

Implementasi Program Vigenère Cipher

Laporan ini disusun untuk memenuhi nilai Praktek Session dengan dosen pengampu

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



Sindi Rahmadani (20123040)

Amanda Aulia Nuraani (20123043)

**C1.23 S1 INFORMATIKA
UNIVERSITAS TEKNOLOGI DIGITAL**

2025

1. Vigenere Cipher

Vigenère Cipher merupakan algoritma kriptografi klasik yang menggunakan pola substitusi polialfabetik. Berbeda dengan Caesar Cipher yang menggunakan satu pergeseran tetap, Vigenère Cipher menggunakan kata kunci (key) untuk menentukan pergeseran tiap huruf plaintext.

Proses enkripsi dilakukan dengan menjumlahkan nilai huruf plaintext dan huruf pada kunci dalam bentuk angka ($A=0, B=1, \dots, Z=25$), lalu hasilnya diambil dalam modulo 26.

Rumus enkripsi:

$$C_i = (P_i + K_i) \bmod 26$$

Sedangkan dekripsi dilakukan dengan rumus:

$$P_i = (C_i - K_i) \bmod 26$$

2. Implementasi Program

Program dibuat menggunakan bahasa Python dengan tiga fungsi utama:

- `vigenere_encrypt(text, key)` → melakukan enkripsi.
- `vigenere_decrypt(cipher, key)` → mengembalikan ciphertext ke plaintext.
- `frequency_analysis(text)` → menghitung frekuensi huruf pada ciphertext.

• Input

```
plaintext = "ATTACKATDAWN"  
key = "LEMON"
```

• Output

```
Ciphertext: LXFOPVEFRNHR  
  
Dekripsi: ATTACKATDAWN  
  
Frekuensi huruf:  
L : 0.083  
X : 0.083  
F : 0.167  
O : 0.083  
P : 0.083  
V : 0.083  
E : 0.083  
R : 0.167  
N : 0.083  
H : 0.083  
PS D:\kkriptografi\Vigenère Cipher> |
```

3. Analisis Frekuensi Ciphertext

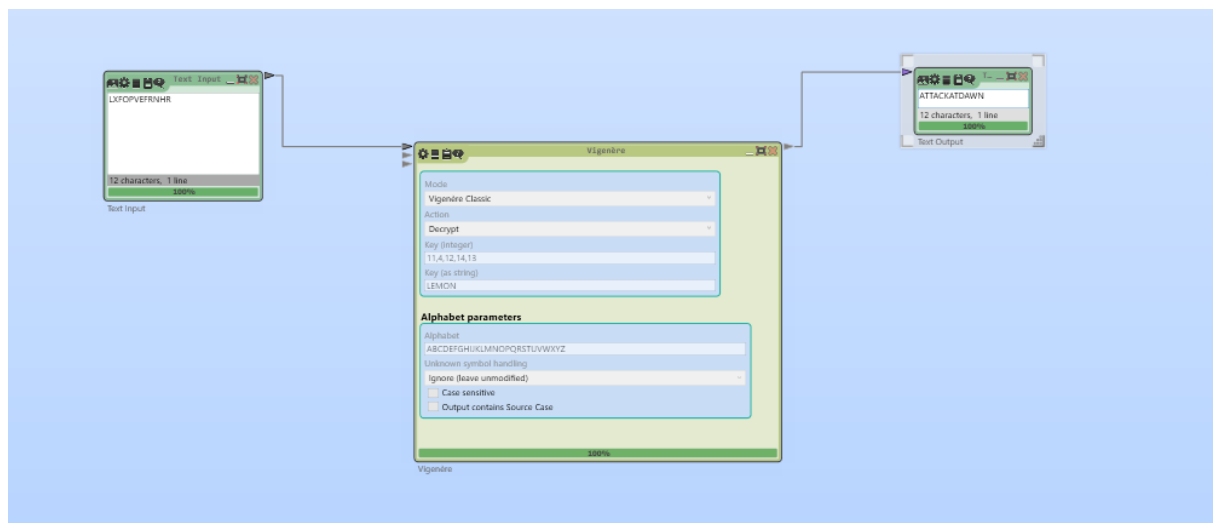
Hasil analisis menunjukkan distribusi huruf yang tidak merata tapi acak, dengan frekuensi berkisar antara 0.083 hingga 0.167. Hal ini menunjukkan bahwa ciphertext tidak memiliki pola yang mudah ditebak.

Distribusi yang acak ini merupakan bukti bahwa Vigenère Cipher berhasil mengaburkan pola huruf asli berkat penggunaan kunci polialfabetik.

4. Validasi dengan CrypTool

Validasi dilakukan menggunakan aplikasi CrypTool, dengan input plaintext dan kunci yang sama. Hasil enkripsi dari CrypTool menghasilkan ciphertext “LXFOPVEFRNHR”, yang identik dengan hasil program Python, sehingga implementasi program terbukti benar. Selain itu, grafik analisis frekuensi pada CrypTool menunjukkan pola yang hampir merata, memperkuat bahwa algoritma Vigenère tidak mudah dipecahkan dengan analisis frekuensi sederhana.

Deskripsi



Encrypt

Text Input

ATTACKATDAWN

12 characters, 1 line

100%

Vigenère

100%

Mode

Vigenère Classic

Action

Encrypt

Key (integer)

11,4,12,14,13

Key (as string)

LEMON

Alphabet parameters

Alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Unknown symbol handling

Ignore (leave unmodified)

Case sensitive

Output contains Source Case

Text Output

LXOPVERNRHR

12 characters, 1 line

100%