LAPORAN PENELITIAN DOSEN MUDA SATEKS
UNIVERSITAS SRIWIJAYA

PENERAPAN ENKRIPSI DAN DEKRIPSI FILE MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES)

Oleh:
Rifkie Primartha, ST., MT.

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
NOVEMBER 2012

Halaman Pengesahan

1.	Judul Penelitian	:	Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Advanced Encryption Standard (AES).
2.	Bidang Penelitian	:	Rekayasa.
3.	Ketua Peneliti		
	a. Nama Lengkap	:	Rifkie Primartha, ST., MT.
	b. Jenis Kelamin	:	Laki-laki.
	c. NIP	:	197706012009121004.
	d. Pangkat dan Golongan	:	- /III.b
	e. Pendidikan Terakhir	:	S2 Magister Teknologi Informasi.
	f. Jabatan Struktural	:	-
	g. Jabatan Fungsional	:	-
	h. Perguruan Tinggi	:	Universitas Sriwijaya.
	I. Fakultas/Jurusan	:	Ilmu Komputer/Teknik Informatika
	j. Alamat Kantor	:	Kampus Unsri Jl. Raya Palembang-Prabumulih KM. 32 Inderalaya, Ogan Ilir, Sumatera Selatan 30662.
	k. Telpon/Faks	:	0711-580169 / 0711-580644.
	l. Alamat Rumah	:	Jl. Rejung Lr. Setia Jaya No. 207 RT. 003 RW. 001 Kel. Sako Baru, Sako, Palembang.
	Mobile Phone/E-mail	:	0852.672.44996 / rifkie@unsri.ac.id
4.	Jumlah Anggota Peneliti	:	-
	a. Nama Anggota	:	-
5.	Jangka Waktu Penelitian	:	1 tahun
6.	Jumlah yang diajukan	:	Rp 7.500.000,-

Inderalaya, 6 November 2012

Mengetahui,
Dekan Fakultas Ilmu Komputer,

Ketua Peneliti,

Dr. Darmawijoyo, M.Si, M.Sc
NIP. 19650828 199103 1 003

Rifkie Primartha, ST. MT.
NIP. 197706012009121004

Menyetujui,
Ketua Lembaga Penelitian,

Prof. Dr. Ir. H. M. Said, Msc
NIP. 19610812198703 1 003

RINGKASAN

Kriptografi adalah bidang ilmu untuk menjaga keamanan pesan (*message*). Kriptografi telah banyak diimplementasikan di banyak hal. Smart card, Anjungan Tunai Mandiri (ATM), Pay TV, *Mobile Phone*, dan Komputer adalah beberapa contoh produk teknologi yang menggunakan kriptografi untuk keamanannya. Cara kerjanya adalah dengan mengubah pesan asli yang dapat dimengerti/dibaca manusia (*plainteks*) ke bentuk lain yang tidak dapat dimengerti/dibaca oleh manusia (*cipherteks*). Proses transformasi *plainteks* menjadi *chiperteks* diistilahkan dengan *enkripsi*. Sedang proses pengembalian pesan *chiperteks* menjadi *plainteks* diistilahkan dengan *dekripsi*. Ada banyak algoritma kriptografi, dalam penelitian ini aplikasi kriptografi yang dikembangkan menggunakan algoritma simetri AES (*Advanced Encryption Standard*) dengan Bahasa Pemrograman Java. AES menggunakan sandi blok kunci simetrik dengan ukuran kunci bervariasi, yaitu 128 bit, 192 bit, dan 256 bit.

Kata Kunci: *Advanced Encryption Standard*, Plainteks, Chiperteks, Kriptografi, Enkripsi, Dekripsi.

BAB I PENDAHULUAN

Zaman telah berubah, dulu nenek moyang kita menggunakan jasa seorang kurir atau seekor burung merpati untuk menghantarkan informasi pesan (surat) kepada orang lain ditempat yang jauh. Sekarang, semua itu mungkin sudah ditinggalkan. Beberapa tahun yang lalu kita masih berdesak-desakkan di kantor pos ketika kita mau mengirimkan surat. Sekarang kantor pos sudah tidak lagi seramai dulu. Zaman telah merubah segalanya. Dengan teknologi modern membuat waktu pengiriman informasi/pesan yang begitu lama menjadi singkat hanya dalam hitungan detik. Tempat yang jauh pun sudah bukan lagi kendala. Internet sebagai media teknologi sudah menjadi keharusan bagi setiap orang untuk membaca informasi berita, informasi iklan, informasi pesan, dan lain-lain. Akan tetapi, internet tetaplah memiliki sisi kekurangan terutama dalam hal keamanan data/informasi (pesan). Informasi yang akan kita kirim sangat rawan disadap, bahkan dipalsukan.

Keamanan informasi merupakan sesuatu yang harus diperhatikan secara serius. Salah satu bidang ilmu untuk menjaga keamanan informasi adalah kriptografi. Dengan kriptografi, informasi yang dianggap rahasia dapat disembunyikan dengan teknik penyandian, sehingga tidak dimengerti oleh orang lain, selain oleh pembuat dan penerimanya saja.

Konsep kriptografi untuk menjaga kerahasiaan data (pesan) adalah dengan cara menyamarkannya menjadi bentuk tersandi yang tidak dapat dibaca. Pesan yang akan disandikan disebut *plainteks*, sedangkan yang telah disamarkan disebut *chiperteks*. Proses penyamaran dari *plainteks* ke *chiperteks* disebut *enkripsi*, sedang proses pengembalian chiperteks menjadi *plainteks* disebut *dekripsi* [2].

Banyak sekali jenis algoritma kriptografi, diantaranya adalah algoritma *Advanced Encryption Standard* (AES). Algoritma ini termasuk jenis simetri yang disebut juga sebagai algoritma konvensional, yaitu algoritma yang menggunakan kunci *enkripsi* dan kunci *dekripsi* yang sama. AES menggunakan sandi blok kunci simetrik dengan ukuran kunci bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. Pemerintah Amerika Serikat telah mengadopsi AES sebagai standar *enkripsi*. Standar ini terdiri dari 3 blok *cipher*, yaitu AES-128, AES-192, dan AES-256 yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai Rijndael. AES telah dianalisis secara luas dan sekarang digunakan di seluruh dunia, seperti halnya dengan pendahulunya, *Data Encryption Standard* (DES).

Sebagai tindak lanjut dari penelitian sebelumnya, yaitu tentang pemanfaatan kriptografi algoritma DES (*Data Encryption Standard)* menggunakan bahasa pemrograman Java. Bahasa Pemrograman Java diciptakan akhir abad 20, di bawah Sun Microsystem pada

tahun 1995-an. Bahasa pemrograman Java adalah bahasa modern yang telah diterima oleh masyarakat komputasi. Hampir semua perusahaan pengembang *software* bersatu mendukung dan mengembangkan sistem berbasis Java. Bahasa Java tidak mensyaratkan *platform* tertentu. Aplikasi yang dikembangkan dengan Java dapat berjalan di *platform* manapun yang sangat beragam. Bahasa Java dirancang untuk mendukung paradigma pemrograman berorientasi objek. Bahasa ini juga dapat membuat beragam aplikasi komputer mulai dari *hand-held devices* seperti *mobile phone* menggunakan J2ME, aplikasi standar dengan J2SE, serta aplikasi *back-end enterprise* dengan J2EE[1].

Pada penelitian ini, akan memadukan algoritma kriptografi AES dan kehandalan bahasa pemrograman Java untuk membuat suatu aplikasi perangkat lunak yang dapat melakukan fungsi kriptografi.

BAB II TINJAUAN PUSTAKA

II.1 Deskripsi Algoritma *Advanced Encryption Standard* (AES)

Jenis algoritma kriptografi AES (atau Rijndael) ini bersifat simetri dan cipher blok. Dengan demikian algoritma ini mempergunakan kunci yang sama saat *enkripsi* dan *dekripsi*, serta masukkan dan keluaran berupa blok dengan urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128 bit tersebut disebut sebagai blok data atau *plainteks* yang nantinya akan di-*enkripsi* menjadi *chiperteks*. *Cipher key* dari AES terdiri dari *key* dengan panjang 128 bit, 192 bit, atau 256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah *round* (putaran) yang akan diimplementasikan pada algoritma AES ini [4]. Ada 10, 12, atau 14 putaran dalam AES yang sesuai dengan ukuran kunci yang digunakan. Setiap putaran mengandung:

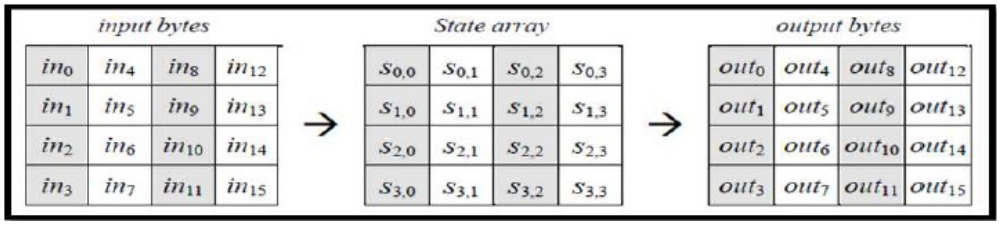
- Penggantian *Byte* yang sama dengan DES.
- Peralihan = pertukaran baris.
- Campur Jalur = peralihan kiri dan XOR bit-bit.
- Penambahan sub-kunci = XOR bagian kunci dengan keputusan kitaran.

Berikut ini adalah Tabel 1 yang memperlihatkan jumlah round/putaran (Nr) yang harus diimplementasikan pada masing-masing panjang kunci.

Tabel 1.
Perbandingan Jumlah Round dan Key [9]

	Jumlah Key (Nk)	Ukuran Blok (Nb)	Jumlah Putaran (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

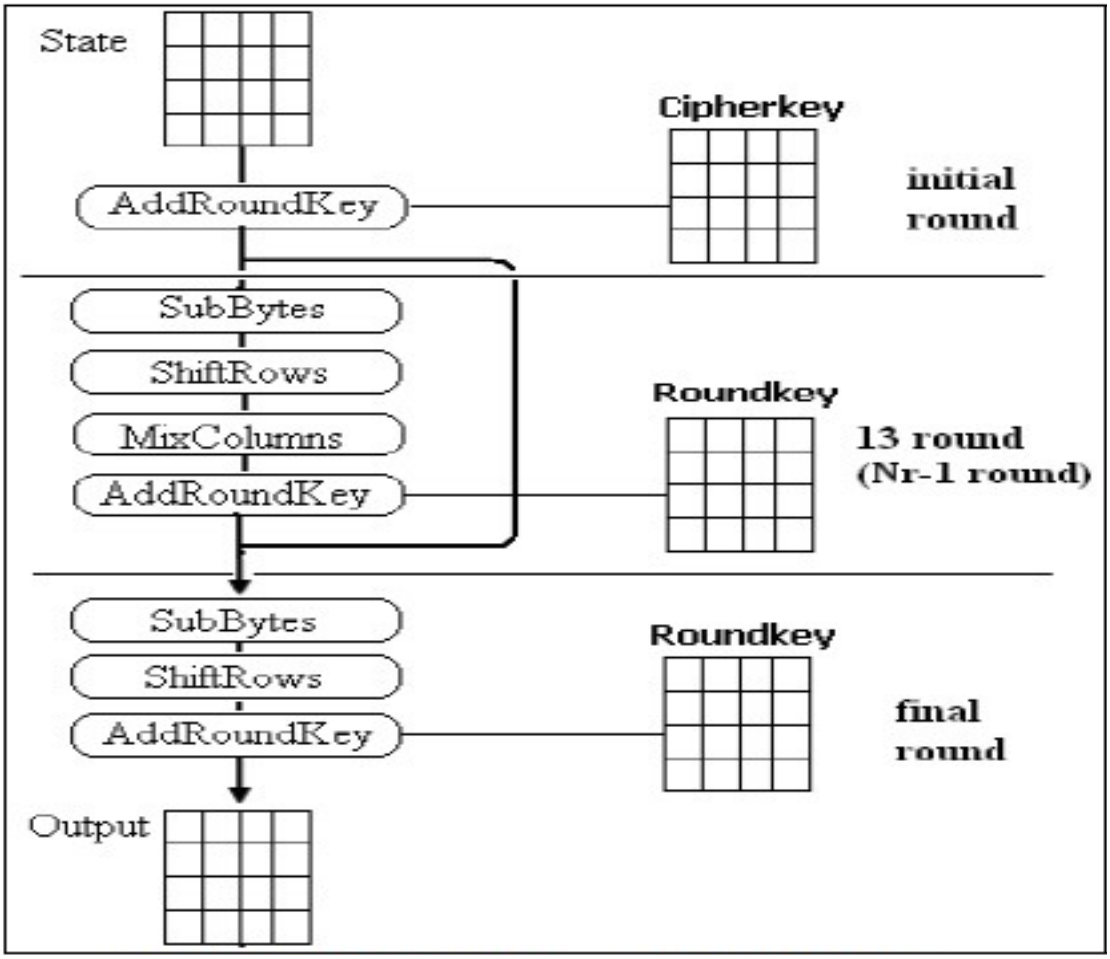
Pada dasarnya, operasi AES dilakukan terhadap *array of byte* dua dimensi yang disebut dengan *state*. *State* mempunyai ukuran NROWS X NCOLS. Pada awal enkripsi, data masukkan yang berupa in0, in2, in3, s.d in15 disalin ke dalam *array state*. *State* inilah yang nantinya dilakukan operasi enkripsi/dekripsi. Kemudian keluarannya akan ditampung ke dalam *array out*. Gambar 1 mengilustrasikan proses penyalinan dari *input bytes*, *state array*, dan *output bytes* [4].



Gambar 1. Proses *Input Bytes*, *State Array*, dan *Output Byte*

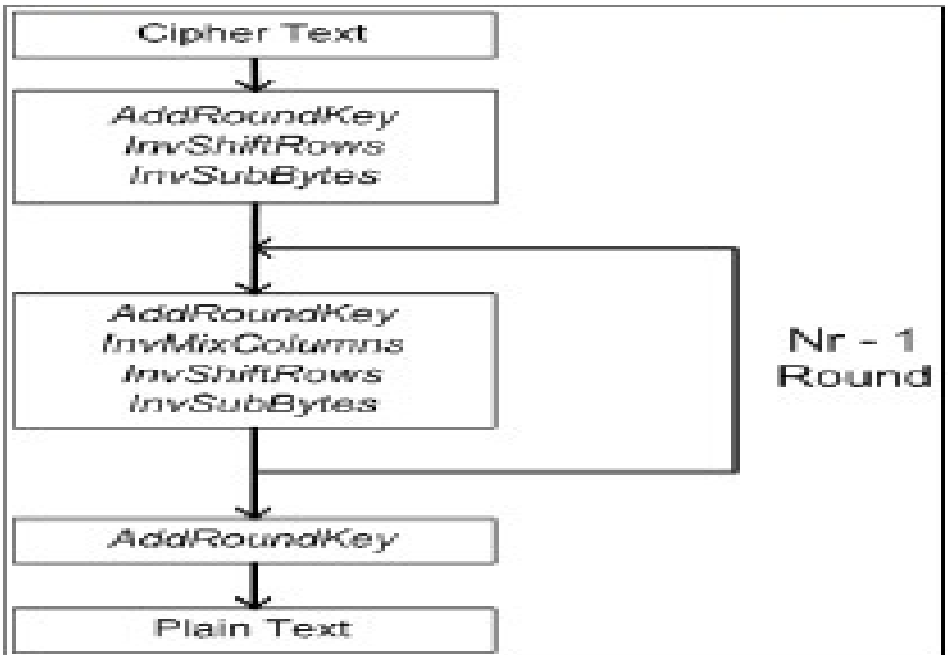
II.2 Proses Enkripsi AES

Proses enkripsi AES terdiri dari 4 jenis transformasi *bytes*, yaitu *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. Pada awal proses enkripsi, *input* yang telah di-*copy*-kan ke dalam *state* akan mengalami transformasi *byte AddRoundKey*. Setelah itu, *state* akan mengalami transformasi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* secara berulang-ulang sebanyak Nr. Proses ini di dalam algoritma AES disebut sebagai *round function*. *Round* yang terakhir berbeda dengan round sebelumnya dimana *round* terakhir, *state* tidak mengalami transformasi *MixColumns*. Ilustrasi proses enkripsi AES dapat digambarkan seperti pada gambar 2 di bawah ini [4].



Gambar 2. Ilustrasi Proses Enkripsi AES [5]

II.3 Proses Dekripsi AES



Gambar 3. Ilustrasi Proses Enkripsi AES [5]

II.4 Transformasi Penambahan Kunci

Algoritma AES mengambil kunci cipher dan melakukan rutin ekspansi kunci (kunci expansion) untuk membentuk *key schedule*. Ekspansi kunci menghasilkan total Nb (Nr+1) *word*. Algoritma ini membutuhkan set awal *key* yang terdiri dari Nb *word*, dan setiap *round* Nr membutuhkan data kunci sebanyak Nb *word*. Hasil *key schedule* terdiri dari *array* 4 *byte word linear* yang dinotasikan dengan (Wi). *SubWord* adalah fungsi yang mengambil 4 *byte word input* dan mengaplikasikan S-Box ke tiap-tiap data 4 *byte* untuk menghasilkan *word output*. Fungsi RotWord mengambil *word* [a0, a1, a2, a3] sebagai *input*, melakukan permutasi siklik, dan mengembalikan *word* [a1, a2, a3, a0]. Rcon[i] terdiri dar nilai-nilai yang diberikan oleh [xi-1, {00}, {00}, {00}], dengan xi-1 sebagai pangkat dari x (x dinotasikan sebagai {02}). *Psudocode* dari proses ekspansi kunci dapat dilihat dari gambar berikut[6].

```
KeyExpansion(byte key[4*Nk], word w[Nb*(Nr+1)], Nk)
begin
   word  temp

   i = 0

   while (i < Nk)
      w[i] = word(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])
      i = i+1
   end while

   i = Nk

   while (i < Nb * (Nr+1)]
      temp = w[i-1]
      if (i mod Nk = 0)
         temp = SubWord(RotWord(temp)) xor Rcon[i/Nk]
      else if (Nk > 6 and i mod Nk = 4)
         temp = SubWord(temp)
      end if
      w[i] = w[i-Nk] xor temp
      i = i + 1
   end while
end
```

Gambar 4. *Psudocode* Ekspansi Kunci [6]

BAB III TUJUAN DAN MANFAAT

Tujuan dari penelitian ini adalah sebagai berikut:

1. Menganalisa algoritma AES dalam melakukan enkripsi dan dekripsi terhadap suatu file dan atau teks.
2. Membuat perangkat lunak berbasis bahasa pemrograman Java yang dapat melakukan enkripsi dan dekripsi suatu file atau teks menggunakan teknik algoritma AES. Sehingga file dan atau teks tersebut tidak akan bisa dibaca kecuali oleh orang yang memiliki perangkat lunak dan kunci yang digunakan untuk mengenkripsinya.
3. Membuktikan algoritma AES dalam mengamankan pesan (informasi) rahasia.

Adapun manfaat dari penelitian ini adalah sebagai berikut:

1. Menghasilkan perangkat lunak yang dapat mengamankan file dan atau teks dengan menggunakan algoritma AES.
2. Dapat memahami algoritma AES dalam melakukan proses enkripsi dan dekripsi file dan teks.

BAB IV METODOLOGI PENELITIAN

Langkah-langkah dalam penelitian ini meliputi pengembangan perangkat lunak yang dijelaskan sebagai berikut yaitu:

1. **Sumber Data**

   Jenis data adalah data sekunder yang diambil dari hasil observasi literatur-literatur di internet.

2. **Studi literatur**

   Pada tahapan ini, akan dilakukan pencarian serta pembelajaran dari berbagai macam literatur dan dokumen lainnya. Selanjutnya hal-hal yang berkaitan dengan algoritma AES dan paket-paket java yang relevan yang akan diimplementasikan dalam rekayasa pengembangan perangkat lunak kriptografi tersebut.

3. **Perancangan**

   Perancangan yang dimaksud adalah merancang antar muka dari perangkat lunak kriptografi yang akan dikembangkan. Antar muka terdiri dari dua macam, yaitu pertama antar muka sebagai masukkan data file dan atau teks. Kedua rancangan antar muka keluaran sebagai hasil dari pemrosesan data masukkan.

4. **Pengembangan**

   Pengembangan perangkat lunak menggunakan metode *Rational Unified Process* (RUP) yang menerapkan konsep *object-oriented.*

5. **Eksperimen (skenario percobaan)**

   Agar pengujian berkualitas, maka perlu didesain skenario percobaan yang bervariasi agar didapat hasil yang sesuai dengan yang diharapkan. Eksperimen akan dilakukan dengan beberapa kali percobaan.

6. **Pengujian dan Evaluasi (pengolahan data, perbandingan)**

   Setelah dilakukan pengujian beberapa kali, selanjutnya data hasil pengujian dievaluasi pada tahapan selanjutnya.

7. **Analisa**

   Analisa dilakukan untuk mendapatkan suatu kesimpulan dari algoritma AES dalam melakukan enkripsi dan dekripsi. Apabila berhasil, maka perangkat lunak yang dibangun dianggap berhasil dengan baik. Dan apabila ternyata hasilnya jauh berbeda, maka akan dijadikan sebagai temuan untuk dijadikan bahan bagi penelitian-penelitian yang selanjutnya.

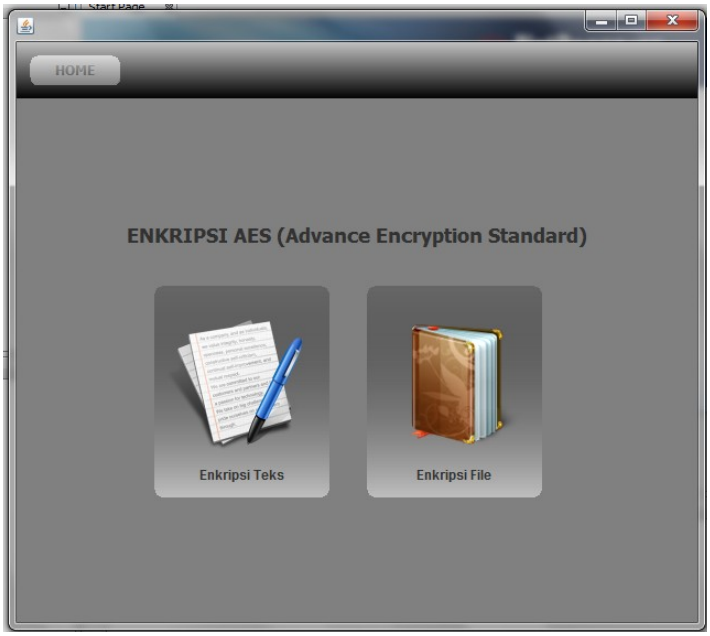
8. Kesimpulan

Hasil dari penelitian ini akan ditarik suatu kesimpulan tentang bagaimana kehandalan dari algoritma AES dalam melakukan enkripsi dan dekripsi file dan teks.

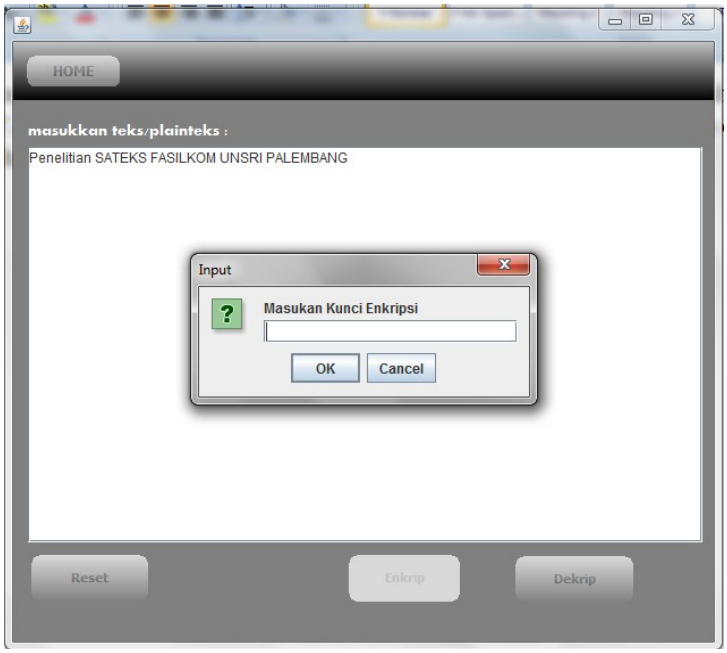
BAB V HASIL PENELITIAN

V.1 Desain Antar Muka Perangkat Lunak

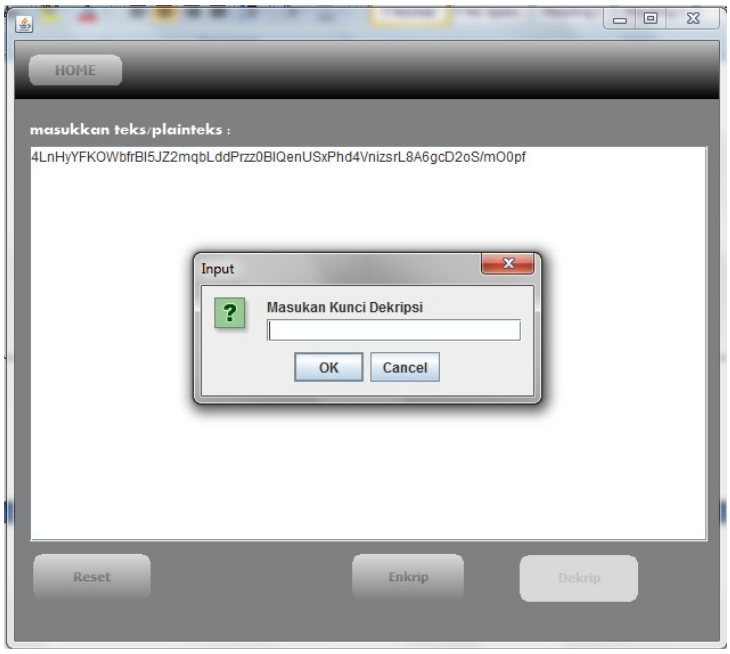
Gambar implementasi antar muka perangkat lunak yang telah dibangun dapat dilihat pada gambar V.1, antar muka enkripsi dapat dilihat pada gambar V.2, dan antar muka dekripsi dapat dilihat pada gambar V.3.



Gambar V.1 Antar Muka Menu Utama



Gambar V.2 Antar Muka Enkripsi Teks



Gambar V.3 Antar Muka Dekripsi Teks

V.2 Pengujian Perangkat Lunak

Pengujian dilakukan dengan menggunakan metode BlackBox Testing, yaitu pengujian yang memfokuskan pada keperluan fungsional dari perangkat lunak.

V.2.1 Pengujian Proses Enkripsi File dan atau Teks

Tahapan	Deskripsi	Prosedur Pengujian	Masukkan	Keluaran Yang Diharapkan	Kriteria Evaluasi Akhir	Hasil Yang Didapat	Kesimpulan
1	Menampilkan open dialog untuk memilih file atau teks yang akan dienkripsi	Menekan tombol “open”	-	Akan ditampilkan sebuah open dialog untuk file atau teks	Tampil sebuah open dialog	Sebuah open dialog	Diterima
2	Melakukan enkripsi file/teks yang dipilih	Menekan tombol enkripsi	Plainteks File/teks	Akan menampilkan file/teks terenkripsi	Tampil sebuah file/teks terenkripsi	Sebuah file/teks yang telah terenkripsi	Diterima

V.2.2 Pengujian Proses Enkripsi File dan atau Teks

Tahapan	Deskripsi	Prosedur Pengujian	Masukkan	Keluaran Yang Diharapkan	Kriteria Evaluasi Akhir	Hasil Yang Didapat	Kesimpulan
1	Menampilkan open dialog untuk memilih file atau teks yang akan didekripsi	Menekan tombol “open”	-	Akan ditampilkan sebuah open dialog untuk chiper file/teks	Tampil sebuah open dialog	Sebuah open dialog chiper file/teks	Diterima
2	Melakukan proses dekripsi file/teks yang dipilih	Menekan tombol dekripsi	Chiper File/teks	Akan menghasilkan plain file/teks	Tampil sebuah plain file/teks	Sebuah file/teks yang telah didekripsi	Diterima

V.3 Hasil Pengujian Perangkat Lunak

Perangkat lunak yang dihasilkan pada penelitian ini merupakan suatu aplikasi yang dapat melakukan enkripsi dan dekripsi file dan atau teks dengan menggunakan algoritma AES.

BAB VI KESIMPULAN DAN SARAN

VI. 1 Kesimpulan

Dari penelitian ini didapatkanlah beberapa kesimpulan, antara lain:

- Dengan adanya aplikasi kriptografi yang dikembangkan berdasarkan algoritma AES, maka data-data penting berupa file dan atau teks dapat diamankan (dienkripsi).
- Proses enkripsi dan dekripsi file maupun teks, pada prinsipnya memiliki mekanisme proses yang sama.
- Waktu yang dibutuhkan untuk melakukan enkripsi maupun dekripsi file dan atau teks sederhana adalah relatif sama.

VI.2 Saran

Penelitian yang telah dilakukan baru membuat suatu aplikasi kriptografi AES menggunakan bahasa pemrograman Java. Perlu juga dilakukan penelitian yang sama menggunakan bahasa pemrograman yang berbeda. Bahasa C, C++, C# atau Pascal dirasa perlu untuk dicoba mengingat masing-masing bahasa pemrograman memiliki karakteristik serta kelebihannya masing-masing.

Antar muka aplikasi ini masih sangat standar, diharapkan pada penelitian selanjutnya dapat dibuat antar muka aplikasi yang lebih menarik dibanding yang sekarang.

DAFTAR PUSTAKA

[1] Bambang Hariyanto, Esensi-esensi Bahasa Pemrograman Java, Edisi 2, Bandung, Penerbit Informatika.

[2] Rinaldi Munir, 2006, Matematika Diskrit, Bandung, Prodi Teknik Informatika ITB.

[3] Didi Surian, 2006, Algoritma Kriptografi AES Rijndael, Jurnal Teknik Elektro, TESLA Vol. 8 No. 2, 97-101.

[4] Voni Y, Gani I, Antonius R, April 2009, Enkripsi dan Dekripsi dengan Algoritma AES 256 Untuk Semua Jenis File, Jurnal Informatika, Vol. 5 No. 1.

[5] Rinaldi Munir, 2006, Kriptografi, Bandung, Penerbit Informatika.

[6] Ariyus Dony, 2006, Kriptografi (Keamanan Data dan Komunikasi).

[7] Nagesh Kumar, Jawahar Thakur, Arvind Kalia, 2011, Performance Analysis of Symmetric Key Cryptography Algorithms: DES, AES and Blowfish, Journal Anu Books.

[8] Hamdan O Alanazi, B.B Zaidan, Hamid A Jalab, M. Shabbir, dan Al-Nabhani, 2010, New Comparative Study Between DES, 3DES, and AES within Nine Factors, Journal of Computing, Vol. 2, Issue 3, ISSN 2151-9617

[9] Atul M. Borkar, R.V. Kshirsagar, M.V. Vyawahare, 2010, Design of AES Algorithm using FPGA, UACEE International Journal of Advances in Electronics Engineering.

[10] Batbold Toiruul, Kyung Oh Lee, 2006, An Advanced Mutual-Authentication Algorithm Using AES for RFID Systems, IJCSNS International Journal of Computer Science and Network Security, Vol. 6 No. 9B.

[11] N. Penchalaiah, R. Seshadri, 2010, Affective Comparison and Evaluation of DES and Rijndael Algorithm (AES), IJCSE International Journal on Computer Science and Engineering Vol. 02, No.05, 1641-1645

LAMPIRAN

Biodata Ketua Peneliti

a.	Nama Lengkap	:	Rifkie Primartha, ST., MT.
b.	Jenis Kelamin	:	Laki-laki
c.	Pangkat/Golongan	:	1. / IIIb
d.	NIP	:	19770601 200912 1 004
e.	Jabatan Fungsional	:	-
f.	Jabatan Struktural	:	-
g.	Fakultas/Jurusan	:	Ilmu Komputer / Teknik Informatika
h.	Perguruan Tinggi	:	Universitas Sriwijaya
i.	Bidang Keahlian	:	Rekayasa (Keamanan Komputer)
j.	Alamat Rumah	:	Jl. Rejung Lr. Setia Jaya No. 207 RT. 003 RW. 001 Kel. Sako Baru, Sako, Palembang.
k.	No. Ponsel	:	0852.672.44996
l.	E-mail	:	rifkie@unsri.ac.id

Riwayat Pendidikan

Perguruan Tinggi	Gelar	Tahun Selesai	Bidang Studi
Universitas Sriwijaya	ST	2002	Teknik Elektro
Universitas Gadjah Mada	MT	2007	Teknologi Informasi

Publikasi

1. **Rifkie Primartha**, Sukemi, “Manajemen Migrasi Untuk Implementasi Linux”, Proceeding Konferensi Nasional Teknologi Informasi dan Aplikasinya, (KNTIA09), Palembang, Unsri, 2009

Penelitian

1. **Rifkie Primartha**, “Penerapan Enkripsi dan Dekripsi *File* Menggunakan *Algoritma Data Encryption Standard* (DES)”, Hibah Penelitian Fakultas Ilmu Komputer, Universitas Sriwijaya, 2011

Inderalaya, 6 November 2012

Peneliti,

Rifkie Primartha, ST., MT.

NIP. 197706012009121004