KRIPTOGRAFI – IMPLEMENTASI CIPHER KLASIK

Laporan ini disusun untuk memenuhi Tugas Mini pada mata kuliah Kriptografi dengan dosen pengampu

Bapak Kodrat Mahatma S.T.,M.Kom.

LINTANG SARI IRVANIATI
(20123012)

C1.23 - S1 INFORMATIKA

UNIVERSITAS TEKNOLOGI DIGITAL

NOVEMBER 2025

A. Latar Belakang Cipher Klasik

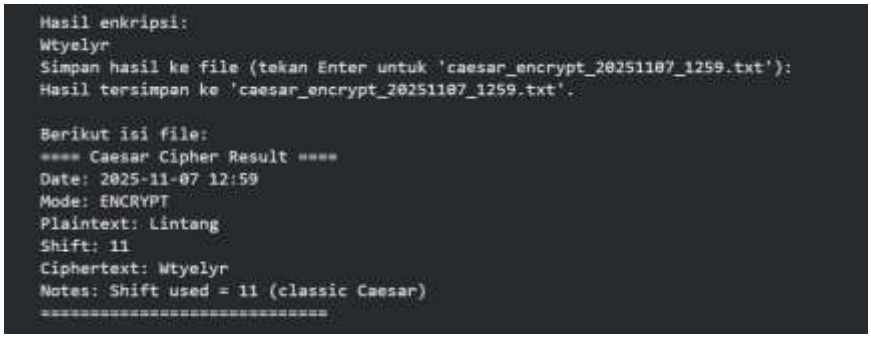
Cipher klasik adalah metode enkripsi awal yang digunakan sebelum munculnya kriptografi modern. Walaupun saat ini tidak lagi dipakai untuk keamanan serius, cipher klasik tetap penting untuk dipelajari karena memperkenalkan konsep dasar seperti substitusi, permutasi, dan penggunaan kunci. Setiap algoritma diuji untuk proses enkripsi dan dekripsi secara otomatis menggunakan Python. Pada laporan ini, saya mengimplementasikan lima algoritma cipher klasik:

1. Caesar Cipher
2. Vigenère Cipher
3. Affine Cipher
4. Playfair Cipher
5. Hill Cipher.

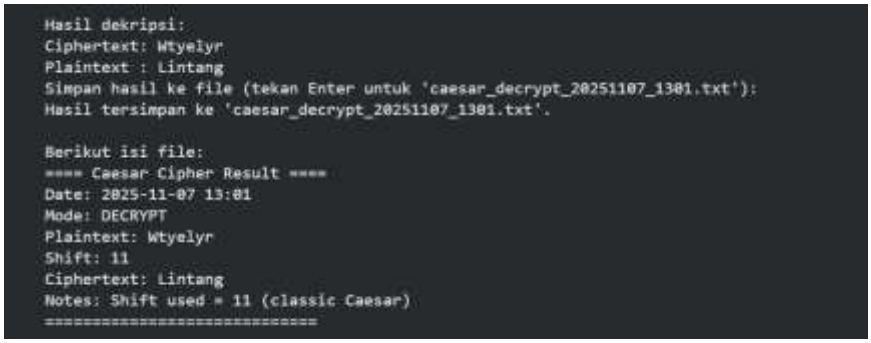
B. Implementasi Kode Program

1. Caesar Cipher

- Hasil Enkripsi



- Hasil Dekripsi



2. Vigenère Cipher

- Hasil Enkripsi

```
=== Vigenere Cipher ===
Mode (ENCRYPT/DECRYPT): Encrypt
Masukkan teks: Lintang Sari
Masukkan key: Pisang

==== Cipher Result ====
Date: 2025-11-07 13:47:23
Mode: ENCRYPT
Plaintext: Lintang Sari
Key: Pisang
Ciphertext: AQFTNTV ASRV
Notes: Rentan terhadap analisis frekuensi jika kunci pendek
======================
```

- Hasil Dekripsi

```
=== Vigenere Cipher ===
Mode (ENCRYPT/DECRYPT): DECRYPT
Masukkan teks: AQFTNTV ASRV
Masukkan key: Pisang

==== Cipher Result ====
Date: 2025-11-07 13:51:18
Mode: DECRYPT
Plaintext: LINTANG SARI
Key: Pisang
Ciphertext: AQFTNTV ASRV
Notes: Rentan terhadap analisis frekuensi jika kunci pendek
======================
```

3. Affine Cipher

- Hasil Enkripsi

```
=== Affine Cipher ===
Mode (ENCRYPT/DECRYPT): encrypt
Masukkan teks: Buah Naga
Masukkan a (coprime dengan 26): 3
Masukkan b: 10

==== Cipher Result ====
Date: 2025-11-07 13:55:09
Mode: ENCRYPT
Plaintext/Ciphertext: Buah Naga
Key: a=3, b=10
Ciphertext/Plaintext: NSKF XKCK
Notes: Memerlukan a coprime dengan 26; rentan analisis frekuensi
======================
```

- Hasil Dekripsi

```
=== Affine Cipher ===
Mode (ENCRYPT/DECRYPT): decrypt
Masukkan teks: NSKF XKCK
Masukkan a (coprime dengan 26): 3
Masukkan b: 10

==== Cipher Result ====
Date: 2025-11-07 13:59:27
Mode: DECRYPT
Plaintext/Ciphertext: BUAH NAGA
Key: a=3, b=10
Ciphertext/Plaintext: NSKF XKCK
Notes: Memerlukan a coprime dengan 26; rentan analisis frekuensi
======================
```

4. Playfair Cipher

- Hasil Enkripsi

```
=== Playfair Cipher ===
Mode (ENCRYPT/DECRYPT): encrypt
Masukkan teks: Padang
Masukkan key: L

==== Cipher Result ====
Date: 2025-11-07 14:03:28
Mode: ENCRYPT
Plaintext: Padang
Key: L
Ciphertext: MDLBSN
Notes: Huruf J digabung dengan I; digraph diproses dengan matriks 5x5
======================
```

- Hasil Dekripsi

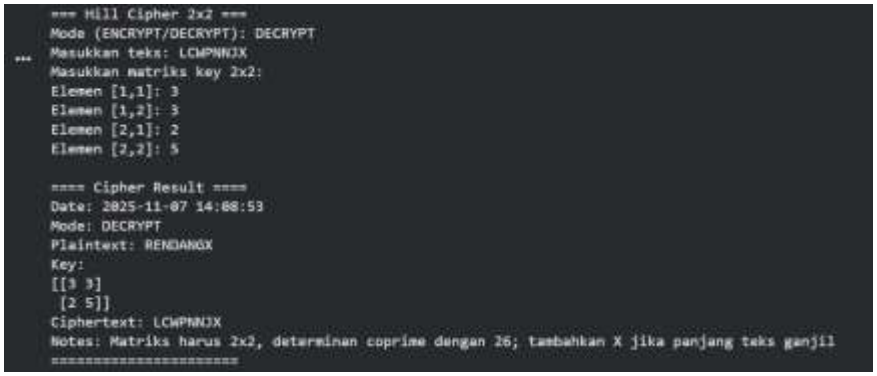
```
=== Playfair Cipher ===
Mode (ENCRYPT/DECRYPT): decrypt
Masukkan teks: MDLBSN
Masukkan key: L

==== Cipher Result ====
Date: 2025-11-07 14:04:21
Mode: DECRYPT
Plaintext: PADANG
Key: L
Ciphertext: MDLBSN
Notes: Huruf J digabung dengan I; digraph diproses dengan matriks 5x5
======================
```

5. Hill Cipher

- Hasil Enkripsi

- Hasil Dekripsi



C. Analisis Kelemahan dan Kekurangan

Cipher	Kekurangan
Caesar Cipher	1. Ruang kunci sangat kecil, hanya 25 kemungkinan. 2. Sangat mudah dipecahkan brute force. 3. Pola frekuensi huruf sama seperti plaintext.
Vigenère Cipher	1. Jika key pendek dan berulang, bisa dipecahkan dengan analisis Kasiski dan Index of Coincidence. 2. Bukan benar-benar polyalphabetic jika panjang key kecil.
Affine Cipher	1. Tetap mempertahankan pola frekuensi seperti substitusi biasa. 2. Jika kunci tidak memenuhi gcd(a,26)=1, dekripsi tidak bisa dilakukan.
Playfair Cipher	1. Bekerja per pasangan huruf, sehingga pola digraph masih dapat dianalisis. 2. Penambahan huruf (X atau Q) pada plaintext bisa mengubah makna pesan.
Hill Cipher	1. Jika sebagian ciphertext berhasil diketahui, matriks kunci dapat dihitung kembali. 2. Butuh matriks invers modulo 26, dan tidak semua matriks valid. 3. Sensitif terhadap kesalahan per karakter, satu error bisa merusak seluruh blok.