

IMPLEMENTASI 2 ALGORITMA CIPHER KLASIK

Nama : Neni

NPM : 20123057

Kelas : C2.23

Prodi : S1 Informatika

1. Caesar Cipher

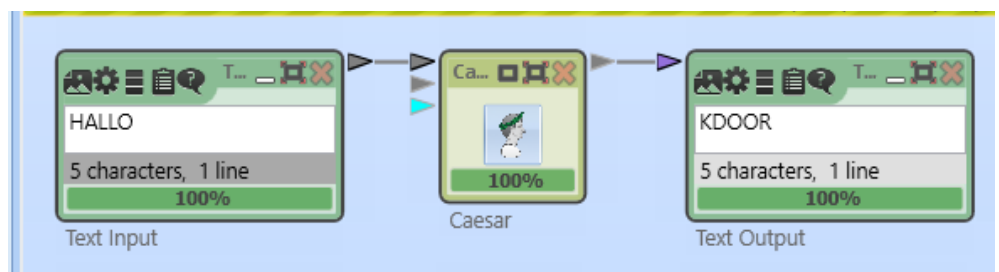
- Implementasi Algoritma menggunakan Python

Caesar Cipher

```
def caesar_encrypt(text, shift):  
    result = ""  
    for char in text:  
        if char.isalpha():  
            base = ord('A') if char.isupper() else ord('a')  
            result += chr((ord(char) - base + shift) % 26 + base)  
        else:  
            result += char  
    return result  
  
print(caesar_encrypt('HELLO', 3))
```

KHOOR

- Implementasi Menggunakan CrypTool



- Analisis Kekuatan
 - Sangat mudah dipahami dan diimplementasikan.
 - Cocok untuk pembelajaran dasar kriptografi
 - Cepat diproses karena hanya menggunakan operasi pergeseran huruf
- Analisis Kelemahan

- Pola huruf tetap mudah ditebak dengan analisis frekuensi.
- Jumlah kunci hanya 25 bisa dipecahkan brute force dalam hitungan detik
- Tidak aman digunakan dalam komunikasi nyata

2. Implementasi Vigenere Cipher

➤ Implementasi Algoritma menggunakan python

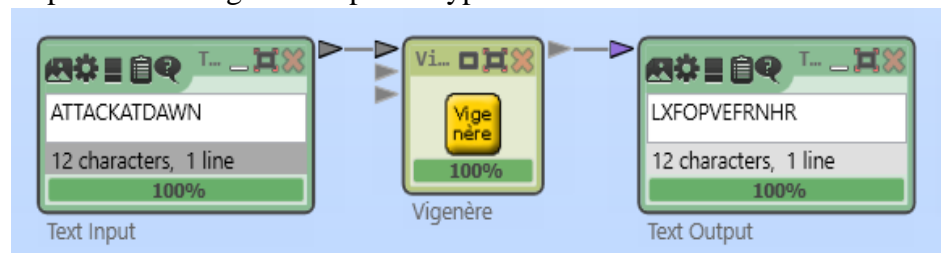
Vigenère Cipher

```
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

print(vigenere_encrypt('ATTACKATDAWN', 'LEMON'))
```

LXFOPVEFRNHR

➤ Implementasi Vigenere Cipher CrypTool



➤ Analisis Kekuatan

- Lebih aman dari caesar karena tiap huruf digeser berbeda (polialfabetik).
- Frekuensi huruf plaintext tidak mudah dikenali
- Mudah diimplementasikan dan efisien untuk teks pendek.

➤ Analisis Kelemahan

- Jika kunci terlalu pendek mudah dianalisis menggunakan kasiski Test atau index of Coincidence
- Tetap termasuk cipher klasik tidak aman untuk komunikasi modern
- Rentan jika penyerang mengetahui sebagian plaintext dan ciphertext.

➤ Tujuan

Tujuan dari praktikum ini adalah untuk memahami dan menerapkan dua algoritma cipher klasik, yaitu **Caesar Cipher** dan **Vigenère Cipher**, menggunakan bahasa pemrograman Python. Melalui percobaan ini, mahasiswa dapat mengetahui proses enkripsi dan dekripsi pesan serta membandingkan tingkat keamanan antara kedua algoritma tersebut.

➤ Kesimpulan

Berdasarkan hasil implementasi, **Caesar Cipher** termasuk algoritma sederhana yang mudah dipahami namun memiliki keamanan rendah karena pola pergeserannya tetap dan mudah ditebak. Sementara itu, **Vigenère Cipher** lebih kuat karena menggunakan kunci yang bervariasi untuk setiap huruf, sehingga pola huruf sulit dikenali, meskipun tetap dapat dianalisis apabila kuncinya pendek atau digunakan berulang.