Protokol E-voting dengan Menggunakan Algoritma Enkripsi AES dan Fungsi hash SHA-1

Riady Sastra Kusuma 13512024
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
riadysastrak@gmail.com

***Abstract*—E-voting adalah cara pemungutan suara dengan menggunakan komputer secara online. Keamanan adalah aspek yang paling penting jika sudah berhubungan dengan jaringan dan komputer. Makalah ini membahas tentang protokol baru yang menggunakan fungsi enkripsi AES dan fungsi hash SHA-1 dalam implementasinya. Terdapat juga analisis dari peformansi dari protokol ini.**

***Index Terms*— e-voting, enkripsi, AES. fungsi hash, SHA**

I. PENDAHULUAN

Pemungutan suara (*voting*) sering dilakukan untuk memilih suatu keputusan dalam suatu organisasi. Pemungutan suara juga biasanya dilakukan untuk memilih pimpinan atau ketua. Pemungutan suara sangat sering dilakukan pada Negara demokrasi seperti Indonesia.

Pemungutan suara umum dilakukan menggunakan kertas. Namun seiring perkembangan teknologi, penggunaan kertas pun sering digantikan dengan penggunakan teknologi informasi. Akibatnya voting biasanya dilakukan menggunakan komputer secara online (*e-voting*).

Sistem e-voting sulit diterapkan pada suatu negara, karena dibutuhkan sistem yang sangat besar dan benar-benar aman. Keamanan adaalah aspek yang paling diutamakan dalam sistem ini. Terutama integritas data dari setiap orang peserta pemungutan suara.

Dalam pemungutan suara menggunakan kertas, terjadi beberapa kecurangan. Kecurangan yang biasa terjadi adalah panitia lokal mengganti hasil voting yang ada di dalam kotak suara. Orang yang memberi suara juga tidak tahu apakah suaranya diganti atau tidak. Maka dari itu perlu dilakukan enkripsi pada hasil suara agar orang lain tidak mengerti isi pesannya dan bagaimana mengubahnya.

Maka dari itu kriptografi diperlukan untuk mengamankan sistem e-voting agar integrtias data terjamin.

II. DASAR TEORI

A. E-voting

Seiring perkembangan teknologi informasi, semua hal dapat dilakukan lebih efisien dengan komputer termasuk pemungutan suara. E-voting adalah metode untuk melakukan pemunggutan suara memakai komputer secara online.

Penilitan tentang e-voting sudah dilakukan sejak tahun 1869. Tetapi sampai sekarang, e-voting hanya dilakukan pada organisasi yang kecil saja. E-voting belum dapat dilakukan pada organisasi besar atau suatu negara karena masalah keamanan.

E-voting dapat dilakukan jika memenuhi syarat-syarat berikut:

1. *Accuracy* yaitu ketepatan hasil perhitungan. Semua suara harus terhitung semua dan valid. Valid disini maskudnya adalah suara yang masuk tidak diubah ditengah proses voting.
2. *Privacy* sesorang tidak boleh tahu suara orang lain.
3. *Democracy* yaitu pemilih berhak memilih jika memenuhi syarat dan setiap pemilih hanya boleh memillih satu kali.
4. *Robustness* yaitu tidak ada gangguan yang dapat menghambat atau menghalangi keberjalanan sistem e-voting.
5. *Verifiability* yaitu setiap suara dapat dibuktikan kevalidannya.
6. *Fairness* yaitu orang tidak dapat mengetahui hasilnya sebelum dilakukan penghitungan suara.

Biasanya orang yang memberikan suara harus memasukan password terlebih dahulu agar orang lain tidak bisa memberikan suara memakai hak orang tersebut.

Awalnya memang terlihat aman, tetapi hal ini dilakukan secara online. Hal itu berarti orang dapat mengganti suaranya di tengah perjalanan pada jaringan.

B.Kriptografi

Kriptografi adalah sebuah ilmu yang mempelajari tentang mengamankan suatu pesan atau data. Dalam proses pengamanan pesan, terdapat beberapa aspek penting yang menjadi inti dari kriptografi yaitu :

1. Confidentiality yaitu data atau pesan yang dikirmkan bersifat rahasia. Harus diyakinkan bahwa pesan atau data tersebut tidak dapat dibaca oleh pihak yang tidak berwenang. Untuk

menjamin confidentiality biasanya dilakukan teknik enkripsi pada pesan

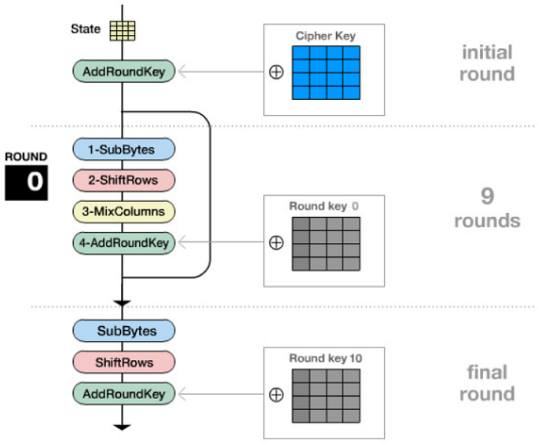
2. Integrity yaitu suatu pesan yang dikirimkan utuh dan sama dengan pesan yang diterima. Jika pesan yang dikirim tidak sama dengan yang diterima, mungkin saja ada orang yang membaca dan mengubah pesan ditengah perjalanan untuk keuntungannya sendiri. Teknik enkripsi dan hash function adalah solusinya.
3. Authentication yaitu pesan yang diterima adalah benar-benar pesan yang ditulis dari orang yang kita duga mengirimkan pesannya. Karena mungkin saja orang lain yang berpura-pura menjadi orang tersebut yang mengirimkan pesannya. Pesan palsu sangat berbahaya karena dapat menimbulkan kesalahpahaman diantara dua pihak yang berkomunikasi Digital signature adalah solusi untuk hal ini
4. Nonrepudiation yaitu mencegah pihak yang berkomunikasi menyangkal bahwa pesan itu yang ditulis oleh pihak tersebut.

Banyak teknik kriptografi untuk mengamankan suatu pesan. Teknik tersebut dibagi menjadi 3 golongan besar, yaitu teknik enkripsi kunci simetri, teknik enkripsi kunci asimetri dan fungsi hash. Masing-masing memiliki kelebihan dan kekurangannya sendiri.

C. Teknik enkripsi AES

AES adalah singkatan dari *Advanced Encryption Standard.* Teknik enkirpsi ini merupakan teknik enkrpsi kunci simteri. Teknik AES merupakan teknik *cipher block.*. Artinya data dienkripsi per satuan blok. Algoritma AES beroperasi dalam orientasi byte. AES mempunyai kunci 128 bit sampai 256 bit. Setiap blok dienkripsi dalam sejumlah putaran tertentu.

Garis besar algoritma AES adalah sebagai berikut :



Gambar 1. Skema dasar algoritma AES

1. *AddRoundKey*: XOR dilakukan antara state awal dengan cipher key
2. Putaran sebanyak Nr – 1 kali. Proses yang dilakukan setiap putaran adalah :
   a. *SubBytes*: subtitusi byte dengan melakukan subtitusi menggunakan tabel subtitusi atau biasa disebut S-Box
   b. *ShiftRows*: Pergeseran baris-baris array state secara wrapping
   c. *MixColumns*: mengacak data di masing-masing kolom array state
   d. *AddRoundKey*: XOR pada state dengan round key.
3. Final round: proses untuk putaran terakhir, terdiri dari:
   a. SubBytes
   b. ShiftRows
   c. AddRoundKey

D. Fungsi hash SHA

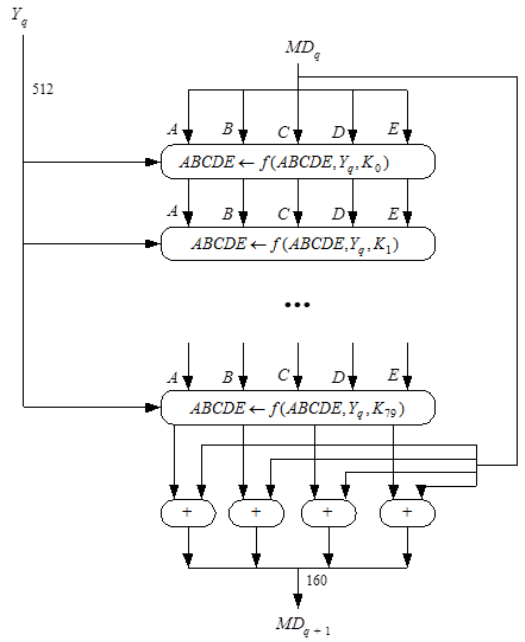
Fungsi hash adalah fungsi yang mengubah string masukan yang panjangnya sembarang menjadi string yang panjangnya tetap. Fungsi hash bekerja dalam satu arah. Jadi string keluaran tidak bisa lalgi diubah menjadi string semula. Fungsi hash bukanlah teknik enkirpsi, karena keluaran tidak bisa ditransformasikan menjadi masukan, dan fungsi hash tidak memerlukan kunci.

SHA adalah fungsi hash yang dibuat oleh NIST. SHA adalah standard fungsi hash satu arah. Algoritma SHA dapat menerima masukan sepanjang 2^{64}bit dan menghasilkan keluaran (*message digest*) sepanjang 160 bit.

Langkah-langkah algoritma SHA adalah sebagai berikut:

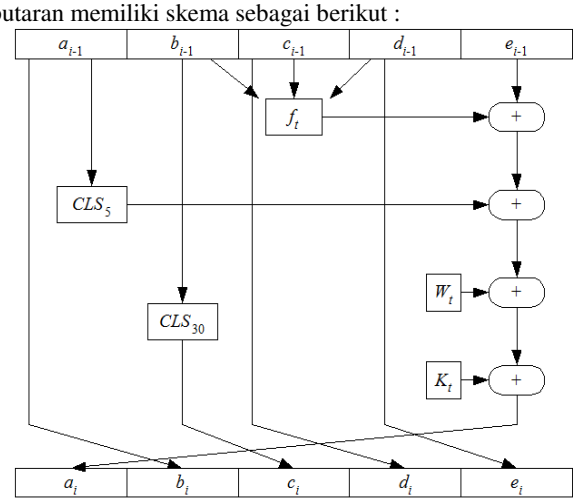
1. Penambahan padding bits.
2. Penambahan nilai panjang pesan semula.
3. Inisialisasi buffer MD.
4. Pengolahan pesan dalam blok berukuran 512 bit.

Pengolahan pesan dalam blok berukuran 512 bit memiliki skema sebagai berikut :



Gambar 2. Skema dasar algoritma SHA

Proses ini terdiri dari 80 putaran. Operasi pada setiap putaran memiliki skema sebagai berikut :



Gambar 3. Skema proses pada setiap putaran SHA

III. IMPLEMENTASI

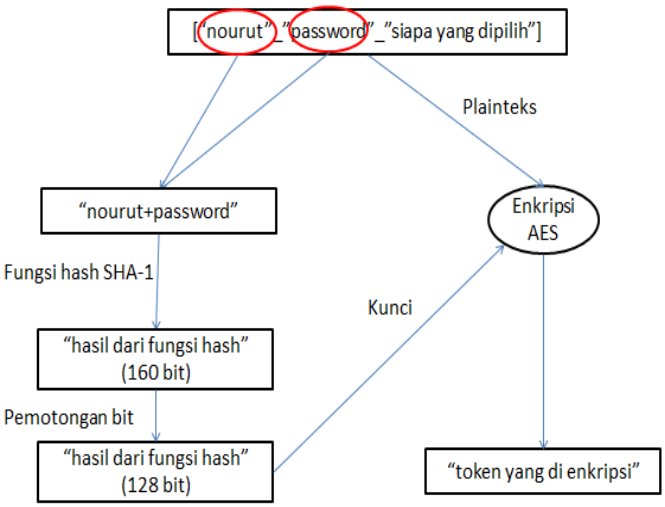
A. Rancangan Protokol E-voting

Berikut proses-proses yang harus diikuti seseorang untuk melakukan e-voting :

1. Setiap pemilih harus mendaftarkan dirinya dulu untuk memilih. Pada pendaftaran, calon pemilih diperiksa dulu syarat-syarat dasar untuk ikut memilih dalam voting tersebut. Jika pemilih memenuhi syarat, maka pemilih akan diberi nomer urut dan password khusus yang degenerate saat itu juga dan hanya diketahui oleh pemilih tersebut.
2. Untuk memilih, setiap pemilih memasukan nomer urut, password dan apa yang dipilih.
3. Setelah memilih, peserta mendapatkan suatu token yang sudah dienkripsi, sehingga orang yang melihat token tersebut tidak tahu siapa yang dia pilih.
4. Token tersebut digunakan untuk menunjukan bahwa dia sudah memilih dan untuk meverifikasi hasil votingnya pada saat penghitungan.

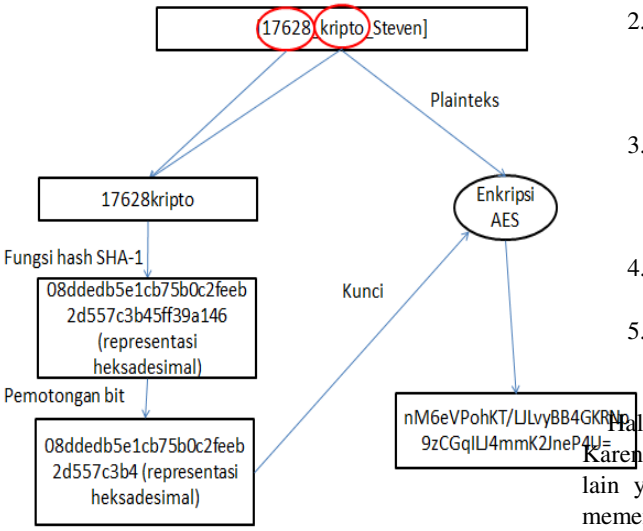
Proses tersebut adalah proses yang dilakukan seseorang untuk melakukan voting. Selanjutnya akan dibahas proses pengiriman data dan penghitungan hasil suara. Berikut adalah prosesnya:

1. Setelah pemilih melakukan voting, token dibangkitkan dengan format
   [“nourut”_”password”_”siapayangdipilih”]
   Contoh : [17628_kripto_Steven]
2. Token tersebut dienkripsi dengan algoritma AES. Algoritma AES membutuhkan kunci sepanjang 128 bit. Kunci dibangkitkan dengan cara menggunakan fungsi hash SHA-1 pada kombinasi nomor urut dan password dari pemilih. Hasil keluaran dari SHA-1 adalah 160 bit. Maka hanya diambil 128 bit terdepannya saja untuk dijadikan kunci AES. Berikut skema proses enkripsinya :



Gambar 4. Skema proses enkripsi pada protokol e-voting

Berikut contoh skema proses enkripsi :



Gambar 5. Contoh skema proses enkripsi pada protokol e-voting

3. Token yang dienkirpsi tersebut dikirimkan pada server pusat untuk dikelola nantinya beserta nomor urut untuk dimasukkan pada database.
4. Selanjutnya pada pengitungan suara dilakukan dekripsi pada token tersebut dengan kunci gabungan no urut + password yang sudah ada didatabase sejak pemilih mendaftar.

B. Analisis awal

Dengan protokol yang diusulkan diatas maka ada beberapa kriteria voting yang terpenuhi. Kriteria yang terpenuhi antara lain :

1. *Accuracy* terpenuhi karena setiap suara dapat dihitung. Selain itu suara yang tidak valid juga bisa dideteksi dengan mencocokan token yang ada di server dengan token yang dipegang oleh pemilih. Jika ada yang mengganti token ditengah perjalanan, dapat juga dideteksi saat mendekripsinya. Jika setelah didekripsi data tidak bisa dibaca, maka sudah ada orang yang mengubah sebelum penghitungan suara.

   Contoh token :

nM6eVPohKT/LJLvyBB4GKRNp9zCGqILJ4m mK2JneP4U=

   Saat didekripsi dengan kunci: 17628kripto maka hasilnya adalah :

[17628_kripto_Steven].

   Jika token diubah sebelum dihitung menjadi :

nM6eVPohKT/LJLvyAB4GKRNp9zCGqILJ4m mK2JneP4U=

   Maka saat didekripsi dengan kunci : 17628kripto maka hasilnya adalah

��,] ;3┬ ►C► ieven]

   Dengan demikian dapat dideteksi apakah suara valid atau tidak.
2. *Privacy* terpenuhi karena token tidak bisa dibaca oleh orang lain kecuali orang lain bisa mendapatkan password dari orang tersebut dan mengetahui nomer urutnya.
3. *Democracy* terpenuhi karena dapat dilihat didatabase jika pada database nomer urut tersebut sudah ada isinya, maka dapat dideteksi bahwa dia sudah pernah memilih.
4. *Verifiability* terpenuhi karena bisa mencocokan hasil dengan token yang dipegang oleh pemilih.
5. *Fairness* terpenuhi karena orang lain tidak bisa tahu isi dari hasil pemilihannya sebelum didekripsi.

Hal yang mungkin tidak terpenuhi adalah *Robustness.* Karena itu tergantung sistem bekerja dan banyak factor lain yang tidak berhubungan dengan kriptografi untuk memenuhi syarat *Robustness* .

Sedangkan untuk aspek kriptografi, protokol ini juga memenuhi aspek-aspek berikut:

1. Confidentiality terpenuhi karena seharusnya orang yang tidak berwenang tidak dapat mengetahui hasil suara yang sudah dienkripsi pada jaringan atau pada database.
2. Integrity terpenuhi karena jika pesan berubah maka dapat dideteksi pada saat dekripsi.
3. Authentication terpenuhi karena yang mengetahui passwordnya seharusnya hanya pemilih saja
4. Nonrepudiation terpenuhi karena ada token yang dipegang pimilih untuk bukti bahwa pemilih sudah pernah memilih.

IV. ANALISIS DAN EKPERIMEN

A. Perbandingan Performansi dengan Fungsi Hash

Untuk menjaga confidentiality suatu suara, tidak harus memakai teknik enkripsi, tapi juga bisa juga memakai fungsi hash. Jika menggunakan fungsi hash maka prosesnya menjadi sebagai berikut:[2]

1. Setelah pemilih melakukan pemilihan, maka hasilnya langsung di hash menjadi token.
2. Setelah itu dimasukan didatabase tanpa index
3. Untuk melakukan penghitungan suara maka dicoba semua kemungkinan pemilih untuk memilih lalu di hash. Setelah itu dicari pada database yang mempunyai kode hash tersebut.

   Contoh:

   Setelah user memilih maka hasilnya adalah :

[17628_kripto_Steven]

   Lalu di hash dengan fungsi hash SHA-1 menjadi:

5c596cbdb0dac2acc835eab11111bf76fc833885

   Lalu setelah itu hasil hash tersebut dimasukan pada database.

   Untuk penghitungan suara maka caranya adalah sebagai berikut:

Semua kemungkinan yang dipilih user adalah:

- [17628_kripto_Steven]
- [17628_kripto_Bob]

Masing-masing kemungkinan itu di hash menjadi:

- 5c596cbdb0dac2acc835eab11111bf76fc833885
- 2572e144e1f8fb08ba990044251ea0127b92de33

Masing-masing kode tersebut dicari didatabase, jika ada yang sama, maka itu pilihannya. Kode pertama akan ditemukan pada database sehingga hasilnya adalah pemilih tersebut memilih Steven.

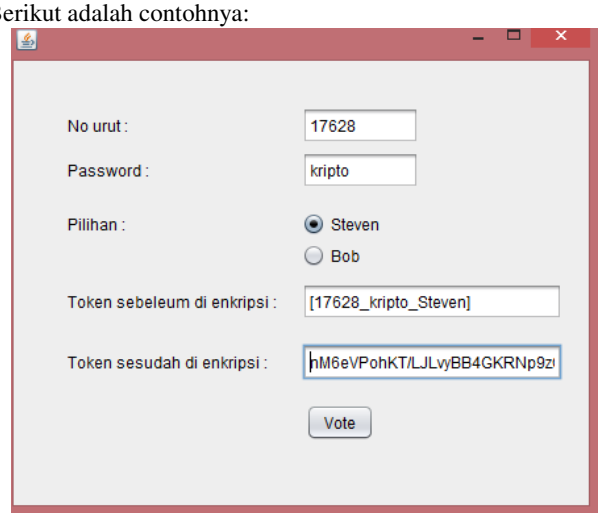
Kompleksitas pencarian pada database jika menggunakan fungsi hash adalah O(n) dengan n adalah banyaknya pemilih atau banyaknya data yang ada pada database. Sedangkan jika menggunakan protokol yang saya usulkan, pencarian pada database adalah O(1) karena langsung memakai index nomor urut pemilih.

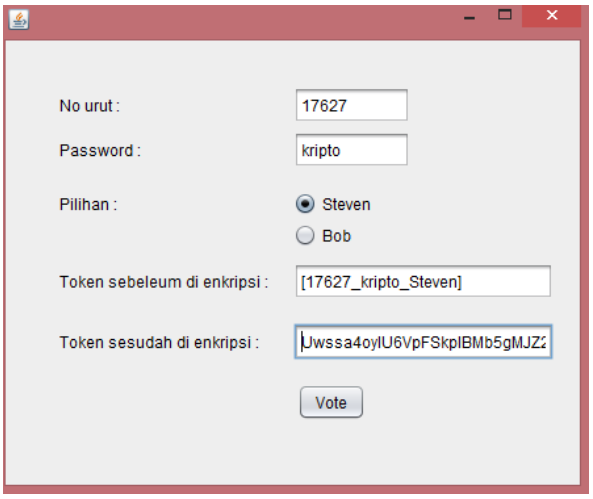
Mungkin saja sesudah menggunakan fungsi hash, data dimasukan di database dengan indeks berupa nomor urut. Tapi untuk mengetahui isinya, maka seluruh kemungkinan harus tetap dihash dan dicocokan. dengan isinya. Dengan begitu kompleksitasnya tetap O(n) dengan n adalah jumlah kemungkinan pilihan seseorang. Sedangkan untuk protokol ini, kompleksitawnya tetap O(1) karena datanya hanya didekripsi saja untuk mengetahui pilihannya.

Jadi untuk metode ini lebih unggul dibanding metode hash dalam proses perhitungan suara.

B. Confidentiality

Hasil enkripsi dapat diketahui plainteksnya jika dapat dilihat kesamaan dari cipherteks dengan beberapa kesamaan plainteks. Kasus ini terjadi pada sistem ini jika ada yang memiliki nomer urut yang hampir sama, mempunyai password yang sama dan pilihan yang sama. Berikut adalah contohnya:





Gambar 6. Perbandingan token dengan perbedaan nomor urut yang sedikit

Dapat dilihat perbandingan token sesudah dienkripsi sangatlah berbeda dan tidak ada kesamaan yang signifikan. Hal ini disebabkan karena nomor urut juga dijadikan kunci untuk enkrpsi. Selain itu, kunci tersebut juga di hash terlebih dahulu. Hal itu menyebabkan walaupun nomor urut dan passwordnya mirip, tetap saja cipherteksnya akan berbeda sangat jauh.

Hal ini menybabkan token yang sudah dienkripsi menjadi sangat sulit dibaca. Untuk mengetahui plainteks suatu token dibutuhkan nomor urut pemilih dan password dari pemilih.

V. KESIMPULAN DAN SARAN

Protokol e-voting ini memenuhi kriteria-kriteria kriptografi dan kriteria voting kecuali *Robustness*. Protokol ini bisa dapat dikembangkan lagi dengan ilmu selain kriptografi untuk memenuhi syarat *Robustness.*

Protokol ini juga cepat dalam proses perhitungan suara karena dibutuhkan kompleksitas O(1) dibandingkan dengan protokol yang hanya mengandalkan fungsi has dengan kompleksitas O(n).

Protokol ini juga dapat dibilang aman, karena walaupun perbedaan parameter yang sedikit, token yang dienkripsi akan sangat berbeda.

VI. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Bapak Rinaldi Munir sebagai dosen mata kuliah kriptografi yang telah mebimbing dalam perkuliahan untuk menyelesaikan makalah ini.

Ucapan terima kasih juga kami berikan kepada seluruhpihak yang tidak dapat disebutkan satu per satu dan telah membantu penulis dalam pembuatan makalah ini sehingga dapat diselesaikan dengan baik.

Semoga makalah ini bermanfaat pada bidang keilmuan

kriptografi terutama pada sistem e-voting.

PUSTAKA

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

[2] Abdurrosyid Broto Handoyo Sistem Pengamanan Data Pemilihan Umum e-Voting dengan Menggunakan Algoritma SHA-1, Bandung: Sekolah Teknik Elektro dan Informatika, 2013

[3] Ricardo Andre Costa, Mario Jogre Leitao, dan Isidro Vila Verde, Electronic Voting: An All-Purpose Platform, Porto.

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, 10 Mei 2015

Riady Sastra Kusuma / 13512024