Protokol Otentikasi Berdasarkan Masalah Konjugasi Pada Grup Unit Atas Ring Endomorfisma *END* $(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$

Muhamad Zaki Riyanto

Program Studi Matematika Fakultas Sains dan Teknologi, UIN Sunan Kalijaga, Jl. Marsda Adisucipto No. 1 Yogyakarta, Indonesia

Korespondensi; Email: muhamad.riyanto@uin-suka.ac.id

Abstrak

Diberikan suatu bilangan prima p, maka *END* $(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ adalah ring non-komutatif dengan elemen satuan dan memuat sebanyak p^5 elemen. Climent et.al. (2011) telah menunjukkan bahwa ring *END* $(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ isomorfis dengan ring $E_p = \left\{\begin{pmatrix} a & b \\ pc & d \end{pmatrix} : a, b, c \in \mathbb{Z}_p, d \in \mathbb{Z}_{p^2}\right\}$, serta memberikan penerapan dari ring tersebut dalam kriptografi, yaitu berupa protokol pertukaran kunci berdasarkan masalah dekomposisi. Pada makalah ini, protokol pertukaran kunci tersebut dikembangkan menjadi suatu protokol otentikasi. Fungsi dari protokol otentikasi adalah sebagai sarana untuk membuktikan kebenaran identitas pihak pengirim (*user*) kepada pihak penerima (*server*). Dalam makalah ini diperkenalkan suatu protokol otentikasi yang didasarkan pada masalah konjugasi pada grup unit $U(E_p)$. Penggunaan grup unit unit $U(E_p)$ didasarkan pada fakta bahwa grup ini memuat sebanyak $p^3(p-1)^2$ elemen. Apabila semakin besar bilangan prima p yang digunakan, maka diharapkan masalah konjugasi pada grup $U(E_p)$ menjadi lebih sulit untuk dipecahkan.

Kata Kunci: Ring endomorfisma; grup unit; masalah konjugasi; kriptografi; protokol otentikasi

Abstract

Let p be a prime number, then *END* $(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ is a non-commutative ring with unity and has p^5 elements. Climent et.al. in 2011 proved that *END* $(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ is isomorphic to the ring $E_p = \left\{\begin{pmatrix} a & b \\ pc & d \end{pmatrix} : a, b, c \in \mathbb{Z}_p, d \in \mathbb{Z}_{p^2}\right\}$ and gives an application to a key exchange protocol based on the decompostion problem. The ring has an important properties about the number of unit elements, it has $p^3(p-1)^2$ unit elements. In this paper, we develop an authentication protocol based on the conjugation problem over the unit group $U(E_p)$. If we use a big prime number, then the number of elements of $U(E_p)$ is very big close to p^5, it may increase the security of the authentication protocol.

Keywords: Endomorphism of rings; unit group; conjugation; authentication; cryptography

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 maupun pemalsuan. Oleh karena itu, keamanan informasi menjadi faktor utama yang harus dipenuhi.

Salah satu solusi untuk mengatasi hal tersebut adalah menggunakan 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 [1]. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Aspek dalam kriptografi

yang umum dibahas adalah tentang keharasiaan data, yaitu menggunakan metode enkripsi-dekripsi. Pesan semula (plainteks) dienkripsi menjadi pesan tersandi (cipherteks) menggunakan suatu metode tertentu dan suatu parameter rahasia yang disebut dengan kunci. Algoritma enkripsi yang dikenal luas selama ini adalah DES, AES, RSA dan ECC.

Selain itu juga dikenal protokol pertukaran kunci yang digunakan pada proses enkripsi dan dekripsi, yaitu kedua belah pihak yang melakukan enkripsi-dekripsi dapat menyepakati kunci yang sama. Salah satu protokol pertukaran kunci yang dikenal luas adalah protokol pertukaran kunci Diffie-Hellman yang didasarkan pada masalah logaritma diskrit atas suatu grup siklik dengan order besar .

Selain aspek kerahasiaan, aspek otentikasi juga merupakan hal penting yang harus dipertimbangan pada saat proses pengiriman informasi dilakukan. Hal ini dilakukan agar tidak terjadi pemalsuan data pengirim. Banyak kasus pemalsuan identitas pengirim yang terjadi, seperti pemalsuan surat dan sms. Dalam perkembangannya, aspek otentikasi dapat diselesaikan menggunakan skema tanda tangan digital. Saat ini, tanda tangan digital yang dikenal luas adalah tanda tangan RSA dan tanda tangan DSA. Tanda tangan RSA yang didasarkan pada masalah faktorisasi billangan bulat yang besar . Tanda tangan RSA bekerja pada ring $\mathbb{Z}_{pq}$ dimana p dan q adalah bilangan prima besar yang berbeda. Tanda tangan DSA didasarkan pada masalah logaritma diskrit seperti pada protokol pertukaran kunci Diffie-Hellman.

Seiring dengan adanya perkembangan komputer kuantum, terjadi ancaman pada masalah faktorisasi dan masalah logaritma diskrit, walauapun komputer kuantum tersebut belum dapat diwujudkan. Diyakini bahwa kedua masalah tersebut dapat diselesaikan dengan mudah menggunakan komputer kuantum di masa yang akan datang [2]. Akibat dari adanya ancaman tersebut, banyak penilitian dilakukan untuk mencari kandidat skema enkripsi-dekripsi, tanda tangan digital, maupun protokol pertukaran kunci yang aman dari serangan komputer kuantum.

Salah satu penelitian yang dilakukan adalah dengan memanfaatkan masalah dalam teori grup, yaitu masalah konjugasi pada grup non-komutatif [3]. Dari masalah konjugasi dapat dikonstruksi protokol pertukaran kunci dan dan protokol otentikasi. Selain itu juga dilakukan penelitian pada masalah dekomposisi pada suatu ring berhingga, penelitian ini dilakukan untuk mengkonstruksi protokol pertukaran kunci. Salah satu ring yang digunakan adalah ring endomorfisma seperti yang dilakukan oleh Climent, Navarro dan Tartosa [4]. Pada makalah ini diperkenalkan suatu protokol otentikasi yang merupakan pengembangan dari protokol pertukaran kunci yang didasarkan pada masalah konjugasi pada grup unit atas ring endomorfisma.

Ring Endomorfisma $\boldsymbol{END}\left(\mathbb{Z}_{\boldsymbol{p}} \times \mathbb{Z}_{\boldsymbol{p^2}}\right)$

Diberikan p adalah suatu bilangan prima, dibentuk himpunan $\mathbb{Z}_p \times \mathbb{Z}_{p^2} = \{(a,b): a \in \mathbb{Z}_p, b \in \mathbb{Z}_{p^2}\}$, maka $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ adalah grup komutatif terhadap operasi penjumlahan biasa. Selanjutnya dibentuk *END* $\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$ adalah himpunan semua endomorfisma pada grup $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$. Dapat dilihat bahwa himpunan *END* $\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$ merupakan ring terhadap operasi komposisi fungsi.

Climent, Navarro dan Tartosa [4] telah menunjukkan bahwa terdapat suatu isomorfisma antara ring *END* $\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$ dan ring

$$E_p = \left\{ \begin{pmatrix} a & b \\ pc & d \end{pmatrix} : a, b, c \in \mathbb{Z}_p, d \in \mathbb{Z}_{p^2} \right\}$$

dengan operasi penjumlahan dan perkaliannya didefinisikan berbeda dengan operasi penjumlahan dan perkalian matriks pada umumnya, yaitu sebagai berikut

$$\begin{pmatrix} a_1 & b_1 \\ pc_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ pc_2 & d_2 \end{pmatrix} = \begin{pmatrix} (a_1 + a_2)\ mod\ p & (b_1 + b_2)\ mod\ p \\ p(c_1 + c_2)\ mod\ p^2 & (d_1 + d_2)\ mod\ p^2 \end{pmatrix}$$

dan

$$\begin{pmatrix} a_1 & b_1 \\ pc_1 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ pc_2 & d_2 \end{pmatrix} = \begin{pmatrix} (a_1 a_2)\ mod\ p & (a_1 b_2 + b_1 d_2)\ mod\ p \\ p(c_1 a_2 + d_1 c_2)\ mod\ p^2 & (pc_1 b_2 + d_1 d_2)\ mod\ p^2 \end{pmatrix}.$$

Untuk selajutnya, penulisan ring *END* $\left(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\right)$ dapat disebutkan dengan ring E_p. Dapat dilihat bahwa E_p memuat sebanyak p^5 elemen, serta memiliki elemen identitas penjumlahannya adalah $O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ dan elemen identitas perkaliannya adalah $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Diberikan $M = \begin{pmatrix} a & b \\ pc & d \end{pmatrix} \in E_p$, dengan $d \in \mathbb{Z}_{p^2}$, maka d dapat ditulis sebagai $d = pu + v$ dimana $u, v \in \mathbb{Z}_p$. Salah satu fakta yang menarik terkait dengan elemen unit (invertibel) pada ring E_p diberikan pada teorema berikut ini.

Teorema 1. [4] Diberikan $M = \begin{pmatrix} a & b \\ pc & pu + v \end{pmatrix} \in E_p$ dengan $a, b, c, u, v \in \mathbb{Z}_p$, maka M merupakan unit jika dan hanya jika $a \neq 0$ dan $v \neq 0$. Lebih lanjut,

$$M^{-1} = \begin{pmatrix} a^{-1} & (-a^{-1}bv^{-1}) mod\ p \\ p[(-v^{-1}ca^{-1}) mod\ p] & p\left[\left(ca^{-1}b(v^{-1})^2 - u(v^{-1})^2 - \left\lfloor \frac{vv^{-1}}{p} \right\rfloor v^{-1}\right) mod\ p\right] + v^{-1} \end{pmatrix}.$$

Bukti: Dapat dilihat dalam [4].

Dalam kriptografi, semakin banyak pemilihan parameter rahasia yang digunakan, maka diharapkan dapat meningkatkan keamanan dari sistem kriptografi yang digunakan. Jumlah elemen unit dari E_p memiliki sifat yang baik untuk membangun sistem kriptografi seperti diberikan dalam teorema berikut.

Teorema 2. [4] Banyaknya elemen unit pada ring E_p adalah $p^3(p-1)^2$.

Bukti: Diketahui bahwa suatu $\begin{pmatrix} a & b \\ pc & pu + v \end{pmatrix} \in E_p$ merupakan elemen non-unit jika dan hanya jika $a = 0$ atau $v = 0$. Banyaknya elemen dari E_p yang berbentuk $\begin{pmatrix} 0 & b \\ pc & pu + v \end{pmatrix}$ adalah p^4, banyaknya elemen dari E_p yang berbentuk $\begin{pmatrix} a & b \\ pc & pu \end{pmatrix}$ adalah p^4, dan banyaknya elemen dari E_p yang berbentuk $\begin{pmatrix} 0 & b \\ pc & pu \end{pmatrix}$ adalah p^3. Oleh karena itu, banyaknya elemen non-unit pada E_p adalah $2p^4 - p^3$. Dengan demikian, banyaknya elemen unit pada E_p adalah $p^5 - (2p^4 - p^3) = p^3(p-1)^2$. ■

Hal menarik yang dapat dilihat adalah bahwa probabilitas suatu elemen dari E_p merupakan unit adalah

$$p^3(p-1)^2 \Big/ p^5 = (p-1)^2 \Big/ p^2 \approx 1,$$

yaitu hampir semua elemen dari E_p adalah unit [4].

Akibat 3. Dibentuk $U(E_p)$ adalah himpunan semua unit dari E_p, maka $U(E_p)$ adalah grup non-komutatif dengan $\left|U(E_p)\right| = p^3(p-1)^2$.

Protokol Pertukaran Kunci dan Protokol Otentikasi

Sistem kriptografi berupa skema enkripsi-dekripsi, tanda tangan digital, protokol pertukaran kunci dan otentikasi seperti RSA, ElGamal dan Diffie-Hellman memanfaatkan permasalahan dalam matematika yang sulit, seperti masalah faktorisasi dan masalah logaritma diskrit [1]. Tingkat keamanan dari sistem

kriptografi tersebut bergantung kepada tingkat kesulitan dalam menyelesaikan masalah tersebut, artinya semakin sulit menyelesaikan masalah yang digunakan berakibat semakin kuat tingkat keamanan sistem kriptografinya. Berikut ini diberikan skema protokol pertukaran kunci Diffie-Hellman.

Tabel 1 Protokol pertukaran kunci Diffie-Hellman.

Alice atau Bob mempublikasikan suatu grup siklik berhingga G dengan elemen pembangun $g \in G$.	
Alice	**Bob**
1. Alice memilih secara rahasia $a \in \mathbb{N}$	1. Bob memilih secara rahasia $b \in \mathbb{N}$
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 $K_B = (g^a)^b = g^{ab}$
Alice dan Bob telah menyepakati kunci rahasia $K = K_A = K_B$.	

Berdasarkan protokol pertukaran kunci Diffie-Hellman tersebut, dapat dikembangkan suatu protokol otentikasi yang didasarkan pada masalah logaritma diskrit sebagai berikut. Misalkan Alice sebagi pihak pembukti (prover) dan Bob sebagai pihak verifikator.

Tabel 2 Protokol otentikasi Diffie-Hellman.

Alice mempublikasikan suatu grup siklik berhingga G dengan elemen pembangun $g \in G$.	
Alice	**Bob**
1. Alice memilih secara rahasia $a \in \mathbb{N}$	1. Bob memilih secara rahasia $b \in \mathbb{N}$
2. Alice menghitung g^a	2. Bob menghitung g^b
3. Alice mengirim g^a kepada Bob	3. Bob mengirim tantangan g^b kepada Alice
4. Alice menerima g^b dari Bob	4. Bob menerima g^a dari Alice
5. Alice merespon dengan bukti $P = \left(g^b\right)^a = g^{ba}$ dan mengirimkannya kepada Bob	5. Bob memverifikasi apakah $(g^a)^b = P$?

Tujuan dari protokol otentikasi adalah sebagai alat untuk melegitimasi Alice sebagai user untuk membuktikan identitasnya kepada Bob sebagai server melalui jalur komunikasi yang tidak aman.

Di dalam teori grup dikenal suatu masalah yang dinamakan dengan masalah konjugasi yang diberikan pada definisi berikut.

Definisi 4. Diberikan G adalah suatu grup dan $g, h \in G$. Masalah konjugasi didefinisikan sebagai masalah dalam menentukan suatu $x \in G$ sedemikian hingga $x^{-1}gx = h$.

Dalam Ko, Lee dkk [5] diberikan suatu protokol pertukaran kunci yang didasarkan pada masalah konjugasi atas grup non-komutatif. Walaupun menggunakan grup non-komutatif, tetapi tetap memanfaatkan beberapa hal yang bersifat komutatif, seperti diberikan berikut.

Tabel 3 Protokol pertukaran kunci berdasarkan masalah konjugasi [5].

Alice atau Bob mempublikasikan suatu grup non-komutatif G, suatu elemen $w \in G$ dan H suatu subgrup komutatif dari G	
Alice	**Bob**
1. Alice memilih secara rahasia $a \in H$	1. Bob memilih secara rahasia $b \in H$
2. Alice menghitung $x = a^{-1}wa$	2. Bob menghitung $y = b^{-1}wb$
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 $K_A = a^{-1}ya$	5. Bob menghitung $K_B = b^{-1}xb$
Alice dan Bob telah menyepakati kunci rahasia $K = K_A = K_B$	

Grup unit $U(E_p)$ dapat diterapkan pada protokol pertukaran kunci yang didasarkan pada masalah konjugasi tersebut, seperti diberikan dalam tabel berikut ini.

Tabel 4 Protokol pertukaran kunci berdasarkan masalah konjugasi atas grup unit $U(E_p)$.

Alice atau Bob mempublikasikan bilangan prima p, suatu elemen $W \in U(E_p)$ dan H suatu subgrup komutatif dari $U(E_p)$	
Alice	**Bob**
1. Alice memilih secara rahasia $A \in H$	1. Bob memilih secara rahasia $B \in H$
2. Alice menghitung $X = A^{-1}WA$	2. Bob menghitung $Y = B^{-1}WB$
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 $K_A = A^{-1}YA$	5. Bob menghitung $K_B = B^{-1}XB$
Alice dan Bob telah menyepakati kunci rahasia $K = K_A = K_B$	

Subgrup komutatif dari $U(E_p)$ dapat dibentuk melalui subgrup siklik yang dibangun oleh suatu elemen dari $U(E_p)$, yaitu $H = \{A^n : n \in \mathbb{Z}\}$ untuk suatu $A \in U(E_p)$. Selain itu juga dapat dibentuk melalui *center* dari E_p yaitu

$$Z(E_p) = \left\{ \begin{pmatrix} v & 0 \\ 0 & pu + v \end{pmatrix} : u, v \in \mathbb{Z}_p \right\}.$$

Protokol Otentikasi pada Grup Unit $U(E_p)$

Protokol pertukaran kunci yang didasarkan pada masalah konjugasi atas grup unit $U(E_p)$ dapat dikembangkan menjadi protokol otentikasi yang didasarkan pada masalah konjugasi. Secara umum, protokol ini diberikan sebagai berikut.

Tabel 5 Protokol otentikasi berdasarkan masalah konjugasi [3].

Alice mempublikasikan suatu grup non-komutatif G serta H *dan* N suatu subgrup dari G sedemikian hingga $hn = nh$ untuk setiap $h \in H$ dan $n \in N$	
Alice	**Bob**
1. Alice memilih $s \in H$ 2. Alice memilih $w \in G$ 3. Alice menghitung $t = s^{-1}ws$ 4. Alice mengirim w dan t kepada Bob	

	5. Bob menerima w dan t dari Alice 6. Bob memilih $r \in N$ 7. Bob mengirimkan tantangan $w' = r^{-1}wr$ kepada Alice
8. Alice menerima w' dari Bob 9. Alice merespon dengan mengirimkan $w'' = s^{-1}w's$ kepada Bob	
	10. Bob mengecek apakah $w'' = r^{-1}tr$

Dapat dilihat bahwa jawaban yang benar dari respon Alice adalah dengan mengecek persamaan $w'' = r^{-1}tr$ berlaku, yaitu

$$w'' = s^{-1}w's = s^{-1}r^{-1}wrs = r^{-1}s^{-1}wsr = r^{-1}tr\,.$$

Berdasarkan Tabel 5 di atas, dapat dikonstruksi suatu protokol otentikasi yang didasarkan pada masalah konjugasi pada grup unit $U(E_p)$. Perbedaan dengan protokol pertukaran kunci adalah penggunaan dua subgrup dari $U(E_p)$ yaitu H dan N sedemikian hingga untuk setiap $S \in H$ dan $R \in N$ memenuhi $SR = RS$. Dua subgrup tersebut dapat dikonstruksi melalui pemilihan dua elemen dari $U(E_p)$ yang saling komutatif. Misalkan dipilih $A, B \in U(E_p)$ sedemikian hingga $AB=BA$. Dibentuk subgrup siklik $H = \{A^n : n \in \mathbb{Z}\}$ dan $N = \{B^n : n \in \mathbb{Z}\}$, maka untuk setiap $S \in H$ dan $R \in N$ berlaku $SR = RS$. Berikut ini diberikan protokol otentikasi berdasarkan masalah konjugasi pada grup unit $U(E_p)$.

Tabel 6 Protokol otentikasi berdasarkan masalah konjugasi pada grup unit $U(E_p)$.

Alice mempublikasikan bilangan prima p serta H *dan* N suatu subgrup dari $U(E_p)$ sedemikian hingga $SR = RS$ untuk setiap $S \in H$ dan $R \in N$	
Alice	**Bob**
1. Alice memilih $S \in H$ 2. Alice memilih $W \in U(E_p)$ 3. Alice menghitung $T = S^{-1}WS$ 4. Alice mengirim W dan T kepada Bob	
	5. Bob menerima W dan T dari Alice 6. Bob memilih $R \in N$ 7. Bob mengirimkan tantangan $W' = R^{-1}WR$ kepada Alice
8. Alice menerima W' dari Bob 9. Alice merespon dengan mengirimkan $W'' = S^{-1}W'S$ kepada Bob	
	10. Bob mengecek apakah $W'' = Rr^{-1}TR$

Sebagai contoh kasus sederhana dari protokol ini diberikan berikut ini. Bob akan mengotentikasi Alice. Oleh karena itu, Alice dan Bob menggunakan protokol otentikasi seperti pada Tabel 6 di atas. Alice memilih bilangan prima $p = 2579$. Alice memilih secara rahasia $A = \begin{pmatrix} 123 & 0 \\ 0 & 45678 \end{pmatrix}$, $B = \begin{pmatrix} 910 & 0 \\ 0 & 11123 \end{pmatrix} \in Z(E_{2579}) \cap U(E_{2579})$. Selanjutnya, Alice membentuk subgrup siklik $H = \langle A \rangle$ dan $N = \langle B \rangle$. Alice mempublikasikan $p = 2579$, H dan N. Langkah berikutnya adalah Alice memilih

secara rahasia $S = \begin{pmatrix} 123 & 0 \\ 0 & 45678 \end{pmatrix}^2 = \begin{pmatrix} 2234 & 0 \\ 0 & 4641251 \end{pmatrix} \in H$ dan $W = \begin{pmatrix} 121 & 232 \\ 5158 & 15618 \end{pmatrix} \in U(E_{2579})$. Alice menghitung

$$\begin{aligned} T &= S^{-1}WS \\ &= \begin{pmatrix} 2234 & 0 \\ 0 & 4641251 \end{pmatrix}^{-1} \begin{pmatrix} 121 & 232 \\ 5158 & 15618 \end{pmatrix} \begin{pmatrix} 2234 & 0 \\ 0 & 4641251 \end{pmatrix} \\ &= \begin{pmatrix} 2123 & 0 \\ 0 & 6473877 \end{pmatrix} \begin{pmatrix} 121 & 232 \\ 5158 & 15618 \end{pmatrix} \begin{pmatrix} 2234 & 0 \\ 0 & 4641251 \end{pmatrix} \\ &= \begin{pmatrix} 121 & 1269 \\ 6323708 & 15618 \end{pmatrix}. \end{aligned}$$

Selanjutnya, Alice mengirimkan $W = \begin{pmatrix} 121 & 232 \\ 5158 & 15618 \end{pmatrix}$ dan $T = \begin{pmatrix} 121 & 1269 \\ 6323708 & 15618 \end{pmatrix}$ kepada Bob. Di lain pihak, Bob menerima $W = \begin{pmatrix} 121 & 232 \\ 5158 & 15618 \end{pmatrix}$ dan $T = \begin{pmatrix} 121 & 1269 \\ 6323708 & 15618 \end{pmatrix}$ dari Alice. Langkah berikutnya adalah Bob memilih secara rahasia $W = \begin{pmatrix} 910 & 0 \\ 0 & 11123 \end{pmatrix}^4 = \begin{pmatrix} 1343 & 0 \\ 0 & 1158689 \end{pmatrix} \in N$. Bob mengirimkan tantangan kepada Bob yaitu

$$\begin{aligned} W' &= R^{-1}WR \\ &= \begin{pmatrix} 1343 & 0 \\ 0 & 1158689 \end{pmatrix}^{-1} \begin{pmatrix} 121 & 232 \\ 5158 & 15618 \end{pmatrix} \begin{pmatrix} 1343 & 0 \\ 0 & 1158689 \end{pmatrix} \\ &= \begin{pmatrix} 699 & 0 \\ 0 & 6489565 \end{pmatrix} \begin{pmatrix} 121 & 232 \\ 5158 & 15618 \end{pmatrix} \begin{pmatrix} 1343 & 0 \\ 0 & 1158689 \end{pmatrix} \\ &= \begin{pmatrix} 121 & 2511 \\ 1547400 & 15618 \end{pmatrix}. \end{aligned}$$

Alice menerima tantangan $W' = \begin{pmatrix} 121 & 2511 \\ 1547400 & 15618 \end{pmatrix}$ dari Alice, maka Alice mengirimkan respon kepada Bob yaitu

$$\begin{aligned} W'' &= R^{-1}WR \\ &= \begin{pmatrix} 2234 & 0 \\ 0 & 4641251 \end{pmatrix}^{-1} \begin{pmatrix} 121 & 2511 \\ 1547400 & 15618 \end{pmatrix} \begin{pmatrix} 2234 & 0 \\ 0 & 4641251 \end{pmatrix} \\ &= \begin{pmatrix} 2123 & 0 \\ 0 & 6473877 \end{pmatrix} \begin{pmatrix} 121 & 232 \\ 5158 & 15618 \end{pmatrix} \begin{pmatrix} 2234 & 0 \\ 0 & 4641251 \end{pmatrix} \\ &= \begin{pmatrix} 121 & 2377 \\ 1508715 & 15618 \end{pmatrix}. \end{aligned}$$

Bob menerima respon $W'' = \begin{pmatrix} 121 & 2377 \\ 1508715 & 15618 \end{pmatrix}$ dari Alice. Untuk melalukan otentikasi, Bob menghitung

$$R^{-1}TR = \begin{pmatrix} 1343 & 0 \\ 0 & 1158689 \end{pmatrix}^{-1} \begin{pmatrix} 121 & 1269 \\ 6323708 & 15618 \end{pmatrix} \begin{pmatrix} 1343 & 0 \\ 0 & 1158689 \end{pmatrix}$$
$$= \begin{pmatrix} 699 & 0 \\ 0 & 6489565 \end{pmatrix} \begin{pmatrix} 121 & 1269 \\ 6323708 & 15618 \end{pmatrix} \begin{pmatrix} 1343 & 0 \\ 0 & 1158689 \end{pmatrix}$$
$$= \begin{pmatrix} 121 & 2377 \\ 1508715 & 15618 \end{pmatrix}.$$

Bob memperoleh hasil bahwa $W'' = R^{-1}TR$, yang berarti bahwa proses otentikasi berhasil.

Penutup

Adanya protokol pertukaran kunci yang didasarkan pada masalah konjugasi dapat melahirkan adanya protokol otentikasi yang didasarkan pada masalah yang sama. Oleh karena itu, pemanfaatan grup unit $U(E_p)$ menjadi baik untuk digunakan dalam protokol otentikasi. Hal ini dikarenakan adanya penggunaan elemen unit pada konsep konjugasi serta banyaknya jumlah anggota dari grup unit $U(E_p)$. Semakin besar bilangan prima p yang digunakan akan mengakibatkan banyaknya pemilihan parameter rahasia yang semakin besar pula. Hal ini diharapkan dapat menjadikan pihak penyerang mengalami kesulitan karena harus menyelesaikan masalah konjugasi yang melibatkan banyak elemen dari grup unit $U(E_p)$. Dalam [4] disarankan menggunakan bilangan prima p dengan jumlah digit minimal sebanyak 60.

Referensi

[1] **Menezes A.J.**, **Van Oorschot P.C.**, dan **Vanstone S.A.**, 1996, *Handbook of Applied Cryptography*, CRC Press, Boca Raton Florida.

[2] **Shor**, **P.W.**, 1997, *Polynomial-time Algorithms for Prime Factorization and Discrete Logarithm on a Quantum Computer*, SIAM Journal on Computing, 26(5), pp. 1484-1509.

[3] **Myasnikov A.**, **Sphilrain V.**, dan **Ushakov A.**, 2008, *Group Based Cryptography*, Birkhauser-Verlag, Basel.

[4] **Climent J.J.**, **Navarro P.R.** dan **Tartosa L.**, 2011, *On the Arithmetic of the Endomorphisms ring* $END(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, Applicable Algebra in Engineering, Communication and Computing, 22(2), pp. 91-108.

[5] **Koo H.K.**, **Lee S.J.**, **Cheon J.H.**, **Han J.W.**, **Kang J.S.** dan **Park C.**, 2000, *New Public-Key Cryptosystem Using Braid Groups*, Advances in Cryptology CRYPTO 2000 Vol.1880 of Lecture Notes in Computer Science, pp. 166-183.