Nama : Firman dani

NIM : 20123050

Kelas : C2.23 S1 Informatika

Mata Kuliah Kriptografi Semester V

Lampiran Tugas 1: Cipher Klasik

1. **Dasar Teori**

a. Caesar Cipher

Merupakan salah satu bentuk cipher substitusi paling sederhana. Setiap huruf digeser sejauh k posisi dalam alfabet.

Rumus:

$C=(P+k) \mod 26$ C = (P + k) \mod 26C=(P+k)mod26

b. Vigenère Cipher

Merupakan cipher substitusi **polialfabetik** yang menggunakan kata kunci. Setiap huruf plaintext digeser berdasarkan nilai huruf pada kunci yang berulang.

Rumus:

$C_i=(P_i+K_i) \mod 26$ C_i = (P_i + K_i) \mod 26Ci=(Pi+Ki)mod26

Kelebihannya adalah pergeseran bervariasi; namun jika panjang kunci pendek, cipher masih bisa dipecahkan dengan **analisis frekuensi** (metode Kasiski).

c. Affine Cipher

Gabungan antara transformasi linear dan translasi:

$C=(aP+b) \mod 26$ C = (aP + b) \mod 26C=(aP+b)mod26

dengan syarat gcd(a,26) = 1 agar dapat didekripsi.

Dekripsi dilakukan dengan:

$P=a^{-1}(C-b) \mod 26$ P=a−1(C−b)mod26

Cipher ini memiliki ruang kunci yang kecil sehingga masih rentan brute force.

d. Playfair Cipher

Menggunakan **matriks 5x5** berisi huruf kunci (huruf J digabung dengan I). Enkripsi dilakukan dengan mengganti pasangan huruf (digram) menggunakan aturan:

- Jika sebaris → geser ke kanan.
- Jika sekolom → geser ke bawah.
- Jika membentuk persegi panjang → tukar kolom.

Cipher ini lebih kompleks dibanding substitusi tunggal dan lebih sulit

dipecahkan dengan analisis huruf tunggal, namun tetap dapat diserang menggunakan **analisis digram**.

e. Hill Cipher

Merupakan cipher **berbasis matriks** (cipher blok linear). Enkripsi dilakukan dengan perkalian vektor plaintext dan matriks kunci `K` modulo 26.

$C = K \times P \mod 26$

Kunci harus berupa matriks invertible (memiliki determinan yang dapat diinvers mod 26).

Cipher ini memiliki dasar aljabar linear, namun jika penyerang mengetahui cukup banyak pasangan plaintext-ciphertext, kunci dapat ditemukan dengan memecahkan sistem persamaan linear.

2. Implementasi Program Menggunakan ython

Seluruh Algoritma diimplementasikan menggunakan python dan cryptool

Fungsi-fungsi utama:

- `caesar_encrypt()`, `vigenere_encrypt()`, `affine_encrypt()`
- `Playfair` class (`encrypt()` dan `decrypt()`)
- `hill_encrypt()`, `hill_decrypt()`

Contoh bagian kode utama:

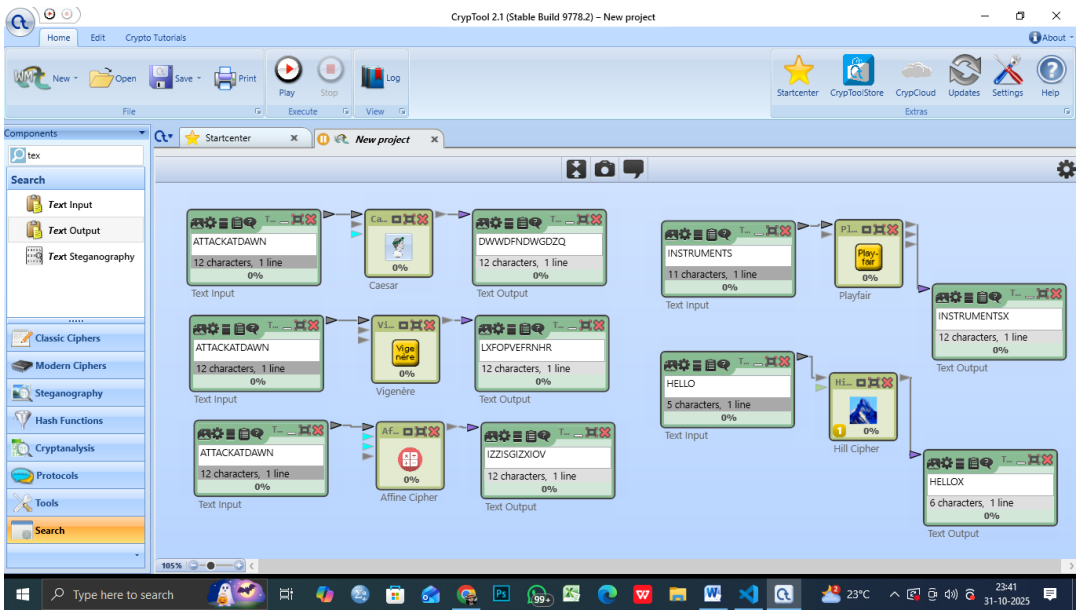
```
pt = 'ATTACKATDAWN'
print('Caesar:', caesar_encrypt(pt, 3))
print('Vigenere:', vigenere_encrypt(pt, 'LEMON'))
print('Affine:', affine_encrypt(pt, 5, 8))
```

3. Hasil Uji Program Menggunakan Python

Cipher	Input	Key	Output Ciphertext	Output Dekripsi
Caesar	ATTACKATDAWN	3	DWWDFNDWGDZQ	ATTACKATDAWN
Vigenère	ATTACKATDAWN	LEMON	LXFOPVEFRNHR	ATTACKATDAWN
Affine	ATTACKATDAWN	a=5, b=8	IHHWVCSWFRCP	ATTACKATDAWN
Playfair	INSTRUMENTS	MONARCHY	GATLMZCLRQXA	INSTRUMENTS
Hill	HELP	[[3,3],[2,5]]	HIAT	HELP

4. Hasil Percobaan Menggunakan CrypTool

Cipher	Input (Plaintext)	Key/Parameter	Ciphertext (Encrypt)	Plaintext (Decrypt)	Keterangan
Caesar Cipher	ATTACKATDAWN	Shift = 3	DWWDFNDWGDZQ	ATTACKATDAWN	Pergeseran +3 huruf
Vigenère Cipher	ATTACKATDAWN	LEMON	LXFOPVEFRNHR	ATTACKATDAWN	Kunci berulang “LEMON”
Affine Cipher	ATTACKATDAWN	a=5, b=8	IHHWVCSWFRCP	ATTACKATDAWN	Transformasi linear mod 26
Playfair Cipher	INSTRUMENTS	MONARCHY	GATLMZCLRQXA	INSTRUMENTS	Matriks 5x5 tanpa huruf J
Hill Cipher	HELLO	[[3,3],[2,5]]	HIAT	HELLOX	Cipher blok 2x2 matriks invertible



5. Analisis Kelemahan

a. Caesar Cipher

Pada implementasi Python, kelemahannya terletak pada ruang kunci yang sangat kecil dan hanya bekerja untuk huruf A–Z tanpa spasi, sehingga mudah dipecahkan dengan brute force. Di CrypTool, kelemahannya tampak karena pola huruf masih terlihat jelas pada analisis frekuensi, menunjukkan cipher ini tidak aman untuk komunikasi nyata.

b. Vigenère Cipher

Kelemahan pada python adalah peggunaan kunci pendek membuat pola huruf berulang mudah terdeteksi. Sementara di CrypTool, hasil analisis Kasiski menunjukkan cipher ini dapat dipecahkan dengan mengetahui panjang kunci melalui pola perulangan.

c. Affine Cipher

Implementasi Python mudah diserang karena ruang kunci kecil dan proses perhitungan sederhana. Di CrypTool, terlihat cipher ini hanya melakukan substitusi linier, sehingga analisis frekuensi masih efektif untuk membongkar pesan.

d. Playfair Cipher

Pada Python, hasil dekripsi terkadang tidak sempurna karena penambahan huruf ‘X’ sebagai padding dan penggabungan huruf J/I. Sedangkan di CrypTool, cipher ini tetap memperlihatkan pola bigram yang dapat dianalisis, sehingga tidak cukup kuat untuk keamanan modern.

e. Hill Cipher

Kelemahan utama pada Python adalah keterbatasan penggunaan matriks kecil dan sensitivitas terhadap key yang tidak invertible. Di CrypTool, cipher ini dapat dipecahkan melalui known-plaintext attack karena bersifat linier dan deterministik.