JURNAL

IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA PADA E-VOTING BUPATI KABUPATEN NGANJUK

RSA CRYPTOGRAPHIC ALGORITHM IMLEMENTATION ON E-VOTING REGENT DISTRICT NGANJUK

Oleh:

AKBAR ARDLIYANSYAH

12.1.03.02.0080

Dibimbing oleh :

1. **Ahmad Bagus Setiawan, ST., M.Kom., MM.**
2. **Risky Aswi Ramadhani, M,Kom**

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS NUSANTARA PGRI KEDIRI

TAHUN 2017

SURAT PERNYATAAN
ARTIKEL SKRIPSI TAHUN 2017

Yang bertanda tangan di bawah ini:

Nama Lengkap	: Akbar Ardliyansyah
NPM	: 12.1.03.02.0080
Telepun/HP	: 085735709546
Alamat Surel (Email)	: hwangakbar@gmail.com
Judul Artikel	: Implementasi Algoritma Kriptografi RSA pada E-Voting Bupati Kabupaten Nganjuk
Fakultas – Program Studi	: Teknik Informatika
Nama Perguruan Tinggi	: Universitas Nusantara PGRI Kediri
Alamat Perguruan Tinggi	: Jl. K.H. Ahmad Dahlan No. 76, Mojoroto, Kediri, Jawa Timur

Dengan ini menyatakan bahwa :

a. artikel yang saya tulid merupakan karya saya pribadi (bersama tim penulis) dan bebas plagiarisme;
b. artikel telah diteliti dan disetujui untuk diterbitkan oleh Dosen Pembimbing I dan II.

Demikian surat pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari ditemukan ketidaksesuaian data dengan pernyataan ini dan atau ada tuntutan dari pihak lain, saya bersedia bertanggungjawab dan diproses sesuai dengan ketentuan yang berlaku.

Mengetahui		Kediri, 25 Januari 2017
Pembimbing I	Pembimbing II	Penulis,
Ahmad Bagus Setiawan, ST., M.Kom., MM. NIDN. 0703018704	**Risky Aswi Ramadhani, M,Kom** NIDN. 0708049001	**Akbar Ardliyansyah** 12.1.03.02.0080

IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA PADA E-VOTING BUPATI KABUPATEN NGANJUK

Akbar Ardliayansyah
12.1.03.02.0080
Teknik - Informatika
hwangakbar@gmail.com
Ahmad Bagus Setiawan, S.T., M.M., M.Kom. dan Risky Aswi Ramadhani, M.Kom.
UNIVERSITAS NUSANTARA PGRI KEDIRI

Abstrak

Pemilihan kepala daerah di Indonesia saat ini menggunakan kertas umtuk melakasanakan pemilu, selain membutuhkan banyak sumber daya dan tenaga. Waktu yang diperlukan juga akan semakin lama serta kurang aman dalam pelaksanaannya. Sistem E-Voting ini menggunakan algoritma kriptografi rsa yang memanfaatkan penghitungan dari kunci publik dan kunci privat untuk mengunci dan membuka hasil suara masyarakat agar lebih aman sampai waktu pemilu selesai dan masa-masa penghitungan suara. Sistem E-Voting merupakan salah satu cara membantu menyelesaikan permasalahan tersebut. Keamanan sistem E-Voting cukup terjamin dan sesuai dengan perkembangan teknologi saat ini. Sistem tersebut dapat dipadukan dengan berbagai macam algoritma kriptografi untuk meningkatkan keamanannya, salah satunya algoritma kriptografi rsa.

Kata Kunci : voting, e-voting, kriptografi, rsa.

I. LATAR BELAKANG

Pemilihan kepala daerah di Indonesia saat ini menggunakan kertas suara yang membutuhkan banyak sumber daya, tenaga, dan waktu terutama perhitungan suara. Dengan menggunakan pemilihan secara digital atau *electronic voting* (*e-voting*) dapat menghemat waktu dan tenaga yang digunakan terutama dalam proses perhitungan suara [4]. Namun, meskipun sistem sudah berjalan, masih ada pihak-pihak luar yang mungkin melakukan kecurangan atau serangan. Karena sistem berjalan *online*, serangan akan langsung menuju web untuk memanipulasi hasil suara. Perlu sebuah keamanan untuk mengatasi masalah serangan tersebut, yaitu dengan diterapkannya sebuah metode *kriptografi RSA*.

Dengan pemanfaatan *kriptogarfi RSA* untuk keamanannya, dapat mewujudkan keamanan informasi pada *e-voting* di Indonesia yaitu mendukung aspek-aspek keamanan informasi meliputi kerahasiaan, integritas data, otentikasi dan nir penyangkalan [1]. Dari hasil penelitian Shelvhi, 2013, membuktikan pemanfaatan *kriptografi RSA* memang mampu untuk mengamankan sistem *e-voting* terutama mengamankan hasil suara. Lalu ada juga

penelitian dari Tika, 2014, juga membuktikan setelah hasil suara di enkripsi maupun dekripsi menggunakan *kriptografi RSA*, tidak ada perubahan pada hasil suara.

Alasan penulis memilih penelitian ini adalah, melihat sistem voting konvesional yang digunakan di Indonesia sampai sekarang masih banyak kekurangan terutama dalam hasil suara. Sering terjadi kecurangan saat pelaksanaan penghitungan suara karena banyak campur tangan manusia. Serta biaya pengadaan pemilu yang cukup besar kurang efektif untuk terus-menerus digunakan. Selanjutnya alasan memilih motode *kriptografi RSA* karena *kriptografi* ini sudah menjadi standar keamanan sistem perbankan. Dengan menggunakan 2 kunci, yaitu kunci *public* dan kunci *private* membuat *kriptografi* ini cukup sulit untuk dijebol.

II. METODE

1. Kriptografi *RSA*

Dalam kriptografi, *RSA* adalah algoritma untuk enkripsi kunci publik (*public-key encryption*). Algoritma ini adalah algoritma pertama yang diketahui paling cocok untuk menandai (*signing*) dan untuk enkripsi (encryption) dan salah satu penemuan besar pertama dalam kriptografi kunci publik. *RSA* masih digunakan secara luas dalam protokol-protokol perdagangan elektronik, dan dipercayai sangat aman karena diberikan kunci-kunci yang cukup panjang dan penerapanpenerapannya yang sangat up-to-date [2].

2. Algoritma Membangkitkan Pasangan Kunci

1) Pilih dua buah bilangan prima sembarang, p dan q.
2) Hitung $n = p \,.\, q$ (sebaiknya $p \neq q$, sebab jika $p = q$ maka $n = p^2$ sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n).
3) Hitung $\phi(\mathrm{n}) = (p-1)(q-1)$.
4) Pilih kunci publik, e, yang relatif prima terhadap $\phi(n)$.
5) Bangkitkan kunci privat dengan menggunakan persamaan (2.5), yaitu $e \,.\, d \equiv 1 \pmod{\phi(n)}$. Perhatikan bahwa $e \,.\, d \equiv 1 \pmod{\phi(n)}$ ekivalen dengan $e \,.\, d = 1 + k\phi(\mathrm{n})$, ,sehingga secara sederhana d dapat dihitung dengan

$$d = \frac{1+k\phi(n)}{e} \quad \text{.....} (1)$$

Hasil dari algoritma diatas :

- Kunci publik adalah pasangan (e, n)
- Kunci privat adalah pasangan (d, n)

Catatan : *n* tidak bersifat rahasia, sebab ia diperlukan pada perhitungan enkripsi/dekripsi [3].

3. **Algoritma Enkripsi/Dekripsi**

Enkripsi

1) Ambil kunci publik penerima pesan, *e*, dan modulus *n*.
2) Nyatakan plainteks m menjadi blok-blok $m_1, m_2, \ldots$, sedemikian sehingga setiap blok merepresentasikan nilai di dalam selang [0, *n* – 1].
3) Setiap blok m_i dienkripsi menjadi blok c_i dengan rumus $c_i = m_i{}^e \bmod n$ .....(2)

Dekripsi

Setiap blok cipherteks c_i dienkripsi kembali menjadi blok m_i dengan rumus

$m_i = c_i{}^d \bmod n$ .....(3)

4. **Perhitungan RSA**

Contoh Kasus :

Hasil suara salah satu calon Bupati adalah Jokowi = 33, maka yang akan diengkripsi adalah menggunakan plainteks "JOKOWI33".

1. Menentukan 2 bilangan prima, misal 47 dan 71. Tapi dalam aplikasi ini nantinya akan memiliki bilangan prima random. Jadi p = 47 dan q = 71
2. n = p x q → n = 47 x 71 = 3337
3. m = (p-1)(q-1) → m = (47-1)(71-1) = 3220
4. Pilih e yang relatif prima terhadap m, misal 79. Jadi gcd(e,m) = 1 → gcd(79,3337) = 1
5. Cari nilai d, d*e = 1 mod m
   d*79 = 1 mod 3220
   d*79 mod 3220 = 1
   d = 1019

Sehingga didapatkan :

1. Public key / kunci publik : (79,3337)
2. Private key / kunci private : (1019,3337)

Poses Enkripsi

Plainteks M = JOKOWI33, dirubah dalam format ASCII.

Karakter	:	J	O	K	O	W	I	3	3
ASCII	:	74	79	75	79	87	73	51	51

Lalu dibagi menjadi betuk perblok (menggunakan simbol Mn), an hasilnya adalah :

M1=74 M2=79 M3=75 M4=79
M5=87 M6 =73 M7=51 M8=51

Setelah dibagi perblok, maka akan dihitung menggunakan rumus :

Ci = Mi ^ e mod n

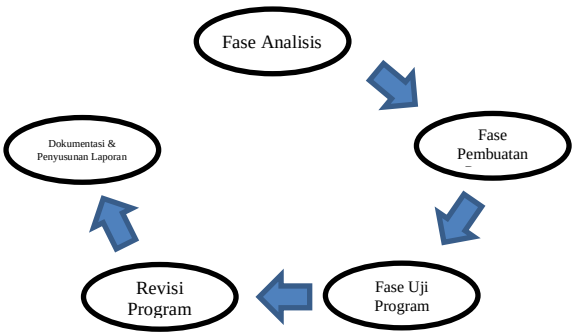
- C1 = 74 ^ 79 mod 3337 = 1294
- C2 = 79 ^ 79 mod 3337 = 251
- C3 = 75 ^ 79 mod 3337 = 2213
- C4 = 79 ^ 79 mod 3337 = 251
- C5 = 87 ^ 79 mod 3337 = 1848
- C6 = 73 ^ 79 mod 3337 = 725
- C7 = 51 ^ 79 mod 3337 = 523
- C8 = 51 ^ 79 mod 3337 = 523

Maka, chiperteks yang didapatkan adalah :

C=1294251221325118487255235 23.

5. Metode Penelitian

Dalam usaha memperoleh data–data yang diperlukan dalam penyusunan skripsi ini penulis menggunakan beberapa metode untuk mendapatkan gambaran yang jelas mengenai *e-voting* dan pemilu Bupati Nganjuk. Metode yang digunakan dalam penelitian ini metode pengembangan *Research & Development*, yaitu sebagai berikut :



A. Fase Analisis

a. Studi pustaka yaitu mempelajari dan memahami landasan teori yang terkait dengan masalah yang akan dibahas, serta konsultasi bimbingan dengan dosen pembimbing dan dosen lainnya.

b. Konsultasi dan bimbingan, yaitu setelah mempelajari teori berdasarkan literatur lalu juga konsultasi dengan dosen pembimbing dan dosen lainnya.

c. Observasi, yaitu melakukan pengamatan langsung di KPU Kabupaten Nganjuk. Untuk memperoleh berbagai informasi dan data faktual serta memahami situasi dan kondisi dinamis obyek penelitian.

B. Fase Pembuatan Program

Bereksperimen membuat program, berdasarkan materi dan algoritma yang telah dipelajari serta penelitian. Fase ini dilakukan secara otodidak (belajar sendiri). Baik itu Coding programnya maupun *layout* program.

C. Fase Uji Program

Dari fase uji coba ini didapat beberapa level untuk proses pengujiannya diantaranya :

a. Uji metode yaitu menguji apakah program yang telah dibangun sesuai dengan metode Algoritma Kriptogarfi RSA

b. Uji Kelayakan yaitu dengan mendemonstrasikan program didepan para dosen dan teman-teman *programmer*.

D. Revisi Program

Setelah fase diatas, tahap ini adalah memperbaiki kesalahan-kesalahan dalam listing program maupun menambah kekurangan dari program yang dikerjakan.

E. Dokumentasi dan Penyusunan Laporan

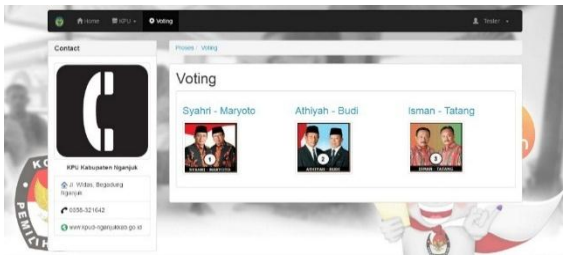
Dokumentasi dilakukan untuk jangka waktu sekarang dan yang akan datang agar memudahkan *maintenance* jika terjadi kesalahan program lagi akibat ketidak stabilan perangkat atau karena gangguan teknis lainnya. Penyusunan laporan adalah tahap dimana melaporkan semua hal dan data-dat yang sudah dikerjakan selama penelitian.

III. HASIL DAN KESIMPULAN

1. Hasil

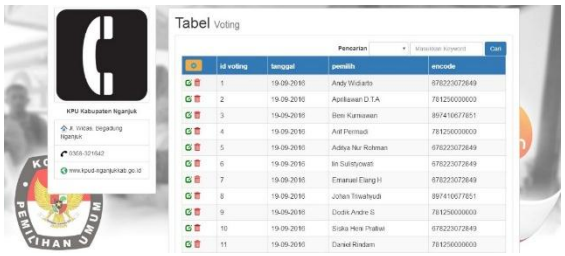
Hasil dari penelitian ini adalah kriptografi RSA dapat di implementasikan kedalam sistem e-voting untuk meningkatkan kemanan hasil suara masyarakat. Berikut adalah beberapa hasil aplikasi dijalankan :

a. Halaman Voting (*user*)



Ini adalah halaman voting, dimana saat pemilih masuk ke menu *Voting*, akan dihadapkan gambar calon Bupati. Pemilih cukup mengklik gambar yang ingin dipilih lalu secara otomatis akan logout dan kembali ke halaman beranda. Pada proses ini hasil suara langsung terenkripsi.

b. Halaman Status Voting



Ini adalah halaman manajemen status voting. Disini juga terdapat hasil enkripsi hasil suara pemilih pada tabel encode.

c. **Halaman Rekapitulasi Hasil Suara**

Ini adalah halaman untuk melihat perolehan suara yang masuk, dengan cara mendekrip hasil suara (pada tabel encode) yang masuk lalu dijumlahkan.

2. Kesimpulan

Kesimpulan dari penelitian sistem E-voting Bupati Kab. Nganjuk adalah sebagai berikut :

a. Sistem e-voting yang dibangun dapat mengatasi permasalahan tentang sistem pilkada konvensional dan mengacu pada UU pilkada.
b. Sistem e-voting menggunakan metode kriptografi RSA dan pemilihan kunci khusus untuk meningkatkan keamanan hasil suara yang tersimpan di database.
c. Memiliki sistem rekapitulasi hasil suara agar dengan cepat mengetahui calon bupati yang terpilih.
d. Sistem e-voting dirancang dan dibangun sangat sesederhana mungkin untuk memudahkan pengguna dalam mengoperasikannya.

IV. DAFTAR PUSTAKA

[1]Agustina, Esti R. 2009. *Pemanfaatan Kriptografi dalam Mewujudkan Keamanan Informasi Pada E-Voting di Indonesia*. Seminar Nasional Informatika. UPN, Yogyakarta.

[2]Arifin, Zainal. 2009. *Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman*. Junrnal Informatika Mulawarman. Vol 4 No. 3 September 2009. FMIPA Universitas Mulawarman.

[3]Munir, Rinaldi. 2006. *Kriptografi*. Bandung : Informatika

[4]Neyman, Shelvie Nidya. 2013. *Penerapan Sistem E-voting pada Pemilihan Kepala Daerah di Indonesia*. 06 Jurnal Sains Terapan Edisi III Vol-3(1). IPB, Bogor.

[5]Rahmadian, Tika. 2014. *Desain Dan Implementasi Sistem Keamanan E-voting Dengan Jaminan Confidentiality Data*. Program Teknologi Informasi dan Ilmu Komputer. Universitas Brawijaya.