RANCANGAN PROTOKOL KEAMANAN DATA UNTUK SISTEM UJIAN *ONLINE*[1]

Wahyu Noviani P.
FMIPA, Universitas Terbuka, Tangerang Selatan

Email korespondensi : novie@ut.ac.id

Ujian merupakan salah satu tahapan evaluasi untuk mengetahui tingkat keberhasilan dari proses belajar mengajar. Sistem ujian konvensional dengan media kertas membutuhkan sumber daya waktu dan tenaga yang besar. Oleh karena itu, perlu adanya metode alternatif untuk dapat melaksanakan ujian dengan baik, cepat, akurat, dan efisien. Salah satu metode alternatif tersebut adalah sistem ujian yang dilakukan secara *online*, melalui media komputer dan koneksi *internet*. Dengan cara ini, waktu yang diperlukan untuk proses penyelenggaraan ujiannya juga menjadi lebih singkat. Suatu sistem ujian secara *online* menuntut ketersediaan data yang jelas dan akurat serta hanya dapat diakses oleh pihak yang sah. Teknik yang banyak digunakan untuk menjaga keamanan data yang tersimpan dalam sebuah sistem melalui media *internet* adalah kriptografi. Penelitian ini bertujuan untuk menghasilkan rancangan protokol yang dapat digunakan untuk mengamankan data yang terkait dengan sistem ujian *online.* Metode penelitiannya dengan melakukan analisis kebutuhan dasar keamanan dan menggunakan metode *Security Life Cycle* dari Bishop. Rancangan protokol keamanan data diimplementasikan dengan program simulasi sederhana menggunakan bahasa pemrograman *Power Builder* 10.0 Build 4500 dan *library java* dari *Java Cryptographic Extension*. Hasilnya berupa *framework* protokol keamanan data yang memenuhi kebutuhan keamanan dari Sistem Ujian *Online.*

Kata Kunci: Kriptografi, Protokol Keamanan, Sistem Ujian *Online*

PENDAHULUAN

Ujian sebagai salah satu tahapan evaluasi dalam proses belajar mengajar, memiliki peran yang sangat penting. Melalui ujian akan dapat diketahui tingkat keberhasilan dari proses belajar mengajar yang telah dilakukan tersebut. Sistem ujian konvensional dengan media kertas akan efektif dan efisien jika digunakan pada ujian dengan jumlah peserta sedikit, lokasi terpusat dan waktu yang fleksibel. Namun berlaku sebaliknya, jika dilakukan pada ujian dengan jumlah peserta sangat banyak, lokasi tersebar dan waktu yang bersamaan seperti Seleksi Penerimaan Mahasiswa Baru Perguruan Tinggi Negeri (SPMB PTN). Oleh karena itu, perlu adanya metode alternatif untuk dapat melaksanakan ujian dengan baik, cepat, akurat, dan efisien, dengan memanfaatkan teknologi informasi yang sedang berkembang saat ini. Salah satu metode alternatif tersebut adalah sistem ujian yang dilakukan secara *online* dengan menggunakan media komputer dan koneksi *internet*.

Sistem untuk ujian secara *online* tersebut menuntut ketersediaan data yang jelas dan akurat dan akan menimbulkan resiko bilamana informasi yang sensitif dan berharga tersebut diakses oleh orang-orang yang tidak berhak. Teknik yang banyak digunakan untuk menjaga keamanan data yang tersimpan dalam sebuah sistem yang menggunakan media *internet* adalah kriptografi. Kriptografi (*Cryptography)* adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan

[1] Sebagian dari Tesis, disampaikan pada Seminar Nasional FMIPA 2012 Universitas Terbuka.

aspek keamanan informasi seperti kerahasiaan, integritas data dan otentifikasi (Menezes 1996). Teknologi kriptografi sangat berperan dalam proses komunikasi, yang digunakan untuk melakukan enkripsi (pengacakan) data yang ditransaksikan selama perjalanan dari sumber ke tujuan dan dekripsi (menyusun kembali) data yang telah teracak tersebut. Keamanan jalur lalu lintas data dijaga dengan menggunakan protokol kriptografi yaitu suatu protokol yang melibatkan algoritma kriptografi. Algoritma kriptografi dapat dibedakan atas dua golongan, yaitu algoritma kriptografi simetri (contoh: DES, Blowfish, AES) dan asimetris (contoh: RSA, DSA, Elgamal). Penggunaan kriptografi pada protokol ini terutama ditujukan untuk mencegah maupun mendeteksi adanya suatu *eavesdropping* (penyadapan) dan *cheating* (kecurangan).

Suatu protokol keamanan harus memenuhi kebutuhan dasar keamanan sesuai dengan aspek-aspek kriptografi yang dibutuhkan. Aspek-aspek kriptografi tersebut menjadi kebutuhan yang tidak terelakkan dalam sebuah transaksi elektronik. Layanan keamanan yang dapat memenuhi kebutuhan sistem keamanan data adalah sebagai berikut (Menezes 1996).

1. Kerahasiaan, merupakan layanan yang digunakan untuk menjaga isi informasi dari semua yang tidak berwenang memilikinya.
2. Integritas data, merupakan layanan yang berkaitan pengubahan atau manipulasi data dari pihak-pihak yang tidak berwenang.
3. Otentikasi, merupakan layanan yang berhubungan dengan identifikasi entitas dan informasi itu sendiri. Otentikasi terbagi menjadi dua kelas besar, yaitu: otentikasi entitas dan otentikasi asal data.
4. Non-repudiasi, merupakan layanan yang ditujukan untuk mencegah terjadinya pelanggaran kesepakatan yang telah dibuat sebelumnya oleh entitas.

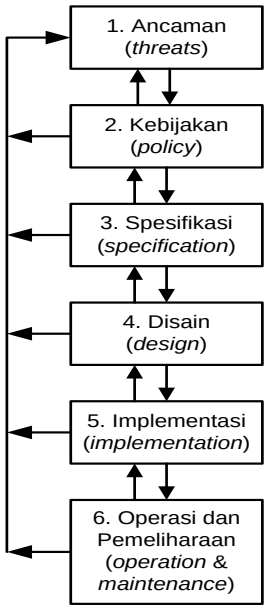
Beberapa penelitian tentang protokol keamanan data pada sistem secara *online* yang telah dilakukan, diantaranya adalah tentang keamanan data sistem *smartcard* untuk layanan kesehatan (*healthcare smartcard*) (Sariasih 1999), sistem jaringan telepon publik (Sharif 2003), serta keamanan pada pada sistem pemilu *online* (DuFeu & Harris, 2001) dan (Sireesha & Chakchai 2005). Dalam penelitian kali ini fokusnya adalah keamanan data pada transaksi elektronik untuk sistem ujian secara *online*.

Tujuan dari penelitian ini adalah untuk menghasilkan suatu rancangan protokol yang dapat digunakan untuk mengamankan data yang terkait dengan Sistem Ujian *Online* tersebut. Rancangan protokol keamanan ini diharapkan dapat digunakan untuk mengatasi masalah-masalah keamanan yang mungkin timbul, antara lain tentang kerahasiaan data, otentikasi pihak yang terlibat dalam protokol, dan kerusakan atau pencurian data. Penelitian dilakukan hanya sampai tahap perancangan

protokol dan tidak termasuk dengan pengembangan aplikasi ujian *online*. Protokol yang dihasilkan bersifat *framework* dan implementasinya akan memanfaatkan algoritma yang telah ada.

METODOLOGI

Penelitian ini dikembangkan dengan melakukan analisis kebutuhan dasar keamanan dan menggunakan metode Siklus Hidup Sistem Keamanan (*Security Life Cycle*) yang diperkenalkan oleh Bishop (2003). Metode penelitian ini terdiri atas beberapa tahap, yaitu: (1) ancaman, (2) kebijakan, (3) spesifikasi, (4) perancangan, (5) implementasi, serta (6) operasi dan pemeliharaan seperti yang ditunjukkan pada Gambar 1. Pada penelitian ini tahap akhir atau tahap operasi dan pemeliharaan ditiadakan.



Gambar 1 Siklus hidup sistem keamanan.

HASIL DAN PEMBAHASAN

Kebutuhan Dasar Keamanan

Protokol keamanan untuk pengiriman data pada Sistem Ujian *Online* (SUO) tentunya harus memenuhi kebutuhan dasar dari SUO, yang juga memenuhi aspek-aspek kriptografi seperti berikut:

1. Kerahasiaan.

   Semua data yang terkait dengan SUO yang meliputi data registrasi, soal ujian dan jawaban hasil ujian harus dijaga kerahasiaannya. Layanan kerahasiaan dilakukan dengan menerapkan protokol kriptografi yaitu enkripsi atau penyandian.

2. Otentikasi.

   Otentikasi entitas dilakukan untuk meyakinkan bahwa, baik peserta ujian (*client*) maupun *server* adalah pihak tujuan (entitas) yang benar. Adapun otentikasi data dilakukan untuk meyakinkan bahwa data registrasi, soal ujian dan jawaban hasil ujian yang diterima oleh masing-masing pihak harus merupakan data yang benar dan berasal dari pihak pengirim yang benar. Oleh karena itu, hanya pengguna yang *valid* yang dapat mengakses SUO ini. Kebutuhan otentikasi dipenuhi dengan menambahkan nonce (*number used once*) dan nilai *hash* pada kunci simetri.

3. Integritas data

   Data registrasi yang diterima oleh *server*, soal ujian yang diterima oleh mahasiswa peserta ujian (*client*) dan jawaban hasil ujian yang diterima oleh *server* harus dalam kondisi utuh dan tidak mengalami perubahan. Integritas data dijamin dengan menggunakan metode kriptografi fungsi *hash*.

4. Nir-penyangkalan

   Baik *client* maupun *server* tidak dapat menyangkal telah mengirim data yang dimaksud. Kebutuhan dasar ini dijamin dengan penggunaan tandatangan *digital*, dimana masing-masing pihak memiliki pasangan kunci yang bersesuaian.

Ancaman (*Threats*)

Protokol keamanan data pada SUO ini sangat berpotensi untuk mendapat ancaman. Ancaman-ancaman yang diperkirakan akan muncul, diantaranya adalah:

a. Penyamaran (*spoofing*) baik oleh *client* ataupun *server* yang memanfaatkan identitas orang lain. Hal yang mungkin terjadi adalah *client* mengirimkan data ke *server* yang telah menyamar menggunakan identitas *server* tujuan asli, demikian pula sebaliknya. Penyamaran juga memungkinkan terjadinya penyangkalan terhadap data yang dikirim oleh pihak tertentu. Ancaman ini akan diatasi dengan layanan otentikasi.

b. *Interception* adalah adanya pihak ketiga yang bertindak sebagai penyusup (*intruder*) berhasil membaca data yang dikirim. Ancaman ini dapat muncul pada semua proses komunikasi yang terjadi antara *client* dan *server*. Ancaman ini akan diatasi dengan layanan privasi/kerahasiaan.

c. Modifikasi (*modification*) terhadap data yang dikirim baik dari *server* ataupun oleh *client* yang dapat dilakukan oleh *client* sendiri maupun oleh pihak ketiga yang bertindak sebagai penyusup (*intruder*). Ancaman yang mungkin terjadi adalah penyerang mengubah kunci simetri/kunci sesi yang digunakan dalam proses komunikasi antara *client* dengan *server*. Hal lain yang mungkin

pula terjadi penyerang mengubah data soal atau jawaban hasil ujian yang terkirim. Ancaman ini akan diatasi dengan layanan integritas.

Kebijakan

Kebijakan keamanan adalah pernyataan atas apa yang diperbolehkan dan tidak diperbolehkan dalam menjalankan sebuah sistem. Kebijakan untuk protokol ujian *online* ini mengacu pada *secure voting requreiment*s yang dipaparkan oleh Schneier (1996).

Adapun hasil adaptasi kebijakan pada *secure voting requreiment*s yang akan diterapkan pada protokol keamanan untuk SUO meliputi 5 persyaratan berikut.

1. Hanya peserta ujian yang sah yang boleh mengikuti ujian
   - Dipenuhi dengan adanya proses registrasi. Setiap peserta ujian terlebih dahulu harus mendaftarkan dirinya agar dapat mengikuti ujian. Setelah itu peserta ujian akan mendapatkan *username* dan *password* yang menjadi bukti bahwa orang tersebut merupakan peserta ujian yang sah dan dapat mengerjakan soal ujian.
2. Peserta ujian tidak boleh mengikuti ujian lebih dari 1 (satu) kali
   - Dapat pula diartikan sebagai pencegahan peserta ujian ganda. Hal tersebut dapat dilakukan dengan terlebih dahulu melakukan pengecekan, apakah seseorang yang mendaftar sebagai peserta ujian sudah pernah mendaftarkan dirinya. Pengecekan ini dapat dilakukan pada *ID* peserta ujian.
3. Tidak ada peserta ujian yang dapat mengisi jawaban ujian peserta lain
   - Dalam hal ini digunakan saluran aman untuk mengirim *username* dan *password* secara langsung untuk setiap peserta ujian, sehingga orang lain selain peserta ujian yang dimaksud tidak akan dapat mengetahui *password* peserta ujian lain
4. Tidak boleh mengubah jawaban hasil ujian peserta lain
   - Hal ini dapat dilakukan dengan cara memberikan *validation ID* yang unik dan aman sehingga orang lain tidak dapat mengganti jawaban hasil ujian peserta lain, termasuk *server* SUO.
5. Setiap peserta dapat memastikan bahwa jawaban hasil ujian sudah terkirim dan nilainya sudah terhitung dengan benar
   - Kebijakan ini dilakukan dengan cara memberikan tampilan hasil jawaban ujian beserta nilainya yang berupa jumlah jawaban benar. Hal ini merupakan sebuah bukti bahwa jawaban hasil ujian sudah masuk dan terhitung oleh sistem.

Spesifikasi

Protokol keamanan data pada ujian *online* ini menggunakan 2 *server* yaitu *server* Registrasi dan *server* SUO. Masing-masing *server* memiliki tugas dan fungsi utama, sebagai berikut.

- ***Server* Registrasi**

  Server Registrasi merupakan *server* yang memiliki tugas utama mengotentikasi dan mengotorisasi peserta ujian (*client*) pada saat melakukan registrasi ujian.

- ***Server* SUO**

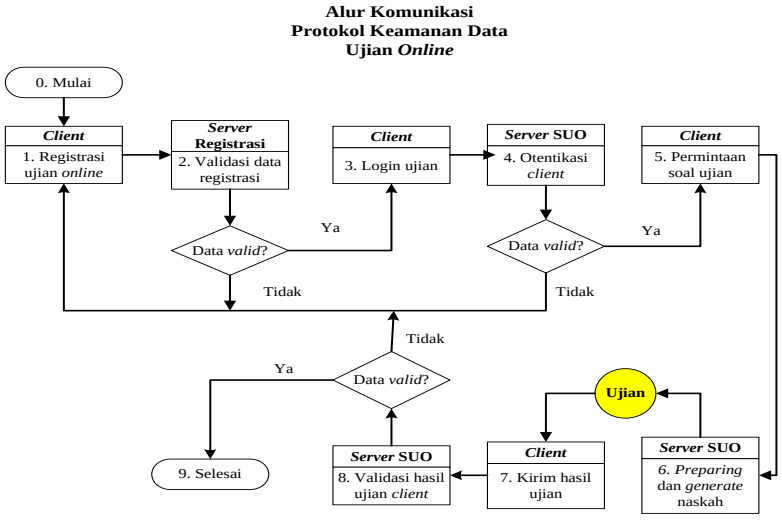
  Server SUO memiliki fungsi utama untuk melayani permintaan *login* ujian, permintaan naskah soal, dan pengiriman hasil jawaban ujian.

Secara umum sistem yang dibangun haruslah memberikan jaminan bahwa informasi yang diakses peserta ujian (*client*) adalah informasi yang benar dan akurat dan terjamin keamanannya. Oleh karena itu, sistem protokol kriptografi pada SUO membutuhkan spesifikasi sebagai berikut.

1. Pengamanan data ke *server registrasi* dan *server* SUO dengan enkripsi kunci simetri *Blowfish*.
2. Pengamanan data untuk pengiriman kunci simetri menggunakan kunci publik RSA.
3. *Server SUO* memperbolehkan peserta ujian untuk masuk/*log in* dan menjawab soal hanya boleh satu kali dengan memberikan *validation ID* untuk setiap peserta ujian.
4. Pengamanan data untuk menjaga keutuhan data dilakukan dengan menggunakan fungsi *hash SHA*-1.
5. Otentikasi dan verifikasi peserta ujian dengan penambahan nilai nounce pada kunci simetri.

Disain

Tahapan disain diawali dengan mengidentifikasi proses komunikasi data pada SUO yang dapat dilihat pada Gambar 2 berikut.



Gambar 2 Diagram alur komunikasi protokol keamanan data ujian *online*.

Disain protokol terbagi menjadi 4 bagian utama, yaitu: protokol untuk proses registrasi, protokol untuk *login* ujian, protokol untuk *generate* dan pengiriman naskah soal ujian serta protokol untuk pengiriman hasil jawaban ujian.

Alur Komunikasi Protokol Ujian *Online*

Protokol untuk ujian *online* yang akan dibuat memiliki alur komunikasi berdasarkan Gambar 3, seperti berikut.

1. Registrasi

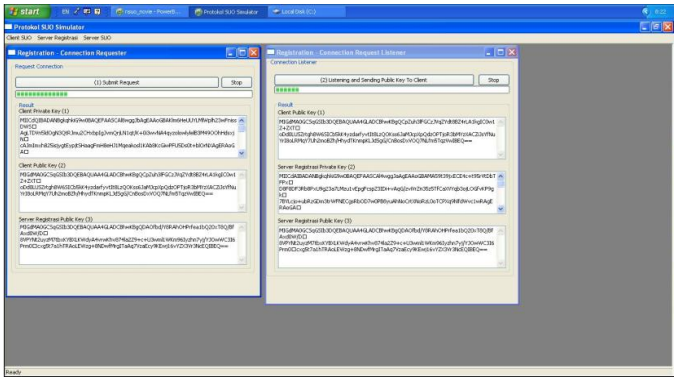
a. Mahasiswa (*client*) meminta untuk melakukan proses registrasi.
b. *Client* dan s*erver* registrasi melakukan pertukaran kunci publik.
c. *Client* memasukkan data NIM (*user name*)
d. *Client* mengirim data NIM ke *server* Registrasi dengan kunci publik.
e. *Server* Registrasi melakukan validasi terhadap data registrasi (NIM). Jika ada datanya, maka *server* akan men-*generate password*. Jika data tidak ada, maka proses registrasi akan dihentikan/mulai dari awal.
f. *Server* Registrasi mengirim NIM, beserta *nonce*+1 dan *password* yang telah dienkripsi ke *client*. NIM (*user name*) dan *password* tersebut akan digunakan sebagai identitas *client*.

2. ***Login* Ujian**
    a. *Client* melakukan proses login ujian ke *server* SUO.
    b. *Client* masuk ke sistem dengan memasukkan *username* (NIM) dan *password* kemudian dikirim ke *server* SUO.
    c. *Server* SUO melakukan otentikasi terhadap *client*. Jika *username* (NIM) dan *password* tersebut *valid*, maka *server* SUO akan membuat *validation ID*.
    d. *Server* SUO mengirim *validation ID* ke *client* untuk divalidasi. Jika *valid*, kemudian *client* bisa membuat permintaan (*request*) naskah soal ujian (*exam paper*) ke *server* SUO.
3. **Permintaan Naskah Soal Ujian (*Request Exam Paper*)**
    a. *Client* membuat permintaan (*request*) naskah soal ujian (*exam paper*) ke *server* SUO.
    b. *Client* mengirimkan pesan yang berisi permintaan naskah soal ujian (*exam paper*) kepada *server* SUO dengan kunci simetri.
    c. *Server* SUO men-*generate* naskah soal ujian (*exam paper*) dan menandatangani.
    d. *Server* SUO mengenkripsi naskah soal ujian (*exam paper*) dan mengirimkan kepada *client*.
    e. *Client* memverifikasi tanda tangan *digital* dari *server* SUO. Jika tanda tangan *valid*, *client* dapat melakukan proses ujian (melalui aplikasi ujian *online* pada *client*).
4. **Kirim Hasil Ujian**
    a. Setelah ujian selesai, *client* memberi tanda tangan *digital* pada jawaban hasil ujian dan mengirimkan ke *server* SUO.
    b. *Server* SUO melakukan validasi terhadap pesan jawaban hasil ujian yang dikirim oleh *client*. *Server* SUO memeriksa *validation ID*. Jika *valid*, maka jawaban hasil ujian akan disimpan di s*erver* SUO. Jika tidak *valid*, maka proses berhenti atau mengulang dari awal.

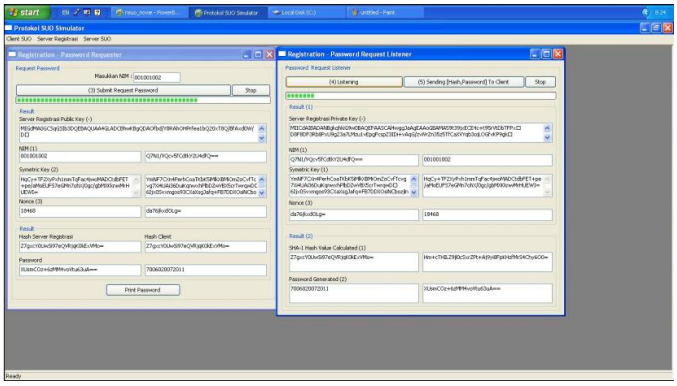
Implementasi

Implementasi dari setiap spesifikasi yang telah dibuat, dilakukan untuk mengimplementasikan disain protokol menjadi aplikasi komputer. Disain protokol diimplementasikan ke dalam aplikasi komputer pada lingkungan pengembangan dengan *OS Host*: *Linux Cent OS Release* 5.5 (Final), *Kernel* 2.6.18-194.32.1 el5.on an X86-64, *OS Guest*: *Microsoft Windows XP Profesional* Versi 2002 *Service Pack* 3, bahasa pemrograman *Power Builder* 10.0 Build 4500 dan *library java* dari *Java Cryptographic Extension* (Weiss 2003).

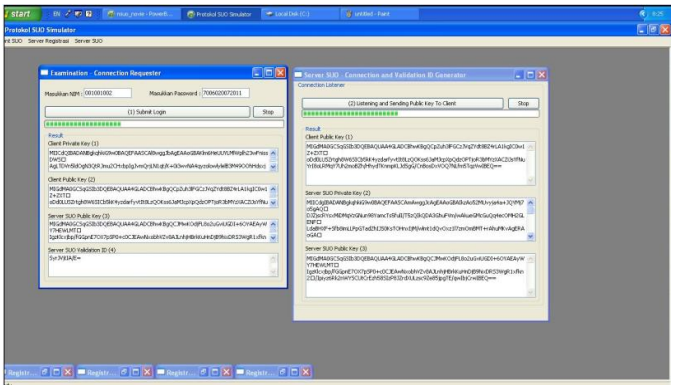
Hasil implementasi dibuat dalam bentuk simulasi sistem kerja protokol, berdasarkan 4 bagian utama dari desain protokol.



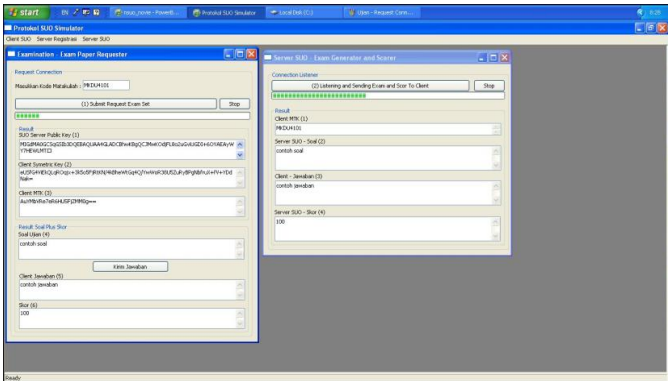
Gambar 3
Tampilan proses registrasi.



Gambar 4
Tampilan proses *login* ujian.



Gambar 5
Tampilan proses *generate* dan pengiriman naskah soal.



Gambar 6
Tampilan proses pengiriman hasil jawaban ujian.

KESIMPULAN

Kesimpulan.

Berdasarkan hasil penelitian dan pembahasan, dapat diambil kesimpulan:

1 Dalam penelitian ini telah dihasilkan *framework* protokol keamanan data pada Sistem Ujian *Online* (SUO).

2 Protokol keamanan pengiriman data untuk ujian *online* telah dirancang dengan menerapkan layanan keamanan dan aspek-aspek kriptografi sesuai kebutuhan keamanan.

3 Berdasarkan hasil simulasi pada aplikasi implementasi, protokol mampu memenuhi kebutuhan keamanan dari SUO dan dapat digunakan untuk menghasilkan suatu SUO yang terjamin keamanannya.

4 Keamanan protokol sangat tergantung pada algoritma kriptografi yang digunakan.

Saran.

1 Perancangan protokol masih bersifat *framework* dengan menggunakan algoritma kriptografi yang telah ada, untuk itu dikembangkan penelitian dengan menggunakan algoritma protokol yang lebih baru dan terjamin keamanannya.

2 Perlu dikembangkan simulasi dengan penggunaan kunci yang lebih panjang agar lebih sulit untuk dipecahkan.

3 Perlu pengembangan penelitian yang lebih lengkap dengan menyertakan aplikasi untuk proses ujian.

DAFTAR PUSTAKA

Bishop, M., 2003. *Computer Security*, Addisson-Wesley. Boston.

DuFeu D, Harris J. 2001. *Online Election System*. Carleton University

Menezes AJ, Oorshot PC van, Vanstone, SA.1996. *Handbook of Applied Cryptography*, CRC Press

Neyman, S. N., 2007. *Perancangan Protokol Penyembunyian Informasi Terotentikasi*, Thesis, S2 Ilmu Komputer, Institiut Pertanian Bogor, Bogor.

Sariasih, C., 1999. *Rancangan Keamanan Data Sistem Smartcard Kesehatan Sesuai Kebutuhan di Indonesia*. Skripsi. Fakutas Ilmu Komputer - UI. Jakarta.

Schneier, B., 1996. *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C*, Wiley Computer Publishing,, Jon Wiley & Sons.

Sharif, M., Wijesekera, D., 2003. *Providing Voice Privacy Over Public Switched Telephone Networks*, In: Proc. of 18th International Conference on Information Security (SEC 2003), May 26-28, 2003, Athens, Greece.

Sireesha J, Chakchai S. 2005. *Secure Virtual Election Booth with Two Central Facilities*, Department of Computer Science Washington University in St. Louis, USA.

Stallings, W., 2003. *Cryptography and Network Security: Principles and Practices*, 3rd edition, Pearson Education International.

Sybase, Inc, 2004. *Using Cryptography in Power Builder 10.0*, White Paper, Power Builder Engineering, Information Technology and Solutions Group, Dublin, California.

Weiss, J., 2004. *Java Cryptography Extensions: Practical Guide for Programmers*, Morgan Kaufmahn.