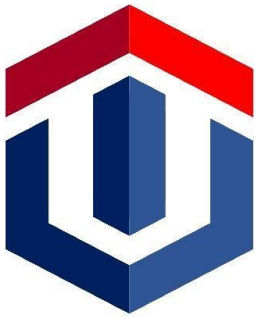
LAPORAN ANALISIS KELEMAHAN VIGENERE CIPHER



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

1. CAESAR CIPHER

Caesar Cipher merupakan salah satu algoritma kriptografi klasik tertua yang diciptakan oleh Julius Caesar. Metode ini menggunakan sistem pergeseran huruf dalam alfabet sebanyak nilai kunci tertentu. Misalnya jika kunci (key) bernilai 3, maka huruf A akan menjadi D, huruf B menjadi E, dan seterusnya. Proses dekripsi adalah kebalikan dari enkripsi dengan cara menggeser huruf ke arah kiri sebanyak nilai kunci.

Contoh Implementasi Program :

In [1]:
```
# Caesar Cipher - Implementasi Klasik
# Oleh: Sayyidah Muthi Nur Aisyah dan Nabilla Maesaroh

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

def caesar_decrypt(cipher, shift):
    return caesar_encrypt(cipher, -shift)

# Input sederhana
teks = input("Masukkan teks: ")
shift = int(input("Masukkan shift: "))
hasil = caesar_encrypt(teks, shift)
print("Hasil Enkripsi:", hasil)

# Untuk dekripsi
print("Dekripsi:", caesar_decrypt(hasil, shift))
```

```
Masukkan teks: tes pertama
Masukkan shift: 3
Hasil Enkripsi: whv shuwdpd
Dekripsi: tes pertama
```

Masukkan teks : tes pertama

Masukkan shift : 3

Hasil Enkripsi : whv shuwdpd

Dekripsi : tes pertama

Hasil enkripsi menunjukkan bahwa setiap huruf pada plaintext bergeser sebanyak tiga langkah ke kanan. Proses dekripsi berhasil mengembalikan teks ke bentuk semula, yang berarti algoritma bekerja sesuai dengan konsep dasar Caesar Cipher.

Analisis Kelemahan:

Caesar Cipher memiliki kelemahan mendasar yaitu ruang kunci yang kecil (hanya 25 kemungkinan pergeseran). Akibatnya, cipher ini mudah dipecahkan menggunakan metode brute force dengan mencoba seluruh pergeseran yang mungkin. Selain itu, distribusi frekuensi huruf pada ciphertext tetap mirip dengan plaintext, sehingga dapat dianalisis dengan metode analisis frekuensi sederhana.

2. VIGENÈRE CIPHER

Vigenère Cipher adalah pengembangan dari Caesar Cipher yang menggunakan kata kunci (key) berupa huruf untuk menentukan pergeseran setiap karakter pada plaintext. Panjang key menentukan variasi pergeseran yang berbeda-beda, sehingga membuat cipher ini lebih sulit dipecahkan dengan brute force sederhana.

Contoh Implementasi Program :

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

Hasil enkripsi menunjukkan bahwa setiap huruf pada plaintext digeser sesuai urutan huruf pada key.Huruf pertama digeser sejauh ‘L’, huruf kedua sejauh ‘E’, dan seterusnya. Dengan demikian, ciphertext yang dihasilkan menjadi jauh lebih acak dibanding Caesar Cipher biasa.

Analisis Kelemahan:

Meskipun lebih kuat dari Caesar Cipher, Vigenère Cipher masih memiliki kelemahan pada pengulangan pola key. Jika panjang key jauh lebih pendek dari plaintext, maka pola pergeseran akan berulang dan dapat dianalisis menggunakan metode Kasiski atau analisis indeks koincidensi. Selain itu, tanpa pengacakan tambahan, Vigenère tetap tergolong cipher substitusi polialfabetik yang tidak tahan terhadap serangan modern.

3. KESIMPULAN

Berdasarkan hasil implementasi dan analisis, dapat disimpulkan bahwa Caesar dan Vigenère Cipher merupakan dua algoritma kriptografi klasik yang sederhana namun memiliki peran penting dalam sejarah kriptografi. Caesar Cipher mudah dipahami dan diimplementasikan, namun sangat rentan terhadap brute force attack.

Sedangkan Vigenère Cipher memberikan keamanan lebih baik dengan penggunaan kunci huruf, tetapi tetap dapat dianalisis menggunakan metode statistik jika key pendek dan berulang.

Kedua cipher ini sangat cocok sebagai dasar pembelajaran konsep enkripsi dan dekripsi dalam mata kuliah. Pengantar Kriptografi karena memperkenalkan prinsip dasar kunci, pergeseran, dan analisis keamanan.