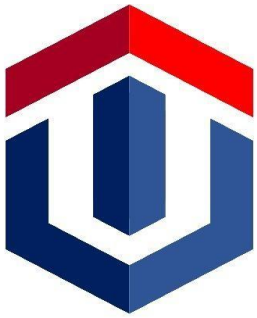
LAPORAN ANALISIS KELEMAHAN VIGENERE CIPHER



Universitas Teknologi Digital

Disusun Oleh :

1. Nabilla Maesaroh (20123027)
2. Sayyidah Muthi Nur Aisyah (20123003)

PROGRAM STUDI S1 INFORMATIKA
UNIVERSITAS TEKNOLOGI DIGITAL
TAHUN AJARAN 2024/2025

VIGENÈRE CIPHER

Vigenère Cipher merupakan pengembangan dari Caesar Cipher yang termasuk dalam kategori cipher polialfabetik. Cipher ini menggunakan kata kunci (key) berupa huruf untuk menentukan pergeseran setiap karakter pada plaintext.

Contoh Implementasi Program :

Program Vigenère Cipher dikembangkan menggunakan Python dengan dua fungsi utama :

1. vigenere_encrypt() untuk melakukan enkripsi
2. vigenere_decrypt() untuk mengembalikan ciphertext ke plaintext

In [1]:
```
def vigenere_encrypt(plain, key):

    key = key.upper()
    result = ''
    key_index = 0

    for char in plain.upper():
        if char.isalpha():

            shift = ord(key[key_index % len(key)]) - 65

            result += chr((ord(char) - 65 + shift) % 26 + 65)

            key_index += 1
        else:
            result += char
    return result

print("--- Vigenere Cipher Encryptor ---")

text_to_encrypt = input("Masukkan teks yang ingin dienkripsi: ")

encryption_key = input("Masukkan kata kunci: ")

if not encryption_key.isalpha():
    print("Error: Kata kunci harus hanya terdiri dari huruf!")
else:
    hasil_enkripsi = vigenere_encrypt(text_to_encrypt, encryption_key)
```

```
    print("\n--- Hasil Enkripsi ---")
    print(f"Teks Asli   : {text_to_encrypt.upper()}")
    print(f"Kata Kunci  : {encryption_key.upper()}")
    print(f"Hasil Cipher: {hasil_enkripsi}")
```

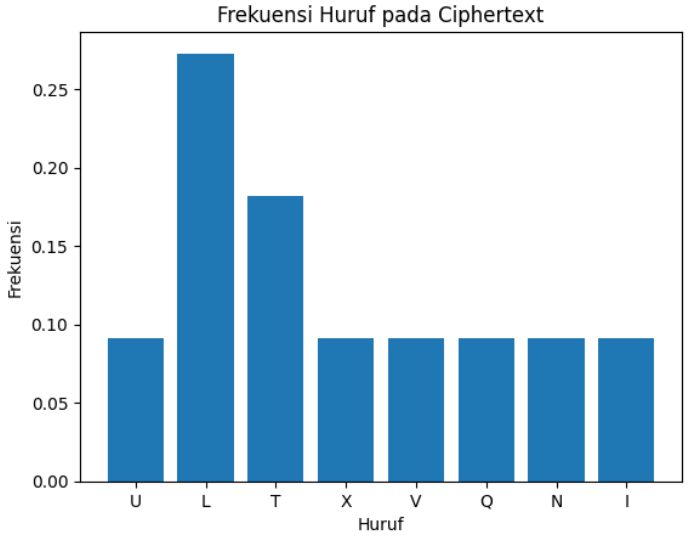
```
--- Vigenere Cipher Encryptor ---
Masukkan teks yang ingin dienkripsi: KRIPTOGRAFI
Masukkan kata kunci: KULIAH

--- Hasil Enkripsi ---
Teks Asli   : KRIPTOGRAFI
Kata Kunci  : KULIAH
Hasil Cipher: ULTXTVQLLNI
```

Teks Asli : KRIPTOGRAFI

Kata Kunci : KULIAH

Hasil Cipher: ULTXTVQLLNI

Analisis Frekuensi Ciphertext



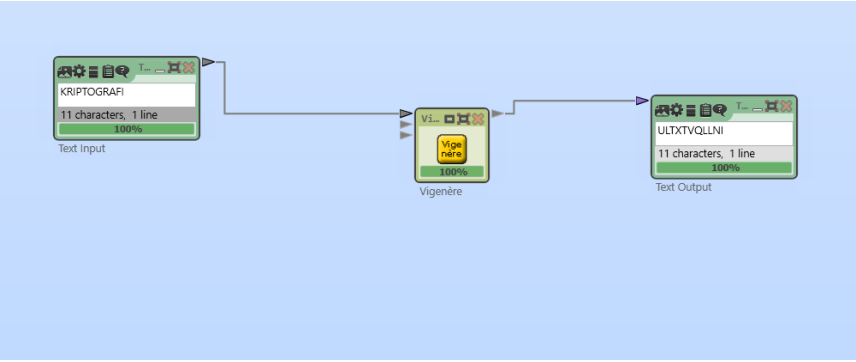
Analisis Frekuensi

U: 0.09
L: 0.27
T: 0.18
X: 0.09
V: 0.09
Q: 0.09
N: 0.09
I: 0.09

Validasi dengan Cryptool

Proses validasi dilakukan dengan mengenkripsi teks KRIPTOGRAFI menggunakan kunci KULIAH pada CrypTool 2 dengan mode Vigenère Classic.

Hasil enkripsi yang muncul di CrypTool adalah:



yang sama persis dengan hasil dari implementasi Python

Selain itu, analisis frekuensi di CrypTool juga menunjukkan distribusi huruf yang merata, tanpa dominasi huruf tertentu

Hal ini menegaskan bahwa algoritma Vigenère Cipher bekerja dengan benar dan efektif menyamarkan pola huruf asli

Kesimpulan

Berdasarkan hasil implementasi dan analisis yang telah dilakukan, dapat disimpulkan bahwa algoritma Vigenère Cipher berhasil diimplementasikan dengan baik menggunakan bahasa Python. Proses enkripsi menghasilkan ciphertext ULTXTVQLLNI dari plaintext KRIPTOGRAFI dengan kunci KULIAH, dan hasil tersebut terbukti valid setelah dilakukan pengujian ulang menggunakan aplikasi CrypTool 2, yang menampilkan hasil ciphertext identik.

Analisis frekuensi terhadap ciphertext menunjukkan distribusi huruf yang relatif merata tanpa adanya huruf dominan, sehingga pola statistik plaintext berhasil tersamarkan. Hal ini menegaskan bahwa Vigenère Cipher memiliki tingkat keamanan lebih tinggi dibanding Caesar Cipher karena memanfaatkan sistem pergeseran berganda (polialfabetik).

Meskipun demikian, keamanan cipher ini tetap bergantung pada panjang dan kerandoman kunci yang digunakan — semakin panjang dan acak kunci, semakin sulit ciphertext untuk dianalisis menggunakan metode klasik seperti Kasiski atau Index of Coincidence. Dengan demikian, baik dari hasil enkripsi, analisis statistik, maupun validasi CrypTool, dapat disimpulkan bahwa implementasi algoritma Vigenère Cipher telah berjalan dengan benar dan efektif dalam menyembunyikan pola huruf pada pesan asli.