PEMBANGKIT KUNCI *LINEAR FEEDBACK SHIFT REGISTER* PADA ALGORITMA *HILL CIPHER* YANG DIMODIFIKASI MENGGUNAKAN *CONVERT BETWEEN BASE*

Srita Tania Bonita[1)], Rini Marwati[2)], Sumanang Muhtar Gozali[3)]

[1), 2), 3)] Departemen Pendidikan Matematika FPMIPA UPI

*Surel: srita.tania.bonita@student.upi.edu

ABSTRAK. Penelitian ini memodifikasi algoritma *Hill cipher* serta program aplikasinya. Modifikasi tersebut yaitu mengubah suatu bilangan ke basis bilangan lainnya menggunakan *convert between base* kemudian menggunakan *linear feedback shift register* sebagai pembangkit kunci. *Linear feedback shift register* biasanya dilakukan untuk membangkitkan kunci pada *stream cipher* yang berbasis bit. Dengan menggunakan *convert between base*, maka *linear feedback shift register* dapat diterapkan pada modifikasi *Hill cipher*. Modifikasi ini mampu mempersulit kriptanalis dalam memecahkan kunci dan menemukan plainteks.

Kata kunci: *cryptography, Hill cipher, linear feedback shift register, convert between base, known plaintext attack*

ABSTRACT. This paper modifies Hill cipher algorithm and application program. The modification is changing a number to another base of the number using convert between base and then use linear feedback shift registers as a key generator. Linear feedback shift register is usually done to generate the key stream cipher based on the bit. By using convert between base, the linear feedback shift register can be applied to the modification of Hill cipher. This modification is able to complicate the cryptanalyst to break the key and find the plaintext.

Keywords: cryptography, Hill cipher, linear feedback shift register, convert between base, known plaintext attack.

1. PENDAHULUAN

Keamanan suatu negara tidak hanya dilihat dari kekuatan militer saja, tetapi juga dilihat dari informasi teknologi yang dikuasai negara tersebut. Dilansir dari penelitian "*2016 Data Threat Report*" yang dilakukan oleh *Vormetric Security Data*, terdapat 91% perusahaan dan pemerintahan yang rentan mengalami kebocoran data dan 61% pernah mengalaminya. Untuk mengatasi masalah tersebut, diperlukan ilmu kriptografi yang memiliki peranan penting dalam keamanan data.

Hill cipher merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi. *Hill cipher* dapat memecahkan cipherteks yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. Namun ada beberapa kekurangan *Hill cipher*, yaitu telah dipecahkan dengan kriptanalisis *known plaintext attack* dan persamaan linier. Makalah berjudul "Modifikasi *Hill cipher* Menggunakan *Convert Between Base*" yang diteliti oleh Alz Danny Wowor membahas modifikasi *Hill cipher* menggunakan *Convert Between Base* (CBB) dan perkalian n-matriks kunci untuk setiap iterasi.

Stream cipher merupakan salah satu algoritma modern. *Stream cipher* sering menggunakan *Linear Feedback Shift Register* (LFSR) sebagai pembangkit kunci *stream*. Ilmu matematika yang digunakan pada *Linear Feedback Shift Register* diantaranya adalah fungsi, teori bilangan, aljabar abstrak.

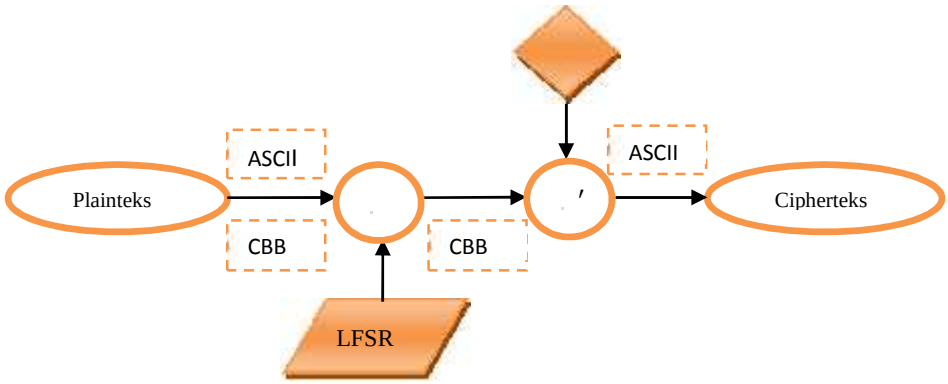
2. METODOLOGI

Salah satu algoritma kriptografi yang kurang aman adalah *Hill cipher* karena dapat dipecahkan dengan kriptanalisis *known plaintext attack* menggunakan perkalian matriks dan persamaan linier. Sehingga perlu dilakukan modifikasi *Hill cipher*, yaitu dengan menggunakan *Convert Between Base* dan *Linear Feedback Shift Register*. Guna mempermudah perhitungan algoritma modifikasi *Hill cipher*, dilakukan pembuatan program aplikasi. Program modifikasi *Hill cipher* dengan menggunakan *Convert Between Base* dan *Linear Feedback Shift Register* dibuat dengan menggunakan MATLAB. Modifikasi algoritma *Hill cipher* dapat digunakan dan dianalisa perbandingan *Hill cipher* dengan modifikasi *Hill cipher* khususnya mengenai kebutuhan waktu.

3. PEMBANGKIT KUNCI *LINEAR FEEDBACK SHIFT REGISTER* PADA ALGORITMA *HILL CIPHER* YANG DIMODIFIKASI MENGGUNAKAN *CONVERT BETWEEN BASE*

a. Modifikasi *Hill Cipher* sebagai Teknik Kriptografi

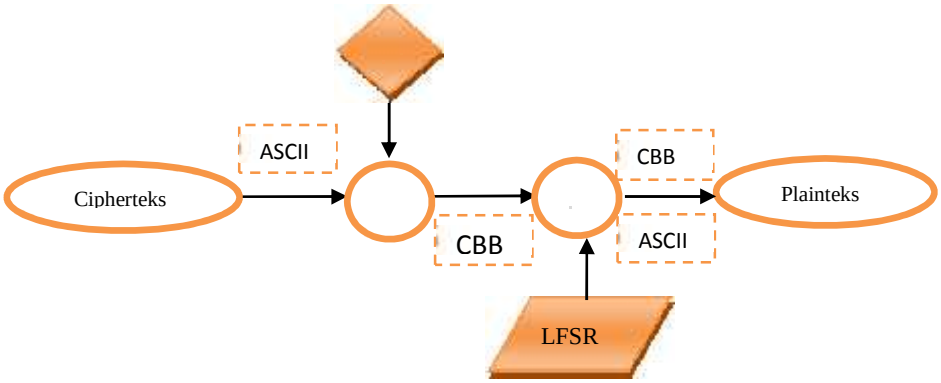
Proses Enkripsi Modifikasi *Hill cipher* menggunakan 2 kunci yaitu inisial awal *Linear Feedback Shift Register* dan matriks kunci yang *invertible*. Untuk prosesnya ditunjukkan pada Gambar 1.



Gambar 1. Enkripsi Modifikasi *Hill cipher*

1. Plainteks dikonversi ke dalam kode ASCII.
2. Pilih inisial kunci dan polinom primitif. Sehingga diperoleh output LFSR.
3. Lakukan proses CBB pada plainteks yang sudah dikonversi ke dalam kode ASCII sehingga diperoleh P.
4. Lakukan peng-XOR-an pada P dan output LFSR. Jika jumlah P dan output tidak sama maka gunakan *padding*.
5. Lakukan proses CBB tahap 2 sehingga diperoleh P'.
6. Pilih matriks kunci K yang *invertible.*
   Jika elemen P' sebanding dengan kelipatan ordo matriks K maka lanjutkan proses selanjutnya. Apabila tidak sebanding, maka tambahkan elemen 0 sampai elemen P' sebanding dengan kelipatan ordo matriks K.
7. Kalikan setiap blok vektor P' dengan matriks.
   $$C = P'K \bmod 127$$
8. Konversikan C ke dalam kode ASCII 7 bit sehingga diperoleh cipherteks.

Hampir sama dengan proses enkripsi, proses dekripsi juga menggunakan 2 kunci. Hanya saja matriks kunci yang digunakan adalah invers matriks yang digunakan pada proses enkripsi.



Gambar 2. Dekripsi Modifikasi *Hill cipher*

Berikut ini proses dekripsi untuk modifikasi *Hill cipher*:

1. Cipherteks dikonversi ke dalam kode ASCII desimal.
2. Hitung $P' = C^{-1}$.
3. Lakukan proses CBB dengan sehingga diperoleh P.
4. Lakukan peng-XOR-an dengan output LFSR.
5. Lakukan proses CBB tahap 2.
6. Konversikan ke dalam ASCII sehingga plainteks diperoleh kembali.

b. Modifikasi *Hill Cipher* sebagai Sistem Kriptografi

Selanjutnya akan diperiksa apakah modifikasi Hill cipher memenuhi sistem kriptografi. Oleh karena modifikasi *Hill cipher* menggunakan 127 karakter, maka himpunan plainteks pada modifikasi *Hill cipher* adalah berhingga. Cipherteks yang dihasilkan dalam bit biner. Ini berarti himpunan cipherteks hanya {0,1} sehingga himpunan cipherteks modifikasi *Hill cipher* adalah berhingga. Terdapat 2 kunci yang digunakan dalam modifikasi *Hill cipher*, yaitu kunci dari inisial awal LFSR dan kunci matriks. Kunci dari LFSR yang digunakan adalah n bit biner yang dibangkitkan menjadi 2^{n-1} bit biner dan kunci matriks yang digunakan berordo $m \times m$ (m^2 entri). Ini berarti himpunan cipherteks modifikasi *Hill cipher* adalah berhingga. Terdapat kunci yang dapat melakukan proses enkripsi sehingga mengubah plainteks menjadi cipherteks dan dapat melakukan proses dekripsi sehingga mengubah cipherteks menjadi plainteks. Oleh karena modifikasi *Hill cipher* sudah memenuhi syarat-syarat dalam sistem kriptografi, maka modifikasi *Hill cipher* merupakan sistem kriptografi.

c. LFSR dan CBB pada *Hill Cipher*

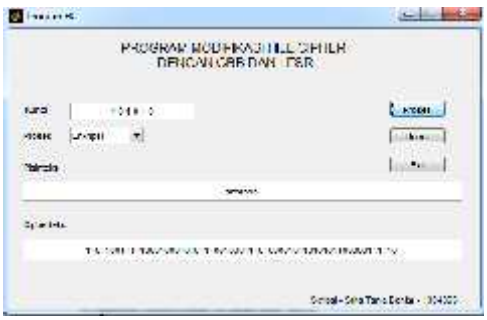
Inisial awal dari LFSR digunakan sebagai kunci. Kunci tersebut kemudian dibangkitkan sehingga menghasilkan *output* 2^{n-1} bit biner dari n bit biner kunci. Sedangkan CBB digunakan di awal dan akhir algoritma yaitu pada saat plainteks telah dikonversi ke dalam kode ASCII dan saat output LFSR di-XOR-kan dengan hasil CBB awal. 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. Hal ini sejalan dengan LFSR membangkitkan kunci, sehingga diperoleh bit biner yang semakin banyak jika inisial awal bit semakin banyak.

d. Ketersediaan Kunci

Bila dikaji ketersediaan kunci, modifikasi *Hill cipher* jauh lebih banyak menghasilkan ketersediaan matriks yang dapat dijadikan kunci dibandingkan dengan *Hill cipher*. Matriks berordo 4×4 modifikasi *Hill cipher* lebih banyak $1.537635886 \times 10^{1}$ kali lipat dari *Hill cipher*. Untuk *Hill cipher*, peluang matriks yang tidak mempunyai invers sebesar 0.462 sedangkan untuk modifikasi *Hill cipher* hampir mendekati satu (yaitu 0.992). Salah satu teknik yang digunakan untuk menemukan kunci adalah *exhausted attack*. Ketika inisial awal yang digunakan adalah 31 bit, maka pihak lawan harus dapat menemukan satu polinom primitif yang digunakan dari sebanyak 9701 polinom primitif yang ada. Hal ini tentu akan membuat pemecahan cipherteks semakin lama.

e. Program Modifikasi *Hill Cipher*

Pembuatan program aplikasi dilakukan guna untuk mempermudah proses perhitungan modifikasi *Hill cipher*. Program modifikasi *Hill cipher* dibuat dengan menggunakan MATLAB. Tampilan program enkripsi ditunjukkan pada gambar 3.



Gambar 3. Tampilan Program Enkripsi Modifikasi *Hill cipher*

Plainteks "sritabon" dienkripsi menggunakan algoritma modifikasi *Hill cipher*. Dengan memilih inisial kunci U=101010, polinom primitif $x^6 + x^5 + 1$, matriks kunci

$$K = \begin{pmatrix} 3 & 1 & 0 \\ 2 & 1 & 1 \\ 6 & 2 & 2 \end{pmatrix}$$

serta basis pada CBB tahap 1 yang digunakan adalah $\alpha = 130, \beta = 2$ dan $\alpha = 2, \beta = 127$ untuk CBB tahap 2, maka diperoleh cipherteks

```
100101101010000100111010010010001001011000000000000101
110100101110011111111010111000000100011100101001111101 1
100110001011010001100001101001100011000100100111100010
010010100011101101100010011111111001010010000011001100 0
111110001010100
```

Sedangkan untuk proses dekripsi, matriks kunci yang digunakan adalah invers matriks K dan CBB menggunakan basis $\alpha = 127, \beta = 2$ dan $\alpha = 2, \beta = 130$ sehingga plainteks diperoleh kembali.

f. Kriptanalisis Modifikasi *Hill cipher*

Dari segi kriptanalisis, modifikasi Hill cipher mampu mengatasi serangan kriptanalis *known plaintext attack* dengan perkalian matriks dan persamaan linear. Misalkan plainteks `Srita Tania Bonita 20 Maret 1996` dan matriks kunci yang digunakan adalah

$$K = \begin{pmatrix} 3 & 1 & 0 \\ 2 & 1 & 1 \\ 6 & 2 & 2 \end{pmatrix}$$

Dengan melakukan proses enkripsi pada modifikasi *Hill cipher*, diperoleh cipherteks

```
100101101010000100111010010010001001011000000000000101
110100101110011111111010111000000100011100101001111101 1
100110001011010001100001101001100011000100100111100010
010010100011101101100010011111111001010010000011001100 0
111110001010100
```

Misalkan plainteks yang diketahui adalah `Srita Tan`. Dengan menggunakan serangan kriptanalisis *known plaintext attack*, diperoleh

$$K_1 = \begin{pmatrix} 24 & 124 & 36 \\ 125 & 32 & 83 \\ 71 & 43 & 85 \end{pmatrix} \neq \begin{pmatrix} 3 & 1 & 0 \\ 2 & 1 & 1 \\ 6 & 2 & 2 \end{pmatrix}$$

Oleh karena matriks K_1 berbeda dengan matriks kunci yang digunakan maka dapat dikatakan bahwa modifikasi *Hill cipher* ini mampu mengatasi serangan kriptanalis *known plaintext attack*. Selain itu juga mampu mengatasi serangan kriptanalisis persamaan linear, diperoleh matriks kunci yang berbeda yaitu

$$K_2 = \begin{pmatrix} 24 & 124 & 36 \\ 125 & 32 & 83 \\ 71 & 43 & 85 \end{pmatrix} \neq \begin{pmatrix} 3 & 1 & 0 \\ 2 & 1 & 1 \\ 6 & 2 & 2 \end{pmatrix}$$

Modifikasi Hill cipher juga mampu menahan pemecahan cipherteks karena polinom yang ditemukan berbeda dengan polinom yang digunakan apabila dilakukan uji ketahanan LFSR.

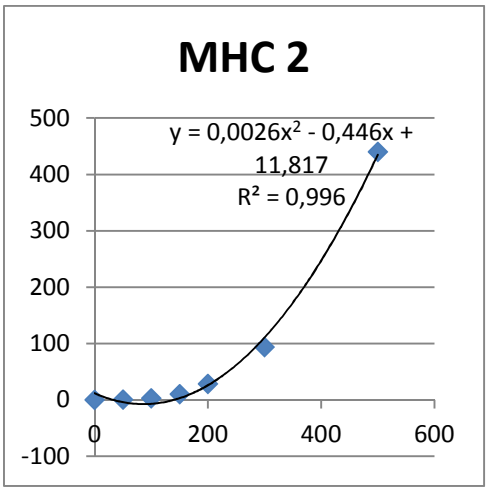
g. Kebutuhan Waktu

Secara kebutuhan waktu, modifikasi ini kurang efisien., Kebutuhan waktu untuk proses enkripsi deskripsi ditunjukkan pada Tabel 4. Dapat disimpulkan bahwa waktu yang dibutuhkan pada modifikasi *Hill cipher* lebih lama dibandingkan *Hill cipher*.

Tabel 1 Kebutuhan Waktu *Hill cipher* dan Modifikasi *Hill cipher*

Banyak Karakter	Waktu HC	Waktu MHC
0	0,017 s	0,133 s
50	0,294 s	0,551 s
100	0,573 s	2,926 s
150	1,483 s	10,137 s
200	1,806 s	28,655 s
300	2,509 s	93,598 s
500	4,387 s	439,802 s

Proses enkripsi dekripsi ketika plainteks sebanyak 500 karakter mengakibatkan modifikasi *Hill cipher* mengalami "*stress point*". Sehingga untuk mengetahui karakteristik dari algoritma modifikasi *Hill cipher* perlu dilakukan pencocokkan kurva pada Tabel 1. Pencocokkan kurva pada modifikasi *Hill cipher* ditunjukkan pada Gambar 4.



Gambar 4 Pecocokkan Kurva Modifikasi *Hill cipher*

Berdasarkan koefisien determinasi yang paling baik, yaitu R^2 mendekati 1, diperoleh persamaan

$$y = 0.0026x^2 - 0.446x + 11.817$$

yang menunjukkan kebutuhan waktu modifikasi *Hill cipher*. Sehingga diperoleh persamaan untuk laju kenaikan banyak waktu terhadap plainteks, yaitu $0.0052x - 0.446$.

4. KESIMPULAN

a. Kesimpulan

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan bahwa konsep algoritma *Hill cipher* yang dimodifikasi menggunakan *convert between base* adalah mengkonversi plainteks yang sudah dikonversi ke dalam kode ASCII dalam suatu basis tertentu ke basis lainnya menggunakan *convert between base*. *Linear feedback shift register* biasa digunakan untuk pembangkit *Stream cipher* yang berbasis biner sedangkan *Hill cipher* berbasis alfabet. Dengan menggunakan *convert between base* maka *linear feedback shift register* dapat diterapkan pada *Hill cipher* dengan cara pembangkitan kunci, proses convert between base, peng-XOR-an kemudian diterapkan pada *Hill cipher*. Implementasi algoritma modifikasi *Hill cipher* dalam bentuk program aplikasi dapat dibuat dengan menggunakan MATLAB. MATLAB mendukung aljabar linear khususnya mengenai matriks sehingga modifikasi Hill cipher dapat diimplementasikan. Modifikasi *Hill cipher* dapat digunakan untuk enkripsi dan dekripsi. Modifikasi ini juga sudah memenuhi sistem kriptografi. Penggunaan *convert between base* dan

pembangkitan kunci dengan *linear feedback shift register* dapat memperkuat keamanan algoritma kriptografi. Hal ini ditunjukkan dengan tidak terpecahkannya kunci pada saat dilakukan kriptanalisis. Selain itu ditunjukkan pula ketersediaan kunci dan banyaknya kemungkinan yang dimiliki oleh kunci *linear feedback shift register* dan matriks kunci untuk dipecahkan sehingga akan mempersulit kriptanalis dalam memecahkan kunci dan menemukan plainteks.

b. Rekomendasi

Untuk pengembangan lebih lanjut, maka penulis memberikan rekomendasi yaitu analisa mengenai kebutuhan memori karena keamanan algoritma dapat diekuivalenkan juga dengan memori. Selain itu juga dapat digunakan kode extended-ASCII sehingga lebih banyak karakter yaitu sebanyak 255 karakter.

5. DAFTAR PUSTAKA

[1] Munir, R. 2006. *Kriptografi*. Bandung: Informatika.

[2] Wowor, A.D. 2013. *Modifikasi Hill cipher Menggunakan Convert Between Base*. Surabaya: ITS.

[3] http://www.vormetric.com/datathreat/2016, diakses tanggal 20 Oktober 2016.