LAPORAN TUGAS 1

Nama: Salsabila Wali Datussyuhada

NIM: 20123017

Kelas: C1.23

Mata Kuliah: Kriptografi

1. Tujuan Program

Program ini dibuat untuk mengenkripsi dan mendekripsi teks menggunakan beberapa metode cipher klasik. Tujuannya agar pengguna dapat memahami cara kerja dasar algoritma kriptografi sederhana, seperti Caesar, Vigenère, Affine, Playfair, dan Hill Cipher.

2. Deskripsi Singkat Program

Program berbasis GUI (Graphical User Interface) menggunakan customtkinter dengan beberapa fitur utama:

- Input teks dan kunci.
- Pemilihan jenis cipher.
- Tombol Enkripsi, Dekripsi, Hapus, dan Simpan hasil.
- Tampilan yang rapi dan mudah digunakan.

3. Analisis Kelemahan Tiap Cipher

a. Caesar Cipher

- Kelemahan:

  - Hanya memiliki 25 kemungkinan pergeseran, sehingga mudah dipecahkan dengan brute-force (coba semua shift).

  - Pola frekuensi huruf masih terlihat jelas (karena substitusi tunggal).

- Dampak: Tidak aman untuk melindungi pesan rahasia modern.

b. Vigenère Cipher

- Kelemahan:

  - Jika panjang kunci pendek, pola pengulangan bisa dianalisis menggunakan metode *Kasiski Examination*.

  - Tidak sepenuhnya kebal terhadap analisis frekuensi jika kunci sering diulang.

- Dampak: Keamanan bergantung pada panjang dan kerahasiaan kunci.

c. Affine Cipher

- Kelemahan:

  - Hanya kombinasi linear sederhana (ax + b mod 26), sehingga bisa dipecahkan jika diketahui dua pasangan plaintext-ciphertext.

  - Harus memastikan nilai a relatif prima terhadap 26; jika tidak, hasil enkripsi rusak.

- Dampak: Lemah terhadap serangan *known plaintext attack*.

d. Playfair Cipher

- Kelemahan:

  - Tidak mengenkripsi huruf tunggal (karena berpasangan dua-dua).

  - Pola huruf masih dapat dianalisis karena setiap pasangan mengikuti aturan tertentu (misal baris sama atau kolom sama).

  - Tidak cocok untuk data digital panjang.

- Dampak: Lebih aman dari Caesar, tapi tetap mudah dipecahkan dengan analisis digram (dua huruf).

e. Hill Cipher

- Kelemahan:

- Bergantung pada matriks yang memiliki invers modulo 26 — tidak semua matriks bisa digunakan.

- Lemah terhadap serangan *known plaintext*, karena persamaan linear bisa diselesaikan untuk menemukan matriks kunci.

- Jika input bukan huruf (angka/simbol), hasilnya bisa salah.

- Dampak: Perlu pengelolaan kunci dan validasi matriks yang lebih ketat.

4. Kelemahan Umum Program

1. Tidak ada validasi input teks dan kunci yang kuat.
   Misalnya, pengguna bisa memasukkan huruf pada kunci Hill, menyebabkan error.
2. Tidak ada pengamanan data.
   Semua hasil enkripsi tersimpan dalam bentuk teks biasa (.txt), mudah dibuka siapa saja.
3. Semua cipher bersifat klasik (substitusi sederhana).
   Tidak cocok untuk penggunaan keamanan data modern.
4. Tidak mendukung karakter non-alfabet.
   Huruf kecil, angka, dan simbol tidak diolah dengan baik.
5. Hill Cipher tidak memeriksa determinan 0 atau non-inversibel.
   Dapat menyebabkan error matematis atau hasil salah.

5. Kesimpulan

Program ini berfungsi baik untuk pembelajaran konsep dasar kriptografi klasik, tetapi tidak aman untuk aplikasi dunia nyata.
Untuk pengembangan lebih lanjut, dapat ditambahkan:

- Validasi input lebih kuat.
- Pengecekan kunci otomatis (Affine dan Hill).
- Dukungan karakter campuran (huruf kecil, angka, simbol).
- Penerapan cipher modern seperti AES atau RSA untuk keamanan nyata.