**KEAMANAN SISTEM INFORMASI**

**TUGAS PERTEMUAN 5 ALGORITMA TRANSPOSITION, SUBSTITUTION CIPHERS, DAN HACKING VIGÈNERE CIPHERS**



**Dosen Pengampu: Nano Yulian Pratama, S.S.T., M.T.**

**Disusun oleh :**

|  |  |
| --- | --- |
| Muhammad Zabbar Falihin | 222112225 |

**PROGRAM STUDI D-IV KOMPUTASI STATISTIK**

**POLITEKNIK STATISTIKA STIS**

**2024**

**DAFTAR ISI**

[**A.** **Transposition Ciphers** 1](#_Toc159292901)

[1. Algoritma 1](#_Toc159292902)

[2. Kompleksitas Waktu 1](#_Toc159292903)

[3. Program *Encrypt* 1](#_Toc159292904)

[4. Program *Decrypt* 1](#_Toc159292905)

[**B.** **Substitution Ciphers** 2](#_Toc159292906)

[1. Algoritma 2](#_Toc159292907)

[2. Kompleksitas Waktu 2](#_Toc159292908)

[3. Program *Encrypt* dan *Decrypt* 2](#_Toc159292909)

[**C.** ***Hacking* Vigènere Ciphers** 4](#_Toc159292910)

[1. Algoritma 4](#_Toc159292911)

[**D.** **Link Github Program Transposition Cipher, Substitution Cipher, dan *Hacking*** **Vigènere Ciphers serta Keseluruhan File** 5](#_Toc159292912)

# **Transposition Ciphers**

## Algoritma

Transposition Cipher melibatkan pengaturan ulang huruf-huruf dalam teks asli berdasarkan suatu skema atau pola tertentu. Salah satu contoh sederhana adalah Rail Fence Cipher, di mana teks dipecah menjadi dua baris berdasarkan urutan genap dan ganjil karakter. Contoh lain adalah Columnar Transposition, di mana teks ditulis dalam baris pada sebuah grid sesuai dengan kata kunci, dan kolom-kolom grid tersebut diatur ulang berdasarkan urutan alfabetis dari huruf-huruf dalam kata kunci.

Algoritma umum untuk Transposition Cipher adalah sebagai berikut.

* Tentukan kunci substitusi. Untuk Caesar Cipher, kunci adalah jumlah pergeseran.
* Untuk enkripsi, geser setiap huruf dari teks asli sesuai jumlah pergeseran yang ditentukan oleh kunci.
* Untuk dekripsi, lakukan proses yang berlawanan dengan enkripsi, yaitu menggeser kembali huruf-huruf yang telah dienkripsi sejumlah langkah yang sama, tapi ke arah berlawanan.

## Kompleksitas Waktu

Kompleksitas waktu dari algoritma enkripsi dan dekripsi dalam Transposition Cipher tergantung pada metode transposisi yang digunakan. Untuk metode sederhana seperti Rail Fence Cipher, kompleksitasnya tetap O(n), karena setiap karakter hanya perlu dituliskan dan dibaca sesuai urutan transposisi. Kompleksitas waktu untuk Columnar Transposition Cipher pada dasarnya adalah O(n), di mana n adalah panjang dari teks. Ini karena setiap karakter dalam teks harus ditulis ke dalam matriks dan kemudian dibaca kembali. Proses pembuatan matriks dan pembacaan kolom dapat dilakukan dalam satu iterasi melalui teks, membuat operasi ini sangat efisien.

## Program *Encrypt* dan *Decrypt*

# **Substitution Ciphers**

## Algoritma

Substitution Cipher adalah teknik kriptografi dasar di mana setiap elemen (biasanya huruf) dalam teks asli (plaintext) diganti dengan elemen lain berdasarkan suatu sistem substitusi. Ini mencakup berbagai jenis cipher, salah satu contohnya adalah Caesar Cipher. Di Caesar Cipher, substitusi dilakukan dengan menggeser huruf-huruf dalam alfabet sejumlah langkah tertentu.

Algoritma umum untuk Substitution Cipher adalah sebagai berikut:

* Tentukan kunci substitusi. Untuk Caesar Cipher, kunci adalah jumlah pergeseran.
* Untuk enkripsi, geser setiap huruf dari teks asli sesuai jumlah pergeseran yang ditentukan oleh kunci.
* Untuk dekripsi, lakukan proses yang berlawanan dengan enkripsi, yaitu menggeser kembali huruf-huruf yang telah dienkripsi sejumlah langkah yang sama, tapi ke arah berlawanan.

## Kompleksitas Waktu

Kompleksitas waktu dari algoritma enkripsi dan dekripsi dalam Substitution Cipher, termasuk Caesar Cipher, adalah O(n), di mana n adalah panjang dari teks yang dienkripsi atau didekripsi. Ini karena setiap huruf dalam teks harus diperiksa dan mungkin digeser satu per satu. Tidak ada operasi yang membutuhkan lebih dari waktu konstan untuk setiap huruf, sehingga total waktu yang diperlukan berkaitan langsung dengan jumlah huruf dalam teks.

## Program *Encrypt* dan *Decrypt*

* **Source Code substitution.py**

*def* encrypt(*text*, *shift*):

    result = ""

    for i in range(len(text)):

        char = text[i]

        if char.isalpha():  *# Cek apakah karakter adalah huruf*

*# Proses untuk huruf kapital*

            if char.isupper():

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

*# Proses untuk huruf kecil*

            else:

                result += chr((ord(char) + shift - 97) % 26 + 97)

        else:

*# Tambahkan karakter asli jika bukan huruf*

            result += char

    return result

*def* decrypt(*encrypted\_text*, *shift*):

    return encrypt(encrypted\_text, -shift)

*# Contoh penggunaan*

text = "Hello World!"

shift = 3

encrypted\_text = encrypt(text, shift)

print("Encrypted Text:", encrypted\_text)

decrypted\_text = decrypt(encrypted\_text, shift)

print("Decrypted Text:", decrypted\_text)

* Fungsi encrypt mengambil teks asli dan jumlah pergeseran sebagai argumen, lalu mengembalikan teks yang telah dienkripsi.
* Fungsi decrypt mengambil teks terenkripsi dan jumlah pergeseran sebagai argumen, menggunakan proses yang sama dengan enkripsi tapi dengan pergeseran ke arah berlawanan untuk mengembalikan teks ke bentuk aslinya.
* Kompleksitas waktu dari kedua fungsi ini adalah O(n), yang efisien dan praktis untuk teks dengan panjang n.

# ***Hacking* Vigènere Ciphers**

## Algoritma

Vigenère Cipher memperluas konsep dari Substitution Cipher dengan menggunakan kunci yang terdiri dari beberapa huruf, di mana setiap huruf menentukan pergeseran untuk huruf-huruf dalam teks asli. Ini menciptakan pola enkripsi yang lebih kompleks dan sulit ditebak dibandingkan dengan Caesar Cipher. Untuk meng-hack Vigenère Cipher tanpa mengetahui kunci, salah satu metode yang digunakan adalah analisis frekuensi dan Kasiski Examination.

* **Identifikasi Sekuens yang Berulang**

Cari sekuens huruf yang berulang dalam teks terenkripsi. Jarak antara sekuens-sekuens yang sama ini bisa memberikan petunjuk tentang panjang kunci. Sekuens berulang merujuk pada pola huruf atau grup huruf yang muncul lebih dari satu kali dalam teks terenkripsi. Pencarian sekuens berulang ini merupakan bagian penting dari Kasiski Examination, sebuah metode untuk membantu menentukan panjang kunci dalam Vigenère Cipher.

* **Kasiski Examination**

Kasiski Examination adalah metode yang lebih spesifik untuk meng-hack Vigenère Cipher. Kasiski Examination menggunakan jarak antar sekuens berulang untuk menentukan panjang kunci yang mungkin. Ide dasarnya adalah bahwa jarak tersebut seringkali merupakan kelipatan dari panjang kunci. Kasiski Examination membantu menentukan panjang kunci, yang merupakan informasi kritikal untuk memecahkan Vigenère Cipher.

* **Analisis Frekuensi**

Setelah panjang kunci diduga, teks terenkripsi dapat dibagi menjadi beberapa bagian berdasarkan panjang kunci, dan analisis frekuensi dapat diterapkan pada setiap bagian untuk menebak huruf kunci.

* **Percobaan dan Kesalahan**

Dengan menggunakan huruf-huruf kunci yang ditebak, dilakukan percobaan untuk mendekripsi teks. Ulangi proses dengan menyesuaikan tebakan sampai teks terdekripsi dengan benar terbaca.

# **Link Github Program Transposition Cipher, Substitution Cipher, dan *Hacking*** **Vigènere Ciphers serta Keseluruhan File**

* **Source Code *Hacking* Vigènere Ciphers dan keseluruhan File dilampirkan di link Github sebagai berikut :**

[**https://github.com/zabbarfalih/ksi-pertemuan5**](https://github.com/zabbarfalih/ksi-pertemuan5)