Jurnal Matematika Integratif
Volume 9 No 1, April 2013, pp 39 - 51
ISSN 1412-6184

Enkripsi dan Dekripsi Teks menggunakan Algoritma *Hill Cipher* dengan Kunci Matriks Persegi Panjang

Akik Hidayat[1], Tuty Alawiyah[2]
[1)] Jurusan Matematika, Fakultas MIPA, Universitas
Jl. Raya Bandung Sumedang KM 21 Jatinangor Sumedang 45363
Email: akik.hidayat@ymail.com
[2)] Jurusan Teknik Informatika STMIK DCI Tasikmalaya
Jl.Sutisna senjaya No. 158 Tasikmalaya
Email: tutie.alawiyah@gmail.com

ABSTRAK

Hill Cipher merupakan salah satu algoritma kriptografi yang memanfaatkan matriks sebagai kunci untuk melakukan enkripsi dan Dekripsi dan aritmatika modulo. Setiap karakter pada *plaintext* ataupun ciphertext dikonversikan kedalam bentuk angka. Enkripsi dilakukan dengan mengalikan matriks kunci dengan matriks *plaintext,* sedangkan Dekripsi dilakukan dengan mengalikan invers matriks kunci dengan matriks *ciphertext*. Karena itulah, *Hill Cipher* hanya bisa menggunakan matriks persegi sebagai matriks kuncinya. Invers semu atau *pseudo invers* dapat dimanfaatkan pada algoritma *Hill Cipher,* sehingga matriks kunci yang digunakan tidak terbatas pada matriks persegi saja. Penggunaan matriks persegi panjang menjadikan *ciphertext* lebih panjang dari *plaintext*. Hal ini tentunya membuat pesan menjadi lebih tersamarkan. Pada tulisan ini, penulis menggunakan modulo 95 artinya inputan data ada 95 simbol. Untuk mempermudah penghitungan pada saat inisialisasi matriks kunci, proses enkripsi dan proses Dekripsi menggunakan program aplikasi C++.
Kata Kunci: kriptografi, enkripsi, Dekripsi, Hill Cipher yang diperluas.

ABSTRACT

Hill Cipher is one of cryptograph algorithm which uses as a key to conduct encryption and description. Encryption is conducted by changing the key matrix with plaintext, more over description is conducted by changing the key of invers matrix with ciphertext. Therefore, Hill Cipher only could use square matrix as its key matrix. Pseudo invers (imagination invers) could be used in Hill Cipher algorithm, thus key matrix used not only in square matrix. The using of square matrix makes ciphertext longer than plaintext. Absolutely, this case makes the message to be more implied. Exactly, the calculation of matrix will be complicated in using matrix with big ordo and longer plaintext, therefore the writer makes an application program to help the key matrix initialization process, encryption and description with Program Aplication C++
Key words: *cryptograph, extended hill chipper, enkripsi, Dekripsi.*

1. Pendahuluan

Pertukaran informasi menjadi hal yang sangat penting di era kehidupan saat ini. Begitu pentingnya pertukaran informasi tentunya harus disertai dengan keamanan informasi (*information security*). Keamanan informasi yang berkaitan dengan penggunaan komputer, tidak dapat dipisahkan dengan kriptografi., Aman bisa berarti bahwa selama pengiriman informasi tentu diharapkan informasi tersebut tidak dapat dibaca oleh orang yang tidak berhak. Algoritma Hill Cipher merupakan salah satu algoritma ktiprografi yang memanfaat aritmatika modulo dan matriks. Setiap karakter pada plaintext dan ciphertext dikonversikan kedalam angka. Proses enkripsi dilakukan dengan mengalikan matriks kunci dengan matriks plaintext, sedangkan proses Dekripsi mengalikan invers matriks kunci dengan ciphertextnya. Karena itulah, Hill Cipher hanya dapat menggunakan matriks persegi. Dengan memanfaatkan *pseudo invers*, penulis mencoba menerapkan matriks persegi panjang mxn dengan $m \geq n$ dan $n > 1$. Dalam paper ini, plaintext yang berupa huruf, angka dan simbol dikonversikan sebanyak 95 karakter dan simbol. Semua operasi bilangan, menggunakan modulo 95 artinya ada 95 simbol, Sedangkan data yang diolah merupakan data yang disimpan pada file text. Untuk mempermudah penghitungan saat inisialisasi matriks kunci, proses enkripsi dan Dekripsi, maka penulis membuat program aplikasi menggunakan bahasa pemrograman C++.

2. Metode Penelitian

Metode penelitian pada penyusunan ini terdiri dari atas Studi pustaka yaitu Mengumpulkan bahan-bahan referensi baik buku, artikel, makalah maupun situs internet mengenai algoritma kriptografi Hill Cipher, aritmatika modulo, teori dasar matriks, *pseudo invers* serta pemrograman untuk pembuatan aplikasinya. Selanjutnya Analisis masalah Pada tahap ini dilakukan analisis terhadap algoritma Hill Cipher dan pseudo invers, kemudian menerapkan pseudo invers pada algoritma Hill Cipher.

Desain Dalam tahap ini hasil analisis dibuat pemodelan sistem, menggunakan konsep algoritma dan struktur program, rancangan antar muka dibuat untuk mempermudah sistem alur yang terjadi dalam pembuatan program dan analisa program sehingga system secara keseluruhan lebih terperinci dan terakhir adalah Coding adalah mengaplikasikan pemodelan sistem (*design*) ke dalam bahasa pemrograman dengan source code/syntax yang sesuai dan bahasa yang digunakan oleh penulis merupakan bahasa pemrograman C++ yaitu suatu bahasa pemrograman yang lebih mudah menentukan model-model matriks.

3. Hasil dan Pembahasan

Menurut [1] dan [2], Enkripsi merupakan proses perubahan data asli (*plaintext*) menjadi *ciphertext* (data yang tidak dapat dimengerti) sedangkan Dekripsi kebalikan dari enkripsi yaitu proses pengembalian bentuk *ciphertext*

menjadi *plaintext* kembali sehingga bisa dipahami. Enkripsi dan Dekripsi dilakukan menggunakan kunci yang sudah ditentukan. Hill Cipher merupakan salah satu algoritma kriptografi kunci simetris yang menggunakan aritmatika modulo terhadap matriks.

Algoritma Hill Cipher menggunakan matriks berukuran *m x m* (matriks persegi) yang invertible dalam modulus *p*, sebagai kunci untuk melakukan enkripsi dan dekripsi. Dasar teori matriks yang digunakan dalam Hill Cipher antara lain adalah perkalian antar matriks dan melakukan invers pada matriks. Proses enkripsi pada algoritma Hill Cipher dimulai dengan mengkonversikan plaintext kedalam angka sesuai dengan table korespondensi. Selanjutnya angka-angka tersebut dikelompokkan menjadi beberapa blok, dimana masing-masing blok terdiri dari m anggota sesuai dengan ordo matriks kunci $K_{(mxm)}$. selanjutnya dicari ciphertext dengan C= K * P. Proses Dekripsi diawali dengan mengkonversikan ciphertext kedalam angka sesuai dengan table korespondensi. Seperti halnya pada proses enkripsi, angka-angka tersebut dikelompokkan menjadi beberapa blok dengan anggota masing-masing blok sebanyak m, lalu dicari plaintextnya dengan $P = K^{-1} * C$.

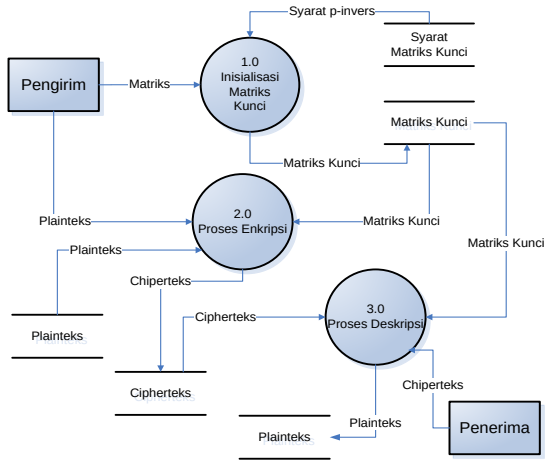
Pada tulisan ini, penulis akan memanfaatkan teori *pseudo invers*, sehingga penggunaan matriks kunci tidak hanya matriks persegi saja, tapi juga dapat menggunakan matriks persegi panjang. Dalam tulisan ini, penulis menggunakan matriks persegi panjang m x n dengan $m \geq n$ dan $n > 1$ yang merupakan matriks *full coloumn rank*. Dengan penggunaan *pseudo invers* diharapkan semakin banyak jenis matriks yang dapat dijadikan matriks kunci. Lihat Gambar 1 untuk DAD level 0 yang menggambarkan rancangan sistemnya

A. Inisialisasi Matriks Kunci

Langkah 1: Tentukan jumlah baris dan kolom matriks *K*, dimana baris $\geq$ kolom dan kolom > 1

Langkah 2: Tentukan elemen matriks *K*. Selanjutnya hitung rank matriks tersebut. Jika rank ≠ kolom, maka kembali ke langkah 1, Jika rank = kolom, lanjutkan ke langkah 3.

Langkah 3: Buat matriks transpose *T* dari matriks *K*



Gambar 1. DAD Level 0 sistem kriptografi algoritma Hill Cipher menggunakan pseudo invers

Langkah 4: Kalikan matriks transpose *T* dengan matriks kunci *K*. Hasil perkalian *TK* dijadikan bilangan bulat modulo 95.

Langkah 5: Hitung determinan dari matriks *TK*. Nilai det (*TK*) dijadikan bilangan bulat modulo 95.

Langkah 6: Cari nilai invers det (*TK*) terhadap modulo 95. Jika tidak memiliki nilai invers, kembali ke langkah 1. Jika memiliki nilai invers lanjutkan ke langkah 7.

Langkah 7: Cari adjoin (*TK*). Setiap elemen hasil penghitungan dijadikan bilangan bulat modulo 95.

Langkah 8: Cari *invers* matriks $(TK)^{-1}$ dengan mengalikan *invers* det (*TK*) dengan adjoin (*TK*). Setiap elemen hasil kalinya dijadikan bilangan bulat modulo 95.

Langkah 9: Kalikan invers matriks $(TK)^{-1}$ dengan matriks transpose *T*. jadikan bilangan bulat modulo 95 untuk setiap elemennya. Sehingga didapat matriks *M*

Langkah 10: Cari matriks *KMK*. Pada setiap penghitungannya, jangan lupa dijadikan bilangan bulat modulo 95 pada setiap elemennya. Selanjutnya periksa, apakah *KMK* = *K*?, jika Ya, lanjutkan ke langkah 11. Jika tidak kembali ke langkah 1

Langkah 11: Cari matriks *MKM*. Pada setiap penghitungannya, jangan lupa dijadikan bilangan bulat modulo 95 pada setiap elemennya. Selanjutnya periksa, apakah *MKM* = *M* ?, jika Ya, lanjutkan ke langkah 12. Jika tidak kembali ke langkah 1

Langkah 12: Cari matriks *KM*dan(*KM*)*. (*KM*)* adalah matriks hermitian. Pada setiap penghitungannya, jangan lupa dijadikan bilangan bulat modulo 95 pada setiap elemennya. Selanjutnya periksa, apakah (*KM*)* = *KM*?, jika Ya, lanjutkan ke langkah 13. Jika tidak kembali ke langkah 1

Langkah 13: Cari matriks *MK* dan (*MK*)*. (*MK*)* adalah matriks hermitian. Pada setiap penghitungannya, jangan lupa dijadikan bilangan bulat modulo 95 pada setiap elemennya. Selanjutnya periksa, apakah (*MK*)* = *MK*?, Jika tidak kembali ke langkah 1. Jika Ya, berarti matriks *K* dapat dijadikan matriks kunci dengan *M* sebagai matriks *p-invers* nya

Contoh: Matriks kunci $A_{(4 \times 2)}$ terdiri dari 4 baris, 2 kolom

$$A = \begin{bmatrix} 1 & 3 \\ 2 & 4 \\ 5 & 7 \\ 6 & 8 \end{bmatrix}$$ jumlah baris > jumlah kolom

Bentuk eselon baris matriks *A* $\begin{bmatrix} 1 & 0 \\ 0 & -2 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$ Rank (*A*) =2

Matriks *Afull coloumn rank* karena rank (*A*) sama dengan jumlah kolom yaitu 2

Matriks A^T adalah transpose matriks kunci *A*

$$T = A^T = \begin{bmatrix} 1 & 2 & 5 & 6 \\ 3 & 4 & 7 & 8 \end{bmatrix}$$

TA adalah Hasil kali matriks A^T dengan matriks kunci *A*

$$TA = \begin{bmatrix} 66 & 94 \\ 94 & 43 \end{bmatrix}$$

Determinan $|TA| = 82$

fpb (*p*,det$|TA|$) ➔*fpb* (95,82) ➔ 95 = (82*1) + 13

82 = (13*6) + 4 13 = (4*3) + 1= (1*4)

Fpb (95,82) = 1, berarti memiliki invers

$t_0 = 0,\ t_1 = 1,\ t_2 = t_0 - t_1*q_1 = 0 - 1*1 = -1,\ t_3 = t_1 - t_2*q_2 = 1 - (-1*6) = 7$

$t_4 = t_2 - t_3*q_3 = (-1) - (7*3) = -22$

invers 82 terhadap 95 adalah -22 = 73

Adjoin (*TA*)

$$adj(TA) = \begin{bmatrix} 43 & 1 \\ 1 & 66 \end{bmatrix}$$

$(TA)^{-1}$ adalah *invers* dari matriks *TA*

$(TA)^{-1}$ = *invers* (*det*) * *adjoin* (*TA*)

$$(TA)^{-1} = \begin{bmatrix} 4 & 73 \\ 73 & 68 \end{bmatrix}$$

B adalah *p-invers* dari matriks kunci A

$$B = ((TA)^{-1} * T,\ B = \begin{bmatrix} 33 & 15 & 56 & 38 \\ 87 & 38 & 81 & 32 \end{bmatrix}$$

Syarat-syarat *p-invers* (lihat [5]):

1. $ABA = A$ dipenuhi, 2. $BAB = B$ dipenuhi, 3. $(AB)^* = AB$ dipenuhi $(AB)^*$ adalah matriks hermitian, 4. $(BA)^* = BA$ dipenuhi $(BA)^*$ adalah matriks hermitian

Dari hasil perhitungan menunjukkan bahwa *Afull coloumn rank* dan syarat-syarat *p-invers* dipenuhi. Sehingga matriks A dapat digunakan sebagai matriks kunci, dengan matriks B sebagai matrik *p-invers* dari matriks A

B. Proses Enkripsi

Langkah 1: Hitung panjang *plaintextmod* kolom matriks kunci K. jika bukan nol, maka tambahkan spasi sehingga panjang *plaintextmod* kolom matriks kunci $K = 0$

Langkah 2: Korespondensikan *plaintext* ke dalam bentuk angka sesuai dengan tabel korespondensi, sehingga didapatkan himpunan angka P

Langkah 3: Partisi P kedalam beberapa blok, dengan masing-masing blok terdiri dari beberapa elemen sesuai dengan jumlah kolom matriks kunci K sehingga didapat P_1 sampai $P_n$dimana n = panjang *plaintext* dibagi jumlah kolom matriks kunci

Langkah 4 Transposkan matriks partisi P_1 sampai P_n

Langkah 5: Kalikan matriks kunci K dengan masing-masing transpose matriks partisi P. Hasil penghitungan dibulatkan kedalam modulo 95.

Langkah 6: Transposkan hasil kali matriks pada langkah 5, kemudian digabungkan sehingga didapatkan himpunan angka *ciphertext*.

Langkah 7: Korespondensikan himpunan angka *ciphertext* dengan karakter sesuai data pada tabel korespondensi, sehingga didapatkan *ciphertext*.

Contoh:

Simulasi enkripsi akan dilakukan menggunakan matriks A sebagai kunci enkripsi dan matriks B sebagai kunci Dekripsi. Plaintext pertama yaitu: "Rahasia 2013!".

Panjang plaintext adalah 13 dan jumlah kolom matriks A adalah 2. Karena 13 mod 2 ≠ 0, maka tambahkan spasi 1 sehingga hasilnya sama dengan nol. Jadi panjang plaintext skarang adalah 14. Selanjutnya dicari korespondensi antara huruf *plaintext* dengan bilangan dalam modulo 95 yang disimpan pada variable P. untuk korespondensi bisa dilihat pada tabel Korespondensi.

P = [17, 26, 33, 26, 44, 34, 26, 62, 54, 52, 53, 55, 81, 62]

P dipartisi menjadi beberapa matriks yang masing-masing memiliki 2 elemen (sesuai dengan jumlah kolom matriks kunci A). jadi P dipartisi menjadi 7 matriks yaitu P_1 sampai dengan P_7

$$P_1 = [17, 26],\ P_2 = [33, 26],\ P_3 = [44, 34],\ P_4 = [26, 62],$$
$$P_5 = [54, 52],\ P_6 = [53, 55], P_7 = [81, 62]$$

Matriks P_1 sampai P_7 ditransposkan, kemudian matriks kunci A dikalikan dengan transpos matriks P_1 sampai dengan P_7.

$$A * (P_1)^{\mathrm{T}} = \begin{bmatrix}1 & 3\\ 2 & 4\\ 5 & 7\\ 6 & 8\end{bmatrix} * \begin{bmatrix}17\\ 26\end{bmatrix} = \begin{bmatrix}0\\ 43\\ 77\\ 25\end{bmatrix} \qquad A * (P_2)^{\mathrm{T}} = \begin{bmatrix}1 & 3\\ 2 & 4\\ 5 & 7\\ 6 & 8\end{bmatrix} * \begin{bmatrix}33\\ 26\end{bmatrix} = \begin{bmatrix}16\\ 75\\ 62\\ 26\end{bmatrix}$$

$$A * (P_3)^{\mathrm{T}} = \begin{bmatrix}1 & 3\\ 2 & 4\\ 5 & 7\\ 6 & 8\end{bmatrix} * \begin{bmatrix}44\\ 34\end{bmatrix} = \begin{bmatrix}51\\ 34\\ 78\\ 61\end{bmatrix} \qquad A * (P_4)^{\mathrm{T}} = \begin{bmatrix}1 & 3\\ 2 & 4\\ 5 & 7\\ 6 & 8\end{bmatrix} * \begin{bmatrix}26\\ 62\end{bmatrix} = \begin{bmatrix}22\\ 15\\ 89\\ 82\end{bmatrix}$$

$$A * (P_5)^{\mathrm{T}} = \begin{bmatrix}1 & 3\\ 2 & 4\\ 5 & 7\\ 6 & 8\end{bmatrix} * \begin{bmatrix}54\\ 52\end{bmatrix} = \begin{bmatrix}20\\ 31\\ 64\\ 75\end{bmatrix} \qquad A * (P_6)^{\mathrm{T}} = \begin{bmatrix}1 & 3\\ 2 & 4\\ 5 & 7\\ 6 & 8\end{bmatrix} * \begin{bmatrix}53\\ 55\end{bmatrix} = \begin{bmatrix}28\\ 41\\ 80\\ 93\end{bmatrix}$$

$$A * (P_7)^{\mathrm{T}} = \begin{bmatrix}1 & 3\\ 2 & 4\\ 5 & 7\\ 6 & 8\end{bmatrix} * \begin{bmatrix}81\\ 62\end{bmatrix} = \begin{bmatrix}77\\ 30\\ 79\\ 32\end{bmatrix}$$

Selanjutnya transposkan hasil kali matriks kunci A dengan matriks $P_1 – P_7$, lalu digabungkan sehingga terbentuk sebuah matriks *ciphertext* (lihat [6]).

$(A*(P_1)^T)^T$ = [0, 43, 77, 25], $(A*(P_2)^T)^T$ = [16, 75, 62, 26], $(A*(P_3)^T)^T$ = [51, 34, 78, 61]

$(A*(P_4)^T)^T$ = [22, 15, 89, 82], $(A*(P_5)^T)^T$ = [20, 31, 64, 75], $(A*(P_6)^T)^T$ = [28, 41, 80, 93], $(A*(P_7)^T)^T$ = [77, 30, 79, 32]

Ciphertext = [0, 43, 77, 25, 16, 75, 62, 26, 51, 34, 78, 61, 22, 15, 89, 82, 20, 31, 64, 75, 28, 41, 80, 93, 77, 30, 79, 32]

Korespondensikan matriks *ciphertext* dengan huruf yang ada di tabel korespondensi sehingga didapatkan *ciphertext* **Ar\ZQ] azi|9WP(@Uf<]cp~=\e`g**

C. Proses Dekripsi

Langkah 1: Korespondensikan *ciphertext* dengan bilangan pada tabel korespondensi. Sehingga didapat matriks$C$

Langkah 2: Partisi matriks C kedalam beberapa blok dengan masing-masing blok terdiri dari elemen sebanyak jumlah baris matriks kunci K sehingga didapat matriks C_1 sampai C_n

Langkah 3: Kalikan p-invers matriks kunci dengan transpose matriks C_1 sampai $C_n$hasil kali dibulatkan kedalam bilangan modulo 95.

Langkah 4: Transposkan matriks hasil langkah 3, kemudian digabungkan sehingga didapatkan matriks *plaintext*

Langkah 5: Korespondensikan angka pada matriks *plaintext* dengan karakter pada tabel korespondensi sehingga didapatkan *plaintext*

Contoh: Korespondensikan *ciphertext* yang didapat dari proses enkripsi dengan bilangan dalam Z_{95} sehingga didapat matriks C yang memiliki 28 Elemen. Partisi matriks C menjadi beberapa matriks yang masing-masing terdiri dari 4 elemen (sesuai dengan jumlah baris matriks A) sehingga didapat C_1 sampai C_7

C_1 = [0, 43, 77, 25], C_2 = [16, 75, 62, 26], C_3 = [51, 34, 78, 61], C_4 = [22, 15, 89, 82]

C_5 = [20, 31, 64, 75], C_6 = [28, 41, 80, 93], C_7 = [77, 30, 79, 32]

Transposkan matriks C_1 sampai dengan C_7, kemudian Kalikan matriks B dengan matriks $(C_1)^T$ sampai dengan $(C_7)^T$

$$B * (C_1)^T = \begin{bmatrix} 33 & 15 & 56 & 38 \\ 87 & 38 & 81 & 32 \end{bmatrix} * \begin{bmatrix} 0 \\ 43 \\ 77 \\ 25 \end{bmatrix} = \begin{bmatrix} 17 \\ 26 \end{bmatrix}$$

$$B * (C_2)^T = \begin{bmatrix} 33 & 15 & 56 & 38 \\ 87 & 38 & 81 & 32 \end{bmatrix} * \begin{bmatrix} 16 \\ 75 \\ 62 \\ 26 \end{bmatrix} = \begin{bmatrix} 33 \\ 26 \end{bmatrix}$$

$$B * (C_3)^T = \begin{bmatrix} 33 & 15 & 56 & 38 \\ 87 & 38 & 81 & 32 \end{bmatrix} * \begin{bmatrix} 51 \\ 34 \\ 78 \\ 61 \end{bmatrix} = \begin{bmatrix} 44 \\ 34 \end{bmatrix}$$

$$B * (C_4)^T = \begin{bmatrix} 33 & 15 & 56 & 38 \\ 87 & 38 & 81 & 32 \end{bmatrix} * \begin{bmatrix} 22 \\ 15 \\ 89 \\ 82 \end{bmatrix} = \begin{bmatrix} 26 \\ 62 \end{bmatrix}$$

$$B * (C_5)^T = \begin{bmatrix} 33 & 15 & 56 & 38 \\ 87 & 38 & 81 & 32 \end{bmatrix} * \begin{bmatrix} 20 \\ 31 \\ 64 \\ 75 \end{bmatrix} = \begin{bmatrix} 54 \\ 52 \end{bmatrix}$$

$$B * (C_6)^T = \begin{bmatrix} 33 & 15 & 56 & 38 \\ 87 & 38 & 81 & 32 \end{bmatrix} * \begin{bmatrix} 28 \\ 41 \\ 80 \\ 93 \end{bmatrix} = \begin{bmatrix} 53 \\ 55 \end{bmatrix}$$

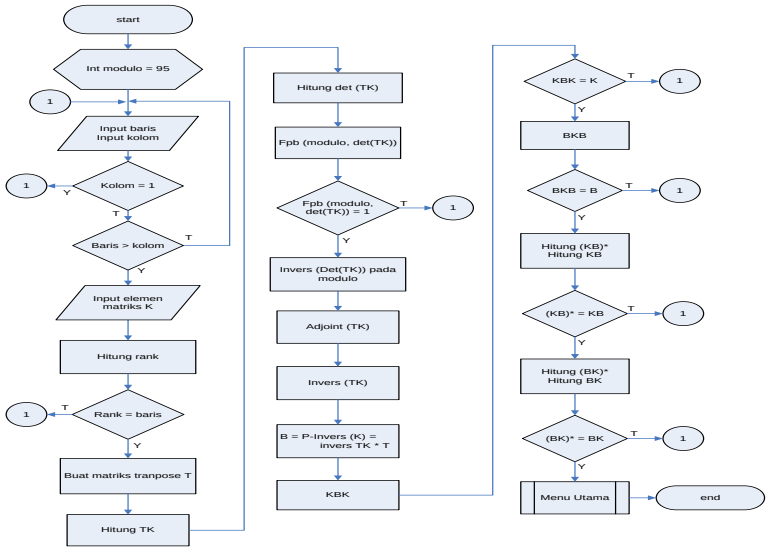
$$B * (C_7)^T = \begin{bmatrix} 33 & 15 & 56 & 38 \\ 87 & 38 & 81 & 32 \end{bmatrix} * \begin{bmatrix} 77 \\ 30 \\ 79 \\ 32 \end{bmatrix} = \begin{bmatrix} 81 \\ 62 \end{bmatrix}$$

Hasil kali $B(C_1)^T$ sampai $B(C_7)^T$ ditransposkan sehingga menjadi $(B(C_1)^T)^T$ sampai $(B(C_7)^T)^T$ $(B(C_1)^T)^T$ = [17, 26], $(B(C_2)^T)^T$ = [33, 26] , $(B(C_3)^T)^T$ = [44, 34], $(B(C_4)^T)^T$ = [26, 62], $(B(C_5)^T)^T$ = [54, 52], $(B(C_6)^T)^T$ = [53, 55], $(B(C_7)^T)^T$ = [81, 62]

Gabungkan $(B(C_1)^T)^T$sampai $(B(C_7)^T)^T$sehingga didapat matriks plaintext [17, 26, 33, 26, 44, 34, 26, 62, 54, 52, 53, 55, 81, 62]

Korespondensikan matriks plaintext dengan huruf pada tabel korespondensi sehingga didapatkan plaintext kembali yaitu **Rahasia 2013!**

Flowchart

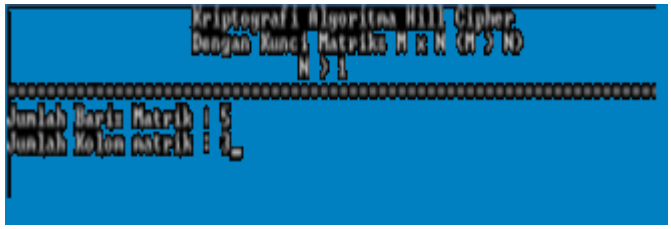


Gambar 2. Proses Inisialisasi Matriks Kunci

D. Program Aplikasi

Kriptografi menggunakan algoritma Hill Cipher yang diperluas ini membutuhkan proses penghitungan yang cukup rumit terutama jika kunci yang digunakan berordo besar atau plaintext terdiri dari kalimat yang sangat panjang, tentunya hal ini mempersulit pengguna. Untuk itu, saya membuat program aplikasi untuk memudahkan proses inisialisasi kunci, enkripsi dan Dekripsinya. Berikut ini simulasi dari program aplikasi yang sudah dibuat:

1. Pertama kali dijalankan user harus input jumlah baris dan kolom matriks kunci.



Gambar 3.
Input baris dan kolom matriks kunci

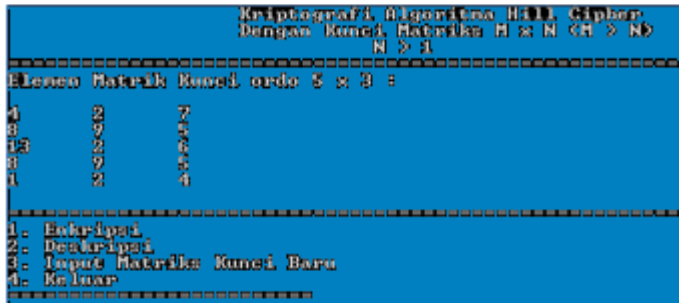
2. Jika Memenuhi syarat, maka akan tampil layout untuk input elemen matriks kunci. Klik enter setiap kali selesai input elemen matriks kunci.

Gambar 4.
Input Elemen Matriks Kunci

3. Setelah input elemen matriks kunci, program akan melakukan check syarat-syarat matriks kunci. Jika memenuhi syarat matrik kunci, user input nama file teks untuk menyimpan data matriks kunci.

Gambar 5.
Input file teks untuk menyimpan data matriks kunci

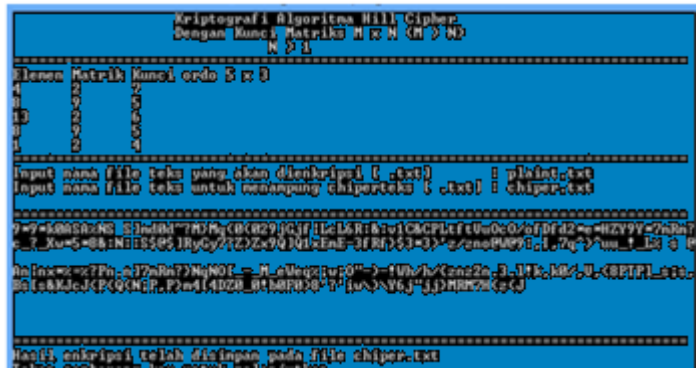
Selanjutnya tampil menu sebagai berikut:



Gambar 6. Menu

4. Klik 1 untuk melakukan proses enkripsi. User input nama file teks tempat plaintext disimpan. Klik enter lalu input nama file teks untuk menyimpan hasil enkripsinya.

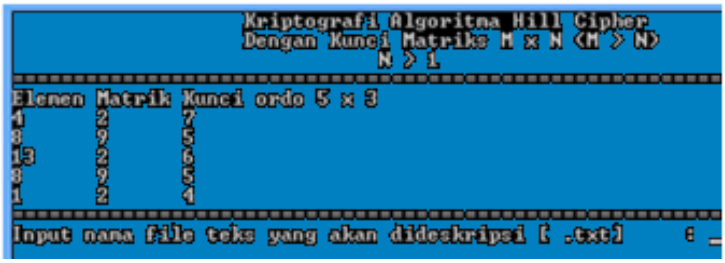
Gambar 7. Menu enkripsi



Gambar 8. Hasil enkripsi

5. Klik 2 untuk melakukan proses Dekripsi.User input nama file teks tempat ciphertext disimpan. Klik enter lalu input nama file teks untuk menyimpan hasil Dekripsinya.

Gambar 9. Menu Dekripsi



Gambar 10. Hasil Dekripsi

6. Klik 3 untuk input kunci matriks baru, sehingga tampil kembali gambar 3.

5. Simpulan

Teori *pseudo invers*, dapat dimanfaatkan pada algoritma Hill Cipher. Hal ini memungkinkan penggunaan matriks persegi panjang m x n ($m \geq n$ dan $n > 1$) pada algoritma Hill Cipher. Sehingga ukuran matriks dapat lebih beragam, Penggunaan matriks persegi panjang, menghasilkan *ciphertext* yang lebih panjang dari *plaintext* nya. Hal ini tentu membuat pesan menjadi lebih tersamarkan. *Plaintext* yang sama akan menghasilkan *ciphertext* yang berbeda jika dienkripsi menggunakan matriks kunci yang berbeda. Penggunaan modulo yang bukan merupakan bilangan prima, menyebabkan terbatasnya matriks kunci yang dapat digunakan. Penggunaan program aplikasi mempermudah penghitungan saat inisialisasi matriks kunci, proses enkripsi dan proses Dekripsi terutama pada penggunaan matriks kunci dengan ordo yang besar dan plaintext yang panjang.

Daftar Pustaka

1. Ariyus, Doni. 2008. Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi. Yogyakarta: Penerbit Andi
2. Munir, Rinaldi. 2007. Kriptografi. Bandung: Informatika
3. Prima, Niken dan Nurdin B. FMIPA UNDIP.

4. Ratnadewi, dkk. 2013. Matematika Teknik Untuk Perguruan Tinggi. Bandung: Informatika
5. Supranto, J. 1997. Pengantar Matrix. Jakarta: Rineka Cipta
6. Widyanarko, arya. 2007. Studi dan Analisis mengenai Hill Cipher, Teknik Kriptanalisis dan Upaya Penanggulangannya. Bandung: Fakultas Teknik ITB