CS 458
Assignment 3

Due in Canvas Assignment Friday, June 20th by **11:59** pm

Task 1: True/False Questions

1. True/False: Symmetric cryptography uses the same key for both encryption and decryption.
2. True/False: The security of a symmetric encryption system depends entirely on the secrecy of the encryption algorithm.
3. True/False: Stream ciphers encrypt data one bit or byte at a time, while block ciphers encrypt fixed-size blocks of data.
4. True/False: In a Feistel cipher, encryption and decryption processes are different.
5. True/False: The Advanced Encryption Standard (AES) is based on the Feistel structure.
6. True/False: The Electronic Codebook (ECB) mode is the most secure mode of operation for a block cipher.
7. True/False: Confusion and diffusion are the two main design principles of a secure block cipher.
8. True/False: The Data Encryption Standard (DES) uses a 128-bit key.
9. True/False: The Avalanche effect ensures that small changes in input produce large changes in output.
10. True/False: The Meet-in-the-Middle attack significantly weakens the security of Double DES.
11. True/False: AES uses a fixed number of rounds regardless of key size.
12. True/False: The Cipher Block Chaining (CBC) mode requires an initialization vector (IV) for encryption.
13. True/False: The Counter (CTR) mode of operation allows block ciphers to behave like stream ciphers.
14. True/False: Key distribution is a major challenge in symmetric cryptography.
15. True/False: The security of the DES algorithm was criticized due to its short key length of 56 bits.

Task 2: Multiple Choice Questions

1. Which of the following is NOT a requirement for secure symmetric encryption?

A) A strong encryption algorithm
B) Secure key exchange
C) A public key infrastructure
D) Confidentiality of the secret key

2. What is the primary weakness of the ECB mode?

A) It encrypts data in multiple rounds
B) Identical plaintext blocks produce identical ciphertext blocks
C) It requires an additional secret key for each block
D) It uses XOR for encryption

3. What is the purpose of the initialization vector (IV) in CBC mode?

A) To ensure identical plaintexts produce different ciphertexts

B) To serve as a secondary encryption key

C) To perform key expansion

D) To allow for parallel encryption

4. Which of the following is a feature of stream ciphers?

A) They encrypt data in fixed-size blocks

B) They are based on the Feistel network

C) They encrypt data bit-by-bit or byte-by-byte

D) They use multiple rounds of encryption

5. What is the main advantage of using the Feistel structure in encryption algorithms?

A) It allows decryption to use the same structure as encryption

B) It increases the speed of key exchange

C) It eliminates the need for subkeys

D) It ensures zero information leakage

6. How many rounds does AES-256 use in encryption?

A) 10

B) 12

C) 14

D) 16

7. What is a major disadvantage of DES?

A) It is too slow for modern applications

B) Its key length is too short for strong security

C) It requires asymmetric keys

D) It cannot be used in block cipher modes

8. Which attack is particularly effective against Double DES?

A) Brute-force attack

B) Differential cryptanalysis

C) Meet-in-the-Middle attack

D) Chosen-plaintext attack

9. Why was Triple DES (3DES) developed?

A) To replace DES with an algorithm that is 3 times faster

B) To extend the key length of DES and improve security

C) To eliminate the need for key exchange

D) To make encryption decryption independent

10. What is the primary function of the S-boxes in DES?

A) They perform bitwise permutations

B) They introduce non-linearity to enhance security

C) They generate key schedules

D) They increase the encryption speed

11. Which of the following is a key feature of AES compared to DES?

A) AES uses a Feistel structure

B) AES has a fixed key size of 128 bits

C) AES allows multiple key sizes and has no known vulnerabilities

D) AES uses a single encryption round

12. What is the primary role of the MixColumns step in AES?

A) It substitutes bytes using an S-box

B) It ensures diffusion by mixing input bytes across columns

C) It expands the encryption key

D) It performs permutation-only operations

13. What is the main reason why AES is preferred over DES today?

A) AES is more computationally expensive

B) AES has a significantly larger key space

C) AES was developed by IBM

D) AES is based on the Feistel network

14. Which mode of operation is best suited for encrypting large files while allowing random access to data?

A) ECB

B) CBC

C) CTR

D) OFB

15. What is the primary challenge in symmetric key cryptography?

A) Encrypting data securely

B) Generating strong keys

C) Distributing the secret key securely

D) Preventing key reuse

Task 3: Coding Report

1. Functionality of the Program

This program is a command-line encryption and decryption tool that allows the user to interact with a menu-driven interface, input plaintext, choose encryption techniques, and validate the encryption by manually re-entering the decryption key. It is designed to simulate real-world usage of classical cryptographic methods.

Supported Encryption Techniques:

1. Shift Cipher
2. Permutation Cipher
3. Simple Transposition
4. Double Transposition Cipher
5. Vigenère Cipher
6. AES / DES / 3DES Block Ciphers
7. Combination Tester for Block Ciphers with All Modes

2. Key Features

- Offers an interactive text-based menu for selecting among classical and modern ciphers.
- Accepts custom encryption keys, with validation, or defaults when applicable.
- Requires manual input for decryption keys, simulating secure key-handling workflows.
- Automatically converts all plaintext to uppercase for consistency across classical ciphers.
- Implements padding logic for block-based methods (e.g., Permutation, AES) to ensure block alignment.
- Validates user input and handles errors gracefully (e.g., key length, type mismatch).
- Includes a "Test All Block Cipher Combinations" mode to apply AES, DES, and 3DES with ECB, CBC, CFB, and OFB.
- Designed for educational use, allowing users to see encryption/decryption results across multiple techniques.

3. Instructions for Use Running the Program

1. Save the complete Python script as:

   MUKESH_A20580319.py

2. install the model using the terminal

   pip install pycryptodome

3. Open a terminal or any Python IDE and run:

   python MUKESH_A20580319.py

Program Workflow Step

1: Select a Cipher

- The menu displays seven options:
  - 1–5: Classical ciphers

    - 6: AES/DES/3DES with mode selection
    - 7: Combination test (AES/DES/3DES × ECB/CBC/CFB/OFB)
- Enter the corresponding number or 'q' to quit.

Step 2: Enter a Message

- Plaintext input must be at least 5 characters long.
- The input is converted to uppercase internally to normalize processing.

Step 3: Provide an Encryption Key

- The user is prompted to provide a key depending on the cipher:
    - Shift value (integer)
    - Permutation pattern (e.g., 2,0,1)
    - Vigenère keyword
    - Block cipher key (padded to 24 characters)

Step 4: View the Ciphertext

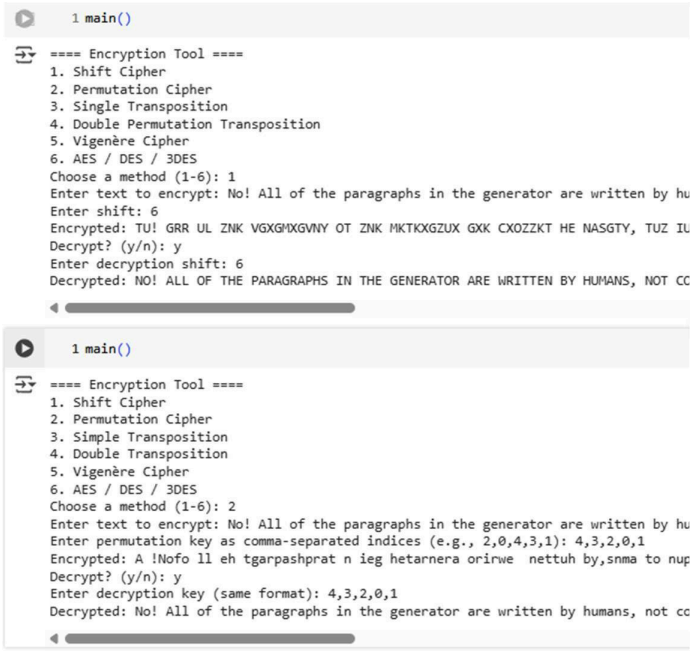
- The encrypted message is printed in a human-readable format.
- For block ciphers, the ciphertext is Base64 encoded.

Step 5: Manual Decryption

- The user is asked to re-enter the decryption key.
- The decrypted message is shown to validate that encryption and decryption were consistent.

1.Shift Cipher

2.Permutation Cipher



3.Simple Transposition

4.Double Transposition Cipher

```
[26]    1 main()

==== Encryption Tool ====
1. Shift Cipher
2. Permutation Cipher
3. Single Transposition
4. Double Permutation Transposition
5. Vigenère Cipher
6. AES / DES / 3DES
Choose a method (1-6): 3
Enter text to encrypt: No! All of the paragraphs in the generator are written by hur
Enter number of rails: 4
Encrypted: Nlhashe r mnmsntdhnrh   torhas wt anenk  ltoo tarhclr ao e wlol tergh ter
Decrypt? (y/n): y
Enter rails used for decryption: 4
Decrypted: No! All of the paragraphs in the generator are written by humans, not cor
```

```
[28]    1 main()

==== Encryption Tool ====
1. Shift Cipher
2. Permutation Cipher
3. Single Transposition
4. Double Permutation Transposition
5. Vigenère Cipher
6. AES / DES / 3DES
Choose a method (1-6): 4
Enter text to encrypt: No! All of the paragraphs in the generator are written by hur
Enter first permutation key: 1,3,0,2
Enter second permutation key: 2,3,1,0
Encrypted: N! oAl lo tfh peaagrrphasin  het engeatro arr werttie bnyhu mnsa,no tco r
Decrypt? (y/n): y
Enter first decryption key: 1,3,0,2
Enter second decryption key: 2,3,1,0
Decrypted: No! All of the paragraphs in the generator are written by humans, not cor
```

4. VigenèreCipher

5. AES x ECB

```
1 main()

==== Encryption Tool ====
1. Shift Cipher
2. Permutation Cipher
3. Single Transposition
4. Double Permutation Transposition
5. Vigenère Cipher
6. AES / DES / 3DES
Choose a method (1-6): 5
Enter text to encrypt: No! All of the paragraphs in the generator are written by huma
Enter Vigenère key: ironmanmukesh
Encrypted: VF! MLY IP LOM DNDATDUZLK QE GTE SYXIJHBFF MRR QBMLAME OK UGGKRK, ECG CBYJ
Decrypt? (y/n): y
Enter decryption key: ironmanmukesh
Decrypted: NO! ALL OF THE PARAGRAPHS IN THE GENERATOR ARE WRITTEN BY HUMANS, NOT COMP
```

```
1 main()

==== Encryption Tool ====
1. Shift Cipher
2. Permutation Cipher
3. Single Transposition
4. Double Permutation Transposition
5. Vigenère Cipher
6. AES / DES / 3DES
Choose a method (1-6): 6
Enter text to encrypt: No! All of the paragraphs in the generator are written by huma
1. AES
2. DES
3. 3DES
Choose algorithm (1-3): 1
1. ECB
2. CBC
3. CFB
4. OFB
Choose mode (1-4): 1
Enter encryption key (padded to 24 chars): ironMAN@2003
Encrypted: XpovBnUZwT91R2MwHF4O5XdsCf9Yb8mIMg4/A+mQtTmuyPukw/GDTuO+v7FMq9IuR2NKYe/CU8
Decrypt? (y/n): y
Enter decryption key (same padding): ironMAN@2003
Decrypted: No! All of the paragraphs in the generator are written by humans, not comp
```

6. DES x CBC

7. 3DES x CFB

```
1 main()

==== Encryption Tool ====
1. Shift Cipher
2. Permutation Cipher
3. Single Transposition
4. Double Permutation Transposition
5. Vigenère Cipher
6. AES / DES / 3DES
Choose a method (1-6): 6
Enter text to encrypt: No! All of the paragraphs in the generator are written by hum
1. AES
2. DES
3. 3DES
Choose algorithm (1-3): 2
1. ECB
2. CBC
3. CFB
4. OFB
Choose mode (1-4): 2
Enter encryption key (padded to 24 chars): ironMAN@2003
Encrypted: +O9jLI3Nsp9T7cuGseU/ZUiKHmUcoRoy1Lk/PO+6ovRGoq/kg5bXSAxNpLNCGL+SvPlFO4Jgt
Decrypt? (y/n): y
Enter decryption key (same padding): ironMAN@2003
Decrypted: No! All of the paragraphs in the generator are written by humans, not com
```

```
[33]  1 main()

==== Encryption Tool ====
1. Shift Cipher
2. Permutation Cipher
3. Single Transposition
4. Double Permutation Transposition
5. Vigenère Cipher
6. AES / DES / 3DES
Choose a method (1-6): 6
Enter text to encrypt: No! All of the paragraphs in the generator are written by hum
1. AES
2. DES
3. 3DES
Choose algorithm (1-3): 3
1. ECB
2. CBC
3. CFB
4. OFB
Choose mode (1-4): 3
Enter encryption key (padded to 24 chars): ironMAN@2003
Encrypted: avG+AT9NpotrZLve1TdRrRgcHK7r+zttq5EYOPnAlYYq8sNroleXXJnwkW3ViFqnUUphLev0h
Decrypt? (y/n): y
Enter decryption key (same padding): ironMAN@2003
Decrypted: No! All of the paragraphs in the generator are written by humans, not com
```

8. AES x OFB

```
1 main()

==== Encryption Tool ====
1. Shift Cipher
2. Permutation Cipher
3. Single Transposition
4. Double Permutation Transposition
5. Vigenère Cipher
6. AES / DES / 3DES
Choose a method (1-6): 6
Enter text to encrypt: No! All of the paragraphs in the generator are written by h
1. AES
2. DES
3. 3DES
Choose algorithm (1-3): 1
1. ECB
2. CBC
3. CFB
4. OFB
Choose mode (1-4): 4
Enter encryption key (padded to 24 chars): ironMAN@2003
Encrypted: BK7RIaRgi3oKFKER+9OdjiA2oiR/DBjqQCOH0/vEP9sxBfwkJnlLAlWk9PuS81UZNJZNMfl
Decrypt? (y/n): y
Enter decryption key (same padding): ironMAN@2003
Decrypted: No! All of the paragraphs in the generator are written by humans, not c
```

9. Combination test (AES/DES/3DES × ECB/CBC/CFB/OFB)

```
Choose a method (1-7): 7

 Test All Combinations: AES, DES, 3DES x ECB, CBC, CFB, OFB
Enter plaintext to encrypt: No! All of the paragraphs in the generator are written by humans, not computers. When first
Enter encryption key (will be padded to 24 chars): ironman@2003

 AES + ECB
   Encrypted: 8dWfuBkXloMcpHSfxNMzFWw6GCESI+psA9efuzOr3TL4peZp+wreIC4NyB2q0et66XZ+Wpa4nounXOeRJ3RqoFHRdzdtfEjMwPls6MCYPs
   Decrypted: No! All of the paragraphs in the generator are written by humans, not computers. When first building this

 AES + CBC
   Encrypted: MPh5x+Haf4JpEh3ZOSFl7irDZI7HbXrQXbUXInEtnrnicfjdMauOYcbvMNrVdzph7hOQ2d0VpNWkwHPPIZbae3gWy59sbnXwJXlWa14BKKJ
   Decrypted: No! All of the paragraphs in the generator are written by humans, not computers. When first building this

 AES + CFB
   Encrypted: xXsZWLbgPA/ee5jr5Uo8NCqTHFkwhPb9zAT1bULemP2XR/v77CNd5F8iU/0PoouyKRDB8NyPhRIcuJZm/Q4CBGFLpQuqkfmn7Hdlfg/UPp
   Decrypted: No! All of the paragraphs in the generator are written by humans, not computers. When first building this

 AES + OFB
   Encrypted: xdnwmEr3Yj8yQjHRMkh6Uu7jtnQ7DP7V9x6hRMx1fGxe8BJ+ARZf6yrxJVhfoVg0O2v5LeZBsyEcApnUVWOAaxAO847J4sx3OCAT/CS41a
   Decrypted: No! All of the paragraphs in the generator are written by humans, not computers. When first building this

 DES + ECB
   Encrypted: lBnPDGtrrkA5S98ZaWAWmi4OdxJBMpaW/yQ3clbvI9DZNhdrzM5w9nkbwprq+EGzOgStzsTbq2lqXt3j2Cs3r+/fPwwtInyDO4OBexn5rE
   Decrypted: No! All of the paragraphs in the generator are written by humans, not computers. When first building this

 DES + CBC
   Encrypted: WGVyKi+cp9VQYFzVkFexmRyfcd77buoEXSicxsxFE+9PHhM4ih1vYlxkhqdL9ic643RbwPP2+KFL56B/LCiBr2Ulkr1hISave7yNuzQMta
   Decrypted: No! All of the paragraphs in the generator are written by humans, not computers. When first building this

 DES + CFB
   Encrypted: LgfQTxFyki5kjvc7hARWQ9J8T/4B1XwwBO7MWbd/jwXnlwBUdBM65fncTnTcvP5yvew31i+VoW13hLiu2mNdl4P8yV3R/K8bosVaKiNEGQ
   Decrypted: No! All of the paragraphs in the generator are written by humans, not computers. When first building this

 DES + OFB
   Encrypted: Lprq9YnYDb/KgGdilL38yuYX0VlLbNdxRUPkLO5D+T9Q0us5V8nC3rZ8mbmE/LEWFV7W/bL1MNte/OOgwtlFug1cIjM1tF7SK5hFrE6Cr
   Decrypted: No! All of the paragraphs in the generator are written by humans, not computers. When first building this

 3DES + ECB
   Encrypted: +mRBcV2UguSZadE2gyNaBKQvReSv5alJwgLuG8xB0GquVCkGO9OxSGJ6onHXMzApcvPznTeMYkKe7/u2/FsNzqPY/HLIMW2czQmOfRFJal
   Decrypted: No! All of the paragraphs in the generator are written by humans, not computers. When first building this

 3DES + CBC
   Encrypted: NaVAszrlJXpjSt4d5yeAMxD1phZAfYLOA5D9LZ2zAoHqBnlvmtA8EJDpHS3ZOemIioLMtmIApUNNgKJtRX+TFzWVQxNa4+ua6EJUgFkdgr
   Decrypted: No! All of the paragraphs in the generator are written by humans, not computers. When first building this

 3DES + CFB
   Encrypted: 6D3ZdOTu9FgXf8Awgc2qrhrP4hIMiTUisMFjJmyk5tZscP5yxvU36Va1cZiRyQCUbreu5T/9N/Yj7i8yCbNeKMdCRC6gPb8k95vna1hIKH
   Decrypted: No! All of the paragraphs in the generator are written by humans, not computers. When first building this

 3DES + OFB
   Encrypted: 6GC0tVzY92iAUqGMBCAZa5lLOxRnl927ECmtWiWyjJlOUe7CbKBK24psTsGb7ze5SZAP1sRRPCL3W0KVCMEEIBpwhiaSx6NLrHOn3J8Q3V
   Decrypted: No! All of the paragraphs in the generator are written by humans, not computers. When first building this
```

Combination test (AES/DES/3DES × ECB/CBC/CFB/OFB) was added much later to the code so the screenshot appears different

4. Observations and Challenges

- Shift and Rail Fence decryption requires precise numeric key re-entry. A wrong number will result in incorrect output.
- Permutation ciphers need exact index patterns; incorrect order breaks decryption.
- Block cipher modes (CBC, CFB, OFB) required careful handling of IVs; ECB mode is simpler but insecure.
- Error handling was essential for invalid key formats (e.g., entering letters instead of numbers).
- The Double Permutation cipher reinforced how layering simple operations can improve security.
- Allowing user-driven key input made the tool realistic but increased the need for input sanitization.

5. Conclusion

The program meets all core requirements:

- It supports five classical ciphers (Shift, Permutation, Simple Transposition, Double Transposition, and Vigenère), as well as modern block ciphers (AES, DES, 3DES) with four standard modes (ECB, CBC, CFB, OFB).
- The program provides a complete encryption-decryption workflow across classical and modern ciphers, allowing users to manually input keys, validate encryption through decryption, and explore cipher behavior with custom or default parameter ensuring realistic simulation.