

# LAPORAN IMPLEMENTASI & ANALISIS VIGENERE CIPHER

Oleh: Sinta Nurhaliza (20123041)

## 1. Tujuan Analisis

- Mengetahui cara kerja algoritma Vigenère Cipher melalui implementasi Python.
- Menganalisis pola frekuensi ciphertext untuk memahami karakteristik cipher.
- Membandingkan hasil enkripsi dan dekripsi Python dengan CrypTool sebagai validasi.
- Memastikan bahwa algoritma Vigenère berjalan akurat dan konsisten pada kedua metode.

## 2. Implementasi

Plaintext : SALAK

Key : LEMON

Kode Pemrograman Python :

```
def vigenere_encrypt(plain, key):  
  
    key = key.upper()  
  
    result = "  
  
    for i, char in enumerate(plain.upper()):  
  
        if char.isalpha():  
  
            shift = ord(key[i % len(key)]) - 65  
  
            result += chr((ord(char) - 65 + shift) % 26 + 65)  
  
        else:  
  
            result += char  
  
    return result
```

```
def vigenere_decrypt(cipher, key):
```

```
key = key.upper()

result = ""

for i, char in enumerate(cipher.upper()):

    if char.isalpha():

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

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

    else:

        result += char

return result
```

```
plaintext = 'SALAK'
```

```
key = 'LEMON'
```

```
ciphertext = vigenere_encrypt(plaintext, key)
```

```
decrypted_text = vigenere_decrypt(ciphertext, key)
```

```
print("Plaintext :", plaintext)
```

```
print("Key      :", key)
```

```
print("Ciphertext:", ciphertext)
```

```
print("Dekripsi :", decrypted_text)
```

## Hasil Eksekusi Python

```
... Plaintext : SALAK  
    Key       : LEMON  
    Ciphertext: DEXOX  
    Dekripsi  : SALAK
```

### 3. Analisis Frekuensi Ciphertext

Ciphertext : DEXOX

Frekuensi Kemunculan Huruf

- D : 1 kali
- E : 1 kali
- X : 2 kali
- O : 1 kali

### Interpretasi

Ciphertext dari Vigenère Cipher biasanya memiliki distribusi huruf yang lebih merata dibandingkan cipher substitusi monoalfabetik seperti Caesar Cipher. Dalam ciphertext “DEXOX” terlihat bahwa huruf muncul dengan distribusi yang tidak terlalu timpang kecuali huruf X yang muncul 2 kali. Ini menunjukkan bahwa Vigenère telah mengurangi pola frekuensi alami pada plaintext.

### 4. Validasi Menggunakan Cryptool

Validasi dilakukan menggunakan Cryptool untuk memastikan bahwa hasil enkripsi dan dekripsi pada program Python sesuai dengan implementasi standar algoritma Vigenère Cipher. Adapun langkah-langkah validasi yang dilakukan adalah sebagai berikut:

1. Membuka Cryptool Online melalui menu *Classic Ciphers* → *Vigenère Cipher*.
2. Memasukkan plaintext “SALAK” ke dalam kolom input.
3. Mengisi key dengan “LEMON” sesuai dengan percobaan pada program Python.
4. Menekan tombol Encrypt untuk melihat ciphertext yang dihasilkan. Cryptool memberikan hasil “DEXOX”, yang sesuai dengan output Python.

5. Untuk validasi dekripsi, ciphertext “DEXOX” dimasukkan kembali ke CrypTool menggunakan key yang sama, kemudian menekan Decrypt.
6. CrypTool menghasilkan plaintext kembali menjadi “SALAK”, sehingga hasil dekripsi identik dengan program Python.

Hasil validasi ini menunjukkan bahwa keduanya identik dengan implementasi Python, sehingga dapat disimpulkan bahwa proses enkripsi dan dekripsi telah benar.

The screenshot displays a web interface for a cryptographic tool. It features three main sections: 'Plaintext', 'Ciphertext', and 'Key'. The 'Plaintext' section shows the input 'SALAK'. A large downward arrow indicates the encryption process. The 'Ciphertext' section shows the output 'DEXOX'. The 'Key' section shows the key 'LEMON'. The interface includes character counts (5 chars) and buttons for 'Copy' and 'Reset'.

Plaintext	5 chars
SALAK	

↓

Ciphertext	5 chars
DEXOX	

  

Key	Text	Copy	Reset
LEMON			

## 5. Kesimpulan

Implementasi Vigenère Cipher menggunakan Python berhasil dilakukan dengan benar, yang dibuktikan melalui kesesuaian hasil enkripsi dan dekripsi dengan CrypTool. Ciphertext yang dihasilkan yaitu “DEXOX”, dan analisis frekuensi menunjukkan distribusi huruf yang lebih menyebar, sesuai karakteristik Vigenère sebagai cipher polialfabetik. Dengan demikian, implementasi Python telah tervalidasi dan dapat digunakan sebagai dasar untuk analisis ciphertext lebih lanjut.