Penerapan Kriptografi Asimetris untuk Pengamanan Pemungutan Suara Pemira KM ITB

Tubagus Andhika Nugraha (13510007)[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13510007@std.stei.itb.ac.id

***Abstract*—The abstract is to be in fully-justified italicized text, at the top of the left-hand column as it is here, below the author information. The abstract is to be in 9-point, single-spaced type, and may be up to 8 cm long. Define all symbols used in the abstract. Do not cite references in the abstract. Do not delete the blank line immediately above the abstract; it sets the footnote at the bottom of this column. Leave two blank lines after the index terms, then begin the main text. All manuscripts must be in English.**

***Index Terms*—About four key words or phrases in alphabetical order, separated by commas.**

I. PENDAHULUAN

A. Latar Belakang

Keluarga Mahasiswa ITB adalah organisasi kemahasiswaan terpusat Institut Teknologi Bandung yang keanggotaannya meliputi seluruh mahasiswa Sarjana di Institut Teknologi Bandung. Organ utama KM ITB terdiri atas Kongres, Kabinet, dan Tim Beasiswa. Kongres memegang peran legislatif, seperti DPR pada tatanan pemerintahan Republik Indonesia, dan mewakili suara dan kepentingan organisasi-organisasi konstituten KM ITB, yakni Himpunan Mahasiswa Jurusan. Kabinet memegang peran eksekutif dan menjalankan kegiatan utama KM ITB sehari-hari.

Kabinet KM ITB dipimpin oleh seorang Ketua Kabinet Keluarga Mahasiswa (K3M), atau yang sebelumnya disebut sebagai Presiden KM ITB. K3M dipilih melalui rangkaian Pemilihan Umum Raya, atau yang disebut dengan Pemira. Pelaksana teknis Pemira berada di bawah kendali Kongres KM ITB.

Sejak tahun 2012, Pemira KM ITB dilakukan dengan mesin e-vote karya FMIPA ITB, yang pada mulanya digunakan untuk pemilihan Ketua Ikatan Alumni ITB. Setelah pemungutan suara selesai, mesin-mesin e-vote berikut catatan perolehan suara masing-masing calon ditahan oleh Panitia Pelaksana Pemira.

Pada tahun 2013, terjadi serangkaian kasus yang menyebabkan Panpel menunda penghitungan suara dan pengumuman pemenang, dan menahan mesin e-vote untuk masa waktu yang lama. Keberadaan mesin e-vote dirahasiakan dari semua kalangan, kecuali sekelompok orang yang identitasnya dirahasiakan dan hanya disebut sebagai ‘aman’.

‘Keamanan’ dari mesin e-vote tersebut sejauh ini hanyalah sebatas persoalan kepercayaan, karena tidak ada kendali teknis untuk memastikan tidak ada *tampering* pada perolehan suara. Tidak ada juga mekanisme kendali teknis untuk memastikan bahwa perolehan suara hanya diketahui oleh orang-orang yang memiliki hak. Pada makalah ini, diusulkan pemanfaatan kriptografi asimetris untuk mengamankan perolehan suara tersebut.

B. Rumusan Masalah

Makalah ini akan membahas:

1. Karakteristik persoalan Pemira KM ITB
2. Penerapan kriptografi asimetris

C. Batasan Masalah

Makalah ini hanya akan membahas persoalan Pemira KM ITB dan bukan pemilihan umum pada umumnya. Makalah ini juga hanya akan membahas secara teoretis bagaimana kriptografi dapat dimanfaatkan dalam Pemira KM ITB, dan tidak membahas bagaimana penerapannya secara fisik.

II. PEMIRA KM-ITB

Keluarga Mahasiswa ITB (KM ITB) adalah organisasi kemahasiswaan terpusat Institut Teknologi Bandung yang anggotanya mencakup seluruh mahasiswa sarjana Institut Teknologi Bandung.

Secara umum, organ KM ITB terdiri atas:

1. Kongres, yang beranggotakan perwakilan masing-masing Himpunan Mahasiswa Jurusan, yang disebut dengan Senator. Kongres merupakan perwujudan kedaulatan tertinggi dalam KM ITB.
2. Kabinet, badan eksekutif pelaksana program di tingkat pusat yang bertugas untuk mendinamisasi kampus melalui pencerdasan dan pemberdayaan mahasiswa di tingkat bawah. Kabinet dipimpin oleh seorang Ketua Kabinet KM ITB dan melapor secara langsung kepada Kongres.
3. Tim Beasiswa yang secara khusus menangani kesejahteraan mahasiswa dan melapor ke Kongres namun tidak bersifat politis.
4. Majelis Wali Amanat Wakil Mahasiswa atau MWA-WM, lembaga yang ditugaskan untuk mewakili mahasiswa dalam Majelis Wali Amanat

sebagai organ tertinggi di Institut Teknologi Bandung

Setiap tahunnya, seorang Ketua Kabinet KM ITB atau yang sebelumnya disebut sebagai Presiden KM ITB, serta seorang MWA-WM dipilih oleh seluruh mahasiswa sarjana di ITB. Proses pemilihan tersebut dinamakan Pemilu Raya KM ITB, atau umumnya dikenal sebagai Pemira.

Pemira memiliki asas-asas sebagai berikut:

1. Langsung, dalam artian anggota KM ITB secara langsung memilih Ketua Kabinet dan MWA-WM pilihannya;
2. Umum, dalam artian seluruh anggota KM ITB berhak untuk mengikuti rangkaian Pemira;
3. Bebas, dalam artian seluruh anggota KM ITB dibebaskan untuk memilih calon pilihannya tanpa paksaan dari pihak manapun;
4. Rahasia, dalam artian suara setiap pemilih tidak dapat dilacak ke pemilihnya, dan setiap pemilih berhak untuk mendapatkan kerahasiaan atas pilihannya;
5. Jujur, dalam artian tidak ada kecurangan selama masa pelaksanaan Pemira;
6. Adil, dalam artian setiap anggota mendapatkan hak dan kewajiban yang sama.

Pelaksana Pemira KM ITB disebut sebagai Panitia Pelaksana Pemira, atau disingkat Panpel. Selain panpel, dibentuk juga sebuah Panitia Pengawas Pemilu, atau Panwaslu, yang bertugas mengawasi seluruh kegiatan Pemira.

Pemira dimulai sejak pendataan daftar pemilih yang dilakukan oleh Panpel Pemira sampai pemberian legitimasi kepada peserta terpilih Pemira KM-ITB. Pemira diselenggarakan di akhir kepengurusan Kabinet dan MWA-WM KM ITB.

Tahapan Pemira meliputi:

1. Pendataan daftar pemilih
2. Pendaftaran calon peserta Pemira
3. Pengujian kelayakan administrasi calon peserta
4. Pengumuman peserta
5. Masa kampanye
6. Masa tenang
7. Pemungutan suara
8. Penghitungan suara
9. Penetapan hasil Pemira
10. Pemberian legitimasi kepada peserta terpilih

Kesepuluh tahapan tersebut diatur lebih lanjut dalam dokumen yang disebut Tata Cara Pemira.

Pada tahap pemungutan suara, sebelum tahun 2012, pemungutan suara menggunakan kertas suara yang kemudian secara manual dihitung bersama. Mekanisme tersebut tidak berbeda jauh dengan rangkaian pemilihan umum yang dilakukan oleh Indonesia untuk memilih anggota legislatif, kepala daerah, dan kepala negara.

Sebelumnya, mekanisme pemungutan suara dilaksanakan dengan menggunakan kertas suara yang kemudian dihitung secara manual. Dengan asumsi kotak suara dijaga dengan ketat dan hanya diisi dengan kertas suara yang dibuat oleh pemilih yang sah, maka keabsahan setiap kertas suara yang ada dapat diperiksa oleh siapapun, dan dapat dipastikan tidak ada *tampering* yang dilakukan terhadap kertas suara. Setiap kertas suara juga sama sekali tidak terhubung ke identitas pemilih di balik kertas suara tersebut.

Meski kesederhanaan pemungutan suara menjamin keabsahan setiap suara, kesederhanaan tersebut juga berarti penghitungan suara dilakukan secara manual, satu per satu. Proses tersebut menghabiskan waktu yang cukup lama dan tenaga yang cukup besar.

Oleh sebab itu, sejak tahun 2012, Pemira KM ITB memanfaatkan mesin *e-voting* karya Laboratorium Elektronika dan Instrumentasi FMIPA ITB. Mesin tersebut pada mulanya digunakan untuk pemilihan Ketua Umum IA ITB tahun 2011. Mesin tersebut terdiri atas tiga bagian:

1. Mesin untuk memilih sekaligus mencetak kertas audit. Mesin tersebut terdiri dari enam tombol, yang masing-masing mewakili satu orang calon, kecuali tombol terakhir, yang digunakan untuk pemilih yang memilih abstain.
2. Mesin untuk menyimpan suara.
3. Lampu bohlam sebagai penanda.

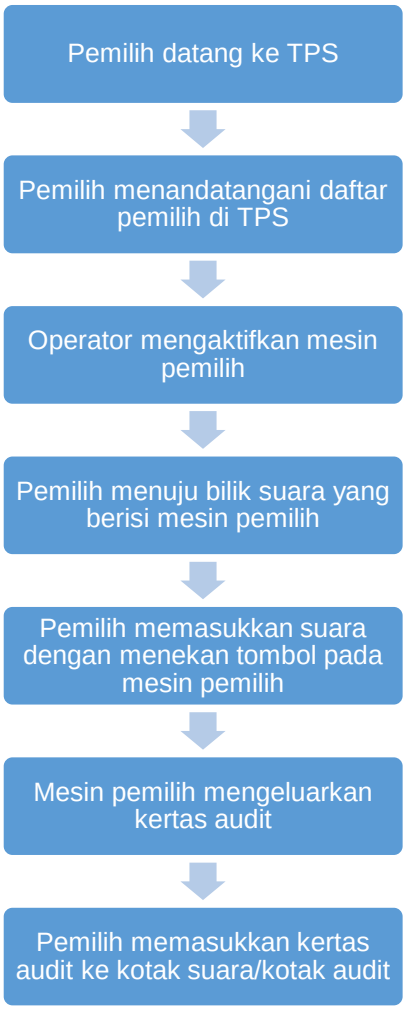
Setiap suara direkam secara elektronik ke dalam memori mesin, kemudian hasil pemungutannya dapat diketahui dengan menjumlahkan hasil penghitungan yang terdapat di masing-masing mesin. Sebagai cadangan, mesin juga mecetak lembaran kertas suara yang dapat digunakan untuk penghitungan secara manual.

Pada mesin *e-vote* yang sudah ada selama ini, setiap suara hanya disimpan sebagai sebuah bilangan yang ditambahkan ke ujung sebuah *string*. Jumlah kemunculan masing-masing bilangan kemudian menentukan siapa pemenangnya.

Teknologi tersebut sangat sederhana dan pada dasarnya tidak berbeda jauh dengan mekanisme pemilu konvensional; hanya saja tindakan mencontreng atau ‘mencoblos’ pada kertas suara diganti dengan tindakan menekan tombol.

Kesederhanaan tersebut juga menjadi kunci keamanan pada mesin e-vote tersebut. Masing-masing mesin tidak terhubung ke internet dan memanfaatkan *microchip* sederhana untuk merekam suara. Dengan demikian, kemungkinan terjadi peretasan melalui jaringan tidak ada. Kemungkinan untuk menggunakan *keylogger* ataupun perangkat lunak berbahaya lainnya yang membutuhan sebuah komputer lengkap (bukan *embedded system*) juga tidak dapat terjadi dengan menggunakan *embedded system* tersebut.

Alur pemilihan dengan e-vote pada Pemira KM ITB sebagai berikut:



Gambar 1 Alur pemilihan *e-vote* Pemira ITB

Selama masa pemilihan berlangsung, Panwaslu bekerja untuk memastikan tidak ada kecurangan. Kecurangan yang mungkin terjadi di antaranya:

1. Pemilih memilih dua kali
2. Pemilih memilih tanpa menandatangani daftar pemilih
3. Pemilih memilih tidak sesuai TPS yang ditentukan
4. Operator memasukkan suara, bukan pemilih
5. Penghitungan suara dibaca sebelum waktunya

Apabila diasumsikan bahwa Panwaslu bekerja sebagaimana mestinya, maka kecurangan-kecurangan tersebut dapat terhindarkan.

Akan tetapi, terdapat persoalan baru yang khusus terjadi pada Pemira KM ITB. Berbeda dengan Pemilu pada umumnya, rangkaian pemungutan suara di Pemira KM ITB berlangsung selama lebih dari satu hari. Karena jadwal kuliah setiap mahasiswa berbeda dan belum tentu setiap hari seluruh mahasiswa berada di kampus, maka pemungutan suara diadakan selama hingga empat hari.

Dengan demikian, dapat terjadi modus kecurangan yang baru, yaitu kecurangan-kecurangan yang sama dengan di atas, namun dilaksanakan di malam hari, saat tidak ada Panwaslu yang bertugas.

Selama ini, untuk menghindari hal tersebut, dilakukan pengamanan secara fisik, dengan menyimpan mesin suara di tempat yang aman, misalnya di ruangan terkunci.

Untuk menghindari penghitungan suara sebelum waktu yang ditentukan, pada mekanisme konvensional non-elektronik, cukup mengunci kotak suara dan menyimpan kuncinya di tempat yang aman. Meskipun kunci dicuri dan kotak suara dibuka untuk dihitung, banyaknya suara yang perlu dihitung mencegah terjadinya penghitungan suara yang lengkap tanpa tindakannya terdeteksi terlebih dahulu.

Dengan demikian, persoalan Pemira KM ITB dapat disimpulkan menjadi dua masalah:

1. Bagaimana menjaga kerahasiaan penghitungan suara sehingga tidak diketahui hasilnya sebelum waktu yang ditentukan
2. Menjaga integritas pengumpulan suara sehingga tidak ada manipulasi terhadap suara selama Panwaslu tidak bertugas (di luar jam kerja)

Kedua masalah tersebut sudah diselesaikan dengan pengamanan fisik, namun untuk meningkatkan pengamanan, kriptografi asimetris dapat menjadi salah satu solusi.

II. RSA

A. Perumusan Algoritma RSA

RSA adalah sebuah algoritma kriptografi kunci-publik yang diciptakan oleh tiga peneliti MIT: Ron Rivest, Adi Shamir, dan Len Adleman, pada tahun 1976. Properti-properti algoritma RSA adalah sebagai berikut:

No	Properti	Sifat
1	p, q (bilangan prima)	Rahasia
2	$n = p \cdot q$	Tidak rahasia
3	$\phi(n) = (p-1) \cdot (q-1)$	Rahasia
4	e (kunci enkripsi)	Tidak rahasia
5	d (kunci dekripsi)	Rahasia
6	m (plainteks)	Rahasia
7	c (cipherteks)	Tidak rahasia

Tabel 1 Properti-Properti dalam algoritma RSA

Pada prinsipnya, algoritma RSA memanfaatkan Teorema Euler, yaitu:

$$a^{\phi(n)} \equiv 1 \pmod{n} \qquad (1)$$

Teorema tersebut berlaku dengan syarat:

1. a relatif prima terhadap n (GCD(a,n) = 1)
2. $\phi(n) = n\,(1 - 1/p_1)\,(1 - 1/p_2)\ldots(1 - 1/p_r)$ di mana $p_1, p_2, \ldots, p_r$ adalah faktor prima dari n.

Berdasarkan sifat $a^k = b^k \pmod{n}$ untuk k = bilangan bulat ≥ 1:

$$a^{k\phi(n)} \equiv 1^k \pmod{n} \qquad (2)$$

Karena 1^k untuk sembarang $k = 1$, maka:

$$a^{k\phi(n)} \equiv 1 (\mathrm{mod}\ n) \quad (3)$$

Bila a diganti m maka persamaan menjadi:

$$m^{k\phi(n)} \equiv 1 (\mathrm{mod}\ n) \quad (4)$$

Berdasarkan sifat $ac \equiv bc \pmod n$ maka bila dikali m, persamaan menjadi:

$$m^{k\phi(n)} \equiv m (\mathrm{mod}\ n) \quad (5)$$

Misallkan dua bilangan e dan d dipilih sedemikian sehingga

$$e \cdot d \equiv 1 (\mathrm{mod}\ \phi(n)) \quad (6)$$

atau

$$e \cdot d \equiv k\phi(n) + 1 \quad (7)$$

Apabila persamaan (7) dan (5) disulihkan maka akan didapatkan:

$$m^{e \cdot d} \equiv m (\mathrm{mod}\ n) \quad (8)$$

Persamaan (8) dapat ditulis ulang menjadi

$$(m^e)^d \equiv m (\mathrm{mod}\ n) \quad (9)$$

Berdasarkan persamaan (9), fungsi enkripsi E dan dekripsi D didapatkan sebagai berikut:

$$E_e(m) = c \equiv m^e \bmod n \quad (10)$$

$$D_d(c) = m \equiv c^d \bmod n \quad (11)$$

B. Pembangkitan pasangan kunci

Untuk membangkitkan sepasang kunci publik dan kunci privat untuk algoritma RSA, digunakan langkah-langkah sebagai berikut:

1. Pilih dua bilangan prima p dan q (rahasia).
2. Hitung $n = pq$.
3. Hitung $\phi(n) = (p - 1)(q - 1)$.
4. Pilih sebuah bilangan bulat e untuk kunci publik, yang relatif prima terhadap $\phi(n)$.
5. Hitung kunci dekripsi d dengan persamaan: $ed \equiv 1 \pmod{\phi(n)}$ atau $d \equiv e^{-1} \bmod (\phi(n))$

Dari algoritma di atas, didapatkan pasangan kunci RSA sebagai berikut:

Kunci publik: pasangan (e, n)
Kunci privat: pasangan (d, n)

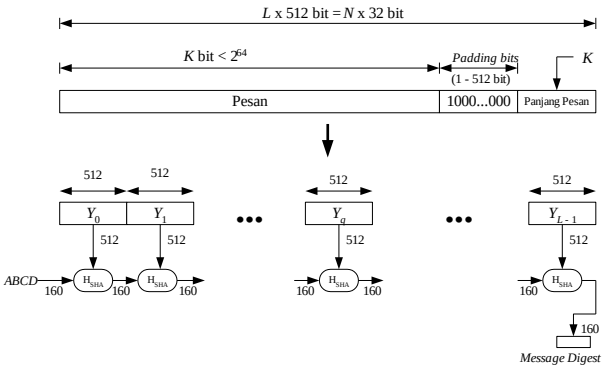
Kekuatan algoritma RSA terletak pada sulitnya memfaktorkan bilangan menjadi faktor-faktor prima, misal $n = a \times b$. Sekali n berhasil difaktorkan menjadi a dan b maka $\phi(n)$ dapat dihitung. Karena kunci enkripsi e tidak rahasia, maka kunci dekripsi d dapat dihitung dari persamaan $e \cdot d \equiv 1 (\mathrm{mod}\ \phi(n))$. Oleh sebab itu, penemu RSA menyarankan panjang nilai a dan b lebih dari 100 digit. Dengan demikian, hasil kali $n = a \times b$ akan berukuran lebih dari 200 digit. Usaha untuk mencari faktor bilangan 200 digit membutuhkan waktu komputasi selama 4 milyar tahun.

III. SHA-1

SHA (*Secure Hash Algorithm*) 1 adalah sebuah standar algoritma *hashing* satu arah yang dibuat oleh NIST, Amerika Serikat. SHA didasarkan pada MD4 yang dibuat oleh Ron Rivest dari MIT. Salah satu pemanfaatan SHA, seperti algoritma *hashing* lainnya, adalah untuk memastikan integritas data.

Algortma SHA menerima masukan berupa plainteks dengan ukuran maksimum 2^{64} bit dan menghasilkan *message digest* dengan panjang 160 bit, atau 40 byte. Panjang *message digest* ini lebih panjang dari yang dihasilkan oleh algoritma MD5 yang sepanjang 128 bit.

Skema pembuatan *message digest* dengan SHA-1 sebagai berikut:



Gambar 2 Skema Pembuatan Message Digest SHA-1

IV. PENERAPAN RSA UNTUK PENGAMANAN PENGHITUNGAN SUARA

A. Gambaran Umum

Seperti yang dijelaskan sebelumnya, salah satu masalah dalam Pemira adalah menjaga kerahasiaan hasil penghitungan suara sebelum waktunya. Saat ini, penghitungan suara dapat dilakukan hanya dengan syarat memiliki perangkat elektronik untuk membaca isi mesin penghitung suara.

Untuk meningkatkan keamanan informasi tersebut, maka algoritma kriptografi asimetris dapat dimanfaatkan. Tujuan pemanfaatan kriptografi tersebut adalah agar penghitungan suara baru dapat dilakukan pada akhir rangkaian kegiatan Pemira.

Dengan penerapan kriptografi asimetris, tidak ada perubahan pada proses pemilihan dari segi *end-user*. Perubahan terletak pada proses pemrosesan pilihan yang terjadi di dalam mesin pemilih serta pada mekanisme penghitungan suara.

Pada mesin pemilih, setiap suara dianggap sebagai sebuah pesan dan kemudian dienkripsi menggunakan kunci publik. Cipherteks hasil enkripsi tersebutlah yang disimpan di mesin penyimpan suara.

Pada saat penghitungan suara, setiap pesan suara pilihan pemilih pada Pemira didekripsi menggunakan kunci privat. Dengan demikian, tidak ada yang dapat mengetahui hasil pemilihan kapanpun tanpa mengetahui kunci privat.

B. Proses Enkripsi Suara

Untuk menjaga keamanan kunci pada algoritma RSA, maka digunakan panjang kunci 512-bit. Pada bentuk dasarnya, pesan hanya berisi pilihan calon yang dipilih. Dengan jumlah calon tidak pernah mencapai lebih dari lima calon, maka dapat diasumsikan bahwa panjang pesan maksimum adalah 3 bit. Dengan demikian, pesan tersebut cukup pendek untuk dienkripsi dengan kunci 512-bit.

Akan tetapi, jika pesan hanya berisi nomor urut calon yang dipilih, atau dengan padding yang selalu sama (misal byte 0), maka setiap suara yang memilih calon yang sama akan menghasilkan cipherteks yang sama. Untuk menghindari hal tersebut, maka pesan di-*padding* dengan *random bytes* hingga panjang pesan sama dengan panjang kunci (512-bit = 64 byte). Pilihan calon diletakkan di 4 bit terakhir. Dengan demikian, pesan yang mengandung pilihan calon yang sama akan berbentuk plainteks yang berbeda dan cipherteks yang berbeda pula.

```
ea 84 af 6e 55 e0 27 40
2d 19 18 15 08 32 51 ac
f5 98 91 f0 69 15 83 e9
44 c4 6c 64 43 0d 18 15
08 05 51 ac f5 76 91 f0
a4 11 44 4d df ff f2 0e
96 3e 40 5f c4 17 05 eb
3b e8 a3 04 32 d4 20 c2
```

Gambar 1 Plainteks yang berisi pilihan pemilih dalam notasi heksadesimal. Calon yang dipilih adalah nomor urut 2, yang tercantumkan dalam 4 bit terakhir pesan.

B. Proses Dekripsi dan Penghitungan Suara

Untuk menghitung perolehan suara, maka masing-masing suara yang berbentuk ciphertext harus didekripsi dengan kunci privat kemudian diekstraksi pilihannya.

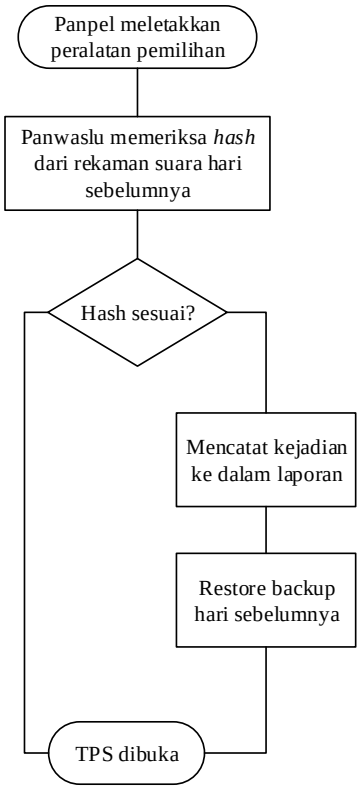
Agar proses tersebut baru dapat dilakukan di akhir rangkaian Pemira, maka kunci dapat dipecah menjadi potongan-potongan yang masing-masing dipegang oleh senator. Senator dianggap sebagai pihak yang berwenang untuk menjadi saksi dalam proses penghitungan suara sehingga senatorlah yang memegang kunci tersebut.

V. PENERAPAN SHA-1 UNTUK PENGAMANAN INTEGRITAS SUARA

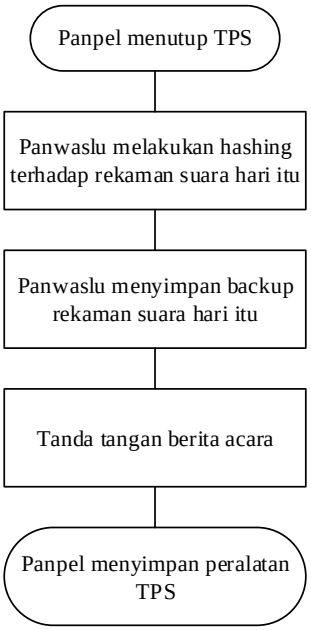
Untuk memastikan bahwa tidak ada perubahan pada hasil pemungutan suara di akhir setiap harinya, maka SHA-1 dapat dilakukan sebagai alat untuk memastikan integritas hasil pemungutan suara tersebut.

Integritas dapat dipastikan dengan Panwaslu yang bertanggung jawab atas sebuah TPS melakukan *hashing* terhadap rekaman suara pada hari tersebut, serta *backup* seluruh suara pada hari tersebut. Esok harinya, pada saat TPS dibuka, Panwaslu tersebut memastikan apakah suara yang tersimpan dari hari sebelumnya sesuai dengan *hash* yang disimpannya. Dengan demikian, terdapat alur baru untuk pembukaan dan penutupan TPS harian.

Untuk pembukaan TPS per hari, alur kerja barunya sebagai berikut:



Untuk penutupan TPS per hari, alur baru adalah sebagai berikut:



VI. ANALISIS KELEMAHAN

Kelemahan pada mekanisme pengamanan Pemira yang dijelaskan pada makalah ini terletak pada lamanya waktu yang dibutuhkan untuk melakukan penghitungan suara. Hal ini disebabkan komputasi yang dibutuhkan untuk melakukan dekripsi dengan algoritma kunci-publik secara signifikan lebih lambat dibandingkan tanpa enkripsi sama sekali.

VII. KESIMPULAN

Berdasarkan pemaparan dalam makalah ini, dapat disimpulkan sebagai berikut:

1. Kriptografi kunci-publik dapat digunakan untuk mengamankan penghitungan suara Pemira KM ITB.
2. Hashing dapat dimafaatkan untuk mengamankan integritas rekaman suara pilihan pemilih pada Pemira KM ITB.
3. Proses pengamanan dengan kriptografi asimetris membutuhkan waktu yang secara signifikan lebih lama dibandingkan tanpa enkripsi.

REFERENCES

[1] Diktat dan materi kuliah IF3058 Kriptografi
[2] Limandra, Timotius Grady. 2008. Implementasi Blind Signature dalam Melakukan Electronic Voting. Makalah IF5054 Kriptografi.

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

Tubagus Andhika Nugraha
13510007