PROTOKOL PERJANJIAN KUNCI BERDASARKAN MASALAH KONJUGASI ATAS GRUP NON-KOMUTATIF

M. Zaki Riyanto

Pendidikan Matematika, JPMIPA, FKIP
Universitas Ahmad Dahlan, Yogyakarta
Email: zaki@mail.ugm.ac.id

Abstrak

Protokol perjanjian kunci merupakan suatu skema dalam kriptografi yang digunakan untuk mengatasi masalah perjanjian kunci rahasia. Kunci rahasia tersebut digunakan pada proses enkripsi-dekripsi di antara dua pihak yang berkomunikasi. Secara umum, tingkat keamanan dari protokol perjanjian kunci diletakkan pada tingkat kesulitan dari suatu permasalahan matematis. Salah satu protokol perjanjian kunci yang telah dikenal luas adalah perjanjian kunci Diffie-Hellman yang didasarkan pada masalah logaritma diskrit pada suatu grup siklik. Dalam makalah ini, diperkenalkan suatu protokol perjanjian kunci yang tingkat keamanannya diletakkan pada permasalahan konjugasi atas grup non-komutatif. Contoh grup non-komutatif yang digunakan dalam makalah ini adalah grup matriks invertibel atas lapangan hingga. Selanjutnya, diberikan penerapannya pada sistem kriptografi Cipher Hill.

Kata kunci: kriptografi, perjanjian kunci, protokol, teori grup

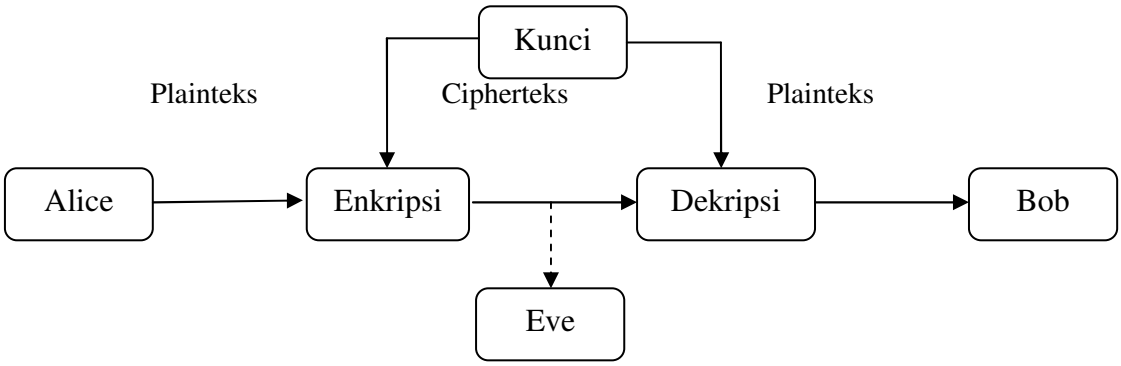
PENDAHULUAN

Perkembangan teknologi informasi dewasa ini telah berpengaruh pada hampir semua aspek kehidupan manusia, tak terkecuali dalam hal berkomunikasi. Dengan adanya internet, komunikasi jarak jauh dapat dilakukan dengan cepat dan murah. Namun di sisi lain, ternyata internet tidak terlalu aman karena merupakan jalur komunikasi umum yang dapat digunakan oleh siapapun sehingga sangat rawan terhadap penyadapan. Oleh karena itu, keamanan informasi menjadi faktor utama yang harus dipenuhi.

Salah satu solusinya adalah kriptografi. Kriptografi adalah suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data (Menezes dkk, 1996). Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi suatu kode yang tidak dapat dimengerti oleh pihak lain. Enkripsi adalah suatu proses penyandian yang melakukan perubahan suatu pesan, dari yang dapat dimengerti, disebut dengan plainteks, menjadi suatu kode yang sulit dimengerti, disebut dengan cipherteks. Sedangkan proses kebalikannya untuk mengubah cipherteks menjadi plainteks disebut dekripsi. Proses enkripsi dan dekripsi memerlukan suatu mekanisme dan kunci tertentu.

Sistem kriptografi atau sering disebut dengan cipher merupakan suatu sistem atau kumpulan aturan-aturan yang digunakan untuk melakukan enkripsi dan dekripsi. Sistem kriptografi simetris adalah sistem kriptografi yang menggunakan kunci enkripsi dan dekripsi yang sama. Sistem ini mengharuskan dua pihak yang berkomunikasi menyepakati suatu kunci rahasia yang sama sebelum keduanya saling berkomunikasi. Keamanan dari sistem ini tergantung pada kunci, membocorkan kunci berarti bahwa orang lain yang berhasil mendapatkan kunci dapat mendekripsi

cipherteks. Sistem kriptografi ini sering disebut dengan sistem kriptografi kunci rahasia, seperti dijelaskan pada gambar berikut ini.



Gambar 1. Sistem Kriptografi Simetris

Pada Gambar 1 di atas, ada dua pihak yaitu Alice dan Bob yang berkomunikasi secara rahasia menggunakan sistem kriptografi simetris. Komunikasi dilakukan melalui jalur komunikasi yang tidak dapat dijamin keamanannya. Untuk dapat melakukan komunikasi secara rahasia, Alice dan Bob harus menyetujui suatu kunci rahasia yang sama. Akan tetapi, ada pihak ketiga yaitu Eve yang berada di antara kedua pihak yang berusaha untuk mendapatkan informasi rahasia yang dikirimkan. Contoh sistem kriptografi simetris adalah Cipher Hill, AES dan DES. Pada makalah ini hanya diberikan penjelesan mengenai Cipher Hill. Untuk penjelasan dari beberapa sistem kriptografi simetris dapat ditemukan dalam Menezes dkk (1996) dan Stinson (2006).

Cipher Hill merupakan suatu sistem kriptografi simetris yang proses enkripsi dan dekripsinya menggunakan operasi matriks yang didefinisikan atas suatu lapangan hingga. Diberikan F adalah lapangan hingga, didefinisikan himpunan semua matriks atas F berukuran $n\times n$, yaitu

$$M_n(F)=\left\{\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}\middle| a_{ij}\in F, 1\le i,j\le n\right\}.$$

Selanjutnya, didefinisikan himpunan semua kunci yaitu himpunan semua matriks di $M_n(F)$ yang invertibel atau yang mempunyai determinan tidak nol, yaitu

$$\mathrm{GL}_n(F)=\left\{A\in M_n(F)\middle|\det(A)\neq 0\right\}.$$

Himpunan $\mathrm{GL}_n(F)$ merupakan grup non-komutatif terhadap operasi perkalian matriks. Himpunan semua plainteks dan cipherteks diberikan dalam vektor kolom yaitu $F^n=\left\{\begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix}\middle| p_1,\ldots,p_n\in F\right\}$. Diberikan plainteks $P=\begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix}\in F^n$ dan kunci

$K = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \in \mathrm{GL}_n(F)$. Proses enkripsi diberikan dalam fungsi

$$e_K(P) = KP = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix} = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix},$$

dengan $C = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \in F^n$ adalah cipherteks. Proses dekripsi diberikan dalam fungsi

$$d_K(C) = K^{-1}C = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}^{-1} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix}.$$

Untuk contoh dari Cipher Hill akan diberikan pada pembahasan selanjutnya mengenai protokol perjanjian kunci. Misalkan Alice ingin mengirimkan pesan rahasia berupa plainteks *P* melalui jalur komunikasi yang tidak aman, maka Alice harus menentukan kunci *K* dan melakukan enkripsi sehingga diperoleh cipherteks *C*. Kemudian cipheteks *C* dikirimkan kepada Bob.

Protokol Perjanjian Kunci

Apabila Alice dan Bob menggunakan sistem kriptografi simetris, masalah utama yang muncul adalah keduanya harus menyepakati kunci yang sama, padahal keduanya tidak dapat bertemu secara langsung. Apabila kunci *K* dikirimkan kepada Bob, maka pihak Eve dapat mengetahui kunci *K*.

Salah satu cara yang dapat digunakan untuk mengatasi masalah ini adalah menggunakan protokol perjanjian kunci (*key establishment protocol*). Protokol perjanjian kunci bertujuan agar kedua belah pihak dapat menentukan kunci yang sama walaupun dilakukan melalui jalur komunikasi yang tidak aman. Salah satu contoh protokol perjanjian kunci yang paling sederhana dan telah dikenal secara luas adalah protokol perjanjian kunci Diffie-Hellman yang ditemukan pada tahun 1976.

Alice atau Bob mempublikasikan suatu grup siklik berhingga *G* dengan elemen pembangun $g \in G$.	
Alice	**Bob**
1. Alice memilih secara rahasia $a \in$ □	1. Bob memilih secara rahasia $b \in$ □
2. Alice menghitung g^a	2. Bob menghitung g^b
3. Alice mengirim g^a kepada Bob	3. Bob mengirim g^b kepada Alice
4. Alice menerima g^b dari Bob	4. Bob menerima g^a dari Alice
5. Alice menghitung $K_A = \left(g^b\right)^a = g^{ba}$	5. Bob menghitung $K_B = \left(g^a\right)^b = g^{ab}$
Alice dan Bob telah menyepakati kunci rahasia $K = K_A = K_B$	

Gambar 2. Skema Protokol Perjanjian Kunci Diffie-Hellman

Karena setiap grup siklik merupakan grup komutatif, maka $ab = ba$, sehingga diperoleh $K = K_A = K_B$. Misalkan Alice dan Bob telah berhasil menyepakati kunci rahasia yang sama yaitu *K*. Selanjutnya, kunci rahasia *K* yang telah disepakati digunakan untuk melakukan proses enkripsi-dekripsi. Di lain pihak, Eve sebagai pihak penyerang hanya dapat mengetahui nilai *g*, g^a dan g^b. Untuk mendapatkan kunci yang telah disepakati Alice dan Bob, Eve harus menentukan nilai *a* atau *b*. Dengan kata lain, Eve harus menyelesaikan masalah logaritma diskrit pada *G*, yaitu menentukan *a* apabila nilai *g* dan g^a diketahui. Tingkat kemanan dari protokol perjanjian kunci Diffie-Hellman didasarkan pada masalah logaritma diskrit pada grup siklik.

Protokol Perjanjian Kunci dan Masalah Konjugasi

Pada protokol perjanjian kunci Diffie-Hellman digunakan grup siklik yang merupakan grup komutatif. Dalam makalah ini diperkenalkan konsep mengenai protokol perjanjian kunci yang menggunakan grup non-komutatif. Untuk dapat menggunakan grup non-komutatif, protokol perjanjian kunci harus dapat dikonstruksi menggunakan suatu permasalahan matematis yang ada pada grup non-komutatif, yaitu masalah konjugasi yang diberikan sebagai berikut.

Diberikan suatu grup G dan $w, x \in G$. Masalah konjugasi didefinisikan sebagai permasalahan menentukan $a \in G$ sedemikian hingga $a^{-1}wa = x$. Myasnikov dkk (2008) telah menyelidiki bahwa untuk mencari solusi penyelesaiannya dibutuhkan perhitungan-perhitungan rekursif dan enumerasi pada setiap elemen di *G*. Oleh karena itu, penentuan grup *G* yang non-komutatif dan order dari *G* yang besar turut menentukan tingkat kesulitan dalam menyelesaikan masalah konjugasi. Myasnikov dkk (2008) memberikan skema protokol perjanjian kunci yang didasarkan pada masalah konjugasi atas grup non-komutatif sebagai berikut.

<table>
<tr><td colspan="2">Alice atau Bob mempublikasikan suatu grup non-komutatif G,
suatu elemen $w \in G$ dan H suatu subgrup komutatif dari G</td></tr>
<tr><th>Alice</th><th>Bob</th></tr>
<tr><td>1. Alice memilih secara rahasia $a \in H$
2. Alice menghitung $x = a^{-1}wa$
3. Alice mengirim x kepada Bob
4. Alice menerima y dari Bob
5. Alice menghitung $K_A = a^{-1}ya$</td><td>1. Bob memilih secara rahasia $b \in H$
2. Bob menghitung $y = b^{-1}wb$
3. Bob mengirim y kepada Alice
4. Bob menerima x dari Alice
5. Bob menghitung $K_B = b^{-1}xb$</td></tr>
<tr><td colspan="2">Alice dan Bob telah menyepakati kunci rahasia $K = K_A = K_B$</td></tr>
</table>

Gambar 3. Skema Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi atas Grup Non-komutatif (Myasnikov, 2008)

Dapat ditunjukkan bahwa Alice dan Bob berhasil menyepakati kunci rahasia yang sama. Diketahui $a, b \in H$ dan *H* merupakan subgrup komutatif dari *G*, sehingga $ab = ba$. Selanjutnya, diketahui $x = a^{-1}wa$ dan $y = b^{-1}wb$, diperoleh

$$K_A = a^{-1}ya = a^{-1}b^{-1}wba = (ba)^{-1}w(ba) = (ab)^{-1}w(ab) = b^{-1}a^{-1}wab = b^{-1}xb = K_B \ .$$

Berikut ini diberikan sebuah contoh yang sangat sederhana mengenai sistem kriptografi Cipher Hill dan protokol perjanjian kunci berdasarkan masalah konjugasi atas suatu grup non-komutatif.

Misalkan Alice dan Bob menggunakan grup non-komutatif

$$\mathrm{GL}_2(\square_{29}) = \left\{ A \in M_2(\square_{29}) \middle| \det(A) \neq 0 \right\}$$

dengan $\mathbb{Z}_{29} = \{0,1,2,...,28\}$ merupakan lapangan hingga. Alice ingin mengirimkan pesan rahasia "SECRET" kepada Bob menggunakan sistem kriptografi Cipher Hill. Apabila Alice mengenkripsi pesan tersebut menggunakan suatu kunci dan menghasilkan cipherteks, maka cipherteks yang dikirimkan kepada Bob tidak dapat dibuka oleh Bob, sebab Bob tidak mengetahui kunci yang digunakan oleh Alice. Alice tidak boleh mengirimkan kunci kepada Bob, karena ada Eve sebagai pihak penyerang yang dapat menyadap dan mendapatkan apapun yang melewati jalur komunikasi. Oleh karena itu, Alice dan Bob harus melakukan suatu perjanjian kunci. Misalkan diberikan dalam gambar berikut ini.

Alice atau Bob mempublikasikan suatu grup non-komutatif $\mathrm{GL}_2(\mathbb{Z}_{29})$,

$w = \begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_{29})$ dan $H = \left\{ \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^m \middle| m \in \mathbb{Z} \right\}$ subgrup komutatif dari $\mathrm{GL}_2(\mathbb{Z}_{29})$

Alice	**Bob**
1. Alice memilih secara rahasia $a = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix} \in H$	1. Bob memilih secara rahasia $b = \begin{pmatrix} 8 & 25 \\ 23 & 2 \end{pmatrix} \in H$
2. Alice menghitung $x = a^{-1}wa$ $= \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}^{-1} \begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}$ $= \begin{pmatrix} 20 & 12 \\ 18 & 9 \end{pmatrix} \begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}$ $= \begin{pmatrix} 17 & 20 \\ 2 & 21 \end{pmatrix}$	2. Bob menghitung $y = b^{-1}wb$ $= \begin{pmatrix} 8 & 25 \\ 23 & 2 \end{pmatrix}^{-1} \begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 8 & 25 \\ 23 & 2 \end{pmatrix}$ $= \begin{pmatrix} 7 & 14 \\ 21 & 28 \end{pmatrix} \begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 8 & 25 \\ 23 & 2 \end{pmatrix}$ $= \begin{pmatrix} 27 & 5 \\ 25 & 11 \end{pmatrix}$
3. Alice mengirim *x* kepada Bob	3. Bob mengirim *y* kepada Alice
4. Alice menerima *y* dari Bob	4. Bob menerima *x* dari Alice
5. Alice menghitung $K_A = a^{-1}ya$ $= \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}^{-1} \begin{pmatrix} 27 & 5 \\ 25 & 11 \end{pmatrix} \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}$ $= \begin{pmatrix} 20 & 12 \\ 18 & 9 \end{pmatrix} \begin{pmatrix} 27 & 5 \\ 25 & 11 \end{pmatrix} \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}$ $= \begin{pmatrix} 22 & 19 \\ 11 & 16 \end{pmatrix}$	5. Bob menghitung $K_B = b^{-1}xb$ $= \begin{pmatrix} 8 & 25 \\ 23 & 2 \end{pmatrix}^{-1} \begin{pmatrix} 17 & 20 \\ 2 & 21 \end{pmatrix} \begin{pmatrix} 8 & 25 \\ 23 & 2 \end{pmatrix}$ $= \begin{pmatrix} 7 & 14 \\ 21 & 28 \end{pmatrix} \begin{pmatrix} 17 & 20 \\ 2 & 21 \end{pmatrix} \begin{pmatrix} 25 & 21 \\ 17 & 13 \end{pmatrix}$ $= \begin{pmatrix} 22 & 19 \\ 11 & 16 \end{pmatrix}$

Alice dan Bob telah menyepakati kunci rahasia $K = K_A = K_B = \begin{pmatrix} 22 & 19 \\ 11 & 16 \end{pmatrix}$

Gambar 4. Contoh Perhitungan Protokol Perjanjian Kunci

Setelah Alice dan Bob berhasil menyepakati kunci rahasia $K = \begin{pmatrix} 22 & 19 \\ 11 & 16 \end{pmatrix}$, selanjutnya Alice akan mengenkripsi pesan "SECRET" menggunakan Cipher Hill dengan kunci *K*. Diberikan tabel korespondensi antara karakter dengan elemen-elemen dari $\square_{29} = \{0,1,2,...,28\}$ sebagai berikut.

Tabel 1. Korespondensi karakter dengan bilangan

0 ↔ A	1 ↔ B	2 ↔ C	3 ↔ D	4 ↔ E
5 ↔ F	6 ↔ G	7 ↔ H	8 ↔ I	9 ↔ J
10 ↔ K	11 ↔ L	12 ↔ M	13 ↔ N	14 ↔ O
15 ↔ P	16 ↔ Q	17 ↔ R	18 ↔ S	19 ↔ T
20 ↔ U	21 ↔ V	22 ↔ W	23 ↔ X	24 ↔ Y
25 ↔ Z	26 ↔ .	27 ↔ ,	28 ↔ -	

Pesan "SECRET" dipotong-potong menjadi "SE-CR-ET". Menggunakan Tabel 1 dapat diperoleh tiga plainteks, misalkan P_1 berkorespondensi dengan "SE", P_2 berkorespondensi dengan "CR" dan P_3 berkorespondensi dengan "ET", yaitu

$$P_1 = \begin{pmatrix} 18 \\ 4 \end{pmatrix},\ P_2 = \begin{pmatrix} 2 \\ 17 \end{pmatrix} \text{ dan } P_3 = \begin{pmatrix} 4 \\ 19 \end{pmatrix}.$$

Selanjutnya, Alice melakukan enkripsi pada ketiga plainteks menggunakan kunci $K = \begin{pmatrix} 22 & 19 \\ 11 & 16 \end{pmatrix}$, yaitu

$$e_K(P_1) = KP_1 = \begin{pmatrix} 22 & 19 \\ 11 & 16 \end{pmatrix}\begin{pmatrix} 18 \\ 4 \end{pmatrix} = \begin{pmatrix} 8 \\ 1 \end{pmatrix}$$

$$e_K(P_2) = KP_2 = \begin{pmatrix} 22 & 19 \\ 11 & 16 \end{pmatrix}\begin{pmatrix} 2 \\ 17 \end{pmatrix} = \begin{pmatrix} 19 \\ 4 \end{pmatrix}$$

$$e_K(P_3) = KP_3 = \begin{pmatrix} 22 & 19 \\ 11 & 16 \end{pmatrix}\begin{pmatrix} 4 \\ 19 \end{pmatrix} = \begin{pmatrix} 14 \\ 0 \end{pmatrix}$$

Dari perhitungan di atas, diperoleh cipherteks $C_1 = \begin{pmatrix} 8 \\ 1 \end{pmatrix},\ C_2 = \begin{pmatrix} 19 \\ 4 \end{pmatrix}$ dan $C_3 = \begin{pmatrix} 14 \\ 0 \end{pmatrix}$. Cipherteks C_1 berkorespondensi dengan "IB", cipherteks C_2 berkorespondensi dengan "TE" dan C_3 berkorespondensi dengan "OA". Dengan demikian, Alice telah mengenkripsi pesan "SECRET" menjadi "IBTEOA" dan selanjutnya dikirimkan kepada Bob.

Misalkan Bob telah menerima cipherteks "IBTEOA". Cipherteks ini dipotong-potong menjadi "IB-TE-OA" yang berkorespondensi dengan $C_1 = \begin{pmatrix} 8 \\ 1 \end{pmatrix}$, $C_2 = \begin{pmatrix} 19 \\ 4 \end{pmatrix}$ dan $C_3 = \begin{pmatrix} 14 \\ 0 \end{pmatrix}$. Bob melakukan dekripsi menggunakan kunci yang telah diperoleh dari perjanjian kunci dengan Alice, yaitu $K = \begin{pmatrix} 22 & 19 \\ 11 & 16 \end{pmatrix}$. Proses dekripsi dilakukan sebagai berikut

$$d_K(C_1) = K^{-1}C_1 = \begin{pmatrix} 22 & 19 \\ 11 & 16 \end{pmatrix}^{-1} \begin{pmatrix} 8 \\ 1 \end{pmatrix} = \begin{pmatrix} 21 & 24 \\ 20 & 18 \end{pmatrix} \begin{pmatrix} 8 \\ 1 \end{pmatrix} = \begin{pmatrix} 18 \\ 4 \end{pmatrix}$$

$$d_K(C_2) = K^{-1}C_2 = \begin{pmatrix} 22 & 19 \\ 11 & 16 \end{pmatrix}^{-1} \begin{pmatrix} 19 \\ 4 \end{pmatrix} = \begin{pmatrix} 21 & 24 \\ 20 & 18 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} = \begin{pmatrix} 2 \\ 17 \end{pmatrix}$$

$$d_K(C_3) = K^{-1}C_3 = \begin{pmatrix} 22 & 19 \\ 11 & 16 \end{pmatrix}^{-1} \begin{pmatrix} 14 \\ 0 \end{pmatrix} = \begin{pmatrix} 21 & 24 \\ 20 & 18 \end{pmatrix} \begin{pmatrix} 14 \\ 0 \end{pmatrix} = \begin{pmatrix} 4 \\ 19 \end{pmatrix}$$

Bob berhasil mendapatkan plainteks yang dikirimkan oleh Alice, yaitu $P_1 = \begin{pmatrix} 18 \\ 4 \end{pmatrix}$, $P_2 = \begin{pmatrix} 2 \\ 17 \end{pmatrix}$ dan $P_3 = \begin{pmatrix} 4 \\ 19 \end{pmatrix}$ yang berkorespondensi dengan pesan "SECRET".

KESIMPULAN

Untuk menjaga keamanan pengiriman pesan rahasia, pesan dapat dirubah menjadi suatu kode yang tidak dapat dimengerti oleh pihak penyadap. Salah caranya adalah dengan menggunakan sistem kriptografi simetris. Pada sistem kriptografi simetris, proses enkripsi dan dekripsi dilakukan menggunakan kunci rahasia yang sama. Oleh karena itu, kedua pihak yang berkomunikasi harus melakukan kesepakatan kunci yang sama. Protokol perjanjian kunci digunakan untuk mengatasi permasalahan dalam melakukan kesepakatan kunci yang akan digunakan untuk proses enkripsi dan dekripsi.

Protokol perjanjian kunci yang selama ini dikenal masih dilakukan atas suatu grup komutatif. Pada grup non-komutatif dapat dikonstruksi suatu protokol perjanjian kunci yang didasarkan pada masalah konjugasi. Tingkat kesulitan dalam menyelesaikan masalah konjugasi pada grup non-komutatif menentukan tingkat keamanan dari protokol perjanjian kunci. Oleh karena itu, perlu dilakukan penelitian mengenai metode-metode yang dapat digunakan untuk menyelesaikan masalah konjugasi pada grup non-komutatif. Selain itu, juga perlu diteliti grup-grup non-komutatif yang dapat digunakan untuk protokol perjanjian kunci.

DAFTAR PUSTAKA

Menezes Alfred J., Paul C. van Oorschot dan Scott A. Vanstone, 1996, *Handbook of Applied Cryptography*, CRC Press, USA.

Myasnikov Alexei, Vladimir Shpilrain dan Alexander Ushakov, 2008, *Group-based Cryptography*, Birkhauser Verlag, Basel Switzerland.

Stinson Douglas R., 2006, *Cryptography: Theory and Practice Third Edition*, Capman and Hall/CRC Press, Boca Raton, Florida.