Experiment no. 4

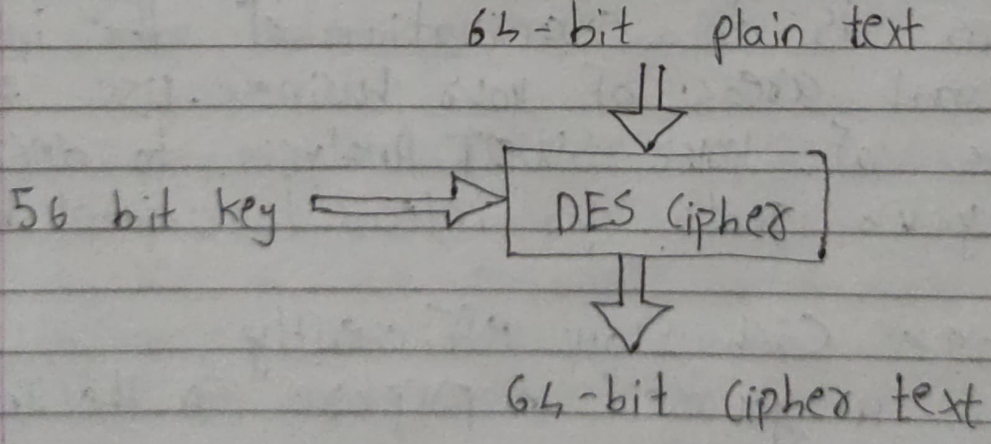
Aim - To Encrypt long messages using Various nodes of operating using AES or DES

Theory -

Data Encrypting Standard (DES)

DES is a symmetric key algorithm for encryption of digital data. Although, its shoot length of 56 bits makes it too insecure for applications, it has been highly influential in advancement of cryptography.

DES is a block Cipher & Encrypts data in blocks of size 64 bit each; means 64 bits of plain text goes as input to DES which produces 64 bit of cipher text. The same algorithm & key are used for encryption & decryption with minor differences. key length is 56 bits.



Advanced Encryption Standard (AES)

AES was developed by NIST (National institute of standards & Technology) in 1977. It was developed For replacing DES which was slow and Vulnerable to Various attacks.

Characteristics

1. AES has three lengths which are 128, 192, 256 bits.
2. It is Flexible & has implementation For both Softwore & harduare.
3. It provides high security & can prevent many attacks
4. It consists of 10 rounds of processing For 128 bits keys.

Advantages

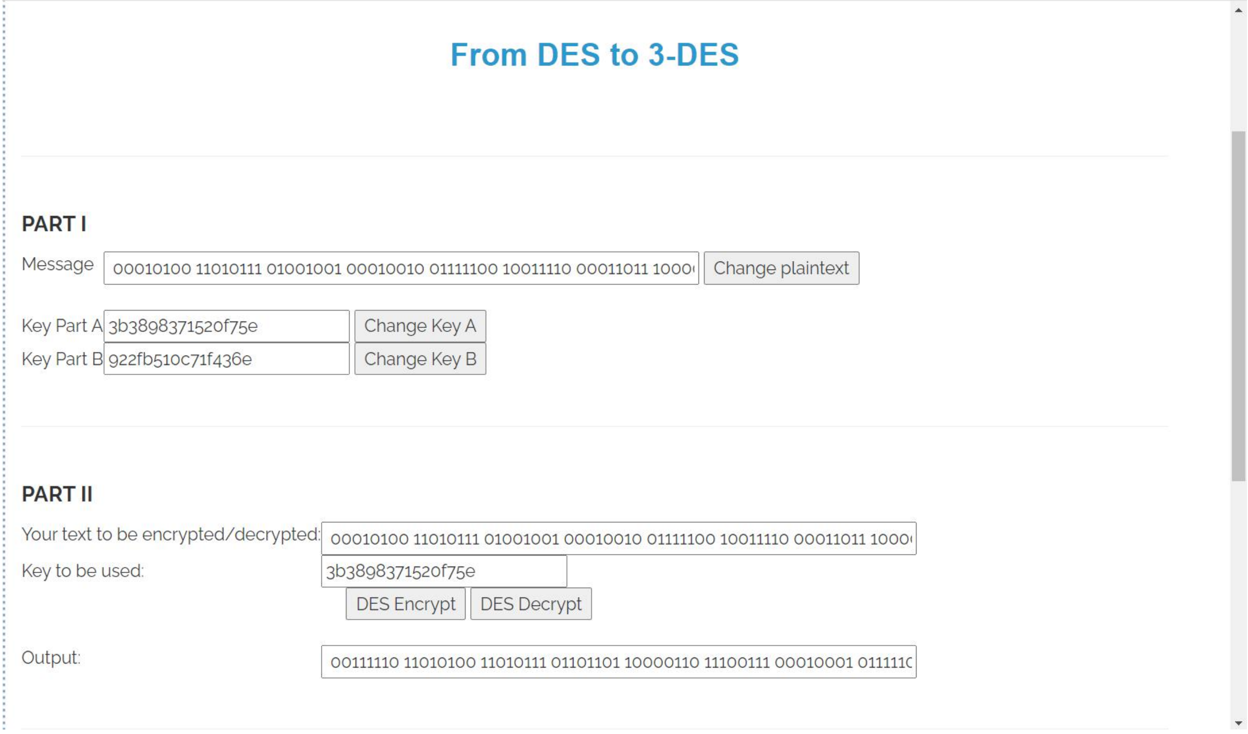
1. It provides high security to the users.
2. It is a very robust algorithm
3. It provides one of the best open sources For Encryption

Disadvantages.

1. It requires many rounds For encryption.
2. It is hard to implement on Software
3. It needs much processing at different stages.
4. It is difficult to implement when performance has to be considered.

DES

DES Encrypt Using Key A



From DES to 3-DES

PART I

Message: 00010100 11010111 01001001 00010010 01111100 10011110 00011011 1000

Key Part A: 3b3898371520f75e

Key Part B: 922fb510c71f436e

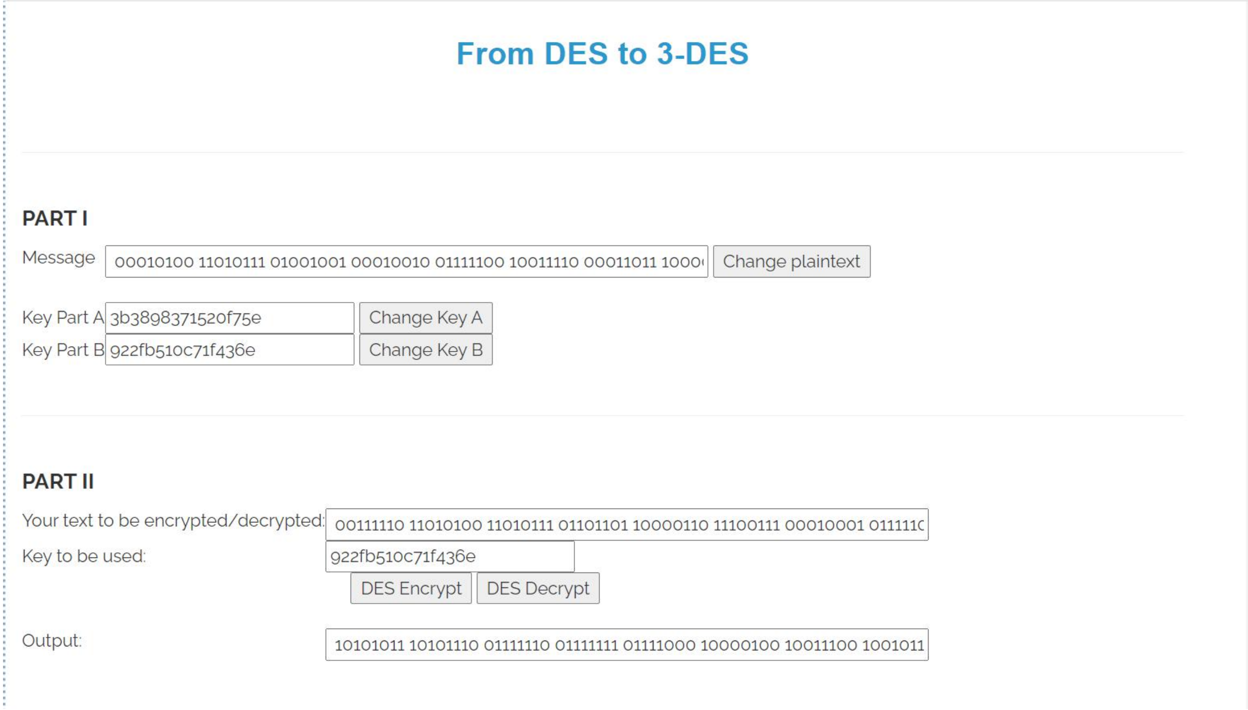
PART II

Your text to be encrypted/decrypted: 00010100 11010111 01001001 00010010 01111100 10011110 00011011 1000

Key to be used: 3b3898371520f75e

Output: 00111110 11010100 11010111 01101101 10000110 11100111 00010001 011111

DES Decrypt Using Key B



From DES to 3-DES

PART I

Message: 00010100 11010111 01001001 00010010 01111100 10011110 00011011 1000

Key Part A: 3b3898371520f75e

Key Part B: 922fb510c71f436e

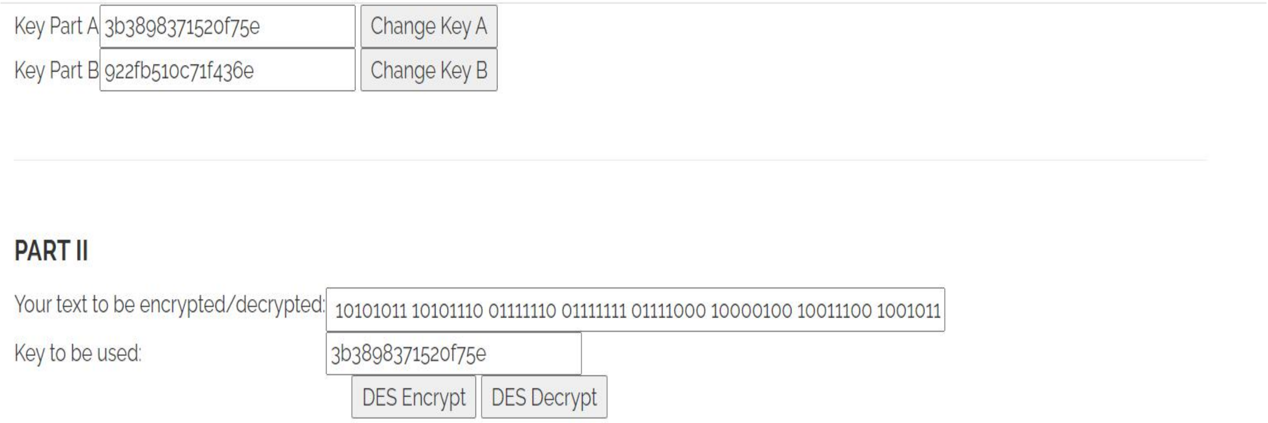
PART II

Your text to be encrypted/decrypted: 00111110 11010100 11010111 01101101 10000110 11100111 00010001 011111

Key to be used: 922fb510c71f436e

Output: 10101011 10101110 01111110 01111111 01111000 10000100 10011100 1001011

DES Encrypt Using Key A



Key Part A 3b3898371520f75e

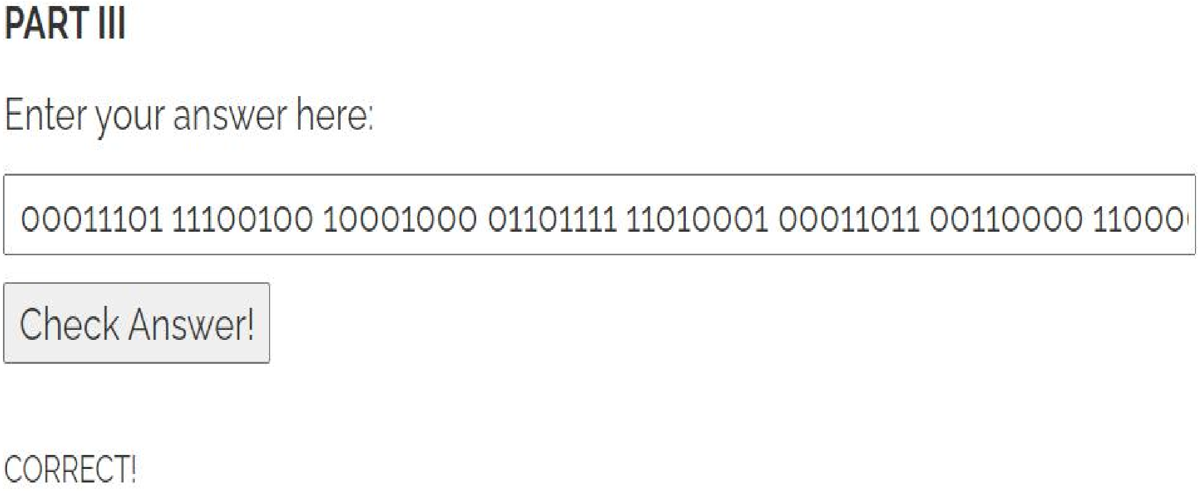
Key Part B 922fb510c71f436e

PART II

Your text to be encrypted/decrypted: 10101011 10101110 01111110 01111111 01111000 10000100 10011100 1001011

Key to be used: 3b3898371520f75e

RESULT



PART III

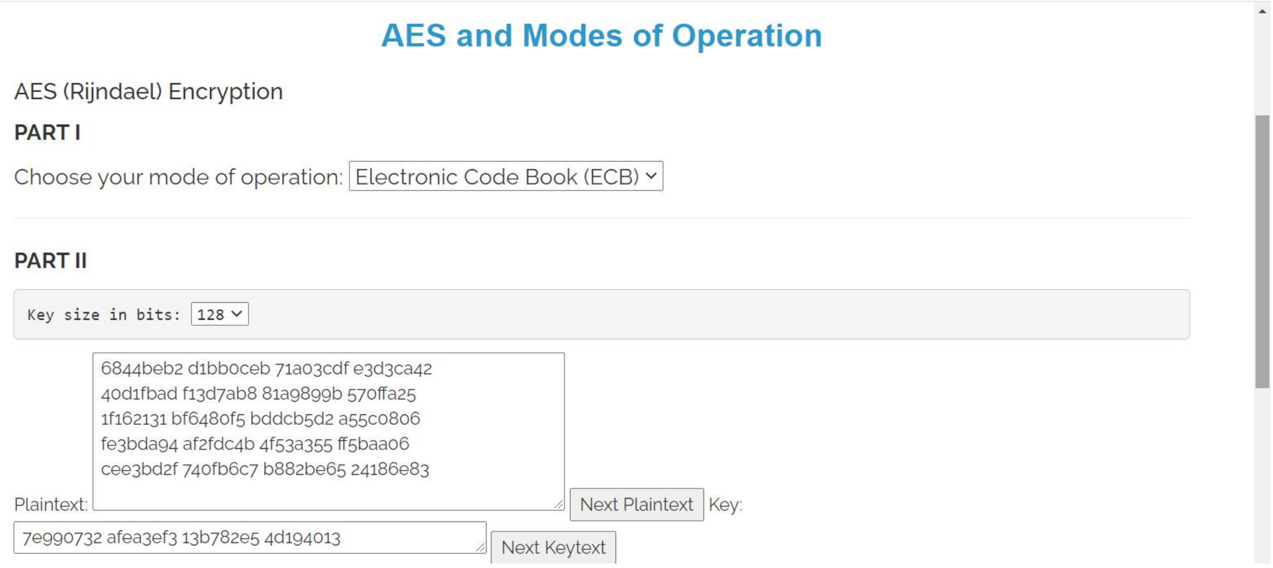
Enter your answer here:

00011101 11100100 10001000 01101111 11010001 00011011 00110000 11000

CORRECT!

AES

ELECTRONIC CODE BOOK (ECB)



AES and Modes of Operation

AES (Rijndael) Encryption

PART I

Choose your mode of operation: Electronic Code Book (ECB)

PART II

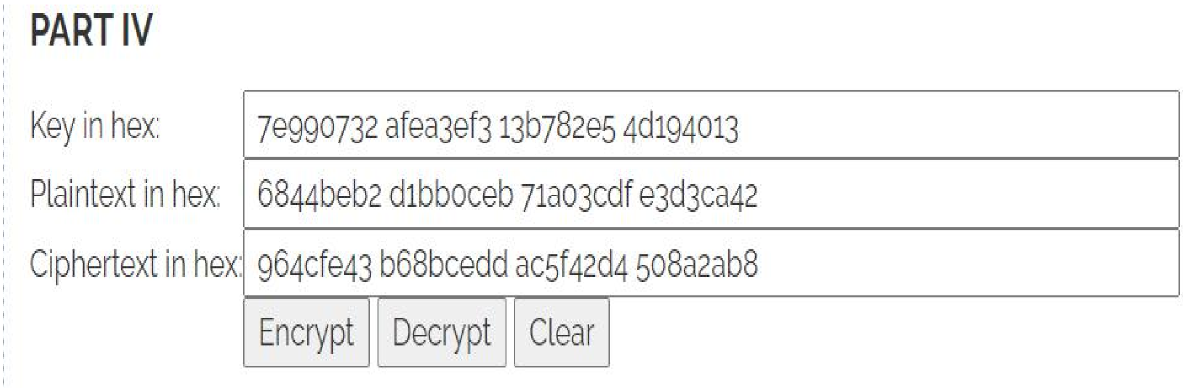
Key size in bits: 128

Plaintext:

```
6844beb2 d1bb0ceb 71a03cdf e3d3ca42
40d1fbad f13d7ab8 81a9899b 570ffa25
1f162131 bf6480f5 bddcb5d2 a55c0806
fe3bda94 af2fdc4b 4f53a355 ff5baa06
cee3bd2f 740fb6c7 b882be65 24186e83
```

Key: 7e990732 afea3ef3 13b782e5 4d194013

Plaintext Line 1:



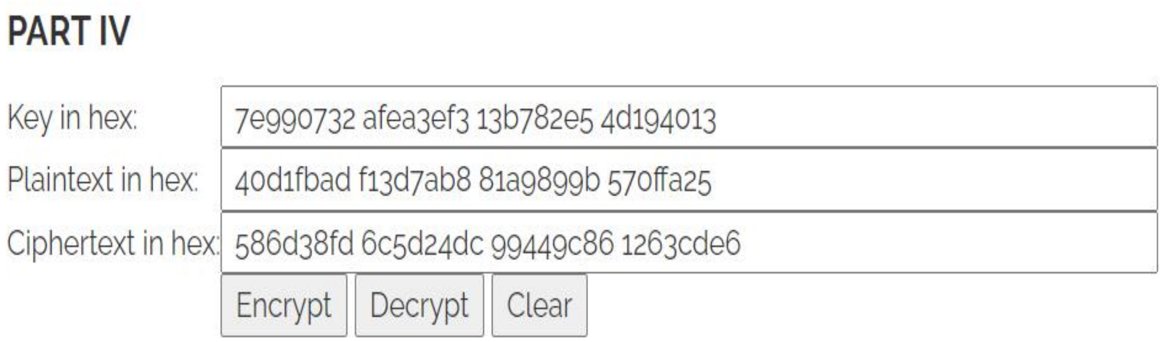
PART IV

Key in hex: 7e990732 afea3ef3 13b782e5 4d194013

Plaintext in hex: 6844beb2 d1bb0ceb 71a03cdf e3d3ca42

Ciphertext in hex: 964cfe43 b68bcedd ac5f42d4 508a2ab8

Plaintext Line 2:



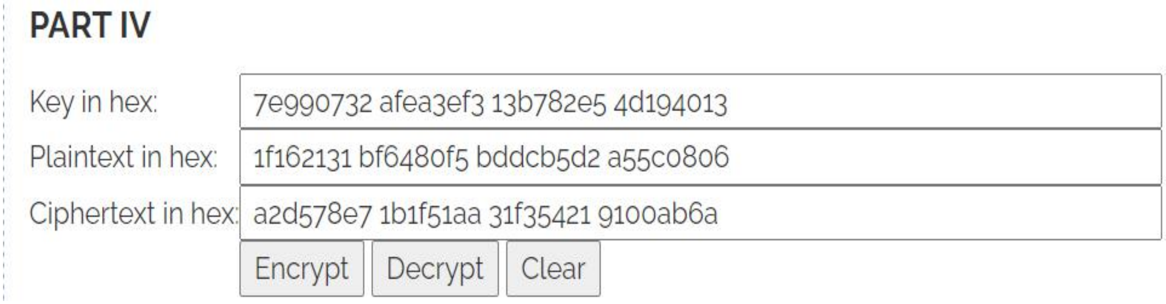
PART IV

Key in hex: 7e990732 afea3ef3 13b782e5 4d194013

Plaintext in hex: 40d1fbad f13d7ab8 81a9899b 570ffa25

Ciphertext in hex: 586d38fd 6c5d24dc 99449c86 1263cde6

Plaintext Line 3:



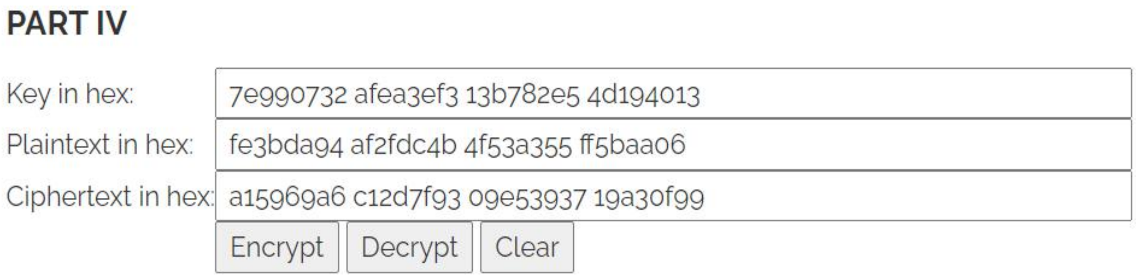
PART IV

Key in hex: 7e990732 afea3ef3 13b782e5 4d194013

Plaintext in hex: 1f162131 bf6480f5 bddcb5d2 a55c0806

Ciphertext in hex: a2d578e7 1b1f51aa 31f35421 9100ab6a

Plaintext Line 4:



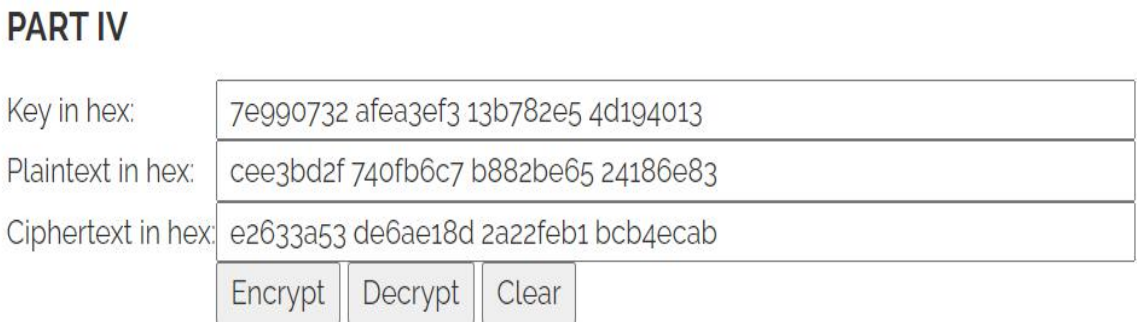
PART IV

Key in hex: 7e990732 afea3ef3 13b782e5 4d194013

Plaintext in hex: fe3bda94 af2fdc4b 4f53a355 ff5baa06

Ciphertext in hex: a15969a6 c12d7f93 09e53937 19a30f99

Plaintext Line 5:



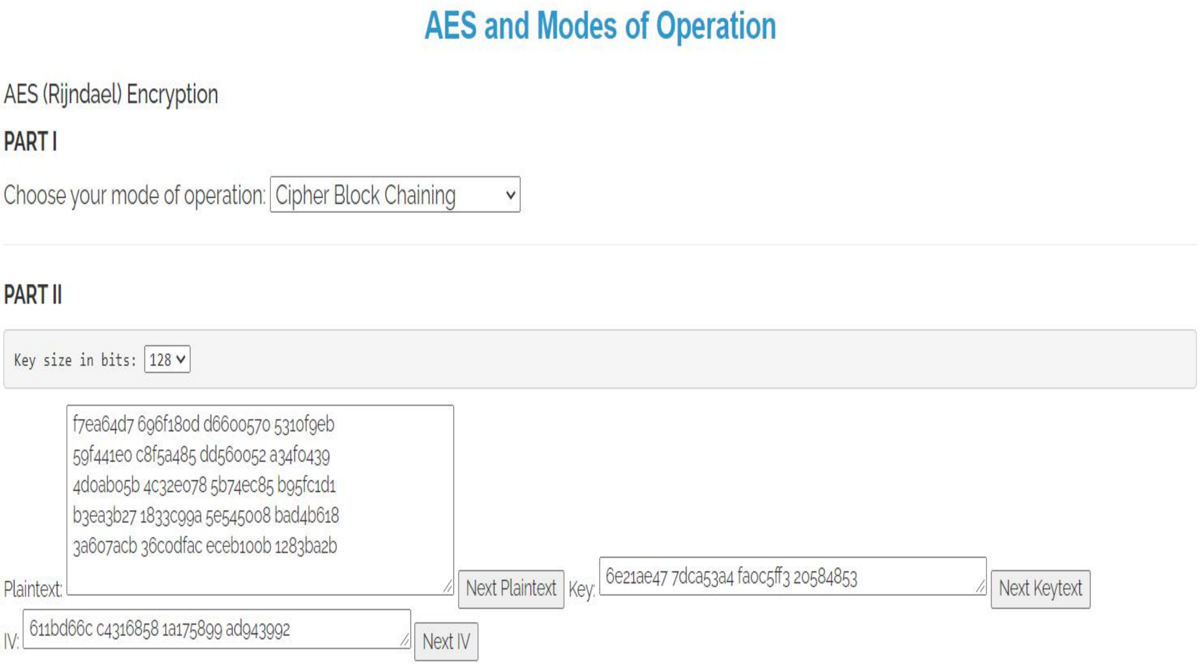
PART IV

Key in hex: 7e990732 afea3ef3 13b782e5 4d194013

Plaintext in hex: cee3bd2f 740fb6c7 b882be65 24186e83

Ciphertext in hex: e2633a53 de6ae18d 2a22feb1 bcb4ecab

CIPHER BLOCK CHAINING (CBC) MODE



AES and Modes of Operation

AES (Rijndael) Encryption

PART I

Choose your mode of operation: Cipher Block Chaining

PART II

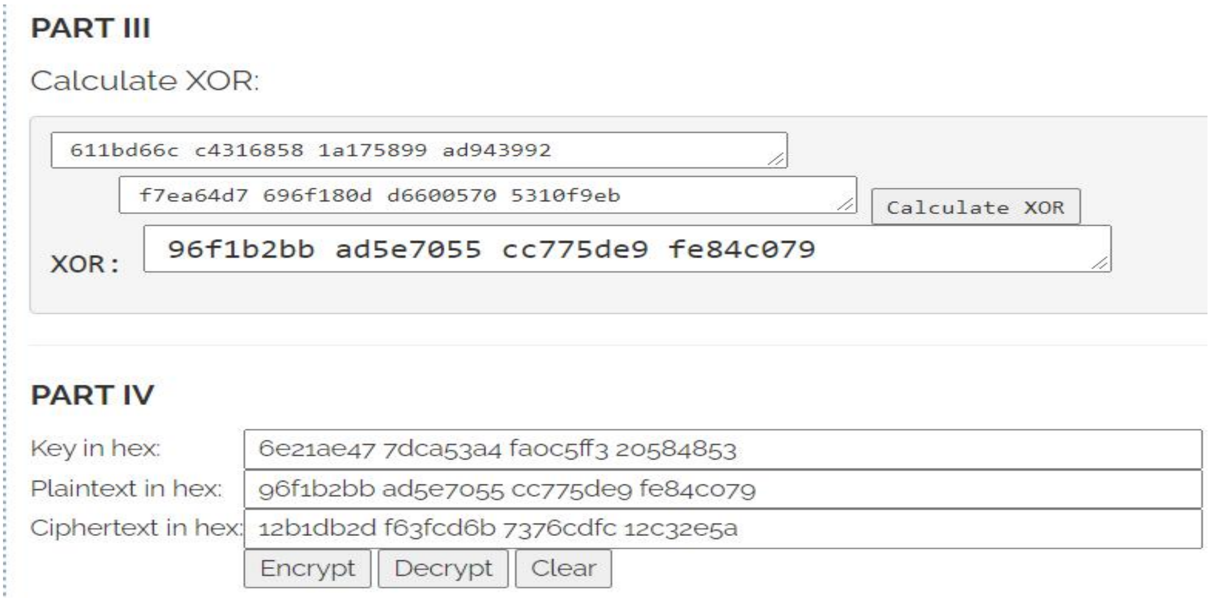
Key size in bits: 128

Plaintext:
```
f7ea64d7 696f180d d6600570 5310f9eb
59f441e0 c8f5a485 dd560052 a34f0439
4d0ab05b 4c32e078 5b74ec85 b95fc1d1
b3ea3b27 1833c99a 5e545008 bad4b618
3a607acb 36c0dfac eceb100b 1283ba2b
```

Key: 6e21ae47 7dca53a4 fa0c5ff3 20584853

IV: 611bd66c c4316858 1a175899 ad943992

PLAINTEXT LINE 1:



PART III

Calculate XOR:

611bd66c c4316858 1a175899 ad943992

f7ea64d7 696f180d d6600570 5310f9eb

XOR : 96f1b2bb ad5e7055 cc775de9 fe84c079

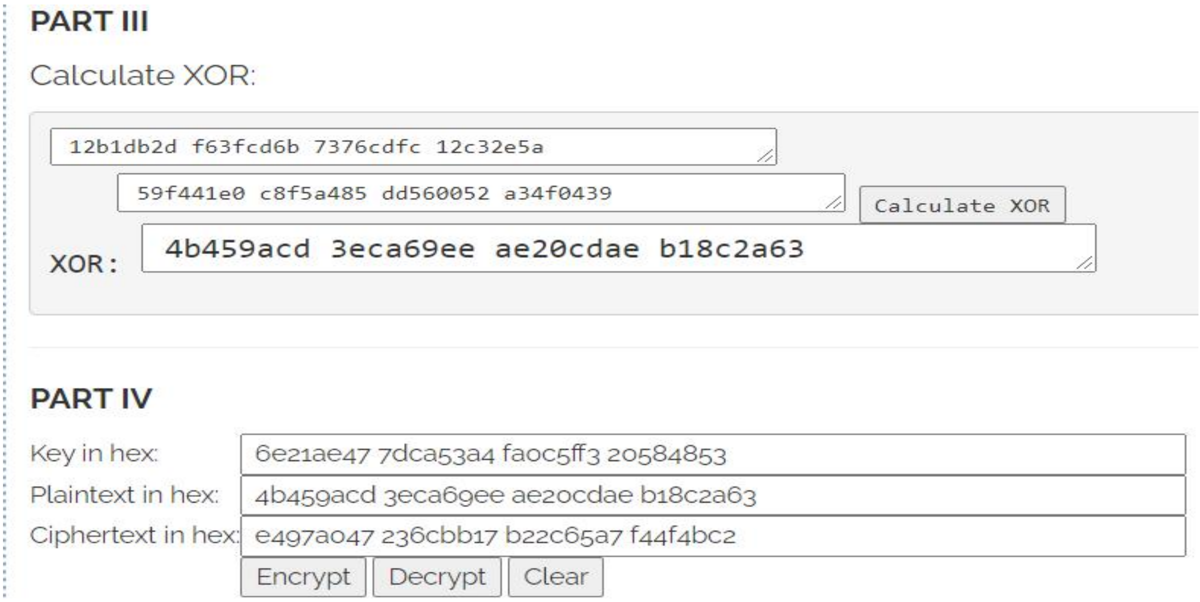
PART IV

Key in hex: 6e21ae47 7dca53a4 fa0c5ff3 20584853

Plaintext in hex: 96f1b2bb ad5e7055 cc775de9 fe84c079

Ciphertext in hex: 12b1db2d f63fcd6b 7376cdfc 12c32e5a

PLAINTEXT LINE 2:



PART III

Calculate XOR:

12b1db2d f63fcd6b 7376cdfc 12c32e5a

59f441e0 c8f5a485 dd560052 a34f0439

XOR : 4b459acd 3eca69ee ae20cdae b18c2a63

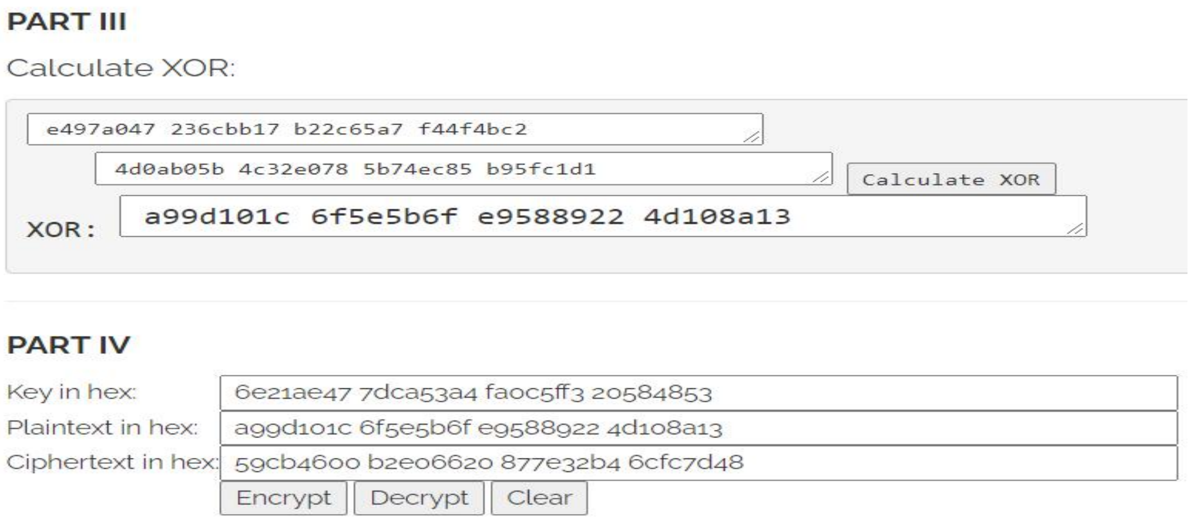
PART IV

Key in hex: 6e21ae47 7dca53a4 fa0c5ff3 20584853

Plaintext in hex: 4b459acd 3eca69ee ae20cdae b18c2a63

Ciphertext in hex: e497a047 236cbb17 b22c65a7 f44f4bc2

PLAINTEXT LINE 3:



PART III

Calculate XOR:

e497a047 236cbb17 b22c65a7 f44f4bc2

4d0ab05b 4c32e078 5b74ec85 b95fc1d1

XOR : a99d101c 6f5e5b6f e9588922 4d108a13

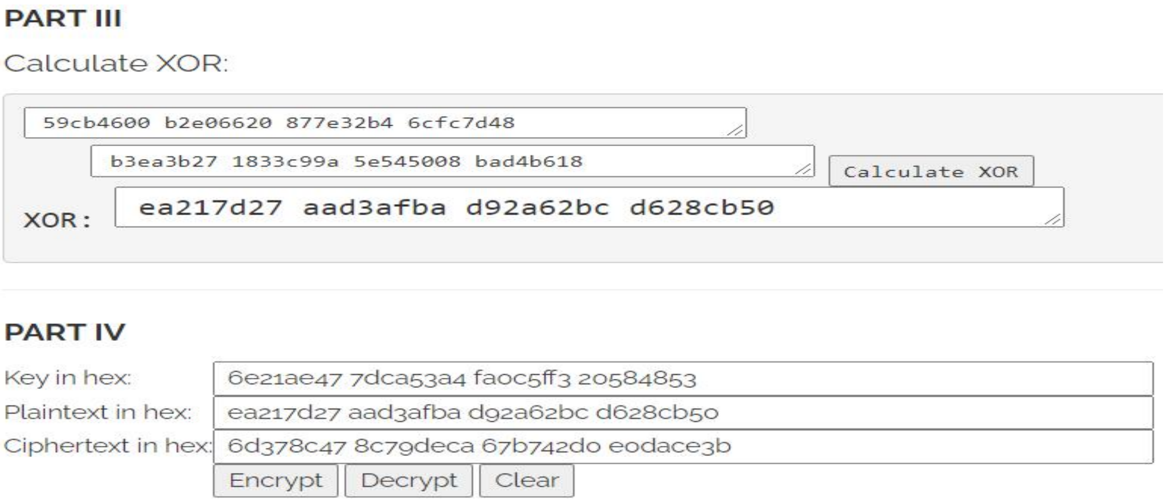
PART IV

Key in hex: 6e21ae47 7dca53a4 fa0c5ff3 20584853

Plaintext in hex: a99d101c 6f5e5b6f e9588922 4d108a13

Ciphertext in hex: 59cb4600 b2e06620 877e32b4 6cfc7d48

PLAINTEXT LINE 4:



PART III

Calculate XOR:

59cb4600 b2e06620 877e32b4 6cfc7d48

b3ea3b27 1833c99a 5e545008 bad4b618

XOR : ea217d27 aad3afba d92a62bc d628cb50

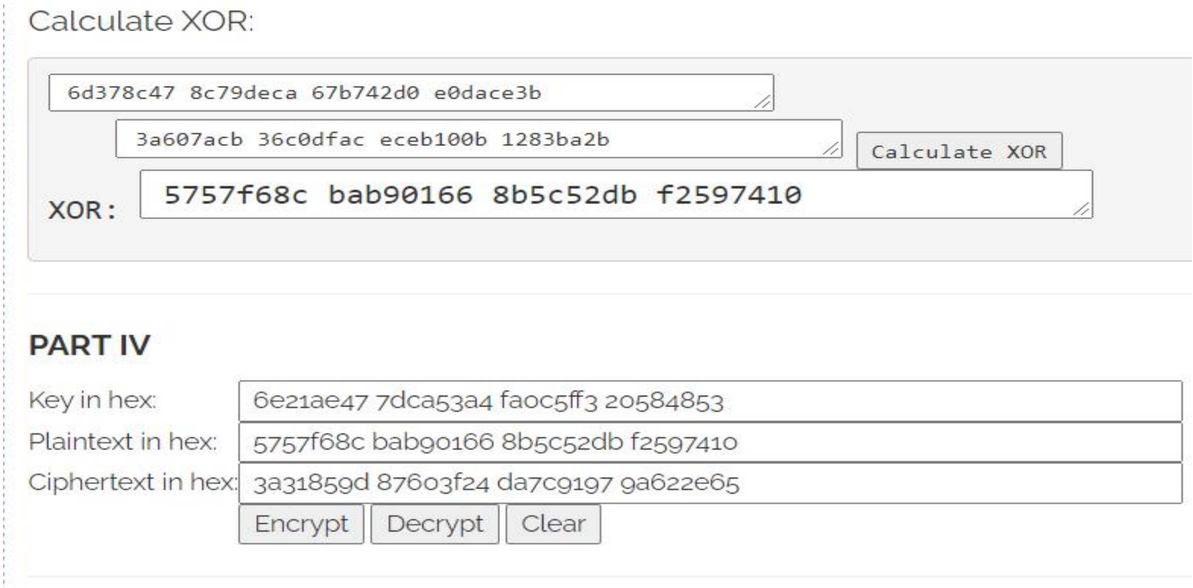
PART IV

Key in hex: 6e21ae47 7dca53a4 fa0c5ff3 20584853

Plaintext in hex: ea217d27 aad3afba d92a62bc d628cb50

Ciphertext in hex: 6d378c47 8c79deca 67b742d0 e0dace3b

PLAINTEXT LINE 5:



Calculate XOR:

6d378c47 8c79deca 67b742d0 e0dace3b

3a607acb 36c0dfac eceb100b 1283ba2b

XOR : 5757f68c bab90166 8b5c52db f2597410

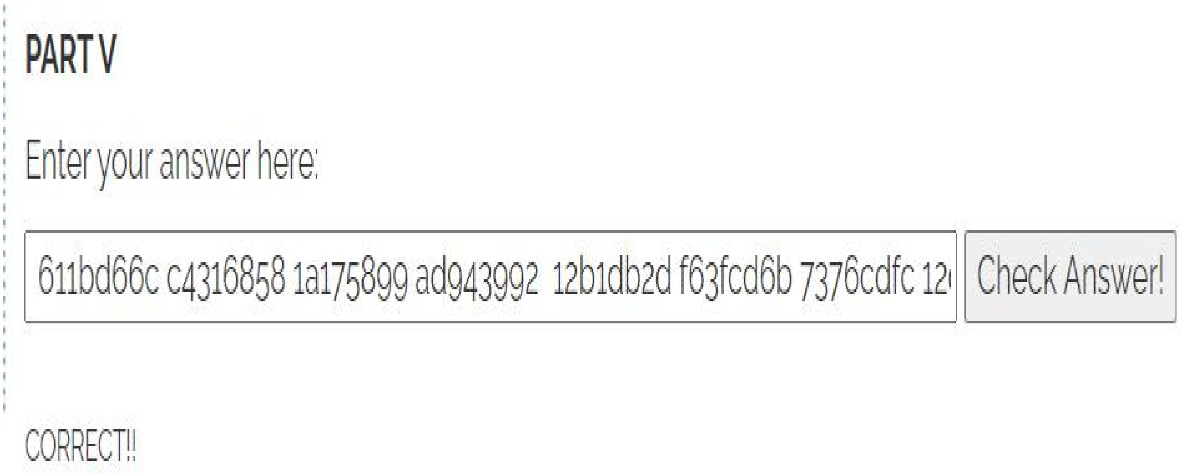
PART IV

Key in hex: 6e21ae47 7dca53a4 fa0c5ff3 20584853

Plaintext in hex: 5757f68c bab90166 8b5c52db f2597410

Ciphertext in hex: 3a31859d 87603f24 da7c9197 9a622e65

RESULT :



PART V

Enter your answer here:

611bd66c c4316858 1a175899 ad943992 12b1db2d f63fcd6b 7376cdfc 12

CORRECT!!

CONCLUSION : Hence we conclude that we learned and implemented encryption of long messages using various modes of operations of AES or DES