SKEMA PERTUKARAN KUNCI MENGGUNAKAN TEORI MATRIKS

A KEY-EXCHANGE SCHEME BASED ON THEORY OF MATRICES

Sujalwo

Fakultas Teknik
Universitas Muhammadiyah Surakarta

ABSTRAK

Penelitian ini bertujuan untuk mengembangkan penggunaan teori matriks, khususnya matriks invers tergeneralisasi dalam field Z_2, dengan menggunakan skema pertukaran kunci. Skema dikembangkan berdasarkan model pertukaran kunci dari Diffie-Hellman. Berdasarkan skema pertukaran kunci yang telah dibuat, disain pembuatan kunci yang dipakai bersama cukup efisien dalam penggunaan ruang kunci serta mempunyai kompleksitas yang rendah, dalam hal ini anggota O (n^2).

Kata kunci : matriks, pertukaran kunci, kriptografi, autofikasi

ABSTRACT

The purpose of this research is to develop an application of matrices theory, especially generalized inverses of matrices in the field of Z2, on a key exchange scheme. A key-exchange scheme is developed based on Diffie-Hellman scheme. The result of the research shows that the key-exchange scheme is efficient enough in use of key space and has low complexity, that is family of O (n2).

Keywords: *matrices theory, key-exchange scheme cryptography and authofication*

PENDAHULUAN

Sejak diperkenalkan teknik baru di bidang kriptografi oleh Diffe dan Hellman tersebut, telah banyak cabang matematika yang digunakan untuk

mengembangkan bidang kriptografi. Beberapa cabang matematika yang telah digunakan untuk mengembangkan kriptografi dapat disebutkan di antaranya adalah aljabar, teori bilangan, dan teori koding. Beberapa jenis kunci publik dapat disebutkan di antaranya adalah RSA yang menggunakan teori bilangan, *-El Gamal* menggunakan logaritma diskrit, *elliptic curve system* yang dikembangkan berdasarkan teori grup, *the Merkle-Ellman knapsack system* yang berdasar pada *subset sum,* dan *McEliece public key system* yang menggunakan teori koding (Stinson, 1995; Patterson, 1987). Sementara itu, matriks invers tergeneralisasi (MIT) juga dapat digunakan untuk mengembangkan sistem kunci publik (Murtiyasa, 2001; Wu and Dawson, 1998).

Adanya desain kunci publik, menimbulkan masalah dalam keaslian pasangan komunikasi data. Hal ini disebabkan dengan kunci yang bersifat publik tersebut, siapa saja dapat mengirimkan pesan ke pemilik kunci rahasia (penerima pesan). Dalam hal ini penerima pesan tidak mengetahui siapa sebenarnya yang telah mengirim pesan kepadanya. Sampai tahap ini komunikasi tidak dapat menjamin autentikasi (*authentication*) antara pengirim (*sender*) dan penerima (*reciever*) pesan. Artinya, penerima pesan tidak dapat menjamin bahwa pengirim pesan adalah orang yang memang dikehendaki. Untuk itulah perlu didesain model autentikasi antara pengirim dan penerima pesan. Skema autentikasi tersebut, di samping harus menjamin keauntetikan pasangan komunikasi (pengirim dan penerima pesan), juga harus mampu menjamin kerahasiaan (*secrecy*) data atau pesan yang dikirimkannya.

Menurut Stalling (1995:114) ada tiga jenis aplikasi dari kriptografi kunci publik. Pertama, aplikasi di bidang enkripsi (*encryption*) dan dekripsi (*decryption*), kedua di bidang autentikasi (*authentication*), dan ketiga pada pertukaran kunci (*key exchange*). Aplikasi yang pertama berhubungan dengan kerahasiaan (*secrecy*) data atau pesan, sedangkan aplikasi yang kedua dan ketiga berhubungan dengan keaslian pasangan komunikasi data.

Autentikasi merupakan teknik verifikasi untuk mengetahui bahwa partner komunikasi memang orang yang diharapkan. Ada dua jenis model autentikasi, yaitu autentikasi berbasis kunci yang dipakai bersama dan autentikasi berbasis kriptografi kunci publik [Tanembaum, 1997:191-200]. Kedua model autentikasi tersebut, dalam pengembangannya banyak menggunakan pendekatan matematis. Beberapa cabang matematika yang telah dipakai untuk mengembangkan model autentikasi di antaranya adalah teori bilangan, teori koding, dan teori matriks.

Autentikasi berbasis kunci yang dipakai bersama untuk pertama kalinya disampaikan oleh Diffie dan Hellman pada tahun 1976, yang selanjutnya lebih dikenal dengan pertukaran kunci (*key exchange*) Diffie-Hellman [Tanem-

baum, 1997:194:195]. Pertukaran kunci Diffie-Hellman dikembangkan berdasarkan teori bilangan dan logaritma diskrit.

Shao (1998:33-36) telah membuat skema autentikasi berbasis kunci publik yang dikembangkan berdasarkan faktorisasi dan logaritma diskrit. Dalam penelitiannya Shao menyimpulkan bahwa desain yang dibangun berdasarkan faktorisasi dan logaritma diskrit telah mampu memberikan layanan autentikasi dan kerahasiaan data. Artinya data yang ditransmisikan tidak dapat diterobos (*unbreakable*) oleh penyusup (*intruder*) jika problem faktorisasi dan logaritma diskrit secara simultan tidak dapat diselesaikan. Tetapi sebagaimana telah ditunjukkan oleh Lee, dalam penelitian Shao tersebut tersirat adanya kelemahan, yaitu jika problem faktorisasi dapat diselesaikan, maka desain kunci publik akan dapat diterobos (Lee, 1999:119). Ini berarti bahwa skema kunci publik berdasarkan logaritma diskrit dan faktorisasi belum dapat memberikan layanan kerahasiaan data yang ditransmisikan secara maksimal.

Teori matriks juga merupakan cabang matematika yang sangat potensial untuk mengembangkan model autentikasi. Setiawan (2002) menggunakan matriks kuadrat simetri untuk membuat skema autentikasi berbasis kunci yang dipakai bersama. Dalam desain yang dibuat Setiawan tersebut, kunci bersama dibangun melalui Pusat Manajemen Kunci (PMK). Tetapi model ini mempunyai kelemahan yaitu, bagaimana jika PMK tidak jujur?.

Sementara itu, Murtiyasa (2002) juga telah mengembangkan autentikasi berbasis kunci publik berdasarkan matriks invers tergeneralisasi. Model autentikasi yang dikembangkan oleh Murtiyasa tersebut cukup efisien dalam penggunaan ruang kunci dan cukup cepat dan mudah dalam proses enkripsi dan deskripsi data sebab mempunyai kompleksitas yang rendah.

Uraian di atas menunjukkan bahwa teori matriks dapat digunakan untuk mengembangkan model autentikasi, baik berdasarkan kunci yang dipakai bersama maupun berbasis kunci publik. Penelitian ini secara khusus akan membuat skema autentikasi berbasis kunci yang dipakai bersama dengan model pertukaran kunci Diffie-Hellman berdasarkan teori matriks invers.

METODE PENELITIAN

Metode Penelitian yang digunakan dalam penelitian ini adalah studi pustaka dengan dukungan implementasi program komputasi. Dengan studi pustaka diharapkan diperoleh berbagai informasi yang berhubungan dengan enkripsi dan dekripsi, kriptografi, kunci publik, dan teori-teori matriks invers yang mendukung model pertukaran kunci. Penggunaan program komputasi dimaksudkan untuk membantu menunjukkan kebenaran hasil-hasil teorema atau proposisi yang berhubungan dengan desain pertukaran kunci yang dipakai

bersama menggunakan matriks invers tergeneralisasi. Secara rinci metode penelitian ini mencakup:

a. Bahan penelitian meliputi literatur-literatur, baik berupa jurnal-jurnal maupun buku–buku yang berhubungan dengan kriptografi dan matriks invers tergeneralisasi.
b. Alat Penelitan meliputi seperangkat komputer dengan *processor* Pentium III, sistem operasi Windows 98, dan *software* MATLAB versi 6.1.
c. Proses penelitian meliputi mengkaji literatur yang diperoleh untuk memecahkan masalah penelitian, kemudian diuraikan dan disajikan secara benar (*mathematically correct*) dalam bentuk teorema atau proposisi. Untuk mendukung kebenaran teorema atau proposisi yang diperoleh diimplementasikan dengan bantuan program komputasi menggunakan *software* MATLAB.
d. Analisis hasil ditekankan pada sifat-sifat yang dimiliki oleh skema pertukaran kunci yang dibuat, termasuk analisis keamanannya.

HASIL DAN PEMBAHASAN

1. Matriks Invers Tergeneralisasi

Diketahui matriks umum **A** yang berdimensi *kxn*. Suatu matriks **B** yang berdimensi *nxk* adalah MIT dari matiks **A** yang berdimensi *kxn*, jika berlaku **ABA = A.** Jika $\mathbf{A}^+$ menyatakan MIT dari **A**, maka:

$$\mathbf{A}\mathbf{A}^+\mathbf{A} = \mathbf{A} \qquad (1)$$

[Israel dan Greville, 1974].

Sebaliknya, untuk matriks **A** tersebut di atas, **matriks re-invers tergeneralisasi** (*generalized re-inverses*) dari matriks **A** adalah suatu matriks **X** berdimensi *nxk* sedemikian hingga **A** adalah *generalized inverses* dari **X**, jadi berlaku **XAX = X**. Jika $\mathbf{A}^-$ menyatakan matriks re-invers tergeneralisasi (MRIT) dari **A**, maka:

$$\mathbf{A}^-\mathbf{A}\mathbf{A}^- = \mathbf{A}^- \qquad (2)$$

[Wu dan Dawson, 1998:321].

Matriks **A** berdimensi *mxn* yang mempunyai rank *r* dapat dibawa ke bentuk:

$$\mathbf{PAQ} = \begin{bmatrix} I_r & O \\ O & O \end{bmatrix}, \text{ atau } \quad \mathbf{A} = \mathbf{P}^{-1}\begin{bmatrix} I_r & O \\ O & O \end{bmatrix}\mathbf{Q}^{-1} \qquad (3)$$

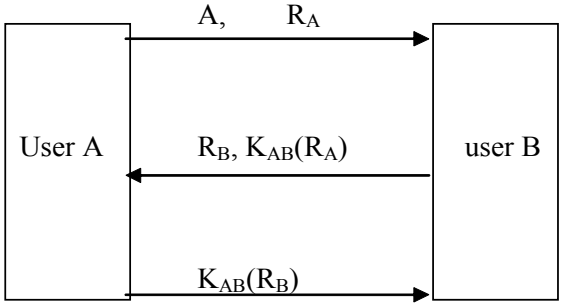
dengan **P** adalah matriks nonsingular hasil penggandaan matriks baris elementer dan **Q** adalah matriks nonsingular hasil penggandaan matriks kolom elementer; $\mathbf{P}^{-1}$ dan $\mathbf{Q}^{-1}$ berturut-turut adalah matriks invers dari **P** dan **Q** (Ayres Jr, 1982 :49). MIT dari **A** dalam bentuk (3) adalah:

$$\mathbf{A}^{+} = \mathbf{Q}\begin{bmatrix} I_r & U \\ V & W \end{bmatrix}\mathbf{P} \qquad (4)$$

dengan sembarang matriks-matriks **U** berdimensi $r \times (m-r)$, **V** berdimensi $(n-r) \times r$ dan **W** berdimensi $(n-r) \times (m-r)$. Pada $Z_2 = \{0,1\}$, banyaknya MIT tergantung dari banyaknya cara untuk memilih **U**, **V**, dan **W** yang berbeda; dalam hal ini banyaknya adalah $2^{r(n-r)+n(m-r)}$ (Murtiyasa, 2001: 3)

2. Model Pertukaran Kunci Diffie-Hellman

Model pertukaran kunci dari Diffie-Hellman dapat dijelaskan sebagai berikut. Pertama-tama user A mengirimkan identitas A dan R_A ke user B. Kemudian user B mengirimkan identitas R_B dan $K_{AB}(R_A)$ kepada user A. Selanjutnya user A mengirimkan $K_{AB}(R_B)$ ke user B [Tanembaum, 1997 : 193]. Model ini secara ringkas dapat digambarkan seperti tercantum pada gambar 1.



Gambar 1: Skema Pertukaran Kunci

Dari gambar 1 tersebut dapat dijelaskan bahwa saat user B menerima A dan R_A, selanjutnya user B menggunakannya untuk membentuk K_{AB} yang digunakan untuk mengenkripsi R_A. Selanjutnya user B mengirimkan identitasnya R_B dan $K_{AB}(R_A)$ kepada user A. Pada saat user A menerimanya, ia yakin bahwa pesan itu berasal dari user B, sebab terdapat identitas dirinya di dalam pesan tersebut, yaitu $K_{AB}(R_A)$. Selanjutnya user A mengenkripsi R_B dengan K_{AB}

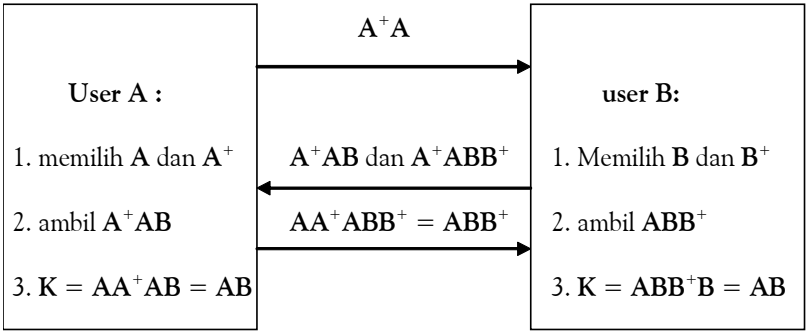
dan mengirimkan $K_{AB}(R_B)$ ini ke user B. Pada saat diterima user B, user B yakin bahwa pesan tersebut berasal dari A, sebab di samping memuat identitas dirinya yang dikirim ke A (yaitu R_B), pesan juga dienkripsi mengunakan kunci K_{AB}. Kunci K_{AB} inilah yang selanjutnya dipakai bersama untuk saling mengen-kripsi pesan. Pada penelitian ini, pengiriman identitas user A maupun user B serta pembentukan kunci bersama akan dikembangkan menggunakan teori matriks invers, dalam hal ini matriks invers tergeneralisasi.

3. Skema Pertukaran Kunci Menggunakan Teori Matriks

Telah disampaikan di atas bahwa model pertukaran kunci mengguna-kan skema yang dipakai Diffie-Hellman dengan teknik matriks invers tergene-ralisasi dalam field Z_2. Diasumsikan bahwa user A ingin mendesain kunci rahasia yang dapat dipakai bersama dengan user B melalui saluran komunikasi umum untuk komunikasi yang bersifat rahasia (aman). Dalam hal ini user A dan user B dapat menempuh langkah-langkah berikut ini untuk mendesain kunci rahasia bersama tersebut :

(1) user yaitu A memilih sembarang matriks **A** berdimensi *kxm* dan menentukan sebuah matriks invers tergeneraalisasi dari **A**, yaitu $\mathbf{A}^+$.
(2) user A mengirimkan ke user B matriks $\mathbf{A}^+\mathbf{A}$.
(3) user B memilih sembarang matriks **B** berdimensi *mxm* dan menentukan sebuah matriks invers tergeneralisasi dari **B**, yaitu $\mathbf{B}^+$.
(4) user B mengirimkan ke user A matriks $\mathbf{A}^+\mathbf{AB}$ dan $\mathbf{A}^+\mathbf{ABB}^+$.
(5) User A mengirimkan ke user B matriks $\mathbf{AA}^+\mathbf{ABB}^+ = \mathbf{ABB}^+$.
(6) User A mendapatkan kunci $\mathbf{K} = \mathbf{AA}^+\mathbf{AB} = \mathbf{AB}$.
(7) User B mendapatkan kunci $\mathbf{K} = \mathbf{ABB}^+\mathbf{B} = \mathbf{AB}$.

Selanjutnya kunci $\mathbf{K} = \mathbf{AB}$ ini dapat dipakai bersama oleh user A dan user B untuk berkomunikasi lebih lanjut secara rahasia dan aman.
Langkah-langkah tersebut di atas dapat digambarkan sebagai berikut.



Gambar 2. Skema Pertukaran Kunci dengan Matriks

Ilustrasi penggunakan model pertukaran kunci di atas dapat dijelaskan sebagai berikut.

1. User A memilih matriks $\mathbf{A} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$, serta menentukan salah satu matriks invers tergeneralisasi dari $\mathbf{A}$, katakanlah $\mathbf{A}^+ = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$.
2. User A mengirimkan $\mathbf{A}^+\mathbf{A} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix} = \mathbf{L}$ ke user B.
3. User B memilih matriks $\mathbf{B} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$, kemudian menentukan salah satu matriks invers tergeneralisasi dari $\mathbf{B}$, katakanlah $\mathbf{B}^+ = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}$.
4. User B mengirimkan ke user A matriks $\mathbf{A}^+\mathbf{AB} = \mathbf{LB} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} =$ $\mathbf{M}$, dan matriks $\mathbf{A}^+\mathbf{ABB}^+ = \mathbf{LBB}^+ = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \mathbf{N}$.
5. User A mengirimkan ke user B matriks $\mathbf{AA}^+\mathbf{ABB}^+ = \mathbf{AN} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$ $= \mathbf{R}$.

6. User A mendapatkan kunci $\mathbf{K} = \mathbf{AA}^{+}\mathbf{AB} = \mathbf{AM} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}$.

7. User B mendapatkan kunci $\mathbf{K} = \mathbf{ABB}^{+}\mathbf{B} = \mathbf{RB} = . \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}$

Selanjutnya user A dan user B dapat melanjutkan komunikasi yang lebih aman dengan menggunakan kunci $\mathbf{K} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}$ untuk melakukan enkripsi data yang akan dikirimkannya.

Pada praktek komunikasi data, kunci **K** ini dapat digunakan dalam beberapa keperluan, di antaranya adalah:

(1) Autentikasi data (*data authentication*). Data yang dienkripsi dengan kunci **K** adalah autentik antara user A dan user B, sebab hanya user A dan user B yang memiliki kunci **K**. Untuk keperluan ini, kunci **K** difungsikan sebagai kunci simetris untuk enkripsi data sebagaimana pada sistem konvensional seperti DES (*data encryption standard*).

(2) Tanda tangan digital (*digital signature*). Data yang dienkripsikan mungkin dienkripsi dengan sistem enkripsi lain, baik sistem konvensional ataupun sistem kunci publik. Selanjutnya pada akhir data yang dienkripsikan tadi disertakan kunci **K**. Jadi kunci **K** di sini berfungsi sebagai pengenal atau identitas pengirim data. Pada waktu user B mendekripsi data, user B tahu bahwa yang mengirimkan data adalah user A, sebab ia menemukan kunci **K** di dalamnya. Sebab hanya user A dan user B yang memiliki kunci **K** tersebut. Dalam istilah komunikasi data digital, data yang dikirimkan oleh user A tersebut telah ditandatangani secara digital.

4. Karakteristik Skema Pertukaran Kunci

Karakteristik protokol pertukaran kunci akan dibahas khususnya tentang ruang kunci, data yang ditransmisikan selama sesi pertukaran kunci, serta kompleksitas perhitungan untuk mendesain kunci yang akan dipakai bersama

tersebut. Diasumsikan bahwa semua operasi, baik yang menyangkut operasi penjumlahan maupun operasi perkalian adalah operasi angka biner (*bit operation*).

a. **Ruang kunci**. Perhatikan ilustrasi di atas, selama sesi pertukaran kunci user A menyimpan **A** berdimensi *kxm*, $\mathbf{A}^+$ berdimensi *mxk*, dan $\mathbf{A}^+\mathbf{AB} = \mathbf{M}$ berdimensi *mxm*. Ini berarti user A memerlukan ruang kunci sebesar ($km + km + m^2$) bit = ($2km + m^2$) bit selama sesi pertukaran kunci. Sedangkan pada akhir sesi pertukaran kunci, user A menyimpan kunci **K** berdimensi *kxm*, yang berarti memerlukan *km* bit. Sehingga jumlah ruang kunci yang diperlukan user A adalah $(2km + m^2) + km = 3km + m^2$ bit.
Sebaliknya bagi user B selama sesi pertukaran kunci menyimpan **B** berdimensi *mxm*, $\mathbf{B}^+$ berdimensi *mxm*, dan $\mathbf{ABB}^+ = \mathbf{R}$ berdimensi *kxm*. Sehingga selama sesi pertukaran kunci user B memerlukan ruang kunci ($m^2 + m^2 + km$) bit = ($2m^2 + km$) bit. Sedangkan pada akhir sesi pertukaran kunci, user B menyimpan kunci **K** berdimensi *kxm*, yang berarti memerlukan *km* bit. Jadi jumlah ruang kunci yang diperlukan user B adalah $(2m^2 + km) + km = 2(m^2 + km)$ bit.

b. **Data yang ditransmisikan**. Dari gambar b.1 dapat diamati bahwa selama sesi pertukaran kunci terjadi tiga kali transmisi data, yaitu dua kali dilakukan oleh user A dan sekali dilakukan oleh user B. Pada transmisi tahap pertama, user A mengirimkan ke user B matriks $\mathbf{L} = \mathbf{A}^+\mathbf{A}$ berdimensi *mxm*, berarti ada m^2 bit data yang ditransmisikan. Pada tahap kedua user B mengirimkan ke user A matriks $\mathbf{M} = \mathbf{A}^+\mathbf{AB}$ berdimensi *mxm* dan matriks $\mathbf{N} = \mathbf{A}^+\mathbf{ABB}^+$ bedimensi *mxm*, berarti secara bersama-sama ada $2m^2$ bit data yang ditransmisikan. Sedangkan pada tahap ketiga user A mengirimkan ke user B matriks $\mathbf{R} = \mathbf{AA}^+\mathbf{ABB}^+ = \mathbf{AN} = \mathbf{ABB}^+$ berdimensi *kxm*, berarti ada *km* bit data yang ditransmisikan. Jadi selama sesi pertukaran kunci ada $m^2 + 2m^2 + km = (3m^2 + km)$ bit data yang ditransmisikan.

c. **Kompleksitas**. Kompleksitas yang dimaksudkan di sini adalah kompleksitas operasi selama sesi pertukaran kunci dan kompleksitas untuk pembuatan kunci **K**. Dalam hal ini kompleksitas dihitung dari banyaknya operasi yang diperlukan, baik operasi penjumlahan maupun perkalian. Pada trans-misi data tahap pertama, user A melakukan perhitungan $\mathbf{L} = \mathbf{A}^+\mathbf{A}$. Mat-riks $\mathbf{A}^+$ berdimensi *mxk* dan matriks A berdimensi *kxm*. Ini berarti pada operasi $\mathbf{A}^+\mathbf{A}$, setiap perkalian baris $\mathbf{A}^+$ dengan kolom **A** memerlukan *k* kali operasi perkalian dan (*k*-1) kali operasi penjumlahan. Jadi banyaknya operasi pada

$\mathbf{A}^{+}\mathbf{A}$ adalah $(m(k + (k\text{-}1))m = (2km^2 - m^2)$ operasi. Ini berarti kompleksitasnya termasuk anggota $O(m^2)$.

Pada transmisi tahap kedua, user B melakukan perhitungan $\mathbf{M} = \mathbf{A}^{+}\mathbf{AB} = \mathbf{LB}$. Baik matriks **L** maupun matriks **B** masing-masing berdimensi *mxm*. Karenanya banyaknya operasi penjumlahan dan perkalian pada **LB** adalah $m(m(m + (m\text{-}1))) = 2m^3 - m^2$ operasi. Ini berarti kompleksitasnya terma-suk anggota $O(m^3)$.

Sedangkan pada tahap ketiga, user A melakukan perhitungan $\mathbf{R} = \mathbf{AN}$. Matriks **A** berdimensi *kxm* dan matriks **N** berdimensi *mxm*. Jadi banyak-nya operasi pada **AN** adalah $k(m(m + (m\text{-}1))) = 2km^2 - km$ operasi. Ini berarti masuk anggota $O(m^2)$. Jadi total kompleksitas selama sesi pertukaran kunci adalah $(2km^2 - m^2) + 2m^3 - m^2 + 2km^2 - km = (2m^3 + 4km^2 - 2m^2 - km)$ ope-rasi. Jadi total kompleksitas pertukaran kunci adalah anggota $O(m^3)$.

Sedangkan kompleksitas pada pembentukan kunci yang dipakai ber-sama, pada dasarnya kunci $\mathbf{K} = \mathbf{AB}$. Karena matriks **A** berdimensi *kxm* dan matriks **B** berdimensi *mxm*, maka banyaknya operasi pada **AB** adalah $k(m(m + (m - 1)))$ operasi $= 2km^2 - km$ operasi. Ini berarti termasuk anggota $O(m^2)$.

SIMPULAN DAN SARAN

Penelitian ini telah menunjukkan bahwa teori matriks dapat digunakan sebagai alat bantu yang potensial untuk riset-riset di bidang kriptografi. Peng-gunaan matriks invers tergeneralisasi untuk membuat desain pertukaran kunci juga sangat menguntungkan, sebab setiap matriks apapun bentuk dan jenisnya pasti memiliki matriks invers tergeneralisasi. Kemudian dari sisi keamanan menjadi terpenuhi sebab banyaknya matriks invers tergeneralisasi adalah tidak tunggal. Sehingga penyusup akan kesulitan menemukan matriks-matriks yang dipakai untuk membangun kunci bersama.

Penelitian lanjutan yang dapat disarankan adalah dalam hal autentikasi dan tanda tangan digital. Dalam bidang autentikasi, bagaimana pemanfaatan kunci bersama **K** tersebut dapat digunakan untuk saling berkomunikasi secara autentik dan aman sehingga menjamin keaslian data yang dikirmkan. Dalam bidang tanda tangan digital, bagaimana pemanfaatan kunci bersama **K** tersebut untuk memverifikasi pesan yang diterima. Artinya sejauh mana kunci **K** dapat menjamin keaslian pasangan komunikasi data.

DAFTAR PUSTAKA

Ayres Jr., F. 1982. *Theory and Problems of Matrices* (Asian Edition) Singapore: McGraw-Hill Book International Company.

Israel, A.B., and Greville, T.N.E. 1974. *Generalized Inverses: Theory and Applications*. New York: John Wiley & Sons.

Lee, N.Y. 1999. "Security of Shao's Signature Schemes Based on Factoring and Discrete Logarithms" dalam *IEE Proceedings Computer Digit. Tech. Vol. 146 No. 2, March 1999, Pp:119-124.*

Murtiyasa, B., 2002, "Aplikasi Matriks Invers Tergeneralisasi pada Autentikasi Kunci Publik". *Laporan Penelitian*. Surakarta: Lembaga Penelitian UMS Surakarta.

Murtiyasa, B. 2001. "Aplikasi Matriks Invers Tergeneralisasi pada Kriptografi" dalam *Jurnal Penelitian Sain dan Teknologi Vol. 1 Nomor 2 Februari 2001. Hal. 82-90*. Surakarta: Lembaga Penelitian UMS.

Patterson, W.1987. *Mathematical Cryptology for Computer Scientists and Mathematicians.* New Jersey: Rowman & Littlefield Publisher.

Setiawan, A.2002. "Key Sharing dengan Matriks Kuadrat Simetrik" dalam *Konferensi Nasional Matematika XI dan Kongres Himpunan Matematika Indonesia tanggal 22-25 Juli 2002*. Malang: UM Malang.

Shao, Z. 1998. "Signature Schemes Based on Factoring and Descrete Logarithms" dalam *IEE Proceedings Computer Digit. Tech. Vol. 145 No. 1, January 1998, Pp:33-36.*

Stalling, W. 1995. *Network and Internetwork Security Principles and Practice*, New Jersey: Prentice Hall.

Stinson, D. R. 1995. *Cryptography Theory and Practice.* Florida: CRC Press LLC.

Tanenbaum, A.S. 1997. *Jaringan Komputer*, Jilid 2, Edisi Bahasa Indonesia, Jakarta: Prenhallindo.

Wu, C.K., and Dawson, E. 1998. "Generalised Inverses in Public Key Cryptosystem Design" dalam *IEE Proceedings Computer Digit. Tech. Vol. 145 No. 5, September 1998, Pp:321-326.*