round 14 :  52 bf 10 9c c1 be d6 7f c6 21 18 1b 32 fb 9c a8
Cipher Text:  52c1c632bfbe21fb10d6189c9c7f1ba8
```

Changed in bits in every round in shown below when we just changed one bit in the plaintext from start.



```
────────────────────Avalanche Effect────────────────────

Round 1 Changed bits: 2
Round 2 Changed bits: 14
Round 3 Changed bits: 62
Round 4 Changed bits: 58
Round 5 Changed bits: 69
Round 6 Changed bits: 65
Round 7 Changed bits: 62
Round 8 Changed bits: 60
Round 9 Changed bits: 75
Round 10 Changed bits: 72
Round 11 Changed bits: 70
Round 12 Changed bits: 61
Round 13 Changed bits: 64
Round 14 Changed bits: 73
```

o return to your computer, move the mouse pointer outside or press Ctrl+Alt.
Type here to search
12°C
8:24 pm
18/03/2024

- ## Calculating Avalanche Effect (altered bit)

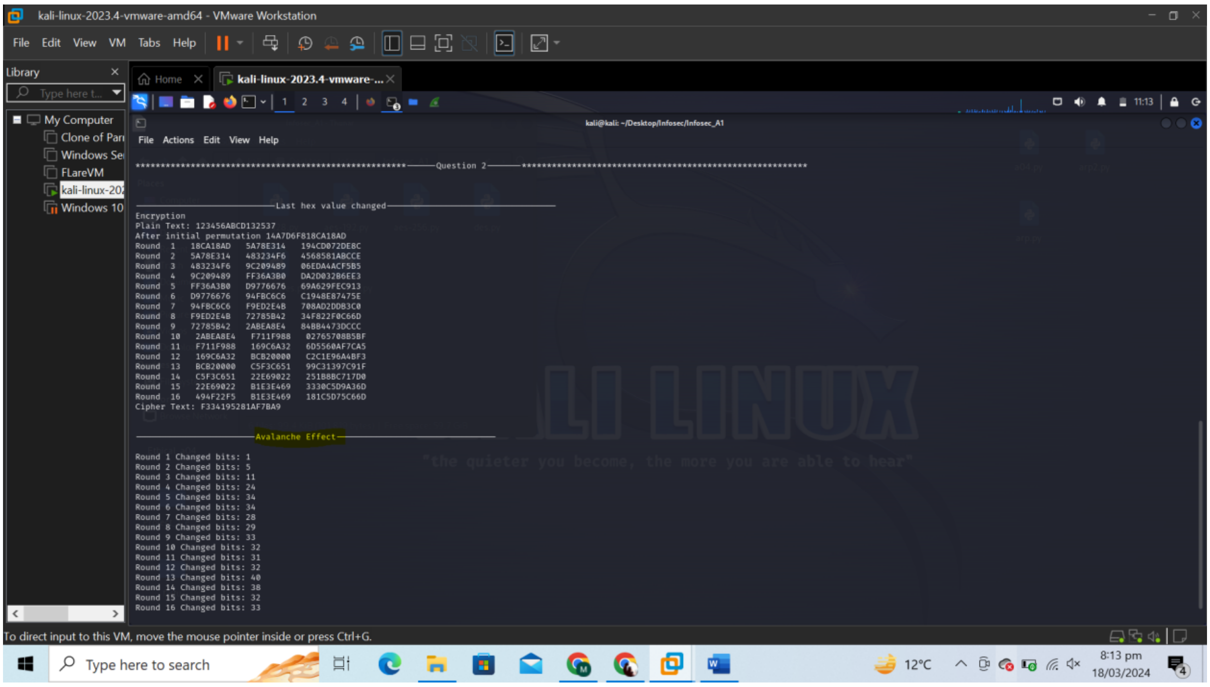
- ## DES

When we changed the bit from last of the plaintext, we got different ciphertext.

Plaintext: "123456ABCD132537".

Ciphertext: "F334195281AF7BA9".

Change in bits in every round is shown below when we change the last bit from plaintext.



```
*****************************************************———Question 2———*****************************************************

————————————————————————Last hex value changed————————————————————————
Encryption
Plain Text: 123456ABCD132537
After initial permutation 14A7D6F818CA18AD
Round  1   18CA18AD   5A78E314   194CD072DE8C
Round  2   5A78E314   483234F6   4568581ABCCE
Round  3   483234F6   9C209489   06EDA4ACF5B5
Round  4   9C209489   FF36A3B0   DA2D032B6EE3
Round  5   FF36A3B0   D9776676   69A629FEC913
Round  6   D9776676   94FBC6C6   C1948E87475E
Round  7   94FBC6C6   F9ED2E4B   708AD2DDB3C0
Round  8   F9ED2E4B   72785B42   34F822F0C66D
Round  9   72785B42   2ABEA8E4   84BB4473DCCC
Round  10   2ABEA8E4   F711F988   02765708B5BF
Round  11   F711F988   169C6A32   6D5560AF7CA5
Round  12   169C6A32   BCB20000   C2C1E96A4BF3
Round  13   BCB20000   C5F3C651   99C31397C91F
Round  14   C5F3C651   22E69022   251B8BC717D0
Round  15   22E69022   B1E3E469   3330C5D9A36D
Round  16   494F22F5   B1E3E469   181C5D75C66D
Cipher Text: F334195281AF7BA9

————————————————————————Avalanche Effect————————————————————————

Round 1 Changed bits: 1
Round 2 Changed bits: 5
Round 3 Changed bits: 11
Round 4 Changed bits: 24
Round 5 Changed bits: 34
Round 6 Changed bits: 34
Round 7 Changed bits: 28
Round 8 Changed bits: 29
Round 9 Changed bits: 33
Round 10 Changed bits: 32
Round 11 Changed bits: 31
Round 12 Changed bits: 32
Round 13 Changed bits: 40
Round 14 Changed bits: 38
Round 15 Changed bits: 32
Round 16 Changed bits: 33
```

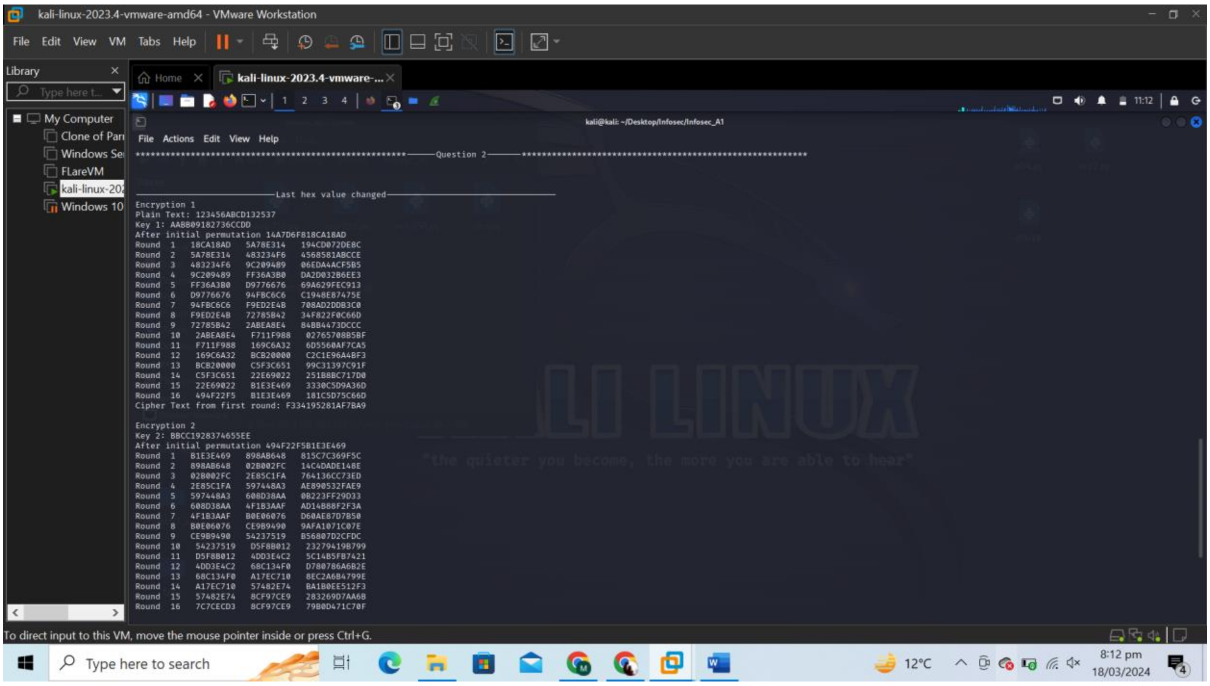
kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Clone of Parr
Windows Ser
FLareVM
kali-linux-202
Windows 10
Home
kali-linux-2023.4-vmware-...
kali@kali: ~/Desktop/Infosec/Infosec_A1
File Actions Edit View Help
"the quieter you become, the more you are able to hear"
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
12°C
8:13 pm
18/03/2024

- ## 2-DES

When we changed the bit from last of the plaintext, we got different ciphertext.

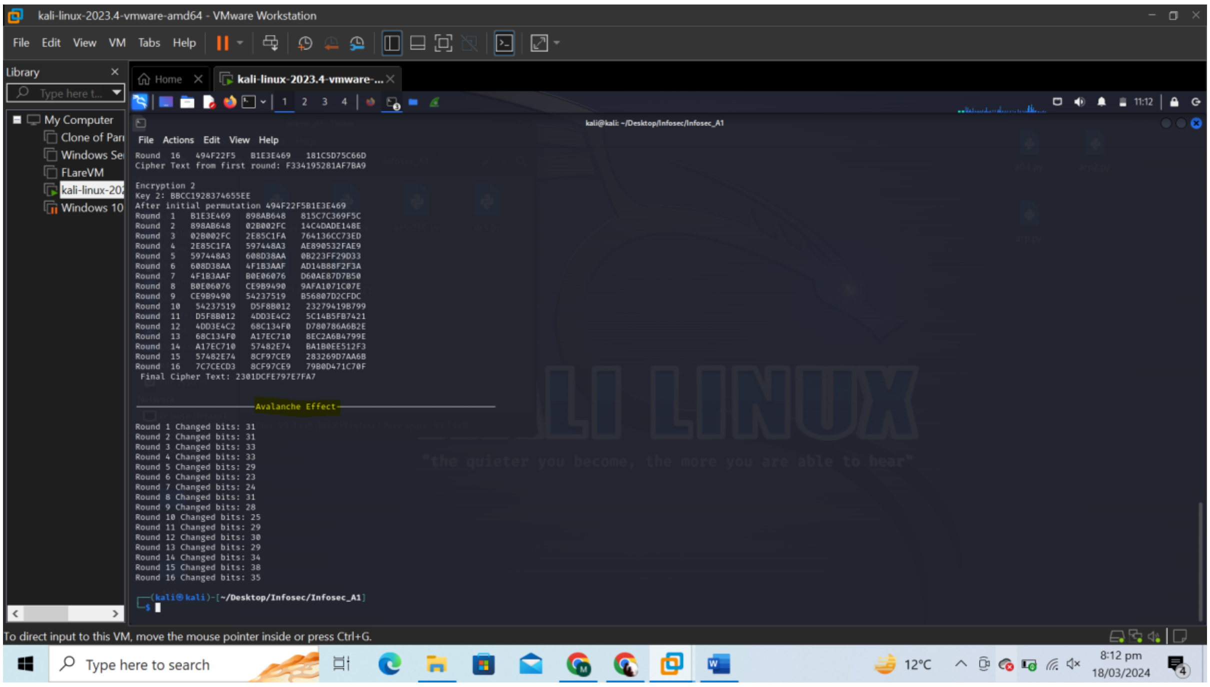
Plaintext: "123456ABCD132537".

Ciphertext: "2301DCFE797E7FA7".


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Clone of Parr
Windows Se
FLareVM
kali-linux-202
Windows 10
Home
kali-linux-2023.4-vmware-...
kali@kali: ~/Desktop/Infosec/Infosec_A1
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
12°C
8:12 pm
18/03/2024

```
*****************************************************************——Question 2——**************************************************************


——————————————————————Last hex value changed——————————————————————
Encryption 1
Plain Text: 123456ABCD132537
Key 1: AABB09182736CCDD
After initial permutation 14A7D6F818CA18AD
Round  1   18CA18AD   5A78E314   194CD072DE8C
Round  2   5A78E314   483234F6   4568581ABCCE
Round  3   483234F6   9C209489   06EDA4ACF5B5
Round  4   9C209489   FF36A3B0   DA2D032B6EE3
Round  5   FF36A3B0   D9776676   69A629FEC913
Round  6   D9776676   94FBC6C6   C1948E87475E
Round  7   94FBC6C6   F9ED2E4B   708AD2DDB3C0
Round  8   F9ED2E4B   72785B42   34F822F0C66D
Round  9   72785B42   2ABEA8E4   84BB4473DCCC
Round  10   2ABEA8E4   F711F988   02765708B5BF
Round  11   F711F988   169C6A32   6D5560AF7CA5
Round  12   169C6A32   BCB20000   C2C1E96A4BF3
Round  13   BCB20000   C5F3C651   99C31397C91F
Round  14   C5F3C651   22E69022   251B8BC717D0
Round  15   22E69022   B1E3E469   3330C5D9A36D
Round  16   494F22F5   B1E3E469   181C5D75C66D
Cipher Text from first round: F334195281AF7BA9

Encryption 2
Key 2: BBCC1928374655EE
After initial permutation 494F22F5B1E3E469
Round  1   B1E3E469   898AB648   815C7C369F5C
Round  2   898AB648   02B002FC   14C4DADE148E
Round  3   02B002FC   2E85C1FA   764136CC73ED
Round  4   2E85C1FA   597448A3   AE890532FAE9
Round  5   597448A3   608D38AA   0B223FF29D33
Round  6   608D38AA   4F1B3AAF   AD14B88F2F3A
Round  7   4F1B3AAF   B0E06076   D60AE87D7B50
Round  8   B0E06076   CE9B9490   9AFA1071C07E
Round  9   CE9B9490   54237519   B56807D2CFDC
Round  10   54237519   D5F8B012   23279419B799
Round  11   D5F8B012   4DD3E4C2   5C14B5FB7421
Round  12   4DD3E4C2   68C134F0   D780786A6B2E
Round  13   68C134F0   A17EC710   8EC2A6B4799E
Round  14   A17EC710   57482E74   BA1B0EE512F3
Round  15   57482E74   8CF97CE9   283269D7AA6B
Round  16   7C7CECD3   8CF97CE9   79B0D471C70F
```

Change in bits in every round is shown below when we change the last bit from plaintext.


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Clone of Parr
Windows Se
FLareVM
kali-linux-202
Windows 10
Home
kali-linux-2023.4-vmware-...
kali@kali: ~/Desktop/Infosec/Infosec_A1
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
12°C
8:12 pm
18/03/2024

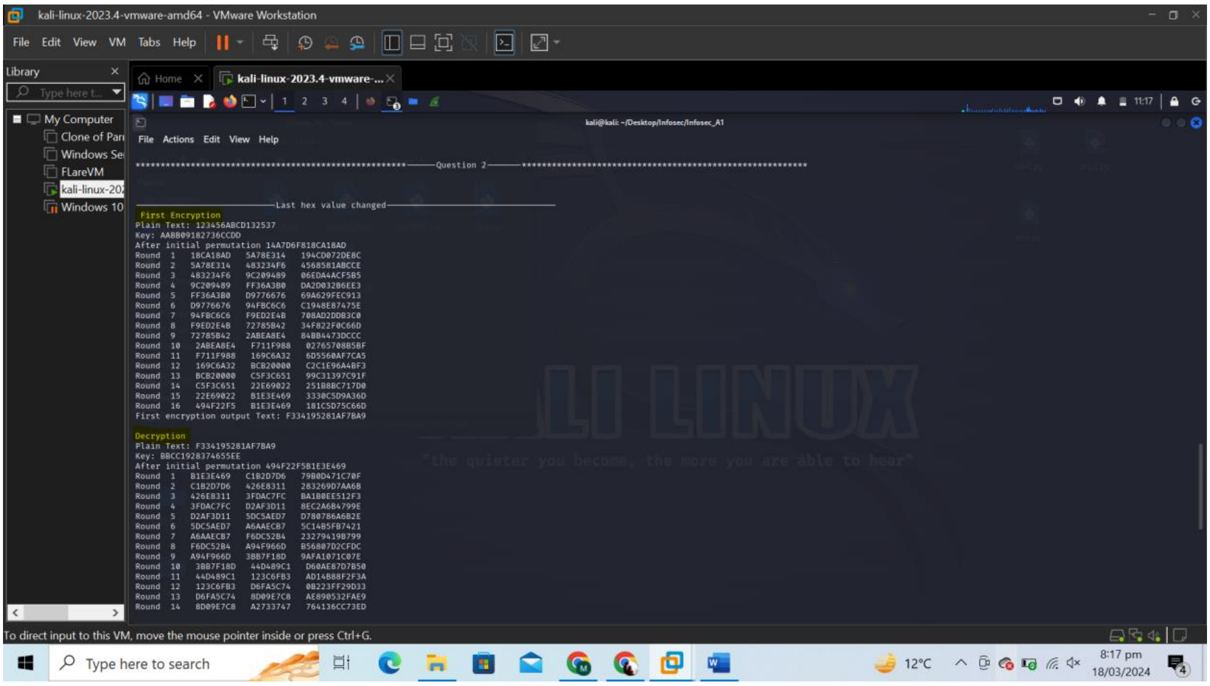
```
Round  16   494F22F5   B1E3E469   181C5D75C66D
Cipher Text from first round: F334195281AF7BA9

Encryption 2
Key 2: BBCC1928374655EE
After initial permutation 494F22F5B1E3E469
Round  1   B1E3E469   898AB648   815C7C369F5C
Round  2   898AB648   02B002FC   14C4DADE148E
Round  3   02B002FC   2E85C1FA   764136CC73ED
Round  4   2E85C1FA   597448A3   AE890532FAE9
Round  5   597448A3   608D38AA   0B223FF29D33
Round  6   608D38AA   4F1B3AAF   AD14B88F2F3A
Round  7   4F1B3AAF   B0E06076   D60AE87D7B50
Round  8   B0E06076   CE9B9490   9AFA1071C07E
Round  9   CE9B9490   54237519   B56807D2CFDC
Round  10   54237519   D5F8B012   23279419B799
Round  11   D5F8B012   4DD3E4C2   5C14B5FB7421
Round  12   4DD3E4C2   68C134F0   D780786A6B2E
Round  13   68C134F0   A17EC710   8EC2A6B4799E
Round  14   A17EC710   57482E74   BA1B0EE512F3
Round  15   57482E74   8CF97CE9   283269D7AA6B
Round  16   7C7CECD3   8CF97CE9   79B0D471C70F
 Final Cipher Text: 2301DCFE797E7FA7


——————————————————————Avalanche Effect——————————————————————————————

Round 1 Changed bits: 31
Round 2 Changed bits: 31
Round 3 Changed bits: 33
Round 4 Changed bits: 33
Round 5 Changed bits: 29
Round 6 Changed bits: 23
Round 7 Changed bits: 24
Round 8 Changed bits: 31
Round 9 Changed bits: 28
Round 10 Changed bits: 25
Round 11 Changed bits: 29
Round 12 Changed bits: 30
Round 13 Changed bits: 29
Round 14 Changed bits: 34
Round 15 Changed bits: 38
Round 16 Changed bits: 35

┌──(kali㉿kali)-[~/Desktop/Infosec/Infosec_A1]
└─$ 
```

- ## 3-DES

When we changed the bit from last of the plaintext, we got different ciphertext.

Plaintext: “123456ABCD132537”.

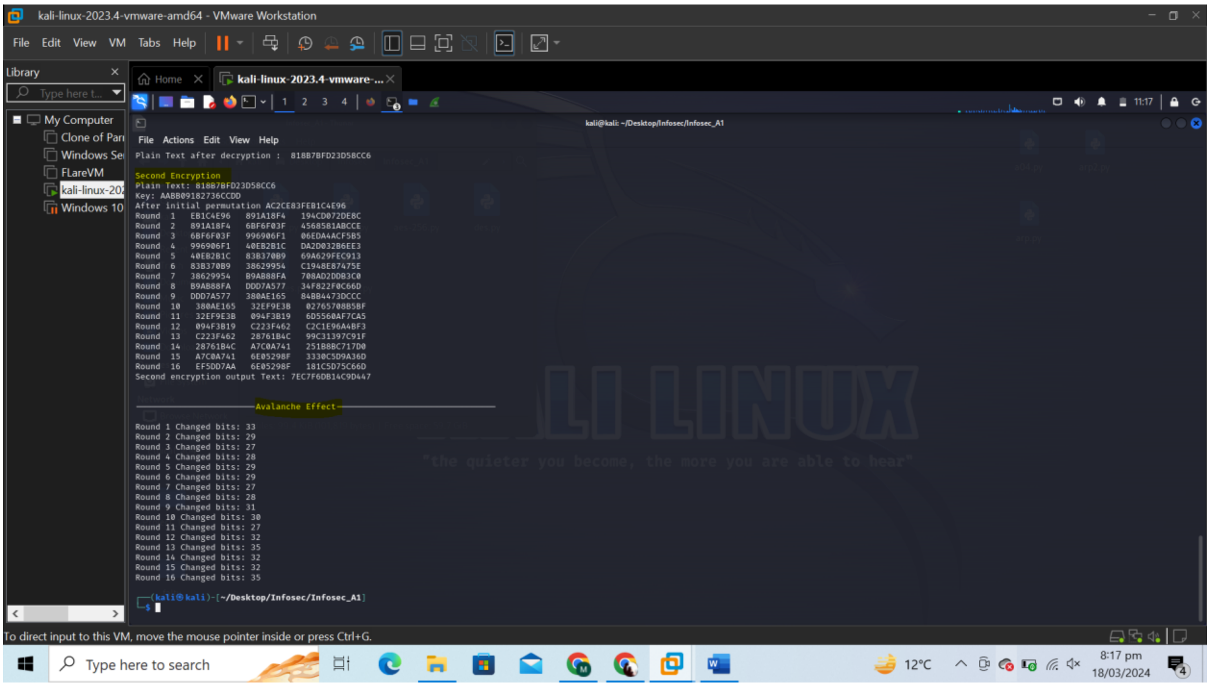
Ciphertext: “7EC7F6DB14C9D447”.


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Clone of Pari
Windows Se
FLareVM
kali-linux-202
Windows 10
Home
kali-linux-2023.4-vmware-...
kali@kali: ~/Desktop/Infosec/Infosec_A1
File Actions Edit View Help
"the quieter you become, the more you are able to hear"
Type here to search
12°C
8:17 pm
18/03/2024

```
*****************************************************——Question 2——*********************************************************

——————————————————————Last hex value changed——————————————————————
 First Encryption
Plain Text: 123456ABCD132537
Key: AABB09182736CCDD
After initial permutation 14A7D6F818CA18AD
Round  1   18CA18AD   5A78E314   194CD072DE8C
Round  2   5A78E314   483234F6   4568581ABCCE
Round  3   483234F6   9C209489   06EDA4ACF5B5
Round  4   9C209489   FF36A3B0   DA2D032B6EE3
Round  5   FF36A3B0   D9776676   69A629FEC913
Round  6   D9776676   94FBC6C6   C1948E87475E
Round  7   94FBC6C6   F9ED2E4B   708AD2DDB3C0
Round  8   F9ED2E4B   72785B42   34F822F0C66D
Round  9   72785B42   2ABEA8E4   84BB4473DCCC
Round  10   2ABEA8E4   F711F988   02765708B5BF
Round  11   F711F988   169C6A32   6D5560AF7CA5
Round  12   169C6A32   BCB20000   C2C1E96A4BF3
Round  13   BCB20000   C5F3C651   99C31397C91F
Round  14   C5F3C651   22E69022   251B8BC717D0
Round  15   22E69022   B1E3E469   3330C5D9A36D
Round  16   494F22F5   B1E3E469   181C5D75C66D
First encryption output Text: F334195281AF7BA9

Decryption
Plain Text: F334195281AF7BA9
Key: BBCC1928374655EE
After initial permutation 494F22F5B1E3E469
Round  1   B1E3E469   C1B2D7D6   79B0D471C70F
Round  2   C1B2D7D6   426E8311   283269D7AA6B
Round  3   426E8311   3FDAC7FC   BA1B0EE512F3
Round  4   3FDAC7FC   D2AF3D11   8EC2A6B4799E
Round  5   D2AF3D11   5DC5AED7   D780786A6B2E
Round  6   5DC5AED7   A6AAECB7   5C14B5FB7421
Round  7   A6AAECB7   F6DC52B4   23279419B799
Round  8   F6DC52B4   A94F966D   B56807D2CFDC
Round  9   A94F966D   3BB7F18D   9AFA1071C07E
Round  10   3BB7F18D   44D489C1   D60AE87D7B50
Round  11   44D489C1   123C6FB3   AD14B88F2F3A
Round  12   123C6FB3   D6FA5C74   0B223FF29D33
Round  13   D6FA5C74   8D09E7C8   AE890532FAE9
Round  14   8D09E7C8   A2733747   764136CC73ED
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Change in bits (avalanche effect) in every round is shown below when we change the last bit from plaintext.



```
Plain Text after decryption :  818B7BFD23D58CC6

Second Encryption
Plain Text: 818B7BFD23D58CC6
Key: AABB09182736CCDD
After initial permutation AC2CE83FEB1C4E96
Round  1   EB1C4E96   891A18F4   194CD072DE8C
Round  2   891A18F4   6BF6F03F   4568581ABCCE
Round  3   6BF6F03F   996906F1   06EDA4ACF5B5
Round  4   996906F1   40EB2B1C   DA2D032B6EE3
Round  5   40EB2B1C   83B370B9   69A629FEC913
Round  6   83B370B9   38629954   C1948E87475E
Round  7   38629954   B9AB88FA   708AD2DDB3C0
Round  8   B9AB88FA   DDD7A577   34F822F0C66D
Round  9   DDD7A577   380AE165   84BB4473DCCC
Round  10   380AE165   32EF9E3B   02765708B5BF
Round  11   32EF9E3B   094F3B19   6D5560AF7CA5
Round  12   094F3B19   C223F462   C2C1E96A4BF3
Round  13   C223F462   28761B4C   99C31397C91F
Round  14   28761B4C   A7C0A741   251B8BC717D0
Round  15   A7C0A741   6E05298F   3330C5D9A36D
Round  16   EF5DD7AA   6E05298F   181C5D75C66D
Second encryption output Text: 7EC7F6DB14C9D447

─────────────────────Avalanche Effect─────────────────────

Round 1 Changed bits: 33
Round 2 Changed bits: 29
Round 3 Changed bits: 27
Round 4 Changed bits: 28
Round 5 Changed bits: 29
Round 6 Changed bits: 29
Round 7 Changed bits: 27
Round 8 Changed bits: 28
Round 9 Changed bits: 31
Round 10 Changed bits: 30
Round 11 Changed bits: 27
Round 12 Changed bits: 32
Round 13 Changed bits: 35
Round 14 Changed bits: 32
Round 15 Changed bits: 32
Round 16 Changed bits: 35

┌──(kali㉿kali)-[~/Desktop/Infosec/Infosec_A1]
└─$ 
```

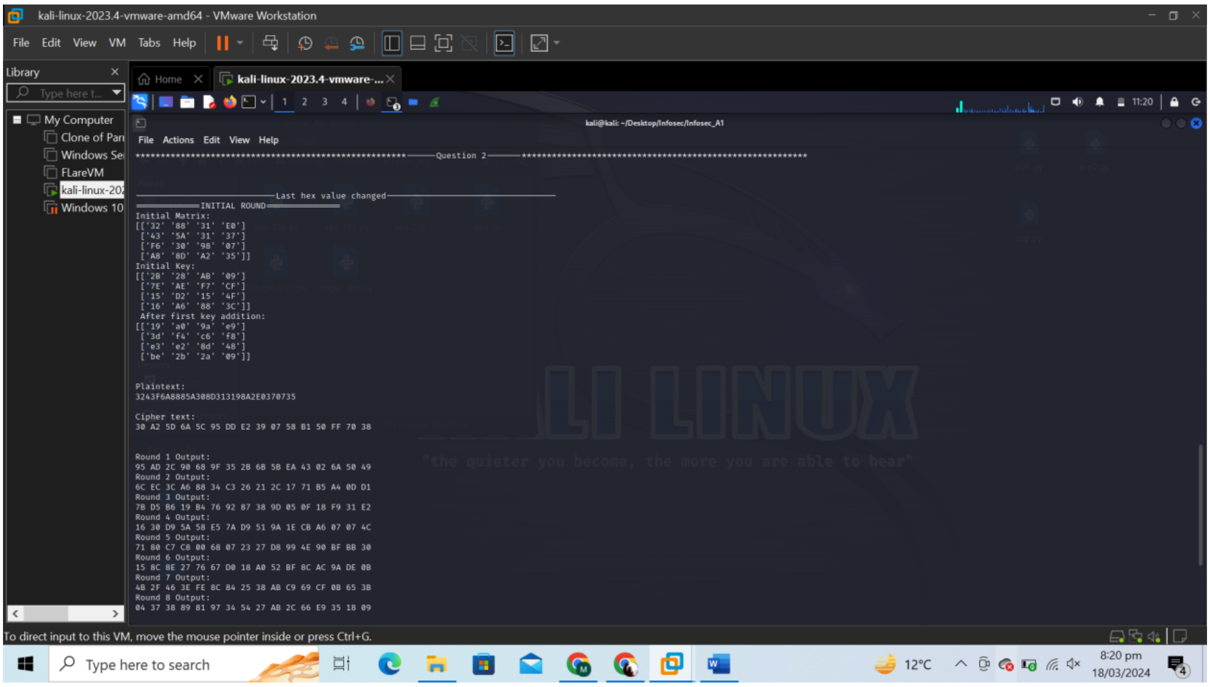
kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Clone of Parr
Windows Se
FLareVM
kali-linux-202
Windows 10
Home
kali-linux-2023.4-vmware-...
kali@kali: ~/Desktop/Infosec/Infosec_A1
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
12°C
8:17 pm
18/03/2024

- ## AES-128

When we changed the bit from last of the plaintext, we got different ciphertext.

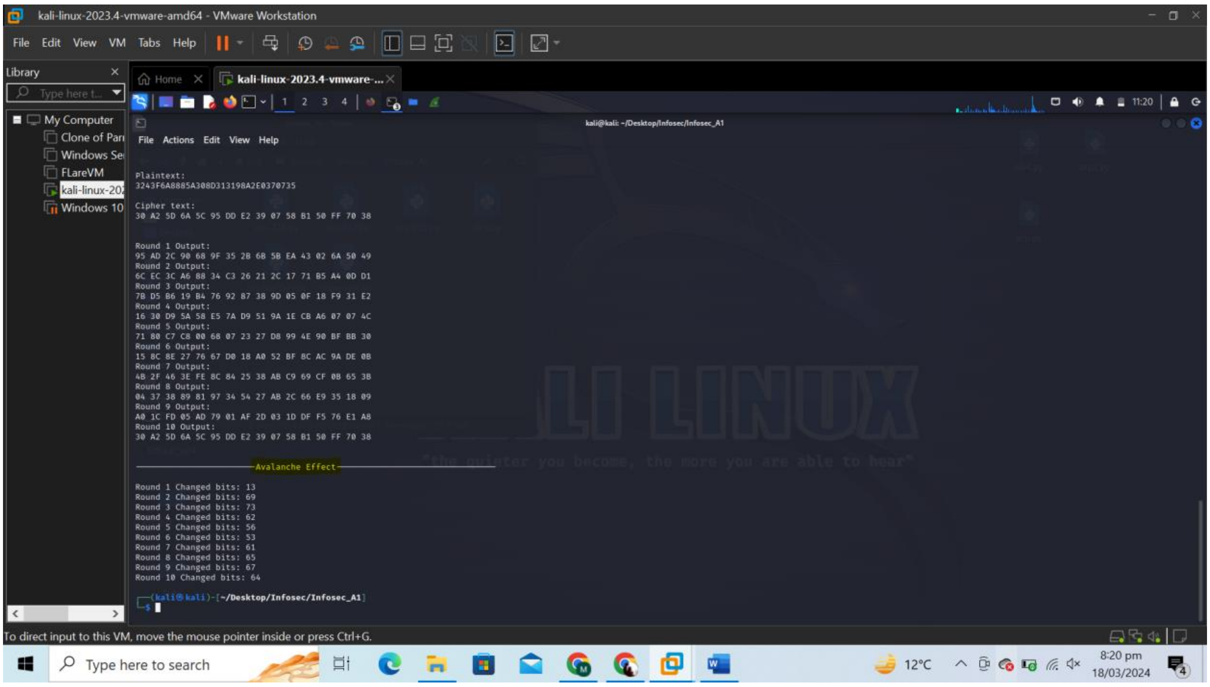
Plaintext: “3243F6A8885A308D313198A2E0370735”.

Ciphertext: “30A25D6A5C95DDE2390758B150FF7038”.



```
****************************************************————Question 2————*******************************************************

——————————————————————Last hex value changed——————————————————————
═══════════INITIAL ROUND═══════════
Initial Matrix:
[['32' '88' '31' 'E0']
 ['43' '5A' '31' '37']
 ['F6' '30' '98' '07']
 ['A8' '8D' 'A2' '35']]
Initial Key:
[['2B' '28' 'AB' '09']
 ['7E' 'AE' 'F7' 'CF']
 ['15' 'D2' '15' '4F']
 ['16' 'A6' '88' '3C']]
 After first key addition:
[['19' 'a0' '9a' 'e9']
 ['3d' 'f4' 'c6' 'f8']
 ['e3' 'e2' '8d' '48']
 ['be' '2b' '2a' '09']]


Plaintext:
3243F6A8885A308D313198A2E0370735

Cipher text:
30 A2 5D 6A 5C 95 DD E2 39 07 58 B1 50 FF 70 38


Round 1 Output:
95 AD 2C 90 68 9F 35 2B 6B 5B EA 43 02 6A 50 49
Round 2 Output:
6C EC 3C A6 88 34 C3 26 21 2C 17 71 B5 A4 0D D1
Round 3 Output:
7B D5 B6 19 B4 76 92 87 38 9D 05 0F 18 F9 31 E2
Round 4 Output:
16 30 D9 5A 58 E5 7A D9 51 9A 1E CB A6 07 07 4C
Round 5 Output:
71 80 C7 C8 00 68 07 23 27 D8 99 4E 90 BF BB 30
Round 6 Output:
15 8C 8E 27 76 67 D0 18 A0 52 BF 8C AC 9A DE 0B
Round 7 Output:
4B 2F 46 3E FE 8C 84 25 38 AB C9 69 CF 0B 65 3B
Round 8 Output:
04 37 38 89 81 97 34 54 27 AB 2C 66 E9 35 18 09
```

Change in bits (avalanche effect) in every round is shown below when we change the last bit from plaintext.



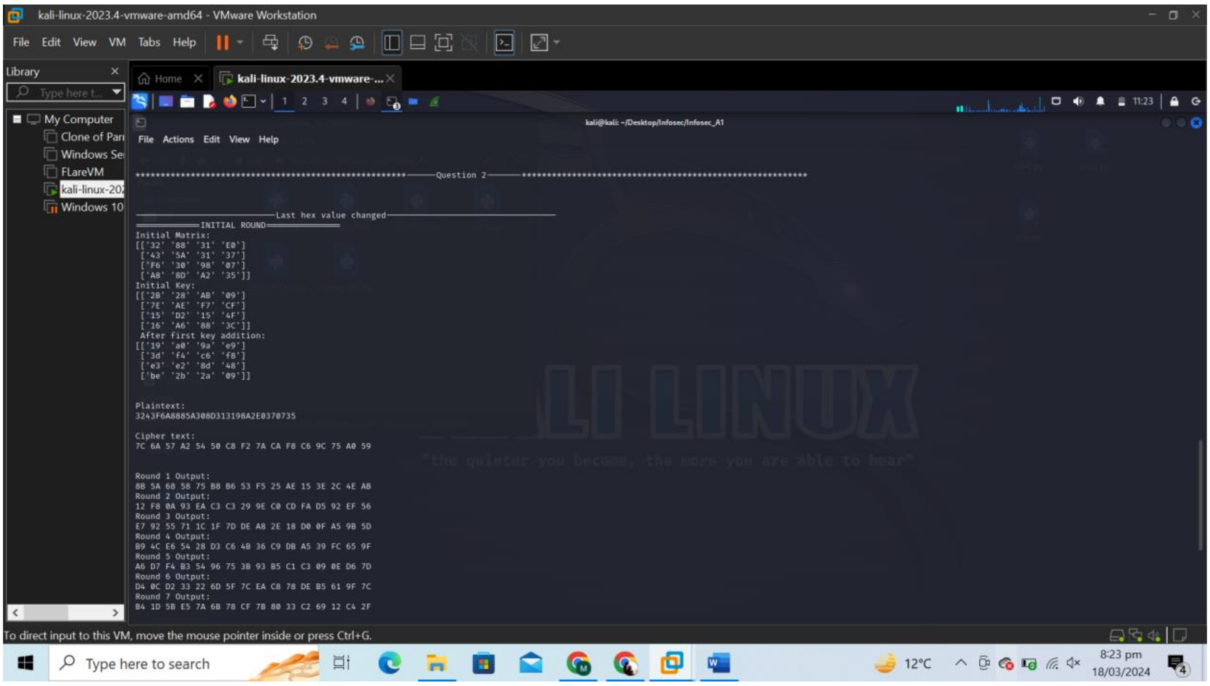
```
Plaintext:
3243F6A8885A308D313198A2E0370735

Cipher text:
30 A2 5D 6A 5C 95 DD E2 39 07 58 B1 50 FF 70 38


Round 1 Output:
95 AD 2C 90 68 9F 35 2B 6B 5B EA 43 02 6A 50 49
Round 2 Output:
6C EC 3C A6 88 34 C3 26 21 2C 17 71 B5 A4 0D D1
Round 3 Output:
7B D5 B6 19 B4 76 92 87 38 9D 05 0F 18 F9 31 E2
Round 4 Output:
16 30 D9 5A 58 E5 7A D9 51 9A 1E CB A6 07 07 4C
Round 5 Output:
71 80 C7 C8 00 68 07 23 27 D8 99 4E 90 BF BB 30
Round 6 Output:
15 8C 8E 27 76 67 D0 18 A0 52 BF 8C AC 9A DE 0B
Round 7 Output:
4B 2F 46 3E FE 8C 84 25 38 AB C9 69 CF 0B 65 3B
Round 8 Output:
04 37 38 89 81 97 34 54 27 AB 2C 66 E9 35 18 09
Round 9 Output:
A0 1C FD 05 AD 79 01 AF 2D 03 1D DF F5 76 E1 A8
Round 10 Output:
30 A2 5D 6A 5C 95 DD E2 39 07 58 B1 50 FF 70 38


————————————————————————Avalanche Effect————————————————————————

Round 1 Changed bits: 13
Round 2 Changed bits: 69
Round 3 Changed bits: 73
Round 4 Changed bits: 62
Round 5 Changed bits: 56
Round 6 Changed bits: 53
Round 7 Changed bits: 61
Round 8 Changed bits: 65
Round 9 Changed bits: 67
Round 10 Changed bits: 64

┌──(kali㉿kali)-[~/Desktop/Infosec/Infosec_A1]
└─$ 
```

- ## AES-192

When we changed the bit from last of the plaintext, we got different ciphertext.

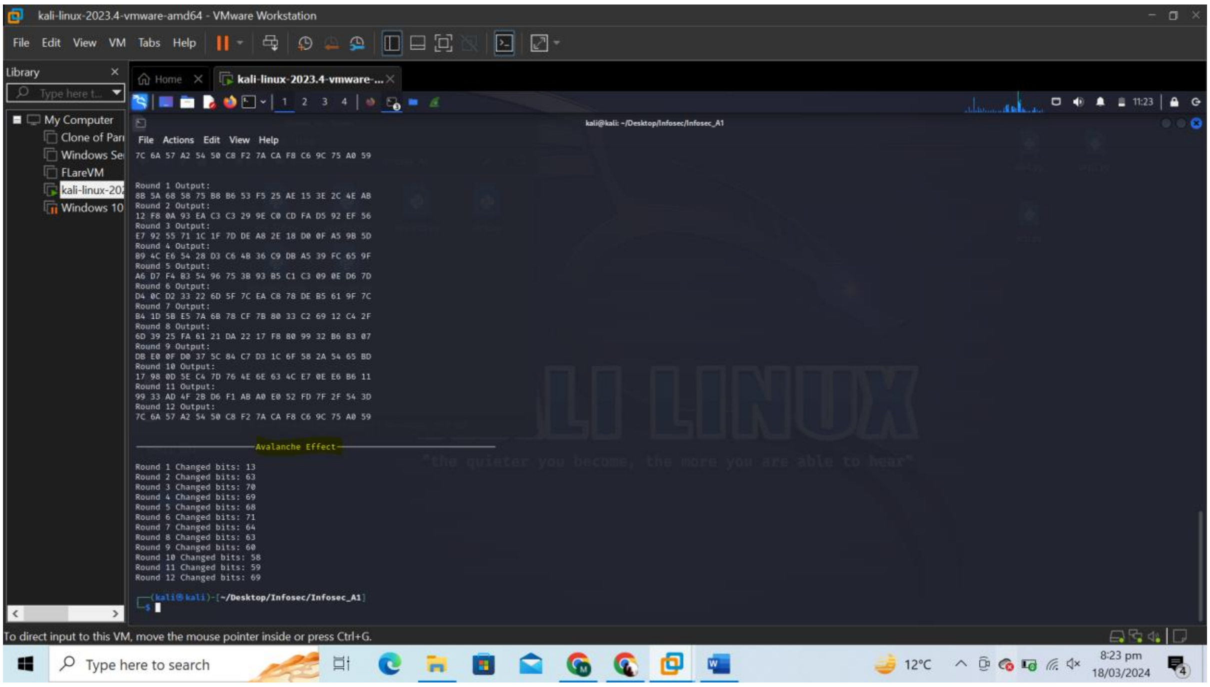
Plaintext: "3243F6A8885A308D313198A2E0370735".

Ciphertext: "7C6A57A25450C8F27ACAF8C69C75A059".


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Clone of Pari
Windows Se
FLareVM
kali-linux-202
Windows 10
Home
kali-linux-2023.4-vmware-...
kali@kali: ~/Desktop/Infosec/Infosec_A1
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
12°C
8:23 pm
18/03/2024

```
****************************************************——Question 2——*******************************************************

————————————————————————Last hex value changed——————————————————————————
═════════════INITIAL ROUND═══════════════
Initial Matrix:
[['32' '88' '31' 'E0']
 ['43' '5A' '31' '37']
 ['F6' '30' '98' '07']
 ['A8' '8D' 'A2' '35']]
Initial Key:
[['2B' '28' 'AB' '09']
 ['7E' 'AE' 'F7' 'CF']
 ['15' 'D2' '15' '4F']
 ['16' 'A6' '88' '3C']]
 After first key addition:
[['19' 'a0' '9a' 'e9']
 ['3d' 'f4' 'c6' 'f8']
 ['e3' 'e2' '8d' '48']
 ['be' '2b' '2a' '09']]


Plaintext:
3243F6A8885A308D313198A2E0370735

Cipher text:
7C 6A 57 A2 54 50 C8 F2 7A CA F8 C6 9C 75 A0 59


Round 1 Output:
8B 5A 68 58 75 B8 B6 53 F5 25 AE 15 3E 2C 4E AB
Round 2 Output:
12 F8 0A 93 EA C3 C3 29 9E C0 CD FA D5 92 EF 56
Round 3 Output:
E7 92 55 71 1C 1F 7D DE A8 2E 18 D0 0F A5 9B 5D
Round 4 Output:
B9 4C E6 54 28 D3 C6 4B 36 C9 DB A5 39 FC 65 9F
Round 5 Output:
A6 D7 F4 B3 54 96 75 3B 93 B5 C1 C3 09 0E D6 7D
Round 6 Output:
D4 0C D2 33 22 6D 5F 7C EA C8 78 DE B5 61 9F 7C
Round 7 Output:
B4 1D 5B E5 7A 6B 78 CF 7B 80 33 C2 69 12 C4 2F
```

Change in bits (avalanche effect) in every round is shown below when we change the last bit from plaintext.



kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Clone of Parr
Windows Se
FLareVM
kali-linux-202
Windows 10
Home
kali-linux-2023.4-vmware-...
kali@kali: ~/Desktop/Infosec/Infosec_A1
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
12°C
8:23 pm
18/03/2024

```
7C 6A 57 A2 54 50 C8 F2 7A CA F8 C6 9C 75 A0 59


Round 1 Output:
8B 5A 68 58 75 B8 B6 53 F5 25 AE 15 3E 2C 4E AB
Round 2 Output:
12 F8 0A 93 EA C3 C3 29 9E C0 CD FA D5 92 EF 56
Round 3 Output:
E7 92 55 71 1C 1F 7D DE A8 2E 18 D0 0F A5 9B 5D
Round 4 Output:
B9 4C E6 54 28 D3 C6 48 36 C9 DB A5 39 FC 65 9F
Round 5 Output:
A6 D7 F4 B3 54 96 75 3B 93 B5 C1 C3 09 0E D6 7D
Round 6 Output:
D4 0C D2 33 22 6D 5F 7C EA C8 78 DE B5 61 9F 7C
Round 7 Output:
B4 1D 5B E5 7A 6B 78 CF 7B 80 33 C2 69 12 C4 2F
Round 8 Output:
6D 39 25 FA 61 21 DA 22 17 F8 80 99 32 B6 83 07
Round 9 Output:
DB E0 0F D0 37 5C 84 C7 D3 1C 6F 58 2A 54 65 BD
Round 10 Output:
17 98 0D 5E C4 7D 76 4E 6E 63 4C E7 0E E6 B6 11
Round 11 Output:
99 33 AD 4F 2B D6 F1 AB A0 E0 52 FD 7F 2F 54 3D
Round 12 Output:
7C 6A 57 A2 54 50 C8 F2 7A CA F8 C6 9C 75 A0 59


────────────────────Avalanche Effect────────────────────

Round 1 Changed bits: 13
Round 2 Changed bits: 63
Round 3 Changed bits: 70
Round 4 Changed bits: 69
Round 5 Changed bits: 68
Round 6 Changed bits: 71
Round 7 Changed bits: 64
Round 8 Changed bits: 63
Round 9 Changed bits: 60
Round 10 Changed bits: 58
Round 11 Changed bits: 59
Round 12 Changed bits: 69

┌──(kali㉿kali)-[~/Desktop/Infosec/Infosec_A1]
└─$ 
```

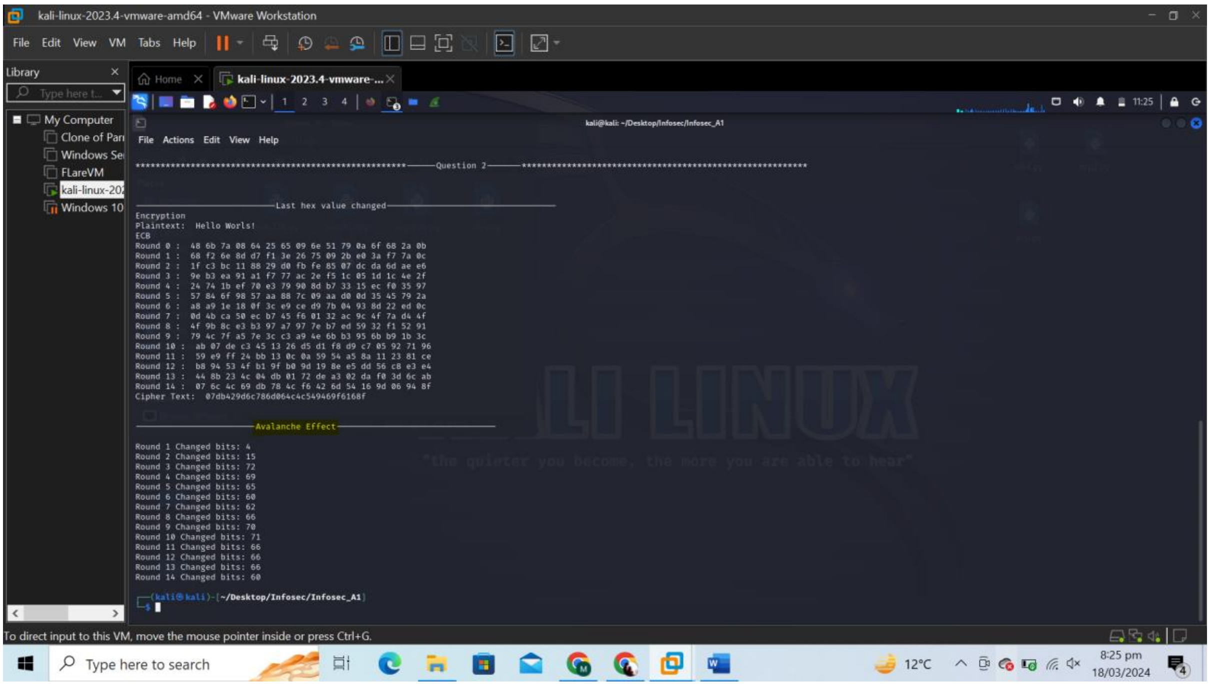
- **AES-256**

When we changed the bit from last of the plaintext, we got different ciphertext.

Plaintext: "Hello Worls".

Ciphertext: "07db429d6c786d064c4c549469f6168f".

Change in bits (avalanche effect) in every round is shown below when we change the last bit from plaintext.


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Clone of Pari
Windows Se
FLareVM
kali-linux-202
Windows 10
Home
kali-linux-2023.4-vmware-...
kali@kali: ~/Desktop/Infosec/Infosec_A1
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
12°C
8:25 pm
18/03/2024

```
**************************************************——Question 2——*******************************************************

————————————————————————————Last hex value changed————————————————————————————
Encryption
Plaintext:  Hello Worls!
ECB
Round 0 :  48 6b 7a 08 64 25 65 09 6e 51 79 0a 6f 68 2a 0b
Round 1 :  68 f2 6e 8d d7 f1 3e 26 75 09 2b e0 3a f7 7a 0c
Round 2 :  1f c3 bc 11 88 29 d0 fb fe 85 07 dc da 6d ae e6
Round 3 :  9e b3 ea 91 a1 f7 77 ac 2e f5 1c 05 1d 1c 4e 2f
Round 4 :  24 74 1b ef 70 e3 79 90 8d b7 33 15 ec f0 35 97
Round 5 :  57 84 6f 98 57 aa 88 7c 09 aa d0 0d 35 45 79 2a
Round 6 :  a8 a9 1e 18 0f 3c e9 ce d9 7b 04 93 8d 22 ed 0c
Round 7 :  0d 4b ca 50 ec b7 45 f6 01 32 ac 9c 4f 7a d4 4f
Round 8 :  4f 9b 8c e3 b3 97 a7 97 7e b7 ed 59 32 f1 52 91
Round 9 :  79 4c 7f a5 7e 3c c3 a9 4e 6b b3 95 6b b9 1b 3c
Round 10 :  ab 07 de c3 45 13 26 d5 d1 f8 d9 c7 05 92 71 96
Round 11 :  59 e9 ff 24 bb 13 0c 0a 59 54 a5 8a 11 23 81 ce
Round 12 :  b8 94 53 4f b1 9f b0 9d 19 8e e5 dd 56 c8 e3 e4
Round 13 :  44 8b 23 4c 04 db 01 72 de a3 02 da f0 3d 6c ab
Round 14 :  07 6c 4c 69 db 78 4c f6 42 6d 54 16 9d 06 94 8f
Cipher Text:  07db429d6c786d064c4c549469f6168f

——————————————————————Avalanche Effect——————————————————————

Round 1 Changed bits: 4
Round 2 Changed bits: 15
Round 3 Changed bits: 72
Round 4 Changed bits: 69
Round 5 Changed bits: 65
Round 6 Changed bits: 60
Round 7 Changed bits: 62
Round 8 Changed bits: 66
Round 9 Changed bits: 70
Round 10 Changed bits: 71
Round 11 Changed bits: 66
Round 12 Changed bits: 66
Round 13 Changed bits: 66
Round 14 Changed bits: 60

┌──(kali㉿kali)-[~/Desktop/Infosec/Infosec_A1]
└─$ 
```

- ## Discussing statistics

  - ### DES

    In DES, when we changed first bit from plaintext avalanche effect is 29 but when we changed bit from last in the plaintext text avalanche effect is 33.

  - ### 2-DES

    In Double DES, when we changed first bit from plaintext avalanche effect is 39 but when we changed bit from last in the plaintext text avalanche effect is 35.

  - ### 3-DES

    In Triple DES, when we changed first bit from plaintext avalanche effect is 31 but when we changed bit from last in the plaintext text avalanche effect is 35.

  - ### AES-128

    In AES-128, when we changed first bit from plaintext avalanche effect is 60 but when we changed bit from last in the plaintext text avalanche effect is 64.

- **AES-192**

  In AES-192, when we changed first bit from plaintext avalanche effect is 66 but when we changed bit from last in the plaintext text avalanche effect is 69.

- **AES-256**

  In AES-256, when we changed first bit from plaintext avalanche effect is 73 but when we changed bit from last in the plaintext text avalanche effect is 60.

The statistics indicate the Avalanche Effect for each encryption algorithm when altering the position of a single bit in the plaintext.

- For DES, both single and double variations, the avalanche effect seems relatively consistent, with variations between 29 and 39. However, for Triple DES, there's a slight increase in the avalanche effect, ranging from 31 to 35, indicating a stronger effect.

- AES encryption shows a more pronounced difference in the avalanche effect across key lengths. AES-128 exhibits a lower avalanche effect compared to AES-192 and AES-256. AES-192 and AES-256 demonstrate higher avalanche effects, with AES-256 having the highest. Interestingly, the effect of changing the position of the altered bit differs between AES-192 and AES-256, with AES-192 showing a consistent increase, while AES-256 shows a decrease when altering the last bit.

These statistics underscore the importance of considering the avalanche effect when assessing the security and cryptographic strength of encryption algorithms. It's evident that key length and algorithm design significantly influence the magnitude of the avalanche effect, with longer keys generally resulting in stronger avalanche effects. Additionally, the position of the altered bit can also impact the degree of the effect, although with varying outcomes depending on the algorithm. These insights are crucial for making informed decisions regarding algorithm selection and ensuring robust encryption practices.

• Summary

In this assignment, the Avalanche Effect is assessed for several encryption methods, including DES, 2-DES, 3-DES, AES-128, AES-192, and AES-256. Through examining the subtle differences between input plaintext and output ciphertext, we attempted to evaluate the cryptographic strength of each algorithm. We also explored whether the avalanche effect's strength is affected by changing the position of a single bit. Our goal is to compare and measure the avalanche effect amongst different algorithms using coding simulations and analysis to reveal more about their security features. Finally, we talked about the results and provide some insights about algorithmic preferences and cryptographic implications.

References

1. ChatGPT
2. https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/
3. https://gist.github.com/definito/b682949741337896718b5d6e3fe95fc8
4. https://github.com/Joshua-Riek/AES/blob/master/aes.py

THE END......