ISSN: 2407 - 3911

Implementasi Algoritma Rijndael Dalam Keamanan Data Format Multimedia

Andy Wijaya[1], Lukman Hakim[2]
Teknik Informatika [1,2]
Universitas Bunda Mulia
Jl. Lodan Raya no 2, Ancol, Jakarta Utara 14430
andyw.rwglc@gmail.com [1], lhakim@bundamulia.ac.id [2]

Abstrak

Data multimedia seperti gambar, video dan suara adalah format data yang sering di gunakan di dunia informasi ini untuk memberikan informasi kepada individu lain atau kelompok dengan mudah karena dapat di akses menggunakan banyak perangkat dimana saja. Karena itu dibutuhkan pengamanan data yang aman sehingga keamanan yang data dapat dijaga dengan baik dan di tujukan pada individu atau kelompok yang tepat. Sangat berbahaya apabila data tersebut jatuh kepada orang yang salah dan tidak bertanggung jawab. Kejahatan dalam dunia teknologi memungkinkan peretas untuk mendapatkan informasi berbasis multimedia dari perangkat teknolgi seperti telefon genggam, penyimpanan daring, email, dll. Kemudahan dalam membaca informasi berbentuk multimedia merupakan salah satu kelemahan dari informasi berformat multimedia, karena itu diperlukan proses enkripsi dalam upaya mengamankan pengiriman dan penyimpanan data berformat multimedia didalam perangkat penyimpanan anda maupun saat berbagi informasi tersebut melalui pesan elektronik. Salah satu metode enkripsi yang dapat di terapkan adalah algoritma rijndael dimana algoritma ini dapat memberikan kata sandi untuk informasi yang inginkan sehingga penyimpanan dan pembagian informasi berbasis multimedia dapat dilakukan dengan aman dan tepat menuju individu atau kelompok yang dituju. Saat informasi berbasis multimedia yang telah di enkripsi diterima oleh seseorang maka individu tersebut harus melakukan proses dekripsi terhadap informasi tersebut dengan cara memasukan kata sandi yang telah dibuat oleh pengirim, bila individu tersebut tidak mengetahui kata sandi tersebut, maka informasi tersebut tidak akan dapat diakses oleh individu tersebut.

Kata kunci : multimedia, enkripsi,rijndael.

Abstract

Multimedia data such as images, video, and audio are data formats that are often used in this world to easily provide information to another individual because they can be accessed with many device anywhere. Therefore, it is necessary to secure data security so that data security can be maintained properly and directed to the right person or group. It's very dangerous if the data information falls to the wrong and irresponsible person. The ease of reading information in the form of multimedia is one of the weaknesses of multimedia format information, Therefore, an encryption process is needed in an effort to secure the sending and storing of multimedia format data in your storage device or when sharing that information via electronic messages. One of the encryption methods that can be applied is the rijndael algorithm where we can give a password for the information we want, so that keeping and sharing of multimedia-based information can be done safely and precisely to the target group or individual. When multimedia-based information that has been encrypted is received by someone, the individual must carry out the decryption process of the information by entering the password that has been made by the sender, if the individual does not know the password, then the information will not be accessible to individuals that.

Keyword : multimedia, encryption,rijndael.

I. PENDAHULUAN

1.1 Latar Belakang

Multimedia adalah salah satu media yang sangat sering dijumpai pada kehidupam sehari-hari. Multimedia merupakan salah satu wadah untuk berbagi informasi dari individu ke individu maupun individu ke kelompok.

Pengiriman informasi berbasis multimedia memudahkan manusia dalam memahami isi dari

sebuah informasi seperti mendengarkan pesan suara, memutar video, melihat gambar, dll. Pengiriman informasi berbasis multimedia juga sangat praktis karena format multimedia dapat di buka hampir di semua perangkat.

Dengan berkembangnya perangkat pemutar multimedia, pertukaran informasi berbasis multimedia ini harus dijaga dengan baik, Karena informasi berbasis multimedia sangat mudah untuk diakses siapa saja dan dimana saja.

Fatalnya penyalahgunaan multimedia sangat pesat di era ini menjadi salah satu perhatian dalam pengamanan data berformat multimedia harus diperhatikan salah satunya adalah dengan cara mengenkripsi data tersebut agar tidak dapat dilihat oleh orang umum atau yang tidak di inginkan.

II. KAJIAN LITERATUR

II.1 Multimedia

Multimedia adalah penyamapian suatu informasi dengan menggunakan media gambar, text, suara, video atau animasi.

Multimedia telah sering ditemukan dalam kehidupan manusia, mulai dari hiburan, pendidikan, iklan, dan lain-lain. Multimedia dapat dijumpai saat musik sedang di putar, video di tv, poster pada majalah, dll.

II.2 Kriptografi

Menurut Kriptografi (*cryptographi*) berasal dari BahasaYunani: "*cryptos*" artinya "*secret*" (rahasia), sedangkan "*graphein*" artinya "*writing*" (tulisan). Sehingga kriptografi berarti "*secret writing*" (tulisan rahasia), menurut (Prasetyo & Hikmawan, 2016)

Jadi kriptografi dapat di artikan sebagai ilmu untuk menjaga keamanan dari suatu data atau informasi dengan cara mengenkripsi data atau informasi tersebut agar hanya orang yang di tuju yang dapat melihat isi konten dari data tersebut.

Teknik enkripsi yang di lakukan adalah dengan menyandikan data sebelumnya yang telah di tambahkan dengan kata sandi sehingga untuk mengakses data tersebut di butuhkan kata sandi untuk mendekripsi kembali data tersebut.

Dalam kriptografi, terdapat beberapa istilah yang sering di gunakan yaitu :

- Enkripsi
  Mengubah sebuah informasi ke bentuk lain yang tidak dapat di mengerti.
- Dekripsi
  Kebalikan dari enkripsi, dekripsi merupakan proses untuk mengembalikan sebuah informasi yang telah di enkripsi sehingga informasi tersebut dapat di pahami kembali maknanya.

- Kunci
  Sebuah karakter yang di gunakan untuk meng enkripsi dan denkripsi suatu informasi sehingga di butuhkan kunci untuk mengubah informasi yang dapat dapat di pahami menjadi data yang tidak dapat di pahami, begitu juga sebaliknya. (Alim & Cancer, 2016)

II.2 Data

Data adalah fakta mentah yang masih belum diolah sehingga masih belum mempunyai nilai yang selanjutnya akan di olah menjadi informasi.

Data dapat berupa karakter, simbol, gambar, tanda, tulisan, suara, angka sesui dengan fakta yang ada.

II.3 Informasi

Infomasi adalah hasil proses atau hasil pengolahan data meliputi : Hasil gabungan, hasil analisa, hasil penyimpulan, dan hasil pengolahan system informasi komputerisasi

II.4 Algoritma rijndael

Rijndael merupakan salah satu algoritma enkripsi yang bersifat simetri, dengan demikian algoritma rijndael menggunakan 1 buah kunci yang sama dalam proses enkripsi dan dekripsi.

Algoritma ini memiliki panjang kunci128 bit, 192 bit, 256 bit. Pemilihan bit yang di gunakan akan mempengaruhi proses enkripsi dan dekripsi yang terjadi,

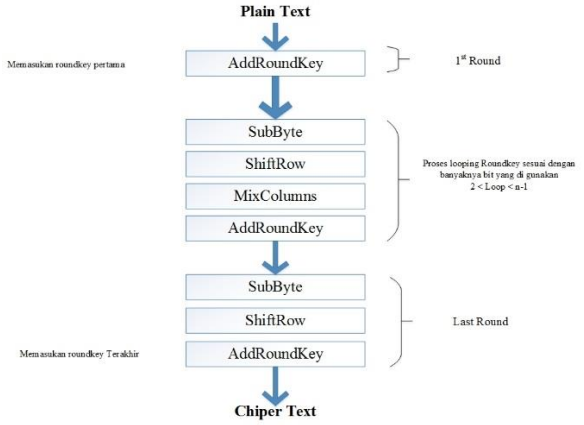
Tabel 1 Jumlah Proses berdasarkan Jumlah Bit

Ukuran Bit	Jumlah Proses
128	10
192	12
256	14

Pada algoritma rijndael terdapat 4 proses transformasi bit yang terjadi, yaitu *SubByte, ShifyRow, MixColumns, AddRoundKey.*

Pada awal enkripsi, Plaintext yang sudah berbentuk array akan mengalami transformasi *AddRoundKey*, lalu array akan mengalami transformasi *SubByte, ShifyRow, MixColumns, AddRoundKey*. Secara terus-menerus sebanyak jumlah bit junci yang di gunakan.

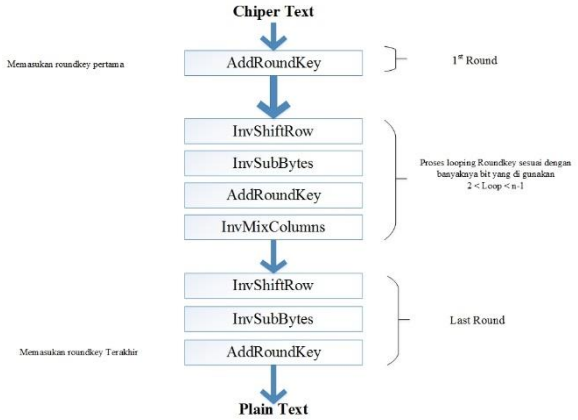
Lalu setelah array melakukan perputaran sampai 2 < loop < n-1, maka array akan memasuki bagian transformasi terakhir yang akan menghasilkan ChiperText, yaitu hasil akhir enkripsi.



Gambar 1. Proses enkripsi pada algoritma rijndael

Setelah *ChiperText* terbentuk, maka cara untuk membaca kembali informasi yang sudah di enkripsi adalah dengan proses dekripsi, yaitu proses mengembalikan *ChiperText* menjadi *PlainText.*

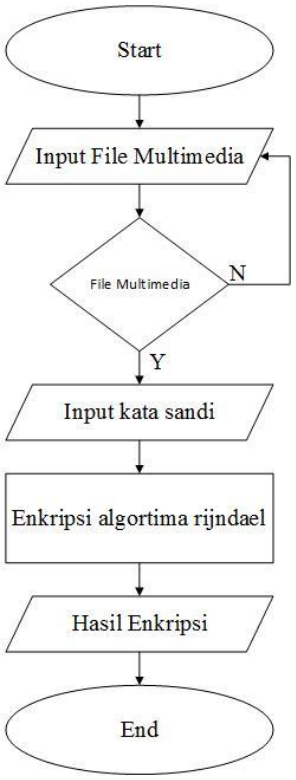
Proses dekripsi yang dilakukan dengan cara melakukan hal yang berlawanan dari proses enkripsi, proses yang dilakukan saat dekripsi meliliki 4 proses yaitu *InvShiftRows, InvSubBytes(), InvMixColumns(), dan AddRoundKey().*



Gambar 2. Proses dekripsi algoritma rijndael

III. ANALISIS DAN PERANCANGAN

III.1 Perancangan Sistem



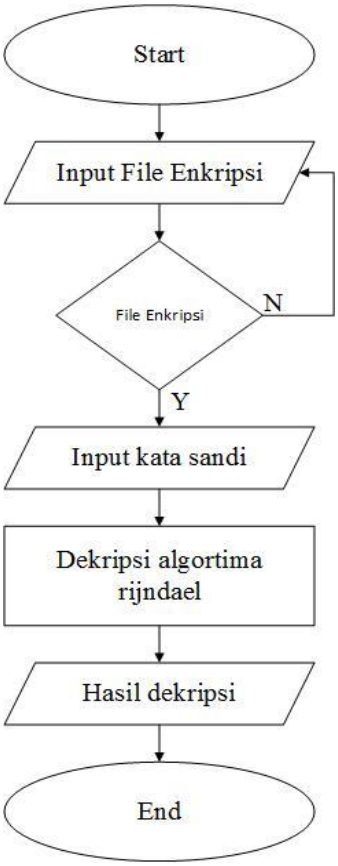
Gambar 3. Proses enkripsi

Flowchart pada gambar 3 menunjukan proses yang perlu di lakukan untuk mengenkripsi sebuah file multimedia. Pertama pengguna harus memilih input berbasis multimedia yang akan di enkripsi, lalu sistem akan memeriksa apakah benar input pengguna adalah file multimedia.

Apa bila file yang di pilih pengguna bukan file multimedia, maka sistem akan meminta kembali user untuk memberikan file multimedia yang akan di enkripsi.

Selanjutnya setelah pengguna memilih file multimedia, maka user dapat memasukan kata sandi yang digunakan untuk mengenkripsi file tersebut.

Setelah itu proses enkripsi akan dimulai dimana algoritma akan berjalan dan pengguna menunggu hasil dari system berupa file yang sudah terenkripsi.



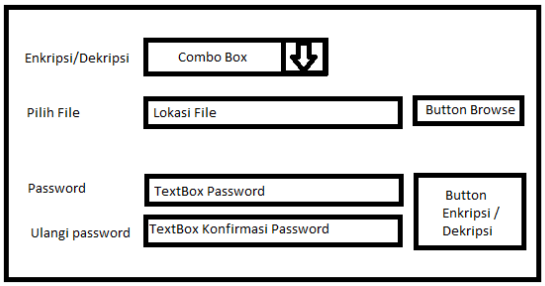
Gambar 4. Proses dekripsi algoritma rijndael

Flowchart pada gambar 4 menunjukan proses yang terjadi saat pengguna ingin melakukan proses dekripsi pada file yang sudah di enkripsi.

pengguna harus memasukan file yang sudah di enkripsi pada input yang di sediakan, lalu system akan memeriksa apakah file tersebut merupakan file multimedia atau bukan.

Selanjutnya pengguna memasukan kata kunci yang digunakan pada saat enkripsi, selanjutnya pengguna hanya menunggu hasil dari dekripsi yang dihasilkan.

III.2 Tampilan Aplikasi

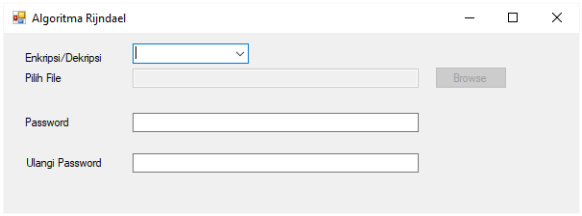


Gambar 5. Tampilan Aplikasi

Gambar 5 menunjukan tampilan awal dari progam saat dijalankan. Combo box untuk memilih perintah enkripsi / dekripsi, tombol untuk mencari file, lalu direktori file tersebut akan di tampilkan pada tectbox lokasi file, 2 buah TextBox dimana textbox atas untuk memasukan kata sandi (ChiperKey) dan TextBox bawah untuk mengkonfirmasi kata sandi tersebut, dan sebuah tombol untuk menjalankan proses enkripsi atau dekripsi.

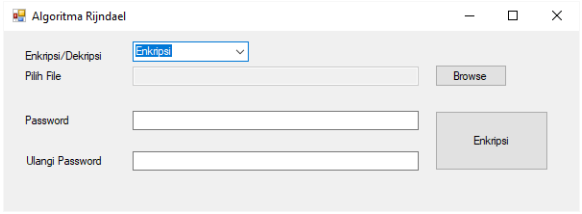
III.3 Tampilan GUI

Pengujian system dilakukan dengan cara menjalankan aplikasi utuk mengetahui keberhasilan dari aplikasi ini.

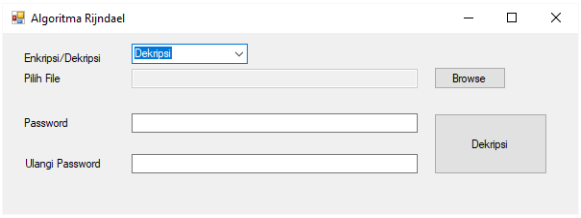


Gambar 6. Tampilan Awal Aplikasi

Pada tampilan awal, user dapat memilih proses yang di inginkan pada combo box.



Gambar 7. Pilihan Enkripsi



Gambar 8. Pilihan Dekripsi

Setelah user memilih proses yang akan di jalankan, maka tombol akan terlihat

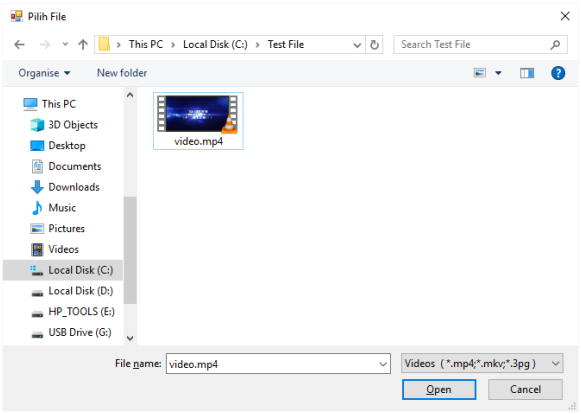
IV. KESIMPULAN DAN SARAN

IV.1 Pengujian Sistem

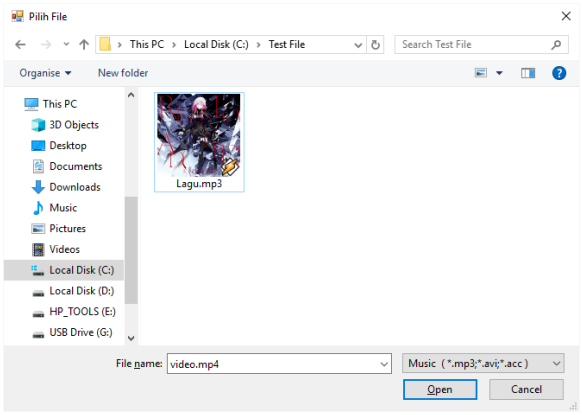
Pengujian system dilakukan dengan cara mengenkripsi dan mendekripi file multimedia yang sudah disiapkan.

Setelah menjalankan aplikasi, pengguna pilih proses enkripsi pada combo box seperti pada gambar 7. Lalu pengguna tekan tombol browse, lalu pilih file yang akan di enkripsi.

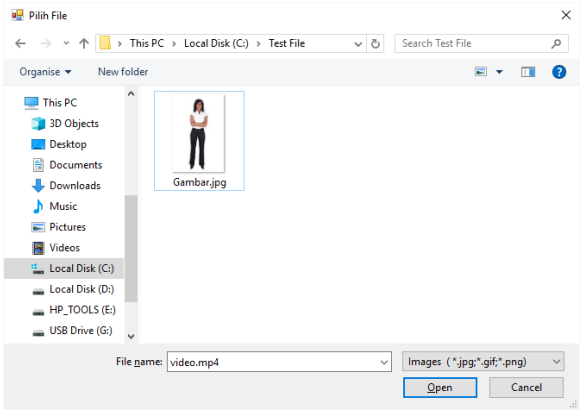
Pada pengujian ini, aka nada 3 file yang akan dip roses yaitu file video, suara, dan gambar. Ketiga file tersebut akan menjalankan proses enkripsi dan dekripsi



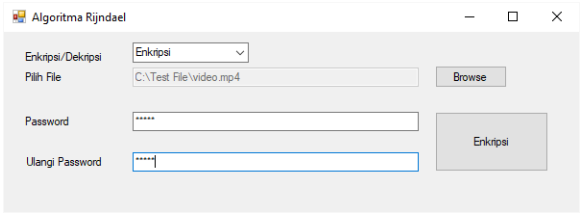
Gambar 9. Pemilihan File Video



Gambar 10. Pemilihan File Suara

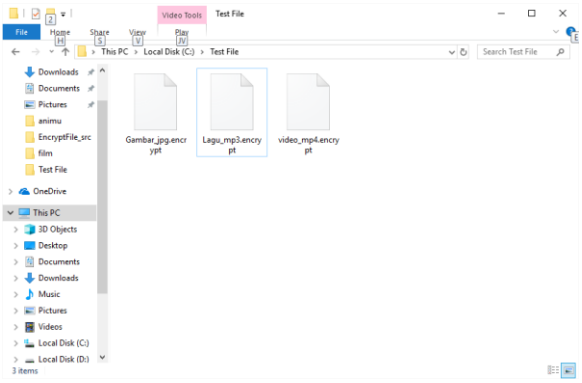


Gambar 11. Pemilihan File Gambar



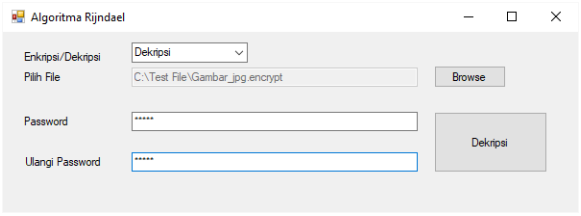
Gambar 12. Input file dan Password Enkripsi

Setelah memilih file masukan password yang akan di gunakan untuk mendekrip file tersebut. Setelah itu tekan enkripsi.

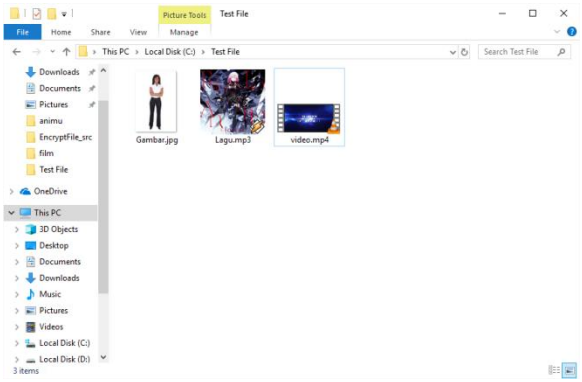


Gambar 13. Hasil Enkripsi

Hasil yang telah ter enkripsi dapat di kembalikan dengan cara menggunakan proses dekripsi dan memasukan password yang digunakan user sebelumnya.



Gambar 13. Input File dan Password Dekripsi



Gambar 13. Hasil Dekripsi

Setelah berhasil mendekripsi file, maka file dapat diakses kembali

IV.3 Kesimpulan

Hasil dari dilakukannya pengujian ini adalah untuk memberikan rasa aman terhadap user dalam membagikan file berbasis multimedia kepada orang lain tampa rasa khawatir akan file tersebut teretas saat pengiriman dan di salah gunakan oleh orang yang tidak bertanggungjawab.

IV.4 Saran

Sebaiknya di penelitian selanjutnya aplikasi ini dapat dikembangkan untuk mengenkripsi format data yang lebih luas sehingga tidak terpaku pada file berbasis multimedia

REFERENSI

Alim, Z., & Cancer, Y. (2016). meningkatkan keamanan data **cloud computing** menggunakan algoritma rijndael. *Jurnal TI , Vol. V No 1*, 2.

JB, K., & Aditya, S. (2012). Implementasi algoritma rijndael untuk enkripsi dan dan dekripsi pada citra digital. *SNATI 2012*, 3.

Prasetyo, T. F., & Hikmawan, A. (2016). Analisis Perbandingan Dan Implementasi Sistem Keamanan Data Menggunakan Metode Enkripsi R. *Infotech Journal*, 41.

sularsono, e. (2014). Implementasi algoritma rijndael 128 pada aplikasi chatting berbasis html5 websocket . *INFORMATIKA Vol. 10 No. 2, ,* 67.

Surian, D. (2006). algoritma kriptografi rijndael. *TESLA Vol. 8 No. 2 97-101*, 97-101.

wibowo, i. (2009). penerapan algoritma kriptografi asimetris rsa untuk keamanan data di oracle. *JURNAL informatika, volume 5 nomor* , 60.

yuniati, v. (2009). enkripsi dan dekripsi dengan algoritma aes 256 untuk semua jenis file. *jurnal informatika, volume 5 nomor 1, ,* 90.