

**LAPORAN PENUGASAN KRIPTOGRAFI
CIPHER VINEGENÈRE DAN ANALISIS FREKUENSINYA**



Nama : Ilham ahmad maulana 20123079
: Farhan azis bisri 20123071

**UNIVERSITAS TEKNOLOGI DIGITAL
BANDUNG
2025**

1. TUJUAN

Tujuan dari kegiatan praktikum ini adalah untuk mengerti konsep dasar dari cipher polialfabetik dengan mencoba algoritma Vigenère Cipher. Dalam aktivitas ini, mahasiswa diharapkan dapat melakukan proses pengkodean dan penguraian pesan menggunakan kunci tertentu, menganalisis pola penyebaran huruf pada pesan terenkripsi melalui cara analisis frekuensi, serta memvalidasi hasil pengkodean dengan menggunakan perangkat lunak CrypTool.

2. DASAR TEORI

Vigenère Cipher adalah salah satu tipe sandi polialfabetik yang termasuk dalam sistem kriptografi tradisional. Berbeda dari sandi monoalfabetik seperti Caesar Cipher yang hanya memakai satu pola ganti untuk seluruh pesan, sandi polialfabetik memanfaatkan lebih dari satu alfabet ganti, yang menjadikan ciphertext lebih sulit untuk dianalisis dengan cara frekuensi biasa. Dasar dari Vigenère Cipher adalah penerapan sebuah kata kunci yang diulang untuk setiap huruf dalam plaintext. Setiap huruf dalam plaintext akan digeser menurut nilai huruf dari kata kunci yang sesuai, berdasarkan letak huruf dalam alfabet (A=0, B=1, C=2, dan seterusnya). Dengan cara ini, pergeseran huruf pada setiap posisi akan bervariasi tergantung pada huruf kunci yang diterapkan. Ini membuat pola dalam ciphertext menjadi lebih acak dan lebih sulit untuk diprediksi dibandingkan dengan metode enkripsi monoalfabetik.

Secara matematis, proses enkripsi dan dekripsi pada Vigenère Cipher dapat dijelaskan dengan operasi modulo 26. Untuk proses enkripsi digunakan rumus $C_i = (P_i + K_i) \bmod 26$, Dimana P_i Adalah huruf plain text dan K_i Adalah huruf kunci. Sedangkan proses dekripsi menggunakan rumus $P_i = (C_i - K_i) \bmod 26$, dengan C_i sebagai huruf ciphertext. Dalam implementasi komputer, huruf di konversi ke nilai numerik berdasarkan kode ASCII sehingga operasi aritmatika dapat dilakukan secara langsung.

3. IMPLEMENTASI PROGRAM

```

1  # === VIGENERE CIPHER IMPLEMENTATION ===
2  # Enkripsi, Dekripsi, dan Analisis Frekuensi
3
4  √ from collections import Counter
5  import matplotlib.pyplot as plt
6
7
8  # Fungsi Enkripsi Vigenere Cipher
9
10 √ def vigenere_encrypt(plain, key):
11     plain = plain.upper().replace(" ", "")
12     key = key.upper()
13     cipher = ""
14     √ for i in range(len(plain)):
15         p = ord(plain[i]) - 65
16         k = ord(key[i % len(key)]) - 65
17         c = (p + k) % 26
18         cipher += chr(c + 65)
19     return cipher
20
21
22 # Fungsi Dekripsi Vigenere Cipher
23
24 √ def vigenere_decrypt(cipher, key):
25     cipher = cipher.upper().replace(" ", "")
26     key = key.upper()
27     plain = ""
28     √ for i in range(len(cipher)):
29         c = ord(cipher[i]) - 65
30         k = ord(key[i % len(key)]) - 65
31         p = (c - k) % 26
32         plain += chr(p + 65)
33     return plain

```

```

36 # Analisis Frekuensi Sederhana
37
38 def frequency_analysis(text):
39     text = text.upper().replace(" ", "")
40     count = Counter(text)
41     total = len(text)
42     freqs = {char: round(count[char] / total, 3) for char in sorted(count)}
43     return freqs
44
45 def plot_frequency(freqs):
46     plt.figure(figsize=(10,4))
47     plt.bar(freqs.keys(), freqs.values())
48     plt.title("Analisis Frekuensi Ciphertext")
49     plt.xlabel("Huruf")
50     plt.ylabel("Frekuensi")
51     plt.show()

```

```

54 # Contoh Pengujian
55
56 plaintext = "ATTACKATDAWN"
57 key = "LEMON"
58
59 ciphertext = vigenere_encrypt(plaintext, key)
60 print("Plaintext :", plaintext)
61 print("Key       :", key)
62 print("Ciphertext:", ciphertext)
63
64 decrypted = vigenere_decrypt(ciphertext, key)
65 print("\nDekripsi :", decrypted)

```

```

68 # Analisis Frekuensi
69
70 freqs = frequency_analysis(ciphertext)
71 print("\nAnalisis Frekuensi:", freqs)
72 plot_frequency(freqs)

```

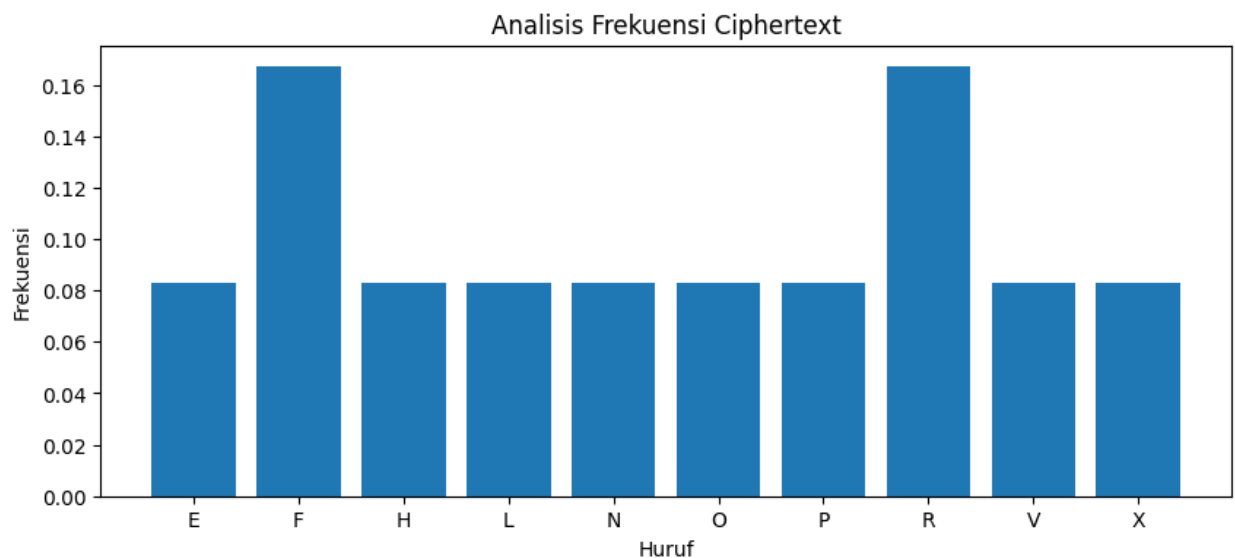
Input:

```
Plaintext : ATTACKATDAWN
Key       : LEMON
```

Output :

```
Ciphertext: LXFOPVEFRNHR
Dekripsi  : ATTACKATDAWN
```

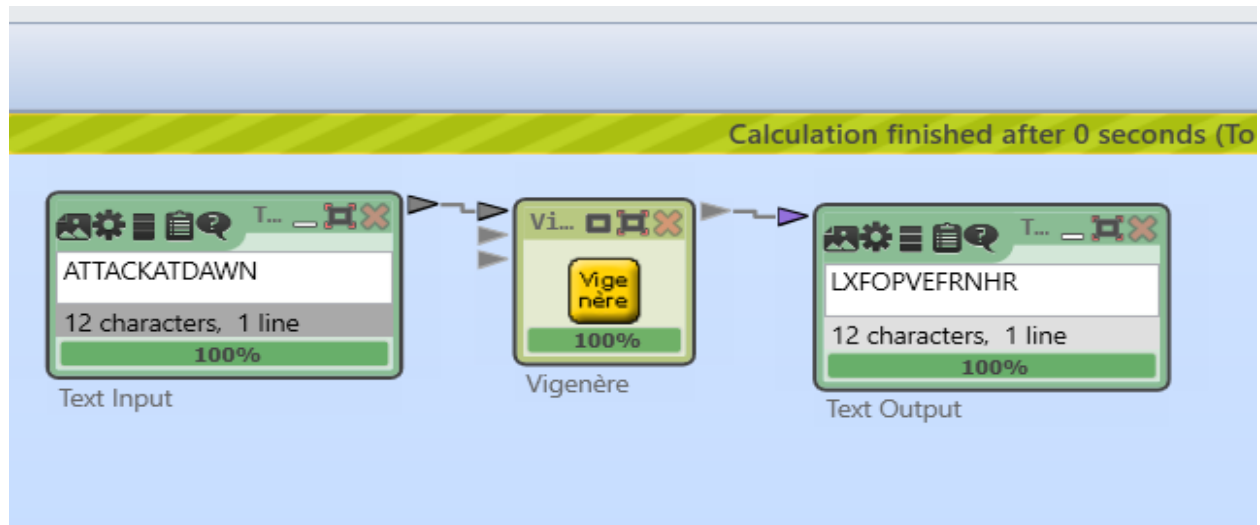
4. ANALISIS FREKUENSI



Hasil grafik :

- Huruf-huruf seperti E, F, H, L, N, O, P, R, V, X muncul dalam ciphertext
- Frekuensi huruf F dan R paling tinggi (sekitar 0.16), sedangkan huruf lain relatif seimbang di sekitar 0.08.
- Pola distribusi huruf tidak menonjol pada satu huruf tertentu, menandakan bahwa ciphertext ini bersifat acak dan merata, ciri khas dari *cipher polialfabetik* seperti Vigenère.

5. HASIL CRYPTOOL



Hasil dari enkripsi di CrypTool 2 menunjukkan bahwa teks asli "ATTACKATDAWN" berhasil dienkripsi dengan penggunaan algoritma Vigenère Cipher menggunakan kunci "LEMON". Proses enkripsi ditunjukkan melalui langkah-langkah komponen Input Teks → Vigenère → Output Teks, di mana hasil akhirnya adalah ciphertext "LXFOPVEFRNHR". Nilai ini sama persis dengan output yang diperoleh lewat implementasi Python, sehingga membuktikan bahwa algoritma tersebut berfungsi dengan baik. Ciphertext yang dihasilkan terlihat acak dan tidak menunjukkan pola tertentu, menandakan bahwa pergeseran huruf menurut kunci telah berfungsi sesuai dengan prinsip cipher polialfabetik.