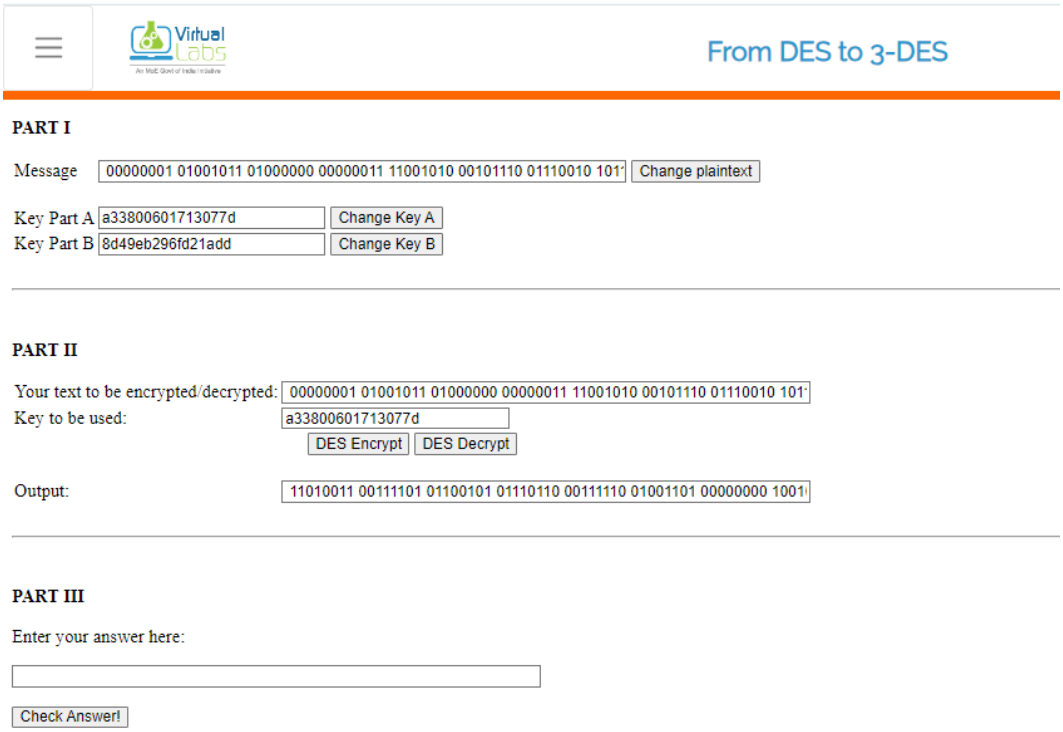
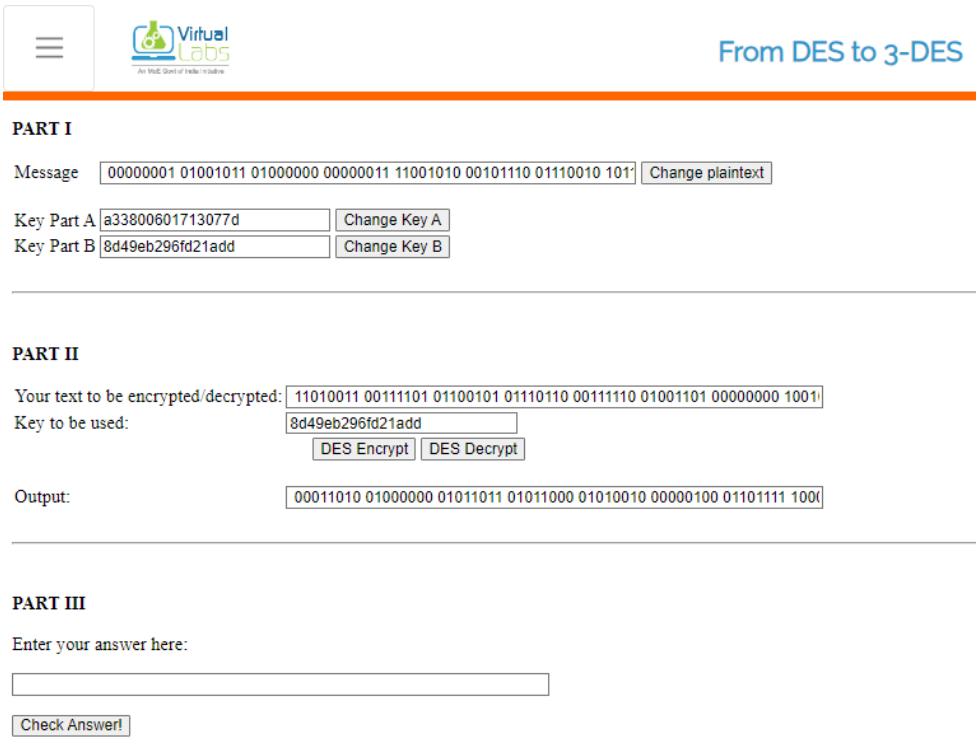
AIM: To understand how to Encrypt long messages using various modes of operation using AES or DES

Step1:First Encryption using Key A.



Step 2: Second Decryption using key B



Step 3:Third Encryption using keyA,Then Check your answer,

Virtual Labs

From DES to 3-DES

PART I

Message 00000001 01001011 01000000 00000011 11001010 00101110 01110010 101 Change plaintext

Key Part A a33800601713077d Change Key A

Key Part B 8d49eb296fd21add Change Key B

PART II

Your text to be encrypted/decrypted: 00011010 01000000 01011011 01011000 01010010 00000100 01101111 100(

Key to be used: a33800601713077d

DES Encrypt DES Decrypt

Output: 01000011 01000001 11000000 00000111 01101011 10111010 10100000 101

PART III

Enter your answer here:

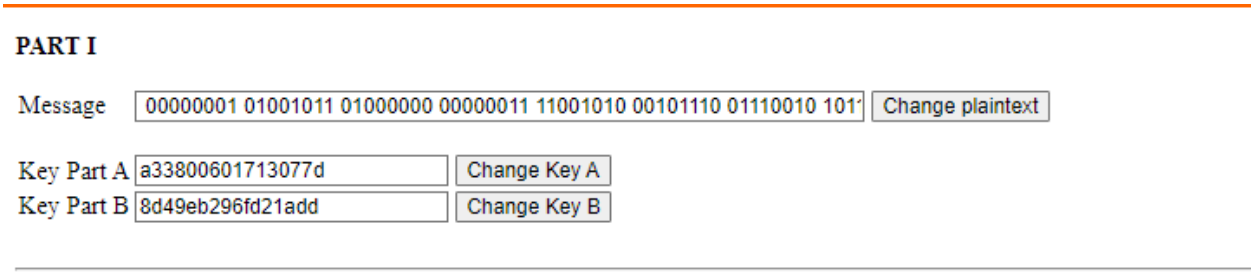
01000011 01000001 11000000 00000111 01101011 10111010 10100000 101

Check Answer!

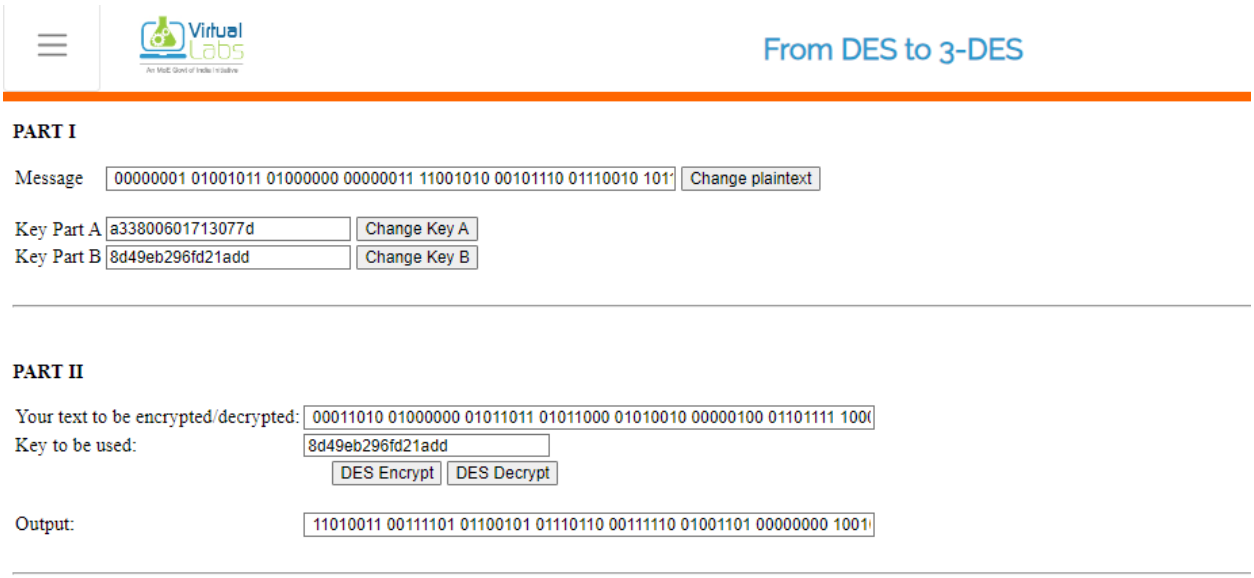
CORRECT!

Now Decrypting the output

Step 1:Paste output in text to be decrypted,use key 1 then decrypt.



Then Encrypt the output



Then Decrypt the output it will be same as message.

PART I

Message 00000001 01001011 01000000 00000011 11001010 00101110 01110010 101 Change plaintext

Key Part A a33800601713077d Change Key A

Key Part B 8d49eb296fd21add Change Key B

PART II

Your text to be encrypted/decrypted: 11010011 00111101 01100101 01110110 00111110 01001101 00000000 1001

Key to be used: a33800601713077d

DES Encrypt DES Decrypt

Output: 00000001 01001011 01000000 00000011 11001010 00101110 01110010 101

AES

In AES,We need to generate the plain text and keytext,

Then we need to copy the key in part 4,

Then we need to encrypt the plaintext line by line,

And copy the cipher text and paste it in part 5 to check the answer

After all the 5 steps we can submit the message and check tha if correct.

PART I

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

PART II

Key size in bits: 128

Plaintext:
```
47fb03e6 3b8a0934 05acf75a 4a8b8e69
3a59ed99 ddb47881 02edcd66 48f13432
08784140 c209c5df 6106fb77 0199c911
d3dda103 09206e78 5e19a486 de356e9a
1d9ccf8a a206cd97 f19b409b 1c3e1fb8
```
Next Plaintext Key: 18c72e28 387ff92a 1eb2debf 8d2ac754 Next Keytext

IV: Next IV

CTR: Next CTR

PART III

Calculate XOR:

Calculate XOR

XOR:

PART IV

Key in hex: 18c72e28 387ff92a 1eb2debf 8d2ac754

Plaintext in hex: 47fb03e6 3b8a0934 05acf75a 4a8b8e69

Ciphertext in hex: b20fa142 dcfc7bcf 40ab930d 49994e2f

Encrypt Decrypt Clear

PART I

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

PART II

Key size in bits: 128

Plaintext:
```
47fb03e6 3b8a0934 05acf75a 4a8b8e69
3a59ed99 ddb47881 02edcd66 48f13432
08784140 c209c5df 6106fb77 0199c911
d3dda103 09206e78 5e19a486 de356e9a
1d9ccf8a a206cd97 f19b409b 1c3e1fb8
```
Next Plaintext Key: 18c72e28 387ff92a 1eb2debf 8d2ac754 Next Keytext

IV: Next IV

CTR: Next CTR

PART III

Calculate XOR:

Calculate XOR

XOR:

PART IV

Key in hex: 18c72e28 387ff92a 1eb2debf 8d2ac754

Plaintext in hex: 3a59ed99 ddb47881 02edcd66 48f13432

Ciphertext in hex: 9dd83b76 ef743870 8195e178 37aee2fd

Encrypt Decrypt Clear

PART I

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

PART II

Key size in bits: 128

Plaintext:
```
47fb03e6 3b8a0934 05acf75a 4a8b8e69
3a59ed99 ddb47881 02edcd66 48f13432
08784140 c209c5df 6106fb77 0199c911
d3dda103 09206e78 5e19a486 de356e9a
1d9ccf8a a206cd97 f19b409b 1c3e1fb8
```
Next Plaintext Key: 18c72e28 387ff92a 1eb2debf 8d2ac754 Next Keytext

IV: Next IV

CTR: Next CTR

PART III

Calculate XOR:

Calculate XOR

XOR:

PART IV

Key in hex: 18c72e28 387ff92a 1eb2debf 8d2ac754

Plaintext in hex: 08784140 c209c5df 6106fb77 0199c911

Ciphertext in hex: 385d87b5 a9c87fa1 f6160d1f 2b2c8f29

Encrypt Decrypt Clear

PART I

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

PART II

Key size in bits: 128

Plaintext:
```
47fb03e6 3b8a0934 05acf75a 4a8b8e69
3a59ed99 ddb47881 02edcd66 48f13432
08784140 c209c5df 6106fb77 0199c911
d3dda103 09206e78 5e19a486 de356e9a
1d9ccf8a a206cd97 f19b409b 1c3e1fb8
```
Next Plaintext Key: 18c72e28 387ff92a 1eb2debf 8d2ac754 Next Keytext

IV: Next IV

CTR: Next CTR

PART III

Calculate XOR:

Calculate XOR

XOR:

PART IV

Key in hex: 18c72e28 387ff92a 1eb2debf 8d2ac754

Plaintext in hex: d3dda103 09206e78 5e19a486 de356e9a

Ciphertext in hex: 01f03dcc ecaf61a8 c7f7ca0b 05cb257e

Encrypt Decrypt Clear

PART I

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

PART II

Key size in bits: 128

Plaintext:
```
47fb03e6 3b8a0934 05acf75a 4a8b8e69
3a59ed99 ddb47881 02edcd66 48f13432
08784140 c209c5df 6106fb77 0199c911
d3dda103 09206e78 5e19a486 de356e9a
1d9ccf8a a206cd97 f19b409b 1c3e1fb8
```
Next Plaintext Key: 18c72e28 387ff92a 1eb2debf 8d2ac754 Next Keytext

IV: Next IV

CTR: Next CTR

PART III

Calculate XOR:

Calculate XOR

XOR:

PART IV

Key in hex: 18c72e28 387ff92a 1eb2debf 8d2ac754

Plaintext in hex: 1d9ccf8a a206cd97 f19b409b 1c3e1fb8

Ciphertext in hex: 9b5dad3f 9a1b6ec9 d7f203e2 34055ba1

Encrypt Decrypt Clear

Plaintext: 47fb03e6 3b8a0934 05acf75a 4a8b8e69
3a59ed99 ddb47881 02edcd66 48f13432
08784140 c209c5df 6106fb77 0199c911
d3dda103 09206e78 5e19a486 de356e9a
1d9ccf8a a206cd97 f19b409b 1c3e1fb8
Next Plaintext Key: 18c72e28 387ff92a 1eb2debf 8d2ac754 Next Keytext

IV: Next IV

CTR: Next CTR

PART III

Calculate XOR:

Calculate XOR

XOR:

PART IV

Key in hex: 18c72e28 387ff92a 1eb2debf 8d2ac754

Plaintext in hex: 1d9ccf8a a206cd97 f19b409b 1c3e1fb8

Ciphertext in hex: 9b5dad3f 9a1b6ec9 d7f203e2 34055ba1

Encrypt Decrypt Clear

PART V

Enter your answer here:

b20fa142 dcfc7bcf 40ab930d 49994e2f 9dd83b76 ef743870 8195e178 37aee Check Answer!

CORRECT!!