RANCANG BANGUN *E-ELECTION* PEMILIHAN DI LINGKUNGAN UNIVERSITAS TANJUNGPURA MENGGUNAKAN ALGORITMA *RIJNDAEL*

Deni Saputra[1], Helfi Nasution [2], M. Azhar Irwansyah[3]
Program Studi Teknik Informatika Universitas Tanjungpura[1, 2, 3]
deni@probowsolution.com[1], helfi_nasution@yahoo.com[2], irwansyah.azhar@untan.ac.id[3]

Abstrak- **Voting telah menjadi salah satu metode untuk mengambil keputusan penting dalam kehidupan manusia. Voting digunakan untuk menghimpun aspirasi dari seluruh elemen masyarakat dan kemudian dijadikan sebagai jalan keluar yang dianggap paling baik untuk menyelesaikan permasalahan. Universitas Tanjungpura adalah salah satu perguruan tinggi yang melaksanakan pemilihan pejabat struktural setiap beberapa tahun sekali. *e-voting* atau *e-Election* adalah sebuah teknologi yang menjanjikan untuk memperbaiki banyak masalah pada pemungutan suara yang dilakukan secara konvensional, dan secara komprehensif memiliki potensi untuk memecahkan masalah yang ada selama ini terutama solusi untuk meminimalkan kemungkinan kerugian walaupun masih terdapat satu masalah yang akan selalu ada pada semua jenis sistem elektronik yaitu kemungkinan kehilangan suara. Aplikasi web ini dapat digunakan dalam beberapa pemilihan yang berlangsung secara bersamaan, dan sifatnya dinamis tanpa perlu mengubah ulang script jika ingin menggunakannya. Salah satu cara untuk melindungi data dari pihak yang tidak diinginkan adalah dengan mengacak data yang dikirim tersebut, sehingga apabila data tersebut diterima oleh pihak lain, mereka tidak memahami maksud data tersebut. Algoritma *Rijndael* terpilih sebagai algoritma kriptografi yang dapat melindungi informasi dengan baik serta efisien dalam implementasinya dan dinobatkan sebagai AES. *Rijndael* termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan blok sandi. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi (bentuk acak) dan dekripsi (mengembalikan ke bentuk semula) serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu. Hasil pengujian dan perancangan menunjukkan bahwa aplikasi ini dapat digunakan untuk pemilihan pejabat struktural di lingkungan Universitas Tanjungpura. Hasil pengujian enkripsi/dekripsi menunjukkan bahwa waktu pemrosesan untuk algoritma *rijndael* tergolong singkat dan cepat, serta algoritma *rijndael* memiliki pola *chipertext* = 44 karakter dari panjang karakter *plaintext* = 32 karakter dan berlaku kelipatannya. Hasil perhitungan suara ditampilkan menggunakan diagram batang tiap kandidat pemilihan.**

Kata Kunci : voting, web, evoting, e-election, algoritma rijndael

I. PENDAHULUAN

Voting telah menjadi salah satu metode untuk mengambil keputusan penting dalam kehidupan manusia. voting digunakan mulai dari tingkat masyarakat terkecil, yaitu keluarga, sampai dengan sebuah negara. Voting digunakan untuk menghimpun aspirasi dari seluruh elemen masyarakat dan kemudian dijadikan sebagai jalan keluar yang dianggap paling baik untuk menyelesaikan permasalahan.

Universitas Tanjungpura adalah salah satu perguruan tinggi yang melaksanakan pemilihan pejabat struktural setiap beberapa tahun sekali. Pelaksanaan pemilihan dilakukan mulai dari tingkat prodi (pemilihan Kaprodi), fakultas (pemilihan Senat dan Dekan), sampai tingkat universitas (pemilihan Rektor).

Pemilihan pejabat struktural di Universitas Tanjungpura masih dilakukan secara manual. Mahasiswa/dosen yang mempunyai hak pilih datang ke tempat pemungutan suara pada saat hari pemilihan. Mereka kemudian mencoblos atau mencontreng (√) kertas suara dan kemudian memasukkan ke kotak suara. Setelah proses pemungutan suara selesai, kemudian dilakukan penghitungan suara.

e-voting atau *e-Election* adalah sebuah teknologi yang menjanjikan untuk memperbaiki banyak masalah pada pemungutan suara yang dilakukan secara konvensional, dan secara komprehensif memiliki potensi untuk memecahkan masalah yang ada selama ini terutama solusi untuk meminimalkan kemungkinan kerugian walaupun masih terdapat satu masalah yang akan selalu ada pada semua jenis sistem elektronik yaitu kemungkinan kehilangan suara.

Dengan adanya teknik kriptografi, berbagai kekhawatiran dan semua yang diharapkan oleh pengirim data dapat teratasi. Salah satu dari teknik kriptografi adalah *rijndael*. *Rijndael* termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan blok sandi. Dengan demikian algoritma ini mempergunakan

kunci yang sama saat enkripsi (bentuk acak) dan dekripsi (mengembalikan ke bentuk semula) serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu. *Rijndael* mendukung berbagai variasi ukuran blok dan kunci yang akan digunakan. Namun *Rijndael* mempunyai ukuran blok dan kunci yang tetap sebesar 128, 192, 256 bit. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi.

II. URAIAN PENELITIAN

A. *E-voting/E-Election*

E-voting atau E-Election adalah sebuah teknologi yang menjanjikan untuk memperbaiki banyak masalah pada pemungutan suara yang dilakukan secara konvensional, dan secara komprehensif memiliki potensi untuk memecahkan masalah yang ada selama ini terutama solusi untuk meminimalkan kemungkinan kerugian walaupun masih terdapat satu masalah yang akan selalu ada pada semua jenis sistem elektronik yaitu kemungkinan kehilangan suara [1].

B. *Kriptografi*

Kriptografi dalam sejarahnya tercatat dipergunakan secara terbatas oleh bangsa Mesir 4000 tahun lalu. Kriptografi (*Cryptography*) berasal dari dua kata yaitu "*Crypto* & *graphy*" yang dalam sudut bahasa "*Crypto*" dapat diartikan rahasia (secret) dan "*graphy*" dapat diartikan tulisan (*writing*) jadi Kriptografi (*Cryptography*) dapat diartikan sebagai suatu ilmu atau seni untuk mengamankan pesan agar aman dan dilakukan oleh "*Cryptographer*". [2].

C. *Algoritma Rijndael*

Rijndael termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan *cipher block*. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu[3].

Rijndael mendukung berbagai variasi ukuran blok dan kunci yang akan digunakan. Namun *Rijndael* mempunyai ukuran blok dan kunci yang tetap sebesar 128, 192, 256 bit. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi. Berikut adalah perbandingan jumlah proses yang harus dilalui untuk masing-masing masukan[3].

Blok-blok data masukan dan kunci dioperasikan dalam bentuk *array*. Setiap anggota *array* sebelum menghasilkan keluaran *ciphertext* dinamakan dengan *state*. Setiap *state* akan mengalami proses yang secara garis besar terdiri dari empat tahap yaitu, *AddRoundKey*, *SubBytes*, *ShiftRows*, dan *MixColumns*. Kecuali tahap *MixColumns*, ketiga tahap lainnya akan diulang pada setiap proses sedangkan tahap *MixColumns* tidak akan dilakukan pada tahap terakhir. Proses dekripsi adalah kebalikkan dari enkripsi.

1. *Add Round Key*
   Pada proses ini subkey digabungkan dengan state. Proses penggabungan ini menggunakan operasi XOR untuk setiap byte dari subkey dengan byte yang bersangkutan dari state. Untuk setiap tahap, subkey dibangkitkan dari kunci utama dengan menggunakan proses key schedule. Setiap subkey berukuran sama dengan state yang bersangkutan.
2. *SubBytes*
   Proses *SubBytes* adalah operasi yang akan melakukan substitusi tidak linear dengan cara mengganti setiap *byte state* dengan *byte* pada sebuah tabel yang dinamakan tabel S-Box. Sebuah tabel S-Box terdiri dari 16x16 baris dan kolom dengan masing-masing berukuran 1 *byte*.
3. *Shift Rows*
   Proses *Shift Row*s akan beroperasi pada tiap baris dari tabel *state*. Proses ini akan bekerja dengan cara memutar *byte-byte* pada 3 baris terakhir (baris 1, 2, dan 3) dengan jumlah perputaran yang berbeda-beda. Baris 1 akan diputar sebanyak 1 kali, baris 2 akan diputar sebanyak 2 kali, dan baris 3 akan diputar sebanyak 3 kali. Sedangkan baris 0 tidak akan diputar.
4. *MixColumns*
   Proses *MixColumns* akan beroperasi pada tiap kolom dari tabel state. Operasi ini menggabungkan 4 *bytes* dari setiap kolom tabel *state* dan menggunakan transformasi linier. Operasi *MixColumns* memperlakukan setiap kolom sebagai *polinomial* 4 suku dalam *Galois field* dan kemudian dikalikan dengan c(x) *modulo* (x4+1), dimana c(x)=3x3 +x2+x+2. *Kebalikkan* dari *polinomial* ini adalah c(x)=11x3+13x2+9x+14. Operasi *MixColumns* juga dapat dipandang sebagai perkalian *matrix*.

D. *Black Box*

Pengujian perangkat lunak merupakan salah satu tahapan penting dalam pembangunan perangkat lunak. Proses pengujian dilakukan untuk menentukan kebenaran perangkat lunak. Aktivitas yang terjadi dalam pengujian perangkat lunak terdiri dari pengujian kode program hingga kegiatan percobaan terhadap perangkat lunak yang sudah berfungsi. Adapun tujuan dari pengujian perangkat lunak adalah sebagai berikut: Untuk mengidentifikasi dan menyatakan sebanyak mungkin *error* yang dimiliki oleh perangkat lunak yang diuji.

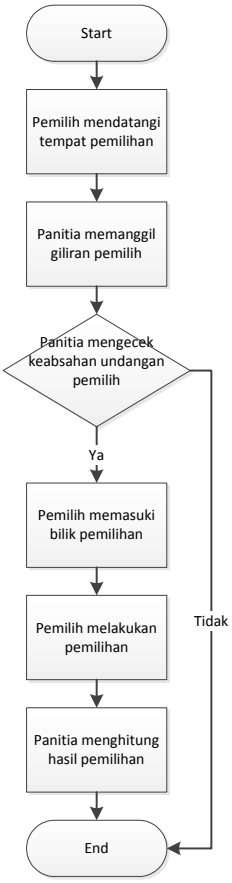
1. Untuk membawa perangkat lunak yang diuji ke tingkat kualitas yang dapat diterima, setelah perangkat lunak tersebut mengalami pembetulan atau koreksi atas *error* yang ditemukan.
2. Untuk melaksakan uji-uji yang dibutuhkan secara efisien dan efektif, dalam keterbatasan *budget* dan waktu penjadwalan.

Pentingnya pengujian perangkat lunak dan implikasinya yang mengacu pada kualitas perangkat lunak tidak dapat terlalu ditekan karena melibatkan sederetan aktivitas produksi di mana peluang terjadinya kesalahan manusia sangat besar dan arena ketidakmampuan manusia untuk melakukan dan berkomunikasi dengan sempurna maka pengembangan perangkat lunak diiringi dengan aktivitas jaminan kualitas.

III. HASIL DAN DISKUSI

A. *Gambar Sistem Usulan*

Sistem yang akan dibangun menggunakan web, sehingga memudahkan dalam pengaksesan dan memanajemen sistem fitur yang ada, adapun gambaran sistem yang dibangun adalah :

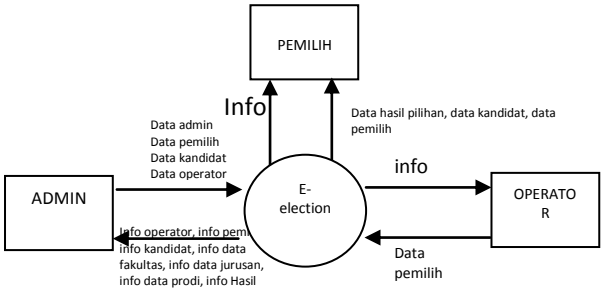


Gambar 1 Gambar Sistem Usulan

B. *Diagram Konteks*

Diagram konteks adalah diagram yang memberikan gambaran umum terhadap aktivitas yang berlangsung pada Rancangan *E-Voting* Pemilihan di Universitas Tanjungpura. Diagram konteks memperlihatkan bahwa subjek yang terlibat langsung dalam proses sistem adalah:

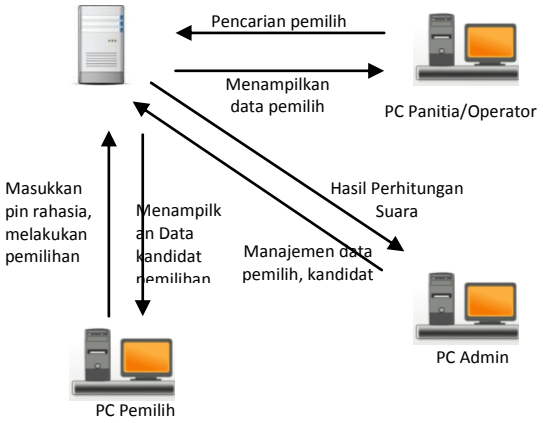
1. Admin
2. Pemilih
3. Operator



Gambar 2 Diagram Konteks Sistem

C. *Analisis Kebutuhan Sistem*

Sistem yang dibangun berbasis web (intranet) dimaksudkan untuk dapat diakses oleh banyak *user* (laptop). Desain arsitektur sistem dapat dilihat pada Gambar 3 sebagai berikut :



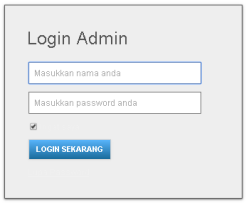
Gambar 3 Perancangan Arsitektur Sistem

D. *Hasil Perancangan Desain*

Halaman awal Pemilih berfungsi sebagai halaman untuk melakukan proses pemilihan suara. Halaman ini merupakan halaman setelah halaman awal dan dapat diakses tanpa melalui proses *login* terlebih dahulu hanya melalui perubahan status memilih yang dioperasikan oleh *Operator*. Jadi Pemilih tidak perlu memasukkan password ataupun sejenisnya untuk mengakses aplikasi, karena aplikasi siap digunakan langsung. Halaman Awal Pemilih diperlihatkan pada gambar 4 dibawah ini

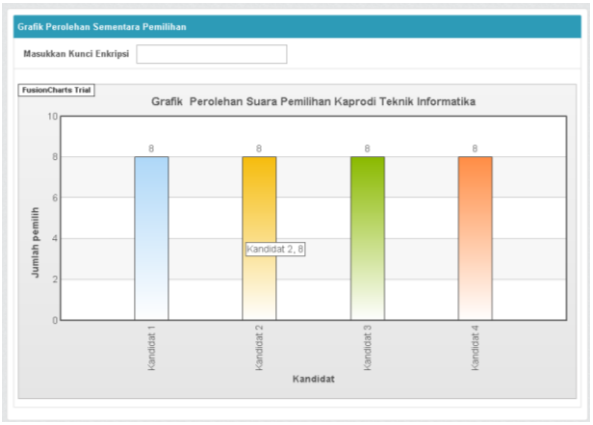
Gambar 4 Halaman Awal Pemilih

Halaman login merupakan halaman bagi *operator* dan *admin* untuk masuk kedalam menu aplikasi untuk mengelola konten. Halaman login diperlihatkan pada gambar 5 dibawah ini :



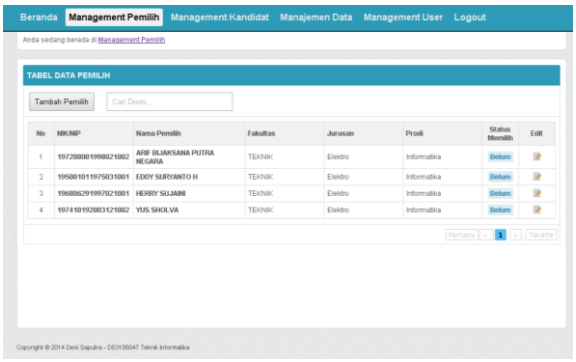
Gambar 5 Halaman *Login Operator dan Admin*

Halaman Dashboard/beranda merupakan halaman bagi admin, untuk menampilkan hasil voting menggunakan grafik. Antarmuka halaman dashboard/beranda admin diperlihatkan pada gambar 6 dibawah ini :



Gambar 6 Halaman Dashboard Admin

Halaman management pemilih, merupakan halaman bagi admin dan operator untuk melakukan proses pengelolaan pemilih tersebut. Halaman management pemilih dapat dilihat pada gambar 8 dibawah ini :



Gambar 7 Halaman Management Pemilih

Halaman management kandidat, merupakan halaman bagi admin dan operator untuk melakukan proses penambahan, pembaharuan serta menampilkan table kandidat. Halaman management kandidat dapat dilihat pada gambar 8 dibawah ini :

Gambar 8 Halaman Management Kandidat

E. Hasil Pengujian Black box

Pengujian berikut dilakukan pada menu login admin dan operator. Hasil pengujian dapat dilihat pada tabel 1 dibawah ini :

Tabel 1 Hasil Pengujian input menu login admin/operator

No. Uji	Input	Contoh Data		Hasil eksekusi	Keterangan
1	Semua data tidak bernilai	Username		Tidak berhasil	Pesan Kesalahan: "Anda Belum Mengisikan Username"
		Password			
2	Beberapa data tidak bernilai	Username	admin	Tidak berhasil	Pesan Kesalahan: "Anda Belum Mengisikan Password"
		Password			
3	Data tidak sesuai	Username	admin	Tidak berhasil	Pesan Kesalahan: "ERROR! Username/Password yang anda masukkan tidak terdaftar"
		Password	1212		
4	Data benar dan sesuai	Username	admin	Berhasil	
		Password	*****		

Pengujian berikut dilakukan pada halaman Input Data Pemilih. Hasil pengujian dapat dilihat pada tabel 2 dibawah ini :

Tabel 2 Hasil Pengujian Halaman Input Data Pemilih

No. Uji	Input	Contoh Data		Hasil eksekusi	Keterangan
1	Semua data kosong	nip_nim		Tidak Berhasil	Pesan Kesalahan: "Harap Isi Bidang Ini"
		nama			
		alamat			
		agama			
		pendidikan			
		jabatan_fungsional			
		golongan_pns			
		pangkat			
		universitas	Tanjungpura		
		fakultas			
		jurusan			
		prodi			
2	Beberapa data tidak bernilai	nip_nim	197208081998021002	Tidak Berhasil	Pesan Kesalahan: "Harap Isi Bidang Ini"
		nama	YUS SHOLVA		
		alamat	-		
		agama	Islam		
		pendidikan	S2		
		jabatan_fungsional			
		golongan_pns	IIIC		
		pangkat	Penata Tk.1		
		universitas	Tanjungpura		
		fakultas	Teknik		
		jurusan	Elektro		
		prodi	Informatika		
3	Data benar dan sesuai	nip_nim	197208081998021002	Berhasil	Pesan Berhasil: "Sukses! Anda berhasil memasukkan data pemilih "
		nama	YUS SHOLVA		
		alamat	-		
		agama	Islam		
		pendidikan	S2		
		jabatan_fungsional	Lektor		
		golongan_pns	IIIC		
		pangkat	Penata Tk.1		
		universitas	Tanjungpura		
		fakultas	Teknik		
		jurusan	Elektro		

Pengujian berikut dilakukan pada halaman Input Data Kandidat. Hasil pengujian dapat dilihat pada tabel 3 dibawah ini :

Tabel 3 Hasil Pengujian Halaman Input Data Kandidat

No. Uji	Input	Contoh Data		Hasil eksekusi	Keterangan
1	Semua Data bernilai Kosong	Nama Kandidat		Tidak berhasil	Pesan Kesalahan: "Harap isi bidang ini"
		Nomor Kandidat			
		Foto Kandidat			
		Tentang Kandidat			
2	Beberapa data bernilai kosong	Nama Kandidat	YUS SHOLVA	Tidak berhasil	Pesan Kesalahan: "Harap isi bidang ini"
		Nomor Kandidat	1		
		Foto Kandidat			
		Tentang Kandidat	-		
3	Data benar dan sesuai	Nama Kandidat	YUS SHOLVA	Berhasil	Pesan Berhasil: "Sukses! Anda berhasil memasukkan data kandidat"
		Nomor Kandidat	1		
		Foto Kandidat	kandidat1.jpg		
		Tentang Kandidat	-		

Pengujian berikut dilakukan pada halaman Input Data Kunci Enkripsi. Hasil pengujian dapat dilihat pada tabel 4 dibawah ini :

Tabel 4 Hasil Pengujian Halaman Input Kunci Enkripsi

No. Uji	Input	Contoh Data		Hasil eksekusi	Keterangan
1	Data Kosong	Kunci Enkripsi		Tidak berhasil	Data Grafik Perhitungan Suaran Tidak Muncul
2	Data Salah	Kunci Enkripsi	123456789	Tidak berhasil	Data Grafik Perhitungan Suaran Tidak Muncul
3	Data benar dan sesuai	Kunci Enkripsi	67dgdjggghfyggvvhfhftdhgu#$@hgjg	Berhasil	

Pengujian berikut dilakukan pada halaman Input Data Enkripsi dan Dekripsi. Hasil pengujian dapat dilihat pada tabel 5 dibawah ini :

Tabel 5 Hasil Pengujian Halaman Input Data Enkripsi dan Dekripsi

No. Uji	Jenis Input	*Plaintext*	Chipertext (Rijndael)	Waktu	Keterangan
1	Id Kandidat	1	dsv9O0edE4G2KA3lw1RVpGgUiWfiaiaRYaMn5rB3kJM=	1.0E5 Detik	Kode Kandidat
2	Id Pemilih	197410192003121002	sbgnMRQ5Bkzd025OBzmbthiFpAbfK2Ea0VrZSpZrgns=	1.0E5 Detik	NIP/NIM Pemilih
3	Tgl Pilih	2014-07-10 09:00:00	IS9p2WOMM6LcEl//W67fLSoJkcZrmFJMJrSOMYV+EEI=	1.0E5 Detik	
4	Dummy Text 1	abcdefghijklmnopqrstuvwxyzabcdef	bIJjp50HLWpQB4M14RR7tHnlwtqQ4CtS0BfkexSNdJU=	1.0E5 Detik	Panjang karakter plaintext = 32, Panjang karakter chipertext = 44

F. Analisis Hasil Pengujian

Berikut merupakan analisis hasil perancangan dan pengujian E-Election Pemilihan Di Lingkungan Universitas Tanjungpura Menggunakan Algoritma Rijndael :

1. Sistem akan menghalangi *user* yang memasukkan *username* dan *password* yang salah ketika proses *login* sehingga sistem hanya dapat diakses oleh *user* yang memiliki hak akses.
2. Hasil pengujian menunjukkan bahwa saat dilakukan *input* data dengan menggunakan metode *black box*, *input* data dengan keseluruhan data kosong akan menimbulkan kesalahan pada program. Akan tetapi pada sistem ini, kemungkinan terjadinya kesalahan sudah ditangani pada kode program sehingga hanya akan muncul pesan kesalahan atau instruksi pengisian data. Dengan kata lain, sistem dapat menangani data tersebut sesuai dengan apa yang diharapkan.
3. Hasil pengujian menunjukkan bahwa saat dilakukan *input* data dengan salah satu data yang bernilai kosong akan menyebabkan kesalahan apabila data tersebut tidak diperbolehkan kosong di dalam basis data. Pada sistem ini kemungkinan tersebut sudah ditangani pada kode program sehingga akan muncul pesan kesalahan jika ada salah satu data yang belum diisi.
4. Hasil pengujian menunjukkan bahwa saat dilakukan *enkripsi/dekripsi* menggunakan rijndael dengan data *teks* yang memiliki panjang karakter sedikit ataupun panjang karakter banyak tidak mempengaruhi waktu pemrosesan *enkripsi/dekripsi* dan hanya berlangsung dalam waktu singkat.
5. Hasil pengujian menunjukkan bahwa saat dilakukan *enkripsi/dekripsi* menggunakan rijndael dengan panjang kunci 256 bit panjang karakter *plaintext* sebanyak kurang dari atau sama dengan 32 karakter menghasilkan *chipertext* dengan panjang karakter 44 karakter dan berlaku kelipatan dari *plaintext.*
6. Hasil perancangan dan pengujian menunjukkan bahwa sistem sudah baik untuk setiap aspek pada metode *Rijndael.*
7. Hasil perancangan dan pengujian sistem menunjukkan bahwa sistem ini menjadi solusi untuk melakukan voting Pejabat Struktural pada Lingkungan Universitas Tanjungpura Pontianak.

DAFTAR PUSTAKA

[1] Carter, Craig. 2003. *E-Election*. Makalah disajikan dalam seminar. Massey University, Albany, Auckland, New Zealand.

[2] Arius, Dony. *Pengantar ilmu kriptografi: teori analisis & implementasi*. Andi. Yogyakarta

[3] Surian, Didi. 2006. *Algoritma Kriptografi Aes Rijndael*. Palembang: Jurusan Teknik Elektro, Universitas Tarumanegara.