EnDcypt

Zadid Bin Azad

September 27, 2024

Design Patterns Lab-03

Problem Statement

You are required to build a flexible encryption and decryption service that works with various encryption algorithms. This system should allow the encryption method to be dynamically selected based on runtime conditions, such as user input. The system will be used to encrypt and decrypt the contents of a text file.

Requirements:

1. Implement the following encryption algorithms:
    - **AES (Advanced Encryption Standard)**
    - **DES (Data Encryption Standard)**
    - **Caesar Cipher** (A basic shift-based cipher)
2. Design your application such that the choice of encryption algorithm can be swapped without modifying the core logic. The system should be able to handle different algorithms in a uniform manner.
3. The program must:
    - Allow the user to select one of the three encryption algorithms at runtime.
    - Take a text file as input, encrypt the contents using the selected algorithm, and save the encrypted data to a new file.
    - Be able to decrypt the file back to its original content for validation.
4. Ensure the system is easily extendable to accommodate new encryption algorithms in the future without requiring changes to the core encryption service.

Additional Considerations:

- For the Caesar Cipher, the system should allow the user to specify the shift value.
- Implement proper error handling, particularly when dealing with file input/output and invalid encryption methods.
- Your solution should demonstrate the separation of concerns and extensibility in software design.