KRIPTOGRAFI HILL CIPHER WITH ANY KEY MATRICES SEBAGAI PENGEMBANGAN KRIPTOGRAFI ALGORITMA HILL CIPHER

Albertus Yogo Prayitno[1)], Maria Anggit Pasca Patriana[2)]
[1]Fakultas Keguruan dan Ilmu Pendidikan, Universitas Sanata Dharma
email: albertusyogoprayitnoo@gmail.com
[2]Fakultas Keguruan dan Ilmu Pendidikan, Universitas Sanata Dharma
email: patrianaanggit@gmail.com

Abstract

Pengiriman sebuah informasi melalui jaringan internet, perlu memperhatikan tingkat keamanan. Oleh sebab itu informasi harus dijaga supaya informasi yang dikirim dapat diterima oleh orang yang tepat. Salah satu cara untuk menjaga keamanan sebuah informasi adalah dengan menggunakan kriptografi. Penelitian sebelumnya telah mengkaji mengenai kinerja algoritma kriptografi dengan mengunakan modifikasi Algoritma Hill Cipher.

Penelitian ini bertujuan untuk mengembangkan modifikasi Algoritma Hill Cipher tersebut, yaitu membuat orang lebih leluasa dalam memilih matriks kunci. Matriks kunci yang digunakan tidak hanya matriks yang berdeterminan 1, namun matriks berordo 2×2 dan invertible. Penggunaan modulo dalam pengembangan Algoritma Hill Cipher yaitu modulo 33.

Penelitian ini menggunakan metode kajian pustaka yang bersifat pengembangan dengan membangun sebuah sistem untuk melakukan uji coba dan analisis.

Hasil penelitian ini menunjukkan bahwa dengan menggunakan pengembangan Algoritma Hill Cipher (Hill Cipher With Any Key Matrices), penyandian menjadi lebih leluasa dalam memilih matriks kunci, karena matriks kunci yang digunakan tidak hanya yang berdeterminan 1. Untuk penyandian tersebut peneliti menggunakan sifat invers matriks, yaitu $(kA)^{-1} = \frac{1}{k} A^{-1}$ *dengan k sebagai suatu skalar tidak sama dengan 0 dan A sebagai sebarang matriks. Akibatnya matriks kunci bisa diambil lebih umum dan bisa dikembangkan, yaitu harus berbentuk* $A = \frac{1}{detB} B$*. Keberhasilan metode ini sama dengan menggunakan Hill Cipher. Hal ini ditunjukan dengan beberapa contoh.*

Keywords: *informasi, kriptografi, algoritma hill cipher,any key matriks, modulo.*

1. PENDAHULUAN

Pada era globalisasi, segala aspek kehidupan manusia dimudahkan oleh jaringan internet, salah satunya dalam bidang ekonomi. E-Commerce secara umum dapat diartikan sebagai transaksi jual beli secara elektronik melalui media internet. Transaksi jual beli melalui internet melibatkan pertukaran informasi antara penjual dan pembeli. Namun pengiriman informasi melaui internet baik dari penjual mapun pembeli, mempunyai risiko di bidang keamanan yaitu dapat disadap dan dimodifikasi oleh cryptanalys. Oleh sebab itu informasi memerlukan pengamanan yan baik saat didistribusikan ataupun saat disimpan.

Salah satu metode yang dapat digunakan sebagai pengamanan data adalah kriptografi. Untuk menentukan algoritma kriptografi perlu dipertimbangkan kekuatan kunci terhadap serangan cryptanalis dan pertimbangan kecepatan dalam proses enkripsi dan deskripsi.

Menurut Lisda Juliana Pangaribuan dalam jurnal teknologi informasi dan komunikasi, Algoritma hill chipper merupakan penerapan arithmetic modulo pada kriptrografi. Teknik kriptrografi ini mengunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan deskripsi. Namun dalam pemilihan matriks kunci dalam algoritma hill cipher masih terbatas, yakni matriks harus berdeterminan 1. Penelitian ini bertujuan untuk mengembangkan modifikasi Algoritma Hill Cipher tersebut, yaitu membuat orang lebih leluasa dalam memilih matriks kunci. Matriks kunci yang digunakan tidak hanya

matriks yang berdeterminan 1, namun matriks berordo 2×2 dan invertible. Penggunaan modulo dalam pengembangan Algoritma Hill Cipher yaitu modulo 33.

2. KAJIAN LITERATUR DAN PEGEMBANGAN HIPOTESIS

Algoritma enkripsi hill cipher diawali dengan menentukan plaintext kemudian korespodensikan abjad pada plaintext dengan bilangan (pada kasus ini bilangannya adalah 0 sampai 32), kemudian tentukan matriks kunci dimana matriks kunci adalah matriks persegi yang memiliki determinan dan invertible yaitu memiliki multiplicative inverse atau A^{-1}. Matriks kunci harus memiliki determinan yang relative prima dengan 33 atau gcd (d,33) = 1. Setelah itu buatlah matriks yang entri-entrinya terdiri dari bilangan yang berkorespondensi dengan abjad pada plaintext. Ordo matriks tersebut ditentukan sedemikian rupa agar bisa dikalikan dengan matriks kunci. Kemudian hitung ciphertext dengan ketentuan $C = A.P \bmod 33$

Dimana C = Ciphertext
P = Plaintext
A = Matriks Kunci

Setelah proses enkripsi dilakukan proses deskripsi. Algoritma deskripsi hill cipher dilakukan dengan mengorespodensikan abjad dengan numeric. Langkah kedua cari invers dari matriks kunci dengan rumus:

$A = \frac{1}{Det\ B} \times B$, dimana A adalah matriks kunci, Det B = nilai determinan matriks kunci

$A^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \times$ Adj A, dimana Adj = Adjoint matriks kunci

A^{-1} = Invers Matriks

Langkah terakhir hitung plaintext dengan rumus :

$P = A^{-1}.C \bmod 33$

Dimana P = Plaintext
A^{-1} = Invers matriks kunci
C = Ciphertext

3. METODE PENELITIAN

Penelitian ini menggunakan metode kajian pustaka yang bersifat pengembangan dengan membangun sebuah sistem untuk melakukan uji coba dan analisis. Kajian pustaka yang dikembangkan adalah sebuah artikel yang membahas tentang kriptografi hill chipper. Rancangan kegiatan penelitian yaitu membuktikan bahwa dalam pemilihan matriks kunci tidak hanya yang bedeterminan 1 saja. Cara pembuktiannya mengunakan sifat invers matriks, yaitu $(kA)^{-1} = \frac{1}{k} A^{-1}$ dengan k sebagai suatu skalar tidak sama dengan 0 dan A sebagai sebarang matriks. Akibatnya matriks kunci bisa diambil lebih umum dan bisa dikembangkan, yaitu harus berbentuk $A = \frac{1}{detB} B$. Melalui sifat invers matriks peneliti melakukan beberapa uji coba penyandian. Bahan dan alat yang digunakan adalah artikel yang kami kaji serta Microsoft exel.

4. HASIL DAN PEMBAHASAN

Pada artikel yang dikaji sebelumnya, telah dikaji contoh penyandian menggunakan algoritma *Hill cipher*. Kalimat yang disandikan adalah "YOU'RE GREAT". Pada pembahasan kali ini akan dibahas bagaimana melakukan penyandian kalimat "YOU'RE GREAT" dengan menggunakan Kriptografi Hill Cipher With Any Key Matrices (pengembangan dari kriptografi algoritma hill cipher).

Langkah pertama adalah memilih matriks kunci yang berbentuk $A = \frac{1}{detB} B$. kita pilih $B = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$ yang berdeterminan -2, sehingga matriks kuncinya menjadi $A = \frac{1}{-2} \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix} = \begin{bmatrix} -1 & -\frac{3}{2} \\ -2 & -\frac{5}{2} \end{bmatrix}$.

Selanjutnya dengan menggunakan tabel pada gambar 1, kita buat matriks berukuran 2×6 yang entri-entrinya terdiri dari bilangan yang berkorespondensi dengan abjad/tanda baca pada kalimat "YOU'RE GREAT" .

A	B	C	D	E	F	G	H	I	J	K
0	1	2	3	4	5	6	7	8	9	10
L	M	N	O	P	Q	R	S	T	U	V
11	12	13	14	15	16	17	18	19	20	21
W	X	Y	Z	.	,	!	?	'	-	
22	23	24	25	26	27	28	29	30	31	32

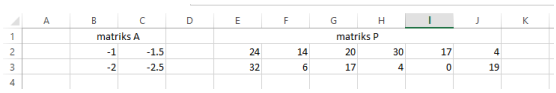
Gambar 1

Berdasarkan tabel di atas, diperoleh matriks sebagai berikut.

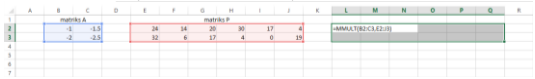
$P = \begin{bmatrix} 24 & 14 & 20 & 30 & 17 & 4 \\ 32 & 6 & 17 & 4 & 0 & 19 \end{bmatrix}$

Langkah selanjutnya adalah mencari hasil dari $C = A.P \bmod 33$. Untuk mempermudah perhitungan, gunakan bantuan Microsoft excel. Langkah-langkahnya sebagai berikut.

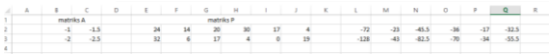
1. Ketik entri-entri dari matriks A dan P pada Microsoft excel sebagai berikut.



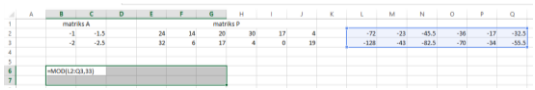
2. Block range yang kosong (dalam hal ini L2:Q3), sebagai tempat untuk memunculkan hasil perkalian matriks A dan P. kemudian ketik fungsi =MMULT(B2:C3,E2:J3).



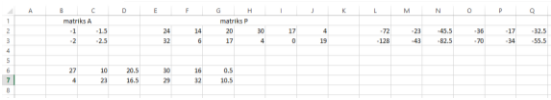
3. Tekan dan tahan secara bersamaan "**Ctrl+Shift"**, lalu tekan **"Enter**", maka pada range L2:Q3 akan muncul hasil perkalian matriks A dan P seperti gambar di bawah ini.



4. Block range yang kosong (dalam hal ini B6:G7), sebagai tempat untuk memunculkan hasil dari $A.P \ mod \ 33$. kemudian ketik fungsi =MOD(L2:Q3,33).



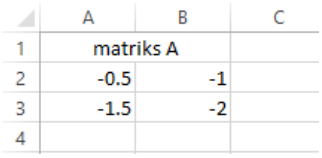
5. Tekan dan tahan secara bersamaan "**Ctrl+Shift"**, lalu tekan **"Enter**", maka pada range B6:G7 akan muncul hasil dari $A.P \ mod \ 33$ seperti gambar di bawah ini.



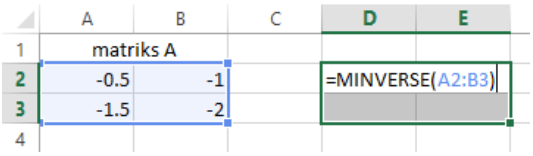
Hasil di atas bisa ditulis kembali menjadi $C = \begin{bmatrix} 27 & 10 & \frac{41}{2} & 30 & 16 & \frac{1}{2} \\ 4 & 23 & \frac{33}{2} & 29 & 32 & \frac{21}{2} \end{bmatrix}$, yang merupakan hasil akhir dari proses enkripsi. Hasil tersebut tidak bisa kita terjemahkan menjadi cipher text karena ada beberapa bilangan yang berbentuk pecahan. Hal tersebut tidak menjadi masalah, karena yang terpenting adalah kita dapat mengubah hasil tersebut (matriks C) menjadi bentuk semula (matriks P), yang dapat diterjemahkan menjadi pesan sebenarnya. Caranya adalah dengan mencari hasil dari $A^{-1}.C \ mod \ 33$.

Untuk mencari A^{-1}, kita juga bisa menggunakan bantuan Microsoft excel, yaitu dengan cara sebagai berikut.

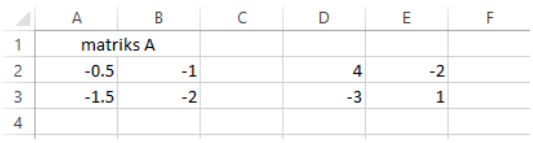
1. Ketik entri-entri dari matriks A pada Microsoft excel sebagai berikut.



2. Block range yang kosong (dalam hal ini D2:E3), sebagai hasil dari A^{-1}. Kemudian ketik fungsi =MINVERSE(A2:B3) seperti pada gambar di bawah ini.

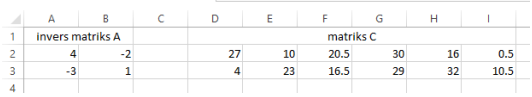


3. Tekan dan tahan secara bersamaan "**Ctrl+Shift**", lalu tekan "**Enter**", maka pada range D2:E3 akan muncul hasil dari A^{-1} seperti gambar di bawah ini.

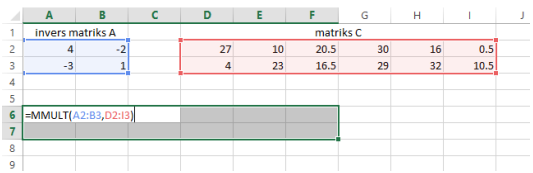


Selanjutnya kita akan mencari hasil dari $A^{-1}.C \ mod \ 33$. Langkah-langkahnya sebagai berikut.

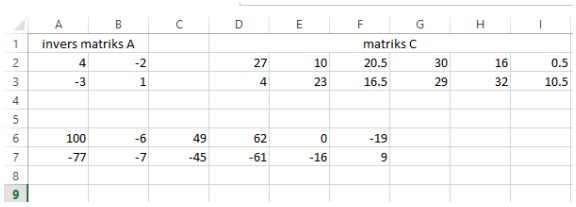
1. Ketik entri-entri matriks A^{-1} dan C pada micrisoft excel sebagai berikut.



2. Block range yang kosong (dalam hal ini A6:F7), sebagai tempat untuk memunculkan hasil perkalian matriks A^{-1}dan C. kemudian ketik fungsi =MMULT(A2:B3,D2:I3).

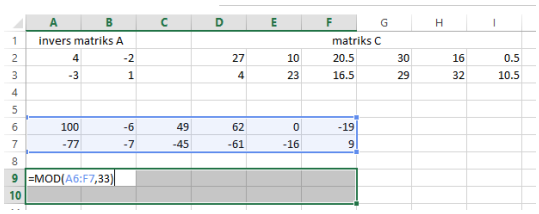


3. Tekan dan tahan secara bersamaan "**Ctrl+Shift"**, lalu tekan "**Enter**", maka pada range A6:F7 akan muncul hasil perkalian matriks A^{-1}dan C seperti gambar di bawah ini.



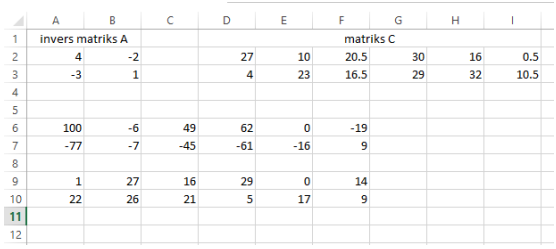
	A	B	C	D	E	F	G	H	I
1	invers matriks A					matriks C			
2	4	-2		27	10	20.5	30	16	0.5
3	-3	1		4	23	16.5	29	32	10.5
4									
5									
6	100	-6	49	62	0	-19			
7	-77	-7	-45	-61	-16	9			
8									
9									

4. Block range yang kosong (dalam hal ini A9:F10), sebagai tempat untuk memunculkan hasil dari $A^{-1}.C \ mod \ 33$. kemudian ketik fungsi =MOD(L2:Q3,33).



	A	B	C	D	E	F	G	H	I
1	invers matriks A					matriks C			
2	4	-2		27	10	20.5	30	16	0.5
3	-3	1		4	23	16.5	29	32	10.5
4									
5									
6	100	-6	49	62	0	-19			
7	-77	-7	-45	-61	-16	9			
8									
9	=MOD(A6:F7,33)								
10									

6. Tekan dan tahan secara bersamaan "**Ctrl+Shift"**, lalu tekan **Enter**", maka pada range A9:F10 akan muncul hasil dari $A^{-1}.C \ mod \ 33$ seperti gambar di bawah ini.



	A	B	C	D	E	F	G	H	I
1	invers matriks A					matriks C			
2	4	-2		27	10	20.5	30	16	0.5
3	-3	1		4	23	16.5	29	32	10.5
4									
5									
6	100	-6	49	62	0	-19			
7	-77	-7	-45	-61	-16	9			
8									
9	1	27	16	29	0	14			
10	22	26	21	5	17	9			
11									
12									

Hasil di atas bisa kita tulis kembali menjadi

$$S = \begin{bmatrix} 24 & 14 & 20 & 30 & 17 & 4 \\ 32 & 6 & 17 & 4 & 0 & 19 \end{bmatrix}.$$

Matriks tersebut sama seperti matriks P yang telah kita bentuk sebelumnya pada proses enkripsi. Jika kita terjemahkan, maka kalimat yang terbentuk sama seperti kalimat yang hendak kita sandikan sebelumnya yaitu "YOU'RE GREAT".

5. KESIMPULAN

Melalui beberapa contoh pengujian sandi, matriks kunci yang digunakan tidak hanya bedeterminan 1. Penelitian ini dapat dikatakan cukup berhasil, karena dapat membuat penyandi lebih leluasa khusunya dalam memilih matriks kunci. Penelitian ini juga memiliki kekurangan yaitu terdapat kemungkinan bahwa penyandi tidak bisa membuat cipher text karena ada beberapa bilangan yang berbentuk pecahan. Peneliti hanya melakukan percobaan untuk beberapa contoh sehingga penelitian ini masih bersifat empiris. Penelitian lain yang mengembangkan hill cipher dengan metode yang berbeda sangat diperlukan untuk menjawab permasalahan serupa.

6. REFERENSI

Hall, Matthew. 2003. *Calculator Cryptography*. National Council Of Theachers Of Mathematics. [artikel JSTOR]

Pangaribuan, Lisda Juliana. 2018. *Kriptografi Hybrida Algoritma Hill Cipher dan Rivest Shamir Adleman (RSA) sebagai Pengembangan Kriptografi Kunci Simetris.* Akademi Manajemen dan Informatika Komputer Medan Business Polytechnic. [Jurnal Tekologi Informasi dan Komunikasi].