Protokol Kriptografi pada Sistem Pemungutan dan Perhitungan Suara Elektronik

Drestanto M. Dyasputro
Program Studi Teknik Informatika
Institut Teknologi Bandung
Jl. Ganesha 10 Bandung 40132, Indonesia
dyas@live.com

***Abstrak*—Protokol kriptografi adalah aturan yang berisi rangkaian langkah-langkah, yang melibatkan dua atau lebih orang, yang dibuat untuk menyelesaikan suatu kegiatan dan menggunakan kriptografi pada langkah-langkahnya. Protokol kriptografi dibuat untuk menjamin kerahasiaan dan kebenaran data dan infromasi. Salah satu protokol kriptografi yang bisa bermanfaat adalah sistem pemungutan dan perhitungan suara elektronik. Protokol ini melibatkan banyak orang dan harus menggabungkan berbagai protokol kriptografi. Protokol ini berkaitan dari mulai pemilih memberikan suaranya hingga akhir dari perhitungan suara.**

Kata kunci—protokol; pemungutan suara; perhitungan suara; kriptografi

I. Latar Belakang

Kriptografi adalah suatu ilmu yang menjaga kerahasiaan pesan dengan mentranslasikan pesan menjadi bentuk yang terlihat tidak bermakna. Ilmu ini sudah ada dan digunakan sejak zaman Mesir kuno dan terus berkembang hingga sekarang. Saat ini, kriptografi banyak digunakan misalnya untuk mengamankan pengiriman pesan, sistem pengamanan gedung, atau bahkan untuk mengamankan telepon seluler.

Pada awal kemunculannya, kriptografi hanya digunakan untuk mengenkripsi pesan sehingga tidak dapat dibaca oleh pihak lain. Namun, seiring dengan perkembangannya, kriptografi juga memberikan aspek-aspek keamanan yang lain, yaitu kerahasiaan (*security*), integritas data (*integrity*), otentikasi (*authenticity*), dan nirpenyangkalan (*non-repudiation*). Ilmu kriptografi pun tersu berkembang hingga terbentuk algoritma-algoritma modern.

Dengan berkembangnya sistem kriptografi dalam hal pengiriman pesan, kriptografi pun menghasilkan ilmu-ilmu lain yang penting yaitu kriptanalisis, steganografi, *watermark*, maupun *digital signature*. Dengan berkembangnya ilmu-ilmu ini semakin luas, maka berbagai tahapan yang ada pada dunia nyata dan berkaitan dengan kerahasiaan dapat dibentuk pula skema standarnya dalam hal kriptografi.

Aturan yang berisi rangkaian langkah-langkah, yang melibatkan dua atau lebih orang, dan dialamnya memiliki aspek-aspek kriptografi yang ada (rahasia, integritas, otentikasi, dan nirpenyangkalan) disebut dengan protokol kriptografi. Protokol-protokol yang umum dalam kriptografi adalah protokol pertukaran kunci, *point to point protocol*, protokol kunci publik, dan lain-lain.

Makalah ini akan membahas tentang sebuah protokol kriptografi spesifik dan dibutuhkan saat ini yaitu protokol kriptografi pada sistem pemungutan dan perhitungan suara elektronik. Protokol ini memiliki asas rahasia dan asas langsung sehingga harus menggunakan protokol kriptografi yang tergabung atas protokol-protokol sederhana lainnya.

II. Dasar Teori

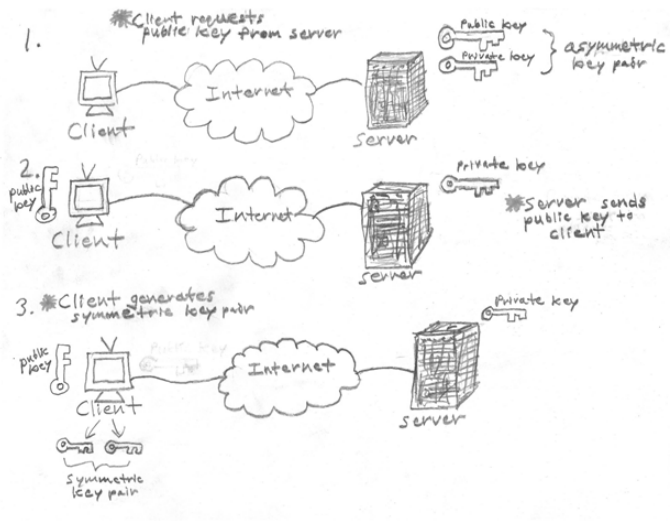
A. Protokol Kriptografi

Protokol adalah aturan yang berisi rangkaian langkah-langkah, yang melibatkan dua atau lebih orang, yang dibuat untuk menyelesaikan suatu kegiatan. Protokol kriptografi adalah protokol yang menggunakan kriptografi untuk kerahasiaan, integritas, otentikasi, maupun nirpenyangkalan.

Setiap protokol kriptografi pasti melibatkan dua atau lebih pihak (bisa berupa orang, mesin, sistem, dll). Protokol ini dibangun dengan melibatkan beberapa algoritma atau skema kriptografi. Fungsi protokol bisa bermacam-macam. Berbagi pesan rahasia, pertukaran kunci, otentikasi identitas adalah contoh-contoh protokol yang membutuhkan kriptografi.

Simulasi sebuah protokol kriptografi biasanya menggunakan nama-nama berikut ini :

- Alice : pihak pertama (dalam semua protokol)
- Bob : pihak kedua (dalam semua protokol)
- Carol : pihak ketiga dalam protokol tiga atau empat orang
- Dave : pihak keempat dalam protokol empat orang
- Eve : pihak penyadap (*eavesdropper*)
- Trent : juru penengah (*arbitrator*) yang dipercaya



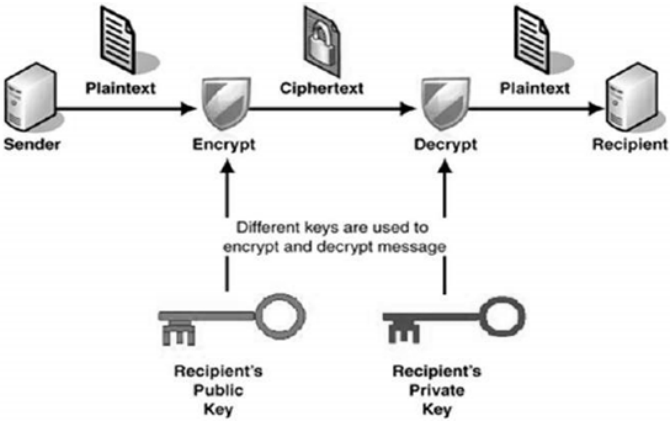
Gambar 1 : Contoh protokol kriptografi *client-server* internet

Sumber gambar : security.stackexchange.com

B. Algoritma Kriptografi Kunci Publik

Pada mulanya, algoritma kriptografi yang berkembang adalah algoritma kriptografi kunci simetri di mana pengirim dan penerima harus memiliki kunci yang sama untuk enkripsi dan dekripsi. Muncul permasalahan, yaitu bagaimana cara mengirimkan kunci ini tanpa diketahui orang lain. Karena masalah ini, ditemukanlah suatu bentuk algoritma kriptografi lain yaitu algoritma kriptografi kunci publik.

Ide kriptografi kunci asimetri muncul pada tahun 1976 oleh Diffie-Hellman. Idenya adalah, pengirim dan penerima tidak perlu menyepakati sebuah kunci bersama. Pengirim melakukan enkripsi dengan kunci publik. Kunci ini dapat diketahui oleh semua orang. Namun, kunci publik ini tidak dapat melakukan dekripsi pesan tersebut. Pesan harus didekripsi dengan menggunakan kunci privat yang dimiliki hanya oleh penerima.



Gambar 2 : Skema algoritma kriptografi kunci publik

Sumber gambar : www.tutorialspoint.com

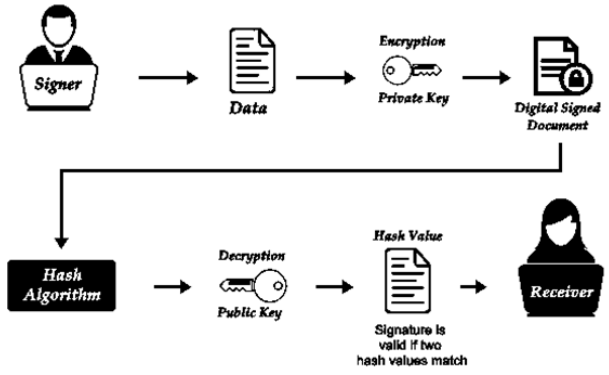
Misalnya, Alice menjadi pengirim dan Bob menjadi penerima. Pertama-tama, Bob akan memberikan kunci publik (kunci ini diketahui oleh siapapun) *pub*. Alice akan melakukan enkripsi dengan kunci publik dan mengirimkan pesan kepada Bob. Eve sebagai penyadap tidak dapat melakukan dekripsi karena kunci yang dimiliki tidak dapat melakukan dekripsi. Bob menerima pesan dan mendekripsinya dengan kunci privat (*pri*) yang bersesuaian dengan kunci publik (*pub*)

C. Tanda Tangan Digital

Salah satu aspek yang penting dalam kriptografi adalah nirpenyangkalan. Dalam dunia nyata, kita pun sangat membutuhkan aspek nirpenyangkalan ini dalam transaksi, perjanjian, dll. Biasanya, tanda tangan menjadi bukti yang otentik dan tidak dapat disangkal. Dokumen yang sudah ditandatangani pun tidak dapat diubah kembali.

Dalam dunia digital ini, tanda tangan juga penting untuk diimplementasi. Namun, ternyata tidak mudah untuk melakukan implementasi tanda tangan ini. Sehingga pada tahun 1976 pun, Diffie-Hellman mengenalkan skema tanda tangan digital. Setelah itu, algoritma yang berhubungan dengan tanda tangan digital ini pun berkembang.

Terdapat dua buah cara melakukan tanda tangan digital, yaitu dengan enkripsi pesan atau dengan menggunakan kombinasi fungsi *hash* dan kriptografi kunci publik. Contoh skema tanda tangan digital disajikan pada gambar di bawah ini.



Gambar 3 : Skema tanda tangan digital

Sumber gambar : comodosslstore.com

III. Ilustrasi Protokol

Pada sistem protokol ini, kita akan memodelkan seluruh *stakeholder* (pemangku kepentingan) yang berkaitan dengan sistem pemungutan dan perhitungan suara. Untuk memudahkan demonstrasi ilustrasi protokol, kita akan menggunakan nama-nama sebagai berikut :

- Alice-1, Alice-2, Alice-3, …, Alice-n : pemilih
- Bob : kotak suara
- Carol : lokasi perhitungan suara
- Dave : saksi perhitungan suara

Ilustrasi protokol dapat dibagi menjadi dua tahapan besar yaitu pemungutan dan perhitungan

A. Protokol Pemungutan Suara

Alice-1, Alice-2, Alice-3, ..., Alice-n (pemilih/*voter*) akan memberikan suara (dalam bentuk pesan) kepada Bob. Bob harus bisa menerima suara (dalam bentuk pesan) dari Alice-1 sampai Alice-n dan memastikan bahwa pemberi suara memang benar adalah Alice, bukan orang lain (asas langsung). Bob meneruskan pesannya kepada Carol untuk dihitung. Carol tidak tahu pesan mana dari Alice yang mana (asas rahasia). Bob tahu siapa saja yang memberikan suara dan siapa saja yang tidak memberikan suara, sehingga Alice tidak dapat melakukan *vote* berulang.

B. Protokol Perhitungan Suara

Carol memiliki seluruh pesan dari Alice (yang didapatkan melalui pihak lain yaitu Bob). Carol tidak dapat membuka pesan tersebut. Pesan dapat dibuka oleh Carol setelah Dave (saksi perhitungan) memberikan kunci. Setelah itu, Carol dan Dave dapat membaca seluruh pesan dari Alice-1 sampai Alice-n dan melakukan perhitungan.

C. Catatan Simplifikasi

Protokol pemungutan dan perhitungan suara pada dunia nyata bisa beragam dan lebih kompleks dibandingkan yang tertera di sini. Sehingga, dilakukan pembatasan masalah sebagai berikut :

- Pada kasus nyata, lebih dari satu Bob (kotak suara) yang akan mengirimkan pesan kepada Carol (lokasi perhitungan suara). Bahkan Carol pun bisa lebih dari satu.
- Selain itu, dibutuhkan lebih dari satu Dave (saksi) untuk membuka pesan dan melakukan perhitungan.

Fokus pada penyelesaian protokol ini adalah dengan membentuk protokol kriptografi yang tetap mempertahankan asas-asas yang telah dijelaskan pada bagian A (Protokol Pemungutan Suara), yaitu asas langsung dan asas rahasia.

IV. Desain Protokol Kriptografi Sistem

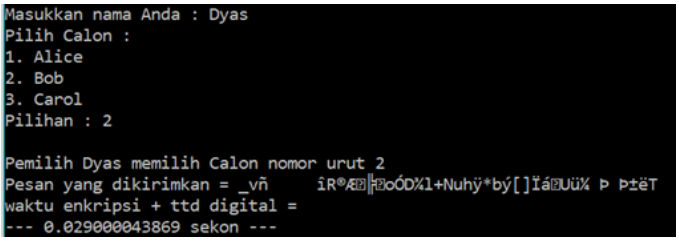
Ilustrasi di atas dapat diterjemahkan ke dalam sebuah protokol kriptografi. Protokol ini memiliki empat jenis subjek (Alice, Bob, Carol, dan Dave) yang saling mengirim pesan.

1. Dave memberikan kunci publiknya untuk enkripsi pesan Alice
    a. Kunci public bebas diketahui siapapun
    b. Enkripsi hanya dapat dibuka oleh Dave (dengan kunci privatnya)
2. Alice-i memilih/vote, kemudian melakukan enkripsi pilihan tersebut dengan kunci publik Dave
    a. Pilihan Alice-i hanya diketahui oleh Alice-i
3. Setelah pilihan dienkripsi, Alice-i memberikan tanda tangan digital pada pesan terenkripsi tadi
    a. Sehingga, jelas bahwa pesan tersebut berasal dari Alice-i
4. Alice-i memberikan pesan tersebut kepada Bob, Bob menerima pesan tersebut dan melakukan verifikasi tanda tangan digital
    a. Bob tidak mengetahui pesan Alice-i karena terenrkipsi kunci Dave
    b. Bob dapat melakukan verifikasi karena tanda tangan Alice-I tidak dienkripsi
5. Apabila pesan terverifikasi, Bob mencatat bahwa Alice telah memilih dan menghapus tanda tangan digital dari Alice
    a. Verifikasi dilakukan oleh Bob sehingga Alice-i tidak dapat memberikan pesan lagi kepada Bob
    b. Pemberian pesan berulang berarti melakukan voting lebih dari sekali dan hal ini tidak diperbolehkan
6. Langkah 1-5 akan diulangi untuk i dari 1 sampai n
7. Setelah waktu pemungutan suara berakhir, Bob meneruskan pesan kepada Carol dengan urutan pesan yang acak
    a. Pada tahap 5, Bob telah menghapus tanda tangan digital Alice sehingga Carol tidak memiliki data, pesan tersebut milik Alice yang mana
    b. Pesan diteruskan secara acak sehingga biarpun Carol mengetahui urutan kedatangan Alice, Carol tetap tidak mengetahui hasil pesannya
8. Pada waktu perhitungan suara, Dave akan datang kepada Carol untuk membukan pesan-pesan yang ada dan melakukan perhitungan
    a. Carol dan Dave tidak tahu masing-masing pesan milik Alice yang mana karena telah diacak oleh Bob
    b. Bob hanya mengetahui hasil dari perhitungan suara, tidak dapat melakukan dekripsi pesan Alice

V. Simulasi Implementasi Protokol

A. Simulasi Pemungutan Suara

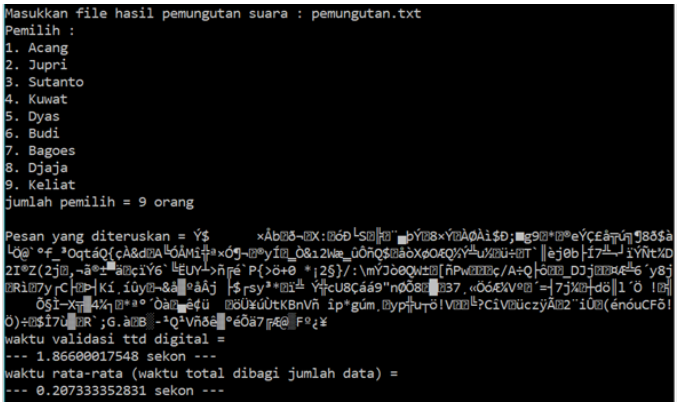
Pemilih melakukan pemungutan suara pada TPS (tempat pemilihan suara) yang berbentuk digital. Identitas pemilih disimulasikan dengan nama. Waktu yang ditampilkan di sini adalah waktu untuk melakukan enkripsi dan memberikan tanda tangan digital.



Gambar 4 : *Screenshot* simulasi pemungutan suara

B. Simulasi Rekapitulasi Pemilih

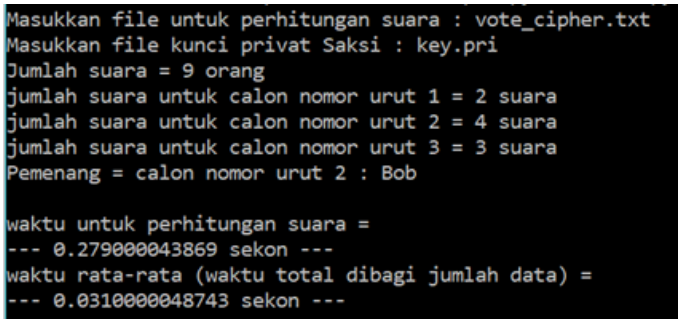
Di sini, Bob akan membuka seluruh tanda tangan digital yang ada. Dari tanda tangan digital ini, Bob menampilkan seluruh data pemilih yang ada. Namun, Bob hanya dapat melakukan validasi tanda tangan dari pemilih, tidak dapat melakukan dekripsi dari pilihan yang ada. Sehingga Bob mendapatkan identitas pemilih dan mengetahui jumlah pemilih. Waktu yang ditampilkan di sini adalah waktu untuk melakukan validasi tanda tangan digital (jumlahnya bergantung dari ukuran datanya).



Gambar 5 : *Screenshot* simulasi rekapitulasi pemilih

C. Simulasi Perhitungan Suara

Perhitungan suara hanya dapat dimulai apabila dihadiri saksi (Dave). Kehadiran saksi disimulasikan dengan melakukan load file kunci privat. File untuk perhitungan suara adalah seluruh data terenkripsi dari pemilih (di titik ini, tidak diketahui pemilih mana memilih calon yang mana, sehingga asas rahasia tetap terjaga). Jumlah suara yang ditampilkan haruslah sama dengan jumlah pemilih yang ditampilkan pada simulasi sebelumnya (Simulasi Rekapitulasi Pemilih).



Gambar 6 : *Screenshot* simulasi perhitungan suara

VI. Pembahasan Hasil

A. Analisis Kinerja (Waktu)

Waktu yang ditampilkan pada simulasi adalah waktu yang dibutuhkan untuk melakukan proses kriptografi. Pada simulasi pemungutan suara, proses yang terjadi adalah proses enkripsi, kemudian tanda tangan digital. Pada simulasi rekapitulasi pemilih, proses yang terjadi adalah proses validasi tanda tangan digital. Pada simulasi perhitungan suara, proses yang terjadi adalah proses dekripsi.

Pada simulasi pemungutan suara, terlihat bahwa proses enkripsi dan tanda tangan digital memakan waktu total 0.029 detik. Waktu ini sangat tidak terasa apabila dilakukan di dunia nyata setiap kali seseorang melakukan pemungutan suara. Sehingga, proses ini dianggap logis untuk diimplementasi di dunia nyata.

Pada simulasi rekapitulasi pemilih, waktu rata-rata yang dibutuhkan untuk setiap data adalah 0.236 sekon. Apabila ini dilaksanakan di tiap TPS, maka akan ada maksimal 800 data (1 TPS memiliki maksimal 800 pemilih). Sehingga, waktu total maksimal yang dibutuhkan untuk melakukan rekaptulasi adalah 0.236*800 = 188.8 detik atau sekitar 3.15 menit. Ternyata, hanya membutuhkan waktu tiga menit lebih sedikit untuk melaksanakan proses vaslidasi seluruh tanda tangan digital pada tiap TPS.

Pada simulasi perhitungan suara, waktu rata-rata yang dibutuhkan untuk setiap data adalah 0.031. Apabila ini dilaksanakan di tiap TPS, maka akan ada maksimal 800 data juga. Sehingga, waktu total maksimal untuk melakukan perhitungan di tiap TPS adalah 0.031*800 = 24.8 detik. Ternyata, perhitungan suara membutuhkan waktu kurang dari setengah menit pada tiap TPS.

Proses yang dilaksanakan di sini pun dengan assumsi proses sekuensial (proses kriptografi dilaksanakan satu persatu). Nyatanya, untuk kebutuhan sesungguhnya, proses dapat dioptimasi dengan melakukan proses kriptografi secara paralel (karena setiap data berdiri sendiri / independen). Hal ini akan mengurangi waktu yang diperlukan.

B. Analisis Kinerja (Memori)

Setelah mengalami enkripsi dan tanda tangan digital, pesan akan memiliki ukuran yang lebih besar dibanding pesan sesungguhnya. Di dalam pesan ini terkandung identitas pemilih dan *vote* (calon yang dipilih). Memori yang dibutuhkan untuk menyimpan pesan setiap pemilih memakan memori yang lebih besar dibanding penyimpanan tanpa terenkripsi. Hal ini terjadi karena untuk pilihan yang sama, pesan yang dienkripsi harus berbeda, sehingga butuh memori yang jauh lebih banyak.

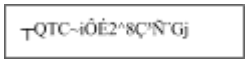
Dilihat dari simulasi pemungutan suara yang dilakukan (identitas menggunakan nama), setiap pemilih membutuhkan sekitar 40 karakter. Karakter ini disimpan sebagai ASCII (1 *byte*), sehingga satu pemilih akan menghabiskan sekitar 40 *byte*. Apabila satu TPS memiliki 800 calon pemilih, maka dibutuhkan 40*800 = 36000 *byte* atau sekitar 36 KB. Ukuran ini sangat logis untuk diterapkan di dunia nyata karena tidak memakan memori yang besar.

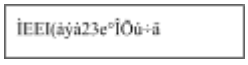
Apabila dihitung untuk kebutuhan pengadaan seluruh indonesia, TPS yang dibutuhkan lebih dari 800 ribu. Jika dianggap 850 ribu TPS, maka dibutuhkan 36*850.000 = 30.600.000 *kilobyte* atau 30,6 GB. Ukuran inipun masih logis untuk diterapkan di dunia nyata.

C. Analisis Keamanan

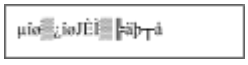
Beberapa contoh pilihan voting untuk pilihan yang sama :

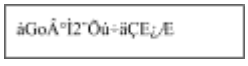
(*vote* = calon nomor urut 1)

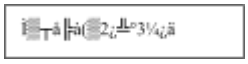




Contoh lain : (*vote* = calon nomor urut 3)







Terlihat bahwa dari contoh-contoh tersebut, untuk pilihan yang sama, pesan akan mengalami enkripsi yang berbeda. Hal ini dikarenakan pada pesan diberikan *padding byte* yang berbeda-beda untuk menyamarkan *vote* dari para pemilih. Dengan begini, seharusnya tidak ada yang akan mengetahui *vote* dari pemilih sebelum dilakukan enrkipsi.

VII. Kesimpulan dan Saran Pengembangan

A. Kesimpulan

Protokol kriptografi pada sistem pemungutan dan perhitungan suara menjadi hal yang penting saat ini. Setelah dilakukan simulasi pemungutan, rekapitulasim dan perhitungan, bisa terlihat bahwa protokol kriptografi ini tidak terlalu sulit. Hanya saja, dibutuhkan ketelitian agar asas-asas pemilihan (pada kasus ini asas langsung dan asas rahasia) tetap terjaga.

Secara waktu, protokol kriptografi tidak memakan waktu yang lama untuk melakukan enkripsi, tanda tangan digital, validasi tanda tangan, maupun dekripsi. Total waktu yang dibutuhkan masih masuk akal untuk diterapkan di dunia nyata.

Secara memori, protokol ini pun tidak memakan memori yang terlalu besar. Ukuran memori yang diperlukan untuk mengakomodir protokol ini masih masuk akal. Analisis keamanan pun telah dilakukan dan setiap pesan-pesan yang ada cukup aman untuk diterapkan.

B. Kelemahan dan Saran Pengembangan

Desain dan simulasi protokol yang telah dilakukan masih bisa dilakukan banyak pengembangan. Pengembangan yang mungkin dilakukan adalah dari segi waktu, memori, maupun rekayasa perangkat lunak.

Dari segi waktu, proses kriptografi masih dilakukan secara sekuensial (satu persatu), biarpun waktu yang diperlukan tidak signifikan, namun proses ini bisa dioptimasi dengan melakukan proses secara paralel sehingga waktu yang dibutuhkan semakin kecil dan bisa diabaikan.

Pengembangan lain yang mungkin dilakukan adalah berkaitan dengan memori. Simulasi yang dilakukan di sini menggunakan *padding byte* untuk menyamarkan pilihan. Sehingga, enkripsi dan tanda tangan digital apabila ditotal memakan memori 40 *byte*. Dengan menggunakan algoritma kriptografi yang lebih baik (seperti ECC), kebutuhan memori dapat diperkecil. Kinerja algoritma tidak terlalu berpengaruh apabila proses dapat dilakukan paralel.

Desain protokol kriptografi ini masih memiliki beberapa pembatasan masalah (yang telah dijelaskan pada bagian III.C Catatan Simplifikasi). Sehingga, secara perangkat lunak, desain perangkat lunak bisa diperbaiki dengan menambah jumlah file eksternal yang dapat di-*load* (*multiple file*) pada simulasi rekapitulasi pemilih (file hasil pemungutan suara) dan pada simulasi perhitungan suara (file kunci privat dan file untuk perhitungan suara).

References

[1] A. Menezes, P. van Oorschot, dan S. Vanstone. 2001. *Handbook of Applied Cryptography (5th ed.)*. CRC Press

[2] Munir, Rinaldi. 2018. *Bahan Kuliah IF4020 Kriptografi: Kriptografi Kunci-Publik*

[3] Munir, Rinaldi. 2018. *Bahan Kuliah IF4020 Kriptografi: Tandatangan Digital*

[4] Munir, Rinaldi. *Bahan Kuliah IF5054 Kriptografi: Protokol Kriptografi*

[5] Stallings, William. 2014. *Cryptography and Network Security (6th ed.)*. Upper Saddle River, N.J.: Prentic Hall

Pernyataan

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 16 Mei 2018

Drestanto M. Dyasputro - 13514099