MODIFIKASI KRIPTOGRAFI HILL CIPHER MENGGUNAKAN CONVERT BETWEEN BASE

Alz Danny Wowor
Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana
Jl. Diponegoro 50-66, Salatiga, 50711
Telp : (0298) 3419240, Fax : (0298) 3419240
E-mail : alzdanny.wr@gmail.com

Abstrak

Hill cipher merupakan sebuah teknik kriptografi klasik, yang menggunakan matriks sebagai kunci. Pada sisi lain, Hill cipher telah dipecahkan dengan kriptanalisis Known Plaintext Attack menggunakan perkalian matriks dan persamaan linier. Tulisan ini memodifikasi Hill cipher menggunakan Convert Between Base dan perkalian n-matriks kunci untuk setiap iterasi. Cipherteks dihasilkan dalam elemen bit sehingga dapat mempersulit kriptanalisis dengan perkalian matriks dan fungsi linier untuk dapat memecahkan kunci dan menemukan plainteks. Modifikasi ini berhasil menyelesaikan berbagai permasalahan pada Hill cipher.

***Kata kunci**: Hill cipher, Known Plaintext Attack, Convert Between Base.*

Abstract

Hill cipher is a clasic cryptography using matrix as a key. On the other hand, Hill cipher can be attacking with cryptanalysis using matrix multiplication and linear equations. This papaer deals with modification of the Hill cipher. In this, we have introduced Convert Beetwen Base on start and end in proces of encription-decryption. Multiplication with key of n-matrix in each step of teh iteration. From the cryptanalysis preformed in the investigation, we have found that chiper is a strong one.

***Keywords**: Hill cipher, Known Plaintext Attack, Convert Between Base.*

1. PENDAHULUAN

Hil Cipher digolongkan sebagai teknik kriptografi klasik yang dibuat oleh Lester S. Hill dan diperkenalkan tahun 1929. Hill cipher termasuk dalam sistem kriptografi polialfabetik dengan menggunakkan 26 huruf dalam bahasa Inggris, yang berkorespodensi dengan angka 0 sampai 25 [1].

Kriptografi digunakan sebagai alat keamanan di komputer maupun jaringan internet. Hill cipher diperhadapkan dalam kondisi sekarang ini, maka terdapat beberapa kekurangan. Pertama, algoritmanya dirancang hanya dapat mengenkripsi karakter alfabet saja. Kedua, cipherteks yang dihasilkan hanya dalam karakter abjat. Ketiga, jumlah elemen plainteks sama dengan cipherteks. Hal-hal ini akan mempermudah kriptanalis untuk dapat menemukan hubungan yang linier antara plainteks dan cipherteks, pada [2] memperlihatkan bagaimana Hill cipher dipecahkan menggunakan perkalian matriks dan persamaan linier.

Oleh karena itu, tulisan ini modifikasi Hill cipher menggunakan *Convert Between Base* yang dapat digunakan untuk mengkonversi bilangan plainteks dari suatu basis terpilih ke basis terpilih yang lain. Harapanya modifikasi ini dapat mengatasi berbagai permasalahan dari kriptografi Hill cipher.

2. KAJIAN PUSTAKA

2.1 *Convert Between Base*

Proses *Convert Between Base* (*CBB*) diberikan dengan kedua defenisi berikut ini.

Defenisi 1 [4]. Konversi sembarang bilangan positif s berbasis 10 ke basis β. Secara umum notasinya,

Konv (s, **base**$_\beta$).

Defenisi 2 [4]. Konversi dari urutan bilangan (*list digit*) ℓ dalam basis α ke basis β, dinotasikan,

Konv (ℓ, $_\alpha$**base**$_\beta$)

dengan jumlahan urutan bilangan (jumlahan ℓ) mengikuti aturan,

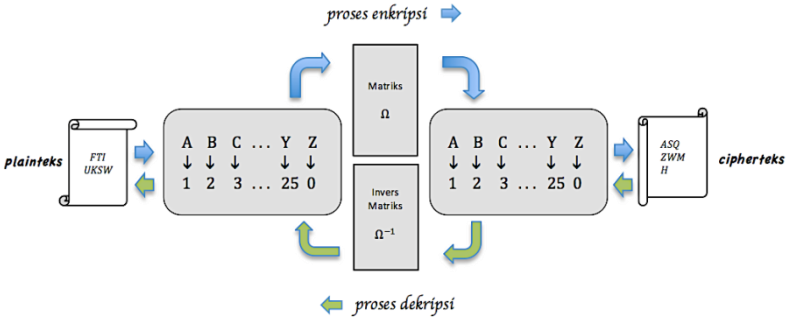
$$\sum_{k=1}^{nops\,(\ell)} I_k \cdot \alpha^{k-1}$$

dimana nops (ℓ) adalah nilai terakhir dari urutan bilangan ℓ.

- $0 \leq I_k \leq \alpha$ dan ℓ adalah bilangan positif.
- Nilai yang diperoleh merupakan kumpulan urutan bilangan dalam basis β.

2.2 Hill cipher

Proses enkripsi-dekripsi Hill cipher secara umum dapat digambarkan



Gambar 1. 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

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

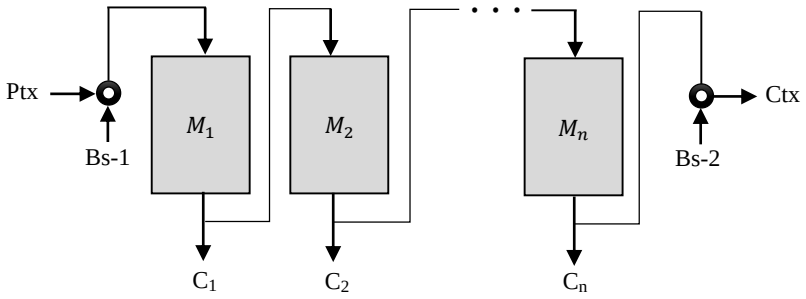
Proses dekripsi secara umum diberikan

$$P = \Omega^{-1} \cdot C \ (mod\ 26) \quad (2)$$

3. RANCANGAN KRIPTOGRAFI

3.1 Proses Enkripsi

Proses enkripsi dilakukan dengan menggunakan *n*-matriks kunci dan bilangan-bilangan pada basis pertama (*Bs-1*) dan basis kedua (*Bs-2*). Secara umum proses perancagan modifikasi kriptografi Hill cipher diberikan pada Gambar 2.



Gambar 2. Diagram Proses Enkripsi

Secara matematis, proses enkripsi modifikasi Hill cipher dinyatakan sebagai

a) Plainteks (Ptx) dikonversi ke dalam kode ASCII, misalnya
$$Q = \{a_1, a, \ldots, a_i\}. \quad (3)$$
Jika elemen $Q \equiv$ (sebanding) dengan kelipatan ordo matriks M_1, maka dilanjutkan pada proses selanjutnya. Apabila $Q \not\equiv$(tidak sebanding)M_1, maka harus ditambah elemen 32 (dalam kode ASCII setara dengan spasi), sesuai kebutuhan sampai elemen $Q \equiv$ kelipatan ordo matriks M_1.

b) Selanjutnya, angka-angka (Q) dilakukan *CBB*, dengan menggunakan *Bs-1* (α dan β) secara umum ditulis
$$\odot: \ Q_{tx} = \mathbf{Konv}(\ell = Q, _{\alpha}\, \mathbf{base}\ _{\beta}) \quad (4)$$

c) Berikutnya mengalikan setiap blok vektor Persamaan (4) dengan matriks kunci M_1, diperoleh
$$C_1 = (Q_{tx})(M_1)\ mod\ 127 \quad (5)$$
dengan μ_i adalah hasil perkalian matriks kunci dan blok vektor plainteks ke-*i*.

d) Untuk proses ke-i dengan $1 < i \leq n$, diperoleh dengan perkalian bilangan matriks kunci, digabungkan menjadi

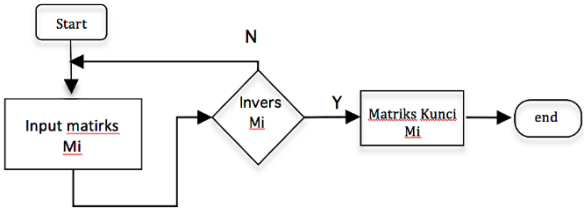
$$C_i = (C_{i-1})(M_i) mod\ 127 \quad (6)$$

e) Dengan menyiapkan *Bs-2* untuk basis α yang akan dikonversi ke basis $\beta = 2$ dengan proses *CBB* untuk memperoleh cipherteks. Secara umum diberikan

$$\circledcirc: C_{tx} = \mathbf{Konv}(\ell = C_{n,\alpha}\ \mathbf{base}_{\beta=2}) \quad (7)$$

3.2 Perancangan Kunci

Modifikasi Hill cipher menggunakan *n*-matriks yang digunakan sebagai kunci. Proses perancagan kunci untuk setiap matriks sebagai berikut.

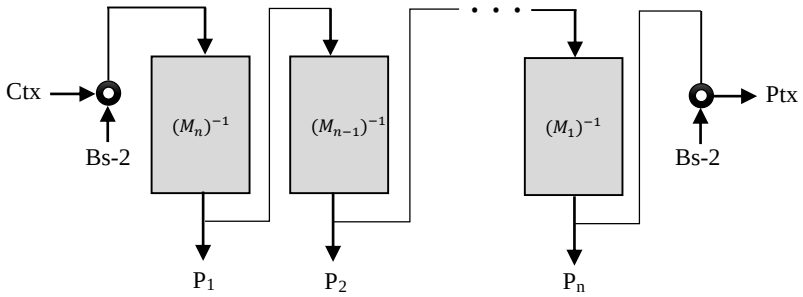


Gambar 3. Flowchart Kunci Matriks

Sedangkan untuk kunci pada proses *CBB*, diperlukan dua bilangan yang dijadikan basis. Perancangan ini menggunakan dua kali proses sehingga digunakan empat basis. Hanya saja perlu untuk diperhatikan misalnya proses dekripsi mengkonversi dari basis α ke β, maka untuk dekripsi dilakukan konversi balik dari β ke basis α.

3.3 Proses Dekripsi

Perancangan modifikasi ini, adalah kriptografi simetris oleh karena itu masih menggunakan kunci yang sama dan proses dekripsi cencerung sama dengan enkripsi. Proses dekripsi modifikasi Hill cipher diberikan pada Gambar 4.



Gambar 4. Diagram Proses Dekripsi

Setiap *n*-matriks yang digunakan diharuskan untuk mempunyai invers seperti yang ditunjukkan pada Gambar 4. Maka proses dekripsi mengalikan dari invers setiap matriks yang dijadikan kunci.

4. HASIL DAN PEMBAHASAN

4.1. Modifikasi Hill Cipher sebagai Teknik Kriptografi

Untuk menguji modifikasi Hill cipher sebagai sebuah teknik kriptografi, proses enkripsi-dekripsi menggunakan plainteks *"FTI UKSW"* dan diambil $n = 10$ sehingga digunakan 10 matriks kunci.

$$\mathrm{M}_1 = \begin{bmatrix} 2 & 0 & 1 \\ 7 & 6 & 3 \\ 0 & 4 & 2 \end{bmatrix}, \mathrm{M}_2 = \begin{bmatrix} 1 & 2 & 2 \\ 5 & 6 & 3 \\ 1 & 4 & 2 \end{bmatrix}, \mathrm{M}_3 = \begin{bmatrix} 7 & 2 & 3 \\ 3 & 6 & 7 \\ 5 & 8 & 2 \end{bmatrix}, \mathrm{M}_4 = \begin{bmatrix} 3 & 4 & 2 \\ 5 & 6 & 7 \\ 1 & 4 & 0 \end{bmatrix}, \mathrm{M}_5 = \begin{bmatrix} 4 & 4 & 5 \\ 1 & 6 & 0 \\ 0 & 1 & 1 \end{bmatrix},$$
$$\mathrm{M}_6 = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 6 & 0 & 1 \end{bmatrix}, \mathrm{M}_7 = \begin{bmatrix} 1 & 2 & 2 \\ 5 & 6 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \mathrm{M}_8 = \begin{bmatrix} 7 & 2 & 2 \\ 3 & 6 & 2 \\ 1 & 4 & 3 \end{bmatrix}, \mathrm{M}_9 = \begin{bmatrix} 1 & 4 & 2 \\ 7 & 5 & 0 \\ 1 & 0 & 3 \end{bmatrix}, \mathrm{M}_{10} = \begin{bmatrix} 6 & 4 & 5 \\ 3 & 2 & 3 \\ 1 & 6 & 1 \end{bmatrix}. \quad (8)$$

Basis bilangan yang untuk *Bs-1* adalah $\alpha = 127, \beta = 17$ sedangkan untuk *Bs-2* dipilih $\alpha = 131,$ dan $\beta = 2$. Setelah disiapkan kunci-kunci yang akan digunakan, maka proses enkripsi-dekripsi dapat dilakukan sesuai dengan langkah-langkah proses enkripsi, sehingga diperoleh cipherteks:

"011000100111"

Untuk proses dekripsi dilakukan dengan menggunakan *CBB* untuk *Bs-2*$\alpha = 2, \beta = 131$ sedangkan basis untuk *Bs-1*, $\alpha = 17, \beta = 127$ proses untuk setiap iterasi dilakukan perkalian dengan invers dari setiap matiks kunci pada (8). Sehingga akan diperoleh kembali palainteks *FTI UKSW*.

Karena dapat melakukan proses enkripsi-dekripsi, maka modifikasi pada Hill cipher dapat dikatakan sebagai sebuah teknik kriptografi.

4.2 Modifikasi Hill Cipher sebagai Sistem Kriptografi

Sebuah sistem kriptografi harus memenuhi 5 tuple $\boldsymbol{P}$, $\boldsymbol{C}$, $\boldsymbol{K}$, $\boldsymbol{E}$, $\boldsymbol{D}$ [5]. Oleh karena itu akan ditunjukan modifikasi ini memenuhi kelima kondisi tersebut.

P*adalah himpunan berhingga dari plainteks*. Dalam modifikasi Hill cipher menggunakan 127 karakter maka himpunan plainteks pada modifikasi Hill Cipher adalah himpunan berhingga.

C *adalah himpunan berhingga dari cipherteks*. Cipherteks dihasilkan dalam elemen bit biner (bilangan 0 dan 1). Karena hipunanan cipherteks hanya {0,1}, maka cipherteks modifikasi Hill Cipher adalah himpunan berhingga.***K****merupakan ruang kunci (keyspace), adalah himpunan berhingga dari kunci*. Kunci tambahan dalam modifikasi Hill Cipher adalah Fungsi Rasional dan Konversi Basis Bilangan yang juga himpunan berhingga. *Untuk setiap* $k \in \boldsymbol{K}$*, terdapat aturan enkripsi* $e_k \in \boldsymbol{E}$*dan berkorespodensi dengan aturan dekripsi* $d_k \in \boldsymbol{D}$*. Setiap* $e_k : \boldsymbol{P} \longrightarrow \boldsymbol{C}$*dan* $d_k : \boldsymbol{C} \longrightarrow \boldsymbol{P}$*adalah fungsi sedemikian hingga* $d_k(e_k(x)) = x$ *untuk setiap plainteks* $x \in \boldsymbol{P}$.

Kondisi ke-4 ini, secara, terdapat kunci yang dapat melakukan proses enkripsi sehingga merubah plainteks menjadi cipherteks. Dan dapat melakukan proses dekripsi yang merubah cipherteks ke plainteks. Karena memenuhi ke-lima kondisi maka modifikasi pada Hill Cipher merupakan sebuah sistem kriptografi.

4.3 *Convert Between Base* pada Modifikasi Hill Cipher

Penggunaan *CBB* merupakan kunci awal dan terakhir pada modifikasi Hill Cipher. Kunci ini digunakan untuk membuat cipherteks dalam elemen bit biner. Selain itu juga, *CBB* dapat membuat elemen cipherteks lebih banyak dari plainteks. Pada tabel berikut menunjukkan banyak elemen bit biner (cipherteks) yang diperoleh berdasarkan basis bilangan adalah.

Tabel 1. Banyak Elemen Cipherteks

Konv ([36, 43, 12, 23, 3, 15,0, 6, 45, 56, 32, 6, 2] $_a$ **base** $_2$)

Banyak basis (*a*)	**Banyak Elemen Cipherteks**
5	31 bit
17^8	394 bit
24^{40}	2220 bit
178244^{112011}	23446360 bit

Pada Tabel 1, terdapat 13 elemen bilangan yang akan dienkripsi, hubungan antara basis bilangan dengan banyak elemen bit biner diperoleh hubungan berbanding yang lurus, artinya semakin besar basis bilangan yang digunakan maka akan semakin banyak elemen bit biner yang diperoleh. KBB dapat juga mempersulit kriptanalis untuk mencari hubungan antara plainteks dengan cipherteks, karena plainteks dalam bentuk karakter tetapi pada cipherteks dalam bit biner, yang berbeda dengan Hill Cipher yang plainteks dan cipherteksnya masih dalam karakter angka.

4.4 Perbandingan Proses Enkripsi-Dekripsi

Dalam proses enkripsi-dekripsi yang dibandingkan adalah ketersediaan plainteks, ketersediaan matriks kunci dan invers matriks kunci.

*Ketersediaan plainteks*sebenarnya untuk melihat kertersediaan ruang sampel dari plainteks. Dengan menggunakan aturan perpangkatan maka diperoleh modifikasi Hill Cipher mengungguli Hill Cipher sebanyak $3.298105963 \times 10^{229}$ kali.

Ketersediaan matriks kunci adalah banyak matriks yang mungkin diambil berdasarkan bilangan yang bersesuaian karakter plainteks (26 pada Hill Cipher dan 127 dalam modifikasi). Entri matriks bergantung pada ordo matriks kunci. Perbandingan banyak matriks yang dapat dijadikan kunci diberikan pada tabel dibawah ini,

Tabel 2. Perbandingan Ketersediaan Matriks Kunci

Ordo Matriks (A)	Banyak entri (k^2)	Banyak Kombinasi matriks yang diperoleh		Perbandingan (Hc : MHc)
		HC ($k = 26$)	MHC ($k = 127$)	
2 x 2	4	14950	10334625	1 :691.279
3 x 3	9	3124550	17722355795375	$1 : 5.672 \times 10^6$
4 x 4	16	5311735	81675143551104405225	$1 : 1.538 \times 10^{13}$

Tabel 2, memberikan informasi bahwa untuk matriks berordo 4×4 modifikasi Hill cipher lebih banyak $1.537635886 \times 10^{13}$ kali lipat dari Hill cipher, semakin banyak kombinasi entri k terhadap karakter n maka akan semakin banyak juga ketersediaan matriks. Dengan demikian dapat disimpulkan bahwa Modifikasi Hill cipher jauh lebih banyak menghasilkan ketersediaan matriks yang dapat dijadikan kunci dibandingkan dengan Hill cipher.

Ketersediaan Invers Matriks Kunci. Invers matriks pada Hill Cipher dan Modifikasi Hill Cipher digunakan untuk melakukan proses dekripsi. Dalam menentukan invers dari matriks, terlebih dahulu dilihat determinan yang mempunyai resperiok (invers perkalian) terhadap $\mathbf{Z_{26}}$ dan $\mathbf{Z_{127}}$. Diperoleh dalam teknik kriptografi Hill cipher, matriks kunci tidak bisa memiliki nilai determinan genap, 0 dan 13 karena tidak memiliki resperiok terhadap modulo 26. Sedangkan Modifikasi Hil Cipher, hanya determinan 0 saja yang tidak memiliki resperok terhadap modulo 127.

Bila dikaji banyak peluang determinan dari matriks kunci yang mempunyai resperiok, maka untuk Hill Cipher diperoleh

$$p(Hil\ Cipher) = \frac{14}{26} = 0.538, \quad (9)$$

sedangkan pada Modifikasi Hill Cipher

$$p(Modifikasi\ Hil\ Cipher) = \frac{126}{127} = 0.992 \quad (10)$$

Diperoleh untuk Hill Cipher diperoleh peluang untuk matriks yang tidak mempunyai invers sebesar 0.462 = (1 – 0.538), sehingga perlu lebih hati-hati dan teliti untuk mengambil matriks kunci. Sedangkan untuk untuk Modifikasi Hill Cipher hampir mendekati satu (yaitu 0.992). Sehingga pengambilan matriks yang dapat dijadikan kunci sangat bebas. Hal ini juga dapat ditunjang dengan peluang matriks yang tidak mempunyai invers sangat kecil hanya sekitar 0.008 = (1 – 0.992).

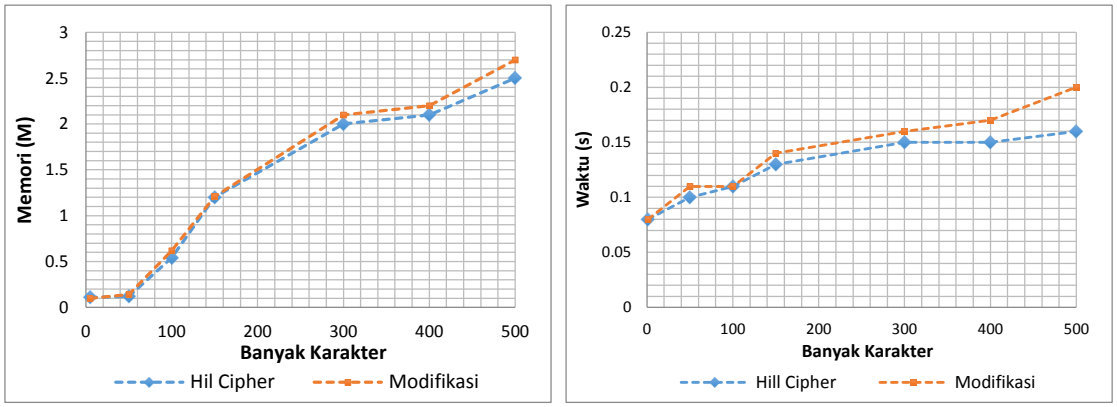
4.5 Kriptananlisis Pada Modifikasi Hill Cipher

Kriptanalisis *known-plaintext attack* menggunakan perkalian matriks dapat memecahkan Hc [5]. Hal ini terjadi penggunaan sebuah matriks kunci yang kemudian dikalikan dengan setiap vektor plainteks yang ukurannya ekuivalen dengan ordo dari matriks kunci. Karena perkalian matriks merupakan suatu kombinasi liner, sehingga pola dari setiap cipherteks dengan plainteks dapat diketahui. Hal ini dipermudah dengan relasi plainteks dan cipherteks adalah $\mathbf{Z}_{26}$ ke $\mathbf{Z}_{26}$. Oleh karena itu perkalian matriks dapat dilakukan dan matriks kunci dapat ditemukan.

Pada MHc, plainteks dalam Z_{127} ke cipherteks dalam Z_2, relasi ini mempersulit kriptananlisis untuk dapat melihat pola yang semula mudah ditemukan pada Hc. Hal ini dipersulit dengan penggunaan perkalian *n*-matriks kunci dan proses CBB. Sehingga kriptanalisis *known-plaintext attack* dengan perkalian matriks tidak dapat menumukan matriks kunci (apalagi ada *n*-matriks kunci).

4.6Kebutuhan Waktu dan Memori

Bgaian ini melihat kebutuhan waktu dan memori antara Hill Cipher dan Modifikasi Hill Cipher ditunjukkan pada Gambar 5. Secara keseluruhan MHc lebih banyak membutuhkan waktu dan memori untuk proses enkripsi dan dekripsi. Hal ini sebanding dengan proses yang dilakukan, kerena beberapa fungsi ditambahkan untuk memperkuat proses kriptografi. Memang secara kebutuhan waktu dan memori modifikasi agak kurang efisien, tetapi disisi lain berimplikasi pada kekuatan terhadap kriptanalisis *known-plaintext attack* yang sebelum memcahkan Hill Cipher.



Gambar 5. Kebutuhan Memori dan Waktu pada proses Enkripsi-Dekripsi bedasrkan banyak karakter plainteks

5. SIMPULAN DAN SARAN

5.1 Simpulan

Modifikasi kriptografi Hill cipher dapat melakukan proses enkripsi dan dekripsi, dan juga dapat memenuhi sebagai sebuah sistem kriptografi. Disisi lain MHc ini dapat menahan kriptanalisis known-plaintext attack dengan perkalian matriks yang sebelumnya memecahkan Hc. Maka dari itu, modifikasi ini dapat digunakan sebagai sebuah teknik kriptografi.

Penggunaan kunci tambahan memberikan perubahan yang signifikan pada algoritma, hal ini dapat dilihat dengan tidak terpecahkannya kunci dan plainteks dari serangan kriptanalisis *known-plaintext attack* dengan teknik perkalian matriks dan fungsi linier, atau modifikasi ini dapat menahan kriptanalisis yang sudah memecahkan Hill Cipher.

5.2 Saran

Saran dari penelitian ini adalah perlu untuk merancang algoritma yang lebih baik sehingga dapat meminimalkan kebutuhan memori dan waktu yang besar, tetapi masih memenuhi standar keamanan.

6. DAFTAR RUJUKAN

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

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

[3] Maplesoft, 2010, *Convert/Base: Convert Between Base*, Maple-14, Waterloo: Waterloo Maple Inc.

[4] Stinson, D.R., 1995, *Cryptography Theory and Practice*, Florida: CRC Press, Inc.

[5] Wowor, A.D., 2011, *Modifikasi Teknik Kriptografi Hill Cipher Menggunakan Fungsi Rasional dan Konversi Basis Bilangan*, M.Cs, Salatiga: Universitas Kristen Satya Wacana.