PEMANFAATAN KRIPTOGRAFI DALAM MEWUJUDKAN KEAMANAN INFORMASI PADA *e-VOTING* DI INDONESIA

Esti Rahmawati Agustina [1)], Agus Kurniati [2)]
[1,2)]Lembaga Sandi Negara, Jl Harsono RM No 70, Ragunan, Pasar Minggu, Jakarta Selatan
Email: rahma_cryptn@yahoo.co.id, aguskurniati@yahoo.com

Abstrak
Sejumlah negara maju seperti Finlandia dan Lithuania serta negara berkembang Brasil dan India telah melangkah dengan memanfaatkan e-Voting (electronic voting) dengan tingkat dan kualitas pemanfaatan TIK yang berbeda-beda dalam kegiatan demokrasinya. e-Voting ternyata bisa dilakukan dan diterima hasilnya oleh rakyat dari negara dengan rata-rata tingkat pendidikan tinggi maupun rendah. Studi awal e-Voting dari Zamrud Technology yang telah diulas oleh majalah warta eGov edisi 4, April/Mei 2008 menunjukkan potensi penghematan anggaran Pemilu/Pilkada hingga mencapai Rp 11 Trilyun.
Dalam beberapa tahun kedepan, melalui program USO (Universal Service Obligation) pemerintah akan menyediakan fasilitas akses komunikasi suara dan data hingga menjangkau seluruh desa di tanah air sehingga e-Voting semakin berpeluang untuk diterapkan. Tersedianya fasilitas akses data secara luas, selain membuka peluang positif atas terapan berbagai aplikasi dan layanan berbasis internet, juga menyisakan persoalan terkait dengan keamanan informasi yaitu keutuhan data (integrity), kerahasiaan informasi (confidentiality), dan ketersediaan informasi (availability).
Kriptografi dapat dimanfaatkan untuk menjawab pertanyaan terkait dengan keamanan informasi berupa kerahasiaan, keutuhan data, nir penyangkalan, serta otentikasi. Dalam paper ini akan dijelaskan bagaimana pemanfaatan kriptografi dalam mewujudkan keamanan informasi pada e-Voting di Indonesia.

Keywords: kriptografi, keamanan informasi, *e-Voting*

1. PENDAHULUAN

Pesatnya perkembangan teknologi informasi dan komunikasi sangat berpengaruh pada kehidupan manusia. Berbagai bidang kehidupan manusia telah mulai memanfaatkan perkembangan teknologi ini. Sebut saja beberapa istilah yang sering kita dengar dengan berawalan huruf *e*, antara lain *e-banking, e-procurement, e-learning, e-commerce, e-government,* dan beberapa istilah lainnya. Huruf *e* dalam setiap istilah merupakan kependekan dari "elektronik" yang berarti bahwa telah dimanfaatkannya teknologi komputer pada setiap hal tersebut. Sebagaimana telah mulai didengarnya istilah-istilah berawalan *e* tersebut, istilah *e-democracy* mulai marak dibicarakan. *e-democracy* diharapkan menjadi sebuah solusi dari berbagai permasalahan proses demokrasi yang saat ini dirasakan masyarakat. *e-democracy* merupakan suatu paradigma baru mengenai pemanfaatan Teknologi Informasi dan Komunikasi untuk menciptakan pelaksanaan demokrasi yang lebih baik. Sebagai contoh pelaksanaan pemilihan dan *voting* dapat dilakukan secara elektronik yang biasa disebut dengan *e-election* dan *e-voting*.

Untuk mengimplementasikan *e-voting* sebagai bagian dari *e-democracy* di Indonesia, banyak hal yang harus dipersiapkan terkait dengan infrastruktur teknologi serta kurangnya pengetahuan masyarakat umum mengenai teknologi. Peluang implementasi *e-voting* di Indonesia semakin terbuka dengan adanya program USO (*Universal Service Obligation*) dalam beberapa tahun ke depan. Pemerintah akan menyediakan fasilitas akses komunikasi suara dan data hingga menjangkau seluruh desa di tanah air .Tersedianya fasilitas akses data secara luas, selain membuka peluang positif atas diterapkannya berbagai aplikasi dan layanan berbasis internet. Namun demikian terdapat hal yang krusial yang tidak boleh dilupakan adalah sistem *e-voting* itu sendiri. Dalam sebuah artikel dari *Association of Information Technology Professionals* (AITP) mengemukakan bahwa ada 4 (empat) persyaratan agar sistem *e-voting* dapat dipercaya oleh masyarakat. Keempat syarat tersebut adalah *secure* (aman/terjamin), *accurate* (akurat), *re-countable* (dapat dihitung kembali), dan *accessible* (kemudahan untuk mengakses). Salah satu syarat tersebut yaitu *secure* terkait dengan keamanan informasi selama pelaksanaan *e-voting*.

Dalam buku *Information Security Management Handbook* dijelaskan bahwa terdapat 3 (tiga) aspek yang harus dipenuhi dalam keamanan informasi di organisasi manapun, yaitu aspek kerahasiaan (*confidentiality*), keutuhan data (*data integrity*), dan ketersediaan (*availability*). Selain ketiga aspek tersebut, terdapat aspek tambahan yang harus dipenuhi yaitu otentikasi penyedia/penerima informasi (*authentication*) serta nir penyangkalan (*non repudiation*). Dengan demikian, pada saat pelaksanaan *e-voting*, kemanan informasi dapat diwujudkan dengan memenuhi kelima aspek keamanan informasi tersebut.

Kriptografi merupakan salah satu teknik untuk menjamin kerahasiaan informasi yang dikomunikasikan. Informasi ini terlindung karena pesan asli akan diubah menjadi pesan *cipher* (pesan sandi) dengan

menggunakan kunci tertentu sehingga pesan ini tidak dapat diketahui pihak yang tidak berkepentingan. Seiring dengan perkembangannya kriptografi ternyata dapat dimanfaatkan untuk mendukung aspek kemanan informasi lainnya. Aspek keamanan informasi yang dapat didukung oleh kriptografi adalah kerahasiaan (*confidentiality*), keutuhan data (*data integrity*), otentikasi penyedia/penerima informasi (*authentication*) serta nir penyangkalan (*non repudiation*).

Paper ini akan menjelaskan bagaimana kriptografi dapat mendukung aspek-aspek keamanan informasi pada pelaksanaan *e-voting* di Indonesia.

2. TINJAUAN PUSTAKA

a. Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani yaitu *cryptos* yang berarti *secret* yaitu rahasia dan *graphein* artinya *writing* yaitu tulisan. Sehingga kriptografi berarti *secret writing* yaitu tulisan rahasia. Menurut Schneier, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Sedangkan menurut Menezes, kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi.

Kriptografi bertujuan untuk memberikan layanan keamanan informasi (yang dinamakan juga sebagai aspek-aspek keamanan informasi), yaitu:

1) Kerahasiaan (*confidentiality*)
   Merupakan layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.
2) Integritas Data (*integrity*)
   Merupakan layanan yang menjamin bahwa pesan masih utuh/asli atau belum pernah dimanipulasi selama pengiriman.
3) Otentikasi (*authentication*)
   Merupakan layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *entity authentication*) maupun mengidentifikasi kebenaran sumber pesan (*data origin authentication*).
4) Nir penyangkalan (*non repudiation*)
   Merupakan layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

b. Algoritma Kriptografi

Dalam matematika dan komputasi, algoritma merupakan kumpulan perintah untuk menyelesaikan suatu masalah. Perintah-perintah ini dapat diterjemahkan secara bertahap dari awal hingga akhir. Algoritma kriptografi diartikan sebagai langkah-langkah untuk mengubah teks terang menjadi teks sandi ataupun sebaliknya. Secara umum algoritma kriptografi terbagi menjadi 2 (dua) yaitu

1) Algoritma enkripsi/dekripsi
   Algoritma enkripsi/dekripsi adalah langkah-langkah atau tahapan dalam melakukan proses pengubahan teks terang menjadi teks sandi/teks sandi menjadi teks terang. Dalam proses enkripsi/dekripsi ini kunci merupakan input yang harus diberikan selain teks terang untuk menyandi ataupun teks sandi untuk membuka sandi. Sehingga kunci ini harus dijaga agar tidak jatuh kepihak yang tidak berkepentingan.
   Berdasarkan kunci, algoritma enkripsi dibagi menjadi dua,yaitu algoritma kunci simetrik (*symmetric key algorithm*) yang merupakan algoritma enkripsi dimana input kunci untuk enkripsi dan dekripsi sama, dan algoritma kunci asimetrik (*asymmetric key algorithm*) yang merupakan algoritma enkripsi dimana input kunci untuk enkripsi dan dekripsi berbeda. Algoritma asimetrik memiliki karakteristik yang unik dimana kunci untuk enkripsi boleh diketahui oleh pihak-pihak yang tidak memiliki otoritas karena dekripsi menggunakan kunci yang berbeda. Karena itu, kunci untuk dekripsi harus dijaga dan dirahasiakan. Pada algoritma kunci asimetrik, kunci untuk enkripsi sering disebut sebagai kunci publik (*public key*) dan kunci untuk dekripsi disebut sebagai kunci privat (*private key*).
2) Algoritma hash
   Merupakan langkah-langkah dalam melakukan fungsi yang mengubah input yang panjangnya sembarang dan mengkonversinya menjadi output dengan panjang yang tetap (*fixed*) (umumnya berukuran jauh lebih kecil daripada ukuran semula). Algoritma ini bersifat satu arah, sehingga input tidak dapat diperoleh dengan memasukkan kembali output kedalam algoritma hashnya.

c. Protokol Kriptografi

Protokol adalah aturan yang berisi rangkaian langkah-langkah yang melibatkan dua orang atau lebih, yang dibuat untuk menyelesaikan suatu kegiatan. Protokol kriptografi adalah protokol yang menggunakan kriptografi. Protokol kriptografi dibangun dengan melibatkan beberapa algoritma kriptografi. Protokol kriptografi digunakan sesuai dengan tujuannya misalkan untuk pembangkitan kunci, pembangkitan bilangan acak, meyakinkan identitas orang lain, dan sebagainya.

d. e-Voting

e-Voting dapat diartikan sebagai penggunaan teknologi informasi dan komunikasi dalam pelaksanaan *voting*. Penggunaan teknologi ini layaknya pisau bermata dua. Satu sisi meberikan banyak kemudahan, kecepatan, sedangkan disisi lain menimbulkan kerawanan. Pada proses *e-voting*, kerawanan yang mungkin timbul adalah terkait dengan keamanan informasinya. Menurut Schneier berikut beberapa *requirement* dasar pada *e-voting:*

1) Hanya orang yang sah yang dapat memberikan suara/memilih.
2) Setiap orang tidak dapat memilih lebih dari sekali
3) Tidak ada seorangpun yang dapat mengetahui pilihan orang lain
4) Tidak ada seorangpun yang dapat menduplikasi suara orang lain
5) Tidak ada seorangpun yang dapat merubah pilihan orang lain tanpa diketahui oleh pihak lainnya.
6) Setiap orang dapat memastikan pilihannya telah masuk ke pusat tabulasi suara
7) Setiap orang mengetahui siapa yang sudah memilih dan tidak memilih.

e. Keamanan Informasi

Informasi merupakan aset yang sangat berharga, untuk itu perlu dijamin keamanannya dalam setiap oraganisasi. Aspek-aspek keamanan informasi adalah:

1) Kerahasiaan (*Confidentialit*y)
   Merupakan aspek pencegahan penyingkapan informasi kepada pihak yang tidak memiliki hak terhadap infomasi tersebut.
2) Integritas (*Integrity*)
   Merupakan aspek pencegahan perubahan informasi oleh pihak yang tidak memiliki otoritas untuk merubah informasi tersebut. Untuk memenuhi kebutuhan ini haruslah dapat untuk mendeteksi perubahan informasi, yaitu penyisipan, penghapusan, dan penggantian.
3) Ketersediaan (*Availability*)
   Merupakan aspek dimana infomasi harus tersedia ketika dibutuhkan.
4) Otentikasi (*Authentication*)
   Merupakan aspek menjamin informasi tersebut adalah asli. Juga untuk menjamin keabsahan orang-orang yang terlibat dalam pertukaran informasi.
5) Nir Penyangkalan (*Non-repudiation*)
   Merupakan aspek menjamin agar pihak-pihak yang terlibat tidak dapat menyangkal dikemudian hari.

3. METODE PENELITIAN

Metode penelitian yang digunakan adalah deskriptif kualitatif. Yaitu dengan mendeskripsikan bagaimana kriptografi dapat mendukung keamanan informasi pada *e-voting* di Indonesia, dengan memanfaatkan algoritma dan protokol kriptografi serta memenuhi *requirement* dasar pada *e-voting.*

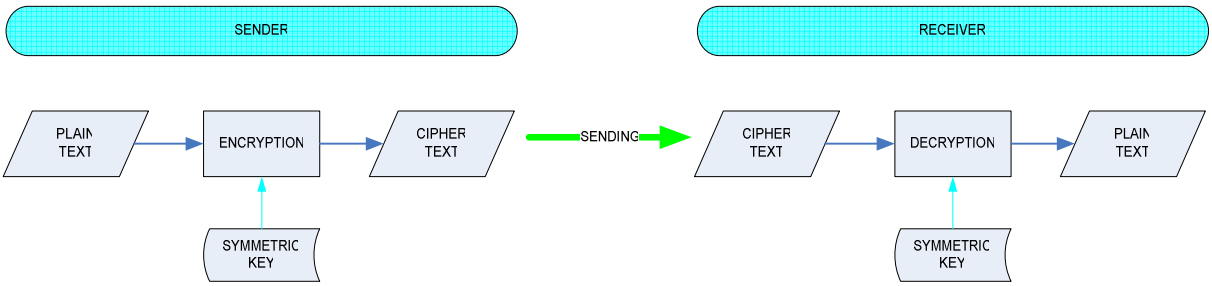
4. PEMBAHASAN

Berikut adalah pembahasan terkait keamanan informasi yang didukung oleh pemanfaatan kriptografi:

a. Kerahasiaan (*confidentiality*)

Aspek kerahasiaan akan didukung dengan memanfaatkan algoritma kriptografi yaitu algoritma enkripsi/dekripsi baik itu simetri maupun asimetri. Aspek ini sangat terkait dengan keberadaan kunci, sehingga kunci tidak boleh jatuh ke pihak yang tidak berkepentingan. Contoh algoritma simetrik yang dapat digunakan antara lain DES, AES, Tripple DES, dll. Sedangkan algoritma asimetrik misalnya RSA, *Knapsack, Rabin, Elgamal,* dll.

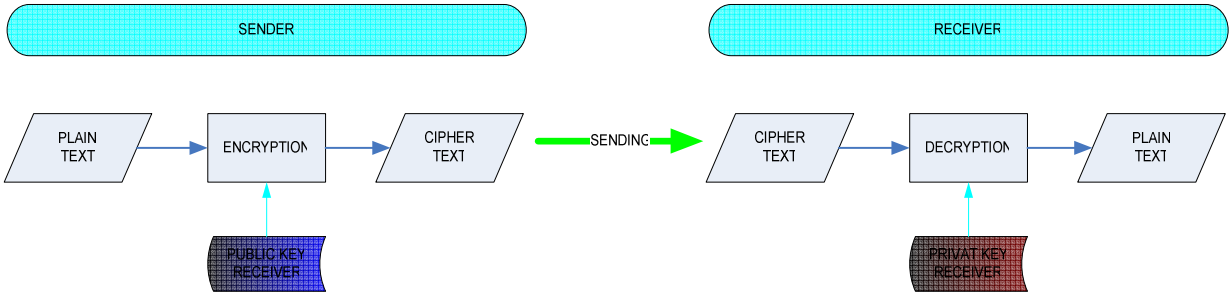
Berikut mekanisme enkripsi dekripsi menggunakan algoritma kunci simetrik:



Gambar 1. Mekanisme Enkripsi Dekripsi Algoritma Kunci Simetrik

Sebelum melakukan pertukaran informasi, pengirim dan penerima telah melakukan kesepakatan untuk menentukan algoritma dan kunci yang digunakan. Selanjutnya, pengirim akan mengenkripsi pesan dengan kunci dan algoritma yang telah disepakati. Pesan tersebut kemudian berubah menjadi pesan *cipher* yang akan dikirimkan kepada penerima. Setelah menerima pesan tersebut, penerima melakukan dekripsi menggunakan algoritma dan kunci yang telah disepakati sebelumnya. Pada mekanisme ini kunci yang digunakan untuk melakukan dekripsi dan enkripsi sama.

Berikut mekanisme enkripsi dekripsi menggunakan algoritma kunci asimetrik:

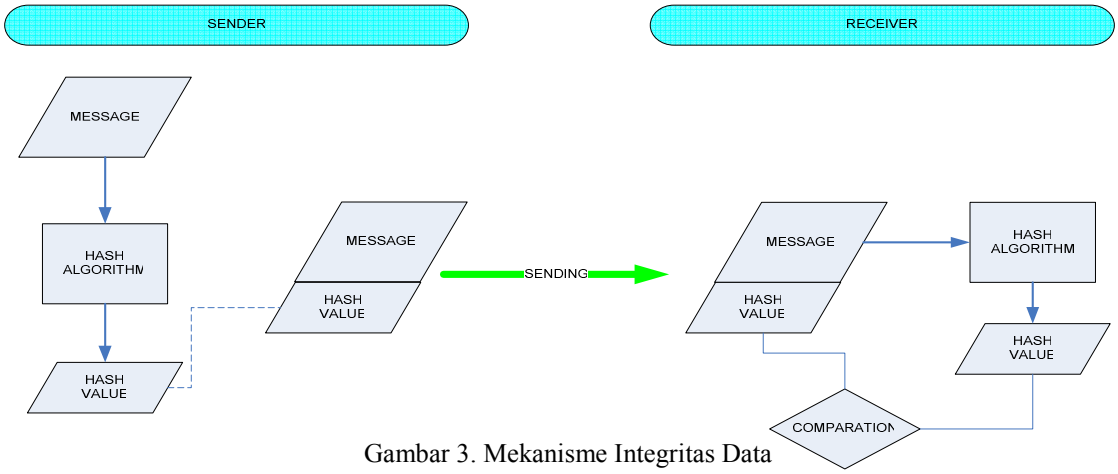


Gambar 2. Mekanisme Enkripsi Dekripsi Algoritma Kunci Asimetrik

Sebelum melakukan pertukaran informasi, pengirim dan penerima telah menyepakati algoritma yang akan digunakan serta telah mengetahui kunci publik masing-masing. Sedangkan kunci privat hanya diketahui oleh masing-masing pihak. Pengirim akan mengenkripsi pesan dengan menggunakan kunci publik penerima, selanjutnya pesan *cipher* yang dihasilkan akan dikirimkan ke penerima. Setelah menerima pesan *cipher* tersebut, penerima akan mendekripsi pesan dengan kunci privat miliknya. Pada mekanisme ini kunci untuk proses enkripsi dan dekripsi tidak sama.

b. Integritas (*integrity*)
Aspek integritas dapat didukung dengan memanfaatkan algoritma *hash*. Fungsi hash ini akan besifat satu arah sehingga nilai hash yang keluar tidah dapat dikembalikan lagi.

Berikut mekanisme pembuktian integritas data:

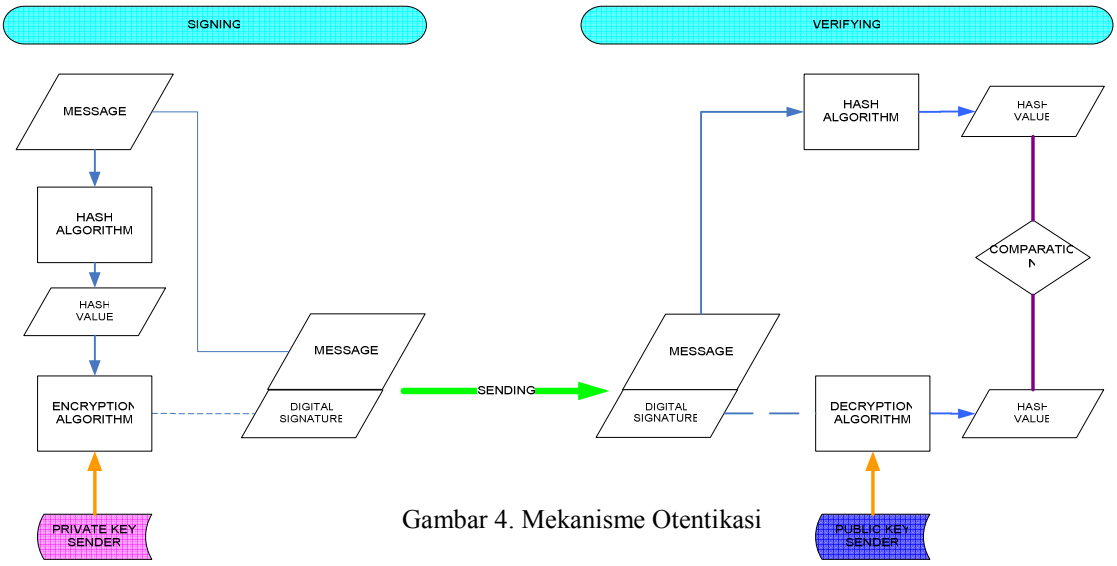


Gambar 3. Mekanisme Integritas Data

Pengirim akan menghitung nilai hash dengan memasukkan pesan ke algoritma hash. Setelah itu nilai hash akan digabungkan (*concate*) dengan pesan. Kemudian pesan dan nilai hash tersebut dikirimkan ke penerima. Penerima akan menerima gabungan pesan dan nilai hash tersebut, selanjutnya pesan dan nilai hash dipisahkan dan memasukkan pesan ke dalam algoritma hash untuk mendapatkan nilah hash dari pesan yang dikirimkan tersebut. Selanjutnya nilai hash yang didapat dari penghitungan tersebut, dibandingkan dengan nilai hash yang diterima dari pengirim. Jika nilai hash tersebut sama maka pesan tidak mengalami perubahan selama pengiriman, tetapi jika nilai hash antara perhitungan penerima dan nilai hash yang diterima dari pengirim berbeda, maka pesan telah berubah selama pengiriman.

c. Ketersediaan (*availability*)
Ketersediaan dalam aspek keamanan informasi ini berarti informasi tersedia ketika dibutuhkan. Kriptografi tidak dapat mendukung aspek ketersediaan, karena kriptografi tidak dapat mencegah adanya sabotase, pengeboman, dan cara-cara penghilangan informasi lainnya. Aspek ketersediaan ini dapat diwujudkan melalui *Business Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP) yang menyediakan informasi ketika diperlukan.

d. Otentikasi (*authentication*)
Otentikasi dalam aspek keamanan informasi dapat didukung melalui mekanisme tanda tangan digital. Tanda tangan digital dihasilkan dari pemanfaatan algoritma asimetrik seperti RSA, DSA, dan *ElGamal.* Berikut mekanisme otentikasi (meyakinkan pengirim adalah pengirim yang sebenarnya serta keaslian pesan):



Gambar 4. Mekanisme Otentikasi

Pada mekanisme otentikasi terdapat 2 (dua) tahapan penting yaitu *signing* dan *verifying*. *Signing* dilakukan oleh pengirim agar dapat dibuktikan keotentikasiannya. *Verifying* dilakukan oleh *verifier* dalam hal ini penerima. Seorang penerima akan memverifikasi apakah pengirim pesan tersebut adalah pengirim pesan yang sebenarnya. *Signing* dilakukan dengan memasukkan pesan ke algoritma hash tertentu dengan menggunakan kunci privat milik pengirim yang akan menghasilkan nilai hash, kemudian nilai hash tersebut dienkripsi dengan menggunakan kunci privat pengirim yang akan menghasilkan *digital signature* (tanda tangan digital). Kemudian *digital signature* yang dihasilkan ditempelkan pada pesan dan bersama-sama dikirimkan ke penerima. Ketika penerima menerima pesan dan *digital signature* tersebut, pesan akan dimasukkan ke dalam algoritma yang sama dengan menggunakan kunci publik milik pengirim. Kemudian *digital signature* didekripsi dengan menggunakan kunci publik pengirim, yang akan menghasilkan nilai hash, kemudian nilai hash tersebut dibandingkan dengan nilai hash yang telah diterima sebelumnya. Jika nilai hash tersebut sama berarti pengirim telah terotentikasi. Hal ini terjadi karena hanya pengirim yang mengetahui kunci privatnya kemudian menggunakannya untuk menyandi nilai hash.

e. Nir penyangkalan (*non repudiation*)
Aspek Nir penyangkalan dapat didukung melalui kriptografi dengan menggunakan algoritma tanda tangan digital (*digital signature algorithm*). Mekanisme penggunaan algoritma ini sama seperti mekanisme pada otentikasi. Seseorang yang telah mengirimkan pesan dan dibubuhi *digital signature* tidak dapat mengelak bahwa dia telah mengirimkan pesan karena *digital signature* tersebut diperoleh dari enkripsi nilai *hash* pesan dengan kunci privatnya.

Pemanfaatan fungsi kriptografi untuk mewujudkan keamanan informasi pada pelaksanaan *e-voting* di Indonesia dapat digabungkan ke dalam sebuah protokol kriptografi yang akan memenuhi *requirement* dasar pada *e-voting*. Salah satu jenis protokol tersebut adalah "*Simplistic Voting Protokol #2*". Berikut tahapan protokol tersebut:

1) Masing-masing pemilih melakukan *signing* dengan kunci privat mereka.
2) Masing-masing pemilih melakukan enkripsi terhadap pilihannya yang telah di-*signing* tersebut dengan menggunakan kunci publik pusat tabulasi data.
3) Masing-masing pemilih mengirimkan pilihannya ke pusat tabulasi data.
4) Pusat tabulasi data akan melakukan dekripsi terhadap pilihan tersebut, memverifikasi *signature*nya, memasukkan datanya dan mengumumkan hasilnya ke masyarakat.

Tabel 1. Pemenuhan *Requirement* Dasar *e-Voting*

REQUIREMENT DASAR *E-VOTING*	PEMENUHAN *REQUIREMENT E-VOTING*
Hanya orang yang sah yang dapat memberikan suara/memilih.	Terpenuhi pada tahap 4) Sah berarti telah terdaftar dan masuk dalam *data base* pemilih di Pusat Tabulasi Data, Pusat Tabulasi Data akan mengetahui semua kunci publik pemilih sehingga hanya pemiilh yang sah yang dapat didekripsi oleh Pusat Tabulasi Data.
Setiap orang tidak dapat memilih lebih dari sekali	Terpenuhi pada tahap 1) Setiap pemilih hanya mempunyai sepasang kunci publik dan kunci privat.
Tidak ada seorangpun yang dapat mengetahui pilihan orang lain	Terpenuhi pada tahap 2) da 4) Setiap pemilih mengenkripsi data dengan kunci publik Pusat Tabulasi Data, sehingga hanya Pusat Tabulasi Data yang dapat membuka pesan terenkripsi tersebut.
Tidak ada seorangpun yang dapat menduplikasi suara orang lain.	Terpenuhi pada tahap 1) dan 4) Hal ini dipenuhi karena setiap pemilih hanya mempunyai sebuah kunci privat dan hanya ia yang mengetahuinya.

Tidak ada seorangpun yang dapat merubah pilihan orang lain tanpa diketahui oleh pihak lainnya.	Terpenuhi pada tahap 1) dan 4) Karena memanfaatkan *digital signature* dari pemilih.
Setiap orang dapat memastikan pilihannya telah masuk ke Pusat Tabulasi Data	Terpenuhi pada tahap 4) Pusat Tabulasi Data akan mengumumkan hasil perolehan suara ke masyarakat.
Setiap orang mengetahui siapa yang sudah memilih dan tidak memilih.	Terpenuhi pada tahap 4) Pusat Tabulasi Data mempunyai seluruh kunci publik pemilih yang telah terdaftar.

5. KESIMPULAN DAN SARAN

a. Kesimpulan

Dari pembahasan yang telah dikemukakan maka pemanfaatan kriptografi dalam mewujudkan keamanan informasi pada *e-voting* di Indonesia yaitu dapat mendukung aspek-aspek keamanan informasi meliputi kerahasiaan, integritas data, otentikasi dan nir penyangkalan. Sehingga sebuah protokol kriptografi dapat memenuhi *requirement* dasar *e-voting*. Namun, terdapat satu aspek dalam keamanan informasi yaitu ketersediaan yang tidak dapat didukung oleh kriptografi.

b. Saran

1) Untuk mengimplementasikan *e-voting* di Indonesia, perlu adanya kesiapan dalam berbagai hal yaitu infrastruktur, pengetahuan SDM terkait dengan perangkat teknologi yang digunakan, serta pengamanan sistem *e-voting*. Oleh karena itu perlu adanya kesiapan dalam berbagai hal tersebut
2) Untuk mewujudkan *e-voting* di Indonesia ada beberapa aspek yang perlu dipersiapkan, terkait dengan masalah pengamanan informasi, maka kriptografi memberikan solusi untuk mengatasi masalah ancaman keamanan infromasi
3) Perlu dikembangkannya protokol kriptografi untuk mewujudkan *e-voting* di Indonesia yang sesuai dengan kondisi geografis dan kependudukan di Indonesia.

6. DAFTAR PUSTAKA

Stinson, Douglas. 1995. *Cryptogaphy: Theory and Practise. CRC Press*.

Stallings, William. 2005. *Cryptography and Network Security Principles and Practise*. Prentice Hall.

J.M., Alfred, Paul C. van Oorschot, and A.V., Scott. 1997. *Handbook of Applied Cryptography*. CRC Press.

Schneier, Bruce. 1996. A*pplied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, Inc.

Munir, Rinaldi. 2006. Kriptografi. Informatika: Bandung.

Azhari, Rakhmad. 2005. *E-Voting.* Fakultas Ilmu Komputer, Universitas Indonesia.

Ferdinang Inoerawan, Abraham. 2009. *Menilik Kriptografi dan Keamanan Informasi*. Lembaga Sandi Negara

www.aitp.org, diakses tanggal 7 Mei 2009

http://sipemilu.org/ti-kpu/10-riset-e-voting/ diakses pada tanggal 8 Mei 2009

Krause, Micky & Tipton,Harold F.2002.*Handbook of Information Management System,* (on line) www.ccert.edu.cn/ diakses tanggal 7 November 2007