

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.

PART I

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

PART II

Key size in bits: 128 ▼

```
c8793e83 20f3884b ec1a10ba 19f4d8ac  
b13825ce e52d01c0 c6fa0902 9e34511e  
910faa27 67029e77 d2d57b9a fc3bd527  
3671237b 73d3592b 4c542c03 080abb6c  
1b922a16 f3e02cca 907bc947 6994c670
```

Plaintext:

Next Plaintext

Key: 7657588f be0ea070 e9510e8c 753c762a

Next Keytext

IV:

Next IV

CTR:

Next CTR

PART IV

Key in hex: 7657588f be0ea070 e9510e8c 753c762a

Plaintext in hex: 1b922a16 f3e02cca 907bc947 6994c670

Ciphertext in hex: 7f4e6fa6 45ab70ea 009e3d54 2775ea63

Encrypt

Decrypt

Clear

PART V

Enter your answer here:

84cd1853 861fc42d 7124342b 7ef10503 e2ef6044 b6a0f49f 51f85f65 449d52f4

Check Answer!

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 I

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

PART II

Key size in bits: 128 ▼

```
c8793e83 20f3884b ec1a10ba 19f4d8ac
b13825ce e52d01c0 c6fa0902 9e34511e
910faa27 67029e77 d2d57b9a fc3bd527
3671237b 73d3592b 4c542c03 080abb6c
1b922a16 f3e02cca 907bc947 6994c670
```

Plaintext: Next Plaintext Key: 7657588f be0ea070 e9510e8c 753c762a

Next Keytext

IV: 8dd039c6 4bb1d5e8 e24a34f8 712aaf6a Next IV

CTR: a4069c6f 5b6820d3 b3869595 bdc77139 Next CTR

PART III

Calculate XOR:

8dd039c6 4bb1d5e8 e24a34f8 712aaf6a
a4069c6f 5b6820d3 b3869595 bdc77139 Calculate XOR

XOR: 29d6a5a9 10d9f53b 51cca16d ccedde53

PART III

Calculate XOR:

38f52387 fe9f197c 9308c54b 98584fd0	Calculate XOR
64fb6d2e 64d42105 1047432e fc4cbec3	
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
	<input type="button" value="Encrypt"/> <input type="button" value="Decrypt"/> <input type="button" value="Clear"/>

PART V

Enter your answer here:

38f52387 fe9f197c 9308c54b 98584fd0 daf5ec4f af57aba5 8563de63 b90fc659	<input type="button" value="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:

7cbc9989 d67627eb 36ac27b0 5fac8d13
3acdeecd 4fc6696c 70969b5c 3514ff44
6c40e6fc 7f53d6eb 58870c92 9e02c296
157a2810 df2d6de7 2f6004c7 6455f8b9
64fb6d2e 64d42105 1047432e fc4cbec3

Next Plaintext

Key:

Next Keytext

CTR:

Next CTR

PART III

Calculate XOR:

Calculate XOR

XOR:

PART IV

Key in hex:

Plaintext in hex:

Ciphertext in hex:

Encrypt

Decrypt

Clear

PART V

Enter your answer here:

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.

PART I

Choose your mode of operation: Output Feedback

PART II

Key size in bits: 128

2d4f848e d779e9e4 3135b18b c07fd150
d7a5e32c 21be3047 7fa92a4c 8adb299a
ac208bf0 5a4dc465 2d6d421b f635064d
5acfdb3f ab05908f 49e3dcf8 6f9a438d
32413a5f 96181aa0 facbb1b4 30c052c7

Plaintext:

Next Plaintext

Key:

954b1518 2042f8de 642504d4 bbba5089

Next Keytext

IV: 388dec05 e8ed8799 aa26e89f 310a4831

Next IV

PART III

Calculate XOR:

32413a5f 96181aa0 facbb1b4 30c052c7

8f9b293e 7bac8928 46ba0b58 8fa61c83

Calculate XOR

XOR: bdda1361 edb49388 bc71baec bf664e44

PART IV

Key in hex: 954b1518 2042f8de 642504d4 bbba5089

Plaintext in hex: 8f9b293e 7bac8928 46ba0b58 8fa61c83

Ciphertext in hex: 8f9b293e 7bac8928 46ba0b58 8fa61c83

Encrypt

Decrypt

Clear

PART V

Enter your answer here:

4b8e6401 16efb156 74e0a1f8 92df6445 35d5b985 1955ead4 ad3f7fe9 236f00b

Check Answer!

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.