EXPERIMENT NUMBER: 4

Date of Performance :

Date of Submission :

AIM: Encrypt long messages using various modes of operation using AES or DES.

THEORY:

Theory – Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as ciphertext. In simpler terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of a cryptographic key a set of mathematical values that both the sender and the recipient of an encrypted message agree on.

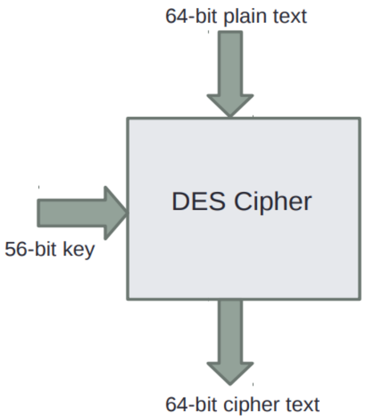
There are two types of encryption:

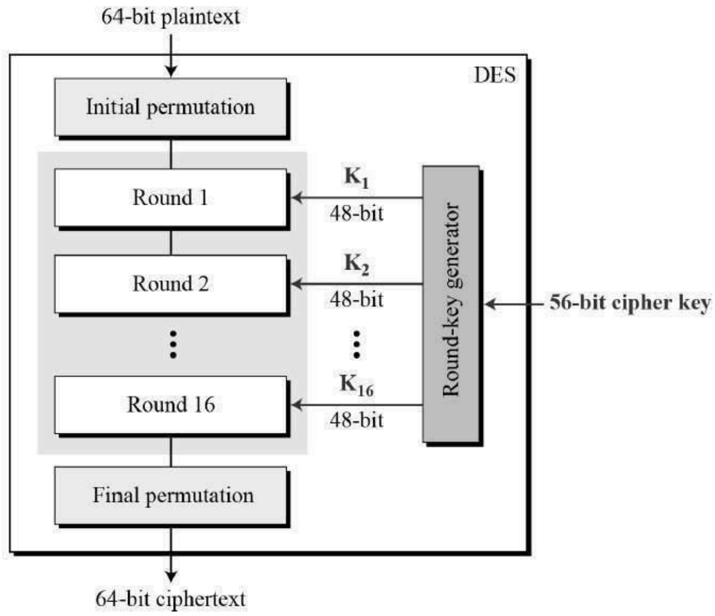
1. Symmetric Encryption.
2. Asymmetric Encryption

Symmetric Encryption: In symmetric encryption, there is only one key, and all parties involved use the same key to encrypt and decrypt information. By using a single key, the process is straightforward, as per the following example: you encrypt an email with a unique key, send that email to your friend Tom, and he will use the same symmetric- key to unlock/decrypt the email. The perks of symmetric encryption are its faster performance and low resource consumption, but it is inherently older and less secure than its counterpart. The reason is simple: if you scale your encryption to a company-wide scale, it means you're putting all your trust into a single key you will need to share around a lot. For this reason, Symmetric encryption is great when working with sensitive data in bulk.

Asymmetric Encryption: Asymmetric encryption, on the other hand, was created to solve the inherent issue of symmetric encryption: the need of sharing a single encryption key around that is used both for encrypting and decrypting data. This newer and safer method utilizes two keys for its encryption process, the public key, used for encryption, and the private key used for decryption. A public key is available for anyone who needs to encrypt a piece of information. This key doesn't work for the decryption process. A user needs to have a secondary key, the private key, to decrypt this information. This way, the private key is only held by the actor who decrypts the information, without sacrificing security as you scale security. A good example is email encryption.

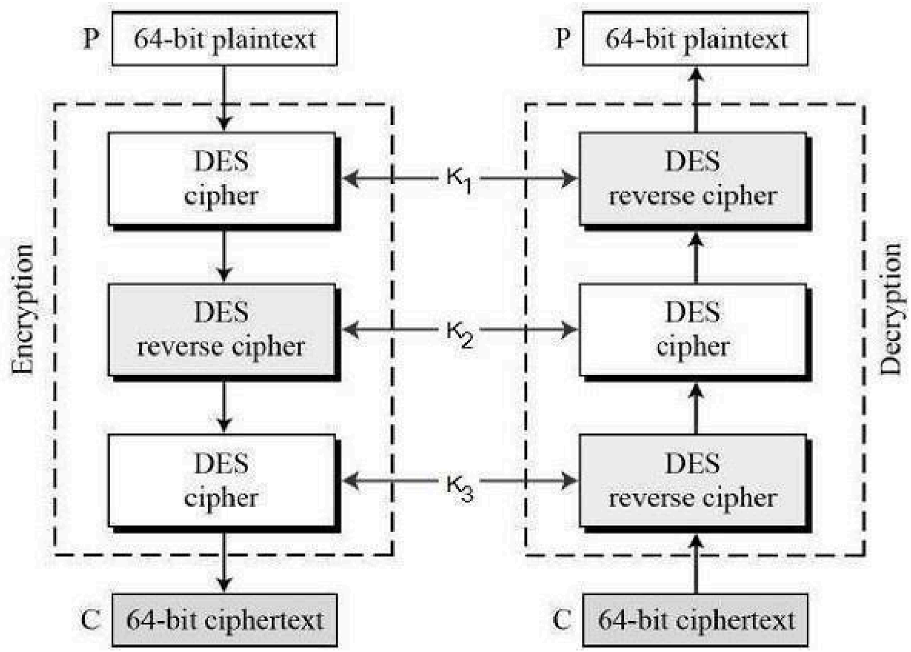
Data encryption standard (DES) has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been found slightly on decline. DES is a block cipher, and encrypts data in blocks of size of 64 bit each, means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits. The basic idea is show in figure.



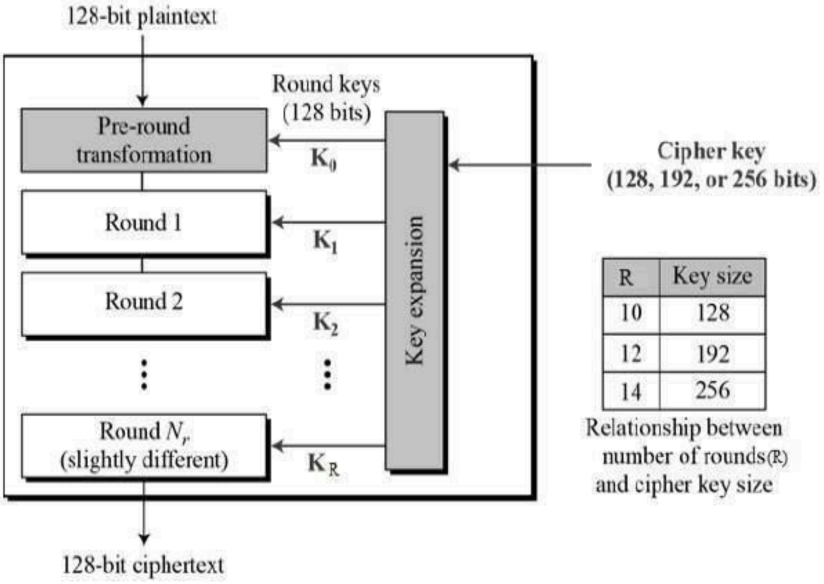


3- KEY Triple DES

Before using 3TDES, user first generate and distribute a 3TDES key K, which consists of three different DES keys K1, K2 and K3. This means that the actual 3TDES key has length 3×56 = 168 bits. The encryption scheme is illustrated as follows –



Advance Encryption Standard (AES) is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Modes of Operation

Mode 1 - Electronic Code Book(ECB) Mode

Mode 2 – Cipher Block Chaining(CBC) Mode
Mode 3 – Output Feedback(OFB) Mode

Mode 4 – Counter(CTR) Mode

AES and Modes of Operation

Step I : Choose a mode of operation from **PART I**

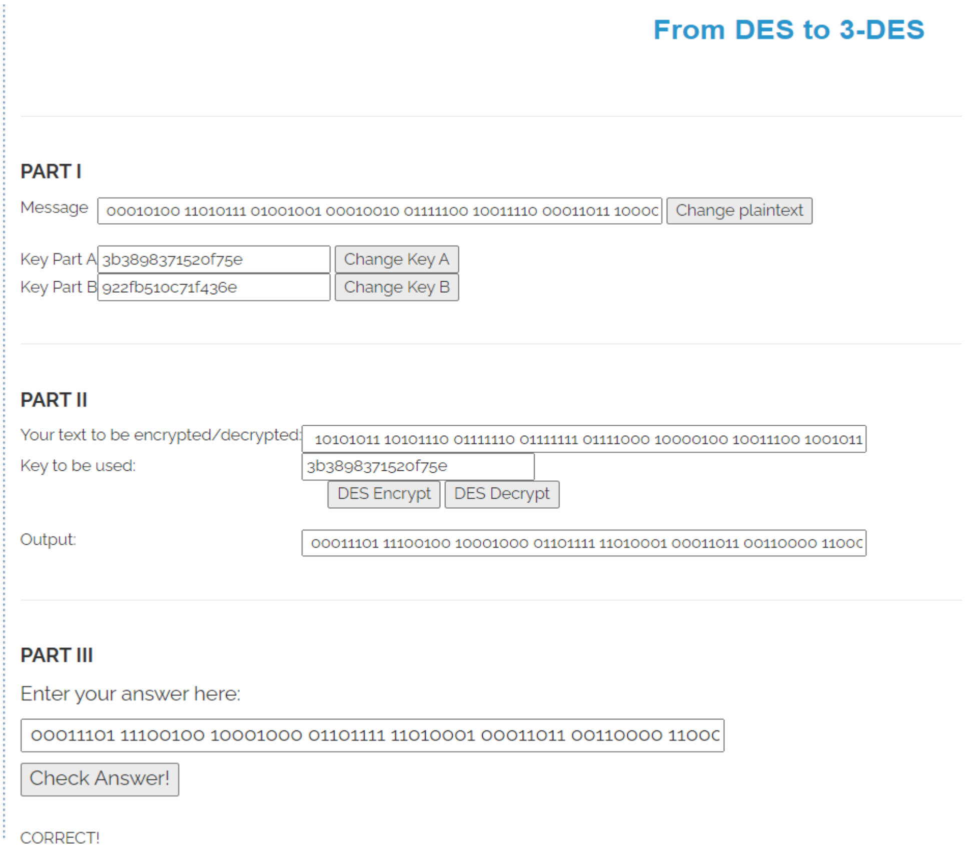
Step II : Select KeySize, Plaintext, KeyText, Intialization vector(IV)(for ECB and OFB modes only) and CTR(forctr mode only) in **PART II**

Step III : Whenever necessay use XOR opeartion in **PART III** in accordance with choosen mode of operation

Step IV : Use fuction **FK** and "Key in hex:" field in **PART IV** should be filled keytext generated in **Step2**

Step V : Fill "Plaintext in hex:" field with approriate value in accordance with choosen mode of operation and click on encrypt button

Step VI : Enter your answer in **PART V** to check your ciphertext



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: 10101011 10101110 01111110 01111111 01111000 10000100 10011100 1001011

Key to be used: 3b3898371520f75e

Output: 00011101 11100100 10001000 01101111 11010001 00011011 00110000 1100

PART III

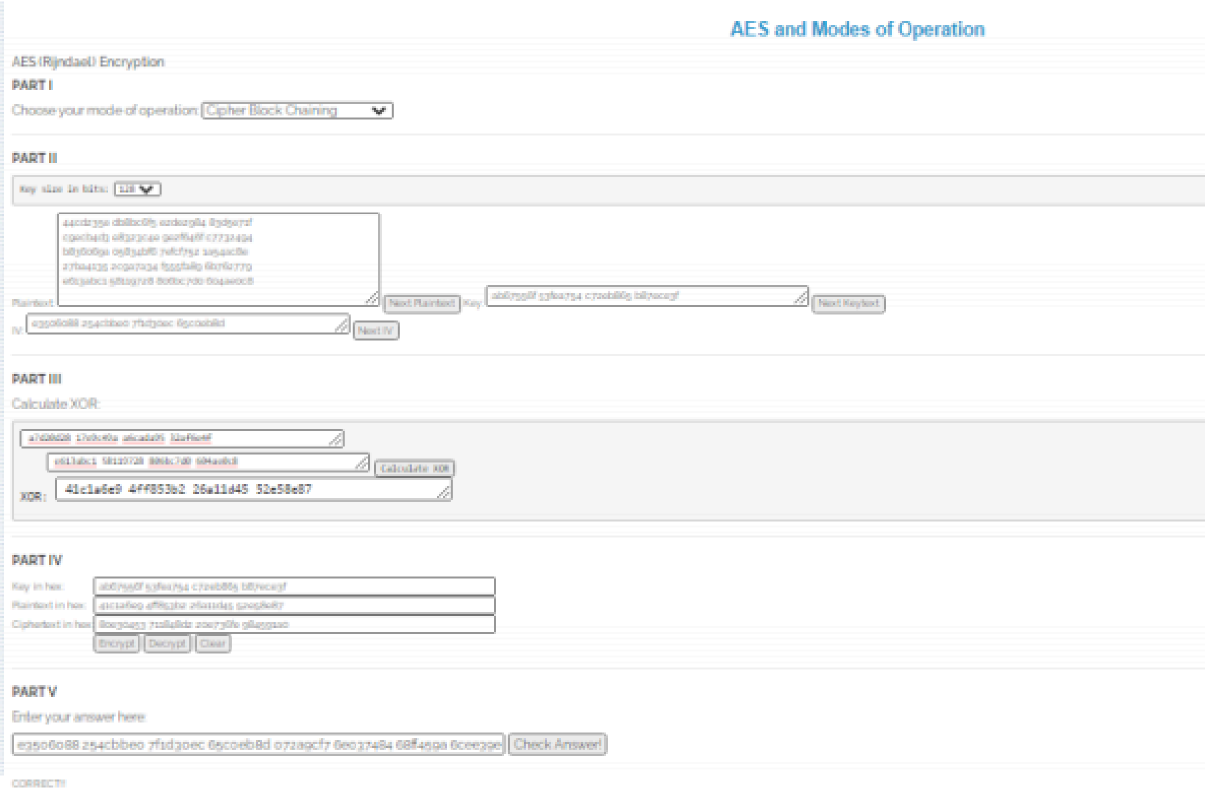
Enter your answer here:

00011101 11100100 10001000 01101111 11010001 00011011 00110000 1100

CORRECT!

OUTPUT :-

Cipher block chaining



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:
```
44cd2350 db8bc0f5 e2de2984 83d5e72f
c9ecb4d3 e8323c40 9e2f64ff c7732494
b83d069a 0583 4bf6 7efcf752 1e542c8e
27b44135 2c9a7a34 f555fa89 6b762779
e6c3abc1 58119728 806bc7d0 604ae0c8
```
Next Plaintext

Key: ab67558f 53fea754 c72eb865 b87ece3f

Next Keytext

IV: e3506088 254cbbe0 7f1d30ec 65c0eb8d

Next IV

PART III

Calculate XOR:
```
a7d20d28 17e9c40a a6cada05 32af6e4f
e613abc1 58110728 806bc7d0 604ae0c8
XOR: 41c1a6e9 4ff853b2 26a11d45 52e58e87
```
Calculate XOR

PART IV

Key in hex: ab67558f 53fea754 c72eb865 b87ece3f

Plaintext in hex: 41c1a6e9 4ff853b2 26a11d45 52e58e87

Ciphertext in hex: 0e230453 7118a8d2 20e730fe 98a59120

Encrypt Decrypt Clear

PART V

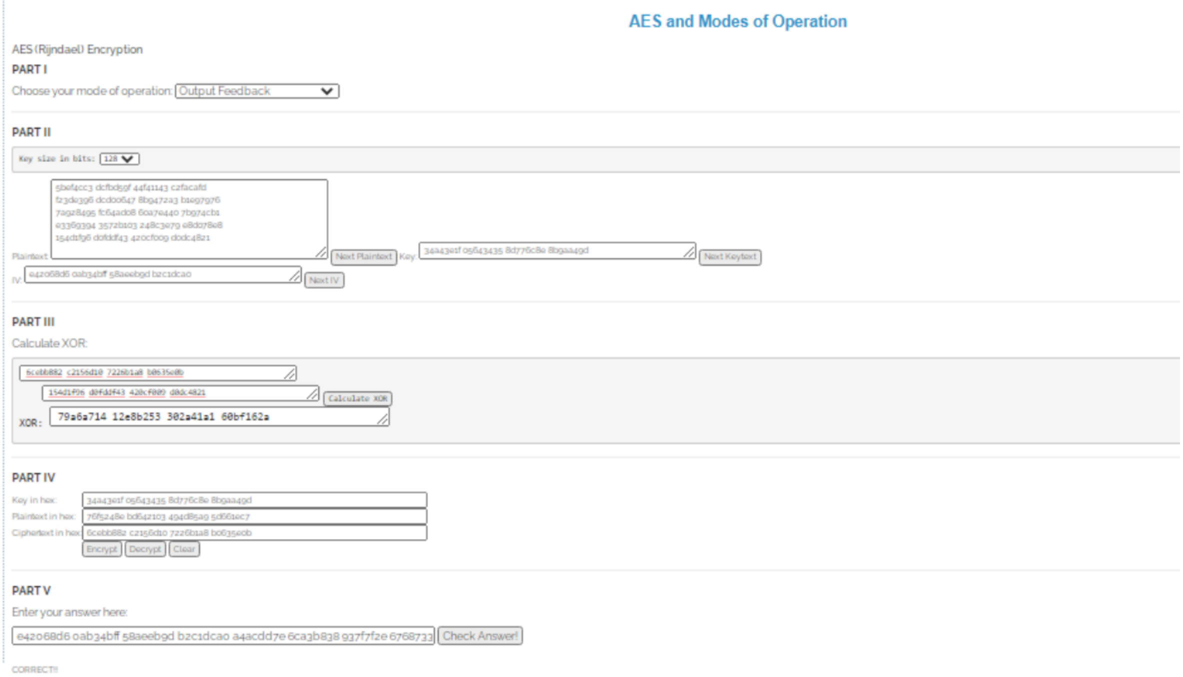
Enter your answer here

e3506088 254cbbe0 7f1d30ec 65c0eb8d 07229cf7 0e037484 68f459a 0cee39e

Check Answer!

CORRECT!!

Output feedback



AES and Modes of Operation

AES (Rijndael) Encryption

PART I

Choose your mode of operation: Output Feedback

PART II

Key size in bits: 128

Plaintext:

```
5bef4cc3 dcfbd59f 44f41143 c2facafd
f23de396 dcd00647 8b9472a3 b1e97976
7a928495 fc64ad08 60a7e440 7b974cb1
e3369394 3572b103 248c3e79 e8d078e8
154d1f96 d0fddf43 420cf009 d0dc4821
```

Key: 34a43e1f 05643435 8d776c8e 8b9aa49d

IV: e42068d6 0ab34bff 58aeeb9d b2c1dca0

PART III

Calculate XOR:

```
6cebb882 c2156d10 7226b1a8 b0635e0b
154d1f96 d0fddf43 420cf009 d0dc4821
```

XOR : 79a6a714 12e8b253 302a41a1 60bf162a

PART IV

Key in hex: 34a43e1f 05643435 8d776c8e 8b9aa49d

Plaintext in hex: 76f5248e bd642103 494d85a9 5d661ec7

Ciphertext in hex: 6cebb882 c2156d10 7226b1a8 b0635e0b

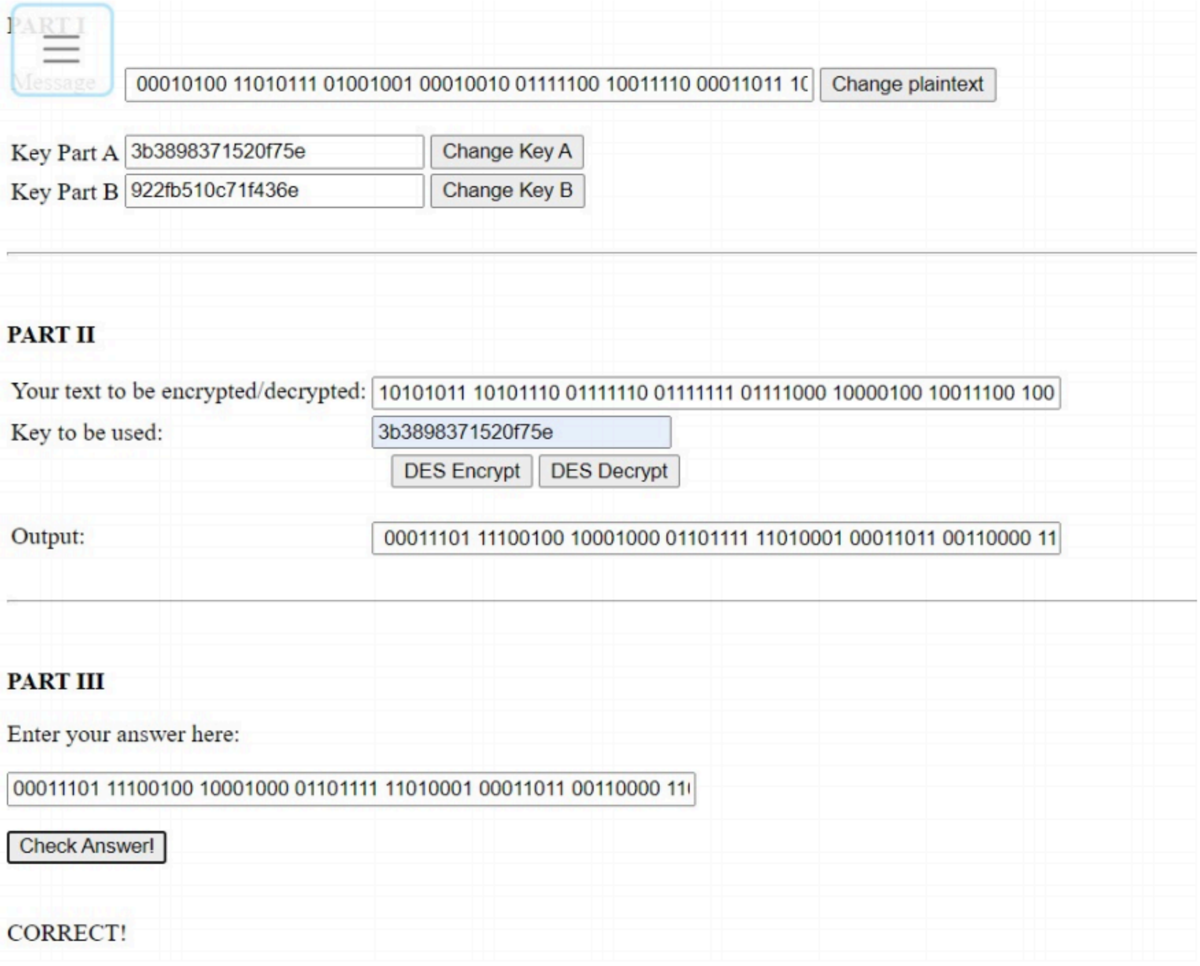
PART V

Enter your answer here:

e42068d6 0ab34bff 58aeeb9d b2c1dca0 a4acdd7e 6ca3b838 937f7f2e 6768733

CORRECT!!

Counter



PART I

Message 00010100 11010111 01001001 00010010 01111100 10011110 00011011 1(

Key Part A 3b3898371520f75e

Key Part B 922fb510c71f436e

PART II

Your text to be encrypted/decrypted: 10101011 10101110 01111110 01111111 01111000 10000100 10011100 100

Key to be used: 3b3898371520f75e

Output: 00011101 11100100 10001000 01101111 11010001 00011011 00110000 11

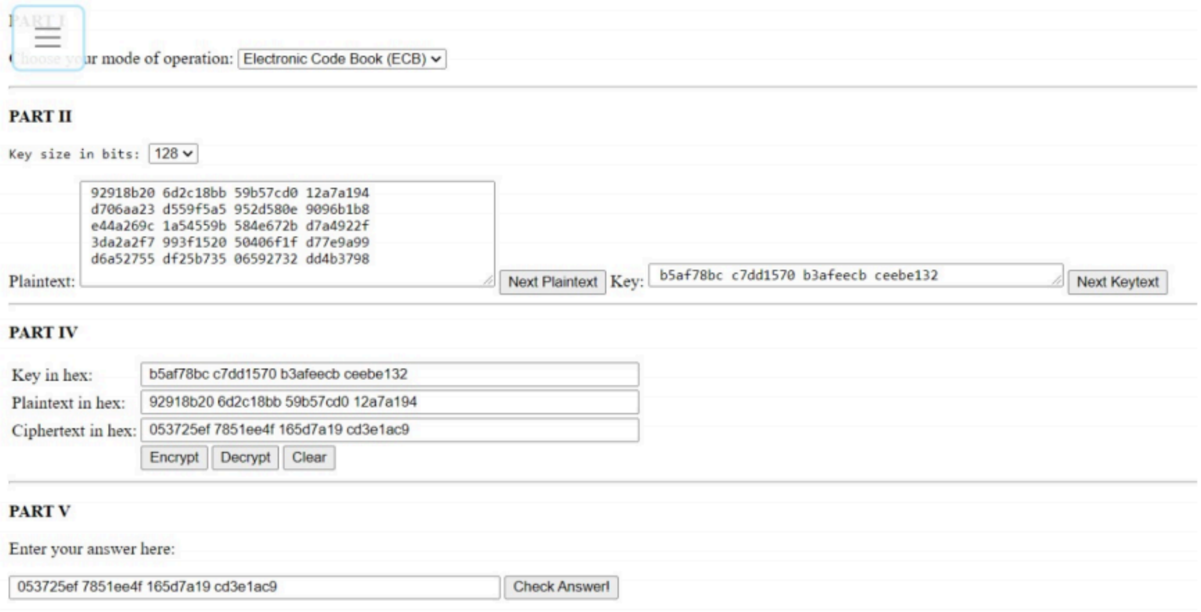
PART III

Enter your answer here:

00011101 11100100 10001000 01101111 11010001 00011011 00110000 11(

CORRECT!

Electronic Code Book



PART I

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

PART II

Key size in bits: 128

Plaintext:

```
92918b20 6d2c18bb 59b57cd0 12a7a194
d706aa23 d559f5a5 952d580e 9096b1b8
e44a269c 1a54559b 584e672b d7a4922f
3da2a2f7 993f1520 50406f1f d77e9a99
d6a52755 df25b735 06592732 dd4b3798
```

Key: b5af78bc c7dd1570 b3afeecb ceebe132

PART IV

Key in hex: b5af78bc c7dd1570 b3afeecb ceebe132

Plaintext in hex: 92918b20 6d2c18bb 59b57cd0 12a7a194

Ciphertext in hex: 053725ef 7851ee4f 165d7a19 cd3e1ac9

PART V

Enter your answer here:

053725ef 7851ee4f 165d7a19 cd3e1ac9

CONCLUSION/ Outcome:

we successfully Hence,long messages have been encrypted using various modes of operation using AES or DES

<u>Marks & Signature:</u>

R1 (5 Marks)	R2 (5 Marks)	R3 (5 Marks)	Total (15 Marks)	Signature