JURNAL TEKNIK KOMPUTER AMIK BSI

ANALISA *CRYPTOGRAPHY* DENGAN PENGHITUNGAN MANUAL MENGGUNAKAN METODE MATRIKS BERDASARKAN ALGORITMA *CHIPER HILL*

Aziz Setyawan. H

Abstract* — *A computer security system main menu concept is how the message is sent by the sender before there is a process to hide the meaning of the message or the data. And if there are people who steal messages and data may not understand the meaning of the message that is taken or received. Cryptography is the science and art to maintain the security of the message when the message is sent from one place to another. Chiper algorithm hill is one method of cryptography that belongs to the symmetric algorithm. Chiper hill is an example of a polyalphabetic cipher that employs modulus and linear algebra techniques. In the process of encrypting hill chipper require help table to encode letters or Abjat are arranged in a sequence of letters or Abjat "A" to "Z". Encryption Abjat and this letter serves as a conversion of plaintext (messages or data) and key that you want to encrypt and decrypt. So that components or figures can be done by calculating the matrix multiplication.

Intisari — **Sebuah system keamanan komputer menu utama konsepnya adalah bagaimana pesan tersebut sebelum dikirim oleh si pengirim ada sebuah proses untuk menyembunyikan pesan arti dari pesan atau data tersebut. Dan jika ada orang yang mencuri pesan atau data tersebut tidak mengerti maksud dari pesan yang diambilnya atau diterima. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Algoritma *Chiper hill* merupakan salah satu metode kriptografi yang termasuk ke dalam algoritma simetris. *Chiper hill* adalah contoh dari chiper polyalphabetic yang mempekerjakan modulus dan teknik aljabar linier. Dalam proses melakukan enkripsi chipper hill memerlukan tabel bantuan untuk menyandikan huruf atau abjat yang disusun secara berurutan dari huruf atau abjat "A" sampai dengan "Z". Penyandian abjat dan huruf ini berfungsi sebagai konversi dari plaintext (pesan atau data) dan *key* yang ingin di enkrip dan di dekrip. Sehingga komponen-komponen atau angka-angka tersebut dapat dilakukan dengan penghitungan perkalian Matriks.**

Kata kunci : *Cryptography*, *Chiper hill*, Matriks, Invers.

Program Studi Teknik Komputer AMIK BSI Tegal, JL Sipelem, No. 8, Kemandungan, Tegal Barat Tegal Jawa-Tengah 52112 Telp +62 283 325114; e-mail: aziz.aiz@bsi.ac.id

I. PENDAHULUAN

Sebuah system keamanan komputer menu utama yang harus dijadikan sebuah ukuran adalah bagaimana dalam mengirimkan pesan dari pengirim ke penerima harus dapat dijaga kerahasiannya. Agar data atau pesan yang dikirimkan tidak dapat dimengerti oleh orang-orang yang tidak diberi hak untuk mengetahuinya. Konsepnya adalah bagamaimana pesan tersebut sebelum dikirim oleh si pengirim ada sebuah proses yang harus dilakukan untuk menyembunyikan pesan arti dari pesan atau data tersebut. Dan jika ada orang yang mencuri pesan atau data tersebut tidak mengerti maksud dari pesan yang diambilnya atau diterima. Untuk mengetahui arti pesan sebenarnya maka penerima harus melakukan proses perubahan pesan teks yang tidak artinya ke pesan atau data aslinya.

Di dalam dunia jaringan komputer saat ini berkembang dunia hacker yang bertujuan melakukan penyadapan pada jaringan komputer yang dikenal dengan sniffing. Banyak sekali tools-tools sniffing yang digunakan untuk melakukan aksinya, seperti : wireshark, cain and abel, kismet dan lain-lainnya.

> "Sniffer adalah sejenis program pencuri informasi yang memantau informasi dalam sebuah jaringan. Ketika digunakan secara legal, sniffer membantu mengidentifikasi tempat yang potensial bermasalah di jaringan atau menelusuri aktivitas criminal di jaringan, namun apabila digunakan untuk tujuan criminal, sniffer dapat bersifat merusak dan sangat sulit dideteksi. Sniffer dapat membuat hacker mampu mencuri informasi berharga dari manapun dalam jaringan, termasuk pesan e-mail, file dan laporan rahasia perusahaan" [8].

Sampai saat ini sniffing tidak bias dicegah, ini dikarenakan untuk mendapatkan tools-tools pendukung sniffing dengan mudah didapat di internet. Sehingga solusinya agar tidak terjadi pencurian data atau pesan si user harus dapat melakukan pencegahan, seperti pada saat melakukan pengirman pesan atau data penting harus melakukan enkripsi data atau pesan tersebut. Walaupun data atau pesan dapat dicuri atau disadap tetapi orang yang mencuri atau menyadap tidak tahu maksud dari data atau pesan tersebut.

Maka dalam penelitian ini penulis menganalisa system enkripsi dan dekripsi, dimana data atau pesan yang ingin dikirimkan oleh pengirim, dirubah tampilan data atau pesan

tersebut dalam bentuk yang tidak lazim, sehingga orang yang tidak diberi izin untuk mengetahui isi dari data atau pesan tersebut bingung dan tidak tahu maksud dari data atau pesan tersebut. Sedangkan penerima data atau pesan yang dituju oleh pengirim tersebut dapat melakukan pengubahan data yang tidak lazim ke dalam bentuk data atau pesan yang dapat dimengerti dan mempunyai arti.

"Enkripsi ialah salah satu cara yang bias digunakan untuk mengubah teks "asli" (sebenarnya) menjadi teks "buatan"" [6]. Jadi hasil output dari enkripsi adalah teks buatan yang tidak mudah dibaca oleh orang yang menerima teks tersebut, baik si penerima yang dimaksud oleh si pengirim atau orang tidak berhak menerima teks tersebut. Selanjutnya bagaimana teks buatan tersebut dirubah kembali ke dalam teks asli agar isi pesan dapat dibaca oleh orang yang dimaksud oleh si penerima bukan orang yang tidak dimaksud oleh si penerima.

Proses tersebut diatas adalah proses kebalikan dari proses enkripsi yang disebut sebagai dekripsi. "Dekripsi adalah kebalikan dari enkripsi, dimana berfungsi untuk mendekripsikan data yang telah dienkripsi, dimana berfungsi untuk mendekripsikan data yang telah dienkripsi sehingga data yang telah menjadi kode rahasia diubaj kembali menjadi data biasa atau aslinya" [11]. Jadi dapat dikatakan bahwa dalam proses dekripsi memerlukan sebuah key yang digunakan pada proses enkripsi.

Dalam proses enkripsi dan dekripsi ini menjadi topic utama dalam ilmu kriptografi. Dalam prosesnya kriptograpi adalah mengubah pesan teks asli yang disebut dengan *plaintext* dirubah menjadi pesan teks tidak asli yang disebut juga *chipertext.* "Ilmu matematika yang mendasari teknik enkripsi dan dekripsi disebut kriptologi sedangkan teknik sains dari proses enkripsi-dekripsi disebut kriptografi" [11].

Maka dalam penelitian ini penulis merumuskan masalah yang diangkat dalam analisa pembelajaran kriptograpi dalam pengaman data atau pesan, adalah sebagai berikut :

1. Menjelaskan proses Algoritma symmetric dengan menggunakan chipper hill ?
2. Bagaimana proses enkripsi sebuah pesan atau data dengan menggunakan chipper hill ?
3. Bagaimana proses dekripsi sebuah pesan atau data dengan menggunakan chipper hill ?

Sedangkan batasan dalam penelitian ini penulis membatasi pada masalah, antara lain :

1. Implementasi enkripsi dan dekripsi berdasarkan cryptool.
2. Pengurutan tabel angka terhadap huruf berdasarkan chipper hill.
3. Melakukan proses matriks-kulasi (penghitungan berdasarkan Metode Matriks) dalam mengenkripsi dan mendekripsi.

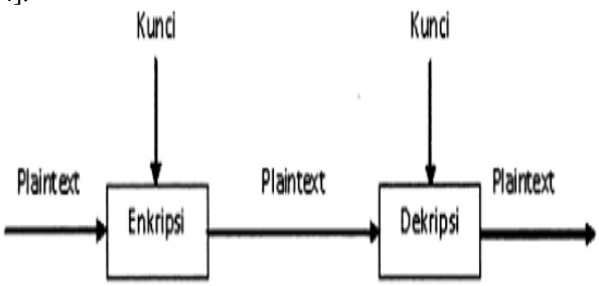
II. KAJIAN LITERATUR

A. Kriptograpi

"Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia. Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain" [2].

Kriptografi ini sangat unik dan beragam dalam implementasinya. Saking uniknya metode kriptografi ini sudah ada sebelum adanya teknologi komputer, 3000 tahun Sebelum Masehi yang lalu bangsa Mesir sudah menggunakan metode ini dengan menggunakan tulisan yang dikenal dengan *hieroglyph*. Jadi bangsa Mesir pada zaman tersebut dalam menyampaikan sebuah perkara atau konsep mereka menyimbolkan dengan gambar-gambar. Sedangkan di Indonesia sendiri khususnya Jawa telah memnggunakan metode Kriptografi mengenai tulisan yang dikenal dengan *syllabary.* Syllabary adalah sebuah tulisan yang mewakili sebuah kalimat, metode ini dikenal juga dengan Hocoroko.

Saat ini dengan teknologi komputer lahir dan terus berkembang maka metode kriptografi pun terus semakin beragam. Keberagaman ini dilihat dari algoritma yang digunakan dalam menuangkan konsep kriptografi. Konsep dasar dari kriptografi adalah merubah *plantext* menjadi teks buatan yang tidak mudah dimengerti yang disebut sebagai *chipertext.* "Proses transformasi dari plaintext menjadi *chipertext* disebut proses Enchiperment atau enkripsi (*encryption*), sedangkan proses mentransformasikan kembali *chipertext* menjadi plaintext disebut dekripsi (*decryption*)" [14].



Sumber: Hasil Penelitian (2015)

Gambar 1 : Proses Enkripsi-Dekripsi sederhana

Sedangkan kriptografi dalam implementasinya ada beberapa komponen-komponen pendukung untuk melakukan proses enkripsi-dekripsi."Pada dasarnya komponen kriptografi terdiri dari beberapa komponen, seperti [2] :

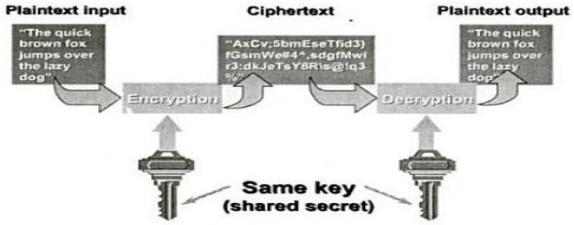
1. Enkripsi
   Merupakan hal yang sangat penting dalam kriptografi, merupakan cara pengamanan data yang dikirimkan sehingga terjaga kerahasiaannya. Pesan asli disebut *plaintext* (pesan-buasa), yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bias diartikan dengan chipper atau kode. Sama halnya dengan tidak mengerti sebuah kata maka kita akan melihatnya di dalam kamus atau daftar istilah. Beda halnya dengan enkripsi, untuk mengubah teks bias ke bentuk bentuk teks-kode kita gunakan algoritma yang dapat mengkodekan data yang kita ingini.
2. Dekripsi
   Merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya. Algoritma

yang digunakan untukdekripsi tentu berbeda dengan yang digunakan untuk enkripsi.

3. Kunci
   Adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, yaitu kunci rahasia (*private key*) dan kunci umum (*public key*).
4. *Chipertext*.
   Merupakan suatu pesan yang telah melalui proses enkripsi. Pesan yang ada pada teks kode ini tidak bias dibaca karena berupa karakter-karakter yang tidak mempunyai makna (arti).
5. Plaintext.
   Sering disebut dengan cleartext. Teks-asli atau teks-biasa ini merupakan pesan yang diketik yang memiliki makna. Teks-asli inilah yang diproses menggunakan algoritma kriptografi untuk menjadi *chipertext* (teks-kode).
6. Pesan.
   Dapat berupa data atau informasi yang dikirim (melalui kurir, saluran komunikasi data, dan sebagainya) atau yang disimpan di dalam media perekam (kertas, storage, dan sebagainya).
7. Cyptanalysis.
   Bisa diartikan sebagai analisis kode atau suatu ilmu untuk mendapatkan teks-asli tanpa harus mengetahui kunci yang sah secara wajar. Jika suatu teks-kode berhasil diubah menjadi teks-asli tanpa menggunakan kunci yang sah, proses tersebut dinamakan breaking code. Hal ini dilakukan oleh para kriptanalis. Analisis kode juga dapat menemukan kelamahan dari suatu algoritma kriptografi dan akhirnya dapat menemukan kunci teks-asli dari teks-kode yang dienkripsi dengan algoritma tertentu.

Di dalam pengimplemenstasian enkripsi dan dekripsi pada kriptografi menggunakan banyak algoritma yang digunakan. “Pada kriptografi modern terdapat berbagai macam algoritma yang dimaksudkan untuk mengamankan informasi yang dikirim melalui jaringan komputer. Algoritma modern terdiri dari dua bagian [2]:

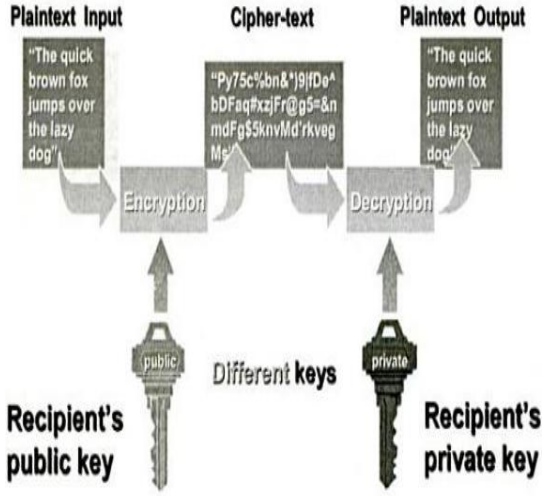
1. Algortima Simetric
   Adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Contoh : Alice ingin mengirim pesan x dengan aman menggunakan saluran umum kepada Bob. Alice menggunakan kunci xo yang sebelumnya telah disepakati antara Alice dan Bob. Untuk mengirim pesan e xo (x) kepada Bob, dia akan mendekripsi teks-kode yang diterima dengan kunci yang sama dengan yang digunakan untuk memperoleh akses ke pesan yang diterima. Begitu juga sebaliknya.



Sumber: Hasil Penelitian (2015)

Gambar 2 : Algoritma Simetris

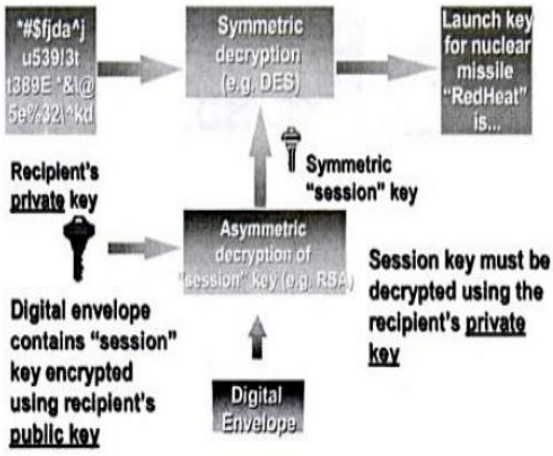
2. Algoritma Asymetric
   Adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan yang satu lagi untuk dekripsi. Semua orang yang mendapatkan kunci public dapat menggunakannya untuk mengenkripsi suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia itu, yang dalam hal ini kunci rahasia, untuk melakukan pembongkaran terhadap kode yang dikirim untuknya. Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA (merupakan singkatan dari nama penemunya, yakni Revest, Shamir dan Adleman).



Sumber: Hasil Penelitian (2015)

Gambar 3 : Algoritma Asimetris

3. Hybrid
   Adalah algoritma yang memanfaatkan dua tingkatan kunci yaitu kunci rahasia (simteri) yang disebut juga session key (kunci sesi) untuk enkripsi data dan pasangan kunci rahasia-kunci public untuk pemberian tanda tangan digital serta melindungi kunci simetri.



Sumber: Hasil Penelitian (2015)

Gambar 4 : Algoritma Hybrida

B. ***Chiper hill***

Algoritma *Chiper hill* merupakan salah satu metode kriptografi yang termasuk ke dalam algoritma simetris. Algoritma ini ditemukan oleh Lester S. Hill pada tahun 1929. "*Chiper hill* adalah contoh dari chiper polyalphabetic yang mempekerjakan modulus dan teknik aljabar linier" [13]. Dalam proses melakukan enkripsi chipper hill memerlukan tabel bantuan untuk menyandikan huruf atau abjat yang disusun secara berurutan dari huruf atau abjat "A" sampai dengan "Z".

"Pada saat proses enkripsi di chipper hill selanjutnya menghitung dari persamaan $y = (ax+b) \bmod 26$, atau ekuivalen $y = (xa+b) \bmod 26$, a dan b diambil data konversi abjat atau hurup A sampai Z dengan jumlah karakter 26 (dua puluh enam), dimana a dipilih sehingga $a^{-1} \bmod 26$ yang ada" [7]. Huruf atau abjat tersebut diurutkan dengan angka yang berurutan juga sesuai dengan urutan angka, jadi sesuai dengan kebutuhan angka yang dibutuhkan dalam mengurutkan huruf atau abjat dengan angka memerlukan angka dari 0 (nol) sampai dengan angka 25 (dua puluh lima) atau bias juga dimulai dengan angka "1" (satu) sampai dengan "26" (dua puluh enam).

Tabel 1 : Pengurutan Abjat berdasarkan Nilai Angka dari "0" null

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

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

Sumber: Hasil Penelitian (2015)

Tabel 2 : Pengurutan Abjat berdasarkan Nilai Angka dari "1" satu

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

O	P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25	26

Sumber: Hasil Penelitian (2015)

Penyandian abjat atau huruf ini digunakan untuk membuat komponen-komponen atau angka-angka dalam Matriks. Penyadian abjat dan huruf ini berfungsi sebagai konversi dari plaintext (pesan atau data) dan *key* yang ingin di enkrip dan di dekrip. Sehingga komponen-komponen atau angka-angka tersebut dapat dilakukan dengan penghitungan perkalian Matriks. "*Key K* yang digunakan dalam chiper ini adalah matriks integer *nxn"* [13]. Jadi *key K* yang akan digunakan dalam proses enkripsi berdasarkan banyaknya identitas dari Matriks, contohnya : 2x2 (*key* berjumlah 4 komponen atau angka), 3x3 (*key* berjumlah 9 komponen atau angka), dan seterusnya.

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

Sehingga rumus enkripsi adalah :

$$\boxed{C = K.P \bmod m}$$

Keterangan :
C : *Chipertext*
K : Key
P : *Plantext*
m : Jumlah tabel karakter
Rumus tersebut diperjelas [10] :

Selanjutnya bagaimana proses dekrip ? Proses dekrip dapat dilakukan dengan mencari invers (kebalikan dari matriks) dengan symbol *key* K^{-1}. *Key* K^{-1} tersebut dikalikan dengan angka-angka dari element matriks *chipertext*. Dan untuk mengkonversi hasil pengalian dari *key* K^{-1} dengan *chipertext* akan dikalikan kembali ke "mod 26".

Rumus yang digunakan dalam melakukan proses dekripsi adalah, sebagai berikut :

$$\boxed{P = K^{-1}.C \bmod m}$$

Keterangan :
P : *Plantext*
K^{-1} : Key Invers
C : *Chipertext*
m : Jumlah tabel karakter

Sedangkan rumus dekripsi diatas [11], adalah sebagai berikut :

$$\text{For Decryption: } D_K(C) = K^{-1}C = K^{-1}KP = P, \text{ i.e.,}$$

$$(p_1\ p_2\ \dots\ p_m) = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1m} \\ k_{21} & k_{22} & \dots & k_{2m} \\ \dots & \dots & \dots & \dots \\ k_{m1} & k_{m2} & \dots & k_{mm} \end{bmatrix}^{-1} (c_1\ c_2\ \dots\ c_m)$$

Sedangkan proses yang terjadi pada saat dekripsi ini dijelaskan dengan rumus proses sebagai berikut [5]:

$$\boxed{D = K^{-1}(x - y) \bmod m}$$

Keterangan :
K^{-1} : Key Invers
x : Plainteks yang dikonversi menjadi bilangan bulat
b : Jumlah pergeseran (*caesar cipher* adalah khusus dari *affine cipher* dengan m = 1)
m : Jumlah tabel karakter

Di mana K^{-1} adalah invers perkalian a modulus m yang dapat memenuhi persamaan sebagai berikut:

$$\boxed{1 = K\ y\ K^{-1} \bmod m}$$

Keterangan :
K : *Key*
K^{-1} : Key Invers
x : Plainteks yang dikonversi menjadi bilangan bulat

m : Jumlah tabel karakter
y : Jumlah pergeseran (*caesar cipher* adalah khusus dari *affine cipher* dengan m = 1)

C. **Matriks**

Sebuah matriks (matriks) adalah sebuah urutan angka-angka (symbol) yang mengikuti dua aturan perhitungan-pertama, hubungan angka-angka lintas kolom dan kedua hubungan angka-angka lintas baris. Kedua hubungan tersebut disebut sebagai identitas matriks, karena kedua hubungan tersebut secara definisi benar adanya [9].

"Suatu matriks(dituliskan dengan menggunakan huruf besar dan tebal) adalah suatu array elemen-elemen segiempat yang tersusun dari baris horizontal dan kolom vertical" [3].

Di asumsikan bahwa matriks yang digunakan memiliki jumlah baris dan kolom yang sama (*n x n*).

a. Perkalian Matriks

"Ada dua jenis perkalian matriks, yaitu perkalian antara matriks A dengan scalar g, dan perkalian antara matriks A dengan B" [12].

1. Perkalian antara matriks A dengan scalar g akan menghasilkan matriks C yang elemennya merupakan perkalian dari setiap elemen pada matriks A dengan g.

$$C = g.A = \begin{Bmatrix} g.a_{11} & g.a_{12} & g.a_{13} \\ g.a_{21} & g.a_{22} & g.a_{23} \\ g.a_{31} & g.a_{32} & g.a_{33} \end{Bmatrix}$$

Contoh dari perkalian matriks dengan scalar adalah : g = 3, sedangkan

$$A = \begin{Bmatrix} 5 & 6 \\ 4 & 3 \end{Bmatrix}$$

$$\boxed{g.A = C}\ C = 3\begin{Bmatrix} 5 & 6 \\ 4 & 3 \end{Bmatrix} = \begin{Bmatrix} 3.5 & 3.6 \\ 3.4 & 3.3 \end{Bmatrix}$$

Maka proses perkalian yang akan terjadi pada persamaan g . A = C adalah

Jadi hasil Perkalian Matriks dengan scalar g . A = C, adalah :

$$C = \begin{Bmatrix} 15 & 18 \\ 12 & 9 \end{Bmatrix}$$

2. Perkalian antara matriks A yang mempunyai ukuran *m x n* dan matriks B yang mempunyai ukuran *n x l* akan menghasilkan matriks C dengan ukuran m x l. Perkalian antara dua matriks dapat dioperasikan jika ukuran interior matriksnya sama.

$$\boxed{C_{m\,x\,l} = A_{m\,x\,n} X\ B_{n\,x\,l}}$$

Contoh dari perkalian antara matriks, adalah :
Matriks A dengan ukuran 2x3 dengan matriks B ukuran 3x2.

$$B = \begin{Bmatrix} n_1 & n_2 & n_3 \\ n_4 & n_5 & n_6 \end{Bmatrix}\quad A = \begin{Bmatrix} m_1 m_2 \\ m_3 m_4 \\ m_5 m_6 \end{Bmatrix}$$

$$AxB = \begin{Bmatrix} m_1n_1 + m_3n_2 + m_5n_3 & m_2n_1 + m_4n_2 + m_6n_3 \\ m_1n_4 + m_3n_5 + m_5n_6 & m_2n_4 + m_4n_5 + m_6n_6 \end{Bmatrix}$$

Diketahui matriks A dengan ukuran 2 x 3, dengan bentuk :

$$A = \begin{Bmatrix} 2 & 3 & 4 \\ 5 & 2 & 3 \end{Bmatrix}$$

Selain itu diketahui matriks B dengan ukuran 3 x 2, dengan bentuk :

$$A = \begin{Bmatrix} 2 & 3 \\ 5 & 2 \\ 4 & 3 \end{Bmatrix}$$

Maka proses dari perkalian antara matriks AxB, adalah :

$$AxB = \begin{Bmatrix} 2 & 3 & 4 \\ 5 & 2 & 3 \end{Bmatrix}\begin{Bmatrix} 2 & 3 \\ 5 & 2 \\ 4 & 3 \end{Bmatrix}$$

$$= \begin{Bmatrix} 2.2 + 3.5 + 4.4 & 2.3 + 3.2 + 4.3 \\ 5.2 + 2.5 + 3.4 & 5.3 + 2.2 + 3.3 \end{Bmatrix}$$

$$= \begin{Bmatrix} 4 + 15 + 16 & 6 + 6 + 12 \\ 10 + 10 + 12 & 15 + 4 + 9 \end{Bmatrix}$$

$$= \begin{Bmatrix} 35 & 24 \\ 32 & 28 \end{Bmatrix}$$

b. Invers Matriks

Sebuah matriks mempunyai invers ditentukan oleh perkalian matriks tersebut dengan kebalikan matriksnya tersebut menghasilkan "1" (satu). "Invers matriks K, yang ditujunkkan dengan K^{-1}, hanya dapat ditentukan bila K adalah bujursangkar, di mana dalam hal ini adalah matriks yang memenuhi kondisi" [4].

Ketentuan tersebut dapat dijelaskan sebagai berikut : Contoh dibawah ini adalah matriks dengan ordo 2x2.

$$K = \begin{Bmatrix} a & b \\ c & d \end{Bmatrix}$$

Jika matriks maka invers matriks A, ditulis A^{-1} dirumuskan sebagai berikut :

$$Invers = (ab - cd)^{-1}\begin{Bmatrix} d & -b \\ -c & a \end{Bmatrix}$$

Dengan syarat ad-bc ≠ 0 (nol).

Contoh untuk mencari invers matriks (K^{-1}), K dengan berordo 2x2 dan mempunyai angka-angka elemennya sebagai berikut :

$$K = \begin{Bmatrix} 1 & 2 \\ 4 & 10 \end{Bmatrix}$$

$$1 = K\ y\ K^{-1}\ mod\ m$$

$$1 = \begin{Bmatrix} a & b \\ c & d \end{Bmatrix} y\ (ad - bc)^{-1}\ \begin{Bmatrix} d & -b \\ -c & a \end{Bmatrix} Mod26$$

$$1 = \begin{Bmatrix} 1 & 2 \\ 4 & 10 \end{Bmatrix} y\ (1.10 - 2.4)^{-1}\ \begin{Bmatrix} 10 & -2 \\ -4 & 1 \end{Bmatrix} Mod26$$

$1 = (1.10 - 2.4)y(2)^{-1}(10.1 - (-2)(-4))\ Mod\ 26$

1 = 2*y* 2^{-1}.2 Mod 26

1 = 2*y* Mod 26

1 = 2 (3,5) Mod 26

Jadi *y*=3,5

D. **CrypTool**

Cryptool merupakan salah satu program perngkat lunak yang digunakan untuk meningkatkan kesadaran dan minat dalam teknik enkripsi dan dekripsi untuk semua orang. Program ini bertujuan untuk pembelajaran juga dalam kriptografi dan sifatnya adalah open source, jika semua orang ingin memiliki program ini tersedia secara gratis untuk mendapatkannya. Cryptool dikembangkan oleh dunia e-learning secara gratis dan yang paling luas digunakan dalam bidang cryptoanalysis.

Relawan, terutama programmer dan mahasiswa berencana untuk menulis tesis mereka di bidang kriptografi, selalu diterima untuk bergabung dalam pengembangan lebih lanjut dari proyek CrypTool. CrypTool telah diproduksi dengan cara yang sangat profesional dan inovatif. Hal ini membantu sebagai alat pendidikan untuk pemula dan memberikan pengalaman praktis yang sangat baik untuk berpengetahuan

Penghargaan atau keunggulan dari tools ini adalah :

1. Germany — *Land of Ideas* 2008
2. *European Information Security Award* 2004
3. *IT Security Award* NRW 2004
4. TeleTrusT *Special Award* 2004.

III. METODE PENELITIAN

Metode penelitian yang digunakan adalah studi literatur dengan pengamatan menggunakan Cryptool untuk melakukan melihat hasil enkripsi dan dekripsi dari sebuah pesan atau kata. Selanjutnya penulis melakukan percobaan-percobaan sebuah pesan atau kata diproses dengan melakukan penghitungan secara manual sesuai dengan teori tentang bagaimana mengenkripsi dan bagaiaman mendekripsi secara manual dengan algoritma chipper hill. Hasil dari penghitungan pesan atau kata tersebut diolah secara manual dengan metode matrikulasi dan hasil yang dikeluarkan akan disamakan dengan keluaran program Cryptool dari pesan atau kata tersebut.

IV. HASIL DAN PEMBAHASAN

Pada penelitian ini penulis menganalisa bagaimana proses pesan atau data di enkripsi atau di dekripsi menggunakan algoritma *chiper hill*. Cara enkripsi-dekripsi dengan algoritma hill menggunakan matriks bujur sangkar, di dalam bujur sangkar tersebut ditentukan matriks berordo 2x2, maka jumlah elemen angka-angka yang ada di dalam bujur sangkar tersebut berjumlah 4 (empat angka).

Angka ini dihasilkan dari konversi teks atau data dan *key K* dengan tabel konversi huruf atau abjat ke angka yang dimulai dari huruf atau abjat "A" sampai dengan "Z". Jadi angka urut dari huruf atau abjat tersebut dari "0" (satu) sampai dengan "26" (dua puluh enam). Teks atau data disini disebut juga dengan *plantext*.

A. Enkripsi

plaintext yang akan dienkripsi adalah : **PASSWORD RASI**.

Membuat bujur sangkar dengan matriks ordo 2x2 dari *key* K : **ASLI**. Sedangkan plantextnya di kelompokkan dua huruf atau abjat, seperti di bawah ini :

P =

P	**S**	**W**	**R**	**R**	**S**
A	**S**	**O**	**D**	**A**	**I**

Selanjutnya *key* dan plantext tersbut di konversi ke dalam angka dengan menggunakan tabel konversi huruf atau abjat ke angka, seperti pada gambar 4. Maka *key* K = A jadi 1, S jadi 19, L jadi 12 dan I jadi 9. Maka bujur sangkar yang terbentuk berdasarkan matriks ordo 2x2 adalah :

$$K = \begin{Bmatrix} 1 & 19 \\ 12 & 9 \end{Bmatrix}$$

Sedangkan untuk *plantext*nya hasil konversi huruf atau abjat ke dalam tabel konversi abjat atau huruf, adalah sebagai berikut : P-A jadi 16-1, S-S jadi 19-19, W-O jadi 23-15, R-D jadi 18-4, R-A jadi 18-1, dan S-I jadi 19-9. Maka *plantext* dalam penulisannya sebagai berikut :

$$P = \begin{Bmatrix} 16 \\ 1 \end{Bmatrix} \begin{Bmatrix} 19 \\ 19 \end{Bmatrix} \begin{Bmatrix} 23 \\ 15 \end{Bmatrix} \begin{Bmatrix} 18 \\ 4 \end{Bmatrix} \begin{Bmatrix} 18 \\ 1 \end{Bmatrix} \begin{Bmatrix} 19 \\ 9 \end{Bmatrix}$$

Berikutnya melakukan proses enkripsi dengan dengan rumus :

$$\boxed{e = K.P\ mod\ 26}$$

1. Enkripsi elemen **P A** dengan angka elemen **(16 1)**, adalah sebagai berikut :

$$e = \begin{Bmatrix} 1 & 19 \\ 12 & 9 \end{Bmatrix} (16\ \ 1)\ mod\ 26$$

$$= (16.1+1.19 \quad 16.12+1.9) \bmod 26$$

$$= (35 \quad 201) \bmod 26$$

$$= (35 \bmod 26 \quad 201 \bmod 26)$$

$$= (9 \quad 19) \rightarrow \text{I S}$$

Maka di dapat angka elemen **(2 23)** hasil enkripsi **P A**, adalah **I S**.

2. Enkripsi elemen **S S** dengan angka elemen **(19 19)**, adalah sebagai berikut :

$$e = \begin{Bmatrix} 1 & 19 \\ 12 & 9 \end{Bmatrix} (19\ \ 19)\ mod\ 26$$

$= (19.1 + 19.19 \quad 19.12 + 19.9) \text{ Mod } 26$

$= (380 \quad 399) \text{ mod } 26$

$= (380 \text{ mod } 26 \quad 399 \text{ mod } 26)$

$= (16 \quad 9) \rightarrow$ P I

Maka di dapat angka elemen **(16 9)** hasil enkripsi **S S**, adalah **P I**.

3. Enkripsi elemen **W O** dengan angka elemen **(23 15)**, adalah sebagai berikut :

$$e = \begin{Bmatrix} 1 & 19 \\ 12 & 9 \end{Bmatrix} (23 \quad 15) \; mod \; 26$$

$= (23.1 + 15.19 \quad 23.12 + 15.9) \text{ Mod } 26$

$= (308 \quad 411) \text{ mod } 26$

$= (308 \text{ mod } 26 \quad 411 \text{ mod } 26)$

$= (22 \quad 21) \rightarrow$ V U

Maka di dapat angka elemen **(22 21)** hasil enkripsi **W O**, adalah **V U**.

4. Enkripsi elemen **R D** dengan angka elemen **(18 4)**, adalah sebagai berikut :

$$e = \begin{Bmatrix} 1 & 19 \\ 12 & 9 \end{Bmatrix} (18 \quad 4) \; mod \; 26$$

$= (18.1 + 4.19 \quad 18.12 + 4.9) \text{ Mod } 26$

$= (94 \quad 252) \text{ mod } 26$

$= (94 \text{ mod } 26 \quad 252 \text{ mod } 26)$

$= (16 \quad 18) \rightarrow$ P R

Maka di dapat angka elemen **(16 18)** hasil enkripsi **R D**, adalah **P R**.

5. Enkripsi elemen **R A** dengan angka elemen **(18 1)**, adalah sebagai berikut :

$$e = \begin{Bmatrix} 1 & 19 \\ 12 & 9 \end{Bmatrix} (18 \quad 1) \; mod \; 26$$

$= (18.1 + 1.19 \quad 18.12 + 9.1) \text{ Mod } 26$

$= (37 \quad 255) \text{ mod } 26$

$= (37 \text{ mod } 26 \quad 255 \text{ mod } 26)$

$= (11 \quad 17) \rightarrow$ K Q

Maka di dapat angka elemen **(11 17)** hasil enkripsi **R A**, adalah **K Q**.

6. Enkripsi elemen **S I** dengan angka elemen **(19 9)**, adalah sebagai berikut :

$$e = \begin{Bmatrix} 1 & 19 \\ 12 & 9 \end{Bmatrix} (19 \quad 9) \; mod \; 26$$

$= (19.1 + 9.19 \quad 19.12 + 9.9) \text{ Mod } 26$

$= (190 \quad 309) \text{ mod } 26$

$= (190 \text{ mod } 26 \quad 309 \text{ mod } 26)$

$= (8 \quad 23) \rightarrow$ H W

Maka di dapat angka elemen **(8 23)** hasil enkripsi **S I**, adalah **H W**.

Hasil enkripsi secara menyeluruh dari teks yang disebut dengan *plantext* "PASSWORDRASI" dan *key* K yang digunakan "ASLI" menghasilkan proses enkripsi dengan teks atau yang disebut *chipertext* "ISPIVUPRKQHW".

B. Dekripsi

Di dalam proses dekripsi ini *key* K yang digunakan harus dirubah terlebih dahulu menjadi kebalikan dari *key* K menjadi invers K^{-1}. Untuk mencari K^{-1} adalah sebagai berikut :

$$K = \begin{Bmatrix} 1 & 19 \\ 12 & 9 \end{Bmatrix}$$

Untuk melakukan proses dekripsi pertama harus melakukan penghtiungan dengan rumus :

$$\boxed{1 = K.y.K^{-1} \; mod \; m}$$

$$1 = (1.9 - 19.12)y \; (1.9 - 19.12)^{-1} \begin{Bmatrix} 1 & -19 \\ -12 & 9 \end{Bmatrix} Mod \; 26$$

$$1 = (9 - 228)y \; (9 - 228)^{-1} \quad (1.9 - (-19).(-12)) \text{ Mod } 26$$

$$1 = (-219) \; y \; (-219)^{-1} \; (-219) \text{ Mod } 26$$

$$1 = (-219) \; y \text{ Mod } 26$$

$$1 = (-219) \; 7 \text{ Mod } 26$$

$$Jadi \; y = 7$$

Selanjutnya setelah mendapatkan nilai *y*, proses berikutnya adalah mencari elemen-elemen dari invers K.

$$K^{-1} = y \begin{Bmatrix} d & -b \\ -c & a \end{Bmatrix} \text{Mod m}$$

$$K^{-1} = 7 \begin{Bmatrix} 9 & -19 \\ -12 & 1 \end{Bmatrix} \text{Mod } 26$$

$$K^{-1} = 7 \begin{Bmatrix} 9 \text{ Mod } 26 & -19 \text{ Mod } 26 \\ -12 \text{ Mod } 26 & 1 \text{ Mod } 26 \end{Bmatrix} \text{Mod } 26$$

$$K^{-1} = 7 \begin{Bmatrix} 9 & 7 \\ 14 & 1 \end{Bmatrix} \text{Mod } 26$$

$$K^{-1} = \begin{Bmatrix} 7.9 \text{ Mod } 26 & 7.7 \text{ Mod } 26 \\ 7.14 \text{ Mod } 26 & 7.1 \text{ Mod } 26 \end{Bmatrix}$$

$$K^{-1} = \begin{Bmatrix} 63 \text{ Mod } 26 & 49 \text{ Mod } 26 \\ 98 \text{ Mod } 26 & 7 \text{ Mod } 26 \end{Bmatrix}$$

$$K^{-1} = \begin{Bmatrix} 11 & 23 \\ 20 & 7 \end{Bmatrix}$$

Setelah mencari invers *key* K^{-1}, proses dekripsi adalah merubah *chipertext* menjadi *plantext* dengan menggunakan

key K^{-1}. *Chipertext* hasil dari enkripsi adalah "ISPIVUPRKQHW", berikutnya akan di uji hasil *chipertext* tersebut akan menjadi teks apa dalam *plantext*. Konversikan teks "ISPIVUPRKQHW" ke dalam tabel konversi abjat ke angka, maka akan menghasilkan, sebagai berikut : I S jadi 9 19, P I jadi 16 9, V U jadi 22 21, P R jadi 16 18, K H jadi 11 8, H W jadi 8 23.

$$P = \begin{Bmatrix} 9 \\ 19 \end{Bmatrix} \begin{Bmatrix} 16 \\ 9 \end{Bmatrix} \begin{Bmatrix} 22 \\ 21 \end{Bmatrix} \begin{Bmatrix} 16 \\ 18 \end{Bmatrix} \begin{Bmatrix} 11 \\ 8 \end{Bmatrix} \begin{Bmatrix} 8 \\ 23 \end{Bmatrix}$$

Berikutnya melakukan proses enkripsi dengan dengan rumus :

$$\boxed{d = K^{-1}.C \ mod \ 26}$$

1. Enkripsi elemen **I S** dengan angka elemen **(9 19)**, adalah sebagai berikut :

$$d = \begin{Bmatrix} 11 & 23 \\ 20 & 7 \end{Bmatrix} (9 \ \ 19) \ mod \ 26$$
$$= (9.11 + 19.23 \ \ 9.20 + 19.7) \text{Mod } 26$$
$$= (99 + 437 \ \ 180 + 133) \text{ Mod } 26$$
$$= (536 \text{ Mod } 26 \ \ 313 \text{ Mod } 26)$$
$$= (16 \ \ 1) \rightarrow \text{P} \ \ \text{A}$$

Maka di dapat angka elemen **(16 1)** hasil dekripsi **I S**, adalah **P A**.

2. Enkripsi elemen **P I** dengan angka elemen **(16 9)**, adalah sebagai berikut :

$$d = \begin{Bmatrix} 11 & 23 \\ 20 & 7 \end{Bmatrix} (16 \ \ 9) \ mod \ 26$$
$$= (11.16 + 23.9 \ \ 20.16 + 7.9) \text{Mod } 26$$
$$= (176 + 207 \ \ 320 + 63) \text{ Mod } 26$$
$$= (383 \text{ Mod } 26 \ \ 383 \text{ Mod } 26)$$
$$= (19 \ \ 19) \rightarrow \text{S} \ \ \text{S}$$

Maka di dapat angka elemen **(19 19)** hasil dekripsi **P I**, adalah **SS**.

3. Enkripsi elemen **V U** dengan angka elemen **(22 21)**, adalah sebagai berikut :

$$d = \begin{Bmatrix} 11 & 23 \\ 20 & 7 \end{Bmatrix} (22 \ \ 21) \ mod \ 26$$
$$= (11.22 + 23.21 \ \ 20.20 + 7.21) \text{Mod } 26$$
$$= (242 + 483 \ \ 440 + 147) \text{ Mod } 26$$
$$= (725 \text{ Mod } 26 \ \ 587 \text{ Mod } 26)$$
$$= (23 \ \ 15) \rightarrow \text{W} \ \ \text{O}$$

Maka di dapat angka elemen **(23 15)** hasil dekripsi **V U**, adalah **WO**.

4. Enkripsi elemen **P R** dengan angka elemen **(16 18)**, adalah sebagai berikut :

$$d = \begin{Bmatrix} 11 & 23 \\ 20 & 7 \end{Bmatrix} (16 \ \ 18) \ mod \ 26$$
$$= (11.16 + 23.18 \ \ 20.16 + 7.18) \text{Mod } 26$$
$$= (176 + 414 \ \ 320 + 126) \text{ Mod } 26$$
$$= (590 \text{ Mod } 26 \ \ 446 \text{ Mod } 26)$$
$$= (18 \ \ 4) \rightarrow \text{R} \ \ \text{D}$$

Maka di dapat angka elemen **(18 4)** hasil dekripsi **P R**, adalah **RD**.

5. Enkripsi elemen **K Q** dengan angka elemen **(11 17)**, adalah sebagai berikut :

$$d = \begin{Bmatrix} 11 & 23 \\ 20 & 7 \end{Bmatrix} (11 \ \ 17) \ mod \ 26$$
$$= (11.11 + 23.17 \ \ 20.11 + 7.17) \text{Mod } 26$$
$$= (121 + 391 \ \ 220 + 119) \text{ Mod } 26$$
$$= (512 \text{ Mod } 26 \ \ 339 \text{ Mod } 26)$$
$$= (18 \ \ 1) \rightarrow \text{R} \ \ \text{A}$$

Maka di dapat angka elemen **(18 1)** hasil dekripsi **KQ**, adalah **RA**.

6. Enkripsi elemen **H W** dengan angka elemen **(8 23)**, adalah sebagai berikut :

$$d = \begin{Bmatrix} 11 & 23 \\ 20 & 7 \end{Bmatrix} (8 \ \ 23) \ mod \ 26$$
$$= (11.8 + 23.23 \ \ 20.8 + 7.23) \text{Mod } 26$$
$$= (88 + 529 \ \ 160 + 161) \text{ Mod } 26$$
$$= (617 \text{ Mod } 26 \ \ 321 \text{ Mod } 26)$$
$$= (19 \ \ 9) \rightarrow \text{S} \ \ \text{I}$$

Maka di dapat angka elemen **(19 9)** hasil dekripsi **HW**, adalah **SI**.

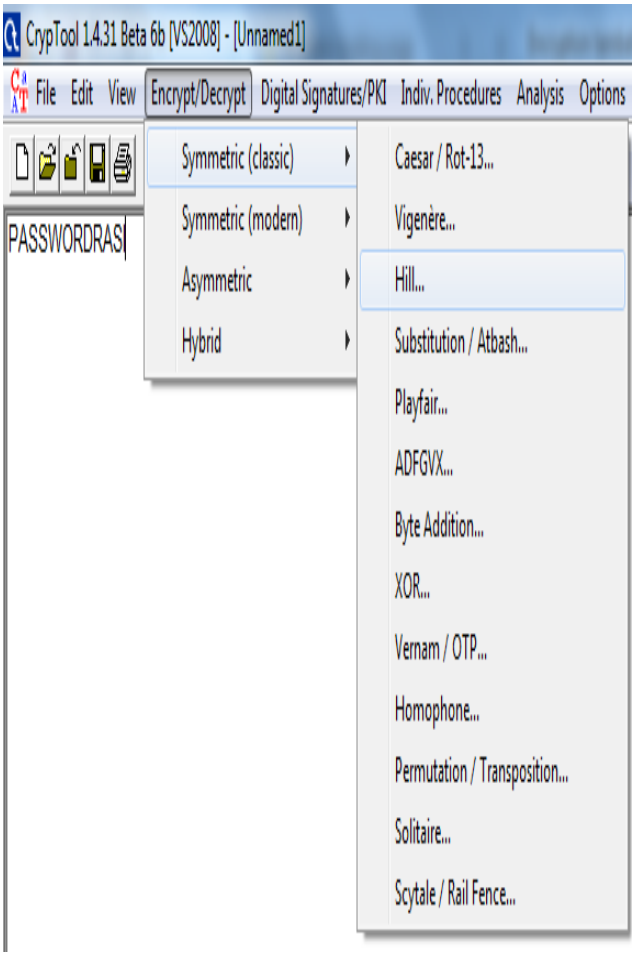
Hasil dekripsi secara menyeluruh dari teks yang disebut dengan *chipertext* "ISPIVUPRKQHW" dan *key* K yang telah mengalami proses invers K^{-1} proses dekripsi dengan teks atau yang disebut *plantext* "PASSWORDRASI".

C. Pengujian Hasil Enkripsi dan Dekripsi

1. Pengujian Enkripsi Cryptool

Setelah melakukan penghitungan secara manual menggunakan metode matriks sebuah teks atau kata yang dienkripsi, dengan *plantext*nya adalah : PASSWORDRASI menghasilkan *chipertext*nya adalah : ISPIVUPRKQHW. Selanjutnya akan diuji kebenaran hasil *chipertext*nya tersebut dengan program Cryptool.

a) Pesan atau kata yang ingin dienkripsi diinputkan pada lembar kerja Cryptool. Berikutnya pada menu Encrypt/Decrypt menuju Symetric (classic) lalu pilih chipper yang digunakan yaitu : hill.

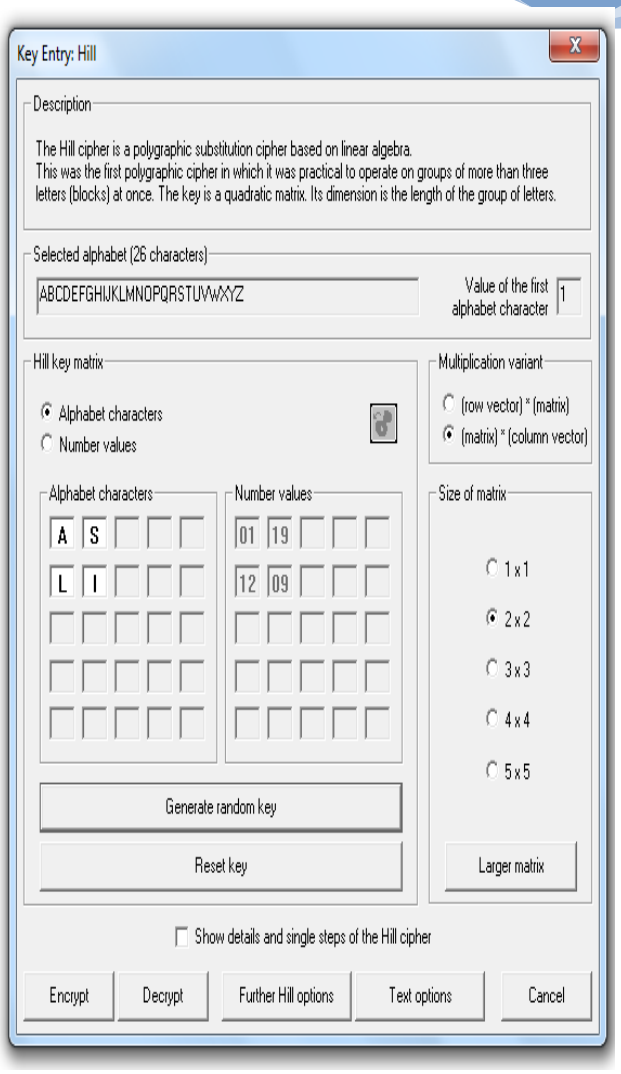


Sumber: Hasil Penelitian (2015)

Gambar 5 : Tampilan Tool Cryptools

b) Jendela Key Entry: Hill muncul, pada jendela ini, ada beberapa tahap yang dipilih antara lain, adalah :

1) Sesuai dengan penelitian pada pembuatan tabel abjat atau huruf "A – Z" dimulai dari angka 1 (satu) bukan 0 (null) maka :Pada jendela ini di Multiplication Variant pilih (matriks)*(coulomb vector). Maka value of the first alphabet carachter dengan nilai 1 (satu).
2) *Key* yang digunakan dalam penelitian ini dengan kata "ASLI", maka inputkan *key* tersebut di dalam Hill Key Matriks dengan Alphabet characters di checklist.
3) Matriks yang digunakan dalam penelitian ini adalah berordo 2x2 pilihlah dalam size of matriks.

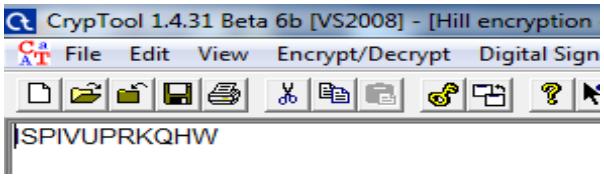


Sumber: Hasil Penelitian (2015)

Gambar 6 : Penginputan Key Cryptografi

c) .Untuk melihat hasil enkripsi dari *plantext* klik button Encrypt, dan akan muncul hasil enkripsi *plantext* "PASWORDRASI" yaitu *chipertext*nya adalah

d)



Sumber: Hasil Penelitian (2015)

Gambar 7 : Hasil Chipertext

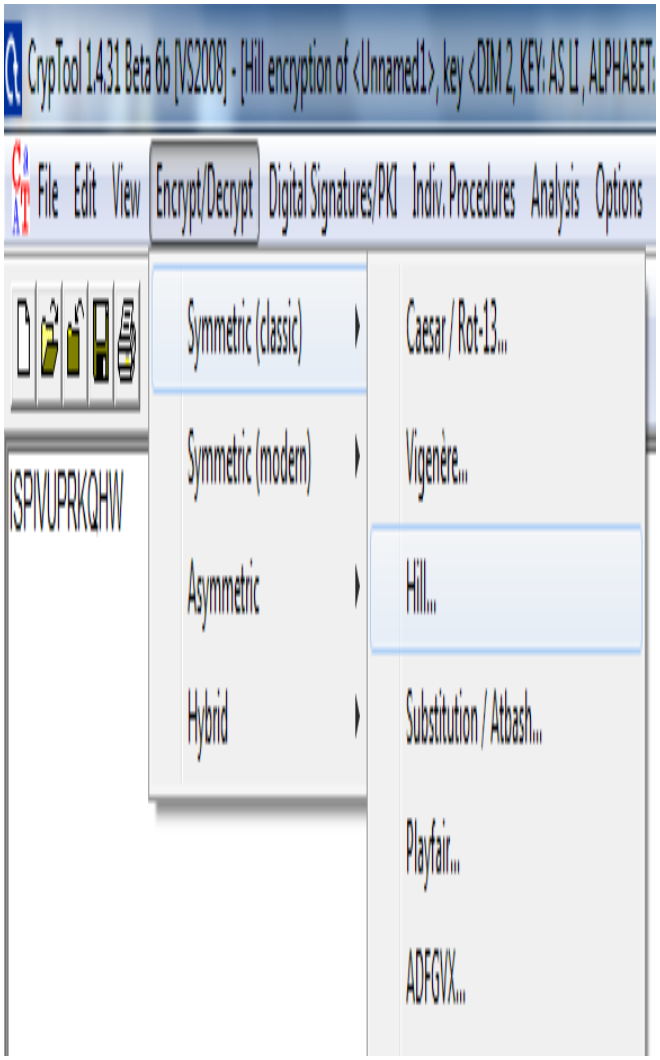
e) Dengan demikian *chipertext* yang dihasilkan dari penghitungan secara manual menggunakan metode matriks dengan program Cryptool sesuai yaitu *chipertext* yang dihasilkan adalah **ISPIVUPRKQHW**.

2. Pengujian Dekripsi Cryptool

Selanjutnya menguji kebenaran hasil *chipertext* di dekripsi ke *plantext* antara penghitungan secara manual

menggunakan metode matrikulasi dengan program Cryptool. Hasil yang didapatkan atau *plantext*nya dari "ISPIVUPRKQHW" adalah "PASSWORDRASI" dengan menggunakan Cryptool adalah sebagai berikut :

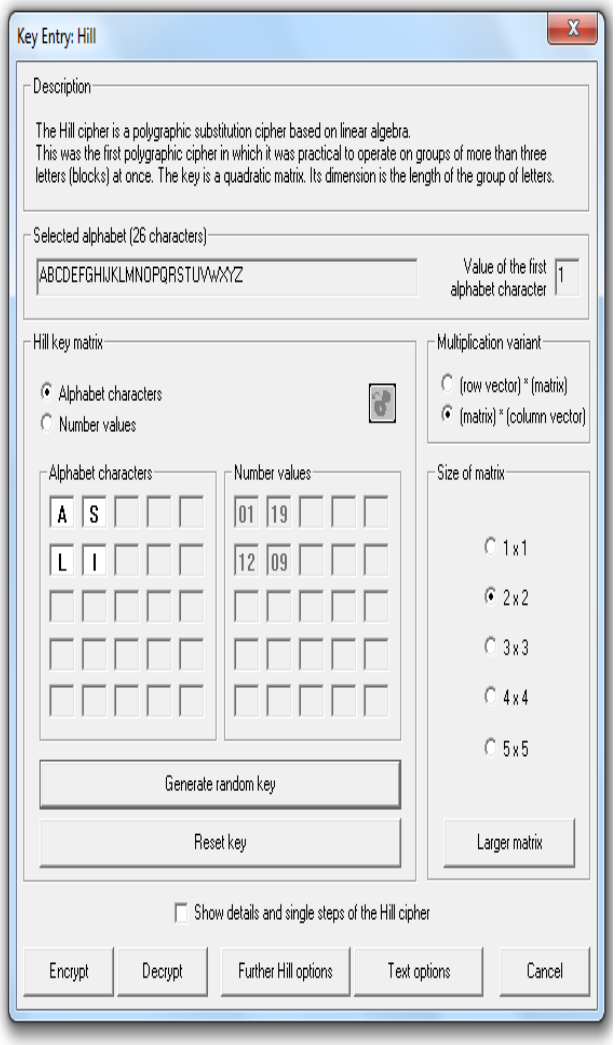
a) Pada *chipertext* hasil enkripsi yang ada pada lembar kerja Cryptool. Berikutnya pada menu Encrypt/Decrypt menuju Symetric (classic) lalu pilih chipper yang digunakan yaitu : hill.



Sumber: Hasil Penelitian (2015)

Gambar 8 : Encrypt/Decrypt pada Cryptool

b) Pada proses dekripsi Cryptool langkahnya sama dengan proses enkripsi, ini dikarenakan sesuai dengan dasar teori kriptografi dasar pada metode symetrik *key* yang digunakan untuk melakukan enkrip-dekrip menggunakan *key* yang sama, yaitu ASLI dan langkahnya sama dengan enkripsi.

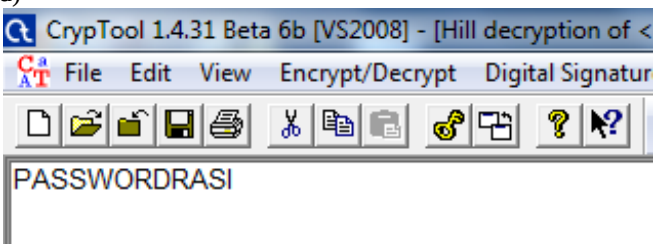


Sumber: Hasil Penelitian (2015)

Gambar 9 : Key yang digunakan Cryptool

c) Yang membedakan proses enkripsi-dekripsi pada Cryptool adalah langkah ini, yaitu dengan mengklik button dekrip maka *chipertext* akan diproses menjadi *plantext*, dan hasilnya adalah seperti gambar dibawah ini :

d)



Sumber: Hasil Penelitian (2015)

Gambar 10 : Hasil Decrypt pada Cryptool

e) Dengan demikian *plantext* yang dihasilkan dari penghitungan secara manual menggunakan metode matriks dengan program Cryptool sesuai yaitu *plantext* yang dihasilkan adalah **PASWORDRASI**.

V. KESIMPULAN

Berdasarkan hasil penelitian maka dapat disimpulkan sebagai berikut :

1. Kriptografi dengan algoritma chipper hill menggunakan metode matrikulasi.
2. Di dalam proses enkripsi-dekripsi pada algoritma chipper hill untuk mengkonversi pesan atau kata menggunakan tabel bantu abjat atau huruf dengan urutan angka.
3. Setelah melakukan proses penghitungan matrikulasi untuk mengkonversi hasil penjumlahan agar supaya masuk ke dalam range tabel abjat atau hurup ke dalam nilai angka menggunakan proses Modulus.
4. Pada proses dekripsi atau mengubah dari *chipertext* ke *plantext* menggunakan matrikulasi invers atau proses terbalik dari *key* yang digunakan.
5. Dengan system matriks berordo 2x2 akan memproses setiap 2 (dua) karakter dari *plantext* dirubah menjadi *chipertext*, begitu juga sebaliknya.

REFERENSI

[1] Anton, Howard and Chris Rores. Aljabar Linear Elementer versi Aplikasi. Erlangga : Jakarta. 2005.
[2] Ariyus, Doni. Pengantar Ilmu Kriptografi Teori dan Implementasi. Andi Offset : Yogyakarta. 2008.
[3] Bronson, Richard Ph.D dan Gabriel D. Costa Ph.D.. Persamaan Difrensial, Edisi Ketiga. Erlangga : Jakarta. 2007
[4] Chiang, Alpha C dan Kevin Wainwright. Dasar-dasar Matematika Ekonomi Edisi 4. Erlangga : Jakarta. 2005.
[5] Hartini dan Sri Primaini. Kriptografi Password Menggunakan Modifikasi Metode Affine Chipers. Jurnal SIGMATA Volume 2 : Nomor : 1 Edisi : Oktober 2013 – Maret 2014 ISSN 2303-5786. 2014.
[6] Juju, Dominikus dan MataMaya Studio. Teknik Menangkal Kejahatan Internet untuk Pemula. PT Elexmedia Komputindo : Jakarta. 2008.
[7] Klima, Richard. E, and Neil P. Sigmon. Cryptology Classical and Modern with Maplets Discrete Mathematics and Its Aplications. CRC Press : Florida. 2012.
[8] Laudon, Kenneth C. dan Jane P. Laudon. Sistem Informasi Manajemen, Edisi 10. Penerbit Salemba Empat : Jakarta. 2007.
[9] Pearson, Scott, Carl Gotsch, Sjaiful Bahri. Aplikasi Policy Analysis Matriks pada Pertanian Indonesia. Yayasan Obor Indonesia : Jakarta. 2005.
[10] Ranka, Sanjay el al. “Contemporary Computing” Proceedings Second International Conference, IC3 2009 Noida, India, August 2009. Springer : Berlin. 2009.
[11] Sanusi, Muzammil.. The Genius : Hacking Sang Pembobol Data. PT Elexmedia Komputindo : Jakarta. 2010
[12] Sasongko, Dr. Ir. Setia Budi. Metode Numerik dengan Scilab. Andi Offset : Yogyakarta. 2010.
[13] Solomon, David. Coding for Data and Komputer Communications. Springer Science and Business Media : New York. 2006.
[14] Komputer, Wahana. The Encryption Tools. PT Elexmedia Komputindo : Jakarta. 2010.

Aziz Setyawan. H, M.Kom. Tahun 2007 lulus dari Program Strata Satu (S1) Program Studi Teknik Informatika STMIK Nusa Mandiri Jakarta. Tahun 2012 lulus dari Program Strata Dua (S2) Program Studi Magister Ilmu Komputer STMIK Nusa Mandiri Jakarta. Tahun 2014 sudah memiliki Jabatan Fungsional Akademik dengan pangkat Asisten Ahli di AMIK BSI Jakarta pada Program Studi Teknik Komputer Jakarta. Aktif mengikuti seminar dan menulis paper di beberapa jurnal diantaranya Jurnal Widya Cipta AMIK BSI Jakarta dan Jurnal Paradigma AMIK BSI Jakarta