DEPARTMENT OF COMPUTER ENGINEERING

Semester	T.E. Semester VI – Computer Engineering
Subject	Cryptography and cyber security
Subject Professor In-charge	Prof. Amit Nerurkar
Assisting Teachers	Prof. Amit Nerurkar
Laboratory	M312B

Student Name	Deep Salunkhe
Roll Number	21102A0014
TE Division	A

Title: **Design and Implementation of DES (Symmetric Key Encryption)**

Roll No: 21102A0014

Title:

Design and Implementation of DES (Symmetric Key Encryption)

Explanation:

DES (Data Encryption Standard) is a symmetric key encryption algorithm that was developed in the 1970s by IBM and eventually adopted by the U.S. government as a federal standard for encrypting sensitive but unclassified information. It has since been widely used in various applications, although its security is now considered inadequate against modern cryptographic attacks due to its relatively short key length of 56 bits.

Here's an overview of DES and its types:

1. DES (Data Encryption Standard) :

   - The original DES algorithm operates on 64-bit blocks of plaintext using a 56-bit key. It goes through a series of 16 rounds of substitution and permutation (known as the Feistel cipher structure) to produce the ciphertext. Each round uses a different 48-bit subkey derived from the original 56-bit key.

   - Despite its widespread use in the past, DES is now considered insecure against brute-force attacks due to its small key space. It is vulnerable to attacks that exploit its short key length, such as exhaustive key search.

2. 3DES (Triple DES) :

   - To address the security weaknesses of DES, 3DES was introduced. It applies the DES algorithm three times sequentially, using two or three different keys. The three-key variant of 3DES provides significantly stronger security than DES, as it effectively uses a key length of 168 bits (three 56-bit keys).

   - While 3DES improves security, it is slower and requires more computational resources compared to DES due to the increased number of rounds.

3. DES Variants and Modes :

- DESX : A variant of DES that involves XORing the plaintext with some key material before and after encryption. This is used to increase resistance against certain attacks.

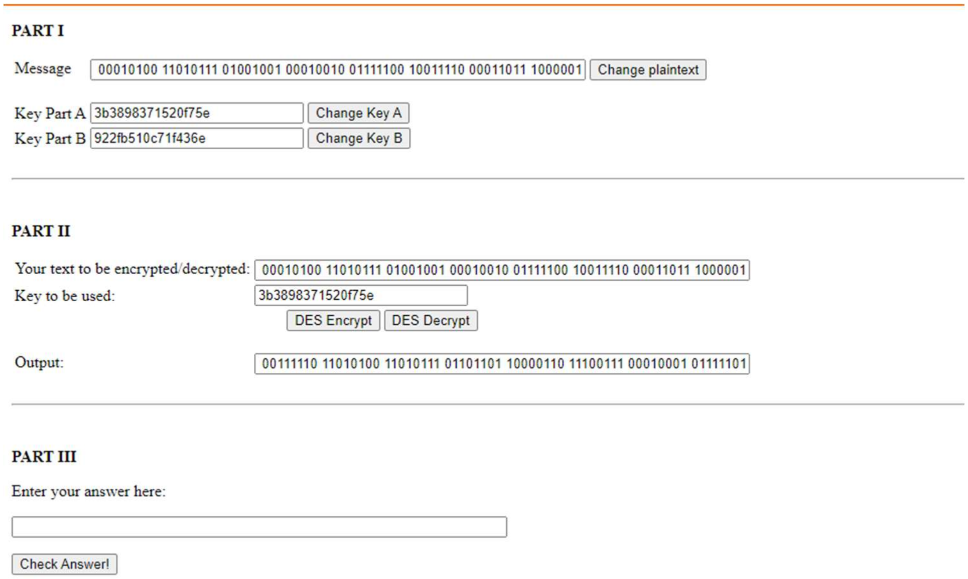
- Modes of Operation : DES can be used in different modes of operation, such as ECB (Electronic Codebook), CBC (Cipher Block Chaining), CFB (Cipher Feedback), OFB (Output Feedback), and CTR (Counter). These modes dictate how the encryption process is applied to plaintext blocks, and they have implications for security and performance in different scenarios.

4. DES Cryptanalysis:

- Over the years, various cryptanalytic techniques have been developed to exploit weaknesses in DES. Differential and linear cryptanalysis are among the most notable techniques used to analyze the security of DES and its variants.

- These attacks exploit patterns in plaintext-ciphertext pairs to recover the encryption key or reduce the effective key space, thereby making brute-force attacks more feasible.

Result:



PART I

Message: 00010100 11010111 01001001 00010010 01111100 10011110 00011011 1000001

Key Part A: 3b3898371520f75e

Key Part B: 922fb510c71f436e

PART II

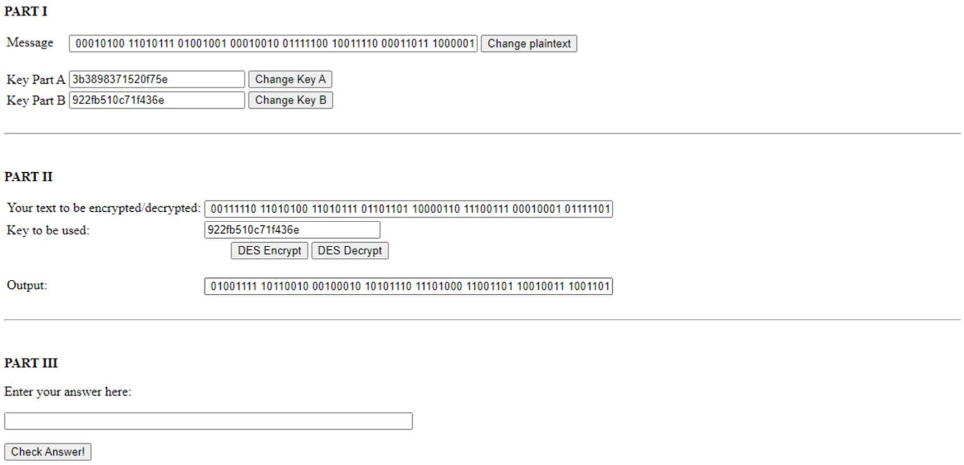
Your text to be encrypted/decrypted: 00010100 11010111 01001001 00010010 01111100 10011110 00011011 1000001

Key to be used: 3b3898371520f75e

Output: 00111110 11010100 11010111 01101101 10000110 11100111 00010001 01111101

PART III

Enter your answer here:



PART I

Message 00010100 11010111 01001001 00010010 01111100 10011110 00011011 1000001

Key Part A 3b3898371520f75e

Key Part B 922fb510c71f436e

PART II

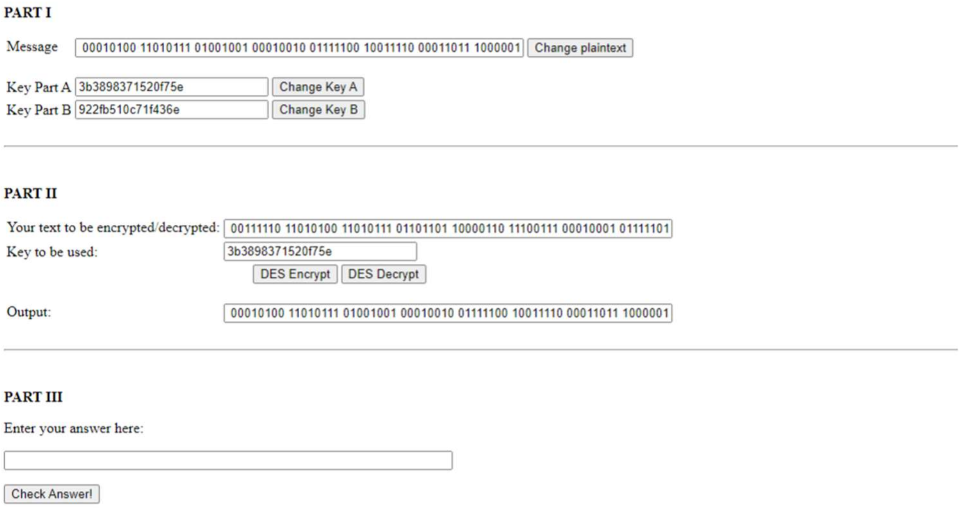
Your text to be encrypted/decrypted: 00111110 11010100 11010111 01101101 10000110 11100111 00010001 01111101

Key to be used: 922fb510c71f436e

Output: 01001111 10110010 00100010 10101110 11101000 11001101 10010011 1001101

PART III

Enter your answer here:



PART I

Message 00010100 11010111 01001001 00010010 01111100 10011110 00011011 1000001

Key Part A 3b3898371520f75e

Key Part B 922fb510c71f436e

PART II

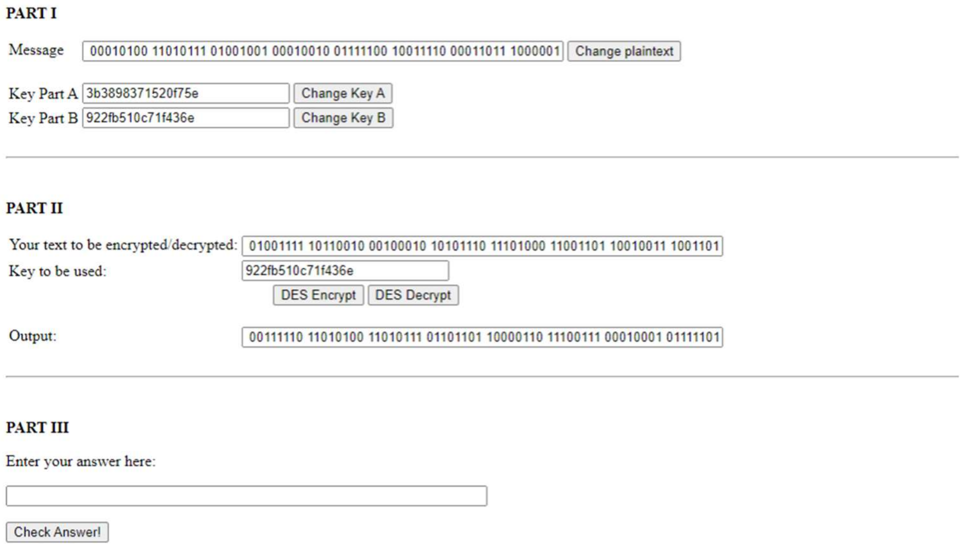
Your text to be encrypted/decrypted: 00111110 11010100 11010111 01101101 10000110 11100111 00010001 01111101

Key to be used: 3b3898371520f75e

Output: 00010100 11010111 01001001 00010010 01111100 10011110 00011011 1000001

PART III

Enter your answer here:



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: 01001111 10110010 00100010 10101110 11101000 11001101 10010011 1001101

Key to be used: 922fb510c71f436e

Output: 00111110 11010100 11010111 01101101 10000110 11100111 00010001 01111101

PART III

Enter your answer here:

Conclusion:

In conclusion, DES (Data Encryption Standard) is a foundational symmetric key encryption algorithm that has been widely used for decades. However, its security is now inadequate due to its small key size of 56 bits, which makes it vulnerable to brute-force attacks. To address these weaknesses, variants like Triple DES (3DES) were introduced, which apply the DES algorithm multiple times with different keys. Despite this, 3DES is slower and less efficient compared to modern encryption standards.