CS 458 – Fall 2024
Introduction To Information Security
Assignment #2

Functionality

- **Shift Cipher**: A simple substitution cipher where each letter in the plaintext is shifted by a fixed number of positions.
- **Permutation Cipher**: Encrypts plaintext by rearranging the characters based on a provided key.
- **Simple Transposition Cipher**: Rearranges the plaintext by taking every second character first, followed by the remaining characters.
- **Double Transposition Cipher**: Applies the simple transposition cipher twice for enhanced security.
- **Vigenère Cipher**: A method of encrypting alphabetic text by using a simple form of polyalphabetic substitution based on a keyword.
- **AES**: A symmetric encryption standard that supports multiple modes of operation (OFB, CBC, CFB).
- **DES**: A symmetric key method for data encryption, also supporting multiple modes.
- **Triple DES**: An enhancement of DES that applies the DES algorithm three times to each data block, increasing security.

Encryption Modes for AES, DES, and 3DES

- **Output Feedback (OFB)**: Converts a block cipher into a synchronous stream cipher.
- **Cipher Block Chaining (CBC)**: Each block of plaintext is XORed with the previous ciphertext block before being encrypted.
- **Cipher Feedback (CFB)**: Similar to OFB, but each ciphertext block is fed back into the cipher to encrypt subsequent blocks.

Usage Instructions

1. **Run the Program**: Execute the script in a Python environment that supports the pycryptodome library.
2. **Select an Encryption Technique**: When prompted, choose a number corresponding to the desired encryption method (1-8).
3. **Input Data**:
    - For classical ciphers, input the necessary key and plaintext when prompted.

    - For AES, DES, and Triple DES, first select the desired mode (1-3), then input the plaintext.
4. **View Results**: The program will display the encrypted message in hexadecimal format. If desired, the user can choose to decrypt the message immediately afterward.