PENGGUNAAN KRIPTOGRAFI PADA ELECTRONIC VOTING

Meliza T.M.Silalahi

Program Studi Teknik Informatika Institut Teknologi Bandung
Ganesha 10, Bandung
if16116@students.if.itb.ac.id

ABSTRAK

Dewasa ini penggunaan *electronic voting* dalam dalam suatu pemilihan sudah biasa diterapkan. Namun pada kenyataannya masih banyak permasalahan yang terjadi, baik dari sisi keamanan, kerahasiaan, demokrasi--hanya boleh memilih satu kali, dan permasalahan lainnya. Kriptografi sebagai ilmu dan seni mengamankan pesan menawarkan solusi atas permasalahan terkait *electronic voting.*

Makalah ini membahas penawaran solusi berupa penggunaan kriptografi atas permasalahan pada *electronic voting*. Fokus permasalahan yang dibahas adalah keamanan suara dan kerahasiaan pemilih. Kriptografi yang digunakan adalah Paillier Cryptosystem dan Dining Cryptographer Protocol. Paillier Cryptosystem digunakan untuk mengamankan pesan suara pemilih, sedang Dining Cryptographer Protocol digunakan untuk merahasiakan identitas pemilih. Pada makalah ini dihadirkan sumbangsi pemikiran baru terkait kombinasi Paillier Cryptosystem dan Dining Cryptographer Protocol pada *electronic voting*.

Kata kunci : Electronic Voting, Paillier Cryptosystem, Dining Cryptographer Protocol, Diffie-Hellman, keamanan, kerahasiaan.

1. PENDAHULUAN

Electronic Voting, merupakan pemungutan suara yang dilakukan melalui alat elektronik. Alat elektronik yang digunakan beragam, di antaranya berupa *handphone, private computer network, direct electronic (DRE) voting system*, internet serta alat berteknologi lainnya. Manfaat yang dirasa dalam penggunaaan *electronic voting* antara lain: menghemat kertas suara, dan menghemat waktu serta tenaga karena dapat menghitung hasil pemilihan secara otomatis.

Electronic voting sudah diterapkan di berbagai negara seperti: Australia, Belgia, Brazil, Kanada, Estonia, Perancis, Jerman, India, Irlandia, Itali, Belanda, Norwegia, Romania, Swiss, dan Inggris. Meskipun demikian di beberapa negara seperti di Amerika Serikat, *electronic voting* dianggap masih sangat rawan terhadap gangguan dari pihak–pihak yang mempunyai maksud tertentu [COU05]. Salah satu hal yang dapat dianggap rawan adalah sisi keamanan. Saat menggunakan *electronic voting,* suara dapat dimanipulasi oleh pihak-pihak yang tidak bertanggungjawab, sudah pasti hasil yang diperoleh juga tidak sesuai dengan yang seharusnya. Satu hal lagi yang juga menjadi penting dalam pemungutan suara adalah kerahasiaan pemilih. Penggunaan *electronic voting* seharusnya menjamin kerahasiaan pemilih, dalam hal ini pemilih tidak dapat ditelusuri.

Salah satu cara mencegah atau menghindari kejahatan dunia maya (*cybercrime*) adalah dengan meningkatkan keamanan sehingga para pelaku kejahatan tidak memiliki celah untuk melakukan manipulasi. Ada satu bidang ilmu yang telah menjadi dasar untuk memahami keamanan pada komputer (khususnya keamanan jaringan), yaitu kriptografi. Kriptografi sudah digunakan hampir di segala bidang yang terkait dengan penggunaan jaringan komputer. Bahkan kehidupan kita saat ini dilingkupi oleh kriptografi, mulai dari transaksi mesin di ATM, bank, kartu kredit, percakapan di telepon genggam, mengakses internet, dan banyak lagi. Begitu pentingnya kriptografi untuk keamanan informasi sehingga jika berbicara mengenai masalah keamanan yang berkaitan dengan penggunaan komputer, maka orang tidak bisa memisahkannya dengan kriptografi [MUN06].

Cukup banyak metode yang terdapat dalam kriptografi, terntunya tergantung pada persoalan yang dihadapi. Untuk masalah keamanan dan

kerahasiaan pada *electronic voting* ini, dibahas dengan kombinasi penggunaan *Paillier Cryprosystem* dan *Dining Cryptographers Protocol.*

Makalah ini membahas solusi yang ditawarkan, yaitu berupa kombinasi *Paillier Cryprosystem* dan *Dining Cryptographers Protocol* diharapkan dapat mengatasi masalah keamanan dan kerahasiaan yang telah dibahas sebelumnya. *Paillier Cryprosystem* akan melindungi suara pemilih sehingga tidak dapat dimanipulasi (*enkripsi)* serta dapat menghitung secara otomatis jumlah suara. Dan dengan mengkombinasikannya dengan *Dining Cryptographers Protocol*, kerahasiaan pemilih akan terjamin, karena dengan protocol ini, tidak akan dapat dilacak siapa memilih siapa atau dengan kata lain, identitas pemilih tidak akan diketahui.

2. ELECTRONIC VOTING

Dalam penggunaannya, *electronic voting* masih memiliki banyak permasalahan. Berikut akan dipaparkan sebagian kecil permasalahan terkait. Laporan hasil penelitian Ohio (2007) : ditemukan permasalahan yang dapat mengancam integritas suara pada pemilu 2008. sistem e-voting di Ohio, yang berbasiskan komputer, tidak sesuai dengan standard keamanan komputer yang ada dan mudah di sadap. Hal ini mengancam integritas proses pemilihan. California (2006) : ditemukan bahwa tombol kuning pada Sequoia,suatu mesin e-voting mengizinkan satu orang memilih lebih dari satu kali. Venezuela (2006) : Isu Hugo Chavez, Presiden Venezuela, memiliki hubungan dengan Sequoia dan kepemilikan atas Smartmatic, perusahaan mesin e-voting yang digunakan saat pemilihan umum presiden Venezuela. Ditemukan pula magnet dan PDA dapat digunakan untuk mengubah suara pada mesin *voting* layar sentuh.

Kenyataan yang ada di lapangan tidak sesuai dengan properti yang seharusnya dimiliki oleh *electronic voting.* Para peneliti di bidang *electronic voting* menyepakati empat properti yang harus dimiliki oleh sistem *electronic voting* [CRA97]. Pertama akurasi. Suatu sistem *electronic voting* dikatakan akurat apabila suara tidak berubah dari suara asal, suara sah tidak dieliminasi dari perhitungan akhir, dan suara tidak sah tidak masuk dalam perhitungan akhir. Kedua adalah demokrasi. Suatu sistem *electronic voting* dikatakan demokrasi apabila hanya yang memenuhi syarat menjadi pemilih yang dapat memilih dan menjamin pemilih hanya dapat memilih satu kali. Ketiga adalah rahasia. Suatu sistem *electronic voting* dikatakan rahasia apabila tidak ada pihak berwenang ataupun pihak lainnya yang dapat memastikan siapa pemilih dari suatu surat suara dan tidak ada pemilih yang dapat membuktikan bahwa dia sudah memilih suatu kandidat tertentu. Faktor kerahasiaan yang kedua dinilai penting untuk mencegah pembelian suara. Pemilih dapat menjual suara mereka jika mampu membuktikan kepada pembeli suara.Keempat adalah terbukti. Suatu sistem *electronic voting* dikatakan terbukti apabila tiap orang dapat membuktikan bahwa semua suara telah dihitung dengan benar.

3. PENGGUNAAN KRIPTOGRAFI

Ketika bertukar pesan dengan orang lain, tentunya pesan yang dikirimkan sampai kepada pihak yang ditujukan dengan aman. Aman berarti selama pengiriman pesan, pesan tersebut tidak dibaca oleh orang yang tidak berhak. Akan berbahaya jika pesan tersebut adalah rahasia. Ini adalah masalah keamanan pesan yang dinamakan kerahasiaan (*confidentiality* atau *privacy*). Aman juga berarti pesan yang disampaikan untuh ke tangan penerima. Tidak ada isi pesan yang diubah atau dimanipulasi oleh pihak ketiga. Ini adalah masalah keamanan pesan yang dinamakan integritas data (*data integrity*). Selain itu, penerima yakin bahwa pesan yang dikirim tersebut berasal dari pengirim asli, begitu juga sebaliknya, si pengirim yakin bahwa yang menerima adalah penerima yang sesungguhnya. Ini adalah masalah kemanan pesan yang dinamakan otentikasi (*authentication*). Sebagai penerima pesan, tidak ingin sang pengirim pesan membantah pernah mengirim pesan kepada penerima. Ini adalah masalah keamanan pesan yang dinamakan penyangkalan (*repudiation*).
Keempat masalah keamanan di atas, yaitu kerahasiaan, integritas data, otentikasi dan penyangkalan dapat diselesaikan dengan menggunakan kriptografi. Kriptografi tidak hanya menyediakan alat untuk keamanan pesan, tetapi juga sekumpulan teknik yang berguna dalam menjawab berbagai permasalahan yang ada [MUN06].

Pada makalah ini dibahas dua teknik kriptogafi dan sumbangsi pemikiran baru terkait kombinasi kedua teknik tersebut untuk menjawab permasalahan keamanan dan kerahasiaan pada *electronic voting* (seperti yang sudah disebut sebelumnya).

3.1 PAILLIER CRYPTOSYSTEM

Paillier Cryptosystem pertama sekali dikemukakan oleh Pascal Paillier pada tahun 1999. Kriptosistem ini menyediakan enkripsi yang aman, dekripsi yang efisien, dan homomorfik adiktif dari perkalian cipherteks [PAI99-a, PAI99-b]. Skemanya terdiri atas tiga bagian utama, yaitu pembangkitan kunci (*key generation*) , enkripsi pesan (*encryption*) dan

dekripsi chiperteks (*decryption*) [PAI99-a, PAI99-b,ADI97].

Penjelasan skema sebagai berikut:

- Pembangkitan kunci, Gen (1^k) : membangkitkan dua bilangan aman prima p_1 dan p_2. Kunci privat *sk* diperoleh dari $\lambda = KPK\ (p_1 - 1\ , p_2 - 1)$

Kunci publik *pk* diperoleh dari $n = p_1\, p_2$ dan $g \in \mathbb{Z}_{n^2}$ di mana $g \equiv 1\ mod\ n$; seringkali terjadi $g = n + 1$.

- Enkripsi, $Enc_{pk}(m; r)$: enkripsi pesan m Z_n dengan bilangan random r , dimana $r \in \mathbb{Z}_n^*$ dan kunci publik *pk* sebagai c.
$$c = g^m\, r^n\ mod\ n^2$$

- Dekripsi, $Dec_{sk}(c)$: dekripsi chiperteks c dimana $c \in \mathbb{Z}_{n^2}^*$

$$Dec_{sk}(c) = \frac{L\left(c^\lambda\ mod\ n^2\right)}{L(g^\lambda\ mod\ n^2)}\ \ mod\ n$$

dengan $L(x) = (x - 1)/n$

Untuk pembuktian dan penjelasan lebih detail mengenai skema ini dapat ditemukan pada [PAI99-a, PAI99-b].
Hasil dekripsi dari perkalian pesan-pesan yang dienkripsi akan menghasilkan jumlah chiperteks yang terkait. Sifat ini dikenal dengan homomorfik adiktif. Praktisnya adalah sebagai berikut:

$$Dec_{sk}\left(Enc_{pk}\ (m1) Enc_{pk}\ (m2)\ mod\ n^2\right) = m_1 + m_2\ mod\ n$$

$$Dec_{sk}\left(Enc_{pk}\ (m)^k\right)\ mod\ n^2 = km\ mod\ n$$

$$Dec_{sk}\left(Enc_{pk}\ g^{m_2}\ mod\ n^2\right) = m_1 + m_2\ mod\ n$$

Sifat homomorfik adiktif ini berguna pada perancangan protokol pemilihan (*voting*), batas ambang kriptosistem (threshold cryptosystem), watermarking dan skema pembagian rahasia [PAI99].

Berikut adalah kajian terkait yang mengimplementasikan konsep *Paillier Cryptosystem*. Ben Adida dan Ronald L. Rivest [ADI97] mengemukakan '*Scratch & Vote*', sistem pemilihan (*voting*) yang menggunakan kriptografi dengan biaya yang murah dan kompleksitas yang minimal. Surat suara berbasiskan kertas (*paper-based*) dan terverifikasi tanpa campur tangan dari panitia pelaksana pemilihan. Perhitungan suara menggunakan kelebihan sifat adiktif homomorfik dari sistem kriptografi seperti Paillier.

3.2 DINING CRYPTOGRAPHERS PROTOCOL

David Chaum ialah orang yang pertama menuliskan artikel mengenai metode yang menjamin pengirim dan penerima pesan anonim pada suatu kelompok. Artikel yang dibuat pada "*Journal of Cryptology*" ini dinamakan *Dining Cryptographers Problem* (Masalah Jamuan Makan Malam para Kriptografer), sesuai dengan contoh yang digunakan oleh Chaum pada artikel tersebut [SCH90].

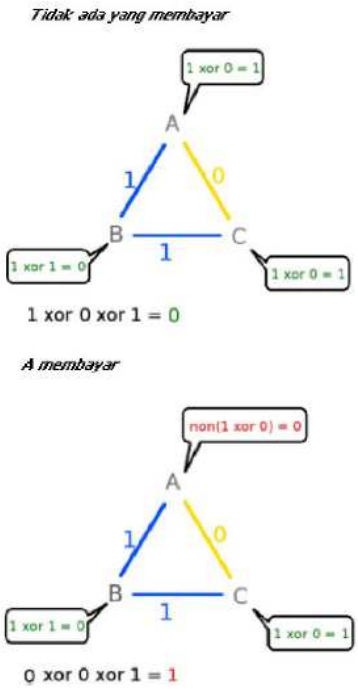
Adapun contoh yang digunakan Chaum dalam menjelaskan permasalahan jamuan makan malam para kriptografer adalah sebagai berikut [CHA88]:
Tiga orang kriptografer sedang berada pada jamuan makan malam di restoran berbintang tiga kesukaan mereka. Pelayan kemudian memberitahu mereka kalau makanan mereka telah dibayar sebelumnya oleh seseorang yang tidak ingin diketahui. Salah satu kriptografer memiliki kemungkinan membayar makan malam tersebut, atau kemungkinan lain si pembayar adalah agen keamanan Amerika (*U.S.National Security Agency / NSA*). Ketiga kriptografer menghormati pembayar yang tidak ingin diketahui tersebut, tapi mereka meragukan apakah NSA yang membayar.

Kemudian, merekapun menyelesaikan ketidakpastian mereka dengan cara yang adil melalui protokol berikut ini :

Tiap kriptografer melempar koin di bawah meja agar tidak tidak terlihat dengan yang lain. Hanya dia dan orang yang berada di sisi sebelah kanannya saja yang dapat melihat hasil lemparan koin. Masing-masing kriptografer kemudian menyatakan kedua koin yang dilihatnya –satu yang dilemparkan olehnya sendiri dan satu lagi lemparan koin dari tetangga sebelah kirinya- menyatakan apakah kedua koin yang dilihatnya 'sama' atau 'berbeda'. Jika ternyata pembayar adalah salah satu dari mereka , demi menjaga kerahasiaanya, si pembayar harus berbohong dan menyatakan kebalikannya. Setelah semua kriptogafer menyatakan 'sama' ataupun 'berbeda', pernyataan 'berbeda'dijumlahkan.

Jika jumlahnya ganjil berarti si pembayar adalah salah satu kriptografer, sedangkan jika jumlahnya genap berarti si pembayar adalah NSA. Jikalaupun si pembayar adalah salah satu dari kriptografer, tetap saja kedua kriptografer lainnya tidak bisa belajar ataupun menyimpulkan apa-apa siapa kriptografer yang berbohong dengan pernyataannya mana yang tidak.

Ilustrasi di atas dapat digambarkan sebagai berikut:



Gambar 1 Ilustrasi Dining Cryptographer Protocol

Tiap kriptografer menukarkan sebuah kunci rahasia dengan kriptografer lain melalui lemparan koin di bawah meja (rahasia). Kemudian ketiganya mengumumkan jumlah dari lemparan koin, kecuali yang si pemayar. Si pembayar harus menambahkan pesannya dengan mengumumkan kebalikan jumlah koinnya. Setelah semua kriptografer menjumlahkan jumlah mereka, keseluruhan jumlah tersebut dijumlah. Jika tidak ada yang membayar maka jumlahnya akan bernilai 0, sehingga makan malam tersebut dibayar oleh NSA.

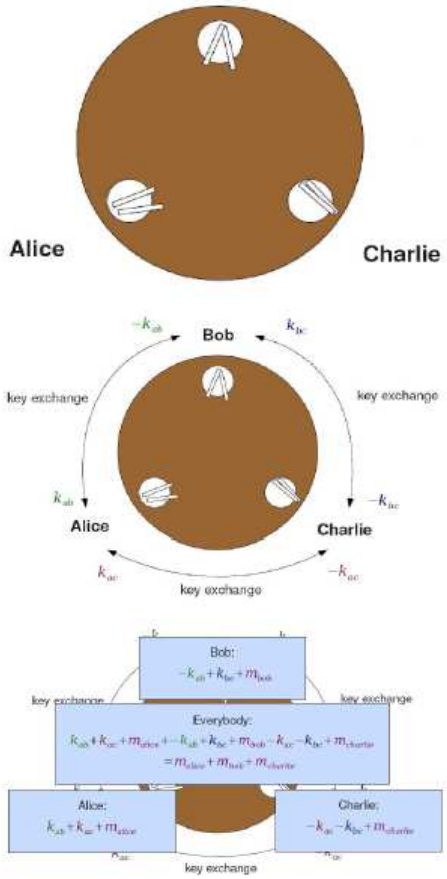
Berikut adalah langkah-langkah membangun *Dining cryptographer network* [SCH90] :

1. Tukarkan kunci simetrik dengan partisipan lain. Contohnya pertukaran kunci antara Alice dan Bob (k_{ab}) , antara Alice dan Charlie (k_{ac}) dan antara Bob dan Charlie (k_{bc}) . Masing-masing dari partisipan juga mendapatkan kebalikan kunci dengan yang lainnya, misalkan ketika Alice memiliki kunci k_{ab} , Bob memiliki - k_{ab}

2. Para partisipan menjumlahkan kunci mereka dan menambahkan pesan mereka untuk dijumlahkan. Alice akan menjumlahkan $k_{ab} + k_{ac} + m_{alice}$, Bob menjumlahkan $-k_{ab} + k_{bc} + m_{bob}$ dan Charlie $-k_{ab} - k_{ac} + m_{charlie}$.
3. Keseluruhan nilai yang diumumkan oleh tiap partisipan dijumlahkan kembali, sehingga didapatkan pesan yang ingin disampaikan oleh partisipan.

$$k_{ab} + k_{ac} + m_{alice} - k_{ab} + k_{bc} + m_{bob} - k_{ac} - k_{bc} + m_{charlie} = m_{alice} + m_{bob} + m_{charlie}$$

Lebih jelasnya dapat dilihat pada gambar di bawah ini.



Gambar 2 Dining Cryptographer Protocol

Sebaiknya hanya satu partisipan yang mengirim sebuah pesan dalam satu waktu agar tidak mengacaukan pesan lainnya [CHA88].

Jika jumlah partisipannya lebih dari tiga orang, maka tidak harus masing-masing partisipan menukarkan kuncinya dengan yang lain, tetapi tidak ada salahnya juga jika melakukan hal tersebut.

4. KOMBINASI PAILLIER CRYPTOSYSTEM DAN DINING CRYPTOGRAPHERS PROTOCOL

Dari hasil analisis terhadap Paillier Cryptosystem dan Dining Cryptographer Protocol dapat dirumuskan kombinasi langkah-langkah sebagai berikut:

1. Pembangkitan kunci.
   Kunci yang dibangkitkan adalah kunci privat dan kunci publik yang akan

digunakan pada enkripsi pesan. Pembangkitan kunci ini sendiri merupakan bagian dari Paillier Cryptosystem.

2. Enkripsi pesan
Pesan suara kemudian dienkripsi dengan menggunakan kunci publik. Enkripsi ini juga merupakan bagian dari Paillier Cryptosystem.

3. Tiap pemilih menukarkan kunci publiknya dengan pemilih lain.
Pada tahap ini, penukaran kunci merupakan bagian dari Dining Cryptographer Protocol. Masing-masing partisipan akan menukarkan kunci simetrik dengan partisipan lainnya. Protokol yang digunakan adalah protokol Diffie-Hellman.

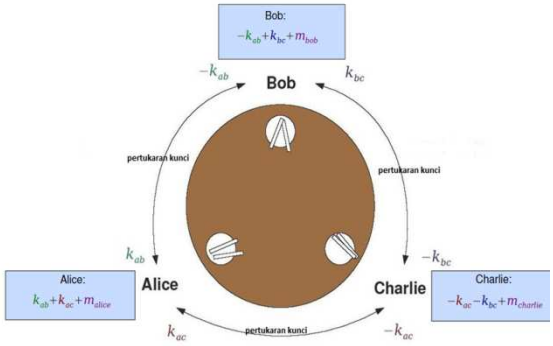
Algoritma ini untuk mempertukarkan kunci sesi (kunci rahasia untuk komunikasi kriptografi simetri) antara dua orang atau lebih. Keamanan algoritma ditentukan oleh sulitnya menghitung logaritma diskrit.

Sebagai contoh, pertukaran kunci antara Alice dan Bob. Mula-mula Alice dan Bob menyepakati dua buah bilangan prima yang besar, n dan g, sedemikian sehingga g < n. Nilai n dan g tidak perlu rahasia.
Langkah-langkah algoritma Diffie-Hellman adalah sebagai berikut:

i. Alice membangkitkan bilangan bulat acak yang besar x dan mengirimkan hasil perhitungan berikut kepada Bob:
$$X = g^x mod\ n$$
ii. Bob membangkitkan bilangan bulat acak yang besar y dan mengirimkan hasil perhitungan berikut kepada Alice:
$$Y = g^y mod\ n$$
iii. Alice menghitung
$$K = Y^X mod\ n$$
iv. Bob menghitung
$$K' = X^Y mod\ n$$

Bila perhitungan dilakukan dengan benar maka $K = K'$. Kunci simetri berhasil diterima oleh kedua belah pihak. Baik K dan K' sama dengan $g^y mod\ n$.

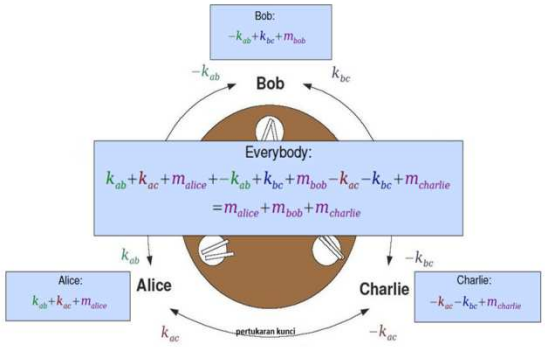
4. Tiap pemilih menjumlahkan kunci dan pesan suara yang dimilikinya.



Gambar 3 Penjumlahan Kunci dan Pesan

Para partisipan menjumlahkan kunci mereka dan menambahkan pesan mereka untuk dijumlahkan. Alice akan menjumlahkan $k_{ab} + k_{ac} + m_{alice}$, Bob menjumlahkan $-k_{ab} + k_{bc} + m_{bob}$ dan Charlie $-k_{ab} - k_{ac} + m_{charlie}$

5. Keseluruhan kunci dan pesan yang dimiliki pemilih dijumlahkan, sehingga diperoleh hanyalah pesan-pesan suara



Gambar 4 Keseluruhan Pesan

Langkah empat dan lima merupakan bagian dari Dining Cryptographer Protocol.

Pesan keseluruhan adalah :
$$k_{ab} + k_{ac} + m_{alice} - k_{ab} + k_{bc} + m_{bob} - k_{ac} - k_{bc} + m_{charlie} = m_{alice} + m_{bob} + m_{charlie}$$

Karena hanya satu partisipan yang sebaiknya mengirim sebuah pesan dalam satu waktu agar tidak mengacaukan pesan lainnya [CHA88], maka akan waktu pengiriman pesan akan diatur sedemikian sehingga tidak ada pesan yang dikirimkan dalam satu waktu dan mengacaukan pesan lainnya.

6. Perhitungan suara
Suara akhir masing-masing kandidat dihitung dengan memanfaatkan sifat Homomorfik Adiktif yang dimiliki oleh Paillier Cryptosystem.

Dekripsi dari perkalian enkripsi pesan-pesan akan menghasilkan jumlah pesan tersebut. Dengan ini, jumlah suara masing-masing kandidat dapat langsung dihitung tanpa mendekripsi suara satu per satu.

5. KESIMPULAN

Berdasarkan hasil analisis penggunaan kriptografi pada *electronic voting,* dapat disimpulkan sebagai berikut:

1. Kriptografi sebagai ilmu dan seni mengamankan pesan mampu menawarkan solusi pada permasalahan electronic voting—dalam hal ini terkait permasalahan keamanan dan kerahasiaan.

2. Paillier Cryptosystem terbukti dapat mengamankan pesan. Telah dilakukan pengujian juga terhadap kebenaran dari sifat homomorfik adiktif yang dimiliki Paillier dimana dekripsi dari enkripsi perkalian pesan-pesan akan menghasilkan jumlah pesan-pesan tersebut. Hasil pengujiannya menyatakan bahwa sifat ini benar adanya.

3. Pertukaran kunci simetrik (salah satu langkah pada Dining Cryptographer Protocol) dapat dilakukan dengan menggunakan algoritma Diffie-Hellman.

4. Sejauh ini kombinasi Paillier Cryptosystem dan Dining Cryptographer Protocol masih belum dapat diuji kinerjanya karena masih dalam tahap pengerjaan. Pada makalah ini hanya dipaparkan idenya saja. Implementasinya sedang dikerjakan oleh penulis dalam Tugas Akhir.

DAFTAR PUSTAKA

[MUN06] Munir , Rinaldi .2006. Kriptografi . Bandung : Informatika.

[CHA88] Chaum, David. 1988. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability

[PAI99-a] Paillier's Cryptosystem *http://www.ippari.unict.it/~catalano/Corsi/Tesi-Cap3-Paillier.pdf*
Waktu akses : September 2009

[PAI99-b] Paillier, Pascal. 1999. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes.

[COU05] Countries with e-voting projects http://aceproject.org/ace-en/focus/e-voting/countries/
Waktu akses : Oktober 2009

[ADI97] Adida, Ben & Rivest, Ronald L. 1997. Scratch & Vote Self-Contained Paper-Based Cryptographic Voting.

[SCH90] Scholz, Immanuel. 1990. Dining Cryptographers-The Protocol.

[CRA97] Cranor, Lorrie F & Cytron, Ron K. 1997. Sensus : A Security-Conscious Electronic Polling System for Internet.

Tugas Akhir Kombinasi Paillier Cryptosystem dan Dining Cryptographer Protovol dengan Studi Kasus Electronic Voting (Meliza, 2010 ,sedang dikerjakan)

PENYATAAN

Dengan ini saya menyatakan bahwa makalah ini tidak mengandung plagiasi.

Meliza Silalahi