Paper

Implementasi Kriptografi Triple Des Dan Blowfish Pada Pengamanan File Multimedia Video

Author: Aldi Wahyudi, Sumi Khairani, Dharmawati

ISBN: 978-623-91911-2-2

Implementasi Kriptografi Triple Des Dan Blowfish Pada Pengamanan File Multimedia Video

Aldi Wahyudi[1], Sumi Khairani[2], Dharmawati[3]

[1,2,3]Universitas Harapan, Medan, Indonesia

[1]aldi.binter@gmail.com, [2]sumibintisyaifullah@gmail.com, [3]dharmawati66@yahoo.com

Abstrak- Pengiriman suatu pesan, data dan informasi yang sangat pentingmembutuhkan tingkat keamanan yang tinggi. Dengan perkembangan teknologi informasisekarang ini yang begitu pesat dimana setiap orang akan mudah untuk mendapatkan suatupesan,data daninformasi, terutama video. Video merupakan salah satu konten multimedia yang sering digunakan, menjaga kerahasiaan dari video menjadi hal yang penting agar orang yang tidak berkepentingan tidak dapat melihat pesan yang ada pada video. Salah satu metode yang digunakan untuk mengamankan video yang dapat digunakan yaitu mengguanakan algoritma triple des dan blowfish, kedua algoritma ini adalah metode kriptografi yang menggunakan konsep block chipper dan kriptografi simetris. Kedua algoritma tersebut menjadi acuan dalam pembuatan perangkat lunak enkripsi dan dekripsi pada file video dan melakukan analisa performansi sistem keamanan yang ada, dan melakukan implementasi dengan melakukan pengujian dan pengukuran sistem, dilihat dari segi waktu proses file video enkripsi dan dekripsi. Perancangan aplikasi menggunakan visual basic 2010 yang merupakan sebuah bahasa pemrograman berbasis OOP (Object Oriented Programming) yang memanfaatkan teknologi .NET yang digunakan untuk membuat aplikasi dilingkungan kerja berbasis windows. Aplikasi ini diharapkan dapat menerima implementasi kriptografi triple des dan blowfish pada pengamanan file multimedia video dengan baik dan mampu melaksanakan proses enkripsi dan dekripsi sesuai dengan algoritmanya.

Kata Kunci: *Video,Kriptografi, Triple Des, Blowfish*

Abstract- Sending a message, data and information are very important and requires a high level of security. Developing of information technology is so rapid where everyone will find it is easy to get a message, data and information, especially video. Video is one of the multimedia content often uses. Maintaining the confidentiality of the video is important so that unauthorized people cannot see the message contained in the video. One of the methods used to secure video is using the triple des and blowfish algorithms, both of these algorithms are cryptographic methods that use the concept of block cipher and symmetric cryptography. These two algorithms are used as a reference in making encryption and decryption software for video files and analyzing the performance of existing security systems, and implementing them by testing and measuring the system, in terms of processing time for video files encryption and decryption. The application designed by using Visual Basic 2010 which is a programming language based on OOP (Object Oriented Programming) that utilizes .NET technology which is used to create applications in a Windows-based work environment. This application is expected to be able to accept the implementation of triple des and blowfish cryptography in securing multimedia video files properly and carry out the encryption and decryption process according to the algorithm.

Keywords: *Video,Kriptografi, Triple Des, Blowfish*.

1. PENDAHULUAN

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatudata, pesan dan informasi. Pengiriman suatu pesan, data dan informasi yang sangat pentingmembutuhkan tingkat keamanan yang tinggi. Dengan perkembangan teknologi informasisekarang ini yang begitu pesat dimana setiap orang akan mudah untuk mendapatkan suatupesan,data daninformasi[1].

Perihal keamanan merupakan salah bagian penting untuk sistem informasi. Banyak hal yang terkait tentang kemanan data ataupun bentuk sistem informasi, salah satunya enkripsi. Dengan kata lain enkripsi merupakan sebuah metode yang digunakan untuk mengubah pesan asli menjadi pesan yang sudah dikodekan. Informasi Asli (plaintext) dan bentuk yang sudah dikodekan yaitu ciphertext. Informasi ciphertext memuat informasi dari pesan plaintext, namun tidak dapat dimengerti oleh manusia maupun komputer tanpa menggunakan metode yang sesuai untuk mengerjakan dekripsi[2].

ISBN: 978-623-91911-2-2

Kriptografi berfungsi untuk menyandikan data yang berupa file teks, gambar, audio dan video. File teks dalam penggunaannya lebih sering dijadikan sebagai pesan atau informasi. Akan tetapi dengan berkembangnya teknologi yang semakin memungkinkan pesan atau informasi disimpan dalam bentuk file lain seperti gambar, audio, dan video. Pada dasarnya, data multimedia lebih rentan dibandingkan data digital yang lain. Penerapan keamanan bisa saja nilainya lebih mahal dibandingkan dengan nilai dari data multimedia yang akan diamankan tersebut dalam hal ini video. Hal ini dapat mengakibatkan pemborosan dana. Untuk itu diperlukan suatu proses enkripsi yang dapat memenuhi dua faktor penting dalam enkripsi video yaitu efisiensi dan tingkat kemanan. Enkripsi selektif merupakan suatu metode yang dapat mengatasi permasalahan tingkat keamanan Enkripsi Selektif merupakan sebuah teknik untuk mengenkripsi sebagian data video sedangkan data lainnya dibiarkan sebagaimana adanya [3]. Pada data video, enkripsi selektif dapat mempermudah agar aspek real-time terwujud. Pada enkripsi selektif, algoritma chipper apapun dapat digunakan.

Pemilihan algoritma Triple Des karena tingkat keamanannya termasuk tinggi dengan penggunaan kunci 3 kali lebih panjang dari algoritma Des yaitu sebanyak 168bit. Sehingga waktu yang diperlukan untuk mencoba seluruh kemungkinan kunci oleh serangan brute force adalah sebanyak 1.183×10^{43}.

Algoritma yang kedua adalah algoritma kriptografi Blowfish, algoritma dengan kunci simetris yang dibuat pada tahun 1993 oleh Bruce Schneier sebagai pengganti DES. Di era tersebut, banyak algoritma yang ditawarkan.

Aplikasi ini diharapkan akan mampu melindungi sebuah file video sehingga tidak dapat dibuka dan di dengar oleh pihak yang tidak diinginkan.

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi (Cryptography), berasal dari bahasa yunani, cryptos berarti secrete atau rahasia sedangkan graphein berarati writing atau tulisan[4]. Kriptografi adalah suatu teknik untuk kemanan data saat data ditransfer ketempat lain.

2.2 Kriptografi dan Sistem Informasi

Keamanan menjadi syarat dasar dari suatu sistem informasi. Pada Umumnya informasi hanya mengarah pada sekolompok tertentu. Oleh karena itu penting untuk mencegahnya jatuh ketangan kelompok yang tidak bertanggung jawab[5].

Kriptografi adalah ilmu yang mempelajari macam-macam matematis berhubungan dengan keamanan informasi seperti : Keabsahan, integritas informasi, serta autentikasi data[6].

Ketiga aspek tersebut merupakan tujuan dasar dari sistem kriptografi :

1) Kerahasiaan, adalah layanan yang digunakan untuk melindungi isi dari informasi dari siapapun kecuali yang memiliki otoritas
2) Integritas data, merupakan yang berhubungan dengan keamanan dari perubahan informasi secara tidak sah seperti penyisipan, penghapusan, pensubtitusian data lain ke dalam data yang sebenarnya.
3) Autentikasi, merupakan yang berhubungan dengan pengenalan data mengenai keaslian data, keaslian pengirim, keaslian informasi data.

2.3 Mekanisme Kriptografi

Seiring berkembangnya teknologi informasi, prosedur yang digunakan masih sama, hanya saja penerapan sistem berbeda. Sebelum pembahasan mekanisme kriptografi modern, berikut istilah dasar yang dipakai dalam pembahasan kriptografi[5].

1) Plaintext
   Plaintext (message) merupakan data asli yang dikirim dan dilindungi keamanannya. Data ini merupakan informasi awal.
2) Ciphertext
   Ciphertext merupakan data yang sudah dikodekan sehingga siap untuk dialih tugaskan.
3) Cipher
   Cipher merupakan rangkaian urutan matematis yang berguna untuk memproses pengkodean plaintext menjadi ciphertext.
4) Key
   Key merupakan nilai yang dipakai pada algoritma kriptografi untuk mengacak plaintext sehinggan menghasilkan ciphertext

ISBN: 978-623-91911-2-2

5) Enkripsi
   Enkripsi merupakan cara atau metode untuk mengubah plaintext menjadi ciphertext
6) Dekripsi
   Dekripsi merupakan proses mengubah kembali ciphertext menjadi plaintext sehingga dapat dimengerti kembali oleh pengguna.

2.4 Enkripsi dan Dekripsi

Pada dasarnya metode kritptografi meliputi dua proses yakni enkripsi dan dekripsi, kedua prosedur tersebut akan dijelaskan sebagai berikut ini(Permana, 2018:111).

2.5 Algoritma Kriptografi

Menurut kunci yang digunakan, algoritma kriptografi dibedakan atas dua kelompok, yaitu kunci simetris dan kunci asimetris.

2.6 Algoritma Triple Des

Algoritma Triple DES tergolong algoritma blok (Block Chiper) dengan dasar kunci simetris. Triple DES merupakan kesatuan dari algoritma DES (Data Encryption Standard). Triple Des memiliki konsep yang sama dengan DES dimana perbedaan hanya terletak pada kunci yang ditampung. DES hanya mampu menampung kunci sebanyak 56bit) sedangkan Triple Des menampung kunci 3 kali lebih panjang dari DES, yaitu 168bit.

2.7 Algoritma Blowfish

Blowfish merupakan proses menyandikan data (enkripsi) kelompok Symmetric Cryptosystem. Yang buat oleh Bruce Schneier. Blowfish tercatat dalam enkripsi cipher block 64-bit menggunakan panjang kunci yang beragam dari 32 bit hingga 448 bit. Algoritma Blowfish meliputi dua bagian [8] yaitu :

1) Key expansion
   Digunakan untuk mengubah kunci (terkecil 32 bit. Terbesara 448 bit) menjadi sebagian penyimpanan beberapa data, dengan pembagian kunci dengan jumlah 4168 byte.
2) Enkripsi Data
   Meliputi perulangan fungsi biasa (Feistel Network) sejumlah 16 perulangan. Setiapan perulangan meliputi dari pergantian kunci dan penukaran kunci.

2.8 Teori Angka

Kriptografi tidak terlepas dari ilmu matematika. Untuk itu di bawah ini dijelaskan tentang berbagai dasar matematika yang digunakan dalam kriptografi.

3. HASIL DAN PEMBAHASAN

3.1 Perancangan Antarmuka Sistem (Interface)

Perancangan ini bertujuan untuk merancang tampilan dari suatu perangkat lunak dibuat berdasarkan kepentingan*user*. Berikut perancangan antarmuka aplikasi enkripsi dan dekripsi pesan video menggunakan algoritma Triple DES dan Blowfish.

3.2 Halaman Utama

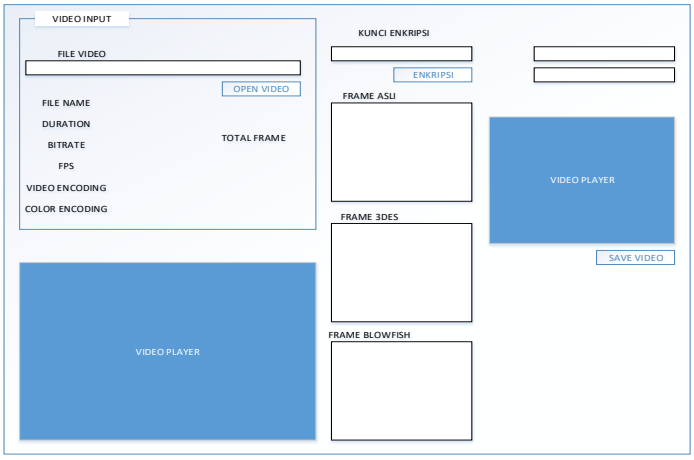
Halaman yang akan pertamakali muncul ketika pengguna memulaiaplikasi enkripsi dan dekripsi Triple DES dan Blowfish. Pada tampilan ini akan membawa pengguna pada pemilihan proses yang akan dilakukan oleh pengguna.

ISBN: 978-623-91911-2-2

Gambar 1. Halaman Utama Aplikasi

3.3 Halaman Enkripsi

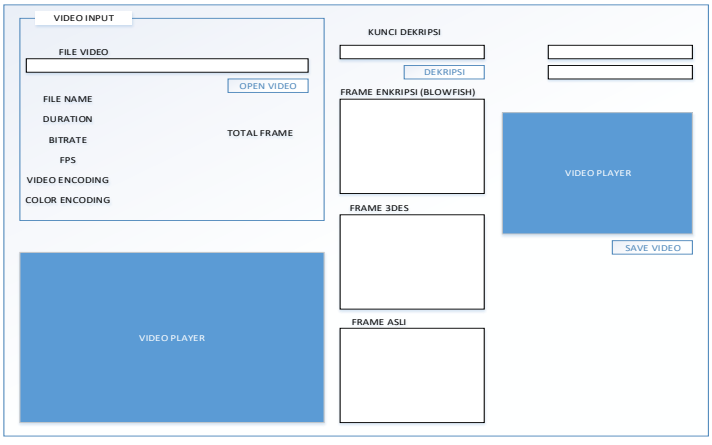
Halaman enkripsi merupakanhalaman yang dipakai oleh user agar dapat mengerjakan enkripsi dan juga pada halaman ini pengguna dapat melakukan analisis frekuensi pada plain video yang akan melewati proses enkripsi pada sistem.



Gambar 2. Halaman Proses Enkripsi

3.4 Halaman Dekripsi

Halaman ini merupakan halaman di mana pengguna akan melakukan proses dekripsi pada file chiper video dari proses enkripsi sebelumnya. Halaman ini akan digunakan untuk mengembalikan data menjadi plain video sebelum file mengalami proses enkripsi dan menjadi chiper video. pengguna perlu memastikan bahwa data chiper video yang digunakan akan sesuai dengan algoritma yang digunakan saat proses dekripsi dikerjakan.

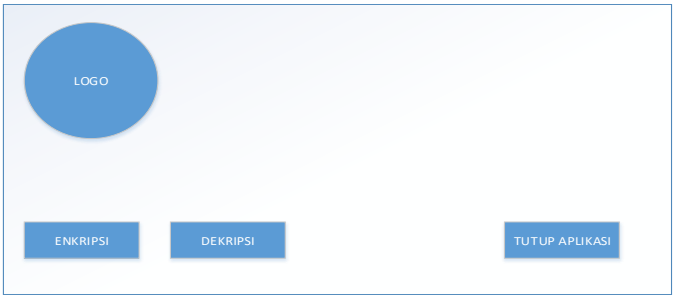


Gambar 3. Halaman Dekripsi

ISBN: 978-623-91911-2-2

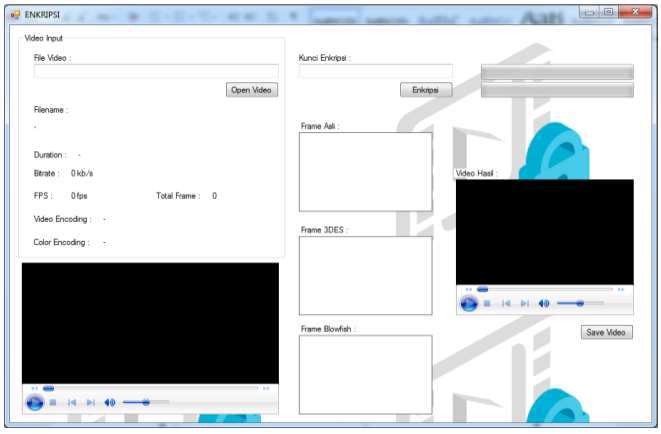
3.5 Implementasi Pengujian Sistem

Langkah pertama dalam pengujian sistem adalah membuka aplikasi, seperti yang bias dilihat padagambar berikut:



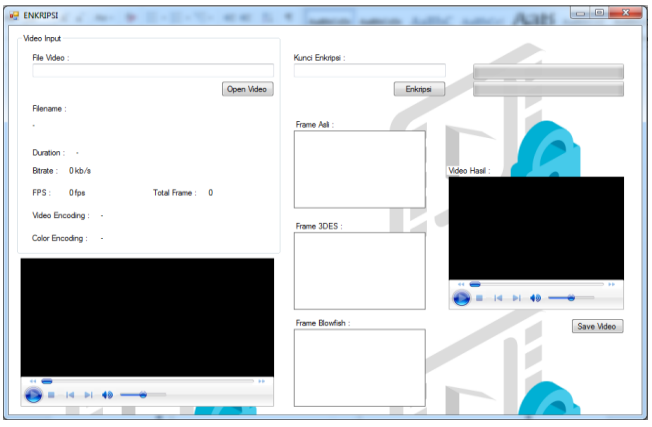
Gambar 4. Halaman Utama Aplikasi

Setelah aplikasi dibuka langkah selanjutnya adalah pemilihan proses yang akan dikerjaka selanjutnya. Untuk memudahkan penggunaan sistem penulis menyarankan untuk pertama kali membuka proses enkripsi terlebih dahulu. Setelah proses enkripsi dipilih pengguna akan dipindahkan kehalaman khusus enkripsi. Pada halaman ini pengguna akan bisa memiih untuk melakukan proses enkripsi yang mana terlebih dahulu. Berikut tampilan dari halaman enkripsi:



Gambar 5. Halaman Proses Enkripsi

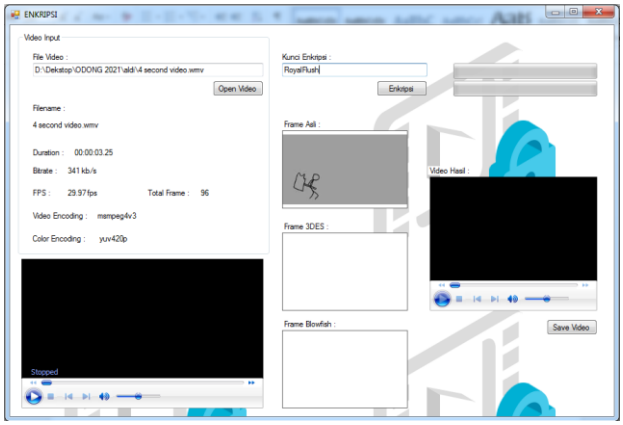
Setelah aplikasi dibuka langkah selanjutnya adalah pemilihan proses yang akan dikerjaka selanjutnya. Untuk memudahkan penggunaan sistem penulis menyarankan untuk pertama kali membuka proses enkripsi terlebih dahulu. Setelah proses enkripsi dipilih pengguna akan dipindahkan kehalaman khusus enkripsi. Pada halaman ini pengguna akan bisa memiih untuk melakukan proses enkripsi yang mana terlebih dahulu. Berikut tampilan dari halaman enkripsi:



Gambar 6. Halaman Proses Enkripsi

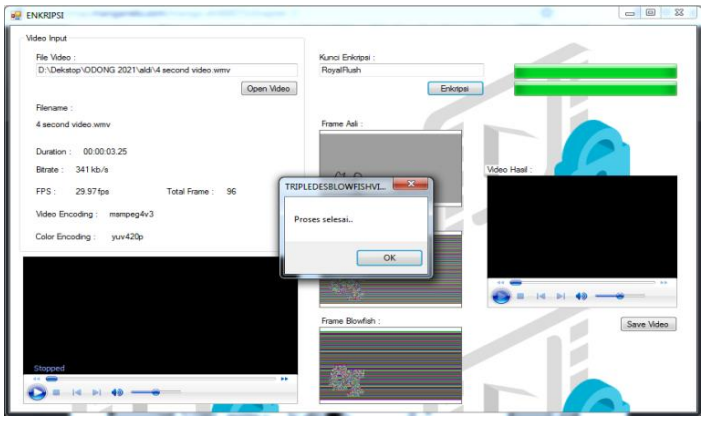
ISBN: 978-623-91911-2-2

Selanjutnya pada tahapan ini pengguna wajib melakukan*input file* plain video yang akan digunakan sebagai bahan enkripsi. Disini telah disiapkan bahan video .wmv. Dan selanjutnya akan dilakukan proses enkripsi menggunakan *file* video "4 second video.wmv" tahapan berikutnya yaitu memasukkan data video percobaan yang terlihat pada ilustrasi dibawah :



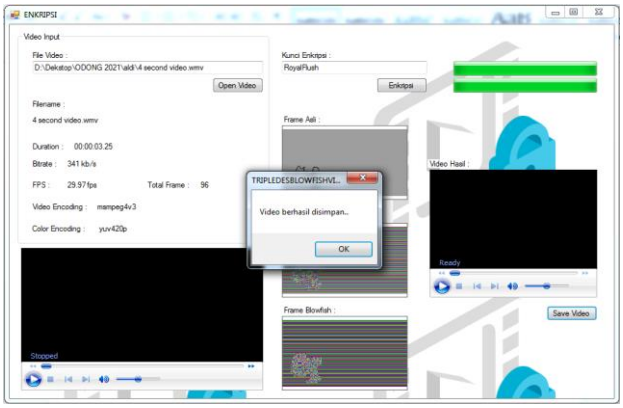
Gambar 7. *Input* Video Uji Kedalam Sistem

Langkah selanjutnya adalah melakukan enkripsi pada data video uji dapat diamati dengan ilustrasi dibawah ini:



Gambar 8. Proses Enkripsi *Triple* DES dan *Blowfish* Berhasil

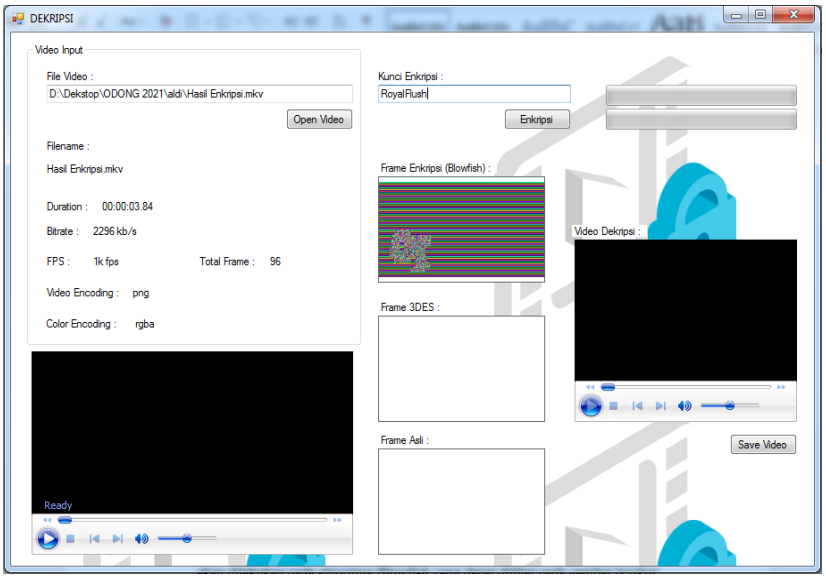
Ilustrasi diatas memperlihatkan bahwa proses enkripsi masing-masing algoritma dapat berjalan dengan baik. Pada proses enkripsi kedua algoritma menggunakan data video uji yang sama dimana hasil enkripsi dari algoritma *Triple* DES akan dilanjutkan proses enkripsinya dengan menggunakan algoritma *Blowfish*, dan juga kedua algoritma menggunakan kunci enkripsi yang sama yaitu "*RoyalFlush*". Sesudah prosedur enkripsi berakhirtahapan berikutnyayaitu menyimpan hasil video hasil enkripsi dan kemudian melanjutkan uji coba pada proses dekripsi:



Gambar 9. Analisis Frekuensi *Triple* DES

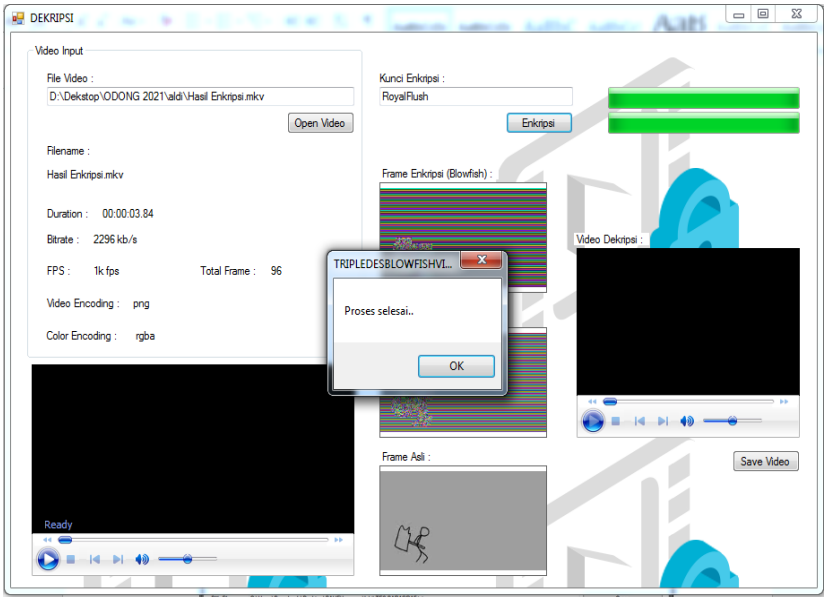
ISBN: 978-623-91911-2-2

Selanjutnya untuk memastikan bahwa sistem yang menggunakan algoritma kriptografi *Blowfish* dan juga *Triple* DES dapat dikategorikan sebagai sistem kriptografi yang berhasil, data hasil enkripsi harus bisa dikembalikan ke kondisi awal dengan melewati proses dekripsi, berikut proses dekripsi pada sistem:



Gambar 10. Dekripsi *Triple* DES

Pada gambar diatas dapat dilihat proses dekripsi dengan menggunakan kunci "*RoyalFlush*" telah berhasil mengembalikan *chiper* video kembali menjadi *plain* video sehingga dapat diambil kesimpulan bahwa algoritma kriptografi *Triple* DES berhasil diimplementasikan dengan baik pada sistem. Selanjutnya pengujian akan dilakukan terhadap algoritma *Blowfish* yang dapat diamati pada ilustrasi berikut:



Gambar 11. Dekripsi *Blowfish*

Gambar diatas dapat dilihat bahwa *chiper* video yang dihasilkan oleh algoritma kriptigrafi *Blowfish* juga berhasil mengembalikan kondisi *chiper* video kembali menjadi *plain* video dengan menggunakan kunci "*RoyalFlush*". Berdasarkan data tersebut maka algoritma kriptografi *Blowfish* juga dapat dinyataan berhasil diimplementasikan dengan baik kedalam sistem.

Ukuran *file* pada setiap langkah atau tahap akan berubah karena proses dari masing-masing algoritma berbeda, dimana pada proses enkripsi dan dekripsi akan membuat *file* asli menjadi *file* yang disandikan dan akan diubah kembali menjadi *file* yang dapat dimengerti. Pada proses ini *file* video bisa menjadi lebih besar, di karenakan *file* enkripsi dan dekripsi disimpan menggunakan ekstensi yang berbeda.

ISBN: 978-623-91911-2-2

4. KESIMPULAN

Dalam perancangan, pembuatan, dan pengujian aplikasi Implementasi Kriptografi Triple DES dan Blowfish Pada Pengamanan File Multimedia Video terdapat beberapa kesimpulan diantaranya adalah sebagai berikut :

1. Sistem dapat menerima implementasi Kriptografi Triple DES dan Blowfish Pada Pengamanan File Multimedia Video dengan baik dan mampu melaksanakan proses enkripsi dan dekripsi sesuai dengan algoritmanya.
2. Besaran data frame dari tiap-tiap video berperan besar terhadap kemampuan kecepatan proses enkripsi dan juga dekripsi system. Pada dasarnya system mampu melakukan enkripsi dan dekripsi namun jumlah file video (frame rate dalam video) adalah faktor utama dalam kecepatan proses.
3. Dengan menggunakan video ekstensi .wmv penulis dapat melakukan uji coba enkripsi dan dekripsi dengan baik, dan system yang dirancang mampu memberikan keamanan tambahan bagi data.
4. Dengan menggunakan video ekstensi .wmv penulis dapat melakukan uji coba enkripsi dan dekripsi dengan baik, dan system yang dirancang mampu memberikan keamanan tambahan bagi data.
5. Dengan menggunakan algoritma Triple Des dan Blowfish pada pengamanan file multimedia video dapat diketahui ukuran file video sebelum (asli) dan sesudah proses enkripsi mengalami penambahan ukuran file pada video asli karena hasil disimpan dalam ekstensi yang berbeda.

UCAPAN TERIMAKASIH

Terima kasih disampaikan kepada pihak-pihak yang telah mendukung terlaksananya penelitian ini.

DAFTAR PUSTAKA

[1] B. Fachri and R. M. Sembiring, “Pengamanan Data Teks Menggunakan Algoritma DES Berbasis Android,” *J. Media Inform. Budidarma*, vol. 4, no. 1, p. 110, 2020, doi: 10.30865/mib.v4i1.1700.

[2] Y. Yusfrizal, “Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android,” *J. Tek. Inform. Kaputama*, vol. 3, no. 2, pp. 29–37, 2019.

[3] A. Pratama and E. Biham, “Enkripsi Selektif Video MPEG dengan Algoritma Serpent,” *Enkripsi Sel. Video MPEG dengan Algoritm. Serpent 1)*, pp. 1–6, 2013.

[4] M. Arifin and Mufti, “Implementasi Kriptografi Chatting Menggunakan Metode Vigenere Dan Aes 128 Berbasis Web,” *Skanika Vol. 1 No. 1 Maret 2018*, vol. 1, no. 1, pp. 102–109, 2018.

[5] H. Situmorang, “Keamanan Basis Data dengan Teknik Enkripsi,” *Mahajana Inf.*, vol. 1, no. 1, pp. 22–27, 2016.

[6] M. Satria *et al.*, “Perancangan Aplikasi Keamanan Data Dokumen Word dengan Menggunakan Algoritma Triple DES,” *J. FTIK*, vol. 1, no. 1, pp. 463–475, 2020.

[7] S. Suhandinata, R. A. Rizal, D. O. Wijaya, P. Warren, and S. Srinjiwi, “Analisis Performa Kriptografi Hybrid Algoritma Blowfish Dan Algoritma Rsa,” *JURTEKSI (Jurnal Teknol. dan Sist. Informasi)*, vol. 6, no. 1, pp. 1–10, 2019, doi: 10.33330/jurteksi.v6i1.395.

[8] M. Natsir, “Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office Menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java,” *Jurnal*, vol. 6, pp. 2089–5615, 2016.