# Pemanfaatan Tanda Tangan Digital Untuk Keamanan Pemilihan Umum Elektronik

Amelia Natalie/13509004[1]
*Program Studi Teknik Informatika*
*Sekolah Teknik Elektro dan Informatika*
*Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia*
[1]13509004@*stei.itb.ac.id*

***Abstrak*— *E-vote* adalah sistem yang memanfaatkan perangkat elektronik dan mengolah informasi digital untuk membuat surat suara, memberikan suara, menghitung dan menayangkan perolehan suara, serta memelihara dan menghasilkan jejak audit. Keuntungan *E-vote* lebih banyak dibandingkan dengan sistem pemilihan umum non-elektronik. Namun, banyak negara masih belum menerapkannya karena keamanan *e-vote* rentan untuk diserang. Salah satu bentuk *E-vote* adalah pemilihan melalui internet. Pada makalah ini dibahas penanganan serangan keamanan pada pemilihan melalui internet dengan memanfaatkan tanda tangan digital. Tanda tangan digital dimanfaatkan pada proses otentikasi dan verifikasi dimana kedua proses ini sangat rentan untuk diserang. Tanda tangan digital menggunakan prinsip *hashing* dan kriptografi kunci publik. Dengan pemanfaatan tanda tangan digital, tujuan otentikasi pengirim dan integritas data dapat tercapai.**

***Kata Kunci*— *e-vote*, tanda tangan digital, SHA, ElGamal, serangan keamanan.**

## I. LATAR BELAKANG

Pemilihan umum elektronik atau lebih dikenal dengan istilah *e-vote* merupakan berita yang sedang diperdebatkan antar negara saat ini. Masyarakat di negara-negara maju sudah lazim dengan penggunaan elektronik dalam kehidupan mereka sehari-hari seperti pemakaian *e-banking*, *e-mail*, dan sebagainya. Selain itu, manfaat-manfaat menarik yang ditawarkan oleh *e-vote* membuat pemerintah di negara-negara maju seperti Amerika, Inggris, dan sebagainya sedang mengkaji bagaimana penerapan *e-vote* pada negara mereka.

Negara yang telah menerapkan *e-vote* dalam proses pemilihan umum skala nasional menurut berita Washington Post adalah Estonia. Negara ini pertama kali menerapkan *e-vote* pada tahun 2005. Untuk mendapatkan surat pemilihan dalam bentuk *online*, seorang pemilih membutuhkan kartu ID spesial, alat untuk membaca kartu tersebut, dan komputer dengan koneksi internet. Kartu ID spesial tersebut dapat menggunakan kartu ID untuk akun bank dan catatan pajak dan sebanyak 80% penduduk Estonia telah memilikinya sehingga *e-vote* dapat berjalan di negara tersebut. . Namun, menurut pemerintah Estonia kelemahan dari *e-vote* yang diterapkan di negara mereka adalah pemilih dimungkinkan untuk memilih lebih dari sekali walaupun hanya pilihan terakhir yang dihitung. Kelemahan tersebut memungkinkan pemilih menukar suaranya dan hal ini tidak sesuai dengan asas pemilu.

Kelebihan dari *e-vote* sangat banyak jika dibandingkan menggunakan sistem pemilihan non-elektronik. Kelebihan pertama adalah memungkinkan pemilih yang berada di luar negeri atau berada di lokasi yang jauh dari tempat pemilihan umum untuk tetap dapat memberikan suaranya. Dengan kelebihan ini, jumlah partisipasi pemilih dapat meningkat tajam dibandingkan menggunakan sistem pemilihan umum non-elektronik. Kelebihan berikutnya adalah proses perhitungan surat suara membutuhkan waktu yang lebih cepat dibandingkan sistem biasa karena perhitungan dapat dilakukan secara otomatis oleh mesin saat surat suara dianggap sah oleh sistem elektronik. Proses perhitungan yang lebih cepat ini membuat hasil pemilihan dapat diumumkan lebih cepat. Ketiga, proses *e-vote* lebih praktis karena para pemilih tidak perlu mengantri berlama-lama untuk memberikan suaranya. Panitia juga tidak perlu mengestimasi jumlah kertas yang dibutuhkan ataupun mengecek surat pemilihan yang cacat. Terakhir, proses *e-vote* ini juga dapat menekan biaya yang dikeluarkan jika menggunakan sistem pemilihan biasa seperti biaya kertas, biaya kotak suara, biaya jasa panitia di posko pemilihan, biaya konsumsi panitia, biaya transportasi surat suara pemilihan umum, dan sebagainya.

Dengan segala kelebihan tersebut, banyak negara baik negara maju maupun negara berkembang masih belum memanfaatkan *e-vote* dalam proses pemilihan umum di negaranya. Hal ini dikarenakan, negara-negara tersebut masih mengkaji keamanan dari *e-vote* ini. Hasil dari pemilihan umum di suatu negara untuk penentuan Presiden atau anggota MPR-DPR sangat berharga untuk diserang agar hasilnya sesuai dengan kepentingan golongan tertentu.

Salah satu cara untuk mengatasi masalah-masalah keamanan dalam sistem *e-vote* yaitu dengan mengaplikasikan kriptografi. Pada makalah ini akan dibahas bagaimana tanda tangan digital dan enkripsi/dekripsi dimanfaatkan dalam menanggulangi serangan-serangan pada keamanan *e-vote*.

## II. DASAR TEORI

### A. Pemilihan Umum Elektronik (*E-Vote*)

*E-vote* merupakan sistem yang memanfaatkan perangkat elektronik dan mengolah informasi digital untuk membuat surat suara, memberikan suara, menghitung dan menayangkan perolehan suara, serta memelihara dan menghasilkan jejak audit (kompas.com). Sebagian besar orang mengidentikkan *e-vote* dengan pemberian suara melalui internet. Padahal, pemberian suara melalui internet merupakan salah satu bentuk *e-vote*.

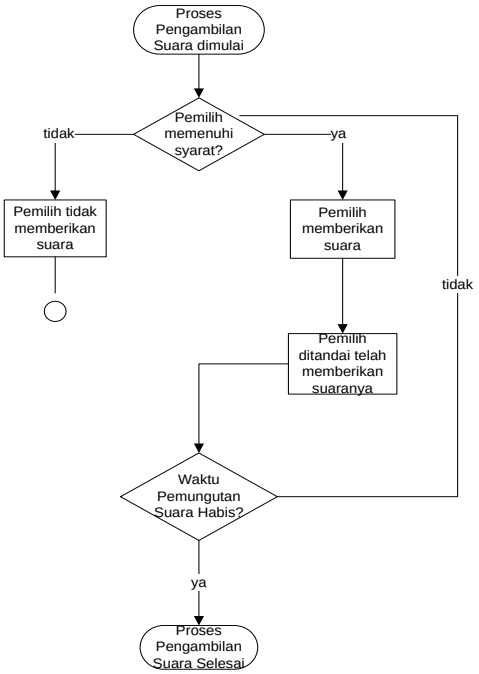
*E-vote* dapat diartikan menjadi dua bentuk. Pertama, elektronik digunakan sebagai alat untuk melemparkan suara dan pengertian pertama ini mengarah ke internet sebagai media pemilihan umum elektronik. Dengan cara ini, pemilihan tidak harus dilakukan pada posko pemungutan suara tetapi dilakukan dimana saja. Pengertian kedua mengarah ke DRE (*Direct Recording Electronic*) sebagai media pemilihan umum elektronik. DRE adalah komputer yang menampilkan surat suara di layar, kemudian pengguna memberikan suaranya baik dengan menekan tombol atau melalui *touchscreen*. Proses perhitungan suara dilakukan secara otomatis saat suara diberikan oleh pemilih.

**Gambar 1 Contoh DRE (*Direct Recording Electronic*)**

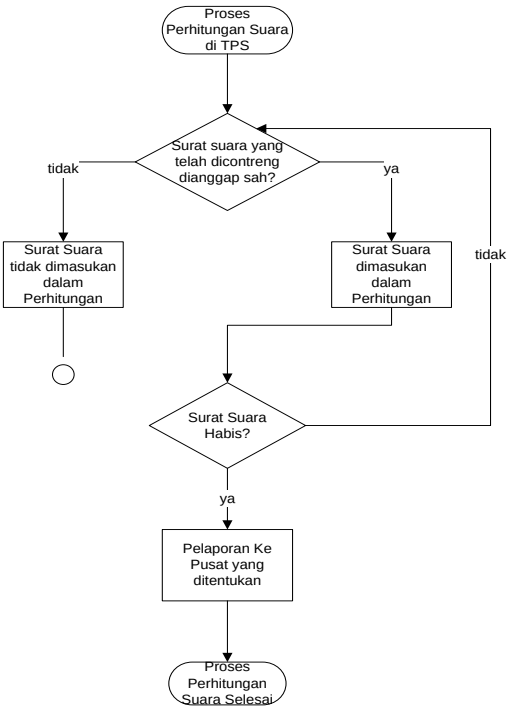
Pada makalah ini penulis lebih menekankan pada pengertian *e-vote* yang pertama yaitu pemberian suara melalui internet. Prosedur *e-vote* berbeda dengan prosedur pemilihan umum non-elektronik. Namun, sampai saat ini belum ada prosedur *e-vote* yang terdefinisi dengan jelas. Pada dasarnya, baik prosedur secara elektronik maupun non-elektronik bertujuan untuk mencapai asas pemilihan umum yaitu langsung, bebas, rahasia, serta jurdil (jujur dan adil).

### B. Prosedur Pemilihan Umum Saat Ini.

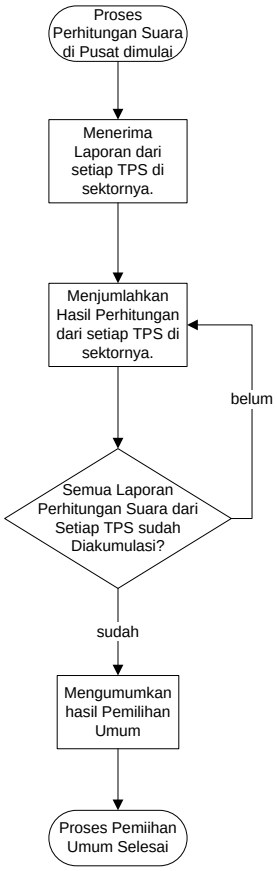
Berdasarkan Pedoman Pemilihan Umum yang dimiliki KPU (Komisi Pemilihan Umum), proses pemilihan umum dimulai dari proses pemberian suara, perhitungan suara, sampai pada penentuan hasil pemilu. Proses pemberian surat suara ditunjukkan pada Gambar 2, proses perhitungan suara pada Gambar 3, dan pengumuman hasil pemilu pada Gambar 4.




**Gambar 2 Prosedur Pemberian Suara**




**Gambar 3 Proses Perhitungan Suara di TPS**




**Gambar 4 Proses Pengumuman Hasil Pemilu**

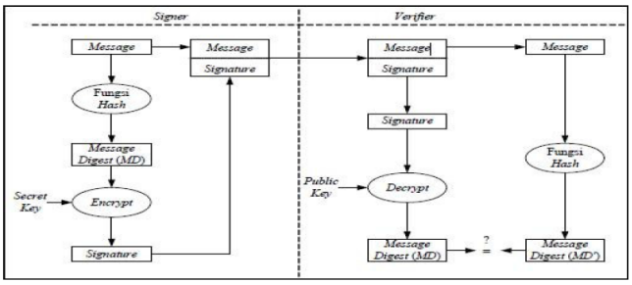
## *C.* Tanda Tangan Digital

Tanda tangan digital adalah nilai kriptografis yang bergantung pada isi pesan dan kunci. Tanda tangan digital berfungsi sebagai otentikasi pada data digital (pesan, dokumen elektronik). Terdapat dua cara menandatangani pesan yaitu enkripsi pesan atau menggunakan kombinasi fungsi hash dan kriptografi kunci-publik. Pada makalah ini metode yang digunakan adalah metode kedua yaitu kombinasi fungsi hash dan kriptografi kunci-publik karena metode ini dapat memberikan solusi otentikasi dan anti-penyangkalan yang dibutuhkan dalam proses pemilu.

Pesan pertama kali dienkripsi dengan kunci privat pengirim dan pesan didekripsi pesan dengan kunci publik pengirim sehingga kerahasian pesan dan otentikasi keduanya dicapai sekaligus. Namun, hanya algoritma kunci-publik yang memenuhi sifat (1) yang dapat dimanfaatkan dalam tanda tangan digital.

$$D_{SK}(E_{PK}(M)) = M \text{ dan } D_{PK}(E_{SK}(M)) = M \qquad (1)$$

Jika tanda tangan digital bertujuan untuk otentikasi dan integritas data, maka penggunaan algoritma kunci-publik dikombinasikan dengan fungsi hash. Diagram proses verifikasi pesan ditunjukkan Gambar 5.




**Gambar 5 Proses Verifikasi pada Tanda Tangan Digital**

Keotentikan dan integritas data dibuktikan dengan melihat *message digest* hasil fungsi *hash* pesan dan hasil dekripsi *signature.* Jika kedua *message digest* bernilai sama, maka dapat ditarik informasi bahwa pesan yang diterima adalah pesan asli dari pengirim yang sebenarnya.

## D. Fungsi *Hash* Satu Arah

Fungsi *hash* adalah fungsi yang menerima masukkan *string* yang panjangnya sembarang dan mengkonversinya menjadi *string* keluaran yang panjangnya tetap (*fixed*). Fungsi ini mengkompresi sembarang pesan menjadi *message digest* yang ukurannya selalu tetap. Fungsi ini satu arah karena pesan yang sudah diubah menjadi *message digest* tidak dapat dikembalikan lagi menjadi pesan semula. Fungsi *hash* selalu memberikan nilai yang berbeda untuk pesan yang berbeda.

## E. Kriptografi Kunci Publik

Kriptografi kunci publik merupakan kriptografi yang melibatkan dua kunci untuk proses enkripsi dan dekripsi. Dua kunci tersebut adalah kunci publik, yaitu kunci yang diketahui umum/publik, dan kunci privat, yaitu kunci yang hanya diketahui seseorang/privat. Dengan kedua kunci ini, tidak ada kebutuhan mengirimkan kunci rahasia seperti halnya pada sistem kriptografi simetri.

# III. ANALISIS *E-VOTE* YANG AMAN

## *A.* Analisis Kebutuhan Keamanan Sistem *E-vote*

Sebelum mendesain prosedur dan sistem keamanan *e-vote* yang aman, terlebih dahulu perlu dianalisis kebutuhan keamanan sistem *e-vote* agar prosedur dan sistem yang dirancang dapat memenuhi kebutuhan tersebut. Analisis kebutuhan yang dibahas pada makalah ini terbatas pada sistem keamanan dimana prinsip kriptografi dapat diterapkan.

Pemilu bertujuan untuk melaksanakan kedaulatan rakyat dengan menghimpun suara masyarakat untuk menentukan para pemimpin negeri. Dengan tujuan tersebut, maka jaminan bahwa suara yang diberikan oleh pemilih tidak berubah dan diperhitungkan untuk menentukan hasil pemilu penting. Selain itu, jaminan hanya orang-orang yang berhak memberikan suara juga penting untuk menghindari kecurangan dalam pemilu.

Pemilihan secara elektronik memungkinkan terjadinya serangan-serangan sebagai berikut:

- Pemilihan melalui internet dilakukan pada tempat pemilih masing-masing tanpa diawasi pengawas/ panitia pemilu. Beberapa serangan dapat terjadi dalam

kondisi seperti ini. Pertama, orang yang tidak berhak dapat memberikan suaranya karena tidak ada panitia yang mengecek/ memvalidasi pemilih. Kedua, pemilih dapat memberikan suara lebih dari satu kali. Pada sistem pemilu menggunakan kertas, setelah pemilih memberikan suaranya maka pemilih ditandai dengan tinta pada jarinya. Hal ini berbeda dengan pemilihan melalui internet dimana belum ada mekanisme untuk menandai pemilih yang telah memberikan suaranya. Selain itu, tidak adanya pengawas pada pemilu melalui internet membuat pendeteksian pemilih yang telah memberikan suara menjadi semakin sulit. Ketiga, orang dapat menggunakan hak suara orang lain karena pemberian suara tidak diawasi panitia sehingga memungkinkan pencurian hak suara orang lain.

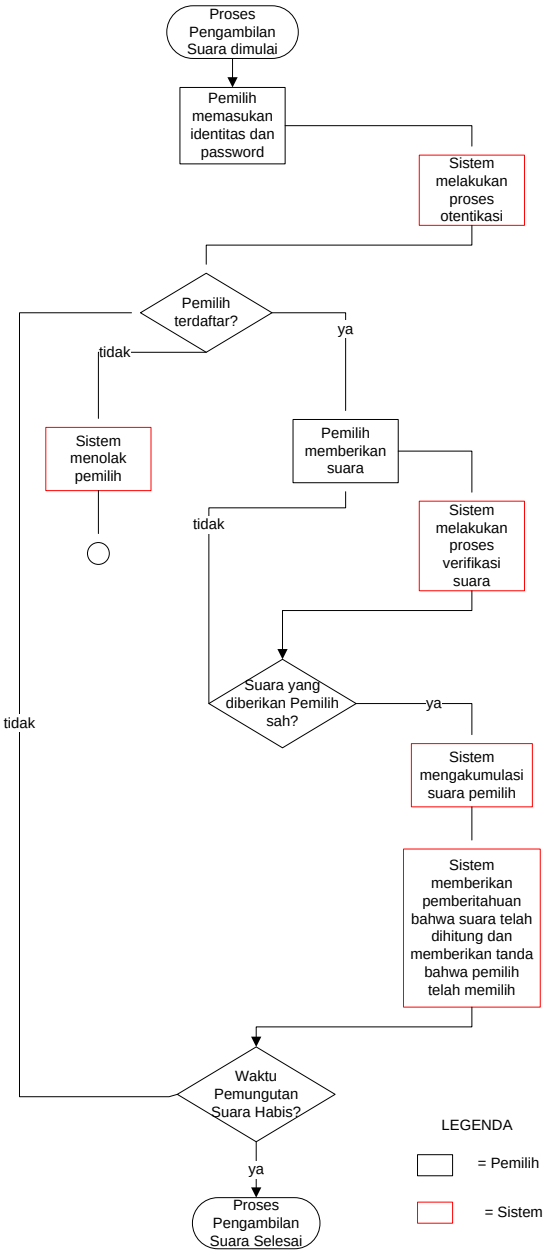
- Penyadapan *password* yang digunakan sebagai proses otentikasi. Pengiriman pesan mulai dari proses otentikasi sampai proses pemberian suara melalui jaringan internet sangat rentan untuk disadap dan disalahguanakan oleh pihak lain.
- Suara yang diberikan oleh pemilih dikirimkan melalui internet. Serangan untuk mengganti isi suara tersebut mungkin dilakukan karena orang dapat menyadap jalur informasi tersebut dan mengubah pesan (isi suara) tersebut. Serangan ini juga berlaku pada kasus pelaporan hasil perhitungan ke pusat. Dengan demikian, setiap kali penerimaan pesan dari pemilih diperlukan pengecekan apakah pesan yang diterima merupakan pesan sebenarnya dan apakah pengirim adalah orang yang sebenarnya.
- Jika pada pemilu non-elektronik, pemilih dapat mengetahui bahwa suara yang diberikan pasti diperhitungkan jika surat suara yang diberikan sah. Namun pada pemilu melalui internet, pemilih tidak dapat mengetahui secara pasti apakah suara yang diberikan sampai pada pihak panitia untuk diperhitungkan. Selain itu, sifat pemilu yang anonim membuat pelacakan surat suara hilang atau malah bertambah menjadi semakin sulit.
- Serangan juga dapat datang dari pihak pengembang *software* sistem *e-vote*. Dengan demikian, pihak pengembang yang jujur dan adil juga penting untuk menghindari *software* dirancang bagi kepentingan golongan tertentu.

### *B.* Analisis Prosedur *E-vote*

Berdasarkan pemaparan di bagian sebelumnya, prosedur *e-vote* memerlukan beberapa modifikasi dari prosedur yang didefinisikan pemilihan non-elektronik saat ini. Berikut ini prosedur yang diusulkan bagi *e-vote* agar meningkatkan aspek keamanan *e-vote*.

Prosedur pemberian suara yang ditunjukkan pada Gambar 6 dimaksudkan untuk mengatasi serangan-serangan berikut ini:

- Serangan orang yang tidak berhak memberikan suara diatasi dengan proses otentikasi dari sistem. Proses otentikasi membutuhkan data rahasia dimana orang yang tidak berhak tidak mengetahui data tersebut sehingga tidak dapat mengakses sistem.




**Gambar 6 Prosedur Pemberian Suara Sistem *E-vote***

- Serangan pemilih yang memberikan suara lebih dari satu kali diatasi juga dengan proses otentikasi. Proses otentikasi tidak hanya memvalidasi apakah pemilih berhak tetapi juga mengecek apakah pemilih telah memberikan hak suaranya. Sistem dapat mengetahui apakah pemilih telah memberikan suaranya dengan tanda yang diberikan saat pemilih telah berhasil memberikan suaranya.
- Serangan penyadapan *password* yang digunakan sebagai proses otentikasi dapat diatasi dengan menggunakan proses otentikasi dengan cara yang tidak memerlukan *password* untuk mengotentikasi pemilih.
- Serangan orang yang menggunakan hak akses orang lain dapat diatasi dengan proses otentikasi yang dapat mengidentifikasi pemilih secara unik seperti sidik jari. Hal ini didukung karena sistem e-ktp saat ini mencatat data sidik jari setiap masyarakat Indonesia yang telah memiliki e-ktp. Dengan demikian, data sidik jari

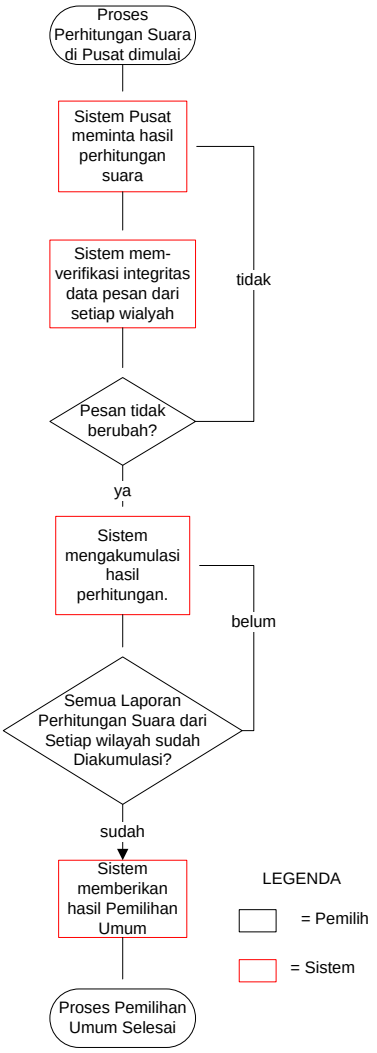
masyarakat Indonesia dapat digunakan untuk proses otentikasi e-*vote* nantinya.

- Serangan penghilangan sejumlah surat suara atau penambahan sejumlah surat suara diatasi dengan perhitungan secara langsung saat suara dianggap sah oleh sistem.
- Serangan ketidakpercayaan pemilih apakah suara yang diberikan ikut diperhitungkan diatasi dengan pemberitahuan jika suara yang diberikan dianggap sah sesuai peraturan yang berlaku. Selain mengatasi masalah ini, sistem juga dapat mengatasi kesalahan pemilih saat memberikan suaranya sehingga tidak ada suara yang cacat.
- Serangan penggantian suara saat pesan dalam perjalanan dari pemilih ke sistem diatasi dengan proses verifikasi. Proses verifikasi melakukan pengecekan apakah pemilih telah memberikan suara secara benar sesuai dengan ketentuan yang berlaku, mengecek apakah suara tersebut berasal dari pemilih yang sebenarnya, dan juga mengecek integritas suara. Jika ketiga kondisi ini terpenuhi, maka suara dianggap sah, dan begitu juga sebaliknya.

Untuk memberikan pemberitahuan jika suara yang diberikan dianggap sah, sistem harus melakukan proses verifikasi terlebih dahulu. Jika proses verifikasi berhasil, maka suara diakumulasi oleh sistem. Dengan demikian, proses perhitungan suara semakin cepat karena perhitungan suara dilakukan bersamaan dengan proses pengumpulan suara sehingga sistem *e-vote* menghemat satu tahapan (tahapan perhitungan suara di TPS) dibandingkan sistem pemilihan biasa.

Setelah waktu proses pengambilan suara selesai, suara dari seluruh wilayah diakumulasi sehingga mendapatkan hasil keseluruhan untuk menentukan kandidat yang terpilih (proses pengumuman hasil pemilu). Serangan yang dapat terjadi pada tahap ini adalah mengganti isi pesan (hasil perhitungan suara di setiap wilayah). Serangan ini dapat diatasi dengan proses verifikasi seperti yang dilakukan pada saat verifikasi suara dalam prosedur pemberian suara (Gambar 6). Namun, proses verifikasi pada prosedur ini (Gambar 7) hanya bertujuan untuk mengecek integritas pesan dan mengecek apakah pesan berasal dari orang yang sebenarnya.

Sistem yang tidak terpusat dan dibagi dalam beberapa wilayah diusulkan karena sistem yang terpusat lebih rentan untuk diserang. Jika sistem terpusat diserang, maka pemilu menjadi gagal. Namun pada sistem tidak terpusat, jika ada sistem yang diserang, maka terdapat sistem di daerah lain yang dapat digunakan sebagai alternatif untuk menggantikan sistem yang rusak tersebut.




**Gambar 7 Prosedur Pengumuman Hasil Pemilu**

## *C.* Penerapan Tanda Tangan Digital pada Keamanan Sistem *E-vote.*

Proses verifikasi pada prosedur yang dijelaskan pada bagian B digunakan untuk mengecek integritas pesan yang diterima dan mengecek apakah pesan berasal dari orang yang sebenarnya. Proses otentikasi pemilih tidak hanya bertujuan untuk mengotentikasi pemiilih dan mencegah kemungkinan pemilih memberikan suara lebih dari sekali, tetapi juga mencegah penyadapan *password*. Semua tujuan pada kedua proses tersebut dapat tercapai dengan memanfaatkan tanda tangan digital. Seperti yang dijelaskan pada bagian C, tanda tangan berfungsi untuk mengetahui otentikasi pesan dan integritas pesan.

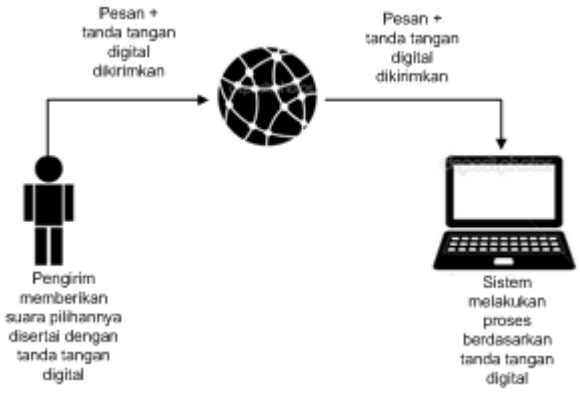
Skema proses otentikasi pemilih yang diusulkan dengan menerapkan tanda tangan digital sebagai berikut:

1. Jika pemilih ingin memberikan suaranya, maka pemilih tidak perlu memasukkan *password* seperti proses otentikasi biasanya, melainkan cukup mengirimkan pesan "identitas pemilih" dan disertai dengan tanda tangan digital.
2. Tanda tangan digital dibuat dengan membuat *message digest* dari pesan "identitas pemilih" dengan fungsi *hash* dan mengenkripsi *message digest* tersebut dengan

kunci privat pemilih yang telah diberikan oleh panitia pemilu.
3. Jika identitas pemilih telah ditandai, maka otentikasi tidak dilanjutkan karena pengirim telah memberikan suaranya.
4. Sistem mendekripsi tanda tangan digital yang diterima dengan kunci publik pada basis data yang dimiliki sistem. Kunci publik diketahui melalui id pemilih.
5. Sistem meringkas pesan yang diterima menjadi *message digest* dengan fungsi *hash* yang sama.
6. Sistem membandingkan *message digest* hasil dekripsi tanda tangan digital dan *message digest* dari fungsi *hash*. Jika kedua *message digest* bernilai sama, maka pemilih berhasil melewati tahap otentikasi.

Skema proses verifikasi yang diusulkan dengan menerapkan tanda tangan digital sebagai berikut:

1. Pemilih mengirimkan pesan "suara pemilih" dan disertai dengan tanda tangan digital.
2. Tanda tangan digital dibuat dengan membuat *message digest* dari pesan "suara pemilih" dengan fungsi *hash* dan mengenkripsi *message digest* tersebut dengan kunci privat pemilih yang telah diberikan oleh panitia pemilu.
7. Sistem mendekripsi *digital signature* yang diterima dengan kunci publik pada basis data yang dimiliki sistem. Kunci publik diketahui melalui id pemilih.
3. Sistem meringkas pesan suara yang diterima menjadi *message digest* dengan fungsi *hash* yang sama.
4. Sistem membandingkan *message digest* hasil dekripsi tanda tangan digital dan *message digest* dari fungsi *hash*. Jika kedua *message digest* bernilai sama, maka suara dianggap sah dan diterima oleh sistem.




**Gambar 8 Arsitektur Penerapan Tanda Tangan Digital dalam Sistem *E-vote***

Inti keamanan komunikasi melalui internet adalah tidak ada pihak lain yang dapat mengubah atau mengambil informasi tersebut selain kedua pihak yang terkait. Prinsip penggunaan tanda tangan digital dalam sistem pemilihan melalui internet ditunjukkan pada Gambar 8. Dengan penggunaan tanda tangan digital, inti keamanan komunikasi melalui internet dapat tercapai.

## IV. IMPLEMENTASI

Seperti yang telah dijelaskan bawa di sisi pemilih dilakukan proses pemberian tanda tangan digital untuk setiap pesan yang dikirmkan dan di sisi sistem dilakukan proses pengecekan pesan yang diterima. Dengan demikian, pada sisi pemilih dibutuhkan aplikasi untuk membuat tanda tangan digital dan menempelkannya pada pesan (suara yang diberikan pemilih) dan pada sisi sistem dibutuhkan aplikasi untuk mengecek pesan yang masuk melalui tanda tangan digital. Kedua aplikasi ini dapat menggunakan modul yang sama yaitu modul fungsi *hash* dan enkripsi/dekripsi kunci publik. Namun, pada sisi sistem terdapat modul tambahan untuk memfasilitasi fungsi membandingkan *message digest*.

Fungsi *hash* yang digunakan kali ini adalah fungsi SHA-1. SHA-1 menerima masukan berupa pesan dengan ukuran sembarang dan maksimal $2^{64}$ bit dan menghasilkan *message digest* yang panjangnya 160 bit. Algoritma pembuatan *message digest* secara garis besar sebagai berikut:

1. Penambahan bit-bit pengganjal (*padding bits*).
2. Penambahan nilai panjang pesan semula.
3. Inisialisasi penyangga *buffer* MD.
4. Pengolahan pesan dalam blok berukuran 512 bit.

Pada proses pembuatan tanda tangan digital, *message digest* yang telah dibentuk dienkripsi dengan algoritma kunci publik untuk memperkuat pengiriman pesan. Algoritma tanda tangan digital yang digunakan adalah ElGamal. Keamanan ElGamal terletak pada sulitnya menghitung logaritma diskrit. Elgamal memiliki kunci privat dan publik untuk proses enkripsi dan dekripsinya. Algoritma pembangkitan kunci dilakukan sebagai berikut:

1. Memilih secara acak nilai x dengan $1 < x < p-1$
2. Hitung $y = g^x \bmod p$
3. Kunci publik adalah (p,g,y)
4. Kunci privat adalah x

Algoritma pembangkitan tanda tangan digital dengan Elgamal sebagai berikut:

1. Memilih secara acak nilai k dimana $0 < k < p-1$ dan $\gcd(k, p-1) = 1$
2. Hitung $r \equiv g^k \pmod p$.
3. Hitung $s \equiv (H(m) - xr)k^{-1} \pmod{p-1}$
4. Jika $s = 0$ mulai lagi dari awal

Pasangan (r, s) adalah tanda tangan digital dari m.

Algoritma proses verifikasi tanda tangan digital sebagai berikut:

1. $0 < r < p$ dan $0 < s < p-1$
2. $g^{H(m)} \equiv y^r r^s \pmod p$

Verifikasi menerima tanda tangan digital jika semua kondisi dipenuhi dan begitu juga sebaliknya.

Untuk implementasi prototipe aplikasi tanda tangan digital, penulis menggunakan bahasa C# dan Microsoft Visual C#. Kebutuhan kelas implementasi prototipe didefinisikan sebagai berikut:

**Tabel 1 Kelas Implementasi Tanda Tangan Digital**

| No | Kelas | Fungsi |
|---|---|---|
| 1. | SHA | Untuk implementasi fungsi *hash* |
| 2. | ElGamalSignature | Untuk implementasi pembangkitan tanda tangan digital dengan algoritma ElGamal |
| 3. | GUI | Untuk antarmuka dan program utama |

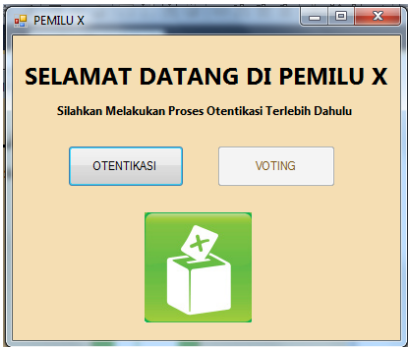
| | | |
|---|---|---|
| 4. | BigInteger | Kelas implementasi bilangan integer besar yang dibutuhkan untuk parameter ElGamal. |

Pada tugas ini, diasumsikan bahwa setiap pemilih telah mengetahui kunci privatnya masing-masing dan sistem memiliki kunci publik yang berpadanan dengan kunci yang dimiliki oleh pemilih. Kunci publik disimpan sesuai dengan identitas pemilih sehingga penggunaan kunci publik berdasarkan identitas yang diterima oleh sistem.Tanda tangan digital ditambahkan pada bagian akhir pesan dengan format <ds><tanda_tangan.></ds>. Aplikasi ini memanfaatkan beberapa fungsi yang telah dibuat pada tugas besar 4 yaitu tanda tangan digital.

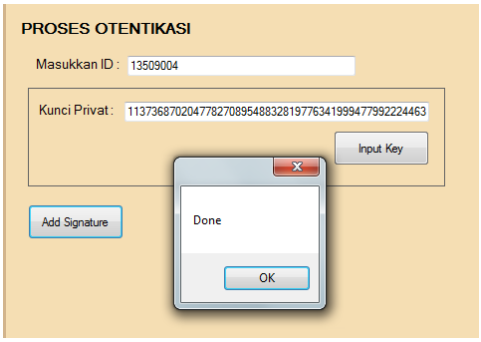
**Tabel 2 Skenario Pengujian Tanda Tangan Digital pada Sistem *E-vote***

| Skenario | Otentikasi | *Voting* |
|---|---|---|
| Sisi Pemilih | 1. Pemilih memilih menu otentikasi pada layar<br>2. Pemilih memasukkan id<br>3. Pemilih memilih menu *input key*<br>4. Pemilih memasukkan nilai kunci privat<br>5. Pemilih memilih menu *add signature*<br>6. Pemilih mengirimkan pesan<br>7. Jika berhasil, menu *vote* dapat diakses oleh pemilih. | 1. Pemilih memilih menu *vote* pada layar<br>2. Pemilih memasukkan suara pilihannya.<br>3. Pemilih memilih menu *input key*<br>4. Pemilih memasukkan nilai kunci privat<br>5. Pemilih memilih menu *add signature*<br>6. Pemilih mengirimkan pesan<br>7. Pemilih mendapatkan pemberitahuan suara telah dicatat<br>8. Jika gagal, maka pemilih dapat mengulang *vote* |
| Sisi Sistem | 1. Sistem menerima id<br>2. Sistem mengecek apakah id tersebut telah memberikan suara.<br>3. Jika berhasil, sistem melakukan proses verifikasi keaslian pesan dan pengirim pesan tersebut melalui tanda tangan digital<br>4. Jika proses otentikasi berhasil, pemilih dapat melanjutkan akses pada tahapan berikutnya dan begitu juga sebaliknya. | 1. Sistem menerima pilihan pemilih.<br>2. Sistem melakukan proses verifikasi keaslian pesan dan pengirim pesan tersebut melalui tanda tangan digital<br>3. Jika proses verifikasi berhasil, suara pemilih langsung diakumulasikan dengan suara lainnya<br>4. Sistem memberikan pemberitahuan jika suara berhasil dianggap sah. |

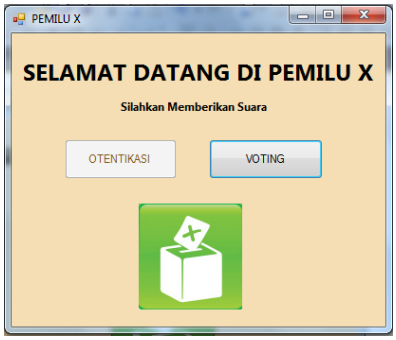
Antar muka hasil pengujian di sisi pemilih ditunjukkan pada gambar di bawah ini.



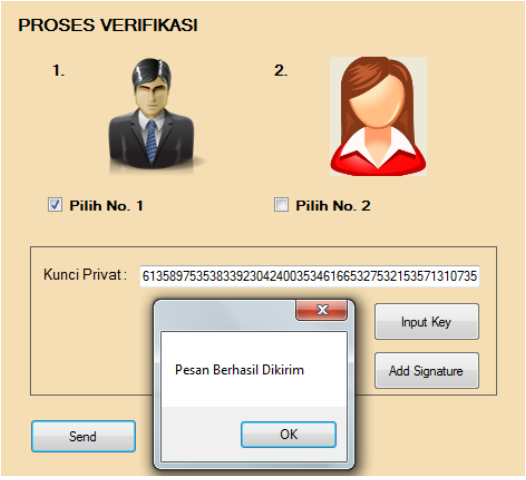

**Gambar 9 Antar Muka Pertama Kali Pemilih Mengakses**




**Gambar 10 Proses Otentikasi di Sisi Pemilih**




**Gambar 11 Proses Otentikasi Berhasil, *Vote* Dapat Diakses**

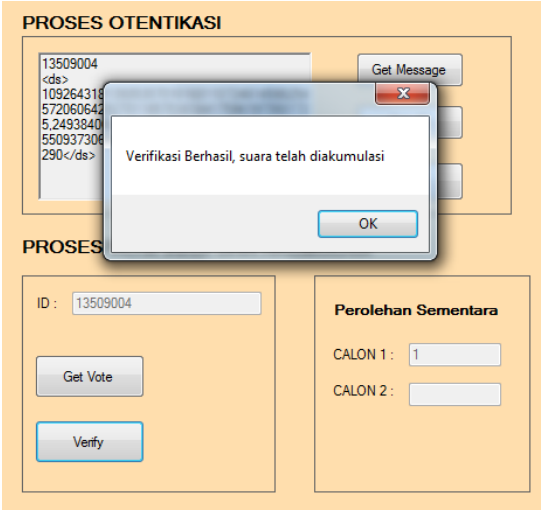



**Gambar 12 Proses *Voting* di Sisi Pemilih.**


**Gambar 13 Pemberitahuan Proses *Voting* Berhasil.**

Antar muka hasil pengujian di sisi sistem/panitia pemilu ditunjukkan pada gambar di bawah ini.


**Gambar 14 Proses Otentikasi Berhasil**




**Gambar 15 Proses Verifikasi dan Akumulasi Berhasil**

## VI. KESIMPULAN

Berdasarkan hasil implementasi dapat disimpulkan bahwa tanda tangan digital dapat dilakukan terhadap pesan yang dikirimkan melalui internet. Pemanfaatan tanda tangan digital pada *e-vote* dapat meningkatkan keamanan dengan cara memanfaatkan tanda tangan digital pada proses otentikasi pemilih dan proses verifikasi suara yang diberikan. Berbagai serangan-serangan yang dapat diatasi dengan pemanfaatan tanda tangan digital pada *e-vote* antara lain serangan orang yang tidak berhak, serangan penyadapan *password* pemilih, serangan pergantian suara saat hilang, dan lain-lain seperti yang dijelaskan pada bab III bagian B.

Selain serangan-serangan yang dapat diatasi tersebut, terdapat pula serangan lain yang belum diatasi misalkan serangan dari pihak pengembang *software*. Sistem ini dapat direalisasikan jika masyarakat di suatu negara sudah terbiasa dengan pengguanaan sistem elektronik. Di Indonesia sendiri, masih banyak daerah dimana masyarakatnya belum terbiasa dengan penggunaan elektronik sehingga perlu dikaji lagi bagaimana penerapan *e-vote* yang sesuai dengan kondisi masyarakat Indonesia. Jaringan internet yang baik di suatu negara juga diperlukan untuk menunjang berjalannya *e-vote* di negara tersebut. Selain itu, pengaturan manajemen kunci dan distribusi pasangan kunci masyarakat dan panitia pemilu juga perlu diperhatikan sehingga keamanan yang telah dirancangkan dapat berjalan dengan baik.

## V. ACKNOWLEDGMENT

Penulis mengucapkan terima kasih kepada Bapak Rinaldi Munir, selaku dosen mata kuliah Kriptografi, atas bimbingannya dalam penyusunan makalah ini.

## VI. REFERENCES

Munir, Rinaldi. 2012. *Algoritma Kriptografi Klasik*, (*http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2010-2011/kripto10-11.htm#SlideKuliah*, diakses tanggal 18 Mei 2013)

Pedoman Teknis Pemungutan dan Perhitungan Suara. 2012. [Online]. Tersedia: http://kpu.tasikmalayakota.go.id/wp-kpu/wp-content/uploads/2012/06/7.-Pedoman-Teknis-Pemungutan-dan-Penghitungan-Suara.pdf. Tanggal Akses: 17 Mei 2013.

Tersedia: http://www.howstuffworks.com/e-voting.htm. Tanggal Akses: 21 April 2013.
Evans, David dan Paul, Nathanael, "Election Security: Perception and Reality," IEEE, 2003. [Online]. Tersedia: www.computer.org/security/. Tanggal Akses: 17 Mei 2013.

## 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, 20 Mei 2013

ttd

Amelia Natalie / 13509004