ISSN 1858-4853

RANCANG BANGUN E-VOTING DENGAN MENGGUNAKAN KEAMANAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) BERBASIS WEB (STUDI KASUS : PEMILIHAN KETUA BEM FMIPA)

Muhammad Ridwan[1)], Zainal Arifin[2)], Yulianto[3)]

[1,2,3)]Program Studi Ilmu Komputer, Fakultas Ilmu Komputer dan Teknologi Informasi,Universitas Mulawarman
Jalan Barong Tongkok Kampus Gunung Kelua Samarinda, Kalimantan Timur
Email : onesious@gmail.com [1)], zainal.ilkom.unmul@gmail.com [2)], yulianto.tile@gmail.com [3)]

ABSTRAK

E-voting adalah suatu sistem pemilihan dimana data dicatat, disimpan dan diproses dalam bentuk informasi digital. Dengan kata lain, *e-voting* merupakan pemungutan suara yang proses pelaksanaannya mulai dari pendaftaraan pemilih, pelaksanaan pemilihan, perhitungan suara dan pengiriman hasil suara dilaksanakan secara elektonik (digital) (Rokhman A, 2011). Namun kepercayaan masyarakat terhadap e-voting masih rendah. Hal ini disebabkan akan ketakutan masyarakat akan manipulasi hasil perolehan setiap kandidat. Untuk itu perlu dibuat sebuah sistem yang dapat menjamin akurasi hasil *e-voting*, integritas data ketika melakukan pengiriman hasil *voting* dari pemilih ke sistem, dan memvalidasi pemilih yang sesungguhnya dalam penerimaan hasil voting. Pada penelitian ini, penulis menerapkan metode keamanan RSA yaitu *public key* dan *private key*, untuk melakukan verifikasi. Aplikasi *e-voting* dibangun dengan bahasa pemrograman PHP, serta memanfaatkan *database* MySQLi sebagai *database server*. Dari hasil pengujian yang dilakukan, dapat disimpulkan bahwa sistem dapat bekerja dengan baik, dapat memvalidasi pemilih dan memverifikasi hasil *voting* apakah mengalami perubahan selama pengiriman.

Kata kunci : *e-voting*, RSA, *public key*, *private key*.

1. PENDAHULUAN

Voting adalah kegiatan yang sangat menentukan pada setiap perhelatan pemilihan, banyak varian kepentingan yang harus diakomodir di dalamnya (Azhari R, 2005), terutama bagaimana sistem pemilihan itu dilaksanakan, bagaimana peraturan yang disepakati dan menjadi aturan main, siapa yang dipilih dan siapa yang berhak memilih. Tidak kalah pentingnya adalah bagaimana proses pemungutan suara dapat menjamin azas langsung, umum, bebas dan rahasia serta bagaimana hasil penghitungan suara dapat berlangsung jujur, transparan, dapat diakses oleh publik. Semua persoalan di atas menjadi fokus perhatian bagi panitia penyelenggara pemilihan. Selama ini, *voting* secara centang atau coblos kertas suara menjadi pilihan dalam penyelenggaraan pemilu di tanah air.

Metode ini oleh banyak kalangan dinilai masih sangat konvensional ditengah kemajuan teknologi dan informasi, memiliki kelemahan dari aspek efisiensi dan efektifitas. Persoalan kesemrawutan data penduduk yang mempengaruhi validasi data pemilih, kebutuhan logistik pemungutan suara yang boros secara anggaran, pemungutan suara dan rekapitulasi penghitungan suara tidak efisien waktu, banyaknya personil penyelenggara pemungutan dan penghitungan suara di TPS yang membutuhkan pembiayaan, sampai rentannya kecurangan dan manipulasi hasil pemungutan suara. Bahwa *e-voting* merupakan sebuah sistem yang memanfaatkan perangkat elektronik dan mengolah informasi digital untuk membuat surat suara, memberikan suara, menghitung perolehan suara, menayangkan perolehan suara dan memelihara serta menghasilkan jejak audit.

Sistem ini membantu mempercepat proses pemungutan dan penghitungan suara serta mengurangi resiko kesalahan dan menghemat biaya. Untuk menjamin bahwa suara dari pemilih yang diterima masih utuh / otentik maka perlunya keamanan dalam suatu sistem voting.

Mengacu pada penelitian sebelumnya yaitu Perancangan E-voting Berbasis WEB (Studi Kasus Pemilihan Kepala Daerah Sukoharjo) (Nugroho, Aditya Wari. 2011). Penelitian tersebut mengenai aplikasi untuk melakukan voting kepala daerah Sukoharjo. Aplikasi yang dibangun menggunakan PHP dan MySQL sebagai database server. Dalam aplikasi voting tersebut, pemilih melakukan login dengan menggunakan nomor KTP yang dimilikinya.

Berdasarkan penelitian yang ada sebelumnya, penulis ingin membuat aplikasi serupa, yaitu aplikasi *e-voting*, yang menggunakan algoritma RSA sebagai sistem keamanan dalam melakukan *voting*. Algoritma RSA merupakan salah satu kriptografi asimetri, yakni jenis kriptografi yang menggunakan dua kunci yang berbeda yaitu

ISSN 1858-4853

kunci publik (*public key*) dan kunci pribadi (*private key*). Di Universitas Mulawarman, pada tahun 2014, telah dibuat sebuah sistem *e-voting* untuk pemilihan presiden Universitas Mulawarman. Namun sistem *e-voting* yang dibuat tidak dilengkapi dengan sistem keamanan. Sehingga perlu adanya sebuah sistem *e-voting* yang dilengkapi dengan sistem keamanan.

Berbagai masalah dalam proses pemungutan suara dapat diatasi dengan menerapkan Teknologi Informasi dan Komunikasi (TIK), yaitu *electronic voting*. *E-voting* dianggap lebih mudah dan lebih efisien dikarenakan semua prosesnya sudah dilakukan oleh komputer. Aplikasi *E-voting* juga mempermudah dalam proses penghitungan suara, karena dilakukan secara *online* maka suara hasil pemilihan yang masuk bisa langsung diketahui tanpa harus menghitung kertas suara seperti proses pemilihan secara manual (Fahmi, H., Handoko Dan Dwi, 2010).

2. TINJAUAN PUSTAKA

a. Rancang Bangun

Rancang Bangun (desain) adalah tahap setelah analisis dari siklus pengembangan sistem yang merupakan pendefinisian dari kebutuhan fungsional, serta menggambarkan bagaimana suatu sistem dibentuk yang dapat berupa penggambaran, perencanaan dan pembuatan sketsa atau pengaturan dari beberapa elemen yang terpisah ke dalam satu kesatuan yang utuh dan berfungsi, termasuk menyangkut mengkonfigurasikan dari komponen- komponen perangkat keras dan perangkat lunak dari suatu sistem (Jogiyanto, 2005).

b. E-voting

E-voting adalah suatu sistem pemilihan dimana data dicatat, disimpan dan diproses dalam bentuk informasi digital. Dengan kata lain, *e-voting* merupakan pemungutan suara yang proses pelaksanaannya mulai dari pendaftaraan pemilih, pelaksanaan pemilihan, perhitungan suara dan pengiriman hasil suara dilaksanakan secara elektonik (digital) (Rokhman, 2011).

Skema *E-voting* adalah satu set protokol yang menjaga keamanan atau kerahasiaan pemilih dalam melakukan pemilihan serta interaksi dengan panitia pemilihan dan perhitungansuara. *E-voting* biasanya dibedakan menjadi dua tipe yaitu *online* (misalnya via internet) dan *off line* (menggunakan mesin perhitungan suara atau kertas suara).

Tujuan dari keamanan sistem e-voting adalah untuk menjamin privasi atau kerahasiaan pemilih dan keakuratan pilihan.Keamanan sistem ini memiliki beberapa kriteria yaitu:

1. *Eligibility* artinya hanya pemilih yang terdaftar yang dapat melakukan pemilihan.
2. *Unreusability* artinya setiap pemilih hanya bisa memberikan satu kali pilihan.
3. *Anonymity* artinya pilihan pemilih dirahasiakan
4. *Accuracy* artinya pilihan tidak bisa diubah atau dihapus selama atau setelah pemilihan dan juga tidak bisa ditambahkan setelah pemilihan ditutup.
5. *Fairness* artinya perhitungan suara sebelum pemilihan ditutup tidak bisa dilakukan.
6. *Vote and Go* artinya pemilih hanya dapat melakukan pemilihan saja.
7. *Public Verifiability* artinya setiap orang dapat melakukan pengecekan pada berjalannya proses pemilihan

c. Badan Eksekutif Mahasiswa (BEM)

Organisasi mahasiswa intrakampus adalah Organisasi mahasiswa intrakampus adalah organisasi mahasiswa yang memiliki kedudukan resmi di lingkungan perguruan tinggi dan mendapat pendanaan kegiatan kemahasiswaan dari pengelola perguruan tinggi dan atau dari Kementerian/Lembaga. Bentuknya dapat berupa Ikatan Organisasi Mahasiswa Sejenis (IOMS), Unit Kegiatan Mahasiswa (UKM) atau Badan Eksekutif Mahasiswa (BEM).

Tugas pokok BEM adalah mewakili mahasiswa, mengkoordinasikan kegiatan organisasi kemahasiswaan dalam beda ekstrakurikuler ditingkat fakultas dan memberikan pendapat, usul dan saran kepada pimpinan akultas terutama berkaitan dengan peran, fungsi dan pencapaian tujuan pendidikan nasional (http://fkip.unmul.ac.id).

d. Keamanan Informasi

Keamanan informasi menurut beberapa sumber/pakar. Menurut Sarno dan Iffano keamanan informasi adalah suatu upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul. Sehingga keamanan informasi secara tidak langsung dapat menjamin kontinuitas bisnis, mengurangi resiko-resiko yang terjadi, mengoptimalkan pengembalian investasi (*return on investment*). Semakin banyak informasi perusahaan yang disimpan, dikelola dan di-*sharing*-kan maka semakin besar pula resiko terjadi kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak diinginkan (Sarno dan iffano : 2009).

Menurut ISO/IEC 17799:2005 tentang *information security management system* bahwa keamanan informasi adalah upaya perlindungan dari berbagai macam ancaman untuk memastikan keberlanjutan bisnis, meminimalisir resiko bisnis, dan meningkatkan investasi dan peluang bisnis

Keamanan Informasi memiliki 3 aspek, diantaranya adalah :

1. Confidentiality
   Keamanan informasi menjamin bahwa hanya mereka yang memiliki hak yang boleh mengakses informasi tertentu. Pengertian lain dari *confidentiality* merupakan tindakan pencegahan dari orang atau pihak yang tidak berhak untuk mengakses informasi.
2. Integrity
   Keamanan informasi menjamin kelengkapan informasi dan menjaga dari kerusakan atau ancaman lain yang mengakibatkan berubah informasi dari aslinya. Pengertian lain dari integrity adalah memastikan bahwa informasi tersebut masih utuh, akurat, dan belum dimodifikasi oleh pihak yang tidak berhak
3. Availability
   Keamanan informasi menjamin pengguna dapat mengakses informasi kapanpun tanpa adanya gangguan dan tidak dalam format yang tidak bisa digunakan. Pengguna dalam hal ini bisa jadi manusia, atau komputer yang tentunya dalam hal ini memiliki otorisasi untuk mengakses informasi. Availability meyakinkan bahwa pengguna mempunyai kesempatan dan akses pada suatu informasi. (http://doc.google.com).

Tiga elemen dasar *confidentiality, integrity, dan availability* (CIA) merupakan dasar diantara program program keamanan yang dikembangkan. Ketiga elemen tersebut merupakan mata rantai yang saling berhubungan dalam konsep *information protection*.

e. Algortima RSA

RSA merupakan algoritma kriptografi asimetri, dimana kunci yang digunakan untuk mengenkripsi berbeda dengan yang digunakan untuk mendekripsi. Kunci yang digunakan untuk mengenkripsi disebut dengan kunci publik, dan yang digunakan untuk mendekripsi disebut dengan kunci privat.

Algortima RSA dijabarkan pada tahun 1976 oleh tiga orang : Ron Rivest, Adi Shamir dan Len Adleman dari Massachusetts Institute of Technology. Huruf '"RSA"' itu sendiri berasal dari inisial nama mereka (‘R’ivest -‘S’hamir -‘A’dleman). Clifford Cocks, seorang matematikawan Inggris yang bekerja untuk GCHQ, menjabarkan tentang sistem equivalen pada dokumen internal di tahun 1973. Penemuan Clifford Cocks tidak terungkap hingga tahun 1997 karena alasan "*top- secret classification*". Algoritma RSA dipatenkan oleh Massachusetts Institute of Technology pada tahun 1983 di Amerika Serikat sebagai US *patent* 4405829. Paten tersebut berlaku hingga 21 September 2000. Setelah bulan September tahun 2000, paten tersebut berakhir, sehingga saat ini semua orang dapat menggunakannya dengan bebas (Kurniawan, 2012).

Algoritma RSA terbagi kedalam tiga bagian utama yaitu Proses Pembuatan Kunci (*Private dan Public Keys*), Proses Enkripsi (*Encrypt*) dan Proses Dekripsi (*Decrypt*).

f. WEB

Menurut Yuhefizar, Web adalah suatu metode untuk menampilkan informasi di internet, baik berupa teks, gambar, suara maupun video yang interaktif dan mempunyai kelebihan untuk menghubungkan (link) satu dokumen dengan dokumen lainnya (hypertext) yang dapat diakses melalui sebuah browser (Saputro, 2007)

g. Unified Modeling Language (UML)

UML adalah suatu bahasa yang digunakan untuk menentukan, memvisualisasikan, membangun, dan mendokumentasikan suatu sistem informasi. UML dikembangkan sebagai suatu alat untuk analisis dan desain berorientasi objek oleh Grady Booch, Jim Rumbaugh, dan Ivar Jacobson. Namun demikian UML dapat digunakan untuk memahami dan mendokumentasikan setiap sistem informasi. Penggunaan UML dalam industri terus meningkat. Inimerupakan standar terbuka yang menjadikannya sebagai bahasa pemodelan yang umum dalam industri peranti lunak dan pengembangan sistem (Fowler, 2005).

h. PHP

PHP adalah bahasa skrip yang dapat ditanamkan atau disisipkan ke dalam HTML/PHP banyak dipakai untuk membuat situs *web* dinamis. PHP dapat juga digunakan untuk membangun sebuah CMS. Sebagian besar sintaks mirip bahasa C, Java, dan Perl, ditambah beberapa fungsi PHP yang lebih spesifik. Tujuan utama penggunaan bahasa ini adalah untuk memungkinkan perancang dan penulis halaman *web* menjadi dinamis dan cepat (Badiyanto, 2013)

i. MySQL

MySQL merupakan salah satu sistem database yang menggunakan sql (*structured query language*) yakni bahasa yang berisi perintah-perintah untuk memanipulasi *database*, mulai dari melakukan perintah *select* untuk menampilkan isi *database*, *insert* atau menambahkan isi kedalam *database*, *delete* atau menghapus isi *database* dan *update* atau mengedit *database*. MySQL pun dapat digunakan secara langsung

ISSN 1858-4853

dengan mengetikkan perintah atau *syntax*nya melalui *console*. Dan bisa juga digunakan secara *embeded* SQL, artinya anda dapat menggunakan perintah sql dengan menyisipkannya kedalam bahasa pemgrogaman tertentu misalnya PHP (Syafii, M. 2013).

3. HASIL DAN PEMBAHASAN

Program yang dibangun merupakan sebuah sistem e-*voting* dalam pemilihan ketua BEM (Badan Eksekutif Mahasiswa) Fakultas Matematika dan ilmu Pengetahuan Alam berbasis *web* dengan menggunakan keamanan RSA (Rivest Shamir Adleman). Program ini dibangun agar mahasiswa mudah dalam memberikan hak suaranya kepada calon kandidat, dan sekaligus mempermudah panitia dalam menghimpun total suara untuk mendapatkan hasil akhir. Mahasiswa yang telah mendaftar, bisa *login* dengan menggunakan nim dan *password*, kemudian membuat kunci keamanan RSA, yaitu *public key* dan *private key*, sebelum memberikan *vote* kepada calon kandidat yang akan dipilih.

a. Analisis Sistem

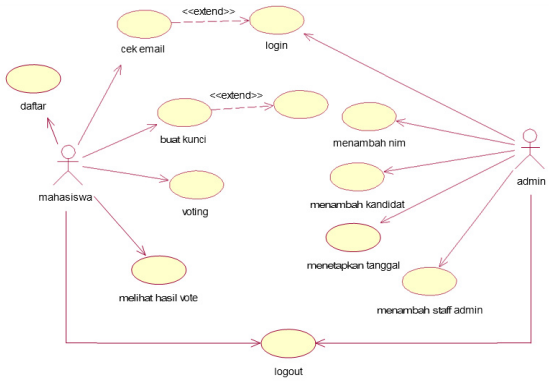
Pada tahap analisis sistem, sebuah skenario yang dirancang oleh penulis, yang terdiri dari beberapa bagian yang merupakan implementasi dari fungsi- fungsi penting yang dapat diakses oleh mahasiswa. Secara garis besar, sistem difungsikan sebagai berikut:

1. Sistem harus mampu melakukan verifikasi data mahasiswa dan mencatat status mahasiswa, apakah mahasiswa telah melakukan voting atau belum.
2. Mahasiswa dapat memasukkan pilihannya ke dalam sistem.
3. Sistem harus dapat menjumlahkan hasil voting, dan menampilkannya

b. Desain Model

Berdasarkan hasil analisis sistem, skenario yang dihasilkan akan direpresentasikan dalam bentuk diagram UML. Dalam penelitian ini, UML digunakan oleh penulis sebagai desain pemodelan sistem, hal ini dikarenakan bahasa pemrograman yang digunakan dalam pembangunan sistem mendukung untuk implementasi bahasa pemrograman berorientasi objek.

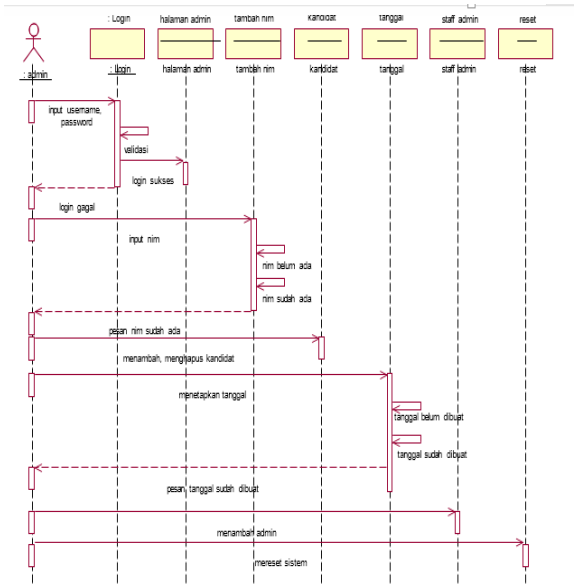
Diagram yang digunakan sebagai pemodelan sistem adalah Use case diagram, Class diagram, Sequence diagram dan Activity diagram



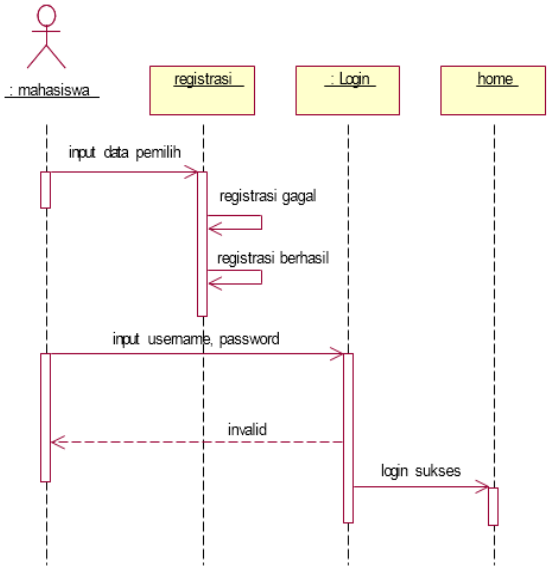
Gambar 2 *Use case Diagram*

Pada gambar 2, terdapat dua aktor yaitu pemilih yang memiliki hak untuk mendaftar, mengecek email untuk aktivasi link, agar bisa melakukan login, membuat kunci keamanan, melakukan voting, melihat hasil dan mencetak bukti vote. Aktor berikutnya yaitu Admin, yang bertugas untuk melakukan kontrol terhadap sistem. Admin dapat menambahkan nim mahasiswa, dalam hal ini adalah mahasiswa FMIPA, menambah calon kandidat, mengatur waktu voting, dan menambah staff admin.

Pada gambar 3, admin harus melakukan login terlebih dahulu. Jika login sukses, maka admin berhak mengakses halaman admin. Admin dapat menginput nim mahasiswa yang akan menjadi partisipan. Sistem akan mengecek apakah nim sudah ada atau belum. Admin juga bisa menambah calon kandidat, menghapus calon kandidat, menetapkan waktu voting, serta menambah staff admin

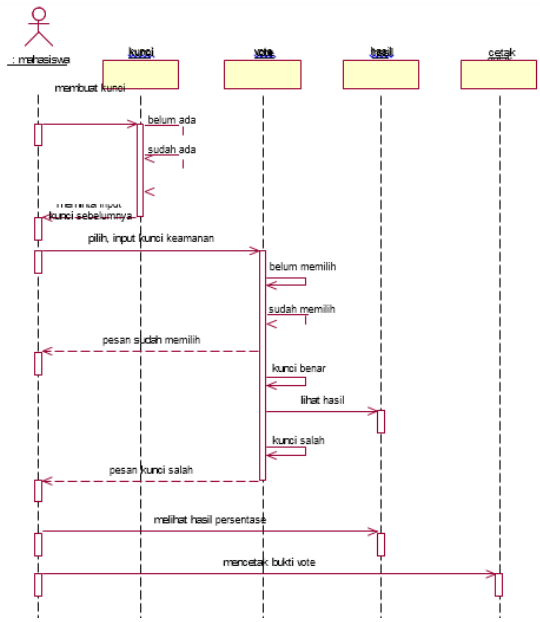


Gambar 3 *Squence* Diagram Admin



Gambar 3 *Squence* Diagram Login Pemilih

Pada gambar 4, pemilih harus melakukan pendaftaran/registrasi untuk bisa mengikuti vote ini. Setelah mendaftar, pemilih harus melakukan aktivasi melalui email masing-masing. Lalu pemilih bisa melakukan login untuk bisa masuk ke sistem. Pada gambar 5, pemilih harus membuat kunci keamanan terlebih dahulu. Kunci keamanan ini akan digunakan pada saat melakukan voting. Sistem akan memvalidasi pemilih dan kunci keamanannya. Apabila benar, maka vote yang diberikan dianggap sah. Pemilih bisa melihat hasil perolehan para calon kandidat. Dan pemilih bisa mencetak bukti dari vote yang dilakukan.



Gambar 5 *Squence* Diagram Melakukan Voting

c. Desain tabel

Pada tahap perancangan sistem terdapat 1 database yang terdiri dari 7 tabel yaitu:

1. Tabel pemilih

Tabel ini terdiri dari delapan *field*, dan id pemilih sebagai *primary key*. Tabel ini digunakan untuk menyimpan informasi mahasiswa yang mendaftar sebagai partisipan.

Tabel 1 Desain tabel pemilih

No.	Field	Tipe	Keterangan
1	Nama	varchar(30)	-
2	Nim	int(11)	Primary key
3	Password	varchar(100)	-
4	Jenkel	varchar(10)	-
5	Jurusan	varchar(50)	-
6	Status	int(2)	-
7	Poto	varchar(50)	-
8	batas_login	Int(2)	
9	blokir	enum	‘Y’,”N’

2. Tabel admin

Tabel admin terdiri dari tiga *field*, dan id sebagai *primary key*. Tabel ini digunakan untuk menyimpan data admin.

Tabel 2 Desain tabel admin

No.	Field	Tipe	keterangan
1	Id	Varchar(25)	Primary Key
2	username	Varchar(50)	-
3	password	Varchar(50)	-

3. Tabel Calon

Tabel calon terdiri dari enam *field*, dan id_calon sebagai *primary key*. Tabel ini digunakan untuk menyimpan data calon kandidat yang akan dipilih.

Tabel 3 Desain tabel calon

No	Field	Tipe	Ketera
1	nama	varchar(50)	-
2	Ni	int(11)	-
3	jurusan	varchar(20)	-
4	Ket	varchar(1000)	-
5	Poto	varchar(50)	-

4. Table hasil.

Terdiri dari empat *field*, dan id_hasil sebagai *primary key*. Tabel ini digunakan untuk menyimpan data perolehan *vote* calon kandidat.

Tabel 4 Desain Tabel Hasil

No.	Field	Tipe	Keterangan
1	nim_mhs	Int(11)	-
2	nim_calon	Int(11)	-
4	nama	varchar(15)	-

ISSN 1858-4853

5. Tabel Kunci
   Tabel kunci terdiri dari lima *field*. Tabel ini digunakan untuk menyimpan data kombinasi kunci RSA yang dibuat oleh mahasiswa.

Tabel 5 Desain tabel kunci

No.	Field	Tipe	Keterangan
1	Nim	Int(11)	-
2	E	Int(11)	-
3	D	Int(11)	-
4	N	Int(11)	-
5	keterangan	Int(11)	-

6. Tabel mhs
   Tabel mhs terdiri dari dua *field*. Tabel ini digunakan untuk menyimpan nim mahasiswa FMIPA

Tabel 6 Desain tabel mhs

No.	Field	Tipe	keterangan
1	Nim	Int(11)	-
2	Jurusan	Varchar(50)	-
3	Email	Varchar(25	-

7. Tabel Tanggal
   Tabel ini terdiri dari lima *field*, Tabel ini digunakan untuk menyimpan waktu dimulai dan berakhirnya kegiatan voting.

Tabel 7 Desain tabel tanggal

No.	Field	Tipe	Keterangan
1	username	Varchar(20)	-
2	awal	Date	-
3	akhir	Date	-
4	start	Time	-
5	end	Time	-

4. IMPLEMENTASI SISTEM

a. Implementasi Antarmuka

Gambar 7 Tampilan Halaman Utama Website

Gambar 7 merupakan halaman utama website. Pada halaman ini, mahasiswa bisa melakukan pendaftaran dan melakukan login.

Gambar 8 Tampilan Halaman Beranda Mahasiswa

Gambar 8 merupakan halaman beranda mahasiswa yang telah sukses melakukan login.

Gambar 9 Halaman Membuat Kunci Keamanan

Pada halaman 9, halaman ini digunakan untuk membuat kunci keamanan. Mahasiswa akan mendapat sepasang *public key* dan *private key*.

Gambar 10. Halaman Voting

Ini merupakan halaman untuk melakukan voting. Mahasiswa akan diminta untuk menginput nilai e dan nilai n, yang merupakan pasangan *public key* yang telah dibuat. Sistem akan memverifikasi pasangan public key yang dimasukkan.

b. Implementasi Algoritma RSA

Contoh untuk implementasi algoritma RSA:

1. Pilih nilai p = 29 dan nilai q = 83, dimana keduanya adalah bilangan prima.
2. Hitung nilai n = p x q = 29 x 83 = 2407
3. Kemudian hitung nilai $\phi(n)$ dengan cara nilai p-1 dikalikan dengan nilai q-1.
   $\phi(n) = (p-1) \times (q-1) = (29-1) \times (31-1)$
   $= 28 \times 82 = 2296$
4. Misal, kita pilih nilai e = 3. Nilai e

harus relativ prima, artinya GCD(e, □(n)) harus menghasilkan nilai 1. Untuk membuktikan bahwa 3 relativ prima tehadap GCD(e, □□(n)), dilakukan dengan cara:

2296 = 765 x 3 + 1

Jadi nilai e = 3 adalah benar

5. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan oleh penulis, dapat diperoleh beberapa kesimpulan, diantaranya:

1. *E-voting* hanya diikuti oleh mahasiswa Fakultas Matematika dan Ilmu Pengetahuan Alam, dengan satu mahasiswa hanya boleh menggunakan satu nim dan satu *email* dalam mendaftar.
2. Implementasi algoritma RSA pada sistem *e-voting* ini telah berjalan dengan baik untuk dapat menjaga integritas data hasil *voting* sehingga dapat diverifikasi bahwa data hasil *e-voting* tidak mengalami perubahan selama proses pengiriman.
3. Keamanan algoritma RSA hanya digunakan pada saat melakukan *voting*, yaitu *public key*. Dan *private key* digunakan untuk melakukan perubahan kunci.

Penulis menyadari masih terdapat banyak kekurangan dalam penelitian ini. Oleh sebab itu, diusulkan beberapa saran sebagai berikut :

1. Sebaiknya dipilih nilai p dan nilai q dengan angka yang besar, karena semakin besar nilai p dan nilai q, maka semakin susah untuk menentukan nilai d, sehingga kombinasi pasangan kunci tidak mudah ditebak.
2. Sebaiknya gambar alur melakukan *voting*, dibuat dalam bentuk gambar bergerak, sehingga semakin mempermudah mahasiswa dalam memahami alur dalam melakukan *voting*
3. Sebaiknya ditambahkan tampilan waktu untuk hitung mundur bahwa *voting* akan ditutup.
4. Sebaiknya pengembangan tampilan lebih menarik lagi tanpa mengurangi kemudahan pengguna

6. DAFTAR PUSTAKA

[1]. Azhari, R. 2005. *E-Voting*, Jurnal Fakultas Ilmu Komputer, Universitas Indonesia, Jakarta.

[2]. Badiyanto. 2013. *Buku Pintar Framework Yii*. Penerbit : Mediakom Yogyakarta.

[3]. Bentuk dan Struktur Organisasi. http://fkip.unmul.ac.id/page/4/45/Bentuk_dan_Struktur_Organisasi_Mahasiswa. Diakses pada tanggal 4 April 2015 14.00 Wita.

[4]. Fahmi, H., Handoko & Dewi. 2010. *Kajian Teknis tentang Pemungutan Suara secara Elektronik Teknologi Informasi dan Komunikasi, Badan Pengkajian dan Penerapan Teknologi*, Jakarta.

[5]. Fowler, M. 2005. *UML Distilled Edisi 3 Panduan Singkat Bahasa Pemodelan Objek*

[6]. *Standar*. Penerbit : Andi Yogyakarta. Jogiyanto. 2005. *Analisis dan Desain* Penerbit : Andi Yogyakarta.

[7]. Kurniawan, I. 2012. *Algoritma RSA*. http://studyinformatics.blogspot.com/2012/07/algoritma-rsa.html. Diakses pada tanggal 14 Agustus 2014 18:30 Wita

[8]. Nugroho, A W. 2011. *Perancangan E-Voting Berbasis WEB (Studi Kasus Pemilihan Kepala Daerah Sukoharjo).* Skripsi, UIN Sunan Kalijaga Yogyakarta.

[9]. Nugroho, B. 2004. *Database Relasional dengan MySQL*. Yogyakarta: Andi.

[10]. Rokhman, A. 2011. *Prospek dan Tantangan Penerapan e-Voting di Indonesia. Seminar Nasional Peran Negara dan Masyarakat dalam Pembangunan Demokrasi dan Masyarakat Madani di Indonesia* Universitas Terbuka, Jakarta.

[11]. Saputro, H W. 2007. *Definisi dan Pengertian Web Menurut Para Ahli*. http://www.sambureki.com/definisi/definisi-dan-pengertian-web-menurut-para-ahli.html. Diakses pada tanggal 2 April 2015 13.30 Wita.

[12]. Sidik, B. 2006. *Pemrograman Web Dengan PHP, Bandung* : Informatika Bandung.

[13]. Syafii, M. 2004. *Membangun Aplikasi Berbasis PHP dan MySQL*. Penerbit : Andi Yogyakarta.