PERTEMUAN 03

ALGORITMA KRIPTOGRAFI KLASIK

Sub Pembahasan

1. Algoritma
2. Ciri-Ciri
3. Alasan
4. Jenis-Jenis Kriptografi Klasik

Algoritma Kriptografi Klasik

Sebelum komputer ada, kriptografi dilakukan menggunakan pensil dan kertas.

Algoritma kriptografi (cipher) yang digunakan saat itu, dinamakan juga algoritma klasik, adalah berbasis karakter, yaitu enkripsi dan dekripsi dilakukan pada setiap karakter pesan.

Semua algoritma klasik termasuk ke dalam sistem kriptografi simetris dan digunakan jauh sebelum kriptografi kunci publik ditemukan.

Kriptografi klasik memiliki beberapa ciri:

1. Berbasis karakter
2. Menggunakan pena dan kertas saja, belum ada computer
3. Termasuk ke dalam kriptografi kunci simetris

Tiga alasan mempelajari algoritma klasik:

1. Memahami konsep dasar kriptografi
2. Dasar algoritma kriptografi modern
3. Memahami kelemahan sistem kode.

(Ariyus, Dony. 2008)

Algoritma kriptografi klasik

Algoritma kriptografi klasik dapat dikelompokkan ke dalam dua macam cipher, yaitu :

1. Cipher substitusi (substitution cipher)

Di dalam cipher substitusi setiap unit plainteks diganti dengan satu unit cipherteks. Satu “unit” disini berarti satu huruf, pasangan huruf, atau dikelompokkan lebih dari dua huruf.

Algoritma substitusi tertua yang diketahui adalah Caesar cipher yang digunakan oleh kaisar Romawi , Julius Caesar (sehingga dinamakan juga casear cipher), untuk mengirimakan pesan yang dikirimkan kepada gubernurnya.

2. Cipher transposisi (transposition cipher)

Pada cipher transposisi, huruf-huruf di dalam plainteks tetap saja, hanya saja urutannya diubah.

Dengan kata lain algoritma ini melakukan transpose terhadap rangkaian karakter di dalam teks.

Nama lain untuk metode ini adalah permutasi atau pengacakan (scrambling) karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.(Munir.2006)

Jenis-Jenis Cipher Substitusi

- Cipher substitusi abjad-tunggal (Monoalphabetic Cipher)
- Cipher Substitusi Homofonik (Homophonic Substitution Cipher)
- Cipher Substitusi Abjad-Majemuk (Polyalphabetic Substitution Cipher)
- Cipher Substitusi Poligram (Polygram Substitution Cipher)

Cipher substitusi abjad-tunggal

(Monoalphabetic Cipher)

Jenis cipher substitusi ini sering juga disebut cipher substitusi sederhana.

Ide cipher substitusi abjad-tunggal adalah menggantikan satu karakter pada plainteks menjadi satu karakter pada cipherteks dengan aturan tertentu.

Fungsi ciphering-nya merupakan fungsi satu ke satu. (mengganti setiap huruf pada plainteks dengan huruf yang bersesuaian).

Pada metode ini string kunci menjadi huruf-huruf awal subtitusi dari plaintext. Setiap huruf dalam kunci hanya diperkenankan muncul sekali.

Berikut contoh penggunaan monoalphabetic chiper.

Contoh kunci: PASSWORD RAHASIAKU

Dikarenakan setiap huruf dalam kunci hanya diperkenan muncul sekali, kunci tersebut kita sederhanakan menjadi: PASWORDHIKU

Plain alphabet

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

Cipher alphabet

Contoh:

Plain text : Ku titipkan rindu pada langit yg kau tatap

Cipher text: Uq ninigupe liewq gpwp bpedin xd upq npnpg

Jenis-Jenis Kriptografi Klasik

1. Vigènere cipher
2. Autokey Cipher
3. Reverse Cipher
4. Zig-Zag Cipher
5. Segitiga Cipher
6. Super Enkripsi
7. Enigma Machine

Vigènere cipher

Vigenere cipher mungkin adalah contoh terbaik dari cipher alphabet-majemuk ‘manual’.

Algoritma ini dipublikasikan oleh diplomat (sekaligus seorang kriptologis) perancis, Blaise de Vigènere pada abad 16.

Vigènere cipher dipublikasikan pada tahun 1586. Cipher ini berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan abad 19. Vigènere cipher digunakan oleh tentara Konfiderasi (Confederate Army) pada perang sipil Amerika (American Civil war).

Vigènere cipher sangat dikenal karena mudah dipahami dan diimplementasikan. Cipher menggunakan bujursangkar Vigènere untuk melakukan enkripsi. Kolom paling kiri dari bujursangkar menyatakan huruf-hurf kunci, sedangkan baris paling atas menyatakan huruf-huruf plainteks. Setiap baris dalam bujursangkar menyatakan huruf-huruf cipherteks, yang mana jumlah pergesaran huruf plainteks ditentukan nilai numerik huruf kunci tersebut (yaitu, A = 0, B = 1, C = 2,…, Z = 25).

- Bujursangkar vigènere digunakan untuk memperoleh cipherteks dengan menggunakan kunci yang sudah ditentukan. Jika panjang kunci lebih pendek dari pada panjang plainteks, maka kunci diulang penggunaanya (sistem periodik). Bila panjang kunci adalah m, maka periodenya dikatakan m.
- Contoh, plainteks: PENJAGA HATI
- Kunci adalah smile
- maka penggunaan kunci secara periodik adalah sebagai berikut:

- Plainteks : PENJAGA HATI
- Kunci : SMILESM ILES
- Cipherteks: HQVEYM OLXA

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

Autokey Cipher

Kriptografi Autokey adalah pengembangan dari kriptografi Caesar dan Vigenere.

Cara melakukan enkripsi sama seperti kedua kriptografi sebelumnya.

Pada kriptografi Autokey juga digunakan sebuah kata sebagai kunci. Kunci ini kemudian diikuti dengan plaintext sehingga membentuk huruf-huruf yang sama panjang dengan plaintext. Urutan huruf-huruf ini yang akan digunakan sebagai kunci pada saat enkripsi.

Rumus yang berlaku untuk kriptografi Autokey sama seperti Caesar dan Vigenere.

Contoh

Plaintext: INI PESAN RAHASIA

Kunci: BESOK

Maka kata BESOK akan disisipkan di depan plaintext INI PESAN RAHASIA.

Kemudian enkripsi dilakukan sama dengan enkripsi Caesar dan Vigenere.

Reverse Cipher

- Adalah contoh kriptografi klasik yang menggunakan substitusi yaitu mengganti satu huruf dengan huruf lain ataupun mengubah suatu kalimat dengan menuliskan setiap kata secara terbalik.
- Ini contoh yang paling sederhana dari transposisi yaitu mengubah suatu kalimat dengan menuliskan setiap kata secara terbalik.
- Contoh Kriptografi Reverse:
- Plaintext : KU TITIP RINDU PADA HUJAN
- Ciphertext : UK PITIT UDNIR ADAP NAJUH

Pada kriptografi kolom (column cipher), plaintext disusun dalam kelompok huruf yang terdiri dari beberapa huruf. Kemudian huruf-huruf dalam kelompok ini dituliskan kembali kolom per kolom, dengan urutan kolom yang bisa berubah-ubah.

- Contoh Kriptografi Kolom:
- Kalimat ‘ AYAH SUDAH TIBA KEMARIN SORE ’, jika disusun dalam kolom 7 huruf, maka akan menjadi kolom - kolom berikut :

AYAHSUD
AHTIBAK
EMARINS
OREAAAA

- Untuk melengkapi kolom terakhir agar berisi 7 huruf, maka sisanya diisi dengan huruf ‘A’atau bisa huruf apa saja sebagai huruf pelengkap. Kalimat tesebut setelah dienkripsi dengan 7 kolom huruf dan urutan kunci 6725431, maka hasil enkripsinya:
- DKSAATAEUANASBIAHIRAAAEOYHMR

Zig-Zag Cipher

- Pada kriptografi kolom zig-zag, plaintext disusun dalam kelompok huruf yang terdiri dari beberapa huruf. Kemudian huruf-huruf dalam uruta kolom yang dimasukkan secara pola zig-zag.

Segitiga Cipher

- Pada kriptografi kolom Triangle, plaintext disusun dalam kelompok huruf yang terdiri dari beberapa huruf. Kemudian huruf-huruf dalam urutan kolom yang dimasukkan secara pola segitiga.

Super Enkripsi

- Kombinasi Antara Cipher Substitusi (Caesar Cipher) dan Cipher Tranposisi (Column Cipher). Sehingga memperoleh Cipher yang lebih kuat (Super) dari pada Satu Cipher saja.

Daftar Pustaka

- https://www.alfianaramadhani.web.id/2016/10/kriptografi-2-pertemuan-4.html
- https://asyafaat.files.wordpress.com/2009/05/achmadsyafaat-perbandingan_kriptografi_cipher_substitusi_homofonikpoligram_dg_caesar-cipher.pdf

TUGAS INDIVIDU

Membuat contoh kriptografi klasik