Jurnal Mahajana Informasi, Vo.4, No.2, 2019
e-ISSN:2527-8290

PENGAMANAN PESAN MENGGUNAKAN ALGORITMA HILL CIPHER DALAM KEAMANAN KOMPUTER

Akbar Serdano[1)], **Muhammad Zarlis**[2)], **Sawaluddin**[3)], **Dedy Hartama**[4)]
[1,2,3,4)] Teknik Informatika S2, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara, Medan
Jl. Abdul Hakim No.1, Padang Bulan, Kec. Medan Baru, Kota Medan, Sumatera Utara 20222
e-mail : akbarserdano27@gmail.com

Abstrak

Dalam sebuah pengamanan data atau informasi pastinya memiliki teknik untuk mengamankan data atau informasi. Kriptografi menjadi salah satu teknik dalam enkripsi (merubah informasi menjadi bentuk yang tidak dimengerti) dan dekripsi (mengembalikan informasi dari bentuk yang tidak dimengerti menjadi informasi aslinya). Ada dua sebutan dalam proses enkripsi dan dekripsi yang digunakan yaitu plainteks merupakan pesan atau informasi asli dan cipherteks yang merupakan hasil dari penyandian.

Algortima hill cipher merupakan salah satu bagian dari algoritma kriptografi yang sangat sulit untuk dipecahkan oleh kriptanalis. Dalam algoritma hill cipher proses yang dilakukan dengan menggunakan matriks kunci dan modulo. Setiap karakter yang berada di plainteks maupun cipherteks akan dikonversikan kedalam bentuk angka atau desimal. Enkripsi dilakukan dengan mengalikan matriks kunci dengan matriks plainteks, sedangkan Dekripsi dilakukan dengan mengalikan invers matriks kunci dengan matriks cipherteks. Matriks yang digunakan pada hill cipher adalah matriks persegi, yang dimana memanfaatkan matriks persegi sebagai matriks kunci untuk plainteks dan cipherteks. Plainteks maupun cipherteks yang digunakan berupa angka huruf dan simbol yang dikonversikan sebanyak 29 karakter.

***Kata Kunci** : Hill Chiper, Cryptography, Enkripsi, Dekripsi, Plainteks*

1. PENDAHULUAN

Dalam suatu informasi terdapat adanya pertukaran data atau informasi dalam proses pengiriman pesan. Pertukaran data atau informasi ini membuat hal yang sangat penting dalam menjaga kerahasiaan data atau informasi tersebut. Pentingnya kerahasiaan tentu harus disertai dengan keamanan informasi (information security). Keamanan informasi pastinya berkaitan dengan keamanan komputer (computer security). Dalam menjaga keamanan informasi terdapat suatu teknik pengamanan informasi yang dikenal dengan kriptografi. Teknik kriptografi bertujuan untuk menjaga kerahasiaan, keaslian data atau informasi serta keaslian pengirim.

Algoritma Hill Cipher merupakan salah satu dari algoritma kriptografi yang cukup baik karena berproses menggunakan operasi matriks dan modulus. Proses dari algoritma hill cipher dalam setiap karakter plainteks maupun cipherteks dikonversikan kedalam bentuk angka atau desimal. Proses enkripsi membutuhkan matriks persegi sebagai mengalihkan dengan matriks plainteks, sedangkan proses dekripsi membutuhkan matriks invers yang untuk mengalihkan dengan cipherteks. Matriks persegi digunakan dalam proses enkripsi dan dekripsi (matriks kunci). Dalam Paper ini, memodifikasi bentuk huruf ditambahkan simbol pada plainteks maupun cipherteks yang dikonversikan sebanyak 29 karakter.

2. TINJAUAN PUSTAKA

2.1. KRIPTOGRAFI

Kriptografi (cryptography) berasal dari Bahasa Yunani: ”cryptos” artinya ”secret” (rahasia), sedangkan ”graphein” artinya ”writing” (tulisan), Jadi, kriptografi berarti ”secret writing” (tulisan rahasia). Kriptografi adalah ilmu yang dimana mengajari teknik-teknik matematika yang berkaitan dengan aspek keamanan berupa data maupun informasi seperti kerahasiaan, integritas data, serta otentikasi.(Munir, Rinaldi, 2007)

Definisi yang dikemukakan pada buku bahwa kriptografi adalah ilmu dan seni yang dapat menjaga kerahasiaan pesan dengan teknik menyandikannya sehingga pesan tersebut tidak dapat dibaca dan tidak mempunyai maknanya. Definisi ini mungkin berkaitan dengan masa lalu yang dimana memanfaatkan kriptografi sebagai keamanan komunikasi seperti komunikasi di kalangan militer, diplomat, dan mata-mata. Namun saat ini berkembangnya teknologi kriptografi lebih dari sekadar privacy, tetapi juga sebagai data integrity, authentication, dan non-repudation.

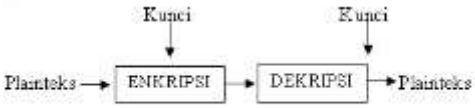
2.1.1. ENKRIPSI

Enkripsi merupakan bagian dari kriptografi, dimana merupakan hal yang sangat penting untuk menjaga data yang dikirimkan dapat terjaga kerahasiaannya. Enkripsi juga disebut cipher atau kode, di

mana pesan asli (plainteks) dapat diubah menjadi kode-kode tersendiri sesuai metode yang disepakati oleh kedua belah pihak, baik pihak pengirim pesan maupun penerima pesan.(Pramono Andy, 2009)

2.1.2. DEKRIPSI

Dekripsi merupakan proses sebaliknya dari enkripsi yaitu mengembalikan kode-kode atau informasi yang telah dilacak kebentuk file aslinya dengan menggunakan kunci.(Munawar, 2012)

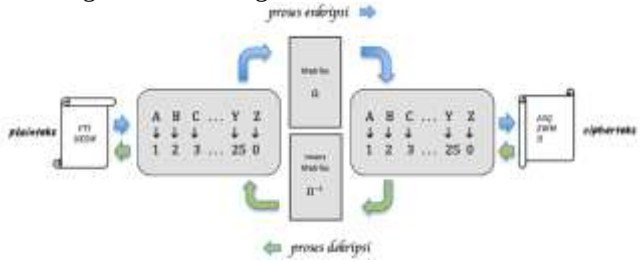


Gambar 1. Proses Enkripsi dan Dekripsi

2.2. ALGORITMA HILL CIPHER

Hill cipher yang merupakan polyalphabetic cipher dapat dikategorikan sebagai block cipher, karena teks yang akan diproses akan dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama pula (Widyanarko, arya. 2007).

Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi. Hill Cipher diciptakan oleh Lester S. Hill pada tahun 1929. Hill Cipher tidak mengganti setiap abjad yang sama pada plainteks dengan abjad lainnya yang sama pada cipherteks karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya.(Anton, H. & Rorres, C., 2005) Hill Cipher termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas cipherteks saja. Namun, teknik ini dapat dipecahkan dengan cukup mudah apabila kriptanalis memiliki berkas cipherteks dan potongan berkas plainteks. Teknik kriptanalisis ini disebut known-plainteks attack. (Widyanarko, arya. 2007). Proses enkripsi-dekripsi Hill cipher secara umum dapat digambarkan sebagai berikut.



Gambar 2. Proses Enkripsi-Dekripsi Hill cipher

Matriks bujursangkar Ω berordo $n \times n$ yang mempunyai invers untuk dijadikan kunci. Misalkan P sebagai plainteks yaitu dan C sebagai cipherteks sehingga proses enkripsi adalah :

$$C=\Omega \cdot P \ (mod\ 26)$$

Proses dekripsi secara umum diberikan :

$$P=\Omega-1 \cdot C \ (mod\ 26)$$

(Alz Danny Wowor, 2013)

2.2.1. TEKNIK ENKRIPSI PADA HILL CIPHER

Proses enkripsi pada Hill Cipher dilakukan per blok plainteks. Ukuran blok tersebut sama dengan ukuran matriks kunci. Sebelum membagi teks menjadi deretan blok-blok, plainteks terlebih dahulu dikonversi menjadi angka, masing-masing sehingga A=0, B=1, hingga Z=25.(Hill, Lester, S., 1929) Secara matematis, proses enkripsi pada Hill Cipher adalah:

C = K . P

C = Cipherteks

K = Kunci

P = Plainteks

Gambar 3. Ilustrasi Proses Enkripsi Hill Cipher

2.2.2. TEKNIK DEKRIPSI PADA HILL CIPHER

Proses dekripsi pada Hill Cipher pada dasarnya sama dengan proses enkripsinya. Namun matriks kunci harus dibalik (invers) terlebih dahulu. Secara matematis, proses dekripsi pada Hill Cipher dapat diturunkan dari persamaan .

C = K . P

K^{-1} . C = K^{-1} . K . P

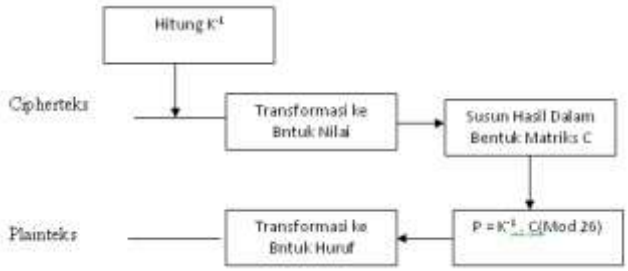
K^{-1} . C =I . P

P = K^{-1} . C

Persamaan yang digunakan : P = K^{-1} . C

Di mana untuk menentukan K^{-1} dengan menggunakan rumus:

1/det K mod 26 x atau (detK * x mod 26 = 1)



Gambar 4. Ilustrasi Proses Dekripsi Hill Cipher

3. HASIL DAN PEMBAHASAN

Proses pertama dalam algortima hill cipher adalah menkoversikan plainteks kedalam bentuk angka, sehingga masing-masing karakter menjadi A = 0, B = 1 sampai simbol ; = 28. Proses enkripsi yang dilakukan membentuk perblok plainteks. Ukuran blok harus sama dengan ukuran baris matriks kunci.

Tabel 1. Konversi Karakter ke Desimal

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Q	R	S	T	U	V	W	X	Y	Z	.	,	;
16	17	18	19	20	21	22	23	24	25	26	27	28

Secara matematis, proses enkripsi pada hill cipher adalah:
C = K . P
C = Cipherteks
K = Kunci
P = Plainteks

3.1. PROSES ENKRIPSI

Plainteks : AKBARSER.

A	K	B	A	R	S	E	R	.
0	10	1	0	17	18	4	17	26

Baris dan kolom yang dipakai pada matriks kunci adalah 3 x 3 berdasarkan sesuai karakter dari plainteks yang digunakan.

$$\begin{pmatrix} 5 & 18 & 25 \\ 9 & 13 & 2 \\ 11 & 21 & 8 \end{pmatrix}$$

Matriks kunci (K)

Dari plaiteks yang digunakan akan dibagi menjadi per 3 bagian untuk dikalikan dengan matriks kunci. Rumus yang digunakan dalam menetukan Cipherteks adalah :
C = K x P mod 29

1. Blok 1 Plainteks

A	K	B
0	10	1

$$C_1 = \begin{pmatrix} 5 & 18 & 25 \\ 9 & 13 & 2 \\ 11 & 21 & 8 \end{pmatrix} \times \begin{pmatrix} 0 \\ 10 \\ 1 \end{pmatrix} \bmod 29$$

$$= \begin{pmatrix} 205 \\ 132 \\ 18 \end{pmatrix} \bmod 29$$

$$= \begin{pmatrix} 2 \\ 16 \\ 15 \end{pmatrix} \rightarrow \begin{matrix} C \\ Q \\ P \end{matrix}$$

2. Blok 2 Plainteks

A	R	S
0	17	18

$$C_2 = \begin{pmatrix} 5 & 18 & 25 \\ 9 & 13 & 2 \\ 11 & 21 & 8 \end{pmatrix} \times \begin{pmatrix} 0 \\ 17 \\ 18 \end{pmatrix} \bmod 29$$

$$= \begin{pmatrix} 756 \\ 257 \\ 501 \end{pmatrix} \bmod 29$$

$$= \begin{pmatrix} 2 \\ 25 \\ 8 \end{pmatrix} \rightarrow \begin{matrix} C \\ Z \\ I \end{matrix}$$

3. Blok 3 Plainteks

E	R	.
4	17	26

$$C_3 = \begin{pmatrix} 5 & 18 & 25 \\ 9 & 13 & 2 \\ 11 & 21 & 8 \end{pmatrix} \times \begin{pmatrix} 4 \\ 17 \\ 26 \end{pmatrix} \bmod 29$$

$$= \begin{pmatrix} 976 \\ 309 \\ 609 \end{pmatrix} \bmod 29$$

$$= \begin{pmatrix} 19 \\ 19 \\ 0 \end{pmatrix} \rightarrow \begin{matrix} T \\ T \\ A \end{matrix}$$

Cipherteks yang dihasilkan dari enkripsi adalah sebagai berikut :

C	Q	P	C	Z	I	T	T	A
2	16	15	2	25	8	19	19	0

3.2. PROSES DEKRIPSI

Proses kedua dalam algortima hill cipher adalah dekripsi yang bertujuan untuk menghasilkan kembali plainteks. Dalam proses dekripsi pada hill cipher prosesnya sama dengan enkripsinya. Untuk melakukan proses deksripsi matriks

kunci harus dibalik (invers) untuk mendapatkan persamaan sebagai berikut :
$C = K . P$
$K^{-1} . C = K^{-1} . K . P$
$K^{-1} . C = I . P$
$P = K^{-1} . C$
Persamaan yang digunakan adalah : $P = K^{-1} . C$

Tahap pertama adalah mencari nilai invers matriks kunci yang akan digunakkan invers modulo determinan matriks kunci. Dengan rumus invers matriks kunci sebagai berikut :

$K^{-1} = A^{-1} \times Adj(k) \bmod 29$

$$\begin{pmatrix} 5 & 18 & 25 \\ 9 & 13 & 2 \\ 11 & 21 & 8 \end{pmatrix}$$
Matriks kunci (K)

Matriks kunci (K) untuk determinan yang didapatkan adalah det(k) = 560, Maka nilai det(k) akan dipakai kedalam A^{-1}. Nilai A yang diketahui adalah sebagai berikut :

A = det(k) mod 29
= 260 mod 29
= 9

Maka perhitungan invers modulo-nya adalah
$9^{-1} \bmod 29$
$9x = 1 \bmod 29$
$9x = 1 + 29k$
x = (1+26k)/9; Nilai k = n sehingga hasil x adalah bilangan bulat.

k = 0 maka,
x = (1+29*0)/9 = 1/9 (bukan bilangan bulat)
k = 1 maka,
x = (1+29*1)/9 = 10/3 (bukan bilangan bulat)
k = 2 maka,
x = (1+29*2)/9 = 59/9 (bukan bilangan bulat)
k = 3 maka,
x = (1+29*3)/9 = 88/9 (bukan bilangan bulat)
k = 4 maka,
x = (1+29*4)/9 = 13 (bilangan bulat)

Sehingga invers dari 9 mod 29 ekuivalen dengan 13 mod 29 yaitu 13. Nilai 13 dinamakan sebagai nilai multiplikatif determinan yang berguna untuk memudahkan mencari nilai invers matriks terutama nilai invers matriks tidak bernilai pecahan. Selanjutnya menghitung nilai invers matriks kunci, untuk menghitung nilai invers matriks kunci tentunya memerlukan adj(k) yang harus dihasilkan.

$$adj(k) = \begin{pmatrix} 4 & 4 & 1 \\ 8 & 26 & 12 \\ 17 & 6 & 19 \end{pmatrix}$$

***Catatan :**
Untuk modulo bilangan negatif dapat diperoleh dengan cara. Misal : -27 mod 26 = -n mod x, maka :
-n mod x = x-(n mod x)
-27 mod 26 = 26-(27 mod 26)
-27 mod 26 = 26-1
-27 mod 26 = 25

$$k^{-1} = 13 \begin{pmatrix} 4 & 4 & 1 \\ 8 & 26 & 12 \\ 17 & 6 & 19 \end{pmatrix}$$
$$= \begin{pmatrix} 52 & 52 & 13 \\ 104 & 338 & 156 \\ 221 & 78 & 247 \end{pmatrix} \bmod 29$$
$$= \begin{pmatrix} 23 & 23 & 13 \\ 17 & 19 & 11 \\ 18 & 20 & 15 \end{pmatrix}$$

Untuk proses dekripsi cipherteks yang digunakan adalah sebagai berikut :

C	Q	P	C	Z	I	T	T	A
2	16	15	2	25	8	19	19	0

1. Blok 1 Cipherteks

C	Q	P
2	16	15

$$P_1 = \begin{pmatrix} 23 & 23 & 13 \\ 17 & 19 & 11 \\ 18 & 20 & 15 \end{pmatrix} \times \begin{pmatrix} 2 \\ 16 \\ 15 \end{pmatrix} \bmod 29$$
$$= \begin{pmatrix} 609 \\ 503 \\ 581 \end{pmatrix} \bmod 29$$
$$= \begin{pmatrix} 0 \\ 10 \\ 1 \end{pmatrix} \rightarrow \begin{matrix} A \\ K \\ B \end{matrix}$$

2. Blok 2 Cipherteks

C	Z	I
2	25	8

$$P_2 = \begin{pmatrix} 23 & 23 & 13 \\ 17 & 19 & 11 \\ 18 & 20 & 15 \end{pmatrix} \times \begin{pmatrix} 2 \\ 25 \\ 8 \end{pmatrix} \bmod 29$$
$$= \begin{pmatrix} 725 \\ 597 \\ 656 \end{pmatrix} \bmod 29$$
$$= \begin{pmatrix} 0 \\ 17 \\ 18 \end{pmatrix} \rightarrow \begin{matrix} A \\ R \\ S \end{matrix}$$

3. Blok 3 Cipherteks

T	T	A
19	19	0

$$P_3 = \begin{pmatrix} 23 & 23 & 13 \\ 17 & 19 & 11 \\ 18 & 20 & 15 \end{pmatrix} \times \begin{pmatrix} 19 \\ 19 \\ 0 \end{pmatrix} \bmod 29$$

$$= \begin{pmatrix} 874 \\ 684 \\ 722 \end{pmatrix} \bmod 29$$

$$= \begin{pmatrix} 4 \\ 17 \\ 26 \end{pmatrix} \rightarrow \begin{matrix} E \\ R \\ . \end{matrix}$$

Plainteks yang dihasilkan dari dekripsi adalah sebagai berikut :

A	K	B	A	R	S	E	R	.
0	10	1	0	17	18	4	17	26

4. KESIMPULAN DAN SARAN

4.1. KESIMPULAN

Berdasarkan hasil yang dilakukan, maka dapat diambil kesimpulan sebagai berikut:

1. Kriptografi algoritma hill cipher dapat dimodifikasi dengan menambahkan banyak karakter yang di konversikan kedalam angka atau desimal yang digunakan sebagai penentuan plainteks dan cipherteks.
2. Algoritma hill cipher sebaiknya menggunakan modulus bilangan prima sehingga memudahkan matriks yang memiliki invers determinan dan dapat sebagai matriks kunci yang baik.
3. Algoritma hill cipher dapat diterapkan dalam berbagai pengamanan data maupun pesan.

4.2. SARAN

Berikut saran-saran untuk pengembangan algoritma hill cipher:

1. Algoritma hill cipher masih perlu dikembangkan lebih lanjut untuk dapat digabungkan dengan algoritma kriptografi lainnya.
2. Sebaiknya dalam penggunaan karakter yang akan digunakan kedalam plainteks dan cipherteks akan lebih baik karakter atau modulus yang dipakai lebih besar sehingga sulit dibaca oleh orang lain.

DAFTAR PUSTAKA

Munir, Rinaldi, 2007, Kriptografi, Penerbit Informatika, Bandung.

Pramono Andy dan sujjada Alun," Implementasi Algoritma Hill Cipher Sebagai media Steganografi Mneggunakan Metode LSB, 2009.

Munawar, "Perancangan Algoritma Sistem Keamanan Data Menggunakan Metode Kriptografi Asimetris ", Vol.1, 2012.

Widyanarko, arya. 2007. Studi dan Analisis mengenai Hill Cipher, Teknik Kriptanalisis dan Upaya Penanggulangannya. Bandung: Fakultas Teknik ITB

Anton, H. & Rorres, C., 2005, Elementary Linear Algebra, Applications Version, 9th Edition, New York: John Wiley & Sons.

Alz Danny Wowor, 2013, Modifikasi Kriptografi Hill Cipher Menggunakan Convert Between Base, Seminar Nasional Sistem Informasi Indonesia (SESINDO), Bali 2-4 Desember 2005, ITS Surabaya.

Hill, Lester, S., 1929, Cryptography in an Algebraic Alphabet: The American Mathematical Monthly, 36 (6), pp.306-312.