Aim:

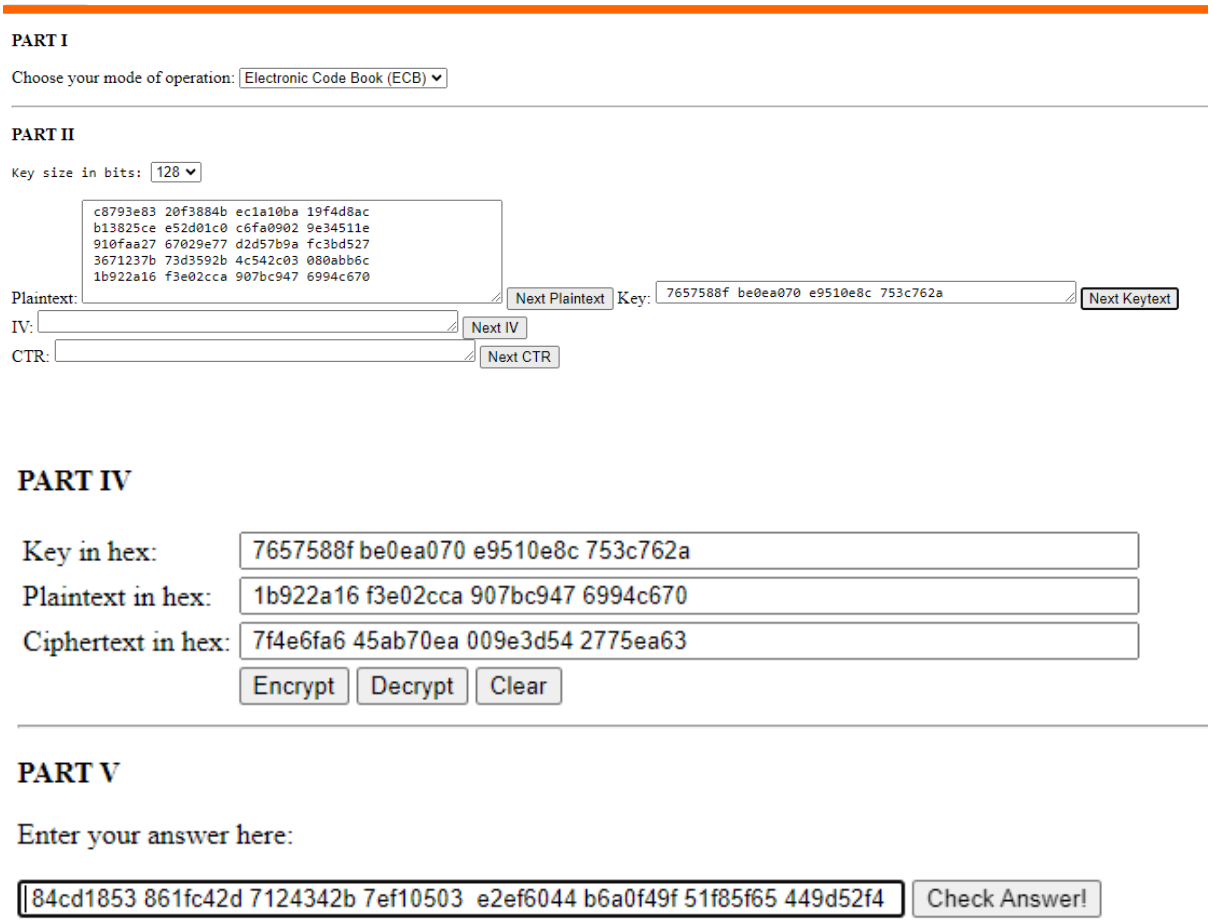
Block cipher modes of operation using Advanced Encryption Standard (AES).

LO Mapping: LO2

Theory & Output:

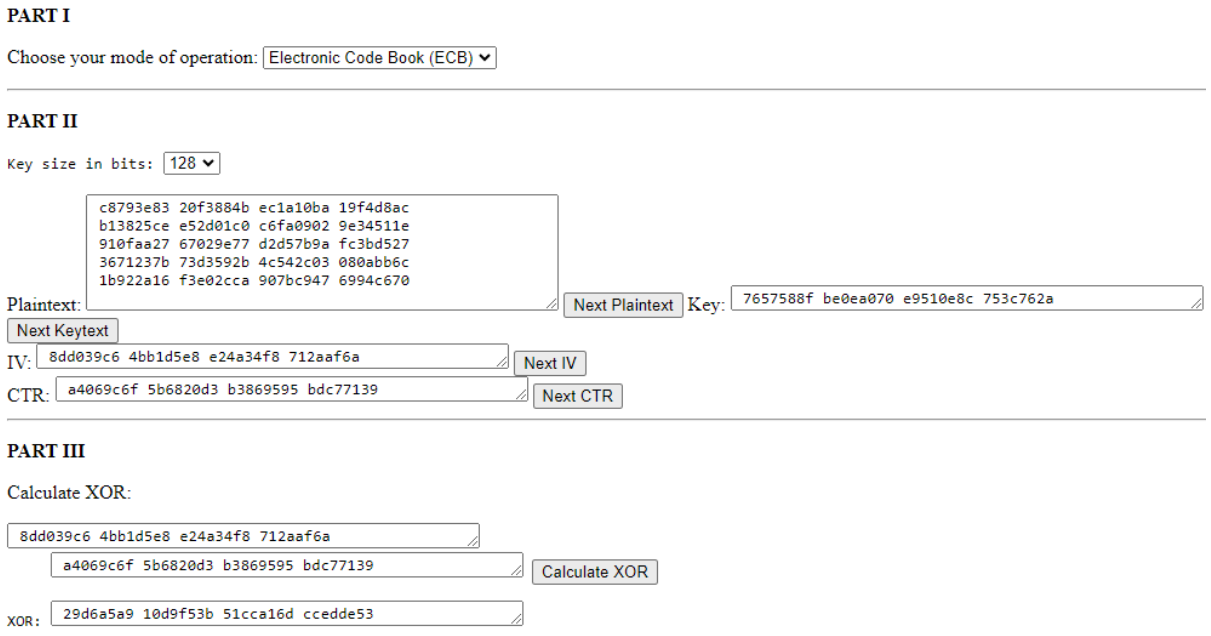
Advanced Encryption Standard (AES):

AES is a symmetric encryption algorithm used to secure data. It operates on blocks of data (128 bits) and supports key sizes of 128, 192, or 256 bits. AES is widely used due to its strength and efficiency. It involves multiple rounds of processing where each round includes substitution (using S-box), permutation (shifting rows), mixing (combining columns), and key addition steps.



Cipher Block Chaining (CBC)

CBC is a mode of operation for block ciphers that ensures that each ciphertext block depends on all previous ciphertext blocks. It starts with an initial value called an Initialization Vector (IV). Each plaintext block is XORed with the previous ciphertext block before being encrypted. This chaining makes patterns in plaintext less detectable and increases security, but it requires that each block be processed sequentially.



PART III

Calculate XOR:

38f52387 fe9f197c 9308c54b 98584fd0

64fb6d2e 64d42105 1047432e fc4cbec3 Calculate XOR

XOR: 5c0e4ea9 9a4b3879 834f8665 6414f113

PART IV

Key in hex: 6e36a027 b704c80e 30da45bc 358aad79

Plaintext in hex: 5c0e4ea9 9a4b3879 834f8665 6414f113

Ciphertext in hex: daf5ec4f af57aba5 8563de63 b90fc659

Encrypt Decrypt Clear

PART V

Enter your answer here:

38f52387 fe9f197c 9308c54b 98584fd0 daf5ec4f af57aba5 8563de63 b90fc659 Check Answer!

Counter Mode

CTR mode turns a block cipher into a stream cipher. It works by encrypting a counter value and then XORing the resulting ciphertext with the plaintext. The counter value is incremented for each block of data processed. Because encryption is done independently for each block, CTR mode allows for parallel processing and is efficient for large volumes of data.

PART II

Key size in bits: 128

Plaintext:
```
7cbc9989 d67627eb 36ac27b0 5fac8d13
3acdeecd 4fc6696c 70969b5c 3514ff44
6c40e6fc 7f53d6eb 58870c92 9e02c296
157a2810 df2d6de7 2f6004c7 6455f8b9
64fb6d2e 64d42105 1047432e fc4cbec3
```
Next Plaintext Key: `6e36a027 b704c80e 30da45bc 358aad79` Next Keytext

CTR: `63c70cca fd8c3515 1a5aa2a1 42ef397c` Next CTR

PART III

Calculate XOR:

`64fb6d2e 64d42105 1047432e fc4cbec3`

`9baa067a e2400c57 71291dcc 9905cf6b` Calculate XOR

XOR: `ff516b54 86942d52 616e5ee2 654971a8`

PART IV

Key in hex: 6e36a027 b704c80e 30da45bc 358aad79

Plaintext in hex: 63c70cca fd8c3515 1a5aa2a1 42ef397c

Ciphertext in hex: 9baa067a e2400c57 71291dcc 9905cf6b

Encrypt Decrypt Clear

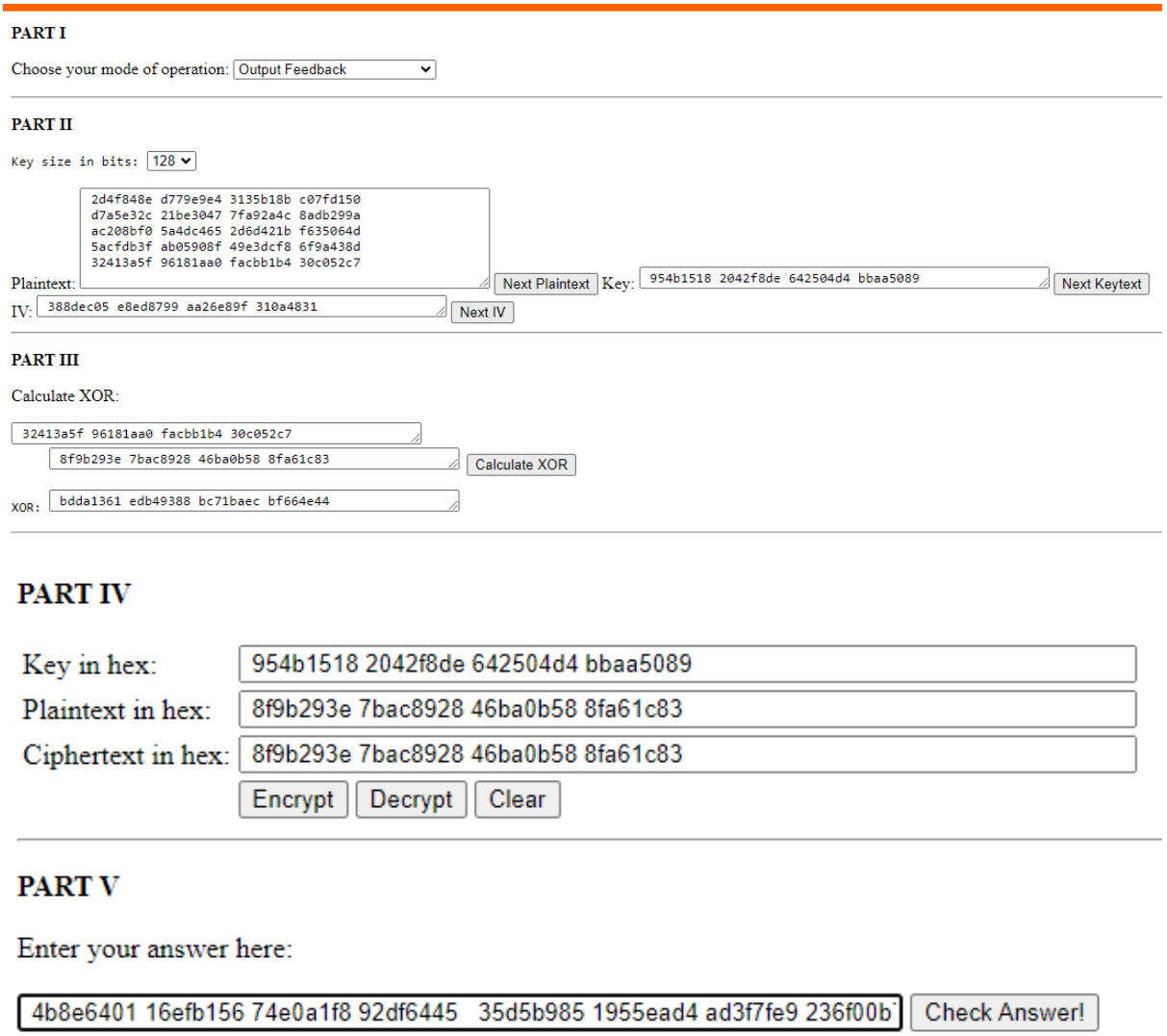
PART V

Enter your answer here:

c948b0 4ee800bc 2eb90d1b 4d391247 ff516b54 86942d52 616e5ee2 654971a8 Check Answer!

Output Feedback Mode

OFB mode is another way to use block ciphers as stream ciphers. Instead of encrypting the plaintext directly, OFB mode encrypts an initialization vector (IV) and then repeatedly encrypts the output to generate a keystream. This keystream is XORed with the plaintext to produce ciphertext. OFB mode's advantage is that it can generate the keystream independently of the plaintext, allowing for parallel encryption and decryption, but it's crucial to use a unique IV for each operation to avoid security risks.



Conclusion:

In conclusion, the Advanced Encryption Standard (AES) employs various block cipher modes of operation, each designed to enhance security and provide specific functionalities. These modes—such as ECB, CBC, CFB, OFB, and CTR—offer different levels of data confidentiality and integrity. Understanding the strengths and weaknesses of each mode is crucial for selecting the appropriate method for a given application, ensuring robust encryption and data protection.