IMPLEMENTASI DAN ANALISIS ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) PADA TIGA VARIASI PANJANG KUNCI UNTUK BERKAS MULTIMEDIA

Natanael Benino Tampubolon[*)], R. Rizal Isnanto, and Enda Wista Sinuraya

Jurusan Teknik Elektro, Universitas Diponegoro Semarang
Jl. Prof. Sudharto, SH, Kampus UNDIP Tembalang, Semarang 50275, Indonesia

[*)]*E-mail: benjcmil@outlook.com*

Abstrak

Salah satu dampak negatif yang paling sering ditakutkan oleh pengguna teknologi adalah masalah privasi dan keamanan data. Karena itu, dibutuhkan suatu metode yang berguna untuk melindungi data tersebut dari serangan orang-orang tersebut. Metode yang dimaksud adalah kriptografi. Salah satu algoritma kriptografi yang saat ini sering digunakan adalah Advanced Encryption Standard atau biasa disingkat AES. Standar ini terdiri atas 3 blok cipher, yaitu AES-128, AES-192 dan AES-256, yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai Rijndael. Pada Penelitian ini dirancang sebuah sistem aplikasi yang dapat melakukan enkripsi dan dekripsi berkas multimedia (teks, citra dan grafis). Aplikasi ini juga membandingkan kinerja dari AES-128, AES-192 dan AES-256. Perbedaan kinerja ini berdasarkan ukuran kunci masing-masing yang sebesar 128, 192 dan 256 bit. Perbandingan kinerja dilihat berdasarkan waktu yang diperlukan untuk enkripsi dan dekripsi. Berdasarkan pengujian yang sudah dilakukan didapati bahwa enkripsi dan dekripsi menggunakan panjang kunci 128 bit membutuhkan waktu paling cepat, yaitu rata-rata 16,11 ms untuk enkripsi dan 10,44 untuk dekripsi. Enkripsi dan dekripsi yang menggunakan panjang kunci 256 bit membutuhkan waktu paling lama, yaitu rata-rata 19,68 untuk enkripsi dan 12,51 untuk dekripsi.

Kata kunci: Advanced Encryption Standard (AES), Teks, Citra, Grafis, Multimedia

Abstract

One of the negative effects of the most commonly feared by users of the technology is the issue of privacy and data security. Therefore, we need a method called cryptography that is useful to protect such data against these threats. One of the cryptographic algorithm that is currently often used is Advanced Encryption Standard or AES. This standard consists of three block ciphers, namely AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. This final project designs a system application that can encrypt and decrypt multimedia files (text, images and graphics). This application also compares the performance of AES-128, AES-192 and AES-256. The performance difference is based on the size of each key are at 128, 192 and 256 bits. Comparison of the performance seen by the time required for encryption and decryption. Based on the testing that has been done, the encryption and decryption using a key length of 128 bits requires the fastest time, which is an average 16.11 ms for encryption and 10,44 ms for decryption. While encryption and decryption using a key length of 256 bits takes the longest, with an average of 19.68 ms for encryption and 12.51 for decryption.

Keywords: Advanced Encryption Standard (AES), Text, Image, Graphic, Multimedia.

1. Pendahuluan

Seiring dengan majunya teknologi berkomunikasi, ternyata dampak yang dibawa tidak hanya dampak positif saja tetapi juga dampak negatif. Salah satu dampak negatif yang paling sering ditakutkan oleh pengguna teknologi adalah masalah privasi dan keamanan data. Zaman sekarang banyak orang-orang yang mempunyai niat kurang baik berusaha untuk menyadap data dan menggunakannya untuk keuntungan pribadi.

Berdasarkan data dari Symantec, pada tahun 2014, kriminal cyber terus mencuri informasi rahasia dalam skala yang sangat besar, dengan cara serangan langsung terhadap institusi-institusi. Meskipun pembobolan dengan skala sangat besar menurun pada tahun 2014, pembobolan data masih menjadi suatu isu yang signifikan.[6] Tahun 2012 terjadi 156 kasus, lalu meningkat 62% menjadi 253 kasus pada tahun 2013. Peningkatan 23% terjadi pada tahun 2014 menjadi sebanyak 312 kasus. [6]

Karena itu, dibutuhkan suatu metode yang berguna untuk melindungi data tersebut dari serangan orang-orang

tersebut. Metode yang dimaksud adalah kriptografi. Salah satu algoritma kriptografi yang saat ini sering digunakan adalah Advanced Encryption Standard atau biasa disingkat AES. AES standar enkripsi yang menggunakan kunci simetris. Standar ini terdiri atas 3 blok cipher, yaitu AES-128, AES-192 dan AES-256, yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai Rijndael. Masing-masing cipher memiliki ukuran 128-bit, dengan ukuran kunci masing-masing 128, 192, dan 256 bit.[3]

Pada Penelitian ini akan dirancang sebuah sistem aplikasi yang dapat melakukan enkripsi plain text sehingga menjadi cipher text dan juga dekripsi dari cipher text menjadi plain text. Aplikasi ini juga membandingkan kinerja dari AES-128, AES-192 dan AES-256. Perbedaan kinerja ini berdasarkan ukuran kunci masing-masing yang sebesar 128, 192 dan 256 bit. Perbandingan kinerja dilihat berdasarkan waktu yang diperlukan untuk enkripsi dan dekripsi. Dengan aplikasi ini diharapkan dapat menjaga kerahasiaan dan keamanan suatu pesan, juga untuk mengetahui kinerja yang terbaik dari beragam kunci yang digunakan dalam AES.

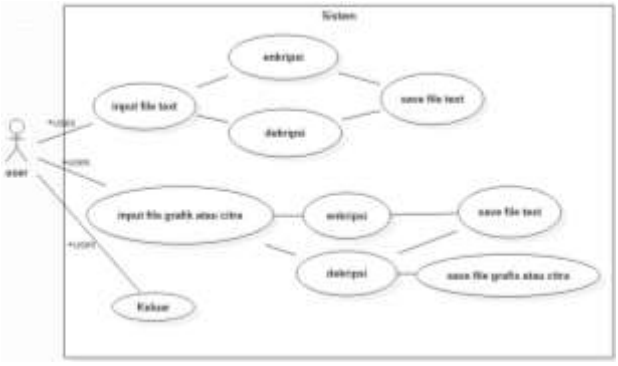
Tujuan yang ingin dicapai dari penelitian ini adalah:
1. Menerapkan algoritma AES untuk enkripsi dan dekripsi berkas multimedia (teks, grafis dan citra)
2. Membandingkan kinerja algoritma AES berdasarkan ragam panjang kunci.

2. Metode

Kebutuhan fungsional adalah fungsi dari sistem yang terlihat setelah sistem selesai dideskripsikan, kebutuhan fungsional ini kelak menjadi fitur utama dari sistem tersebut. Kebutuhan fungsional dari sistem ini adalah sebagai berikut

2.1. Diagram *Use Case*

Terdapat 1 aktor pada aplikasi yang akan dibangun ini, yaitu *user*. *User* adalah seseorang yang berperan untuk menjalankan proses enkripsi dan dekripsi.

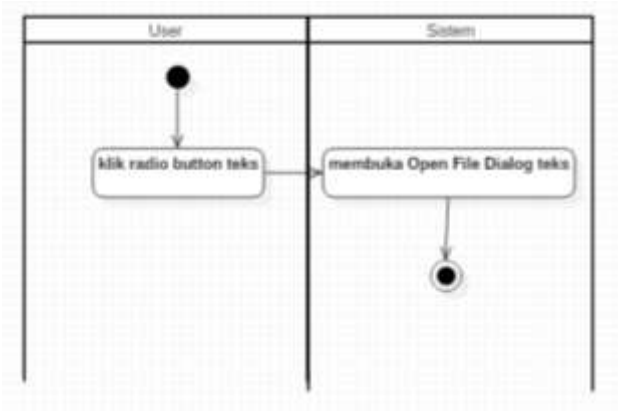


Gambar 1. Use Case Diagram

2.2. Diagram Aktivitas

2.2.1. Diagram Aktivitas Pemilihan Input Berkas Teks

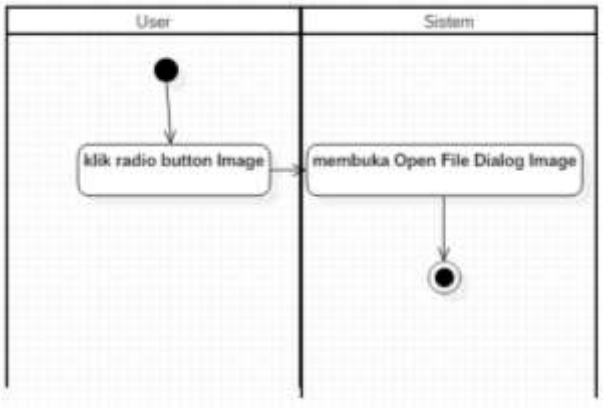
Aktivitas pemilihan input berkas teks adalah aktivitas membuka dialog *OpenFile* teks dan untuk memilih input teks.



Gambar 2. Diagram Aktivitas Pemilihan Input Berkas Teks

2.2.2. Diagram Aktivitas Pemilihan Input Berkas Image

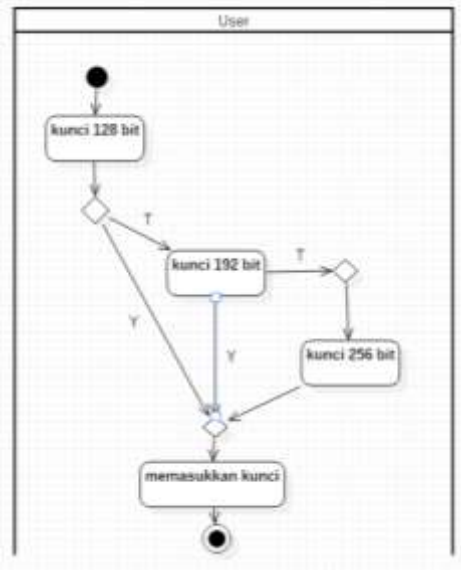
Aktivitas pemilihan input berkas image adalah aktivitas membuka dialog *OpenFile* grafis atau citra dan untuk memilih input grafis atau citra.



Gambar 3. Diagram Aktivitas Pemilihan Input Berkas Image

2.2.3. Diagram Aktivitas Pemilihan Panjang Kunci

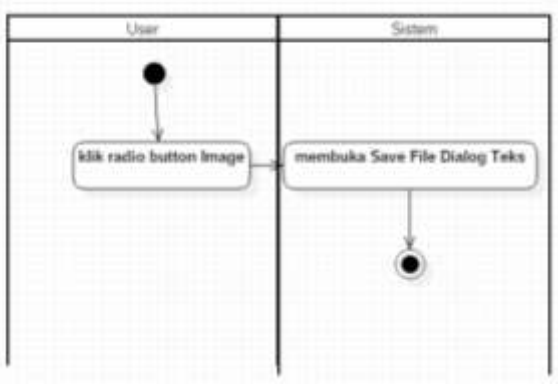
Aktivitas pemilihan panjang kunci adalah aktivitas membuka dialog *OpenFile* teks dan untuk memilih input grafis atau citra.



Gambar 4. Diagram Aktivitas Pemilihan Input Panjang Kunci

2.2.4. Diagram Aktivitas Pemilihan Output Berkas Teks

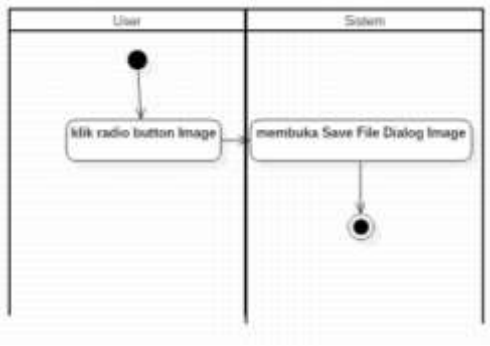
Aktivitas pemilihan output berkas teks adalah aktivitas membuka dialog *SaveFile* teks dan untuk memilih input teks.



Gambar 5. Diagram Aktivitas Pemilihan Output Berkas Teks

2.2.5. Diagram Aktivitas Pemilihan Output Berkas Image

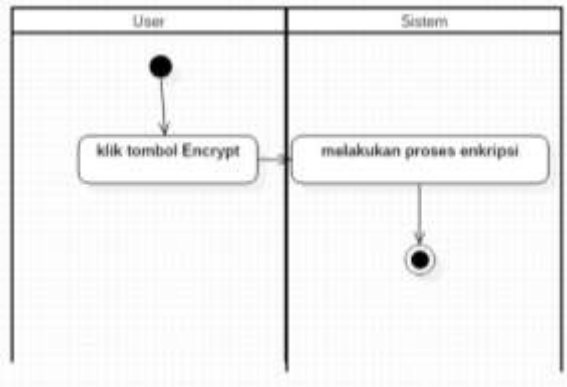
Aktivitas pemilihan output berkas image adalah aktivitas membuka dialog *SaveFile* grafis atau citra dan untuk memilih output grafis atau citra.



Gambar 6. Diagram Aktivitas Pemilihan Output Berkas Image

2.2.6. Diagram Aktivitas Proses Enkripsi

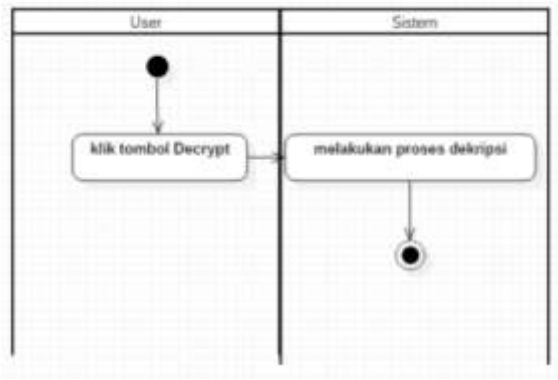
Aktivitas proses enkripsi adalah aktivitas pemrosesan enkripsi input berkas.



Gambar 7. Diagram Aktivitas Proses Enkripsi

2.2.7. Diagram Aktivitas Proses Dekripsi

Aktivitas proses dekripsi adalah aktivitas pemrosesan dekripsi input berkas.

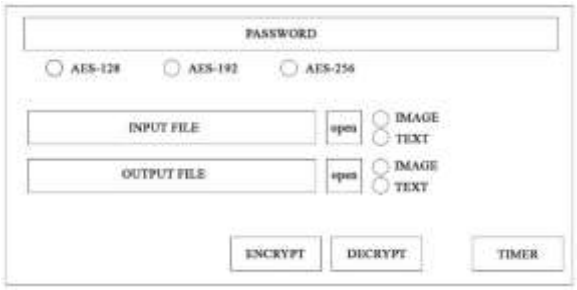


Gambar 8. Diagram Aktivitas Proses Dekripsi

2.3. Perancangan Antarmuka

Navigasi pada antarmuka utama:

1. Klik salah satu *radio button* dari AES-128, AES-192 atau AES-256 untuk memilih panjang kunci yang akan digunakan. AES-128 untuk panjang kunci 16 bit. AES-192 untuk panjang kunci 24 bit. AES-256 untuk panjang kunci 32 bit.
2. Klik salah satu *radio button* dari Image atau Text pada Input File, maka akan muncul antarmuka membuka berkas.
3. Klik salah satu radio button dari Image atau Text pada Output File, maka akan muncul antarmuka menyimpan berkas.
4. Klik tombol Encrypt untuk memulai proses enkripsi.
5. Klik tombol Decrypt untuk memulai proses dekripsi.
6. Timer akan mulai menghitung waktu setelah tombol Encrypt atau Decrypt ditekan dan otomatis berhenti saat proses enkripsi atau dekripsi selesai.



Gambar 9. Antarmuka Utama

3. Hasil dan Analisis

3.1. Perbandingan Kecepatan Enkripsi Dekripsi Tiga Variasi AES

Grafik perbandingan kecepatan enkripsi dan dekripsi menggunakan 30 data uji dengan tiga variasi AES ditunjukkan pada Gambar 4.56, dapat dilihat bahwa untuk melakukan proses enkripsi teks, AES-128 membutuhkan waktu rata-rata 11,57 ms, AES-192 membutuhkan waktu rata-rata 12,4 ms dan AES-256 membutuhkan waktu rata-rata 19,87 ms. Untuk dekripsi teks, AES-128 membutuhkan waktu rata-rata 10,33 ms, AES-192 membutuhkan waktu rata-rata 10,77 ms dan AES-256 membutuhkan waktu rata-rata 11,03 ms. Dapat disimpulkan bahwa baik proses enkripsi maupun dekripsi teks, AES-128 adalah yang paling cepat, sedangkan AES-256 adalah yang paling lambat.

Untuk proses enkripsi citra, AES-128 membutuhkan waktu rata-rata 22,07 ms, AES-192 membutuhkan waktu rata-rata 22,7 dan AES-256 membutuhkan waktu rata-rata 23,6 ms. Untuk dekripsi citra, AES-128 membutuhkan waktu rata-rata 10,57 ms, AES-192 membutuhkan waktu 11,9 ms dan AES-256 membutuhkan waktu 13,83 ms. Dapat disimpulkan bahwa baik proses enkripsi maupun dekripsi citra, AES-128 adalah yang paling cepat, sedangkan AES-256 adalah yang paling lambat.

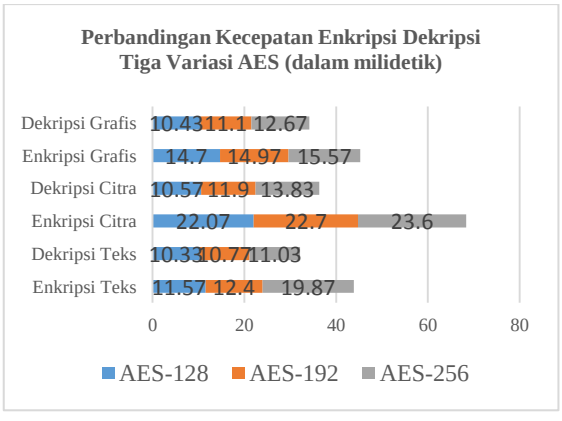
Untuk proses enkripsi grafis, AES-128 membutuhkan waktu rata-rata 14,7 ms, AES-192 membutuhkan waktu rata-rata 14,97 dan AES-256 membutuhkan waktu rata-rata 15,57 ms. Untuk dekripsi grafis, AES-128 membutuhkan waktu rata-rata 10,43 ms, AES-192 membutuhkan waktu 11,1 ms dan AES-256 membutuhkan waktu 12,67 ms. Dapat disimpulkan bahwa baik proses enkripsi maupun dekripsi grafis, AES-128 adalah yang paling cepat, sedangkan AES-256 adalah yang paling lambat.

Alasan mengapa berkas teks dapat dienkripsi lebih cepat daripada berkas citra maupun grafis adalah berkas teks dienkripsi tanpa perlu melakukan konversi. Sedangkan pada berkas citra maupun grafis membutuhkan waktu yang lebih banyak karena harus dikonversi dulu menjadi byte.

Dekripsi dari hasil enkripsi teks memerlukan waktu yang lebih cepat daripada dekripsi dari hasil enkripsi berkas citra dan grafis. Hal ini disebabkan oleh hasil dekripsi teks tidak memerlukan konversi. Sedangkan hasil dekripsi citra dan grafis harus dikonversi menjadi citra dan grafis kembali sehingga memerlukan waktu lebih.

Hal ini mirip dengan proses encoding atau penyandian dan decoding dan pengawasandian pada suatu berkas. Proses penyandian adalah proses mengubah suatu informasi menjadi bentuk lain agar bisa dikodekan. Sedangkan proses pengawasandian adalah proses kebalikannya, yaitu konversi kembali ke dalam bentuk asli.

Grafik perbandingan kecepatan enkripsi dan dekripsi tiga variasi AES dapat dilihat pada Gambar 10.



Gambar 10. Grafik Perbandingan Kecepatan Enkripsi Dekripsi Tiga Variasi AES

4. Kesimpulan

Berdasarkan uraian dan hasil analisis yang telah dilakukan selama pengerjaan aplikasi enkripsi dan dekripsi AES ini, dapat diambil kesimpulan bawha hasil enkripsi AES dengan ketiga variasi kunci terhadap berkas teks, citra dan grafis tidak mengubah besar ukuran pada berkas tersebut, begitupun juga dengan berkas hasil dekripsi tidak mengubah besar ukuran pada berkas.
Untuk enkripsi dan dekripsi menggunakan panjang kunci 128 bit membutuhkan waktu paling cepat, yaitu rata-rata 16,11 ms untuk enkripsi dan 10,44 ms untuk dekripsi. Enkripsi dan dekripsi menggunakan panjang kunci 192 bit membutuhkan waktu rata-rata 16,69 ms untuk enkripsi dan 11,26 ms untuk dekripsi. Sedangkan enkripsi dan dekripsi yang menggunakan panjang kunci 256 bit membutuhkan waktu paling lama, yaitu rata-rata 19,68 ms untuk enkripsi dan 12,51 ms untuk dekripsi.

Untuk ukuran berkas teks, citra dan grafis yang sama, waktu enkripsi paling cepat adalah berkas teks, karena tidak memerlukan konversi. Sementara untuk berkas grafis dan citra memiliki waktu enkripsi yang relatif sama, karena sama-sama memerlukan konversi menjadi byte terlebih dahulu.

Untuk ukuran berkas teks, citra dan grafis yang sama, waktu dekripsi paling cepat adalah berkas teks, karena tidak memerlukan konversi. Sementara untuk berkas grafis dan citra memiliki waktu dekripsi yang relatif sama, karena sama-sama memerlukan konversi menjadi citra dan grafis.

Sebagai saran untuk pengembangan aplikasi enkripsi dan dekripsi AES ini adalah perlu dilakukan penelitian lanjutan untuk melakukan enkripsi dan dekripsi pada berkas multimedia lainnya, misal video dan audio, serta perlu dilakukan penelitian lanjutan untuk mengembangkan sistem enkripsi dan depkripsi pada perangkat bergerak, misalkan yang berbasis Android dan iOS.

Referensi

[1]. Goldreich, Oded. 2001. *Foundations of Cryptography, Volume 1: Basic Tools*. Cambridge University Press.
[2]. Kurniawan. 2004. *Kriptografi: Keamanan Internet dan Jaringan Komunikasi*. Bandung: Informatika.
[3]. National Institute of Standards and Technology. 2000. *Advanced Encryption Standard, FIPS-197*, (Online), (http://csrc.nist.gov/archive/aes/index.html.)
[4]. Singh, Simon. 2000. *The Code Book*. New York: Anchor Books.
[5]. Stinson, Doug. 2000. *Cryptography, Theory and Practice*. CRC Press.
[6]. Symantec. 2015. *Internet Security Threat Report volume 20.*