Tugas Akhir Pribadi Ke-1
Mata Kuliah Keamanan Sistem

Dibuat oleh :

Ichsan Purnomo Aji (19.240.0021)

5P43

Teknik Informatika | Mobile App

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

(STMIK)

Jl. Patriot No.25, Dukuh, Pekalongan Utara, Kota Pekalongan, Jawa Tengah 51146

Daftar Isi

BAB I.
Pendahuluan

1. Latar Belakang

Salah satu hal yang penting dalam komunikasi menggunakan computer untuk menjamin kerahasiaan data adalah Enkripsi. Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca). Enkripsi dapat diartikan sebagai kode atau chiper. Sebuah system pengkodean menggunakan suatu table atau kamus yang telah didefinisikan untuk mengganti kata dari informasi atau yang merupakan bagian dari informasi yang dikirim.

Sebuah chiper mengunakan suatu algoritma yang dapat mengkodekan semua aliran data (stream) bit dari sebuah pesan menjadi cryptogram yang tidak dimengerti (unintelligible).

Karena teknik chiper merupakan suatu system yang telah siap untuk di automasi, maka teknik ini digunakan dalam system keamanan computer dan jaringan.

2. Rumusan Masalah

Jelaskan apa yang anda ketahui mengenai algoritma kriptografi klasik berikut:

a. *Substitution Ciphers* dan berikan contohnya!
b. *Transposition Ciphers* dan berikan contohnya!

3. Tujuan

Menjelaskan apa yang diketahui mengenai algoritma kriptografi klasik berikut:

a. *Substitution Ciphers* dan contohnya
b. *Transposition Ciphers* dan contohnya

BAB II.
Pembahasan

1. Substitution Chipers

Chipers subtitusi adalah algoritma kriptografi yang mula-mula digunakan oleh kaisar Romawi, Julius Caesar (sehingga dinamakan juga *caesar cipher*), untuk menyandikan pesan yang ia kirim kepada para gubernurnya.

Caranya adalah dengan mengganti (menyulih atau mensubstitusi) setiap karakter dengan karakter lain dalam susunan abjad (alfabet). Misalnya, tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan akjad. Dalam hal ini kuncinya adalah jumlah pergeseran huruf (yaitu $k = 3$).

Tabel substitusi:

Pi : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Ci : D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Contoh :

Pesan

HALO NAMA SAYA ICHSAN PURNOMO AJI

disamarkan (enskripsi) menjadi

KDOR QDPD VDBD LFKVDQ SXUQRPR DML

Penerima pesan men-dekripsi cipherteks dengan menggunakan tabel substitusi, sehingga cipherteks

KDOR QDPD VDBD LFKVDQ SXUQRPR DML

dapat dikembalikan menjadi plainteks semula:

HALO NAMA SAYA ICHSAN PURNOMO AJI

Jenis – jenis chipper subtitusi yaitu,

a. Cipher abjad-tunggal (monoalphabetic cipher atau cipher substitusi sederhana - simple substitution cipher)

   Satu karakter di plainteks diganti dengan satu karakter yang bersesuaian. Jadi, fungsi ciphering-nya adalah fungsi satu-kesatu. Jika plainteks terdiri dari huruf-huruf abjad, maka jumlah kemungkinan susunan huruf-huruf cipherteks yang dapat dibuat adalah sebanyak 26! = 403.291.461.126.605.635.584.000.000.

b. Cipher substitusi homofonik (Homophonic substitution cipher)

   Seperti cipher abjad-tunggal, kecuali bahwa setiap karakter di dalam plainteks dapat dipetakan ke dalam salah satu dari karakter cipherteks yang mungkin. Misalnya huruf A dapat berkoresponden dengan 7, 9, atau 16, huruf B dapat berkoresponden dengan 5, 10, atau 23 dan seterusnya. Fungsi ciphering-nya memetakan satu-ke-banyak (one-tomany).

Cipher substitusi homofonik lebih sulit dipecahkan daripada cipher abjad-tunggal. Namun, dengan known-plaintext attack, cipher ini dapat dipecahkan, sedangkan dengan ciphertext-only attack lebih sulit.

c. Cipher abjad-majemuk (Polyalpabetic substitution cipher)

Polyalphabetic merupakan cipher substitusi-ganda (multiple-substitution cipher) yang melibatkan penggunaan kunci berbeda. Cipher abjad-majemuk dibuat dari sejumlah cipher abjadtunggal, masing-masing dengan kunci yang berbeda.

d. Cipher substitusi poligram (Polygram substitution cipher)

Pada chipper ini blok karakter disubstitusi dengan blok cipherteks. Misalnya ABA diganti dengan RTQ, ABB diganti dengan SLL, dan lainlain.

2. Transposition Chipers

Pada cipher transposisi, plainteks tetap sama, tetapi urutannya diubah. Dengan kata lain, algoritma ini melakukan transpose terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah permutasi, karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.

Contoh:

Misalkan plainteks adalah

DEPARTEMEN TEKNIK INFORMATIKA ITS

Untuk meng-enkripsi pesan, plainteks ditulis secara horizontal dengan lebar kolom tetap, misal selebar 6 karakter (kunci k = 6):

```
DEPART
EMENTE
KNIKIN
FORMAT
IKAITS
```

maka cipherteksnya dibaca secara vertikal menjadi

```
DEKFIEMNOKPEIRAANKMIRTIATTENTS
```

Untuk mendekripsi pesan, kita membagi panjang cipherteks dengan kunci. Pada contoh ini, kita membagi 30 dengan 6 untuk mendapatkan 5.

Algoritma dekripsi identik dengan algoritma enkripsi. Jadi, untuk contoh ini, kita menulis cipherteks dalam baris-baris selebar 5 karakter menjadi:

```
DEKFI
EMNOK
PEIRA
ANKMI
RTIAT
TENTS
```

Dengan membaca setiap kolom kita memperoleh pesan semula:

DEPARTEMEN TEKNIK INFORMATIKA ITS

BAB III.
Penutup

1. Kesimpulan

Dari penjelasan yang disebutkan diatas maka kesimpulannya yaitu, Chipers subtitusi adalah algoritma kriptografi yang mengganti (menyulih atau mensubstitusi) setiap karakter dengan karakter lain dalam susunan abjad (alfabet). Misalnya, tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan akjad. Adapun jenis – jenisnya yaitu Cipher abjad-tunggal (monoalphabetic cipher atau cipher substitusi sederhana - simple substitution cipher), Cipher substitusi homofonik (Homophonic substitution cipher), Cipher abjad-majemuk (Polyalpabetic substitution cipher), dan Cipher substitusi poligram (Polygram substitution cipher).

Sedangkan cipher transposisi adalah algoritma yang melakukan transpose terhadap rangkaian karakter di dalam teks Nama lain untuk metode ini adalah permutasi, karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.

Mungkin untuk penjelasan cukup sampai disini, apabila terdapat kesalahan penulis berharap agar dosen dapat memakluminya. Terima kasih, salam.

Daftar Pustaka

Munir, Rinaldi. 2004. “Algoritma Kriptografi Klasik”, https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Algoritma%20klasik.pdf , diakses pada 07 Januari 2022 pukul 23.09 WIB.

Widiyono. 2022. “Sistem Keamanan”, https://drive.google.com/file/d/1XdzLcOQQD8rGHZ1TL3YIQgYfdyjB4AiF/view , diakses pada 07 Januari 2022 pukul 23.12 WIB.