Jurnal Gammath, Volume 3 Nomor 1, Maret 2018

PROTOKOL PERJANJIAN KUNCI STICKEL ATAS GRUPOID NON KOMUTATIF DAN PERUBAHANPEMBOBOTANHURUF

Aswar Anas
FPMIPA IKIP PGRI Jember
anas939@gmail.com

Abstrak

Pengiriman pesan lewat jaringan komunikasi global sangat rawan disadap oleh musuh. Faktor keamanan pengiriman pesan menjadi aspek yang penting ditengah-tengah kemajuan teknologi sekarang ini. Chiperteks adalah pesan yang dikirim seseorang setelah melalui enkripsi dan di terjemahkan atau dideskripsi menjadi Plainteks. Chiper Vigenere salah satunya. Namun kelemahan Chper Vigenere terletak pada kunci yang diberikan. Jika kunci tersebut terlalu mudah, maka dengan kemajuan teknologi sekarang kunci tersebut dapat dibaca dengan cepat. Protokol perjanjian stikel merupakan kunci yang menggunakan grup non komutatif *G*. Protokol ini mempublikasikan tiga elemen dari grup *a,b,* dan *g*. para pengirim dan penerima pesan akan saling menerima *u* dan *v*, yang merupakan hasil perkalian *a,b,g* yang *a* dan *b* dipangkatkan bilangan asli tertentu yang dipilih secara acak. Akan tetapi processor yang semakin cepat dan algoritma pemecah kode sudah banyak ditemukan dikhawatirkan akan mempercepat musuh mendapatkan informasi. Hal ini dapat diatasi dengan pembobotan huruf yang di bedakan dengan pemecahan graf. graf yang dikirimkan dapat disamarkan berupa gambar jalan, bentuk pohon atau yang lain yang berisikan informasi pembobotan huruf. Jika hal ini dilakukan, maka ada 26! kemungkinan yang terjadi. Dengan demikian tujuan untuk mempersulit musuh mendapatkan pesan tercapai.

Kata Kunci: Stickel, Graf, Matriks.

Abstract

A Sending a message from a global communication network is very disturbed by an enemy. Safety of sending a message is an important aspect between of technology development. Chypertext is a message from someone after encrytion process and tranlseted to plainteks. Chiper vigenere is on of them. But the weakness of this Chiper is from sharing secret key. If key is too easy, then with newest technology, the sharing secret key can be translated fastly. Stikel Agreement Protocol is a key based from non commutative group *G*. This Protocol plubishing *a, b,* and *g* element of *G*. The Sender and Receiver a message will be accepted *u* and *v*. *u* and *v* is from multiplication of *a*, *b*, and *g* with *a* and *b* has exponentated with any natural number random. However,now, the processor is very fast and a lot of reading code algorithm is funded, worried that enemy can get the information. But this problem can be solved by giving a different number of alpabhet by graf solve problem. The sending graf can be given by addressing road or tree's model. If this doing, then 26! Probability can be happened on giving a number of alphabet. Then difficulty of enemy to read a messege has been get.

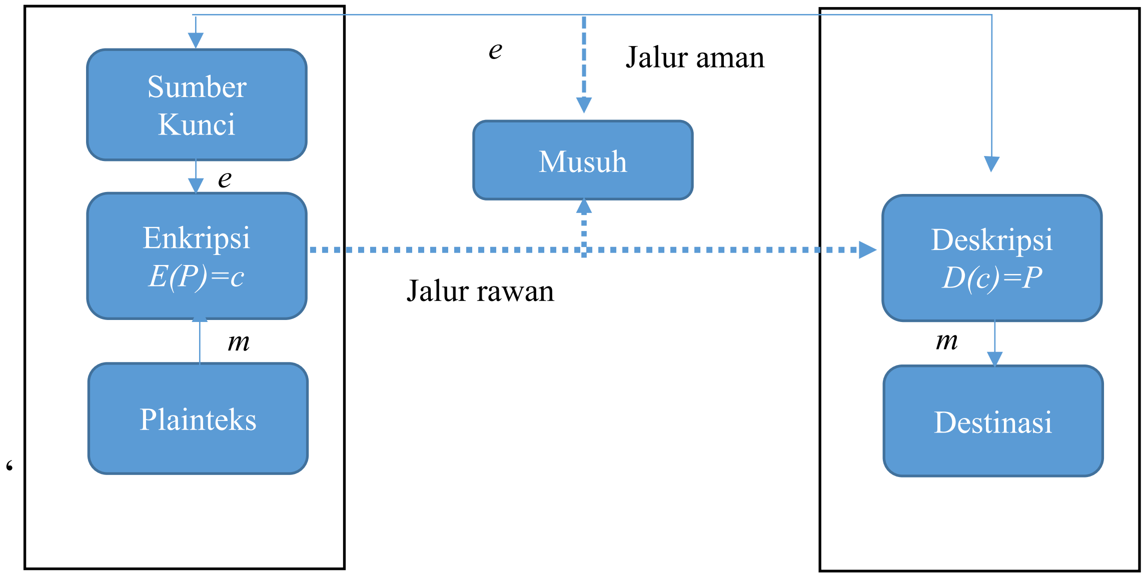
Keywords: Stickel, Graf, Matrix

PENDAHULUAN

Perkembangan teknologi pada saat ini telah memasuki aspek-aspek kehidupan manusia, salah satunya dalam kemajuan komunikasi. Komunikasi sekarang dapat dilakukan secara cepat, luas dan murah, yang dulu hanya bisa dilakukan dengan komunikasi kabel sekarang sudah menggunakan jaringan internet. Namun jaringan internet memiliki kelemahan. Kelemahan tersebut dikarenakan jaringan internet merupakan jalur komunikasi umum yang sewaktu-waktu dapat disadap dan disalahgunakan. Sehingga keamanan komunikasi menjadi faktor utama yang penting.

Solusi untuk mengatasi hal tersebut adalah kriptografi. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika dan berhubungan dengan aspek-aspek ekeamanan informasi seperti kerahasiaan, integritas, entitas dan autensifikasi keaslian data [3].Kriptografi dapat dikatakan sebagai suatu cara untuk menjaga kerahasiaan pesan dari pengirim dan penerima dari pihak-pihak yang tidak berhak mengetahuinya. Untuk menjaga kerahasiaan suatu pesan, maka pesan tersebut diubah menjadi kode-kode yang susah dimengerti pihak lain. Pada tahap pertama, pengirim pesan akan mengubah teks, proses mengubah pesan menjadi kode disebut dengan Enkripsi. Kemudian teks yang telah ter-enkripsi atau yang disebut dengan plainteks dikirim menuju penerima teks. Setelah diterima oleh penerima teks, plainteks akan di Deskripsi menjadi teks yang asli. Tentu saja dibutuhkan kunci untuk menerjemahkan teks tersebut.

Sistem pengubahan pesan atau informasi dari enkripsi dan deskripsi disebut dengan Chiper. Namun ada kelemahan dari proses pengiriman kunci kepada penerima Chiperteks. Yaitu kedua pihak harus mengetahui kunci yang diberikan dan disepakati. Bila kunci terlalu mudah diterjemahkan oleh pihak yang tidak bertanggung jawab, maka pesan atau informasi sangat mudah bocor. Proses tersebut dapat digambarkan berikut ini.



Gambar 1. Komunikasi satu arah dengan menggunakan enskripsi dengan kunci enkripsi simetris

Gambar 1 di atas menjelaskan ada dua pihak yang sedang melakukan komunikasi yaitu yaitu Alice dan Bob. Komunikasi ini bersifat rahasia dan menggunakan kunci enkripsi simetris. Namun komunikasi tersebut melalui jalur yang tidak aman atau rawan. Sehingga dua belah pihak harus menggunakan kunci rahasia yang disetujui dua pihak. Namun, pihak musuh berada diantara dua belah pihak tersebut dan berusaha untuk mendapatkan pesan yang dikirim pengirim. Ada beberapa macam sistem kriptografi menurut [2] yaitu *block chipers, stream chipers, affine chpers, affine linear block chipers, vigenere chipers, hill chipers.* Dalam penelitian ini hanya menggunakan Chiper Vigenere dengan perjanjian kunci*Stikel.*

Berdasarkan [2] Chiper vigenere merupakan sistem kriptografi simetris dengan kunci $K = \square_{\dots}$ dengan K adalah vektor atau matriks dan deskripsi teks menggunakan penjumlahan vektor atau matriks. Jika $\vec{k} \in \square_{\dots}$ maka

$$E_{\vec{k}} \; \square_{\dots} \qquad \square_{\dots} \; \vec{} \mapsto \vec{} \quad \vec{} \qquad \vec{v} \bmod m$$

Dan

$$D_{\vec{k}} \; \square_{\dots} \qquad \square_{\dots} \; \vec{} \mapsto \vec{} \quad \vec{} \qquad \vec{v} \bmod m$$

Dan dalam matriks menurut [5] Jika jika R adalah ring komutatif hingga dan $R \neq \{0\}$, didefinisikan himpunan semua matriks $n \times n$ atas ring R dengan

$$M_{n\times n}(R) = \left\{ \left(\begin{matrix} a_{11} & a_{12} & \cdots & \\ a_{21} & a_{22} & \cdots & \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \cdots & \end{matrix} \right) \Bigg| \; a \;\; \in R, 1 \leq i, j \leq n \right\}$$

Diberikan plainteks P dan kunci K dengan bentuk:

$P = \begin{pmatrix} p_{11} & \cdots & \\ \vdots & \ddots & \vdots \\ p_{i1} & \cdots & \end{pmatrix}$ dan kunci $K = \begin{pmatrix} k_{11} & \cdots & \\ \vdots & \ddots & \vdots \\ k_{i1} & \cdots & \end{pmatrix}$. selanjutnya dilakukan proses enkripsi metode Vigenere dengan

$e_K(P) = P + K = \begin{pmatrix} p_{11} & \cdots & \\ \vdots & \ddots & \vdots \\ p_{i1} & \cdots & \end{pmatrix} \begin{pmatrix} & \cdots & \\ \vdots & \ddots & \vdots \\ & \cdots & \end{pmatrix} \begin{pmatrix} & \cdots & \\ \vdots & \ddots & \vdots \\ & \cdots & \end{pmatrix}$, C merupakan chiperteks. Selanjutnya dilakukan proses deskripsi pesan yang telah diterima yaitu,

$d_K(C) = C - K = \begin{pmatrix} c_{11} & \cdots & \\ \vdots & \ddots & \vdots \\ c_{i1} & \cdots & \end{pmatrix} \begin{pmatrix} & \cdots & \\ \vdots & \ddots & \vdots \\ & \cdots & \end{pmatrix} \begin{pmatrix} & \cdots & \\ \vdots & \ddots & \vdots \\ & \cdots & \end{pmatrix}$. Perhitungan matriks diatas merupakan gambaran tentang pesan yang dikirim Alice yang telah di enkripsi kemudian diteria oleh Bob yang kemudian di deskripsikan.

Protokol Perjanjian Kunci Diffie-Hellman

Ada permasalahan ketika Alice dan Bob menyepakati penggunaan sistem kriptografi simetris, keduanya harus menyepakati kunci yang sama. Seperti yang diketahui Alice dan Bob tidak saling bertemu secara langsung. Jika Alice mengirimkan kunci ke Bob lewat jalur yang rawan tersebut, maka pihak musuh dapat dengan mudah mengetahuinya. Untuk mempersulit musuh mengetahui kunci tersebut, perlu dilakuka protokol perjanjian kunci. Protokol perjanjian kunci yang umum dipakai adalah protokol perjanjian kunci Diffie-Hellman menurut [4] . Diberikan grup siklik G dan pembangun dari G adalah g dengan g dan ordernya d diketahui oleh publik, berikut alur komunikasi yang dilakukan oleh Alice dan Bob. [6] :

1. Alice mengambil secara acak bilangan bulat $a \in [2, d-1]$, selanjutnya Alice menghitung g^a dan mengirimkannya ke Bob.
2. Bob juga mengambil secara aca bilangan bulat $b \in [2, d-1]$, menghitung g^b dan mengirimnya ke Alice.
3. Bob menghitung Kunci $K_b = (g^b)^a$ sedangkan alice menghitung $K_a = (g^a)^b$
4. Kunci tersebut $K = (g^a)^b = (g^b)^a \in G$ karena $ab = ba$

Protokol perjanjian kunci ini dapat diketahui pihak musuh jika musuh mengetahui *g* dan g^a yang dikirim Alice kepada Bob. Dengan menggunakan perhitungan canggih seperti sekarang. Maka musuh harus menentukan nilai *a* atau *b*.

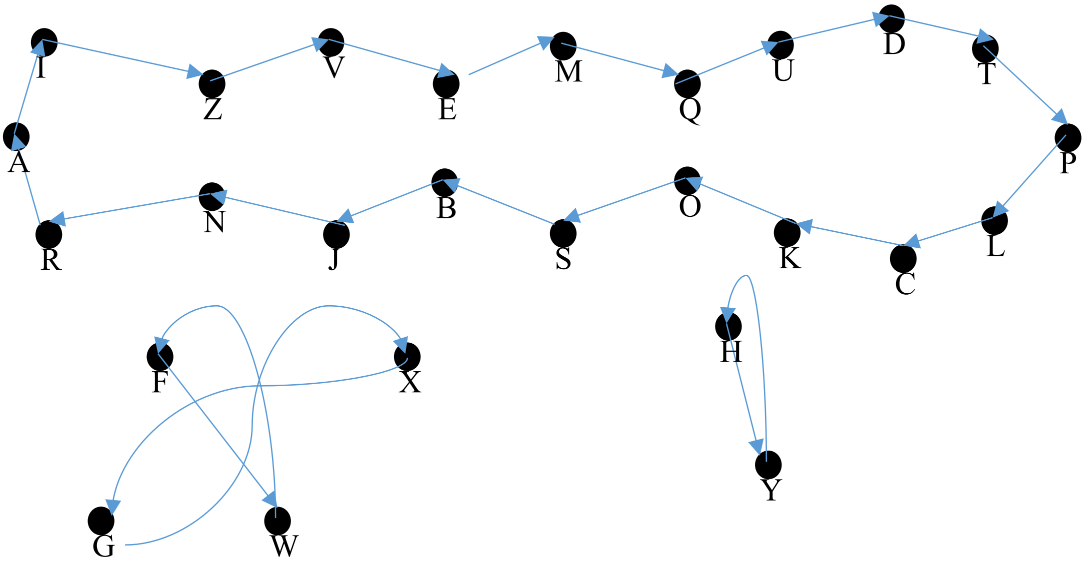
Perjanjian Protokol Kunci Stickel

Perjanjian Protokol kunci stickel didefinisikan oleh [2] merupakan perjanjuan kunci yang didasarkan pada grup yang tidak komutatif. Misal $G = GL(n, F)$ dan misalkan $g \in G$, dan $a, b \in G$ dengan order masing-masing n_a dan n_b, sehingga $ab \neq ba$. proses yang dilakukan Alice dan Bob adalah:

1. Alice memilih sebarang bilangan bulat *l,m* dengan syarat, $0 < l < n_a$ dan $0 < m < n_b$ sehingga $u = a^l g b^m$ dikirimkan ke Bob.
2. Bob juga memilih sebarang bilangan bulat r, s dengan syarat $0 < r < n_a$ dan $0 < s < n_b$ sehingga $v = a^r g b^s$ dikirimkan ke Alice.
3. Alice menghitung $K_a = a^l v b^m$ dan Bob menghitung $K_b = a^r u b^s$
4. Kunci yang disepakati $K_a = a^l w b^m = a^l a^r g a^s a^m = a^{l+r} g a^{s+m} = a^{r+l} g a^{m+s} = a^r v a^s = K_b$

Pembobotan Huruf

Kelemahan kriptografi terletak pada pembobotan huruf yang hampir semua diketahui. Misal huruf A dibobot dengan angka nol sampai dengan huruf Z yang dibobot dengan angka dua puluh lima. Kejadian ini dapat mempermudah musuh dalam mengidentifikasi huruf-huruf yang muncul. Dari sini muncul ide, bagaimana agar huruf yang diberikan dapat disamarkan dari musuh dengan cara pembobotan dalam bentuk graf atau dapat divisualkan dalam bentuk jalur jalan. Berikut graf berarah berdasarkan [1]dan tabelperubahan pembobotan.



0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Gambar 2. Graf dan Tabel perubahan Pembobotan huruf berdasarkan Konektivitas

Tabel diatas dibaca pada kolom huruf A sampai dengan Z dan pada baris huruf A sampai Z. pada baris pertama bobot A yang seharusnya nol diubah pada huruf I, pada

baris ke empat belas huruf O yang seharusnya berbobot 14 diubah padahuruf S, begitu seterusnya.
Dengan tabel korepondensi dibawah, karakter diubah dengan elemen-elemen dari □ … sebagai berikut:

$0 \leftrightarrow I$	$1 \leftrightarrow J$	$2 \leftrightarrow K$	$3 \leftrightarrow L$	$4 \leftrightarrow M$
$5 \leftrightarrow W$	$6 \leftrightarrow X$	$7 \leftrightarrow Y$	$8 \leftrightarrow Z$	$9 \leftrightarrow N$
$10 \leftrightarrow O$	$11 \leftrightarrow P$	$12 \leftrightarrow Q$	$13 \leftrightarrow R$	$14 \leftrightarrow S$
$15 \leftrightarrow T$	$16 \leftrightarrow U$	$17 \leftrightarrow A$	$18 \leftrightarrow B$	$19 \leftrightarrow C$
$20 \leftrightarrow D$	$21 \leftrightarrow E$	$22 \leftrightarrow F$	$23 \leftrightarrow G$	$24 \leftrightarrow H$
$25 \leftrightarrow V$				

Gambar 3. Pembobotan Huruf

HASIL DAN PEMBAHASAN

Berikut ini akan diberikan sistem sederhana Chiper Vigenere dan Protokol perjanjian Stickel menggunakan Grupoid non komutatif dengan perubahan pembobotan Huruf. Misalkan Alice dan Bob menyepakati matriks grupoid non komutatif sederhana, yaitu:

$$M_{2\times 2} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d \in \square \right\}$$

Alice akan mengirimkan sebuah pesan kepada Bob yang berisikan "SERANG LAWAN ESOK SORE" . sebelum mengirimkan pesan, Alice mengirimkan sebuah peta yang menggambarkan jalur-jalur yang merupakan visualisasi titik dan sisi kepada Bob. Sedangkan titik awal dan tujuan divisualisasikan sebuah tempat yang berawalan huruf pada abjad. Selanjutnya Alice dan Bob menyepakati tiga buah matrik berdasarkan Perjanjian Kunci Stikel yaitu:
$a = \begin{pmatrix} 11 & 2 \\ 13 & 22 \end{pmatrix}$, $b = \begin{pmatrix} 6 & 8 \\ 1 & 19 \end{pmatrix}$ dan $g = \begin{pmatrix} 3 & 7 \\ 6 & 12 \end{pmatrix}$. Selanjutnya mereka melakukan perhitungan dalam mod 26

1. Alice secara acak memilih bilangan asli l=6, dan m=5 dan menghitung
$$u = \begin{pmatrix} 11 & 2 \\ 13 & 22 \end{pmatrix}^6 \begin{pmatrix} 3 & 7 \\ 6 & 12 \end{pmatrix} \begin{pmatrix} 6 & 8 \\ 1 & 19 \end{pmatrix}^5 = \begin{pmatrix} 25 & 24 \\ 13 & 14 \end{pmatrix} \begin{pmatrix} 3 & 7 \\ 6 & 12 \end{pmatrix} \begin{pmatrix} 14 & 18 \\ 25 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 11 \\ 7 & 3 \end{pmatrix}$$

2. Bob juga melakukan hal yang sama, memilih secara acak bilangan asli $r = 8$ dan $s = 9$ dan menghitung $v = \begin{pmatrix} 11 & 2 \\ 13 & 22 \end{pmatrix}^8 \begin{pmatrix} 3 & 7 \\ 6 & 12 \end{pmatrix} \begin{pmatrix} 6 & 8 \\ 1 & 19 \end{pmatrix}^9 = \begin{pmatrix} 1 & 5 \\ 5 & 21 \end{pmatrix}$

3. Alice mengirimkan u ke Bob dan menerima v darinya

4. Bob mengirimkan v ke Alice dan menerima u darinya.

5. Alice menghitung kunci $K_A = \begin{pmatrix} 11 & 2 \\ 13 & 22 \end{pmatrix}^6 \begin{pmatrix} 1 & 5 \\ 5 & 21 \end{pmatrix} \begin{pmatrix} 6 & 8 \\ 1 & 19 \end{pmatrix}^5 = \begin{pmatrix} 23 & 15 \\ 23 & 7 \end{pmatrix}$

6. Bob menghitung kunci $K_A = \begin{pmatrix} 11 & 2 \\ 13 & 22 \end{pmatrix}^8 \begin{pmatrix} 1 & 5 \\ 5 & 21 \end{pmatrix} \begin{pmatrix} 6 & 8 \\ 1 & 19 \end{pmatrix}^9 = \begin{pmatrix} 23 & 15 \\ 23 & 7 \end{pmatrix}$

Selanjutnya Alice mengirim Pesan graf dan kunci yang telah disepakati. Pesan graf berfungsi untuk pembobotan pada huruf yang secara umum A di bobot dengan nilai nol. Pada graf diatas pesan yang dikirim menjadi potongan-potongan huruf yang dipecah menjadi:

SERA-NGLA-WANE-SOKS-OREE

Selanjutnya potongan huruf tersebut dibobot dengan bobot yang disesuaikan dengan graf yaitu
S=14,E=21,R=13,A=17,N=9,G=23,L=3,A=17,W=5,A=17,N=9,E=21,S=14,O=10,K=2,S=14,O=10,R=13,E=21,E=21.
Kemudian diubah dalam matriks 2×2 menjadi

$$P1 = \begin{pmatrix} 14 & 21 \\ 13 & 17 \end{pmatrix}, P2 = \begin{pmatrix} 9 & 23 \\ 3 & 17 \end{pmatrix}, P3 = \begin{pmatrix} 5 & 17 \\ 9 & 21 \end{pmatrix}, P4 = \begin{pmatrix} 14 & 10 \\ 2 & 14 \end{pmatrix}, P5 := \begin{pmatrix} 10 & 13 \\ 21 & 21 \end{pmatrix}$$

Kemudian dengan kunci yang telah disepakati, $K = \begin{pmatrix} 23 & 15 \\ 23 & 7 \end{pmatrix}$ dan proses enkripsi Chiper Vigenere diperoleh:

$$e_{k1} = \left(\begin{pmatrix} 14 & 21 \\ 13 & 17 \end{pmatrix} + \begin{pmatrix} 23 & 15 \\ 23 & 7 \end{pmatrix} \right) \bmod 26 = \begin{pmatrix} 11 & 10 \\ 10 & 24 \end{pmatrix}$$

$$e_{k2} = \left(\begin{pmatrix} 9 & 23 \\ 3 & 17 \end{pmatrix} + \begin{pmatrix} 23 & 15 \\ 23 & 7 \end{pmatrix} \right) \bmod 26 = \begin{pmatrix} 6 & 12 \\ 0 & 24 \end{pmatrix}$$

$$e_{k3} = \left(\begin{pmatrix} 5 & 17 \\ 9 & 21 \end{pmatrix} + \begin{pmatrix} 23 & 15 \\ 23 & 7 \end{pmatrix} \right) \bmod 26 = \begin{pmatrix} 2 & 6 \\ 6 & 2 \end{pmatrix}$$

$$e_{k4} = \left(\begin{pmatrix} 14 & 10 \\ 2 & 14 \end{pmatrix} + \begin{pmatrix} 23 & 15 \\ 23 & 7 \end{pmatrix} \right) \bmod 26 = \begin{pmatrix} 11 & 25 \\ 25 & 21 \end{pmatrix}$$

$$e_{k5} = \left(\begin{pmatrix} 10 & 13 \\ 21 & 21 \end{pmatrix} + \begin{pmatrix} 23 & 15 \\ 23 & 7 \end{pmatrix} \right) \bmod 26 = \begin{pmatrix} 7 & 2 \\ 18 & 2 \end{pmatrix}$$

Chiper teks kalau diterjemahkan dalam huruf menjadi:

POOH-XQIH-KXXK-PVVE-YKBK

Setelah pesan di terima oleh Bob. Maka pesan tersebut di deskripsikan menggunakan kunci yang telah disepakati, yaitu

$$d_{k1} = \left(\begin{pmatrix} 11 & 10 \\ 10 & 24 \end{pmatrix} - \begin{pmatrix} 23 & 15 \\ 23 & 7 \end{pmatrix} \right) \bmod 26 = \begin{pmatrix} 14 & 21 \\ 13 & 17 \end{pmatrix}$$

$$d_{k2}=\left(\begin{pmatrix}6 & 12\\ 0 & 24\end{pmatrix}-\begin{pmatrix}23 & 15\\ 23 & 7\end{pmatrix}\right)\mathrm{mod}\,26=\begin{pmatrix}9 & 23\\ 3 & 17\end{pmatrix}$$

$$d_{k3}=\left(\begin{pmatrix}2 & 6\\ 6 & 2\end{pmatrix}-\begin{pmatrix}23 & 15\\ 23 & 7\end{pmatrix}\right)\mathrm{mod}\,26=\begin{pmatrix}5 & 17\\ 9 & 21\end{pmatrix}$$

$$d_{k4}=\left(\begin{pmatrix}11 & 25\\ 25 & 21\end{pmatrix}-\begin{pmatrix}23 & 15\\ 23 & 7\end{pmatrix}\right)\mathrm{mod}\,26=\begin{pmatrix}14 & 10\\ 2 & 14\end{pmatrix}$$

$$d_{k5}=\left(\begin{pmatrix}7 & 2\\ 18 & 2\end{pmatrix}-\begin{pmatrix}23 & 15\\ 23 & 7\end{pmatrix}\right)\mathrm{mod}\,26=\begin{pmatrix}10 & 13\\ 21 & 21\end{pmatrix}$$

Sehingga pesan yang diterima oleh Bob adalah “SERA-NGLA-WANE-SOKS-OREE”. Andaikan musuh tidak tahu tentang graf yang diberikan sebelum kata kunci diberikan, dengan memakai pembobotan secara umum yaitu huruf A dibobot nol, B dibobot satu dan seterusnya sampai Z dibobot 25, maka pesan chiperteks yang diterima musuh berupa,

LKKY-GMAY-CGGC-LZZV-HCSC

andaikan pula, ditengah kemajuan teknologi dan prosesor makin cepat, musuh dapat mengidentifikasi kunci yang telah disetujui, maka pesan yang dibaca musuh adalah.

OVNR-JXDR-FRJV-OKCO-KNVV

Dengan demikian makin sulit musuh untuk menerjemahkan pesan yang seharusnya dapat diketahui dan membutuhkan waktu yang lama.

KESIMPULAN

Pengamanan suatu komunikasi sangat penting, hal ini untuk menjaga kerahasiaan suatu informasi atau pesan. Mengirim pesan melalui jaringan komunikasi global sangat tidak aman. Hal ini dikarenakan musuh dapat menyadap pesan-pesan yang dikirim. Untuk mengatasi hal tersebut dipergunakanlah kriptografi, salah satunya kriptografi simetris menggunakan Chiper Vigenere. Namun semakin canggih alat yang digunakan, semakin mudah musuh mengetahui. Untuk mengatasinya digunakan protokol perjanjian kunci stikel dalam proses enkripsi dan deskripsinya. Kelemahan protokol perjanjian stikel adalah dipublikasikannya matriks-matriks kunci yang disepakati, pihak musuh bila dilengkapi dengan alat super canggih, dapat menemukan bilangan-bilangan asli yang diambil oleh masing-masing pihak yang saling berkomunikasi. Perubahan bobot secara umum pada huruf-huruf dapat memperlambat kinerja musuh. Perubahan bobot yang dikirim dapat berupa petunjuk jalan atau graf. tingkat kesulitan graf yang diberikan, dapat meningkatkan keamanan dari pesan-pesan yang dikirim. Perlulah untuk diteliti graf-graf baru yang mempersulit musuh membacanya.

DAFTAR RUJUKAN

[1] Bondy, JA. Et al. 2008. Graph Theory. Springer. France
[2] Buchmann, A Johannes. 2000. Introduction to Cryptography. Springer. New York
[3] Menezes, A J, Et al. 1996. Handbook of Applied Crytography, CRC Press. USA.
[4] Myasnikov, Alexei, Et al. 2008. Group Based Chryptography. Birkhauser Verlag. Berlin
[5] Riyanto, Z. 2012. Protokol Perjanjian Kunci Berdasarkan Masalah Faktorisasi Atas Semigrup Non Komutatif. Prosiding seminar nasional UNY. ISBN:978-979-99314-6-7
[6] Simon R, Blackbourn, Et al. 2009.Groups St Andrews 2009 9n Bath. The London Mathematical Society. Cambridge. London.