Course Name:	Applied Cryptography	Semester:	IV
Date of Performance:	25 / 08 / 2005	DIV/ Batch No:	AC2
Student Name:	Aaryan Sharma	Roll No:	16010123012

Experiment No:4
Title: Understanding Symmetric Key Cryptography Algorithms (DES and AES)

Aim and Objective of the Experiment:

Understanding Symmetric key cryptography algorithms (DES and AES) using, Virtual Lab:

1. https://cse29-iiith.vlabs.ac.in/exp/des/
2. https://cse29-iiith.vlabs.ac.in/exp/aes/

COs to be achieved:

CO2: Demonstrate and implement various Cryptographic Algorithms for securing systems.

Books/ Journals/ Websites referred:

1. Stallings, W., Cryptography and Network Security: Principles and Practice, Second edition, Person Education
2. Forouzan, B. A. (2018). Cryptography and Network Security. McGraw-Hill Education.
3. https://cse29-iiith.vlabs.ac.in/exp/des/docs/DES1.pdf

Theory: Explain the following.

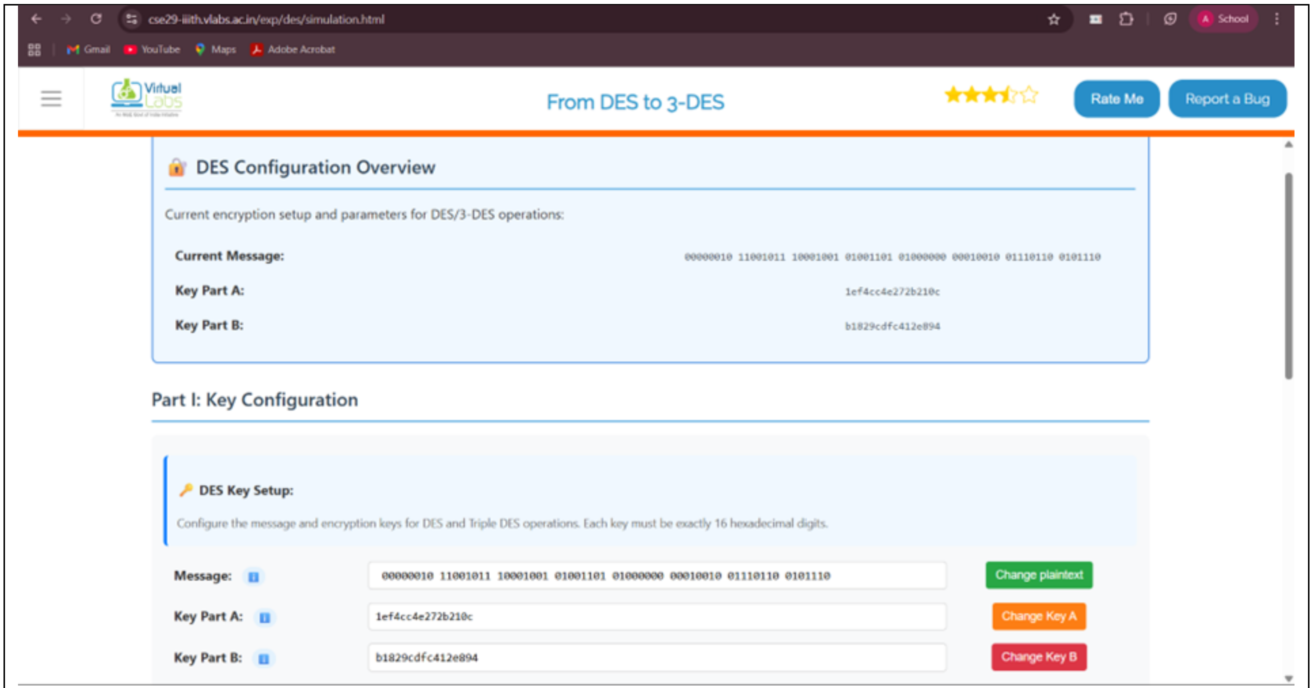
Symmetric key cryptography:

- Symmetric key cryptography concepts: Fiestel and non-Fiestel ciphers, confusion, diffusion
- The basic structure of a DES, 3DES (diagrams)
- Basic structure of AES.

Code and Output :

Refer to the virtual Lab for theory and simulation **https://cse29-iiith.vlabs.ac.in**

1. Screenshots: DES execution step by step, simulation, assignment



From DES to 3-DES

DES Configuration Overview

Current encryption setup and parameters for DES/3-DES operations:

Current Message:	00000010 11001011 10001001 01001101 01000000 00010010 01110110 0101110
Key Part A:	1ef4cc4e272b210c
Key Part B:	b1829cdfc412e894

Part I: Key Configuration

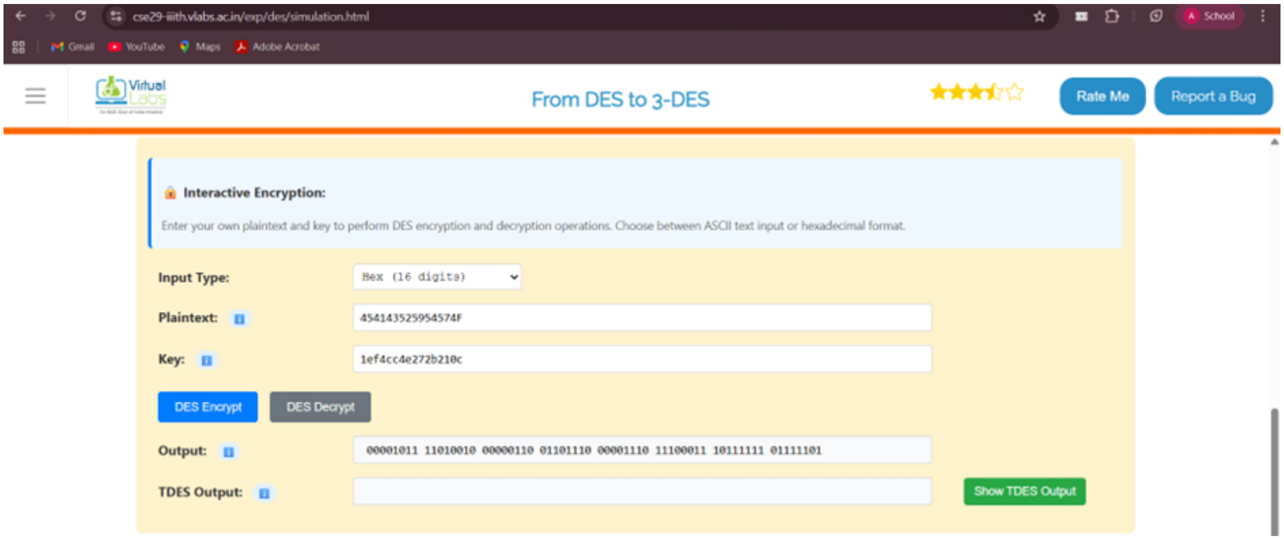
DES Key Setup:

Configure the message and encryption keys for DES and Triple DES operations. Each key must be exactly 16 hexadecimal digits.

Message: 00000010 11001011 10001001 01001101 01000000 00010010 01110110 0101110

Key Part A: 1ef4cc4e272b210c

Key Part B: b1829cdfc412e894



From DES to 3-DES

Interactive Encryption:

Enter your own plaintext and key to perform DES encryption and decryption operations. Choose between ASCII text input or hexadecimal format.

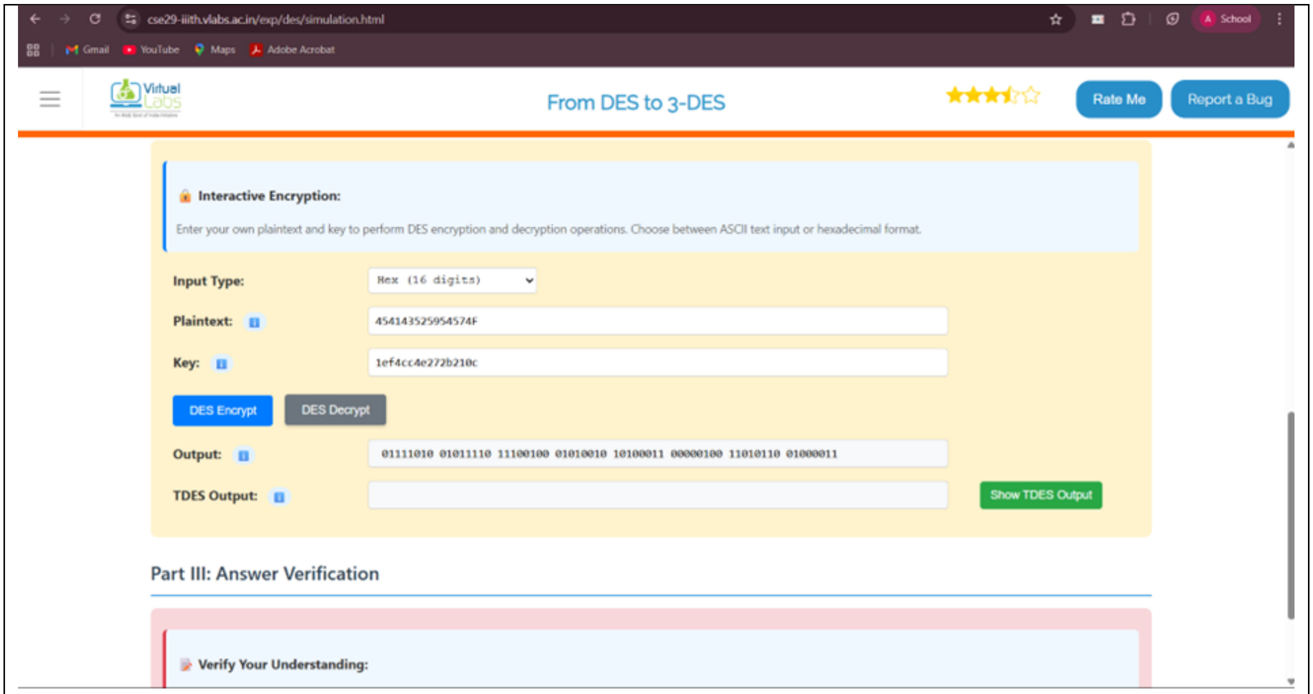
Input Type: Hex (16 digits)

Plaintext: 454143525954574F

Key: 1ef4cc4e272b210c

Output: 00001011 11010010 00000110 01101110 00001110 11100011 10111111 01111101

TDES Output:



From DES to 3-DES

Interactive Encryption:

Enter your own plaintext and key to perform DES encryption and decryption operations. Choose between ASCII text input or hexadecimal format.

Input Type: Hex (16 digits)

Plaintext: 454143525954574F

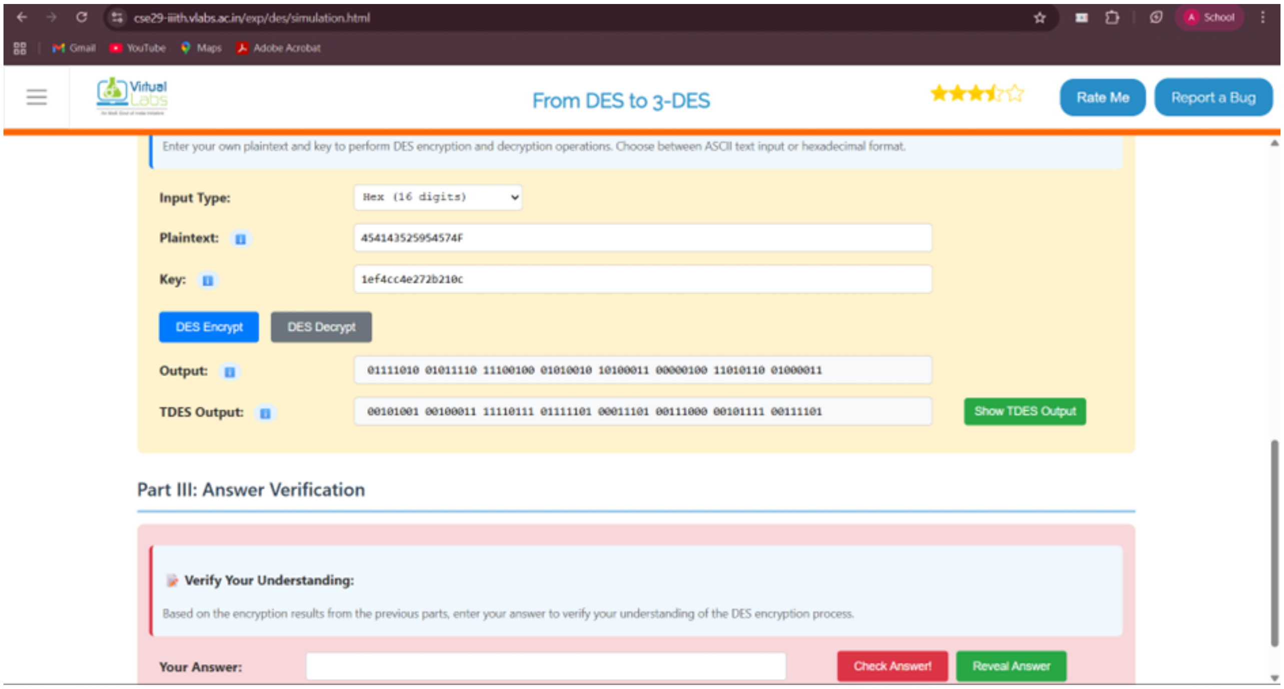
Key: 1ef4cc4e272b210c

Output: 01111010 01011110 11100100 01010010 10100011 00000100 11010110 01000011

TDES Output:

Part III: Answer Verification

Verify Your Understanding:



From DES to 3-DES

Enter your own plaintext and key to perform DES encryption and decryption operations. Choose between ASCII text input or hexadecimal format.

Input Type: Hex (16 digits)

Plaintext: 454143525954574F

Key: 1ef4cc4e272b210c

Output: 01111010 01011110 11100100 01010010 10100011 00000100 11010110 01000011

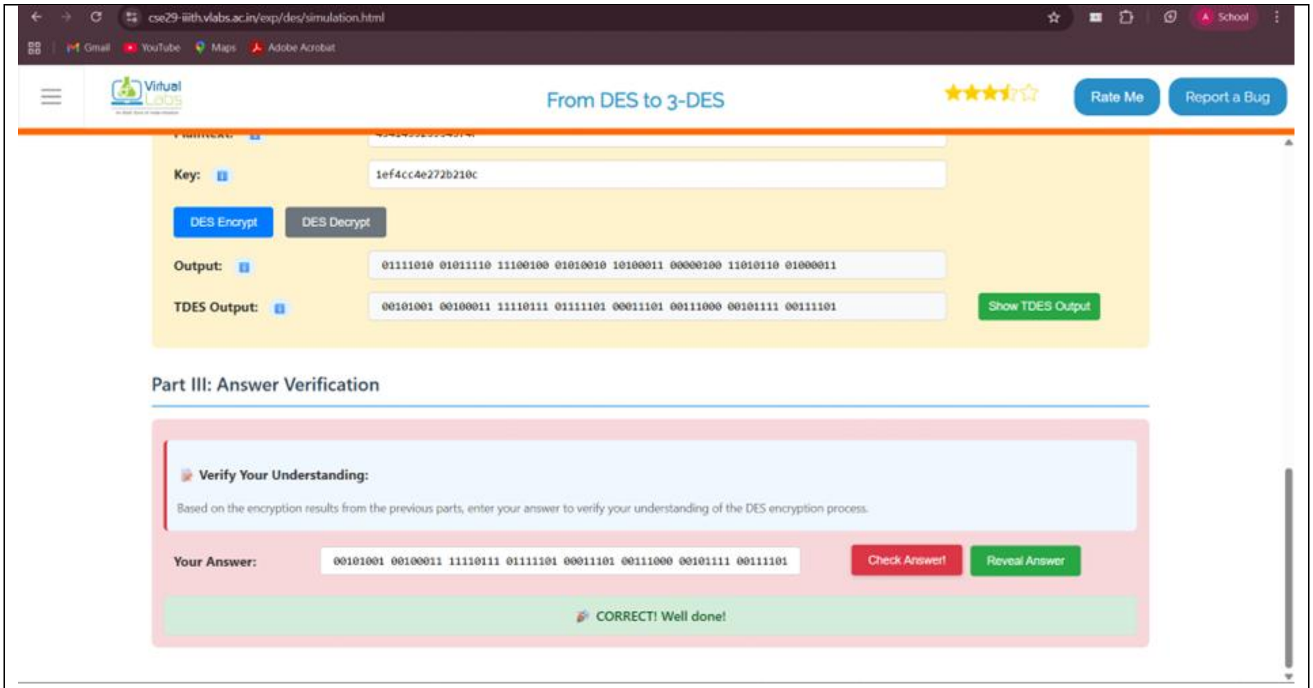
TDES Output: 00101001 00100011 11110111 01111101 00011101 00111000 00101111 00111101

Part III: Answer Verification

Verify Your Understanding:

Based on the encryption results from the previous parts, enter your answer to verify your understanding of the DES encryption process.

Your Answer:



From DES to 3-DES

Key: 1ef4cc4e272b210c

Output: 01111010 01011110 11100100 01010010 10100011 00000100 11010110 01000011

TDES Output: 00101001 00100011 11110111 01111101 00011101 00111000 00101111 00111101

Part III: Answer Verification

Verify Your Understanding:

Based on the encryption results from the previous parts, enter your answer to verify your understanding of the DES encryption process.

Your Answer: 00101001 00100011 11110111 01111101 00011101 00111000 00101111 00111101

CORRECT! Well done!

1. **In DES input, key length ___ bits and plaintext length ____ bits.**

   (a) 56 bit key length, 64 bit plaintext

   (b) 56 bit key length, 120 bit plaintext

   (c) 64 bit key length, 120 bit plaintext

   (d) 64 bit key length, 64 bit plaintext

2. **DES stands for _________ and AES stands for __________**

   (a) Data Encryption software, Advanced Encryption Software

   (b) Data Encryption Standard, Advanced Encryption Standard

   (c) Data Encryption System, Advanced Encryption System

   (d) None

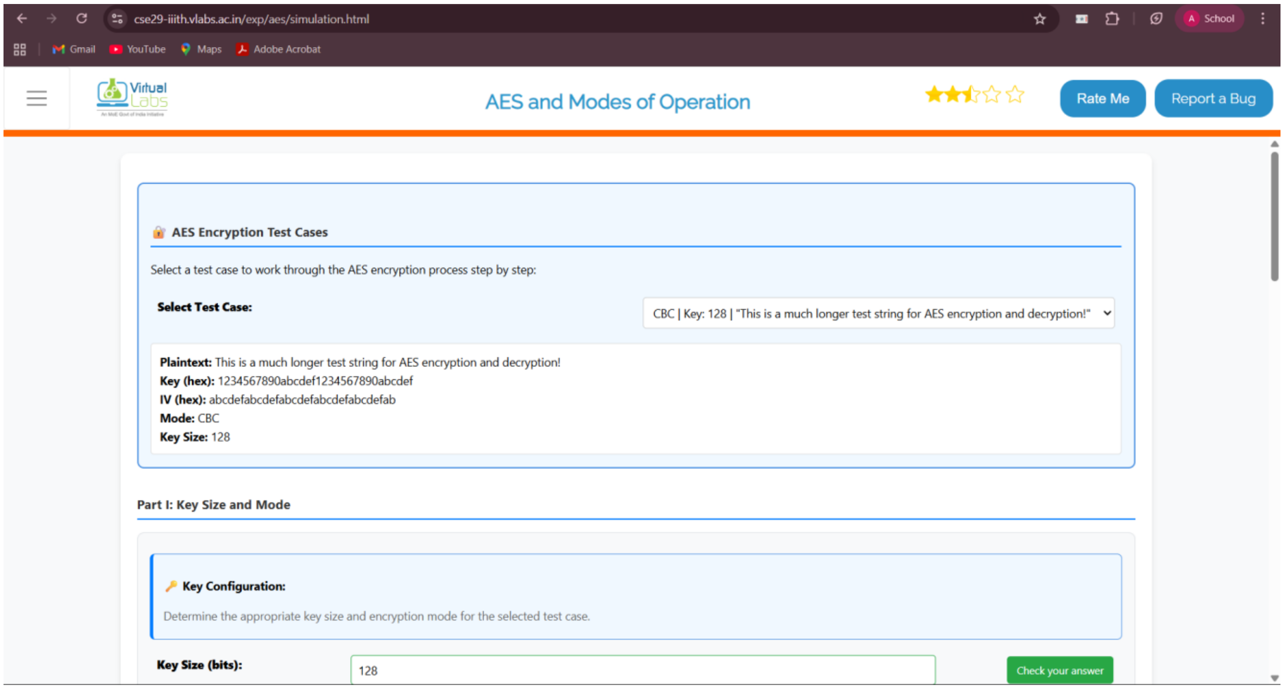
3. **DES has an initial and final permutation block and ____ rounds**

   (a) 14 (b) 16 (c) 8 (d) 12

4. **In DES the length of each round key?**

   (a) 16 bit (b) 32 bit (c) 54 bit (d) 48 bit

2. Screenshots: AES execution step by step, simulation, assignment



AES and Modes of Operation

AES Encryption Test Cases

Select a test case to work through the AES encryption process step by step:

Select Test Case: CBC | Key: 128 | "This is a much longer test string for AES encryption and decryption!"

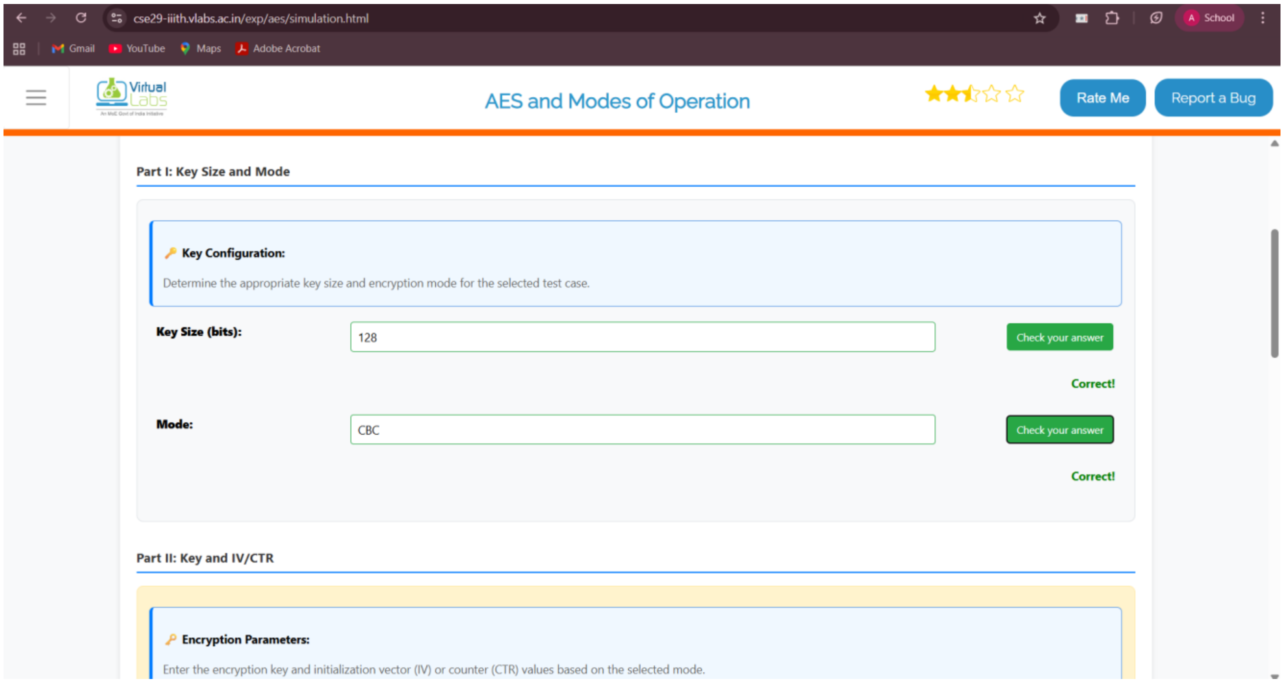
Plaintext: This is a much longer test string for AES encryption and decryption!
Key (hex): 1234567890abcdef1234567890abcdef
IV (hex): abcdefabcdefabcdefabcdefabcdefab
Mode: CBC
Key Size: 128

Part I: Key Size and Mode

Key Configuration:

Determine the appropriate key size and encryption mode for the selected test case.

Key Size (bits): 128 Check your answer



AES and Modes of Operation

Part I: Key Size and Mode

Key Configuration:

Determine the appropriate key size and encryption mode for the selected test case.

Key Size (bits): 128 Check your answer

Correct!

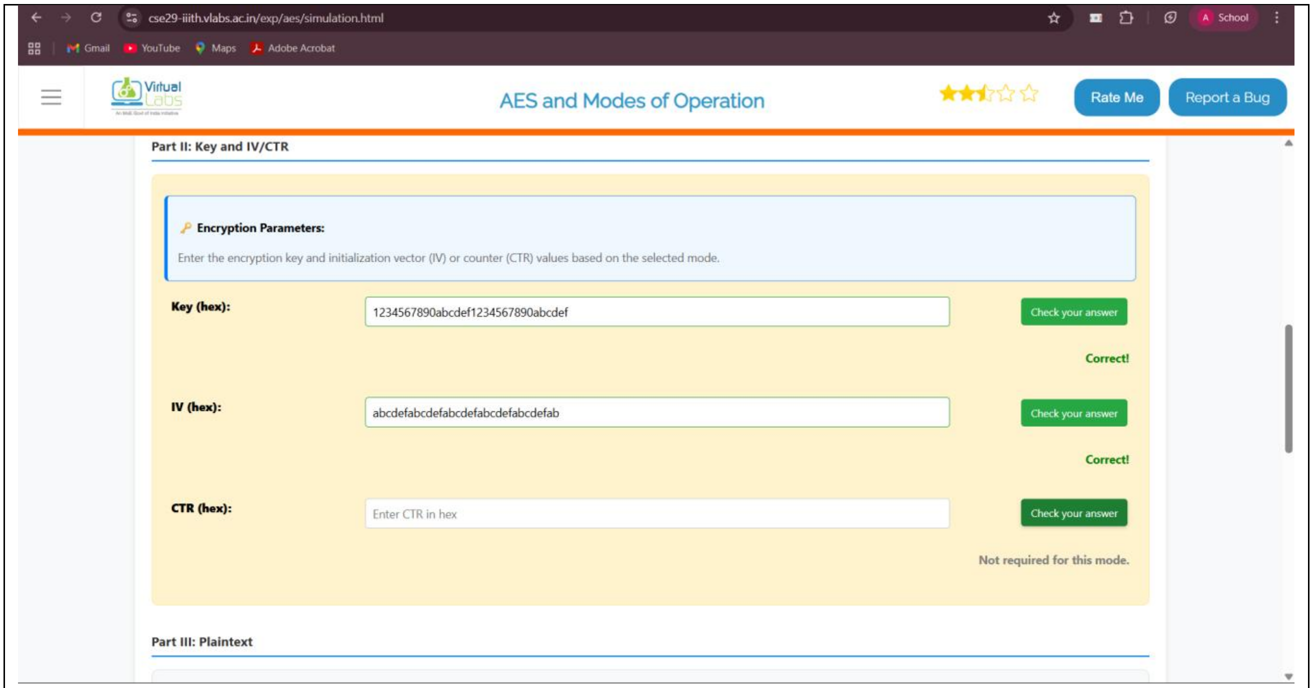
Mode: CBC Check your answer

Correct!

Part II: Key and IV/CTR

Encryption Parameters:

Enter the encryption key and initialization vector (IV) or counter (CTR) values based on the selected mode.



AES and Modes of Operation

Part II: Key and IV/CTR

Encryption Parameters:

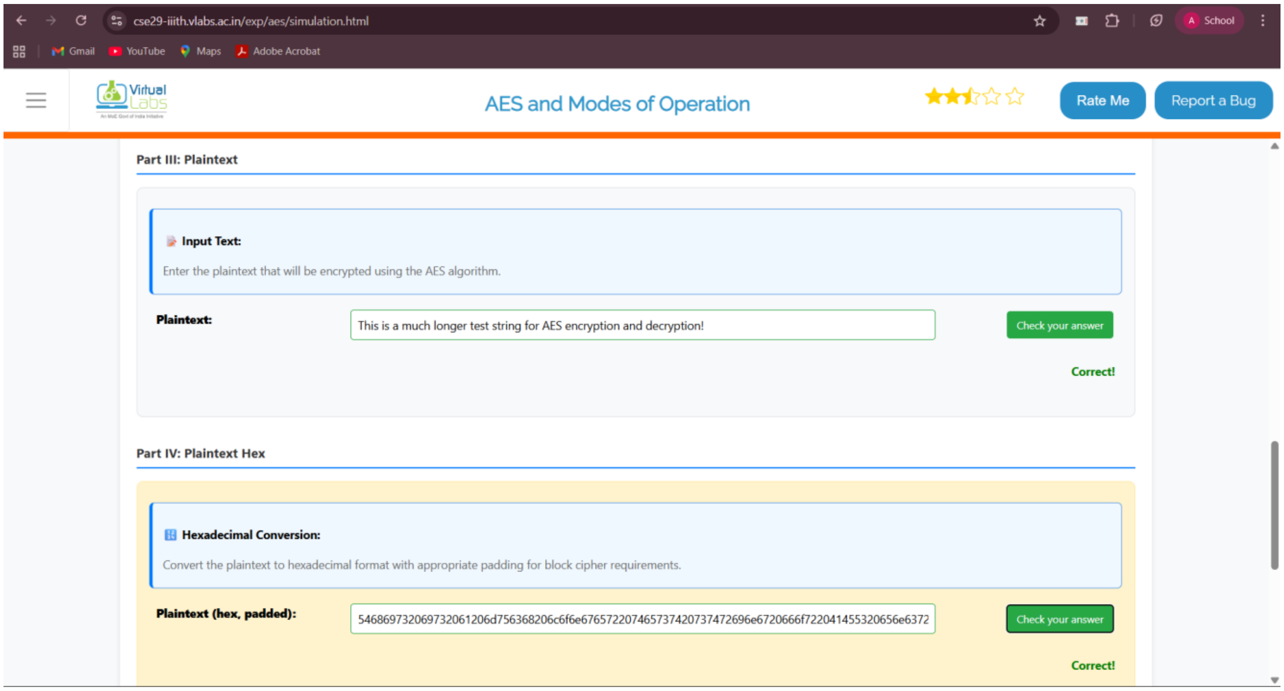
Enter the encryption key and initialization vector (IV) or counter (CTR) values based on the selected mode.

Key (hex): 1234567890abcdef1234567890abcdef — Check your answer — Correct!

IV (hex): abcdefabcdefabcdefabcdefabcdefab — Check your answer — Correct!

CTR (hex): Enter CTR in hex — Check your answer — Not required for this mode.

Part III: Plaintext



AES and Modes of Operation

Part III: Plaintext

Input Text:

Enter the plaintext that will be encrypted using the AES algorithm.

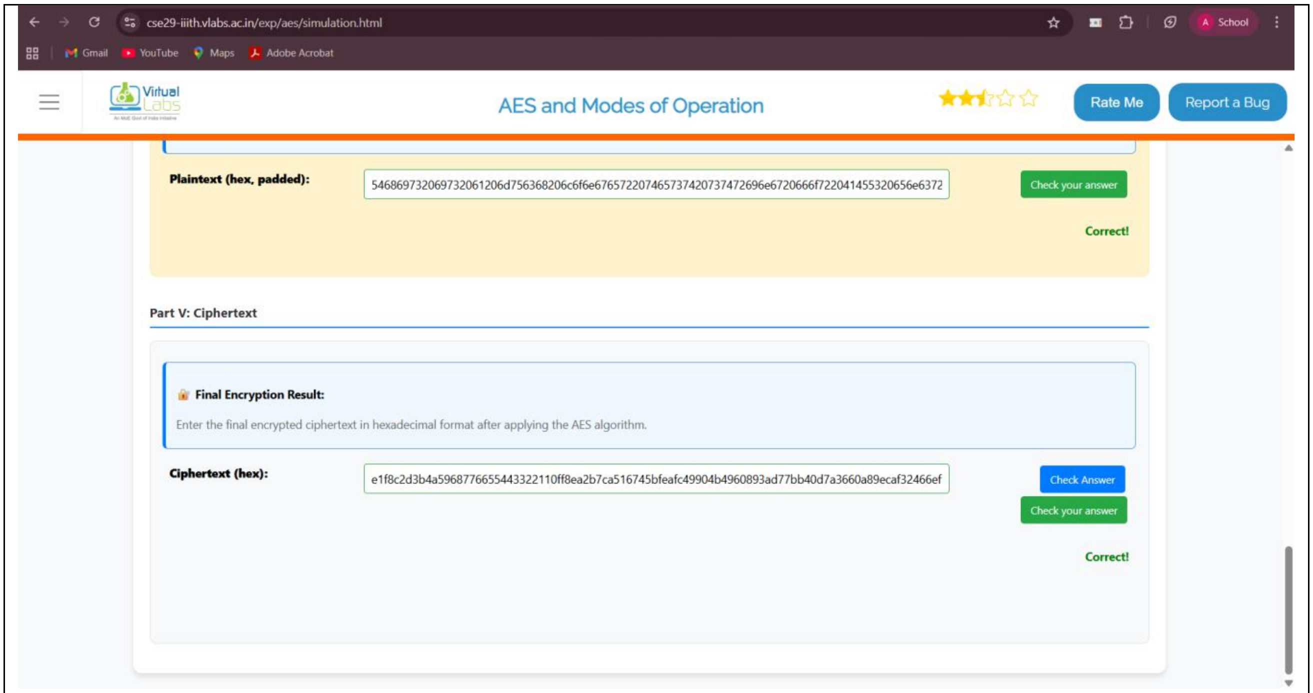
Plaintext: This is a much longer test string for AES encryption and decryption! — Check your answer — Correct!

Part IV: Plaintext Hex

Hexadecimal Conversion:

Convert the plaintext to hexadecimal format with appropriate padding for block cipher requirements.

Plaintext (hex, padded): 546869732069732061206d756368206c6f6e676572207465737420737472696e6720666f722041455320656e6372 — Check your answer — Correct!


cse29-iiith.vlabs.ac.in/exp/aes/simulation.html
Gmail
YouTube
Maps
Adobe Acrobat
School
Virtual Labs
AES and Modes of Operation
Rate Me
Report a Bug

Plaintext (hex, padded): 546869732069732061206d756368206c6f6e676572207465737420737472696e6720666f722041455320656e6372

Check your answer

Correct!

Part V: Ciphertext

🔒 **Final Encryption Result:**

Enter the final encrypted ciphertext in hexadecimal format after applying the AES algorithm.

Ciphertext (hex): e1f8c2d3b4a5968776655443322110ff8ea2b7ca516745bfeafc49904b4960893ad77bb40d7a3660a89ecaf32466ef

Check Answer

Check your answer

Correct!

1. **ECB stands for**

   (a) Electronic cipher Block

   (b) Electronic code Block

   (c) Electronic code Book

   (d) Electronic cipher Book

2. **Which among the following is not CPA secure?**

   (a) ECB (b) CBC (c) CFB (d) None

3. **Which of the following are block ciphers?**

   (a) ECB (b) CBC (c) CFB (d) All

4. **Which is the fastest mode of operation among four modes of operation? -** CTR

5. **Which mode of operation is more secure? -** CBC and CTR

6. **What is the importance of Initialization Vector(IV) and CTR?**

   Vector ensures that encrypting the same plaintext twice produces different ciphertexts, preventing pattern leakage. CTR converts a block cipher into a stream cipher using counters

+ IV, enabling parallel encryption and security under CPA.

7. **Why is ECB not CPA-secure and Why CBC is CPA-secure?**

ECB not CPA-secure: It deterministically maps identical plaintext blocks to identical ciphertext blocks, so an attacker can distinguish ciphertexts of chosen plaintexts.
CBC CPA-secure: CBC uses a random IV and chains blocks so that each ciphertext block depends on all previous plaintext blocks, making ciphertexts unpredictable.

8. **Suppose IV is not random, then is CBC and OFB mode both secure?**

CBC is not secure if IV is predictable. An attacker can craft chosen plaintexts for the first block. OFBis not secure if IV is not random. A fixed IV leads to the same keystream, turning OFB into a simple XOR with a repeated key, making it vulnerable.

Post Lab Subjective/Objective type Questions:

1. **Compare and contrast AES/DES**

AES (Advanced Encryption Standard) and DES (Data Encryption Standard) are both symmetric key block ciphers but differ significantly in design, security, and efficiency. DES uses a 64-bit block size with an effective 56-bit key and follows the Feistel network structure with 16 rounds of processing. Over time, DES became vulnerable to brute-force attacks due to its small key size and is now considered insecure for modern applications. AES replaced DES and is based on a substitution-permutation network rather than a Feistel structure. It operates on a 128-bit block size and supports key sizes of 128, 192, and 256 bits, offering much stronger security. AES is also faster and more efficient in both hardware and software implementations, making it suitable for modern encryption needs such as securing web communications, VPNs, and data storage. To conclude, while DES laid the foundation for block cipher encryption, AES addresses its shortcomings by providing superior security, scalability, and performance.

2. **Comment on the strengths and weaknesses of a symmetric key cryptosystem.**

Strengths of Symmetric Key Cryptosystems

1. Speed and Efficiency - Faster than asymmetric cryptography (public key) for large data.
2. Lower Computational - Requires less processing power; ideal for bulk data encryption.
3. Security - Algorithms like AES are thoroughly analyzed and trusted.
4. Confidentiality - Provides strong confidentiality if keys are managed properly.

Weaknesses of Symmetric Key Cryptosystems

1. Key Distribution Problem - Securely sharing the secret key between parties is challenging, especially over insecure channels.
2. Scalability Issues - For n users, n(n-1)/2 unique keys are needed (pairwise).
3. No Non-Repudiation - Since both parties share the same key, you cannot prove which one created a message.
4. Compromise of Key = Compromise of All Data - If the key is exposed, all communications encrypted with it are vulnerable.

Conclusion:

I have successfully completed this experiment on understanding symmetric key cryptography algorithms DES and AES using the virtual lab. Through this experiment, I learned the working principles, structure, and differences between DES and AES. I understood how DES uses a Feistel network with a smaller key size, making it less secure in modern applications, whereas AES uses a substitution-permutation network with larger key sizes, providing stronger security and efficiency.