Laporan Implementasi Cipher Klasik – 5 Algoritma

Nama	: Yulianti Saidah Awaliyah
NIM	: 20123059
Mata Kuliah	: Cryptografi
Dosen Pengampu	: Kodrat Mahatma, S.Kom., M.Kom

PROGRAM STUDI INFORMATIKA

UNIVERSITAS TEKNOLOGI DIGITAL

BANDUNG

2025

1. **Pendahuluan**

Kriptografi klasik merupakan dasar dari ilmu keamanan informasi modern. Teknik-teknik ini digunakan untuk menyembunyikan isi pesan dengan cara mengganti atau mengacak huruf berdasarkan aturan tertentu.

Pada laporan ini diimplementasikan lima algoritma kriptografi klasik, yaitu **Caesar Cipher, Vigenere Cipher, Affine Cipher, Playfair Cipher,** dan **Hill Cipher**, menggunakan bahasa pemrograman **Python** dengan antarmuka GUI berbasis tkinter.

Tujuan dari implementasi ini adalah:

- Memahami prinsip kerja masing-masing algoritma klasik.
- Menganalisis kelemahan keamanan dari setiap algoritma.
- Menampilkan proses enkripsi dan dekripsi secara interaktif.

2. **Implementasi**

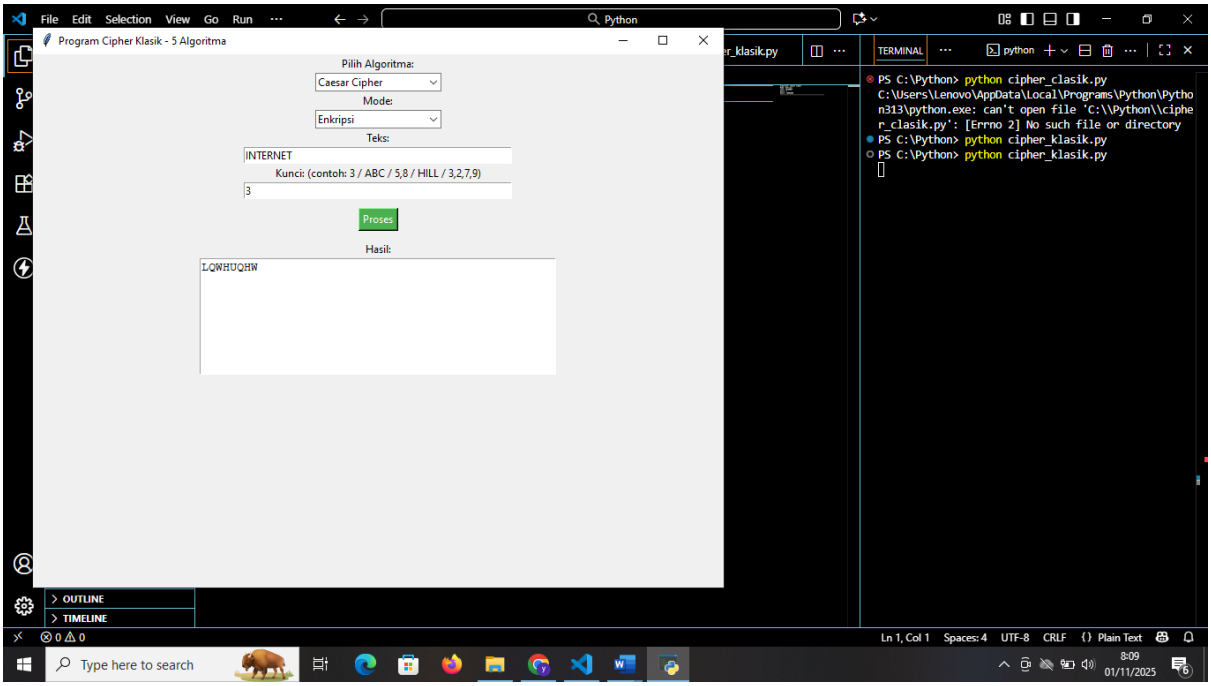
Program dibuat menggunakan bahasa **Python** dengan antarmuka GUI berbasis **Tkinter**. Pengguna dapat memilih algoritma, memasukkan teks dan kunci, serta menekan tombol untuk melakukan enkripsi atau dekripsi.

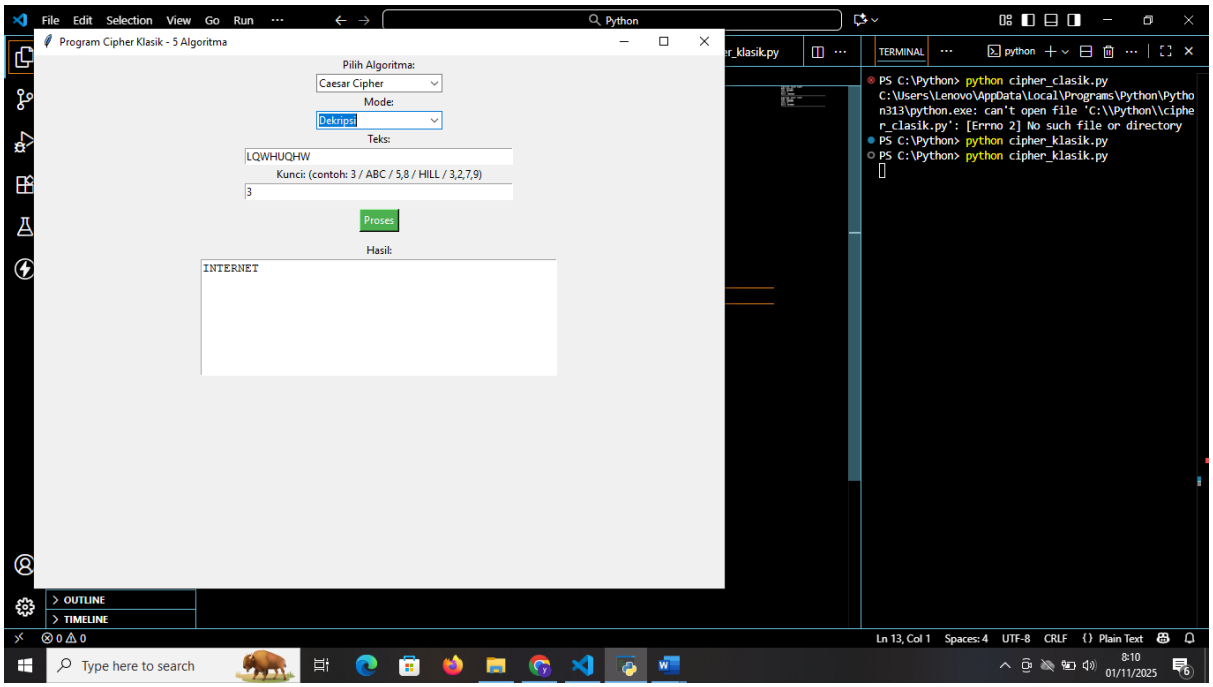
3. **Analisis kelemahan**

Algoritma	Mekanisme	Kelemahan
Caesar Cipher	Pergeseran huruf tetap	Mudah dipecahkan dengan brute-force (25 kemungkinan)
Vigenere Cipher	Pergeseran berdasarkan kata kunci	Pola kunci berulang bisa dianalisis dengan metode Kasiski
Affine Cipher	Transformasi linear dengan parameter a dan b	Rentan terhadap analisis frekuensi
Playfair Cipher	Penggantian pasangan huruf (5x5 matrix)	Masih bisa diserang dengan analisis digraf
Hill Cipher	Operasi matriks (mod 26)	Jika diketahui sebagian plaintext, kunci bisa dihitung kembali

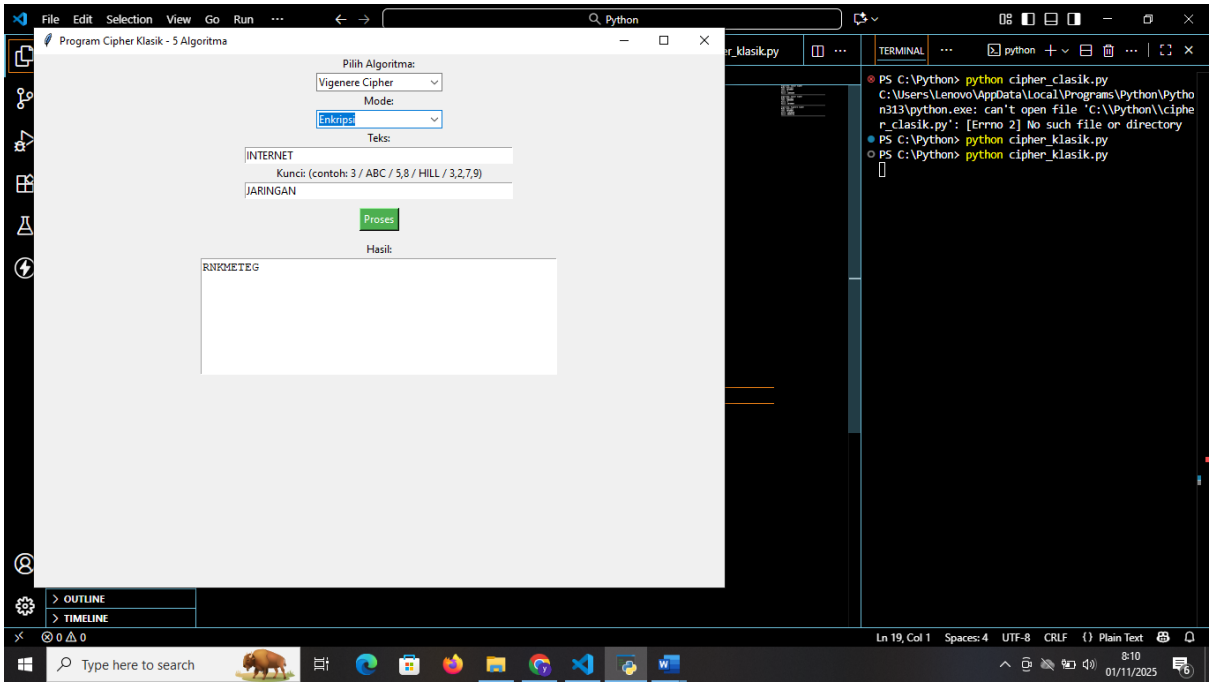
4. **Contoh Pengujian**

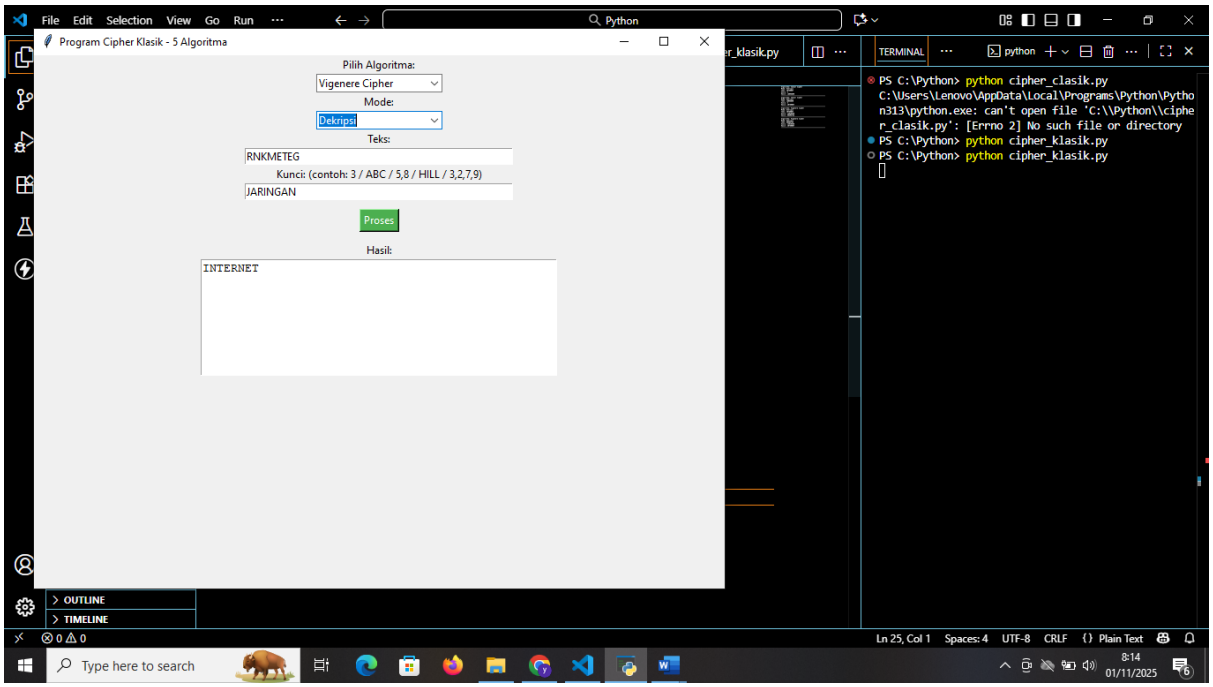
   a. **Caesar Cipher**



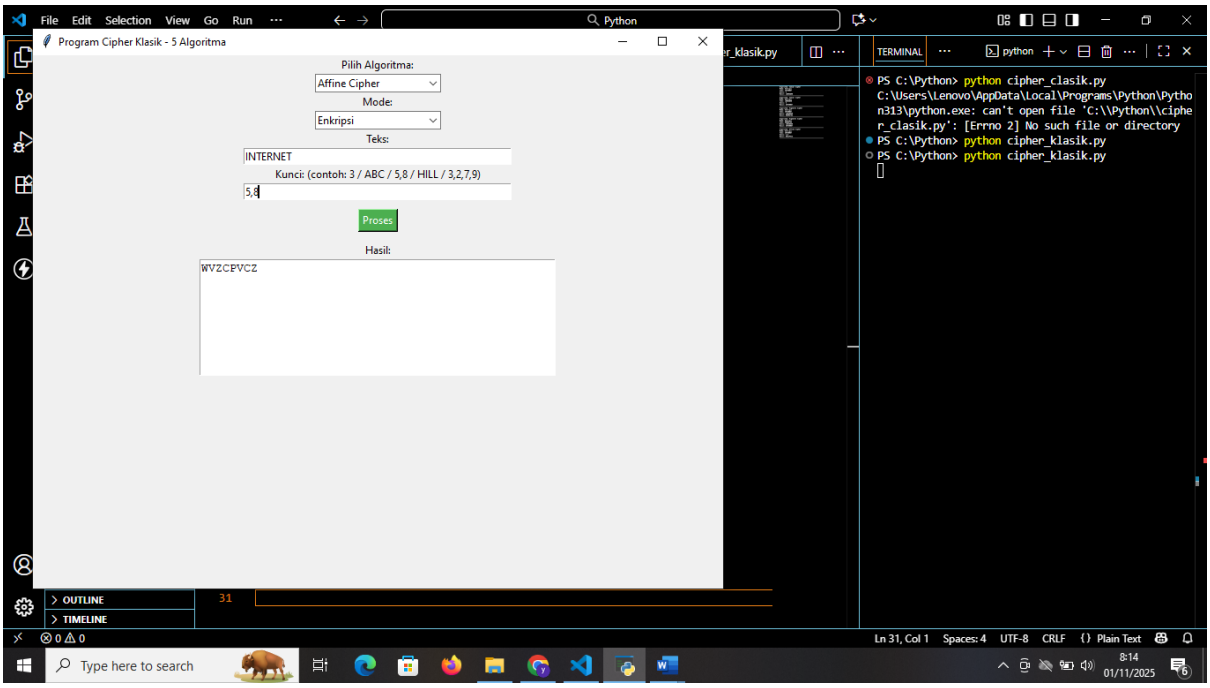


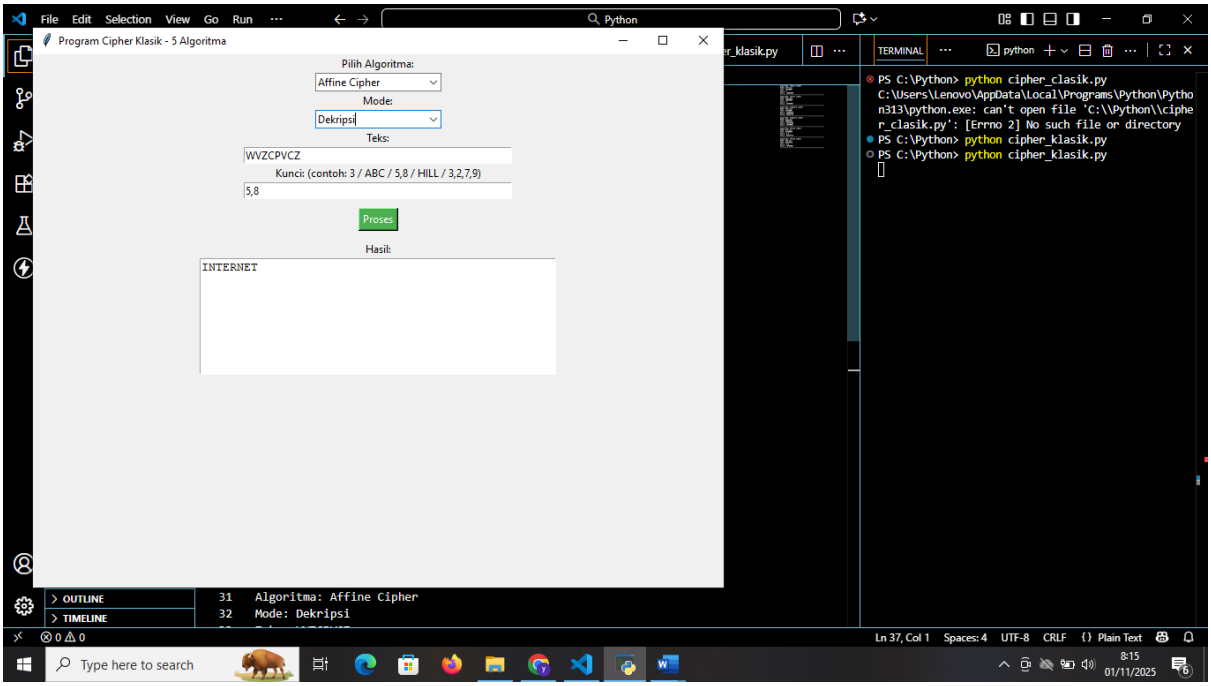
b. Vegenere Cipher



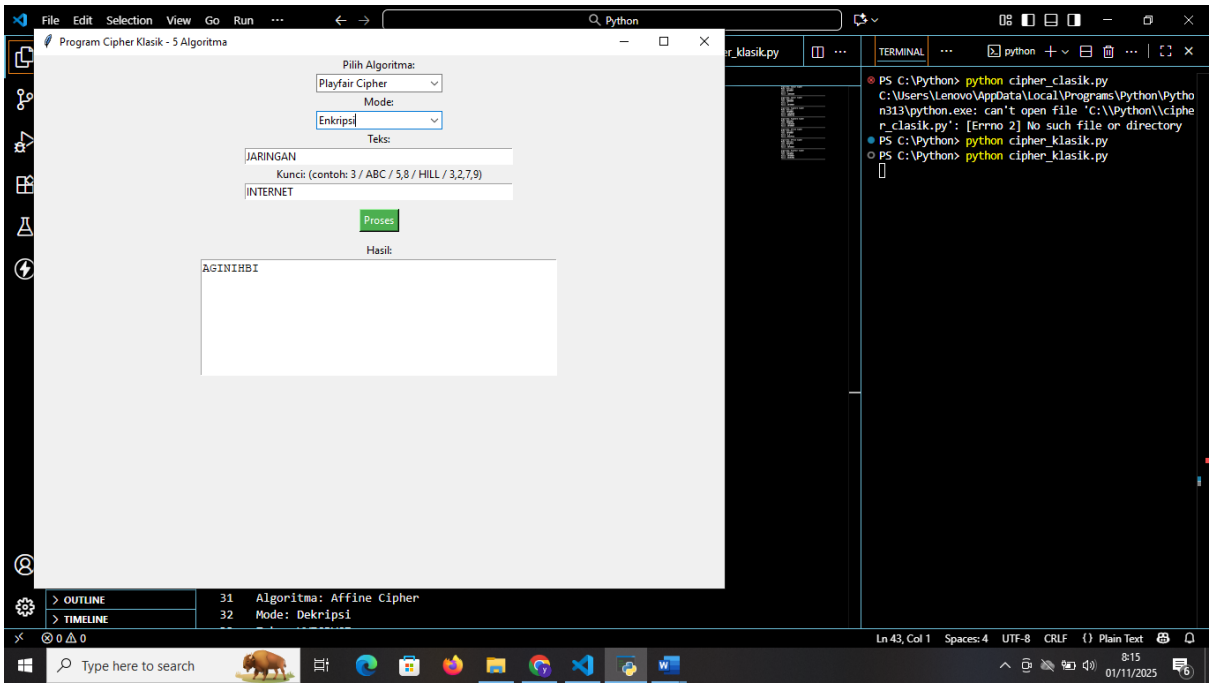


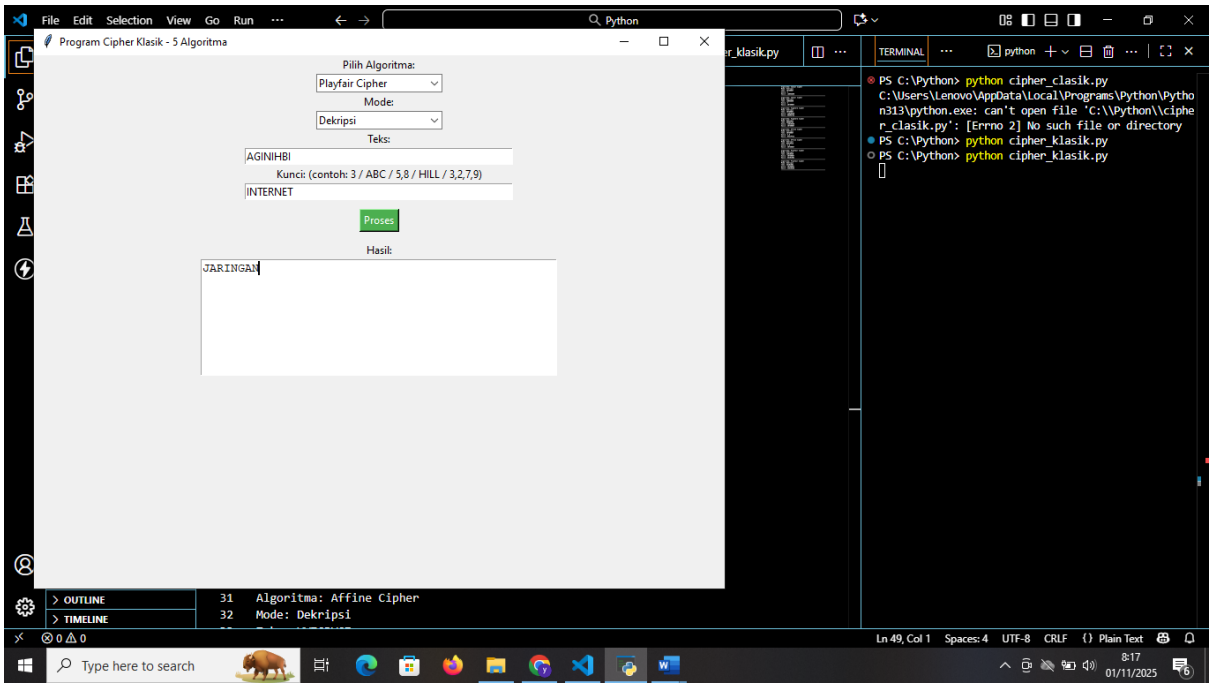
c. Affine Cipher



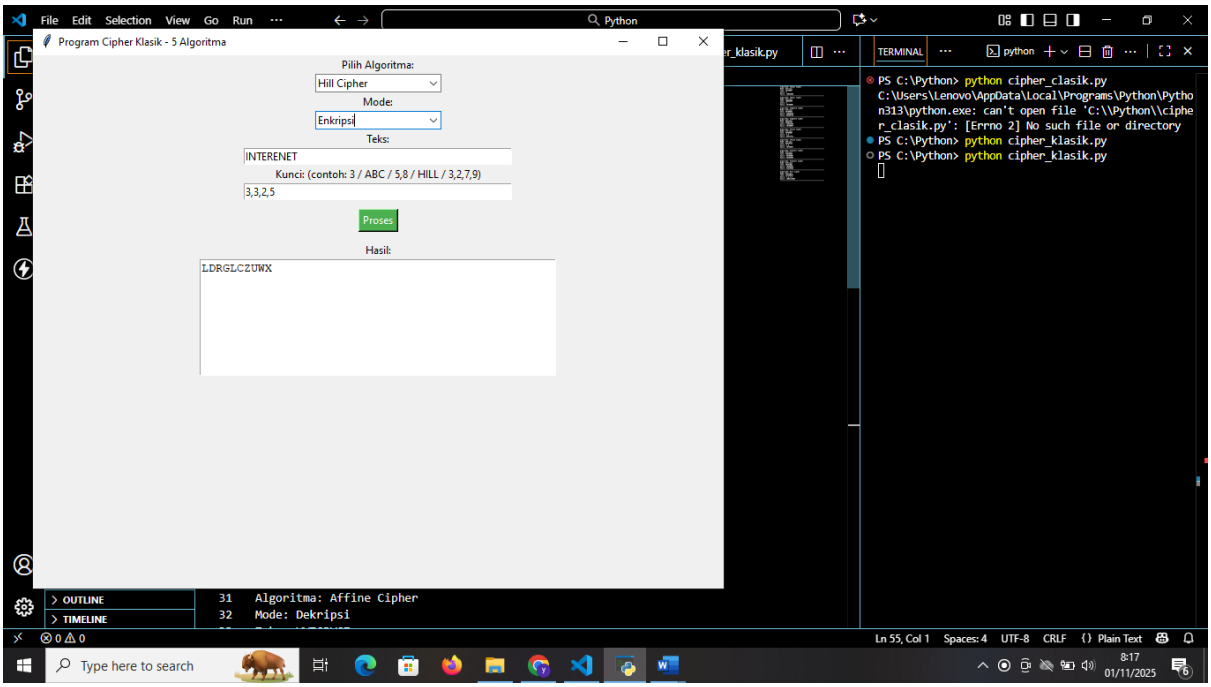


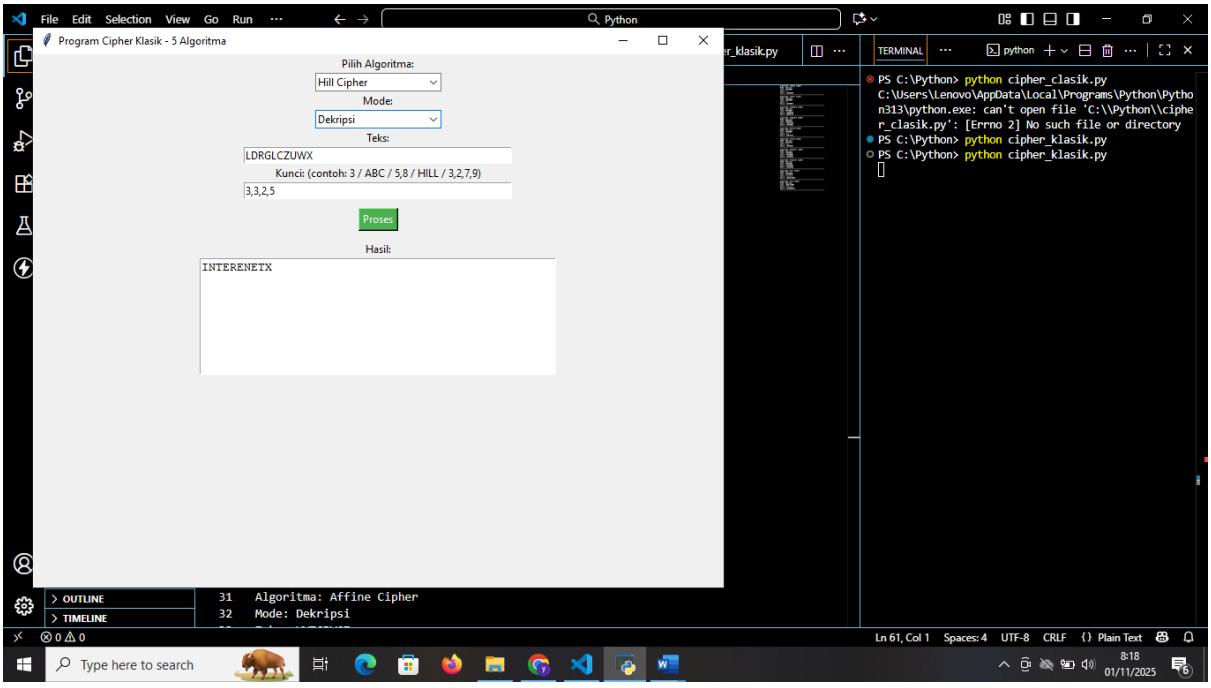
d. Plyafair Cipher





e. Hill Cipher





5. Kesimpulan

Lima algoritma klasik ini menunjukkan dasar-dasar penting dari kriptografi modern, yaitu substitusi, permutasi, dan penggunaan kunci.

Namun, semuanya memiliki kelemahan besar dari sisi keamanan — terutama karena masih dapat dipecahkan dengan analisis frekuensi atau brute force.

Meski begitu, implementasi ini bermanfaat untuk memahami prinsip dasar enkripsi yang menjadi fondasi bagi algoritma modern seperti AES dan RSA.

6. **Lampiran**

   Link Github: https://github.com/Yuliantii20/cipher.git