PEMECAHAN SANDI KRIPTOGRAFI DENGAN MENGGABUNGKAN METODE HILL CIPHER DAN METODE CAESAR CIPHER

Indria Eka Wardani

Jurusan Matematika, Universitas Islam Darul Ulum Lamongan
e-mail: arinds.0810@gmail.com

ABSTRAK

Pesan merupakan suatu pernyataan rahasia yang dibuat oleh pembuat pesan dan ditujukan kepada penerima pesan. Perkembangan teknologi yang modern mengakibatkan tingkat kerahasiaan suatu pesan tidak terjamin keamanannya. Apalagi akhir-akhir ini ulah haeker (pembobol keamanan) yang semakin mengkhawatirkan para pembuat pesan. Berdasarkan hal tersebut maka penulis akan mengkaji sandi kriptografi untuk menyampaikan pesan rahasia agar aman sampai pada penerima pesan. Dalam makalah ini pesan yang berbentuk sandi kriptografi digunakan untuk menggabungkan metode Hill Cipher dan Caesar Cipher. Pada pengoperasian enkripsi dan dekripsi sandi kriptografi, langkah-langkahnya yang digunakan adalah metode Caesar cipher, sedangkan dalam langkah-langkah tersebut menggunakan kunci dengan memakai metode Hill Cipher. Dalam pembuatan maupun penguraian sandi tersebut hanya pembuat pesan dan penerima pesan yang mengetahui bagaimana teknik pengoperasiannya. Dengan demikian diharapkan penyampaian pesan rahasia terjamin keamanannya.

Kata kunci: Sandi Kriptografi, metode Hill Cipher, Metode Caesar Cipher, penggabungan Metode Hill Cipher dan Metode Caesar Cipher .

ABSTRACT

Message is a privacy statement which is made by a person and addressed to another person with the consent of people who have made the message. But with the development of modern technology resulted in a high level of privacy for their safety message. Especially lately act haeker (security breaker) are increasingly rampant and alarming message makers. To address this, the authors will examine and discuss the cryptographic cipher to convey a secret message privacy. Message in the form of a password using cryptography in this paper Combining of Hill Cipher Method and Caesar Cipher Methods.In the operation process of encryption and decryption passwords cryptography, the steps using the Caesar CipherMethods, whereas in steps using keys by using Hill Cipher method. In the making and the first decoding the message makers and recipients know how the operation technique. Thus the expected delivery of message privacy secured.

Keywords: *Password Cryptography, methods of Hill Cipher, Caesar Cipher method,Combining of Hill Cipher Method and Caesar Cipher Method.*

PENDAHULUAN

Pesan merupakan pernyataan rahasia yang di buat oleh seseorang dan ditujukan kepada orang lain dengan seijin orang yang telah membuat pesan itu. Tetapi dengan perkembangan teknologi yang modern mengakibatkan tingkat kerahasiaan suatu pesan tidak terjamin keamanannya. Apalagi akhir-akhir ini ulah haeker (pembobol keamanan) yang semakin merajalela dan mengkhawatirkan para pembuat pesan. Maka diperlukan untuk mempelajari ilmu kriptografi yaitu ilmu penyandian terutama dikalangan militer maupun agen-agen rahasia dan yang lainnya mereka sudah tidak asing lagi dalam mempelajari ilmu kriptografi bahkan mereka sudah menggunakan alat-alat penyandian yang modern, sehingga mengkibatkan algoritma klasik menjadi terkesampingkan.

Sehubungan dengan itu maka masyarakat umum yang kurang mengetahui tentang ilmu kriptografi supaya dapat mempelajarinya juga, karena dalam setiap individu mempunyai hak dalam keamanan suatu pesan.Dan dengan algoritma klasik yang tidak terlalu sulit dalam mempelajarinya dapat dijadikan alternatif untuk keamanan suatu pesan. Maka penulis ingin memaduhkan bagian dari algoritma klasik yaitu metode Hill cipher dan metode Caesar cipher.

KRIPTOGRAFI

Kriptografi *(chrytography)* berasal dari bahasa yunani: *"chrytos"* artinya *"secret"* (rahasia),

sedangkan *"graphein"* artinya *"writing"* (tulisan). Jadi, Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (Munir,2006:2) Menezes, van Oorschot dan Vanstone (1997) menyatakan bahwa kriptografi adalah suatu studi teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi entitas dan otentikasi keaslian data. Kriptografi tidak hanya berarti penyandian keamanan informasi, melainkan sebuah himpunan teknik-teknik.

Jadi, secara umum dapat diartikan sebagai seni menulis atau memecahkan *cipher* (Talbot dan Welsh,2006). Didalam mempelajari ilmu kriptografi terdapat beberapa istilah atau termologi antara lain, pesan (*message*) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Keamanan pesan diperoleh dengan menyandikannya menjadi pesan yang tidak mempunyai makna. pesan yang dirahasiakan dinamakan **plainteks (***plainteks*, artinya teks jelas yang dapat dimengerti), sedangkan pesan hasil penyandian disebut **cipherteks** (*ciherteks*, artinya teks tersandi). Pesan yang telah disandikan dapat dikembalikan lagi kepesan aslinya hanya oleh orang yang berhak (orang yang berhak adalah orang yang mengetahui metode penyandian atau memiliki kunci penyandian). Proses menyandikan plainteks menjadi cipherteks disebut **enkripsi** (*encryption*) dan proses membalikkan cipherteks menjadi plainteksnya disebut **dekripsi** (*decryption)* (Rinaldi Munir,2005:203).

Dalam ilmu kriptografi terdapat pula algoritma-algoritma yang bisa dipelajari. Algoritma kriptografi atau sering juga disebut dengan *cipher* adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi (Schneier, 1996). Salah satunya yaitu algoritma simetri (menggunakan satu kunci untuk enkripsi dan dekripsinya) dan disebut juga algoritma klasik. Contoh dari algoritma simetri yaitu Caesar Cipher dan Hill Cipher.

HILL CIPHER

Hill cipher termasuk dalam salah satu kriptosistem polialfabetik, artinya setiap karakter alphabet bisa dipetakkan ke lebih dari satu macam karakter alphabet. Cipher ini ditemukan pada tahun 1929 oleh Laster S. Hill. Misalkan *m* adalah bilangan bulat positif, dan P = C = $(Z_{26})^m$ (Dony Ariyus, 2008:59).

Adapun menurut Widyanarko,2007. Hill Cipher merupakan algoritma kunci simetri yang menggunakan kunci yang sama pada proses enkripsi dan dekripsinya Hill Cipher merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi serta menggunakan *m* buah persamaan linier. Dalam penerapannya, Hill Cipher menggunakan teknik perkalian matriks dan teknik invers terhadap matriks.

Ide dari algoritma Hill Cipher adalah untuk membuat *m* kombinasi linier dari *m* karakter alfabetik didalam suatu elemen plainteks, sehingga dihasilkan *m* karakter alfabetik sebagai elemen dari cipherteks.

Secara umum jika A adalah matriks *mxm* atas Z_{26} dan $x = (x_1 \ldots . x_n)^T \epsilon P$ sehingga dihitung $y = e_A(x) = (y_1 \ldots . y_m)^T \epsilon C$ sebagai berikut:

$$\begin{bmatrix} y_1 \\ \ldots \\ y_n \end{bmatrix} = \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mm} \end{bmatrix} \begin{bmatrix} x_1 \\ \ldots \\ x_m \end{bmatrix}$$

sehingga dapat ditulis $y = Ax$. Fungsi dekripsinya diturunkan dari formula di atas, karena $y = Ax$ jika A^{-1} ada maka $x = A^{-1}y$.

CAESAR CIPHER

Subtitusi cipher yang pertama dalam dunia penyandian pada waktu pemerintahan Yulius Caesar yang dikenal dengan Caesar Cipher, dengan mengganti posisi huruf awal dari alphabet. (Donny Arius,2006:17). Pada buku edisi ke dua mengatakan dengan mengganti posisi huruf awal dari alphabet atau disebut juga dengan algoritma ROT3.

Caesar Cipher (ROT3)

Plain Text	Encoded Text
ABC	DEF
Hello	Khoor
Attack	Dwwdfn

yang artinya mengganti (menggeser) tiap-tiap huruf dalam alphabet sebanyak tiga huruf kedepan sehingga A, B, C menjadi D, E, F dan 0, 1, 2 menjadi 3, 4, 5.

Pada algoritma Caesar cipher untuk plainteksnya diberikan simbol "P", cipherteksnya simbolnya "C" dan kunci diberikan symbol "K". Rumus yang digunakan adalah:

C = f(P) = (P + K) mod (26)

Untuk proses enkripsinya sedangkan untuk proses dekripsinya menggunakan rumus:

P = f(C) = (C - K) mod (26)

Metode caesar cipher dapat dipecahkan dengan cara*brute force attact*, suatu bentuk serangan yang dilakukan dengan mencoba-coba berbagai kemungkinan untuk menemukan kunci. Karena jumlah kunci sangat sedikit (hanya ada 26 kunci) meskipun membutuhkan waktu yang cukup lama.

PENGGABUNGAN METODE HILL CIPHER DAN METODA CAESAR CIPHER.

Merujuk pada metode Caesar cipher dan Hill cipher maka penulis ingin membuat penerapan dari kedua metode tersebut. Sesuai metode Caesar cipher dan Hill cipher yang menggunakan Z_{26} maka disini penulis ingin memberikan Z_{30} dengan modulo 30. Yaitu dengan menambahkan titik (.), koma (,), tanda Tanya (?), dan tanda seru (!). karena dalam penulisan suatu pesan mengandung banyak maksud dan tujuan sehingga supaya pesan yang dikirimkan mengandung maksud serta tujuan yang jelas maka dipergunakan tanda-tanda tersebut.

Pada proses enkripsi dan dekripsi penulis menggabungkan kedua metode Caesar cipher dan Hill cipher yaitu untuk proses pengoperasian enkripsi menggunkan metode Caesar cipher terlebih dahulu yaitu dengan menggunakan persamaan sebagai berikut.

$$C = f(P) = (P+K) \bmod (30)$$

Setelah itu dilanjut dengan menggunakan metode Hill cipher yaitu dengan menggunakan matriks *K* sebagai kuncinya, rumusnya adalah $\boldsymbol{C = K.P}$

sedangkan untuk proses dekripsinya sama seperti proses enkripsi tetapi terlebih dahulu menggunakan metode Hill Cipher dimana matriks K harus di inverskan selanjutnya $K.K^{-1} = I$ yaitu menghasilkan matriks identitas, rumus Hill cipher pada proses dekripsi adalah $\boldsymbol{P = K^{-1}.C}$

Selanjutnya tahap berikutnya dengan menggunakan metode Caesar cipher yaitu.

$$P = f(C) = (C-K) \bmod (30)$$

Dalam persamaan tersebut terdapat $\boldsymbol{P}$ yaitu Plainteks (pesan asli), $\boldsymbol{C}$ yaitu Cipherteks (pesan yang tersandi) dan $\boldsymbol{K}$ yaitu kuncinya. Disini matriks yang digunakan yaitu matriks persegi berordo n x n dan dengan entri-entrinya bilangan bulat. Untuk lebih jelasnya maka berikut ini merupakan langkah-langkah proses enkripsi dan dekripsi.

Sebelum menginjak pada proses enkripsi dan dekripsi hal yang harus dilakukan yaitu membuat tabel korespondensi satu-satu dengan mengkonversikan setiap huruf alphabet ke dalam bilangan bulat.

Tabel 1. Korespondensi satu-satu

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z	.	,	?	!
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

PROSES ENKRIPSI

Pada proses enkripsi ini langkah-langkah yang ditempuh hampir sama dengan langkah-langkah proses enkripsi pada metode Caesar cipher dan Hill cipher. Disini penulis menggeser sebanyak tiga huruf kedepan dan menggunakan matriks berordo 2 x 2 dan 3 x 3 sebagai kuncinya. Berikut ini merupakan langkah-langkah proses enkripsi.

1. Konversikan tiap-tiap huruf alphabet kedalam sebuah bilangan 0 sampai 30 karakter. Kemudian geser tiga huruf kedepan. Sehingga persamaannya menjadi $\boldsymbol{C = f(P) = (P+3) \bmod (30)}$
2. Membuat teks aslinya (plainteks) kemudian konversikan kedalam bilangan bulat dengan melihat tabel 1 koresponden satu-satu. Selanjutnya masukkan ke persamaannya.
3. Setelah diperoleh cipherteks dari metode Caesar cipher selanjutnya dengan metode Hill cipher dimana persamaannya yaitu $\boldsymbol{C = K.P}$.
4. Memilih matriks 2 x 2 atau 3 x 3 dengan elemen-elemennya bilangan bulat untuk melakukan penyandian dengan syarat *K* punya invers.
   Karena matriks kunci *K* berukuran 2 x 2, maka plainteks dibagi menjadi blok yang msing-masing bloknya berukuran *K2* karakter. Kemudian dienkripsi dengan kunci *K* dengan persamaan $C = K \,.\, P \bmod 30$ .Jika perkalian tersebut menghasilkan lebih dari angka 29 maka dilakukan modulo 30 pada hasil yang lebih dari 29.
   $$K = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$
5. Mengkonversikan masing-masing pesan yang sudah diurutkan P_1, P_2 ke vektor kolom $P = \begin{bmatrix} p^1 \\ p^2 \end{bmatrix}$ dan bentuk perkalian *KP*, dengan *P* sebagai vektor teks biasa dan *KP* disebut vektor teks yang sudah tersandikan
6. Mengganti sisa modulo 30 pada masing-masing elemen matriks dengan huruf alphabet sesuai dengan tabel korespondensi satu-satu.

Dari ilustrasi tersebut maka penulis akan memberikan contoh yaitu:

Contoh: Pesan yang akan disampaikan yaitu:

BELAJAR YANG RAJIN

Langkah-langkah enkripsinya adalah sebagai berikut:

1. Konversikan tiap-tiap huruf alphabet ke dalam sebuah bilangan 0 sampai 30 karakter. Dengan melihat tabel korespondensi satu-satu.

BELAJAR YANG RAJIN

Hasil konversiannya adalah:

1 4 11 0 9 0 17 24 0 13 6 17 0 9 8 13

2. Selanjutnya masukkan ke persamaan ***C =f(P) = (P+3) mod (30)*** sehingga menghasilkan:

4 7 14 312 3 20 27 3 169 203 12 11 16

Menggunakan proses Hill cipher

3. Disini penulis memilih matriks 2 x 2 sebagai kuncinya, dengan elemen-elemennya bilangan bulat dan mempunyai invers. Yaitu matriks $K = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}$
4. Kelompokkan masing-masing bilangan secara berpasangan

4 7 14 3 12 3 20 27 3 16 9 17 3 12 11 16

5 Kemudian pesan teks tersebut dimasukkan kedalam vektor kolom.

$P_1 = \begin{bmatrix} 4 \\ 7 \end{bmatrix}$, $P_2 = \begin{bmatrix} 14 \\ 3 \end{bmatrix}$, $P_3 = \begin{bmatrix} 12 \\ 3 \end{bmatrix}$, $P_4 = \begin{bmatrix} 20 \\ 27 \end{bmatrix}$, $P_5 = \begin{bmatrix} 3 \\ 16 \end{bmatrix}$, $P_6 = \begin{bmatrix} 9 \\ 20 \end{bmatrix}$, $P_7 = \begin{bmatrix} 3 \\ 12 \end{bmatrix}$, $P_8 = \begin{bmatrix} 11 \\ 16 \end{bmatrix}$,

Selanjutnya kalikan matriks K dengan vektor kolom *(P)*.

$$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}\begin{bmatrix} 4 \\ 7 \end{bmatrix} = \begin{bmatrix} 8+21 \\ 12+35 \end{bmatrix} = \begin{bmatrix} 29 \\ 47 \end{bmatrix} = \begin{bmatrix} 29 \\ 17 \end{bmatrix} mod\ 30 = \begin{bmatrix} ! \\ R \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}\begin{bmatrix} 14 \\ 3 \end{bmatrix} = \begin{bmatrix} 28+9 \\ 42+15 \end{bmatrix} = \begin{bmatrix} 37 \\ 57 \end{bmatrix} = \begin{bmatrix} 7 \\ 27 \end{bmatrix} mod\ 30 = \begin{bmatrix} H \\ , \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}\begin{bmatrix} 12 \\ 3 \end{bmatrix} = \begin{bmatrix} 24+9 \\ 36+15 \end{bmatrix} = \begin{bmatrix} 33 \\ 51 \end{bmatrix} = \begin{bmatrix} 3 \\ 21 \end{bmatrix} mod\ 30 = \begin{bmatrix} D \\ V \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}\begin{bmatrix} 20 \\ 27 \end{bmatrix} = \begin{bmatrix} 40+81 \\ 60+135 \end{bmatrix} = \begin{bmatrix} 121 \\ 195 \end{bmatrix} = \begin{bmatrix} 1 \\ 15 \end{bmatrix} mod\ 30 = \begin{bmatrix} B \\ P \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}\begin{bmatrix} 3 \\ 16 \end{bmatrix} = \begin{bmatrix} 6+48 \\ 9+80 \end{bmatrix} = \begin{bmatrix} 54 \\ 89 \end{bmatrix} = \begin{bmatrix} 24 \\ 29 \end{bmatrix} mod\ 30 = \begin{bmatrix} Y \\ ! \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}\begin{bmatrix} 9 \\ 20 \end{bmatrix} = \begin{bmatrix} 18+60 \\ 27+100 \end{bmatrix} = \begin{bmatrix} 78 \\ 127 \end{bmatrix} = \begin{bmatrix} 18 \\ 7 \end{bmatrix} mod\ 30 = \begin{bmatrix} S \\ H \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}\begin{bmatrix} 3 \\ 12 \end{bmatrix} = \begin{bmatrix} 6+36 \\ 9+60 \end{bmatrix} = \begin{bmatrix} 42 \\ 69 \end{bmatrix} = \begin{bmatrix} 12 \\ 9 \end{bmatrix} mod\ 30 = \begin{bmatrix} M \\ J \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}\begin{bmatrix} 11 \\ 16 \end{bmatrix} = \begin{bmatrix} 22+48 \\ 33+80 \end{bmatrix} = \begin{bmatrix} 70 \\ 113 \end{bmatrix} = \begin{bmatrix} 10 \\ 23 \end{bmatrix} mod\ 30 = \begin{bmatrix} K \\ X \end{bmatrix}$$

6 Setelah itu konversikan tiap-tiap hasil penyandian terhadap tabel koresponden satu-satu dan diperoleh:

!R H, DV BP Y ! SH MJ KX

PROSES DEKRIPSI

Pada proses dekripsi yaitu dengan menggunakan metode Hill cipher dan dilanjut dengan metode Caesar cipher dimana pada pengoperasian Hill cipher menggunakan invers dari matriks *K*, dengan persamaan sebagai berikut

$$P = K^{-1}.C$$

Sdangkan untuk Caesar cipher pengorerasiannya menggunakan persamaan:

$$P = f(C) = (C-K)\ mod\ (30)$$

Disini penulis akan menjabarkan beberapa langkah-langkah proses dekripsi

1. Mencari invers matriks dari matriks K yang sudah ditetapkan yaitu menggunakan matriks berordo 2 x 2 atau 3 x 3.
   Untuk matriks A = ($a_{i,j}$) berukuran 2 x 2, nilai determinannya adalah:
   Det A = $a_{1,1}\ a_{2,2} - a_{1,2}\ a_{2,1}$
   Dan matriks invers dari A adalah:
   $A^{-1} = (\det A)^{-1}\begin{bmatrix} a_{2,2} & -a_{1,2} \\ -a_{2,1} & a_{1,1} \end{bmatrix}$
   (Dony Ariyus,2006:30)
2. Pesan yang sudah tersandi kemudian dikelompokkan secara berurutan kedalam pasangan-pasangan dan menggantinya dengan bilangan bulat.
3. Mengkonversikan masing-masing pesan tersandi yang sudah diurutkan C_1, C_2 ke vektor kolom $C = \begin{bmatrix} c^1 \\ c^2 \end{bmatrix}$ dan bentuk perkalian $K^{-1}\ C=P$, dengan C sebagai vektor teks yang sudah tersandi dan K^{-1}Cdisebut vektor teks aslinya.
4. Selanjutnya hasil dari perkalian tersebut masukkan dalam persamaan Caesar Cipher yaitu ***P= f(C) = (C-K) mod (30)***
5. Mengganti sisa modulo 30 pada masing-masing hasil persamaan Caesar Cipher dengan huruf alphabet sesuai dengan tabel korespondensi satu-satu

Selanjutnya penulis akan memberikan contoh sebagai berikut:

Contoh: pesan berikut merupakan pesan yang sudah tersandi

!R H, DV BP Y ! SH MJ KX

Langkah-langkah enkripsinya adalah sebagai berikut:

1. Disini penulis menggunakan matriks berordo 2 x 2, Yaitu matriks $K = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}$
   Sedangkan K^{-1} adalah $K^{-1} = \begin{bmatrix} 5 & -3 \\ -3 & 2 \end{bmatrix}$

2. Kelompokkan huruf alphabet secara berpasangan.
   !R H, DV BP Y ! JW MJ KX

   Kemudian konversikan kedalam bilangan bulat sesuai dengan tabel korespondensi satu-satu.

29 17 7 27 3 21 1 15 2429187 1291023

3. Kemudian pesan teks tersebut dimasukkan ke dalam vektor kolom.
   $P_1 = \begin{bmatrix}29\\17\end{bmatrix}$, $P_2 = \begin{bmatrix}7\\27\end{bmatrix}$, $P_3 = \begin{bmatrix}3\\21\end{bmatrix}$, $P_4 = \begin{bmatrix}1\\15\end{bmatrix}$, $P_5 = \begin{bmatrix}24\\29\end{bmatrix}$, $P_6 = \begin{bmatrix}9\\22\end{bmatrix}$, $P_7 = \begin{bmatrix}12\\9\end{bmatrix}$, $P_8 = \begin{bmatrix}10\\23\end{bmatrix}$
   Selanjutnya kalikan matriks *K* dengan vektor kolom *(P)*.

$$\begin{bmatrix}5 & -3\\-3 & 2\end{bmatrix}\begin{bmatrix}29\\17\end{bmatrix} = \begin{bmatrix}145-51\\-87+34\end{bmatrix} = \begin{bmatrix}94\\-53\end{bmatrix} = \begin{bmatrix}4\\7\end{bmatrix} mod\ 30$$

$$\begin{bmatrix}5 & -3\\-3 & 2\end{bmatrix}\begin{bmatrix}7\\27\end{bmatrix} = \begin{bmatrix}35-81\\-21+54\end{bmatrix} = \begin{bmatrix}-46\\33\end{bmatrix} = \begin{bmatrix}14\\3\end{bmatrix} mod\ 30$$

$$\begin{bmatrix}5 & -3\\-3 & 2\end{bmatrix}\begin{bmatrix}3\\21\end{bmatrix} = \begin{bmatrix}15-63\\-9+42\end{bmatrix} = \begin{bmatrix}-48\\33\end{bmatrix} = \begin{bmatrix}12\\3\end{bmatrix} mod\ 30$$

$$\begin{bmatrix}5 & -3\\-3 & 2\end{bmatrix}\begin{bmatrix}1\\15\end{bmatrix} = \begin{bmatrix}5-45\\-3+30\end{bmatrix} = \begin{bmatrix}-40\\27\end{bmatrix} = \begin{bmatrix}20\\27\end{bmatrix} mod\ 30$$

$$\begin{bmatrix}5 & -3\\-3 & 2\end{bmatrix}\begin{bmatrix}24\\29\end{bmatrix} = \begin{bmatrix}120-87\\-72+58\end{bmatrix} = \begin{bmatrix}33\\-14\end{bmatrix} = \begin{bmatrix}3\\16\end{bmatrix} mod\ 30$$

$$\begin{bmatrix}5 & -3\\-3 & 2\end{bmatrix}\begin{bmatrix}18\\7\end{bmatrix} = \begin{bmatrix}90-21\\-54+14\end{bmatrix} = \begin{bmatrix}69\\-40\end{bmatrix} = \begin{bmatrix}9\\20\end{bmatrix} mod\ 30$$

$$\begin{bmatrix}5 & -3\\-3 & 2\end{bmatrix}\begin{bmatrix}12\\9\end{bmatrix} = \begin{bmatrix}60-27\\-36+18\end{bmatrix} = \begin{bmatrix}33\\-18\end{bmatrix} = \begin{bmatrix}3\\12\end{bmatrix} mod\ 30$$

$$\begin{bmatrix}5 & -3\\-3 & 2\end{bmatrix}\begin{bmatrix}10\\23\end{bmatrix} = \begin{bmatrix}50-69\\-30+46\end{bmatrix} = \begin{bmatrix}-19\\16\end{bmatrix} = \begin{bmatrix}11\\16\end{bmatrix} mod\ 30$$

4. Hasilnya adalah:
   47 14 3 12 3 20 27 3 16 9 20 3 12 11 16
   Selanjutnya hasil dari perkalian tersebut masukkan dalam persamaan
   P= f(C) = (C-3) mod (30) sehingga menjadi
   1 4 11 0 90 17 24 0 136 17 0 98 13
5. Mengganti sisa modulo 30 pada masing-masing hasil persamaan Caesar Cipher dengan huruf alphabet sesuai dengan tabel korespondensi satu-satu

BE LA JA RY AN GR AJ IN

Sehingga diperoleh pesan asli (plainteks) adalah ***BELAJAR YANG RAJIN***

DAFTAR PUSTAKA

[1] Dony, Ariyus. 2006 . ***Kriptografi Keamanan Data Komunikasi***. Edisi Pertama. Yogyakarta: Graha Ilmu

[2] Dony,Ariyus. 2008 . ***Pengantar Ilmu Kriptografi***. Edisi Dua. Yogyakarta: C.V Andi Offset

[3] Rinaldi, Munir. 2005. ***Matematika Diskrit***. Bandung: Informatika