IMPLEMENTASI KRIPTOGRAFI PADA FILE DOKUMEN *MENGGUNAKAN ALGORITMA AES-128*

Veronica Lusiana

Abstract

Penyadapan terhadap pesan atau informasi merupakan hal yang sangat merugikan bagi pengguna jaringan komunikasi saat ini. Dengan adanya kemungkinan penyadapan informasi tersebut, maka aspek keamanan dalam pertukaran informasi menjadi penting. Pada saat ini, pertukaran data atau informasi sangat sering dilakukan sehingga aspek keamanan terhadap isi dokumen perlu untuk mendapat perhatian khusus. Penelitian ini akan mengimplementasikan kriptografi algoritma AES-128 untuk menyandikan file digital, khususnya adalah file dokumen PDF, DOC, dan TXT.

Algoritma AES (Advanced Encryption Standard) dipilih karena memiliki tingkat keamanan yang tinggi, dengan tiga pilihan tipe kunci yaitu AES-128, AES-192 dan AES-256. Penelitian ini secara khusus akan mengamati kebutuhan waktu untuk proses enkripsi dan dekripsi, dan ukuran file yang dihasilkan dari proses tersebut.

Keywords - Kriptografi, AES-128, Enkripsi, Dekripsi

1. PENDAHULUAN

Kriptografi memberikan beberapa layanan yang mendukung untuk meningkatkan keamanan pesan atau informasi antara lain: otentikasi (*authentication*), nirpenyangkalan (*non-repudiation*), dan kerahasiaan (*confidentiality*). Otentikasi merupakan layanan yang berhubungan dengan identifikasi kebenaran sumber informasi. Nirpenyangkalan merupakan layanan untuk mencegah penyangkalan dari pelaku yang telah mengirimkan informasinya. Sedangkan kerahasiaan adalah layanan yang ditujukan untuk menjaga agar informasi tidak dapat dibaca atau dipahami oleh pihak yang tidak berhak. Kerahasiaan informasi dapat diperoleh melalui proses enkripsi dan dekripsi.

Proses enkripsi yaitu mengubah pesan asli (*plaintext*) menjadi pesan dalam bentuk tersandi (*ciphertext*). Proses enkripsi akan menghasilkan data tersandi dan hanya dapat dibuka atau dibaca oleh pihak penerima yang memilki kunci (*key*) sedangkan proses dekripsi adalah mengembalikan data tersandi menjadi bentuk data asli.

Proses enkripsi dan dekripsi yang dilakukan dengan menggunakan kunci yang sama dikenal dengan istilah kriptografi algoritma kunci simetri. Pada algoritma jenis ini, kunci bersifat rahasia dan hanya boleh diketahui oleh pihak pengirim dan penerima saja. Selain kriptografi algoritma kunci simetri telah dikembangkan juga kriptografi algoritma kunci asimetri, yaitu proses enkripsi dan dekripsi yang dilakukan dengan menggunakan kunci yang berbeda. Terdapat sepasang kunci yaitu kunci publik (*public key*) yang digunakan untuk proses enkripsi dan kunci privat (*privat key*) yang digunakan untuk proses dekripsi. Kunci publik tidak bersifat rahasia dan harus diketahui oleh pengirim pada saat akan mengenkripsi data. Sebaliknya untuk kunci privat adalah bersifat rahasia dan hanya diketahui oleh penerima data.

Penelitian ini adalah membuat implementasi perangkat lunak menggunakan Matlab 7.0.4, program ini dapat digunakan untuk meningkatkan keamanan informasi menggunakan kriptografi algoritma kunci simetri AES(*Advanced Encryption Standard*)-128. Informasi menjadi lebih aman setelah diubah ke dalam bentuk data tersandi, karena informasi hanya dapat dibaca oleh pihak yang berhak.

2. METODE PENELITIAN

2.1. Algoritma AES

Algoritma AES merupakan algoritma simetris yaitu mengunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci yaitu tipe: AES-128, AES-192 dan AES-256. Masing-masing tipe menggunakan kunci internal yang berbeda yaitu *round key* untuk setiap proses putaran. Proses putaran enkripsi AES-128 dikerjakan sebanyak 10 kali (a=10), yaitu sebagai berikut:

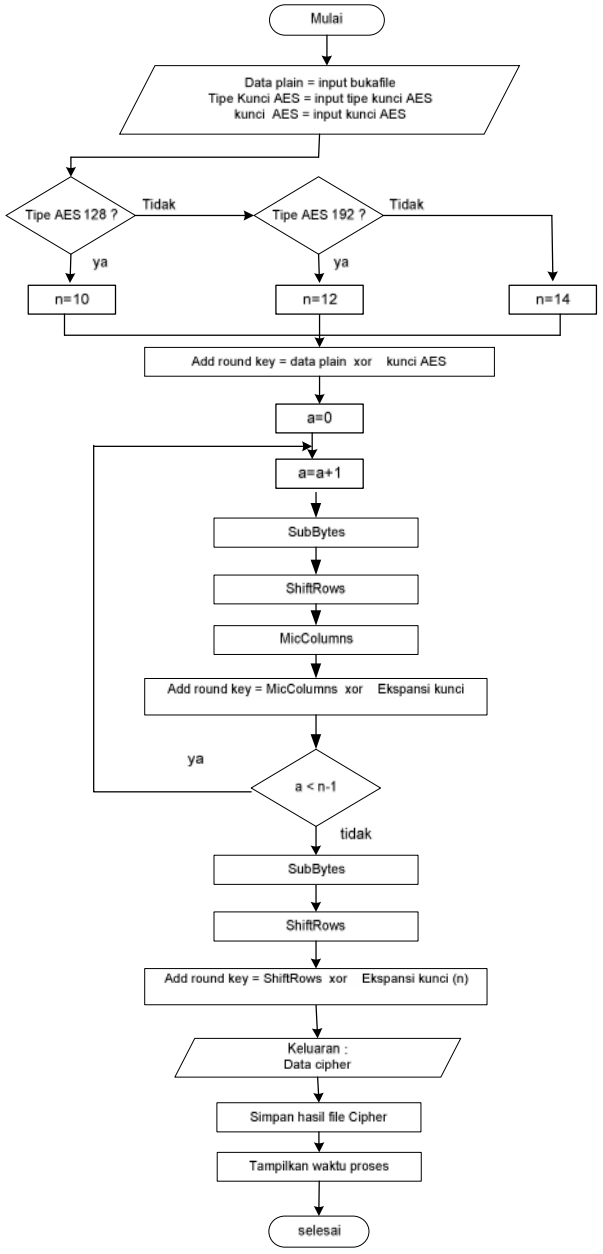
1. Addroundkey
2. Putaran sebanyak a-1 kali, proses yang dilakukan pada setiap putaran adalah: *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*.
3. Final round, adalah proses untuk putaran terakhir yang meliputi *SubBytes*, *ShiftRows*, dan *AddRoundKey*.

Sedangkan pada proses dekripsi AES-128, proses putaran juga dikerjakan sebanyak 10 kali (a=10), yaitu sebagai b

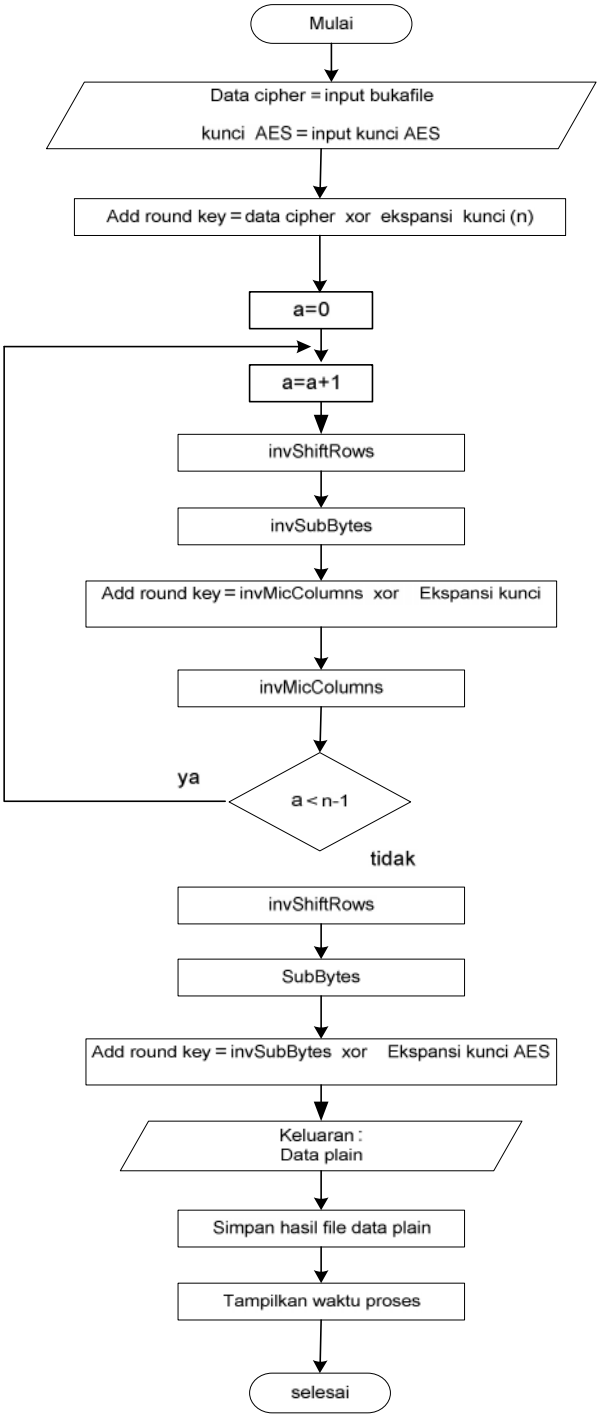
1. Addroundkey
2. Putaran sebanyak a-1 kali, dimana pada setiap putaran dilakukan proses: *InverseShiftRows*, *InverseSubBytes*, *AddRoundKey*, dan *InverseMixColumns*.
3. Final round, adalah proses untuk putaran terakhir yang meliputi *InverseShiftRows*, *InverseSubBytes*, dan *AddRoundKey*.

Pada enkripsi dan dekripsi AES-192 proses putaran dikerjakan 12 kali (a=12), sedangkan untuk AES-256 proses putaran dikerjakan 14 kali (a=14).

Algoritma AES pada penelitian ini digunakan untuk mengenkripsi dan mendekripsi file dokumen digital khususnya adalah file dokumen PDF, DOC, dan TXT. Pada Gambar 2.1 dan Gambar 2.2 dapat dilihat diagram alir yang berisi langkah-langkah dari proses enkripsi dan dekripsi algoritma AES.



Gambar 2.1 Diagram alir Enkripsi Algoritma AES



Gambar 2.2 Diagram alir Dekripsi Algoritma AES

2.2. Perancangan Antar Muka

Perancangan antarmuka (*interface*) dilakukan dengan mempertimbangkan faktor kemudahan pengguna dan secara tidak langsung dapat digunakan untuk menuntun pengguna agar terhindar dari kekeliruan pada saat mengisi masukan ke dalam perangkat lunak.

a. Proses Input Output Menu Enkripsi

Perancangan antarmuka menu enkripsi AES pada penelitian ini menyediakan fungsi masukan, fungsi keluaran, dan beberapa fungsi yang lain. Fungsi masukan beru

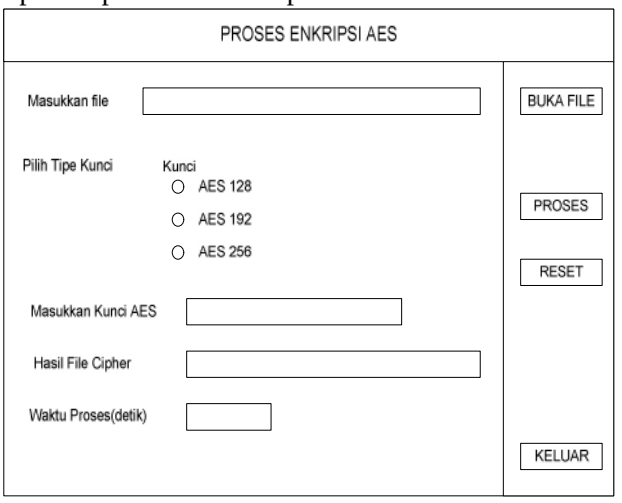
disandikan (dienkrip), pemilihan tipe kunci AES (pengguna dapat memilih tipe kunci AES), dan kunci AES. Fungsi keluaran berupa: file hasil enkripsi (*ciphertext*), dan keterangan waktu yang dibutuhkan dalam proses enkripsi.

Fungsi yang lain adalah sebagai berikut: fungsi Buka File untuk membuka file yang akan disandikan, fungsi Proses untuk melakukan proses enkripsi, fungsi Reset untuk melakukan reset terhadap isian yang telah ada, dan fungsi Keluar untuk keluar dari program. Pada Gambar 2.3 dapat dilihat susunan fungsi proses input output menu Enkripsi.

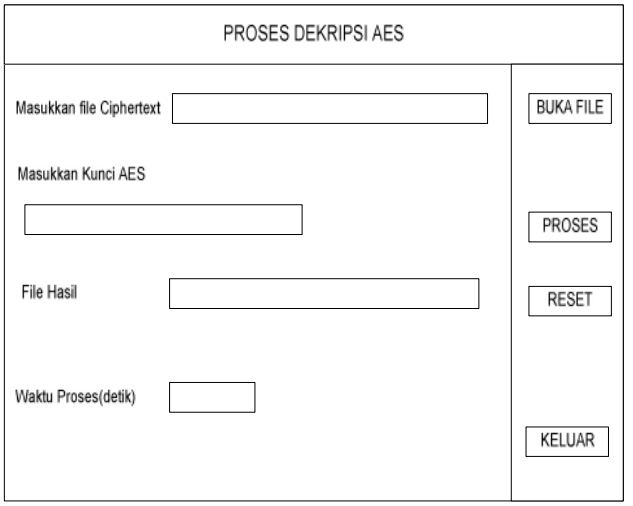
b. Proses Input Output Menu Dekripsi

Perancangan antarmuka menu dekripsi AES pada penelitian ini menyediakan fungsi masukan, fungsi keluaran, dan beberapa fungsi yang lain. Fungsi masukan berupa: file yang akan didekrip, dan kunci AES. Fungsi keluaran berupa: file hasil dekripsi (*plaintext*), dan keterangan waktu yang dibutuhkan dalam proses dekripsi.

Fungsi yang lain adalah sebagai berikut: fungsi Buka File untuk membuka file yang telah disandikan (*ciphertext*), fungsi Proses untuk melakukan proses dekripsi file *ciphertext*, fungsi Reset untuk melakukan reset terhadap isian yang telah ada, dan fungsi Keluar untuk keluar dari program. Pada Gambar 2.4 dapat dilihat susunan fungsi proses input output menu Dekripsi.



Gambar 2.3 Perancangan Antarmuka Menu Enkripsi

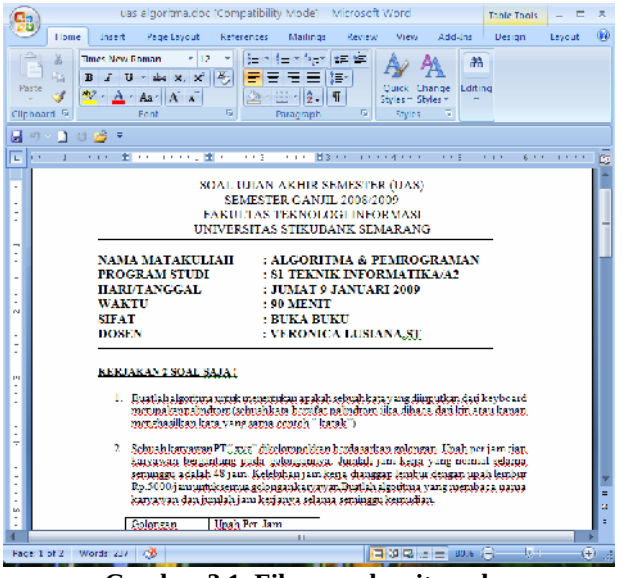


Gambar 2.4 Perancangan Antarmuka Menu Dekripsi

3. IMPLEMENTASI DAN PENGUJIAN

3.1. Proses Enkripsi

Perangkat lunak Matlab versi 7.0.4 digunakan untuk mengimplementasikan proses enkripsi dan dekripsi algoritma AES-128. Berikut ini adalah contoh dari proses tersebut untuk file *uas_algoritma.doc* yang memiliki ukuran 34.816 byte. File ini berisi soal ujian sehingga kategori isi file tersebut adalah bersifat rahasia, seperti dapat dilihat pada Gambar 3.1.

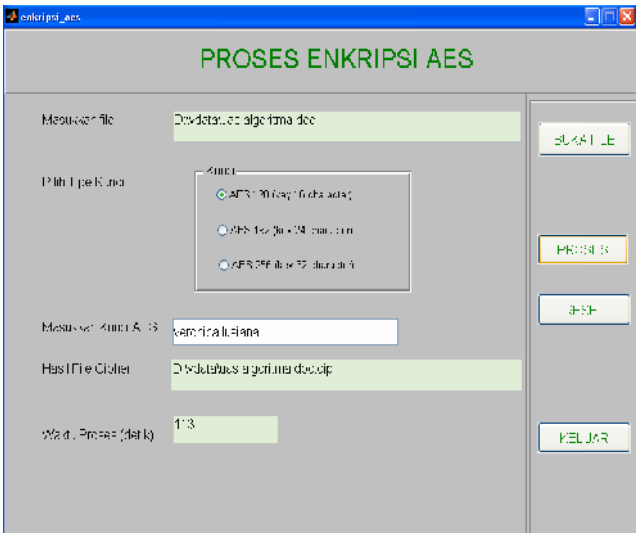

SOAL UJIAN AKHIR SEMESTER (UAS)
SEMESTER GANJIL 2008/2009
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS STIKUBANK SEMARANG

NAMA MATAKULIAH : ALGORITMA & PEMROGRAMAN
PROGRAM STUDI : S1 TEKNIK INFORMATIKA/A2
HARI/TANGGAL : JUMAT 9 JANUARI 2009
WAKTU : 90 MENIT
SIFAT : BUKA BUKU
DOSEN : VERONICA LUSIANA,ST

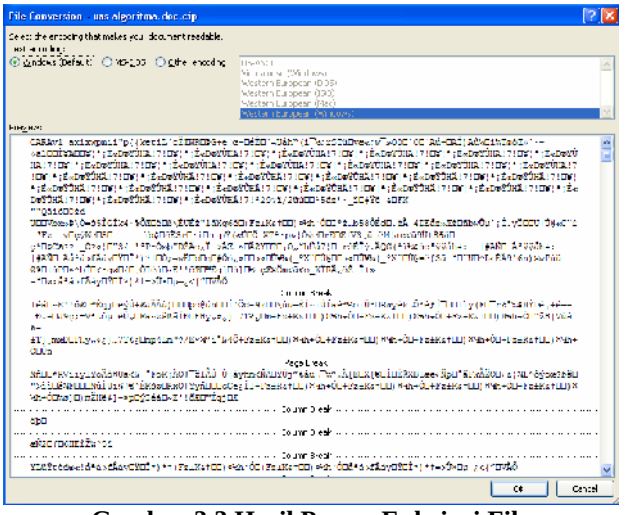
KERJAKAN 2 SOAL SAJA !

Gambar 3.1. File uas_algoritma.doc

Untuk menjaga kerahasiaan isinya maka file ini akan dienkripsi menggunakan AES-128 dengan kunci '*veronica lusiana*' (16 karakter), program untuk proses enkripsi AES-128 dapat dilihat pada Gambar 3.2. Hasil proses enkripsi berupa file cipher '*uas_algoritma.doc.cip*' yang berukuran 34.856 byte dengan waktu proses 113 detik, seperti dapat dilihat pada Gambar 3.3.



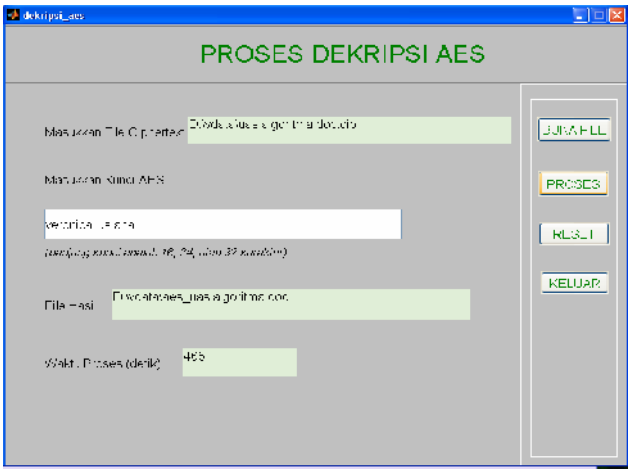
Gambar 3.2 Tampilan proses enkripsi AES-128



Gambar 3.3 Hasil Proses Enkripsi File uas_algoritma.doc.cip

3.2. Proses Dekripsi

Proses dekripsi AES yaitu mendekripsi file *uas_algoritma.doc.cip* menggunakan AES-128 dengan kunci '*veronica lusiana*'. Proses ini membutuhkan waktu 465 detik serta menghasilkan ukuran file 34.816 byte, seperti dapat dilihat pada Gambar 3.4. Hasil proses dekripsi adalah file *aes_uas algoritma.doc*, sama seperti file semula.



Gambar 3.4 Tampilan proses dekripsi AES

3.3. Hasil Pengujian

Proses pengujian meliputi waktu yang diperlukan untuk proses enkripsi dan dekripsi dengan beberapa macam format dan ukuran file yang berbeda, dan ukuran file yang dihasilkan dari proses enkripsi (menghasilkan file *.cip)

Pengujian dilakukan terhadap tiga jenis file dokumen yaitu: PDF, DOC (Microsoft word), dan txt. Nama file dan besar file selengkapnya dapat dilihat di Tabel 3.1. Pada kolom besar file terdapat variasi antara 64 byte sampai dengan 182.059 kilo byte. Data ini diperlukan untuk mengetahui berapa waktu yang dibutuhkan dan berapa besar ukuran file yang dihasilkan dari proses enkripsi dan dekripsi. Hasil proses enkripsi dan dekripsi selengkapnya dapat dilihat di Tabel 3.2.

Tabel 3.1 Daftar file yang akan diproses

No	Nama file	Keterangan format file	Size (byte) plain
1	v_pesanpdf01	dokumen – pdf	6.865
2	v_pesanpdf02	dokumen – pdf	12.461
4	v_paperpdf06	dokumen – pdf	182.059
5	v_pesandoc01	dokumen – doc	24.064
6	v_pesandoc02	dokumen – doc	24.064
7	v_pesantext01	dokumen – txt	64
8	v_pesantext02	dokumen – txt	129
9	v_pesantext03	dokumen – txt	265

Pada Tabel 3.2 dapat diamati bahwa ukuran file hasil enkripsi AES dan kebutuhan waktu prosesnya akan berbanding lurus dengan ukuran file aslinya (*plain file*). Ukuran file hasil enkripsi dan kebutuhan waktu proses dipengaruhi oleh ukuran file asli, namun tidak dipengaruhi oleh jenis format file. Semakin besar ukuran file asli maka semakin besar pula ukuran file hasil enkripsi dan kebutuhan waktu prosesnya. Ukuran file hasil proses dekripsi adalah sama seperti ukuran file aslinya. Proses dekripsi algoritma AES meme

kompleks jika dibandingkan dengan proses enkripsinya, sehingga menyebabkan waktu yang dibutuhkan untuk proses dekripsi menjadi lebih lama.

Tabel 3.2 Hasil proses pengujian

No	Nama file	Ket. format file	Size (byte)			Waktu (detik)	
			Plain	enkripsi	dekripsi	enkripsi	dekripsi
1	v_pesantext01	Dok. txt	64	104	64	0,28	1
2	v_pesantext02	Dok. txt	129	168	129	0,46	2
3	v_pesantext03	Dok. txt	265	296	256	0,82	4
4	v_pesanpdf01	Dok. txt	6.865	6.904	6.865	19	80
5	v_pesanpdf02	Dok. pdf	12.461	12.488	12.461	36	153
6	v_pesandoc01	Dok.doc	24.064	24.104	24.064	70	297
7	v_pesandoc02	Dok. doc	24.064	24.104	24.064	70	297
8	v_paperpdf06	Dok. pdf	182.059	182.088	182.059	1.223	3.792

File hasil enkripsi (file *.cip) disusun dari dua komponen yaitu: *informasi header* dan *data cipher*. *Informasi header* terdiri dari 8 karakter identitas yaitu "*CARAv1 x*" dengan karakter *x* mencatat jenis AES (AES-128, AES-192, atau AES-256), dan ditambah dengan kunci AES yang telah diacak (sebanyak 16, 24, atau 32 karakter) sesuai dengan jenis AES yang digunakan. Informasi header ini sebagai pengenal file hasil enkripsi dan digunakan untuk mendeteksi benar atau salah kunci yang digunakan pada awal proses dekripsi.

4. PENUTUP

1.1. Kesimpulan

1. Sistem yang dikembangkan dapat dimanfaatkan untuk proses enkripsi dan dekripsi file dengan berbagai macam ukuran dan jenis file, menggunakan algoritma AES-128.
2. Ukuran file lampiran hasil enkripsi tidak dipengaruhi oleh format file lampiran, tetapi dipengaruhi oleh ukuran awal file lampiran. Semakin besar ukuran file dan semakin panjang kunci AES yang digunakan maka semakin besar ukuran file enkripsi yang dihasilkan.
3. Pada saat proses dekripsi maka memerlukan komputasi lebih banyak jika dibandingkan dengan proses enkripsi, sehingga kebutuhan waktu proses dekripsi menjadi lebih lama dibandingkan dengan proses enkripsi.

1.2. Saran

1. Untuk file yang berukuran relatif besar sebelum proses enkripsi akan lebih baik apabila dikompres terlebih dulu, hal ini berguna untuk mempercepat proses enkripsi dan dekripsi menggunakan algoritma AES.
2. Agar program aplikasi ini dapat digunakan oleh masyarakat secara bebas sehingga dapat lebih bermanfaat, maka sebaiknya program aplikasi memiliki lisensi *free software*, serta bersifat *stand alone*.

DAFTAR PUSTAKA

1] Daemen, Joan; & Rijmen, Vincent. November 26 2001. *Advanced Encryption Standard (AES)*. Federal Information Processing Standards Publication 197.

2] Konheim, G.A. 2007. *Computer Security And Cryptography*. New Jersey: A John Wiley&Sons, Inc.

3] Menezes, J.A; Oorschot, C.P; & Vanstone, A.S. 1997. *Handbook of Applied Crypthography*. USA: CRC Press LLC.

4] Munir, Rinaldi. 2006. *Kriptografi*. Bandung: Penerbit Informatika.

5] Schneier, Bruce. 1996. *Applied Cryptography, Protocols, Algorithms, and Source Code in C*. New York: A John Wiley&Sons, Inc.

6] Song, Beomsik. 2004. *Observations on the Cryptologic Properties of the AES Algorithm*. Submitted for the degree of Doctor of Philosophy. Australia: University of Wollongong.

7] Stallings, William.1999. *Cryptography and Network Security Principles and Practice second edition*. New Jersey : Prentice Hall, Inc.

8] Stinson, R.D. 2002. *Cryptography Theory and Practice*. USA: Chapman&Hall/CRC.

9] Sugiharto, Aris. 2006. *Pemrograman GUI Dengan Matlab*. Yogyakarta: ANDI.

The MathWorks Inc. 2001. *Matlab The Language of Technical Computing Creating Graphical User Interfaces*. Natick. MA USA.