Course Name:	**Information and Cyber Security Laboratory**	**Semester:**	**VII**
Date of Performance:	**06 / 08 / 25**	**Batch No:**	**B - 1**
Name:	**Dr. Makrand Kulkarni**	**Roll No:**	**16014022050**
Faculty Sign & Date:		**Grade/Marks:**	**25**

Experiment No: 3

Title: To understand how to convert a DES implementation to a triple-DES implementation.

Aim and Objective of the Experiment:

To understand how to convert a DES implementation to a triple-DES implementation.

COs to be achieved:

CO1: Explain various security goals, threats, vulnerabilities and controls with various cryptographic algorithms for software security.

Books/Journals/Websites referred:

Virtual Laboratory Experiment- (http://cse29- iiith.vlabs.ac.in/)

Tools required:

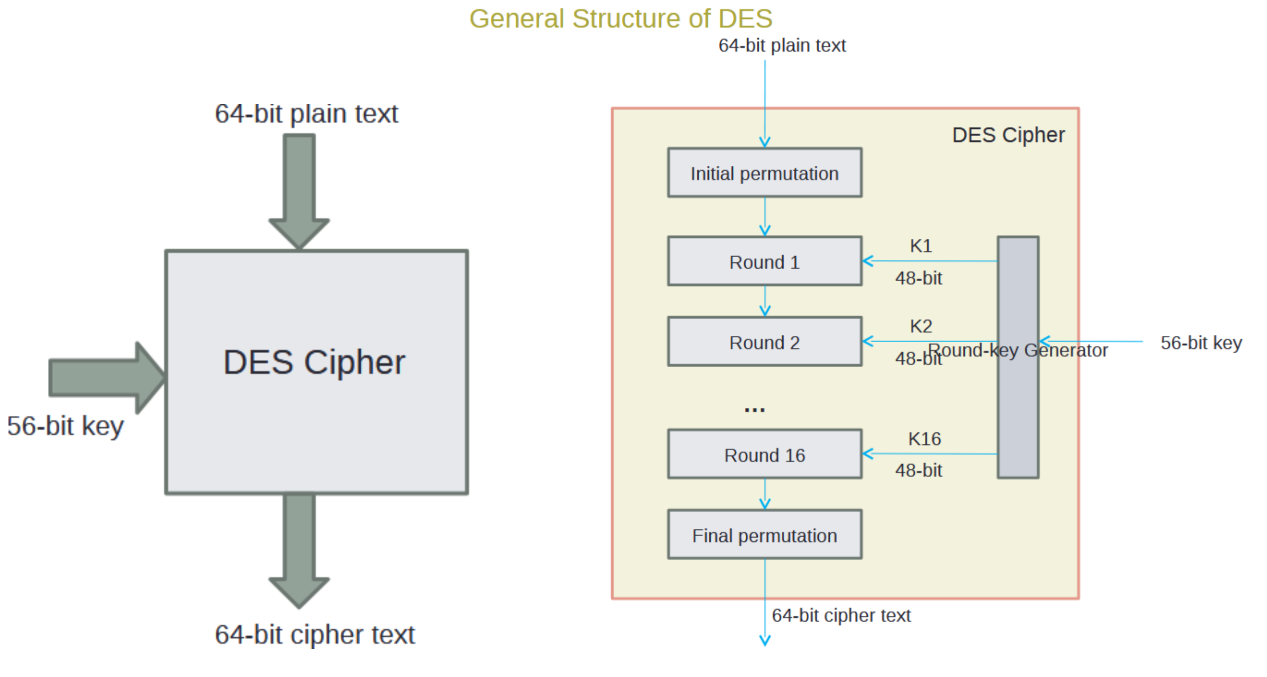
Virtual Laboratory Experiment- (http://cse29- iiith.vlabs.ac.in/)

Theory:

DES is a Symmetric block cipher, which takes 64-bit plain text and creates a 64-bit cipher text. Developed in 1976 by IBM for the US National Institute of Standards and Technology (NIST)

A simple trick does indeed enhance the security of DES. Using three keys adds significant strength. The so-called triple DES procedure is C = E(k3, E(k2, E(k1,m))). That is, you encrypt with one key, then with the second, and finally with a third. This process gives a strength roughly equivalent to a 112-bit key (because the double DES attack defeats the strength of one of the three keys, but it has no effect on the third key). A minor variation of triple DES, which some people also confusingly call triple DES, is C = E(k1, D(k2, E(k1,m))). That is, you encrypt with one key, decrypt with a second, and encrypt with the first again. This version requires only two keys. (The second decrypt step also makes this process work for single encryptions with one key: The decryption cancels the first encryption, so the net result is one encryption. The encrypt–decrypt–encrypt form is handy because one algorithm can produce results for both conventional single-key

DES and the more secure two-key method.)



(a) (b)

Fig. 1 (a) DES block diagram (b) DES Algorithm

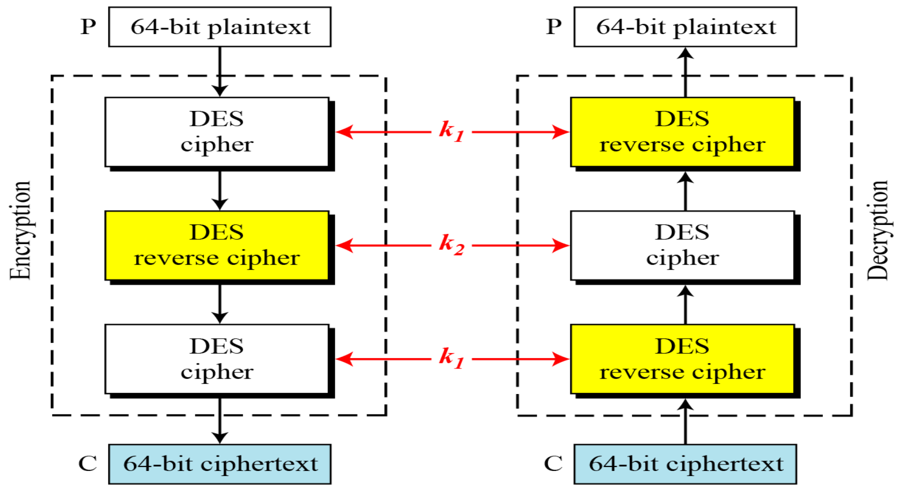


Fig. 2 Triple DES Algorithm

Stepwise Implementation details:

STEP 1 : Generate Plaintext m, keyA and keyB by clicking on rexpective buttons PART I of the simulation page.

STEP 2: Enter generated Plaintext m from PART I to PART II in "Your text to be encrypted/decrypted:" block.

STEP 3 : Enter generated **keyA** from **PART I** to **PART II** "Key to be used:" block and click on DES encrpt button to output ciphertext **c1**.This is First Encryption

STEP 4 : Enter generated ciphertext c1 from PART II "Output:" Block to PART II in "Your text to be encrypted/decrypted:" block.

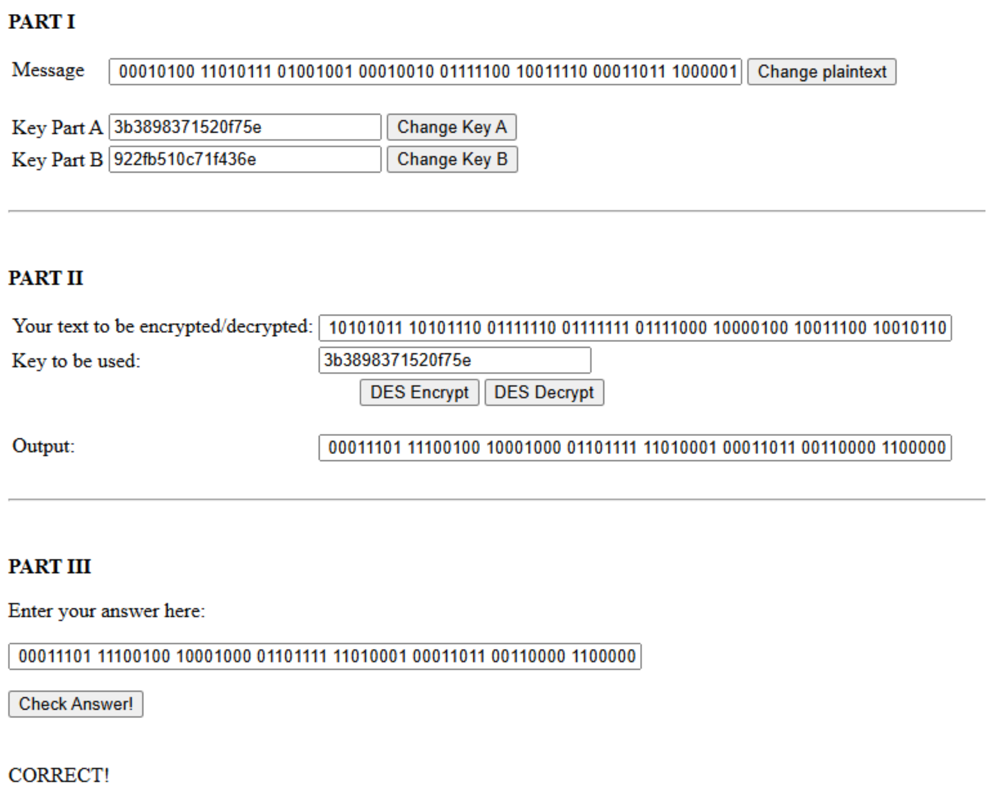
STEP 5 : Enter generated keyB from PART I to PART II in "Key to be used:" block and click on DES decrypt button to output ciphertect c2.This is Second Encryption.

STEP 6 : Enter generated ciphertext c2** from PART II "Output:" block to PART II in "Your text to be encrypted/decrypted:" block.

STEP 7 : Enter generated keyA from PART I to PART II "Key to be used:" block and click on DES encrpt button to output ciphertext c3.This is Third Encryption. As Encryption is done thrice.This Scheme is called triple DES.

STEP 8 : Enter generated ciphertext **c3** from **PART II** "Output:" Block to PART **III** "Enter your answer here:" block inorder to verify your Triple DES.

ScreenShots



PART I

Message: 00010100 11010111 01001001 00010010 01111100 10011110 00011011 1000001

Key Part A: 3b3898371520f75e

Key Part B: 922fb510c71f436e

PART II

Your text to be encrypted/decrypted: 10101011 10101110 01111110 01111111 01111000 10000100 10011100 10010110

Key to be used: 3b3898371520f75e

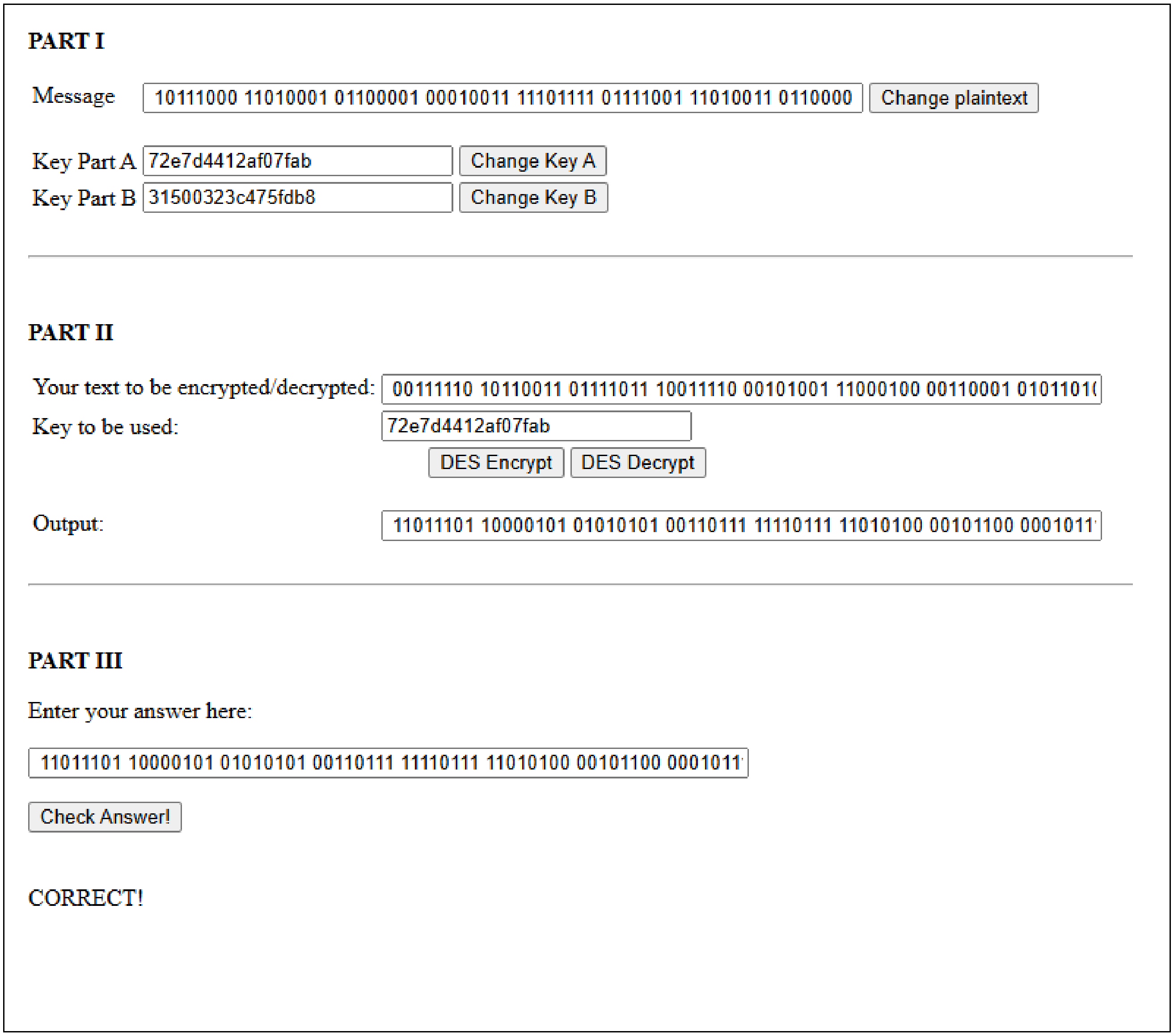
Output: 00011101 11100100 10001000 01101111 11010001 00011011 00110000 1100000

PART III

Enter your answer here:

00011101 11100100 10001000 01101111 11010001 00011011 00110000 1100000

CORRECT!



PART I

Message 10111000 11010001 01100001 00010011 11101111 01111001 11010011 0110000

Key Part A 72e7d4412af07fab

Key Part B 31500323c475fdb8

PART II

Your text to be encrypted/decrypted: 00111110 10110011 01111011 10011110 00101001 11000100 00110001 0101101

Key to be used: 72e7d4412af07fab

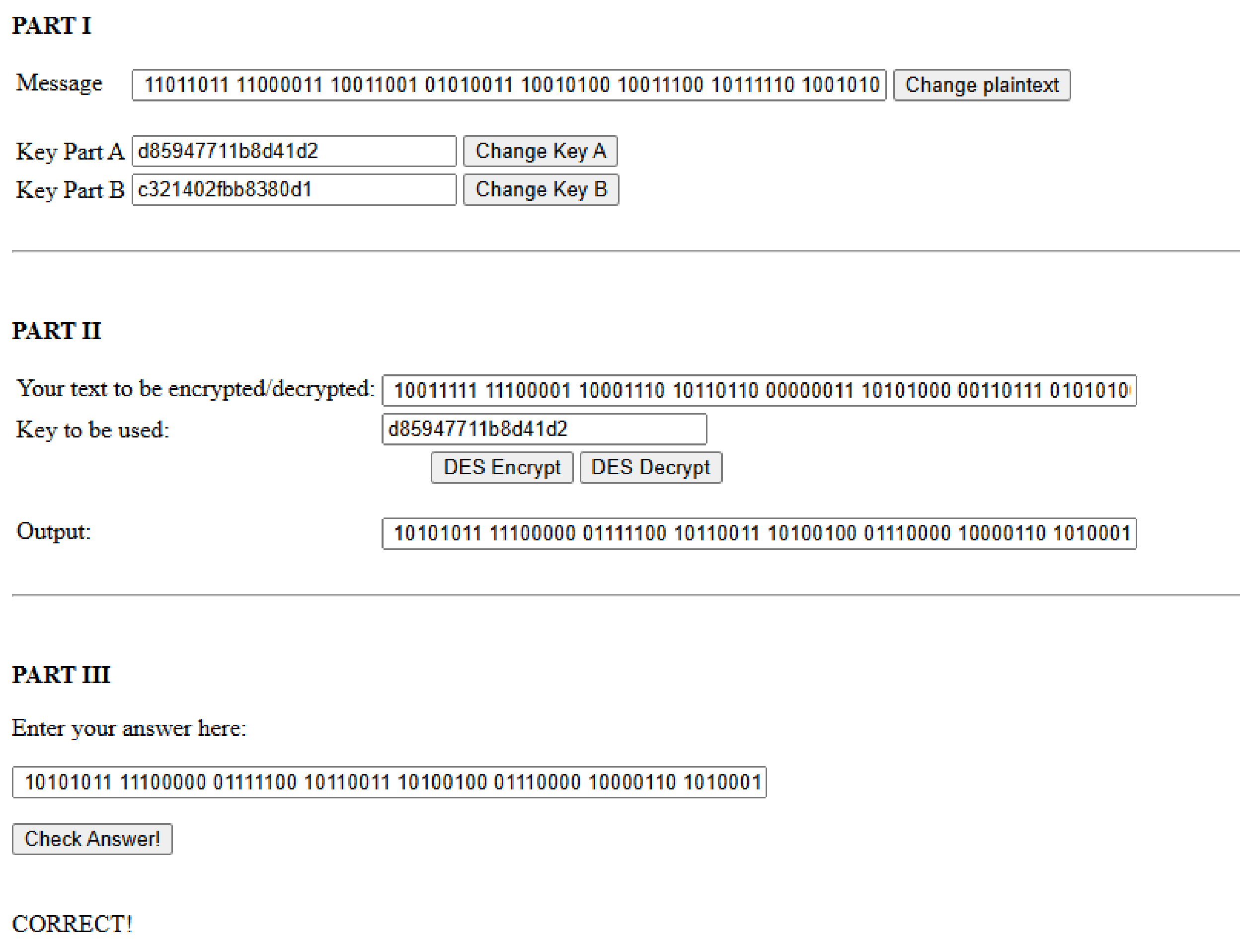
Output: 11011101 10000101 01010101 00110111 11110111 11010100 00101100 0001011

PART III

Enter your answer here:

11011101 10000101 01010101 00110111 11110111 11010100 00101100 0001011

CORRECT!



PART I

Message 11011011 11000011 10011001 01010011 10010100 10011100 10111110 1001010

Key Part A d85947711b8d41d2

Key Part B c321402fbb8380d1

PART II

Your text to be encrypted/decrypted: 10011111 11100001 10001110 10110110 00000011 10101000 00110111 0101010

Key to be used: d85947711b8d41d2

Output: 10101011 11100000 01111100 10110011 10100100 01110000 10000110 1010001

PART III

Enter your answer here:

10101011 11100000 01111100 10110011 10100100 01110000 10000110 1010001

CORRECT!

Output/ program results after execution:

Post Lab Subjective/Objective type Questions:

1. Explain what is two key and there key triple DES

   Triple DES (3DES) is a symmetric encryption algorithm that applies the DES cipher three times to each data block to enhance security.

   Two-Key Triple DES

- **Keys Used**: K1 and K2 (K1 ≠ K2)

- **Encryption Steps**:
  1. Encrypt the plaintext with K1
  2. Decrypt the result with K2
  3. Encrypt again with K1
- **Notation**: E(K1, D(K2, E(K1, plaintext)))
- **Effective Key Length**: 112 bits (since each DES key is 56 bits)
- **Purpose**: Provides stronger security than single DES while being more efficient than full three-key 3DES

Three-Key Triple DES

- **Keys Used**: K1, K2, and K3 (all distinct)
- **Encryption Steps**:
  1. Encrypt the plaintext with K1
  2. Decrypt the result with K2
  3. Encrypt again with K3
- **Notation**: E(K3, D(K2, E(K1, plaintext)))
- **Effective Key Length**: 168 bits
- **Purpose**: Offers maximum security in the Triple DES family

2. Explain Avalanche Effect in DES?
   The Avalanche Effect is a critical property of secure cryptographic algorithms. It refers to the phenomenon where a small change in the input (such as flipping a single bit) results in a significant and unpredictable change in the output.
   In DES:

   - DES uses 16 rounds of Feistel structure, along with substitution and permutation operations.
   - A one-bit change in the plaintext or key typically causes about half of the output bits to change.
   - This ensures:

   - High confusion and diffusion

Example:

- Original plaintext: `1010101010101010...`
- Modified plaintext (1 bit flipped): `1010101010101011...`
- Resulting ciphertexts: Completely different

Conclusion:

The experiment provided a clear understanding of converting a DES implementation into a triple-DES by applying encryption-decryption-encryption (EDE) with multiple keys. This approach enhances security by mitigating vulnerabilities inherent in single DES encryption.

Signature of faculty in-charge with Date: