

IMPLEMENTASI ALGORITMA RIJNDAEL UNTUK ENKRIPSI DAN DEKRIPSI PADA CITRA DIGITAL

R. Kristoforus JB¹, Stefanus Aditya BP²

¹Jurusan Teknik Informatika, Sekolah Tinggi Teknik Musi

Jl. Bangau No. 60 Palembang 30113

Telp. (0711) 366326, Faks. (00711)351782

²Jurusan Teknik Informatika, Sekolah Tinggi Teknik Musi

Jl. Bangau No. 60 Palembang 30113

E-mail: kristojb@gmail.com, steva777@gmail.com

ABSTRAK

Masalah keamanan dan kerahasiaan data dan informasi merupakan suatu hal yang penting. Salah satu cara menjaga keamanan dan kerahasiaan data dan informasi adalah dengan teknik enkripsi dan dekripsi atau yang dikenal juga dengan kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan dengan cara mengubahnya menjadi suatu bentuk yang tidak dapat dikenali lagi. Salah satu algoritma kriptografi yang sering digunakan saat ini adalah Rijndael atau yang dikenal juga dengan AES (Advanced Encryption Standard). Kriptografi dapat diterapkan pada berbagai jenis file, salah satunya adalah citra digital. Perangkat lunak yang akan dibangun adalah perangkat lunak enkripsi dan dekripsi dengan algoritma Rijndael untuk citra digital. Perangkat lunak ini akan dibangun dengan menggunakan metode Waterfall. Hasil dari pembangunan perangkat lunak ini telah dapat mengimplementasikan algoritma kriptografi Rijndael untuk menjaga keamanan dan kerahasiaan citra digital dengan format file citra bitmap.

Kata Kunci: kriptografi, Rijndael, citra digital

1. PENDAHULUAN

1.1 Latar Belakang

Masalah keamanan merupakan suatu aspek penting dalam pengiriman data maupun komunikasi melalui jaringan. Salah satu cara untuk menjaga keamanan dan kerahasiaan suatu data maupun informasi adalah dengan teknik enkripsi dan dekripsi guna membuat pesan, data, maupun informasi tidak dapat dibaca atau dimengerti oleh orang lain, kecuali untuk penerima yang berhak (Tjiharjadi dan Wijaya, 2009). Teknik pengamanan data dengan enkripsi dan dekripsi dikenal dengan kriptografi.

Kriptografi adalah ilmu yang mempelajari mengenai cara mengamankan suatu informasi. Pengamanan ini dilakukan dengan melakukan enkripsi dan dekripsi pada informasi tersebut dengan suatu kunci khusus. Informasi yang belum mengalami proses enkripsi disebut *plaintext*, sedangkan informasi yang telah mengalami proses enkripsi disebut *ciphertext*. Berbagai algoritma kriptografi telah diciptakan oleh para ahli kriptografi, namun berbagai usaha untuk memecahkannya tidak sedikit yang membawa keberhasilan. Hal ini mendorong para ahli kriptografi untuk menciptakan algoritma-algoritma baru yang lebih aman. Pada bulan Oktober 2000, algoritma *Rijndael* terpilih sebagai AES, dan pada bulan November 2001, algoritma *Rijndael* ditetapkan sebagai AES, dan diharapkan algoritma *Rijndael* menjadi standar kriptografi yang dominan paling sedikit selama 10 tahun (Surian, 2006).

Citra digital telah digunakan secara luas dalam berbagai macam proses sehingga perlindungan citra

digital dari pihak yang tidak memiliki hak akses menjadi sangat penting (Krikor, dkk., 2009). Pemerintah, militer, badan keuangan, rumah sakit, dan perusahaan swasta telah menggunakan citra digital untuk menyimpan informasi penting, misalnya hasil pemeriksaan pasien (untuk rumah sakit), area geografi (untuk penelitian), posisi musuh (untuk militer), produk baru (untuk perusahaan swasta), status keuangan, dan lain-lain. Hampir semua informasi ini dikumpulkan dan disimpan dalam komputer kemudian dikirimkan melalui jaringan, misalnya internet. Bila informasi penting ini jatuh ke tangan orang yang salah, maka akan menyebabkan hal yang tidak diinginkan, misalnya perang (untuk militer) dan penanganan pasien yang salah (untuk rumah sakit). Hal inilah yang menyebabkan perlindungan citra digital menjadi sangat penting (Kushwaha dan Roy, 2010). Penelitian ini akan membangun sebuah perangkat lunak untuk mengimplementasikan algoritma kriptografi *Rijndael* pada citra digital.

1.2 Rumusan dan Batasan Masalah

Permasalahan yang akan dibahas adalah bagaimana mengimplementasikan algoritma kriptografi *Rijndael* untuk enkripsi dan dekripsi pada citra digital.

Permasalahan yang dibahas pada penelitian ini akan dibatasi pada.

- (a). Kriptografi yang digunakan adalah kriptografi kunci simetri dengan algoritma *Rijndael* mode ECB dengan ukuran blok 128 bit.

- (b). Implementasi algoritma kriptografi akan dilakukan untuk enkripsi dan dekripsi citra digital format *file* citra bitmap 24 bit.

1.3 Tujuan dan Manfaat Penelitian

Tujuan dari diadakannya penelitian ini adalah membangun sebuah perangkat lunak untuk mengimplementasikan enkripsi dan dekripsi pada citra digital dengan algoritma *Rijndael*.

Manfaat yang diharapkan dapat dicapai melalui penelitian ini adalah :

- Membantu pemahaman alur kerja kriptografi kunci simetri dengan algoritma *Rijndael*.
- Perangkat lunak yang dibangun dapat menjadi salah satu alternatif untuk mengenkripsi dan mendekripsi *file* berupa citra digital.

2. TINJAUAN PUSTAKA

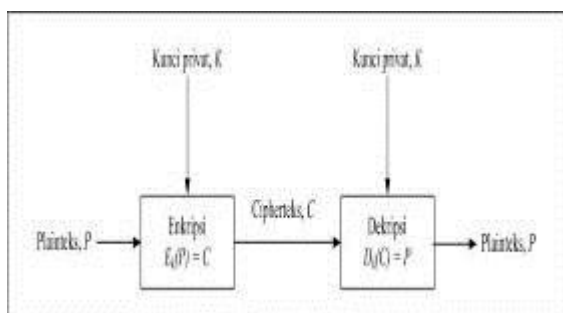
2.1 Kriptografi

Schneier (1996) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (*Cryptography is the art and science of keeping message secure*), sedangkan Menezes, dkk (1996) menyatakan bahwa kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, dan otentikasi. Jadi, dapat disimpulkan bahwa kriptografi adalah ilmu yang mempelajari teknik-teknik matematika untuk menjaga keamanan informasi.

Sistem kriptografi (*cryptosystem*) adalah kumpulan yang terdiri dari algoritma kriptografi dengan semua *plaintext*, *ciphertext*, dan kunci yang mungkin (Schneier, 2006). Sistem kriptografi dapat diklasifikasikan ke dalam 3 dimensi yang berbeda, yaitu (Stallings, 2005) :

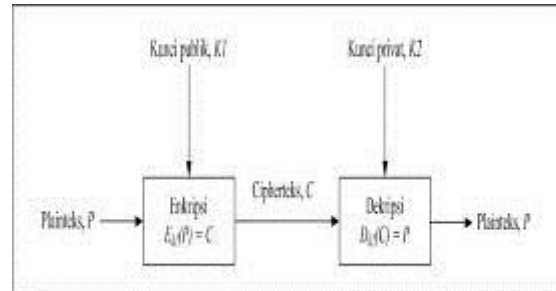
- Tipe operasi yang digunakan untuk mentransformasikan *plaintext* ke *ciphertext*.
- Jumlah kunci yang digunakan.
- Cara memproses *plaintext*.

Dalam perkembangannya ada dua jenis algoritma kriptografi, yaitu algoritma enkripsi kunci simetris (*symmetric-key encryption algorithm*) dan algoritma enkripsi kunci publik (*public-key encryption algorithm*). Algoritma enkripsi kunci simetris menggunakan kunci yang sama atau disebut juga kunci rahasia.



Gambar 1. Skema Kriptografi Kunci Simetris (Munir, 2006)

Algoritma enkripsi kunci publik menggunakan dua kunci yang berpasangan tetapi berbeda. Satu kunci dipakai untuk enkripsi dan satu kunci lainnya dipakai untuk dekripsi. Pengirim mengenkripsi pesan dengan menggunakan kunci publik si penerima pesan (*receiver*). Hanya penerima pesan yang dapat mendekripsi pesan karena hanya ia yang mengetahui kunci privatnya sendiri.



Gambar 2. Skema Kriptografi Kunci Publik (Munir, 2006)

2.2 Citra Digital

Citra adalah suatu representasi (gambaran), kemiripan, atau imitasi dari suatu objek. Citra terbagi menjadi dua, yaitu citra analog dan citra digital. Citra analog adalah citra yang bersifat kontinu, seperti gambar pada monitor televisi, foto sinar-X, foto yang tercetak di kertas foto, lukisan, pemandangan alam, hasil CT *scan*, gambar-gambar yang terekam pada pita kaset, dan sebagainya. Citra digital adalah citra yang dapat diolah oleh komputer.

Sebuah citra digital dapat diwakili oleh sebuah matriks yang terdiri dari M kolom dan N baris, di mana perpotongan antara kolom dan baris disebut piksel (*picture element*), yaitu elemen terkecil dari sebuah citra. Piksel mempunyai dua parameter, yaitu koordinat dan intensitas atau warna. Nilai yang terdapat pada koordinat (x,y) adalah $f(x,y)$, yaitu besar intensitas atau warna dari piksel di titik itu. Oleh sebab itu, sebuah citra digital dapat ditulis dalam bentuk matriks berikut.

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,M-1) \\ f(1,0) & \dots & \dots & f(1,M-1) \\ \dots & \dots & \dots & \dots \\ f(N-1,0) & f(N-1,1) & \dots & f(N-1,M-1) \end{bmatrix}$$

Berdasarkan gambaran tersebut, secara matematis citra digital dapat dituliskan sebagai fungsi intensitas $f(x,y)$, di mana harga x (baris) dan y (kolom) merupakan koordinat posisi dan $f(x,y)$ adalah nilai fungsi pada setiap titik (x,y) yang menyatakan besar intensitas citra atau tingkat keabuan atau warna dari piksel di titik tersebut.

Dua jenis format *file* citra yang sering digunakan dalam pengolahan citra, yaitu citra bitmap dan citra vektor. Citra vektor dihasilkan dari perhitungan matematis dan tidak berdasarkan piksel, yaitu data tersimpan dalam bentuk vektor posisi, di

mana yang tersimpan hanya informasi vektor posisi dengan bentuk sebuah fungsi. Citra bitmap sering disebut juga dengan citra raster. Citra bitmap menyimpan data kode citra secara digital dan lengkap (cara penyimpanannya adalah per piksel). Citra bitmap direpresentasikan dalam bentuk matriks atau dipetakan dengan menggunakan bilangan biner atau sistem bilangan lain (Sutoyo, dkk., 2009). Beberapa format citra bitmap, yaitu *.bmp, *.jpeg, *.gif, dan sebagainya.

2.3 Kriptografi Pada Citra Digital

Terdapat beberapa penelitian mengenai kriptografi pada citra digital yang telah dilakukan sebelumnya. El-Fishawy, dkk. (2007) membahas enkripsi pada citra digital format *.bmp menggunakan tiga buah algoritma yang berbeda, yaitu RC6, MRC6, dan Rijndael. Penelitian ini ditujukan untuk mengukur kualitas citra hasil enkripsi masing-masing algoritma dengan tiga metode yang berbeda, yaitu ECB, CBC, dan OFB.

Krikor, dkk. (2009) mengusulkan metode baru untuk enkripsi selektif pada citra digital berdasarkan pendekatan enkripsi pada koefisien DCT. Penelitian ini menggunakan citra digital format bmp sebagai file yang akan mengalami proses enkripsi. Perangkat lunak yang digunakan untuk implementasi adalah Visual C#.NET. Hasil yang didapat menunjukkan proses enkripsi berjalan dengan baik pada citra digital.

Ahmed, dkk. (2007) melakukan pengujian, analisa keefektifan enkripsi, dan evaluasi keamanan enkripsi citra digital dengan algoritma RC6. Hasil yang didapat menunjukkan enkripsi pada citra digital dengan algoritma RC6 menunjukkan hasil yang memuaskan dan cukup menjanjikan untuk menjaga keamanan file berupa citra digital.

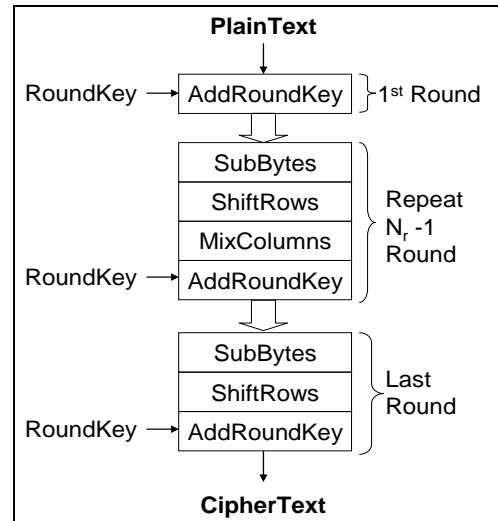
Pada penelitian ini akan dilakukan proses enkripsi dan dekripsi pada citra digital dengan format file citra bitmap dengan menggunakan algoritma Rijndael. Citra digital dipilih karena telah digunakan secara luas dalam berbagai proses (Krikor, dkk., 2009), sedangkan algoritma Rijndael dipilih karena mudah diimplementasikan dalam hardware maupun software, membutuhkan memori yang tidak terlalu besar, dan eksekusinya cepat (Munir, 2006).

2.4 Algoritma Rijndael

Algoritma Rijndael merupakan algoritma yang ditetapkan oleh NIST sebagai AES pada bulan Oktober 2000. Algoritma Rijndael ditemukan oleh Vincent Rijmen dan Joan Daemen dari Belgia. Rijndael termasuk dalam algoritma kriptografi yang sifatnya simetris dan block cipher. Rijndael mendukung panjang kunci 128 bit, 192 bit, dan 256 bit. Panjang kunci dan ukuran blok dapat dipilih secara independen.

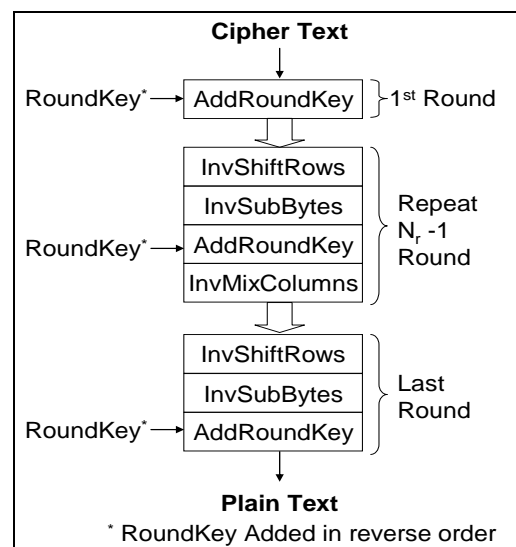
Proses enkripsi pada algoritma Rijndael terdiri dari 4 jenis transformasi byte, yaitu SubBytes(),

ShiftRows(), MixColumns(), dan AddRoundKey(). Pada awal proses enkripsi, masukan yang telah berbentuk array state akan mengalami transformasi AddRoundKey(). Setelah itu, array state akan mengalami transformasi SubBytes(), ShiftRows(), MixColumns(), dan AddRoundKey() secara berulang-ulang sebanyak N_r . Proses ini dalam algoritma Rijndael disebut sebagai round function. Round yang terakhir agak berbeda dengan round-round sebelumnya di mana pada round terakhir, array state tidak mengalami transformasi MixColumns().



Gambar 3. Diagram Proses Enkripsi Rijndael (Stallings, 2005)

Transformasi cipher dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan inverse cipher. Transformasi yang digunakan pada inverse cipher adalah InvShiftRows(), InvSubBytes(), InvMixColumns(), dan AddRoundKey() (FIPS Publication, 2001).

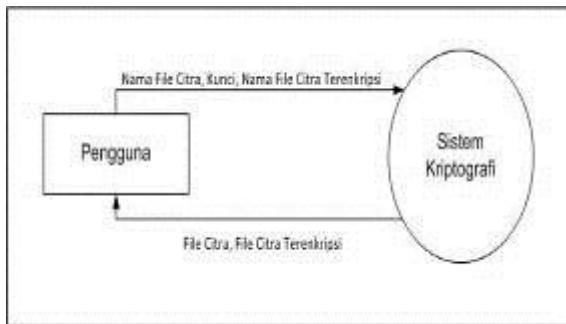


Gambar 4. Diagram Proses Dekripsi Rijndael (Stallings, 2005)

3. ANALISIS

Dalam menerapkan keamanan data dengan menggunakan algoritma *Rijndael*, maka akan dibangun sebuah perangkat lunak untuk melakukan proses enkripsi dan dekripsi. Perangkat lunak ini memerlukan sebuah kunci untuk menjalankan proses enkripsi. Kunci yang sama diperlukan untuk melakukan proses dekripsi dengan benar. Bila kunci yang dimasukkan untuk proses dekripsi berbeda dengan kunci enkripsi, maka hasil yang didapat juga berbeda dengan data awal. Data yang dapat mengalami proses enkripsi maupun proses dekripsi hanya data berupa citra digital. Seluruh proses enkripsi dan dekripsi akan dilakukan dengan ukuran blok data 128 bit dan mode operasi ECB.

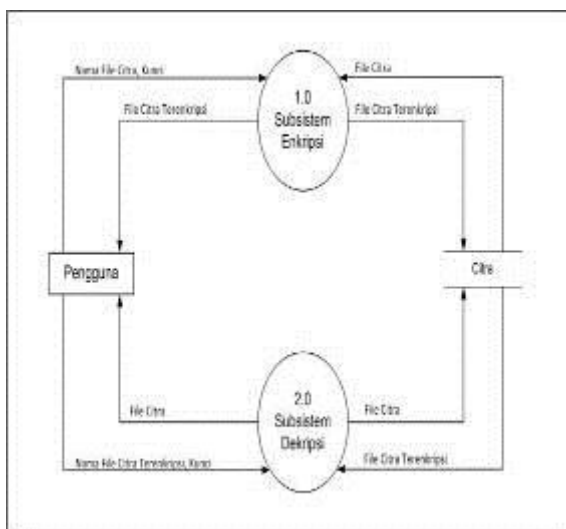
Diagram Konteks



Gambar 5. Diagram Konteks

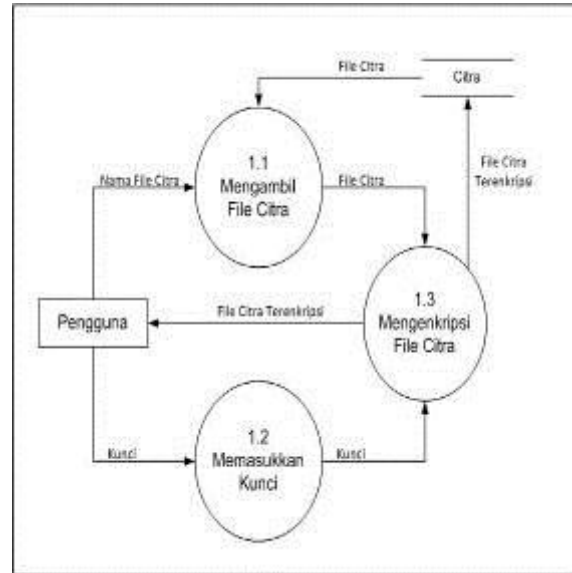
Diagram konteks pada gambar 5 menjelaskan aliran data pada sistem kriptografi yang dibangun. Sistem yang akan dibangun memiliki sebuah terminator, yaitu pengguna sistem. Aliran data yang masuk ke sistem berupa nama *file* citra, kunci, dan nama *file* citra terenkripsi. Aliran data yang dihasilkan oleh sistem berupa *file* citra dan *file* citra terenkripsi.

Data Flow Diagram

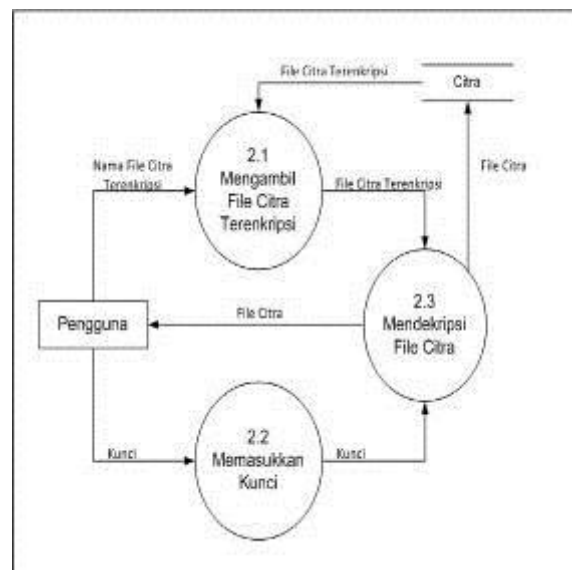


Gambar 6. DFD Level 0

Diagram pada gambar 8 menunjukkan pembagian sistem kriptografi yang dibangun menjadi dua subsistem, yaitu subsistem enkripsi dan subsistem dekripsi.























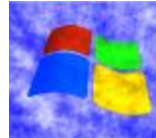
Gambar 7. DFD Level 1 Subsistem Enkripsi






Gambar 8. DFD Level 1 Subsistem Dekripsi

4. HASIL DAN PEMBAHASAN

Pengujian terhadap perangkat lunak ini dilakukan untuk mengetahui apakah perangkat lunak telah berjalan sesuai dengan rancangan atau tidak. Berikut ini adalah beberapa pengujian yang dilakukan, antara lain pengujian enkripsi dan dekripsi pada citra digital dan pengujian kecepatan proses enkripsi dan dekripsi. Pengujian dilakukan pada beberapa *file* citra digital dengan kedalaman warna 24 bit yang mengalami proses enkripsi dan dekripsi. Proses enkripsi dan dekripsi dilakukan dengan kunci "KunciUntukKripto" dengan ukuran panjang kunci yang digunakan 128 bit.

1. kenshin.bmp (176 x 132)

Citra Asli

Hasil Enkripsi

Hasil Dekripsi
2. bridge.bmp (300 x 225)

Citra Asli

Hasil Enkripsi

Hasil Dekripsi
3. numerus.bmp (400 x 418)

Citra Asli

Hasil Enkripsi

Hasil Dekripsi
4. guanping.bmp (450 x 600)

Citra Asli

Hasil Enkripsi

Hasil Dekripsi
5. ninja.bmp (640 x 480)

Citra Asli

Hasil Enkripsi

Hasil Dekripsi
6. liverpool.bmp (800 x 600)

Citra Asli

Hasil Enkripsi

Hasil Dekripsi
7. windows.bmp (1024 x 768)

Citra Asli

Hasil Enkripsi

Hasil Dekripsi

8. gunung.bmp (1600 x 1200)

Citra Asli

Hasil Enkripsi

Hasil Dekripsi

Berdasarkan hasil pengujian di atas dapat terlihat hasil enkripsi citra *ninja.bmp* dan *liverpool.bmp* masih terlihat kemiripan dengan citra asli. Hal ini disebabkan kedua citra tersebut memiliki daerah yang didominasi oleh warna tunggal. Perangkat lunak yang dibangun menggunakan mode *cipher block* ECB, sehingga bila ada daerah yang didominasi oleh warna tunggal, maka hasil enkripsi pada daerah tersebut cenderung sama. Hal inilah yang menyebabkan citra hasil enkripsi *ninja.bmp* dan *liverpool.bmp* masih memiliki kemiripan dengan citra asli.

Pengujian Kecepatan Proses Enkripsi Dan Dekripsi

Tabel 1. Hasil Pengukuran Kecepatan Proses Enkripsi

Nama File Citra	Kecepatan Proses Enkripsi (milisecond)		
	128 Bit	192 Bit	256 Bit
kenshin.bmp	172	203	218
bridge.bmp	468	530	609
numerus.bmp	1092	1311	1482
guanping.bmp	1779	2044	2340
ninja.bmp	2028	2340	2652
liverpool.bmp	3151	3635	4196
windows.bmp	5148	6021	6786
gunung.bmp	12589	14727	16973

Tabel 2. Hasil Pengukuran Kecepatan Proses Dekripsi

Nama File Citra	Kecepatan Proses Dekripsi (milisecond)		
	128 Bit	192 Bit	256 Bit
kenshin.bmp	171	203	219
bridge.bmp	452	531	608
numerus.bmp	1076	1295	1466
guanping.bmp	1747	2075	2371
ninja.bmp	2012	2308	2668
liverpool.bmp	3167	3697	4134
windows.bmp	5179	5990	6801
gunung.bmp	12480	14601	16536

Berdasarkan hasil pengujian kecepatan proses enkripsi dan dapat terlihat bahwa semakin panjang kunci yang digunakan, maka waktu proses semakin lama. Proses enkripsi dengan panjang kunci 192 bit mengalami peningkatan waktu rata-rata sebesar 16,59% lebih lama dibandingkan dengan panjang

kunci 128 bit, sedangkan proses enkripsi dengan panjang kunci 256 bit mengalami peningkatan waktu rata-rata sebesar 33,41% lebih lama dibandingkan dengan panjang kunci 128 bit. Proses dekripsi dengan panjang kunci 192 bit mengalami peningkatan waktu rata-rata sebesar 16,71% lebih lama dibandingkan dengan panjang kunci 128 bit, sedangkan proses dekripsi dengan panjang kunci 256 bit mengalami peningkatan waktu rata-rata sebesar 32,23% lebih lama dibandingkan dengan panjang kunci 128 bit.

Seminar Nasional Aplikasi Teknologi Informasi
2009. Yogyakarta, 20 Juni 2009

PUSTAKA

- Ahmed, H.E.H., Kalash, H.M., dan Allah, O.S.F. (2007). Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images. *International Journal of Computer, Information, and System Science, and Engineering* Vol. 1 No. 1.
- El-Fishawy, N. dan Zaid, O.M.A. (2007). Quality of Encryption Measurement of Bitmap Images With RC6, MRC6, and Rijndael Block Cipher Algorithms. *International Journal of Network Security* Vol. 5 No. 3, 241-251.
- Federal Information Processing Standards Publication 197. (2001). *Announcing the Advanced Encryption Standard (AES)*.
- Krikor, L., Baba, S., Arif, T., dan Shaaban, Z. (2009). Image Encryption Using DCT and Stream Cipher. *European Journal of Scientific Research* Vol. 32 No. 1, 47-57.
- Kushwaha, J., dan Roy, B.N. (2010). Secure Image Data by Double Encryption. *International Journal of Computer Application* Vol. 5 No. 10, Agustus 2010.
- Menezes, A.J., van Oorschot, P.C., dan Vanstone, S.A. (1996). *Handbook of Applied Cryptography*. CRC Press, Inc.
- Munir, R. (2006). *Kriptografi*. Bandung : Informatika.
- Schneier, Bruce. (1996). *Applied Cryptography, Second Edition : Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, Inc.
- Stallings, William. (2005). *Cryptography and Network Security Principles and Practices, Fourth Edition*. Prentice Hall.
- Sukrisno, dan Utami, E. (2007). Implementasi Steganografi Teknik EOF Dengan Gabungan Enkripsi Rijndael, Shift Cipher dan Fungsi Hash MD5. *Seminar Nasional Teknologi 2007*. Yogyakarta, 24 November 2007.
- Surian, D. (2006). Algoritma Kriptografi AES Rijndael. *Tesla Jurnal Teknik Elektro* Vol. 8 No. 2, 97-101.
- Sutoyo, T., Mulyanto, E., Suhartono, V., Nurhayati, O.D., dan Wijanarto. (2009). *Teori Pengolahan Citra*. Yogyakarta : Andi.
- Tjiharjadi, S., dan Wijaya, M.C. (2009). Pengamanan Data Menggunakan Metoda Enkripsi Simetri Dengan Algoritma Feal.