Jurnal Sarjana Institut Teknologi Bandung Bidang Teknik Elektro dan Informatika
Volume 1, Number 2, Juli 2012

# Sistem Keamanan Data e-Voting Menggunakan Algoritma Kriptografi Rijndael

Syaugi Mamdudi[*1] dan Aciek Ida Wuryandari[*2]
[*]*Program Studi Teknik Elektro STEI, Institut Teknologi Bandung*
*Jalan Ganesha No.10, Bandung 40132, Indonesia*
[1]syaugi_m@students.itb.ac.id
[2]aciek@lskk.ee.itb.ac.id

***Abstrak*—Penggunaan teknologi komputer pada pelaksanaan pemilu dikenal dengan istilah *electronic voting* atau lazim disebut dengan *e-voting*. Sistem ini sendiri telah digunakan di banyak negara karena memiliki kelebihan dalam hal skalabilitas, efisiensi, dan akurasi pada proses pemilu. Walaupun demikian, terdapat beberapa permasalahan yang muncul akibat dari implementasi sistem ini antara lain : tingkat keamanan sistem, penggunaan internet yang rentan dengan gangguan dari luar, dan penggunaan perangkat lunak yang tidak dapat diaudit oleh publik. Untuk mencegah terjadinya perubahan data oleh pihak-pihak yang tidak berhak, maka dikembangkanlah berbagai teknik pengamanan data, salah satunya dengan kriptografi. Pada penelitian ini akan dibahas terkait salah satu algoritma yang dapat digunakan untuk menjamin suatu aspek keamanan pada sistem *e-voting*, yaitu dengan menggunakan algoritma Rijndael. Algoritma ini dipilih karena proses enkripsi dan dekripsi membutuhkan waktu yang singkat, kunci yang digunakan relatif pendek, dan dapat digunakan untuk mengamankan data hasil pemilu yang jumlahnya besar. Implementasi dari algoritma ini menggunakan bahasa Java.**

Keywords— ***e-voting, kriptografi, Rijndael, Java.***

## I. PENDAHULUAN

### Latar Belakang Masalah

Seiring dengan kemajuan teknologi, pelaksanaan demokrasi di dunia saat ini telah menuju ke arah demokrasi elektronik. Proses pemungutan suara dalam pemilu di negara-negara maju kini mulai sepenuhnya dilakukan oleh sistem elektronik (*e-voting*). *e-Voting* dapat membawa pemerintahan Indonesia ke arah yang sehat dan mengurangi segala bentuk kecurangan di dalam birokrasi. Pelaksanaan *e-voting* tidak dapat di pelopori oleh pemerintah saja, tetapi haruslah didukung sepenuhnya oleh rakyat Indonesia sendiri.

Saat ini telah banyak dikembangkan aplikasi *e-voting* baik di negara maju maupun di Indonesia sendiri. Namun, penerapan *e-voting* di Indonesia sendiri belum dapat dilaksanakan karena rakyat Indonesia belum siap menerima aplikasi *e-voting* tersebut. Masalah keamanan dan kerahasiaan data hasil pemilu merupakan salah satu aspek penting yang menyebabkan rakyat masih sulit mempercayai pelaksanaan *e-voting*. Pemungutan suara dengan komputerisasi hanya dapat dilakukan jika protokol menjamin bahwa privasi individu dapat dilindungi dan berbagai bentuk kecurangan dengan teknologi ini dapat dicegah. Untuk melaksanakan tujuan tersebut, maka dirancang suatu sistem keamanan yang berfungsi melindungi sistem informasi tersebut. Salah satu upaya pengamanan sistem informasi yang dapat dilakukan adalah kriptografi. Enkripsi dilakukan pada saat pengiriman dengan cara mengubah data asli menjadi data rahasia, sedangkan dekripsi dilakukan pada saat penerimaan dengan cara mengubah data rahasia menjadi data asli. Proses ini dapat menjamin data tersebut tetap rahasia selama pengiriman dan tetap utuh pada saat penerimaan di tujuan.

Salah satu algoritma yang banyak digunakan dalam bidang keamanan adalah algoritma Rijndael. Algoritma ini memiliki kinerja yang baik, dan merupakan algoritma kriptografi simetrik yang beroperasi dalam mode block cipher yang memproses blok data 128-bit dengan panjang kunci 128-bit (AES- 128), 192-bit (AES-192), atau 256-bit (AES-256). Algoritma ini juga tidak dipatenkan sehingga penggunaannya tidak perlu mengeluarkan biaya.

### Tujuan

Tujuan umum dilakukan Tugas Akhir ini adalah untuk memenuhi syarat kelulusan mata kuliah EL4096, sekaligus sebagai syarat kelulusan dari pendidikan program Strata 1 di Program Studi Teknik Elektro – Sekolah Teknik Elektro dan Informatika – Institut Teknologi Bandung. Adapun tujuan khusus yang hendak dicapai yaitu :

- ✓ memperdalam pengetahuan tentang dunia kriptografi dan teknik pengamanan data digital;
- ✓ merancang sistem enkripsi dan dekripsi untuk menjaga keamanan, kerahasian dan keaslian data hasil pemungutan suara pada sistem *e-voting*.

### Batasan Masalah

Pada penelitian ini akan dibahas implementasi algoritma Rijndael dalam pengamanan data hasil *e-voting*. Berikut adalah beberapa batasan masalah yang diambil.

- ➢ Algoritma kriptografi yang digunakan adalah algoritma simetri Rijndael dengan panjang kunci 128 bit.
- ➢ Penekanan pembahasan tugas akhir ini didasarkan pada penggunaan algoritmanya, bukan pada perangkat keras dimana perangkat lunak ditanam, maupun pada bahasa pemrograman yang digunakan. Pendalaman

pembelajaran algoritma kriptografi hanya terbatas pada algoritma Rijndael saja.
- Algoritma kriptosistem ini hanya dapat mengenkripsi dan mendekripsi data yang berupa teks atau tulisan, bukan suara maupun gambar.
- Implementasi penelitian ini menggunakan bahasa pemrograman Java.

## II. DASAR TEORI

### e-Voting

Sebuah sistem *e-voting* dapat didefinisikan sebagai sebuah sistem yang memanfaatkan perangkat elektronik dan mengolah informasi digital untuk membuat surat suara, memberikan suara, menghitung perolehan suara, menayangkan perolehan suara, serta memelihara dan menghasilkan jejak audit. Beberapa syarat keamanan yang telah disepakati bagi sebuah sistem *e-voting* adalah seperti berikut.

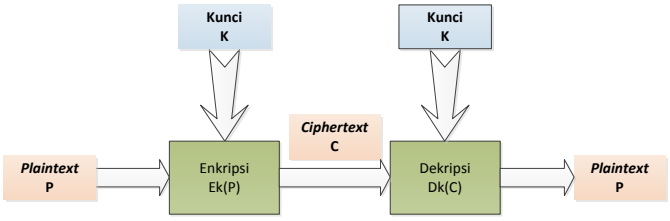
- ✓ Akurasi
- ✓ Demokrasi
- ✓ Rahasia
- ✓ Verifikasi
- ✓ Adil
- ✓ Ketersediaan
- ✓ Kehandalan
- ✓ Pertanggungjawaban
- ✓ Dapat diaudit
- ✓ Dapt dibuka
- ✓ Kejernihan

### Kriptografi

Kriptografi (*Cryptography*) merupakan bagian dari suatu cabang ilmu matematika yang disebut *Cryptology*. Kriptografi berasal dari bahasa Yunani, yang terdiri dari dua kata yaitu *cryptos* yang berarti rahasia, dan *graphein* berarti tulisan. Sehingga menurut bahasa, kriptografi berarti tulisan rahasia. Sedangkan definisi kriptografi adalah suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, integritas suatu data, serta otentifikasi data[2]. Ada empat hal yang menjadi tujuan dasar dari kriptografi, antara lain sebagai berikut.

- ✓ Kerahasiaan (confidentiality)
- ✓ Kerahasiaan (data integrity)
- ✓ Otentikasi (authentication)
- ✓ Nirpenyangkalan (non-repudiation)

Kriptografi secara umum terdiri dari dua proses, yaitu enkripsi dan dekripsi. Secara sederhana, dapat digambarkan sebagai berikut.




Gambar II.1 Proses enkripsi/dekripsi sederhana.

Enkripsi merupakan suatu proses untuk menyandikan pesan jelas (*plaintext)* menjadi pesan tersandikan (*ciphertext*). Sedangkan dekripsi adalah proses pengembalian dari *ciphertext* menjadi *plaintext* dengan tujuan agar pesan yang diterima dapat dimengerti.

### Kriptanalisis

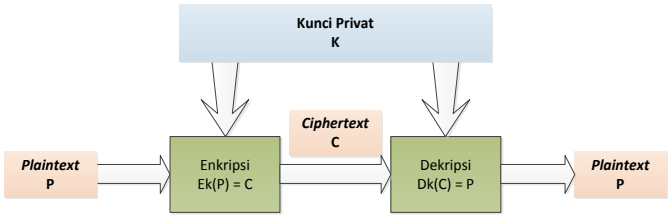
Kriptanalisis (*cryptanalysis*) adalah suatu ilmu dan seni yang dipelajari untuk memecahkan mekanisme kriptografi dengan cara mendapatkan *plaintext* atau kunci dari *ciphertext* yang digunakan untuk mendapatkan informasi berharga kemudian mengubah atau memalsukan pesan dengan tujuan untuk menipu penerima yang sesungguhnya. Pelakunya disebut kriptanalis. Seorang kriptografer mengubah *plaintext* menjadi *chipertext* dengan suatu algoritma dan kunci. Sedangkan seorang kriptanalis berusaha memecahkan chiperteks untuk menemukan *plaintext* atau kunci.

Berdasarkan ketersediaan data yang ada dan dengan asumsi kriptanalisis mengetahui algoritma kriptografi yang digunakan, serangan terhadap kriptografi dapat dikelompokkan menjadi beberapa macam seperti berikut.

1. ***Ciphertext-only attack***
2. ***Known-plaintext attack***
3. ***Chosen-plaintext attack***
4. ***Adaptive-chosen-plaintext attack***
5. ***Chosen-ciphertext attack***
6. ***Chosen-text attack***
7. ***Chosen-key attack***
8. ***Rubber-hose cryptanalysis***
9. ***Man-in-the middle attack***

### Algoritma Kriptografi Kunci Simetri

Algoritma kriptografi kunci simetri merupakan algoritma kriptografi klasik yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi.

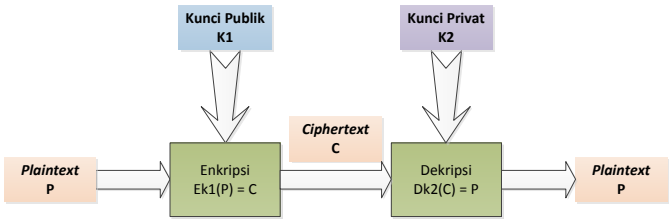



Gambar II.2 Skema kriptografi kunci simetri.

Contoh algoritma kriptografi kunci simetri adalah DES, Double DES, Triple DES, GOST, OTP, RC2, RC4, RC5, RC6, IDEA, Twofish, Magenta, FEAL, SAFER, LOKI, CAST, Rijndael (AES), Blowfish, dan lain-lain.

**Algoritma Kriptografi Kunci Asimetri**

Algoritma kriptografi kunci asimetri adalah algoritma yang menggunakan kunci yang berbeda untuk setiap proses enkripsi dan dekripsi. Kriptografi ini dinamakan pula kriptografi kunci publik (*public-key cryptography*) karena kunci untuk mengenkripsi boleh disebarluaskan kepada umum (*public key*) sedangkan kunci untuk mendekripsi hanya disimpan oleh orang yang bersangkutan secara pribadi (*private key*).




Gambar II.3 Skema kriptografi kunci publik.

Contoh algoritma kunci asimetri antara lain adalah RSA, ECC, LUC, EI-Gamal, DH, dan lain-lain.

***Advanced Encryption Standard***

Pada bulan Agustus 1998, Konferensi umum NIST memutuskan lima finalis dari 15 proposal yang masuk yang didasarkan pada aspek keamanan algoritma, efisiensi, fleksibilitas, dan kebutuhan memori. Finalis tersebut adalah : Rijndael, Serpent, Twofish, RC6, dan MARS. Setelah melalui berbagai pengujian dan pertimbangan, maka pada Oktober 2000, NIST memutuskan Rijndael yang keluar sebagai pemenangnya.

Dari segi keamanan, kecepatan eksekusi, kebutuhan flash memory dan RAM, Rijndael dapat menjadi pilihan yang paling baik dibandingkan algoritma kriptografi kunci simetri lainnya. Rijndael memiliki panjang kunci yang bervariasi yang cukup panjang tetapi menghasikan blok *ciphertext* yang tetap. Penerapan Rijndael pada sistem *e-voting* dapat menampung data hasil pemilu dalam jumlah yang besar. Oleh karena itu, maka dipilihlah algoritma Rijndael dalam penelitian Tugas Akhir ini.

## III. ANALISIS DAN DESAIN SISTEM

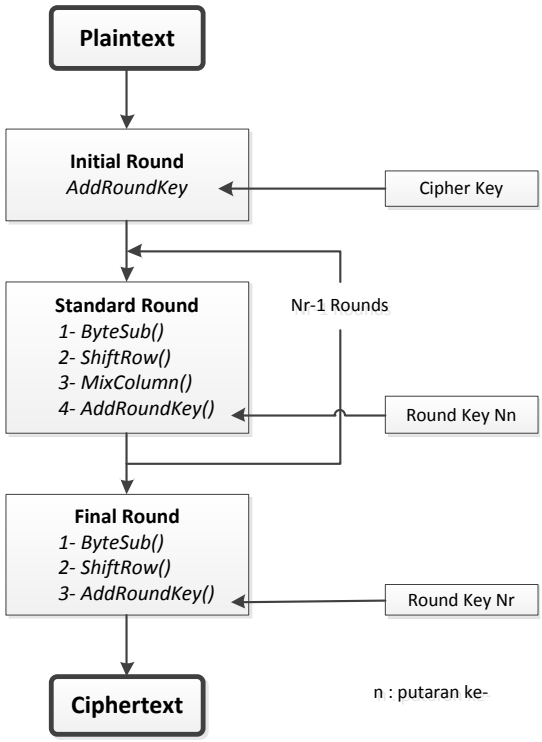
### III.1 Pengenalan Algoritma Kriptografi Rijndael

Algoritma Rijndael dinamakan juga algoritma AES, merupakan algoritma cipher blok yang menggunakan teknik substitusi, permutasi, dan sejumlah putaran pada tiap blok yang akan dienkripsi. Pada setiap putaran digunakan kunci yang berbeda yang disebut kunci ronde (*round key*). Ukuran blok dari algoritma Rijndael adalah 128 bit (16 byte). Rijndael mendukung panjang kunci bervariasi yaitu, 128, 192, dan 256 bit, sehingga dinamakan AES-128, AES-192, dan AES-256. Panjang kunci (Nk) dan panjang blok (Nb) dinyatakan dalam ukuran *word* (32 bit).

### III.2 Proses Enkripsi Algoritma Rijndael

Garis besar algoritma *Rijndael* yang beroperasi blok 128-bit dengan kunci 128-bit adalah sebagai berikut.

1. ***Initial Round***, pada tahap ini dilakukan operasi *AddRoundKey* : melakukan *XOR* antara *state* awal (*plaintext*) dengan *cipher key*.
2. ***Standard Round***, terjadi putaran sebanyak Nr – 1 kali. Proses yang dilakukan pada setiap putaran adalah :
   a. *ByteSub*: substitusi *byte* dengan menggunakan tabel substitusi (S-Box).
   b. *ShiftRow:* pergeseran baris-baris *array state* secara siklik.
   c. *MixColumn*: mengacak data di masing-masing kolom *array state*.
   d. *AddRoundKey:* melakukan *XOR* antara *state* sekarang dengan *round key*.
3. ***Final round***, merupakan proses untuk putaran terakhir. Pada tahap ini dilakukan operasi :
   a. *ByteSub*.
   b. *ShiftRow*.
   c. *AddRoundKey*.

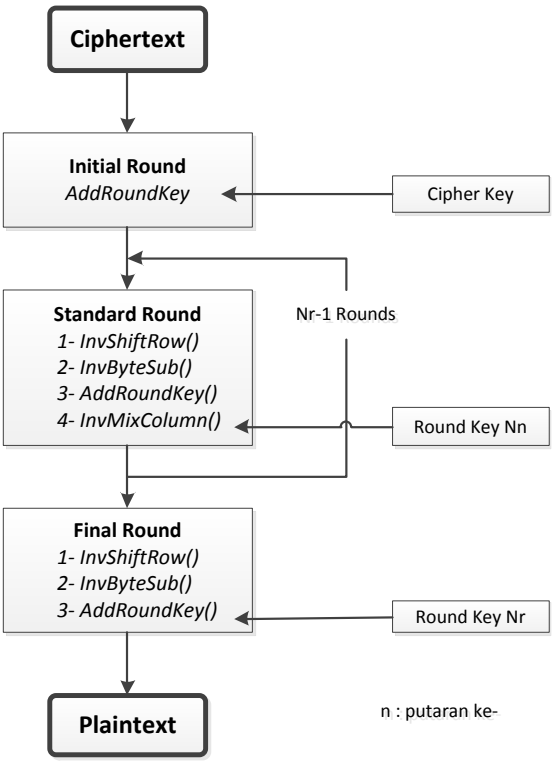



Gambar III.1 Skema proses enkripsi algoritma Rijndael.

### III.3 Proses Dekripsi Algoritma Rijndael

Urutan proses dekripsi AES tidak merupakan kebalikan dari enkripsi. Ada proses yang dipertukarkan urutannya, walaupun

penggunaan kuncinya sama. Jika urut-urutan proses pada enkripsi adalah *SubBytes(), Shift Rows() , MixColumns()* dan *AddRoundKey()* , maka urutan proses pada dekripsi adalah *InvShiftRows(), InvSubBytes(), InvAddRoundKey(),* dan *InvMixColumns().*




Gambar III.2 Skema proses dekripsi algoritma Rijndael.

### III.4 Batasan Sistem

Batasan dari sistem pada penelitian ini adalah sebagai berikut:

- hasil akhir dari perancangan sistem ini bukan sebuah produk aplikasi dengan tampilan GUI melainkan hanya proses yang dijalankan dalam Netbeans IDE;
- sistem ini menggunakan algoritma Rijndael pada proses enkripsi dan dekripsinya;
- Sistem hanya dapat memproses data dalam bentuk file teks, sehingga input data yang ingin dienkripsi harus disimpan dalam bentuk file berekstensi *.txt;
- bahasa pemograman yang digunakan untuk membuat aplikasi ini adalah Java.

Pada penelitian ini teknologi dan *tools* yang digunakan untuk perancangan sistem adalah sebagai berikut.

- ✓ Development Tool: Netbeans dan Eclipse.
- ✓ Library: Java 2.0 SDK

### III.5 Analisis Kebutuhan Sistem

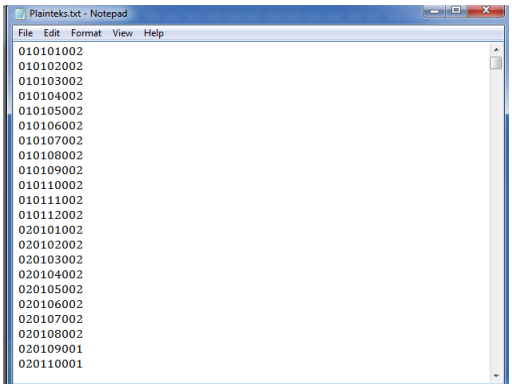
Persyaratan dasar yang mutlak harus ada untuk mencoba sistem ini adalah :

- ❖ 1 unit komputer dengan spesifikasi sebagai berikut :
  - prosesor min 1,6 GHz,
  - memori min 512 MB;
- ❖ telah terinstal Java 2.0 SDK, dan terdapat *development tools* seperti Netbeans atau Eclipse;
- ❖ data input hasil pemungutan suara yang telah disimpan dalam bentuk file *.txt.

## IV. IMPLEMENTASI DAN ANALISIS HASIL IMPLEMENTASI

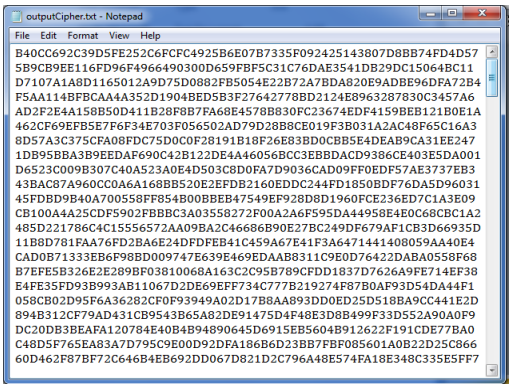
### Implementasi Pada Perangkat Komputer (PC)

Sistem akan membaca file input yang telah disediakan sebelumnya. Contoh file input Plainteks.txt dapat dilihat pada gambar berikut.



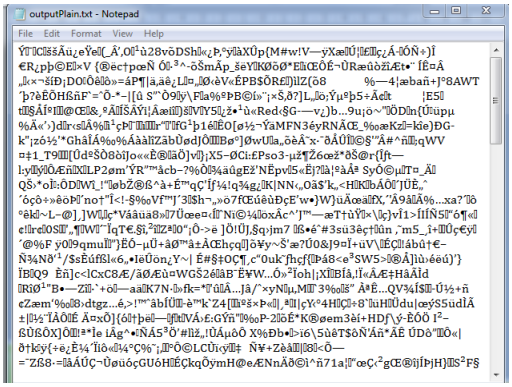

Gambar IV.1 Teks jelas pada file Plainteks.txt.

Selanjutnya sistem akan mengenkripsi file tersebut dengan kunci tertentu sehingga menghasilkan file Cipherteks.txt seperti pada gambar berikut.




Gambar IV.2 Hasil enkripsi menggunakan kriptografi Rijndael.

File tersebut berisi data yang telah terenkripsi dengan aman. Apabila kita ingin mendekripsikan file tersebut, maka harus digunakan kunci yang sama dengan kunci pada proses enkripsi. Ketika kita mencoba mendekripsikan file tersebut dengan kunci yang salah, maka akan dihasil kan file yang berisi data seperti pada gambar berikut.




Gambar IV.3 Hasil dekripsi menggunakan kunci yang salah.

File tersebut akan sulit dibaca sehingga data yang akan dikrimkan akan terjamin keamanannya.

## V. KESIMPULAN

Setelah melakukan proses perancangan, implementasi, pengujian, dan analisis dari program Enkripsi-Dekripsi maka penulis dapat menarik kesimpulan sebagai berikut.

- ✓ Algoritma Rijndael (AES) dapat digunakan untuk mengenkripsi data teks dengan proses yang cepat dan aman.
- ✓ Ukuran file *ciphertext* mengalami peningkatan antara 2-4 kali lipat dibanding ukuran file *plaintext*, dan hanya file *.txt saja yang dapat digunakan untuk mengirimkan data terenkripsi pada pengujian ini.
- ✓ Dengan penerapan yang tepat, proses kriptografi simetri Rijndael dapat digunakan pada sistem e-Voting mendatang.

## DAFTAR PUSTAKA


[1] Ariyus, Doni, *Kriptografi*, CV. Andi offset, Yogyakarta, 2006.

[2] Menezes, Oorcshot, and Vanstone, *Handbook of Applied Cryptography*, CRC Press, Florida, 1996.

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

[4] Paar, Christof, and Pelzl, Jan, *Understanding Cryptography*, Springer-Verlag, Heidelberg, 2010.

[5] Schneier, Bruce, *Applied Cryptography: Protocol, Algorithms, and Source Code in C*, John Wiley and Sons, Inc., Second Edition, 1996.

[6] Schneier, Bruce, et. al., A performane Comparison of the five AES Finalist. 1998.
http://www.schneier.com/paper-aes-comparison-twofish.pdf/
Diakses tanggal 20 Maret 2012 pukul 14:13 WIB.

[7] Daemen, Joan & Rijmen, Vincent, *AES Proposal : Rijndael*, 1999.
http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf/
Diakses tanggal 16 Maret 2012 pukul 13:24

[8] Federal Information Processing Standards Publication 197, *Announcing the ADVANCED ENCRYPTION STANDARD (AES)*, 2001.

[9] Fahmi, Husni, dan Handoko, Dwi, Kajian Teknis tentang Pemungutan Suara secara Elektronik (Electronic Voting), 2010.
http://www.husnifahmi.com/papers/Pemungutan_Suara_secara_Elektronik_e-voting_11_Mei_2010.pdf/
Diakses tanggal 14 Februari 2012 pukul 20.34.

[10] Fahmi, Husni, dan Faidah, Haret, Aplikasi Kriptografi Modern Untuk Pengiriman Data Teramankan, 2010.
http://www.husnifahmi.com/papers/Aplikasi_Kriptografi_Modern.pdf/
Diakses Pada tanggal 14 Februari 2012 pukul 23:30.