IMPLEMENTASI KRIPTOGRAFI ALGORITMA RC4 DAN 3DES DAN STEGANOGRAFI DENGAN ALGORITMA EOF UNTUK KEAMANAN DATA BERBASIS DESKTOP PADA SMK AS-SU'UDIYYAH

Zahrul Basim[1)], Painem[2)]
Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : 1411502642@student.budiluhur.ac.id[1)], painem@budiluhur.ac.id[2)]

Abstrak

Informasi adalah suatu hal yang penting sejak jaman dahulu kala. Baik itu berupa gambar, suara, dokumen ataupun teks. Informasi bisa sangat berguna bagi orang yang berhak mendapatkannya. Namun juga bisa berakibat fatal jika diketahui oleh orang yang tidak bertanggung jawab. Dan informasi pada saat ini yang berkembang dengan pesat membuat informasi kita semakin rawan untuk dicuri. Oleh karena itu, demi menjaga kerahasiaan informasi tersebut maka pada penelitian ini dibuatlah sistem pengaman data dengan menerapkan algoritme kriptografi RC4 (Ron's Code 4) dan 3DES (Triple Data Encryption Standard) dan dilanjutkan dengan steganografi EOF (End of File) yang dibuat dengan bahasa pemrograman Java berbasis desktop. Aplikasi ini dapat mengamankan dan menjaga kerahasiaan data atau informasi pada SMK AS-SU'UDIYYAH dari terjadinya pencurian dan manipulasi data oleh pihak yang tidak bertanggung jawab. Data atau informasi yang dapat dienkripsi dan disisipkan berupa soal-soal ujian dan dokumen penting lainnya, sedangkan untuk file penampung data rahasia berupa file video yang berjenis .mp4. Berdasarkan hasil uji coba yang dilakukan, sistem pengaman data ini cukup membantu dalam menjaga kerahasiaan data atau informasi yang disimpan pada SMK AS-SU'UDIYYAH. Dengan menggunakan aplikasi ini, diharapkan pengguna dapat mengenkripsi pesan dan data yang sifatnya rahasia tanpa takut akan ada orang lain yang dapat membaca isi pesan dan data tersebut

.

Kata kunci: Kriptografi, Steganografi, RC4, 3DES, EOF

1. PENDAHULUAN

1.1. Latar Belakang

Kemajuan dan perkembangan teknologi informasi saat ini telah berpengaruh pada setiap aspek kehidupan manusia, yang dapat dengan mudah melakukan pertukaran data pada komputer dalam berbagai bentuk. Pertukaran data atau informasi sudah semakin mudah dilakukan dengan atau tanpa melalui media fisik. Namun keamanan pertukaran data atau informasi tersebut kurang disadari, salah satu dampak negatif dalam perkembangan teknologi adalah adanya pencurian dan manipulasi data atau informasi. Dengan adanya pencurian data atau informasi maka aspek keamanan dalam pertukaran serta penyimpanan data atau informasi dianggap penting.

SMK As-Su'Udiyyah Tangerang Selatan merupakan salah satu sekolah menengah kejuruan yang berkawasan di Kota Tangerang Selatan. Pada suatu sekolah tentunya kita mendapati beberapa soal ujian pada setiap semesternya. Maka, dapat dipastikan bahwa sekolah tersebut memiliki dokumen-dokumen yang bersifat penting dan rahasia sehingga tidak boleh disebarluaskan kepada pihak luar yang tidak bertanggung jawab. Dokumen-dokumen yang bersifat penting dan rahasia yang dimiliki oleh sekolah yang merupakan suatu instansi sangatlah rawan akan terjadinya pencurian data, sehingga dokumen-dokumen yang semestinya diamankan yakni soal-soal ujian. Karena soal-soal ujian yang disimpan dengan begitu saja pada sebuah *file* yang memudahkan untuk dicuri dan disebarluaskan kepada seluruh siswa sehingga mengakibatkan resiko yang cukup fatal bagi sekolah maupun siswa.

Oleh karena itu, demi menjaga kerahasiaan data/informasi tersebut maka pada penelitian ini dibuatlah sistem keamanan data pada SMK As-Su'udiyyah Tanggerang Selatan. Salah satu cara yang digunakan untuk menjamin keamanan data atau informasi adalah dengan menerapkan algoritme kriptografi dan metode steganografi pada SMK As-Su'udiyyah Tanggerang Selatan yang akan di fokuskan pada pengamanan *file*. Sehingga *file* yang tersimpan menjadi lebih aman sampai dengan *file* dapat di akses oleh pihak yang memiliki hak untuk mengakses *file* tersebut.

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah maka dapat dirumuskan sebagai masalah berikut:

1. Bagaimana cara mengamankan isi data khususnya dalam bentuk *file* dokumen pada SMK As-Su'udiyyah dari pencurian data?
2. Bagaimana cara mengembalikan data yang telah di enkripsi menjadi data yang asli tanpa mengalami perubahan?

1.3. Tujuan Penelitian

Tujuan dari penulisan tugas akhir ini adalah mengamankan data rahasia SMK As-Su'udiyyah dari pihak yang tidak bertanggung jawab dengan membuat aplikasi pengamanan data menggunakan metode kriptografi dan steganografi.

1.4. Metode Penelitian

Dalam penelitian ini, beberapa metode digunakan untuk memperoleh informasi yang diperlukan untuk menyelesaikan masalah yang ditemui. Adapun metode–metode ini sebagai berikut:

a. Studi literatur
   Metode ini menggunakan pembelajaran dengan cara mengumpulkan, membaca dan memahami jurnal ilmiah, buku, skripsi, artikel, makalah serta refrensi lain guna mendapatkan informasi yang dibutuhkan dalam menunjang penelitian.
b. Analisa Data
   1) Menganalisa algoritme kriptografi yang digunakan yaitu algoritme RC4 dan 3DES, serta teknik-teknik yang digunakan.
   2) Menganalisa fungsi steganografi EOF, serta teknik-teknik yang digunakan.
c. Perancangan Sistem
   Merancang sistem aplikasi untuk mengimplementasikan algoritme kriptografi RC4 dan 3DES dengan kombinasi steganografi EOF menggunakan bahasa pemrograman Java berbasis *desktop*.
d. Pengujian Sistem
   Metode ini dilakukan dengan menguji dan mengecek jalannya program.

2. LANDASAN TEORI

2.1. Definisi Kriptografi

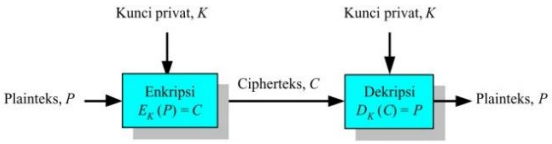
Kriptografi membentuk sebuah sistem yang dinamakan sistem kriptografi. Sistem Kriptografi (*Cryptosystem*) adalah kumpulan dari fungsi enkripsi dan dekripsi yang berkoresponden terhadap kunci enkripsi dan dekripsi. Menurut Katz, kriptografi adalah studi ilmiah atau teknik untuk mengamankan informasi digital, transaksi dan komputasi yang terdistribusi. Kriptografi bertujuan untuk memberikan layanan keamanan sebagai berikut Kerahasiaan (*Confidentiality*) Informasi dirahasiakan dari semua pihak yang tidak berwenang, Keutuhan Data (*Integrity*), Pesan tidak berubah dalam proses pengiriman hingga pesan diterima oleh si penerima, Autentikasi (*Message Autentication*) Kepastian terhadap identitas yang terlibat dan keaslian sumber data, Nirpenyangkalan (*Nonrepudiation*), Setiap entitas yang berkomunikasi tidak dapat menolak atau menyangkal atas data yang telah dikirim atau diterima.

2.2. Teknik Dasar Kriptografi

Algoritma kriptografi terbagi menjadi dua jenis berdasarkan kunci yang digunakan, yaitu Algoritma Simetri dan Algoritma Asimetri[2].

a. Algoritma Simetri

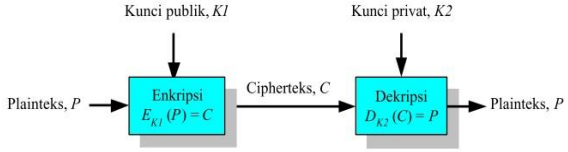
Sistem kriptografi kunci simetri (atau disingkat menjadi "kunci simetri" saja), mengasumsikan pengirim dan penerima pesan sudah menerima kunci yang sama sebelum bertukar pesan. Keamanan algoritma kriptografi simetri terletak pada kerahasiaan kuncinya. Biasanya, *cipher* yang termasuk kriptografi simetri diproses dalam mode blok (*block cipher*), yaitu setiap kali proses enkripsi/dekripsi dilakukan pada satu blok data, atau diproses dalam aliran penyandian (*stream cipher*), yaitu pada setiap proses enkripsi/dekripsi dilakukan terhadap satu bit atau *byte* data. Pada aplikasi kriptografi simetri yang menjadi utama adalah melindungi kerahasiaan data yang dikirim melalui saluran yang tidak aman dan melindungi kerahasiaan data yang disimpan pada media penyimpanan yang tidak aman. [2] Skema proses dari kriptografi simetri dapat dilihat pada Gambar 1:



Gambar 1. Algoritma Kriptografi Simetri

b. Algoritma Asimetri

Pada kriptografi asimetri, kunci/*key* untuk enkripsi bersifat tidak rahasia dan dapat diketahui/digunakan oleh siapapun (publik), sementara kunci/*key* untuk dekripsi bersifat rahasia/privasi yang hanya diketahui oleh penerima pesan. Pada kriptografi asimetri, setiap orang yang menggunakan aplikasi mempunyai sepasang kunci, yaitu kunci rahasia dan kunci publik. Pengirim men-enkripsi pesan dengan menggunakan kunci publik si penerima pesan (*receiver*). Hanya penerima pesan yang dapat men-dekripsi pesan karena hanya ia yang mengetahui kunci rahasianya sendiri.[2] Skema kriptografi dapat dilihat pada Gambar 2:



Gambar 2. Algoritma Kriptografi Asimetri

2.3. Algoritma *Rivest Code* 4 (RC4)

Rivest Code 4 (RC4) pertama kali di temukan oleh Ron Rivest pada tahun 1987 di Laboratorium RSA. RC sendiri memiliki singkatan resmi yaitu "*Rivest Cipher*", namun juga dikenal dengan "*Ron's*

Code". *Rivest Code 4* (RC4) sebenarnya dirahasiakan dan tidak dipublikasikan, tetapi pada tahun 1994, kode tersebut telah dikirim oleh seseorang yang misterius yang disebut *cipher analyst Chypermunks* dan menyebar ke banyak situs internet. Kode yang tersebar tersebut dikonfirmasi sebagai *Rivest Code 4* (RC4) dikarenakan memiliki *output* yang sama dengan *software* berlisensi *Rivest Code 4* (RC4) di dalamnya. Karena algoritma *Rivest Code 4* (RC4) sudah diketahui, *Rivest Code 4* (RC4) tidak lagi menjadi rahasia dagang. Nama *Rivest Code 4* (RC4) diberi hak paten, sehingga disebut "ARCFOUR" atau "ARC4" (Alleged RC4) untuk menghindari pelanggaran hak paten. RSA Security merilis secara tidak resmi algoritma tersebut, namun Ron Rivest yang telah merilisnya secara pribadi dengan menggunakan Wikipedia Inggris ke catatan yang ia punya. *Rivest Code 4* (RC4) telah menjadi bagian dari protokol enkripsi dan sering digunakan. Faktor utama yang menjadi kesuksesan *Rivest Code 4* (RC4) adalah kecepatannya dan kesederhanaannya dalam implementasi pada banyak aplikasi, sehingga mudah untuk dikembangkan implementasi yang efisien ke *software* dan *hardware*. Algoritma *Rivest Code 4* (RC4) adalah salah satu algoritma kriptografi simetri. Disebut sebagai algoritma kriptografi simetri dikarenakan memiliki kunci yang sama untuk men-enkripsi atau men-dekripsi suatu pesan, data, ataupun informasi[11].

Algoritma RC4 menggunakan dua buah S-Box *array* dengan panjang 256 dan berisi permutasi dari bilangan 0 hingga 255, dan S- Box kedua, yang berisi hasil permutasi merupakan fungsi dari kunci dengan panjang yang bervariasi. Cara kerja algoritma RC4 yaitu inisialisasi S-Box pertama, S[0], S[1], S[2],..., S[255], dengan bilangan 0 hingga 255. Pertama S-Box diisi secara berurutan dengan S[0] = 0, S[1] = 1, S[2] = 2,...,S[255] = 255. Kemudian menginisialisasi *array* kedua (S-Box kedua), misalkan *array* K dengan panjang 256. Isi *array* K dengan kunci yang diulangi sampai seluruh *array* K[0], K[1],...,K[255] telah terisi seluruhnya[10].

1) Proses inisialisasi S-Box (*Array* S) inilialisasi dengan persamaan berikut:

   ***for* i = 0 to 255**
   S[i] = i (1)

2) Selanjutnya proses inisialisasi S-Box (*Array* K) dengan persamaan berikut:

   ***Array* kunci dengan panjang kunci "length" *for* i = 0 to 255**
   K[i] = Kunci [i mod *length*] (2)

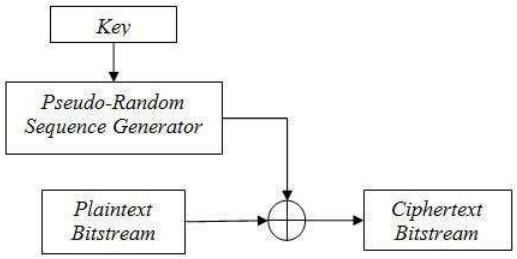
3) Kemudian langkah pengacakan S-Box dirumuskan dengan persamaan berikut:

   I = 0 ; j = 0
   ***for* i = 0 to 255**
   j = (j + S[i] + K[i]) mod 256
   ***swap* S[i] dan S[j] (3)**

4) Lalu membuat *pseudo random code* dengan rumus persamaan berikut:

   i = (i + 1) mod 256
   j = (j + S[i]) mod 256
   swap S[i] dan S[j]
   t = (S[i] + S[j]) mod 256
   K = S[t] (4)

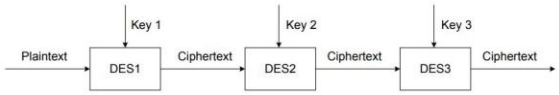
Byte K di-XOR-kan dengan plaintext untuk menghasilkan ciphertext atau di-XOR-kan dengan ciphertext untuk menghasilkan plaintext[10].



Gambar 3. Diagram algoritma RC4

2.4. Algoritma Triple Data Encryption Standard (3DES)

Algoritma penyandian data yang telah dikenal sejak tahun 1977 adalah *Data Encryption Standard* (DES) setelah disetujui oleh *National Bureau of Standard* (NBS) dan diuji kekuatannya oleh *National Security Agency* (NSA). Algoritma DES dikembangkan di IBM di bawah kepemimpinan W.L. Tuchman pada tahun 1972. Kekuatan DES saat itu terletak pada panjang kuncinya yaitu 56-bit. Akibat perkembangan teknologi yang begitu pesat. DES, telah terbukti kurang terjami dalam aspek keamanan. Perangkat keras khusus yang bertujuan untuk menentukan kunci 56-bit DES hanya dalam waktu beberapa jam sudah dapat dibangun. Dan pada tahun 1998, *Electronic Frontier Foundation* menggunakan suatu mesin komputer yang dikembangkan secara khusus yang bernama DES *Cracker*, dalam waktu kurang dari tiga hari telah dapat untuk memecahkan DES. Beberapa pertimbangan tersebut telah manandakan bahwa diperlukan sebuah pengembangan algoritma baru dan kunci yang lebih panjang. Setelah itu, dibuatlah beberapa pengembangan dari DES dengan cara memperbesar ruang kunci. Varian pengembangan DES yang paling dikenal adalah DES Berganda, yakni pemanfaatan DES berkali-kali untuk proses enkripsi dan dekripsinya. *Double* DES mempunyai kelemahan yaitu dapat diserang dengan algoritma yang dikenal sebagai *meet-in-the-middle-attack*, yang pertama kali ditemukan oleh Diffie dan Hellman. Sebagai bentuk pencegahan terhadap serangan tersebut, maka digunakanlah tiga kali langkah DES. Bentuk tersebut dinamakan sebagai *Triple* DES[8].



Gambar 4. Skema Triple DES

Triple Data Encryption Standard (3DES) merupakan algoritma simetri pada kriptografi yang digunakan untuk mengamankan data/informasi dengan cara menyandikan data. Algoritma 3DES adalah suatu algoritma pengembangan dari algoritma *Data Encryption Standard* (DES). Pada dasarnya algoritma yang digunakan sama, hanya pada 3DES dikembangkan dengan melakukan enkripsi dengan implementasi algoritma DES sebanyak tiga kali. 3DES memiliki tiga buah kunci yang berukuran 168-bit (tiga kali kunci 56-bit dari DES). Pada algoritma 3DES dibagi menjadi tiga tahap, setiap tahapnya merupakan implementasi dari algoritma DES. Algoritma 3DES dirumuskan sebagai berikut[3]:

Enkripsi : C = K3(K2(K1(P)))

Dekripsi : P = K1(K2(K3(C)))

Keterangan:

P = plaintext

C = ciphertext

Proses dilakukan dalam penyandian datanya yaitu proses enkripsi dan dekripsi. Algoritma 3DES merupakan algoritma pengembangan dari algoritma *Data Encryption Standard* (DES). Perbedaan DES dengan 3DES terletak pada panjangnya kunci yang digunakan. Pada DES menggunakan satu buah kunci yang panjangnya 56-bit sedangkan pada 3DES menggunakan tiga buah kunci yang panjangnya 168-bit (dengan panjang masing-masing 56-bit). Pada 3DES, tiga kunci yang digunakan bisa bersifat saling bebas (K1 ≠ K2 ≠ K3) dan hanya dua kunci yang saling bebas dan satu kunci lainnya sama dengan kunci pertama (K1 ≠ K2 dan K3 = K1) ataupun hanya menggunakan satu kunci yang sama (K1 = K2 = K3). Karena tingkat kerahasiaan algoritma 3DES terletak pada panjang kunci yang digunakan, maka penggunaan algoritma 3DES dianggap lebih baik dalam aspek keamanan dibandingkan dengan algoritma DES[3].

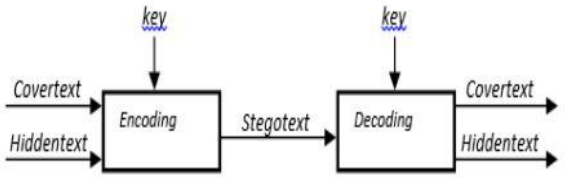
2.5. Pengertian Steganografi

Kata steganografi (*steganography*) berasal dari bahasa Yunani yaitu steganos artinya tersembunyi/terselubung dan *graphein*, yang artinya menulis, sehingga dapat diartikan "menulis tulisan yang tersembunyi/terselubung". Secara umum steganografi merupakan seni atau ilmu yang digunakan untuk menyembunyikan pesan rahasia sehingga orang lain tidak akan menyadari keberadaan dari pesan rahasia tersebut. Dari definisi diatas, maka dapat disimpulkan bahwa steganografi dibuat untuk membantu mengamankan informasi dengan cara menyembunyikan pesan pada sebuah media, agar pihak lain tidak mengetahui keberadaan informasi rahasia tersebut[1].

[1] Dalam proses Steganografi terdapat tiga kriteria yang harus terpenuhi, sebagai berikut:

1) *Impercepbility*
   Keberadaan pesan rahasia tidak dapat dipersepsi oleh indra manusia, baik indra pendengaran maupun indra penglihatan.
2) *Fidelity*
   Mutu dari media penampung tidak jauh berubah. Setelah penambahan pesan rahasia, hasil steganografi masih terlihat dengan baik. Orang lain tidak mengetahui kalau di dalam media terdapat pesan rahasia.
3) *Recovery*
   Pesan rahasia yang disembunyikan di dalam media harus dapat kembalikan seperti semula.

Steganografi yang menggunakan media gambar ini, *hidden text* atau *embedded message* yang dimaksudkan adalah teks yang akan disisipkan ke dalam *covertext* atau *coverobject* yaitu *file* video yang digunakan sebagai media penampung terhadap pesan yang akan disisipkan. Dari hasil *encoding* atau *embedding* pesan rahasia kedalam *file* gambar akan dihasilkan *stegotext* atau *stego-object* yang merupakan *file* yang berisikan pesan *embedding*[1].



Gambar 5. Cara Kerja Steganografi Secara Umum

2.6. Video Digital

Video adalah sebuah film atau gambar hidup yang dihasilkan dengan rekaman atau dibuat dari orang atau benda (termasuk fantasi dan figure palsu) dengan menggunakan kamera ataupun hal lain, dan memiliki fungsi dua dimensi yang terbentuk dari penglihatan dalam suatu tempat (*scene*) yang merupakan basis dalam pembentukan video[1]. Secara umum video dibagi menjadi dua macam, yaitu:

1) Analog, adalah video hasil tangkapan lensa kamera terhadap tempat (*scene*) yang di*scene* secara vertikal dan horizontal oleh kamera.
2) Digital, adalah video yang direpresentasikan sebagai sebuah matriks yang masing-masing elemennya merepresentasikan nilai intensitas tersendiri.

Video digital pada awalnya tersusun atas serangkaian *frame*. Rangkaian *frame* tersebut

ditampilkan dengan gambar *frame by frame* dengan kecepatan tertentu, tergantung pada *frame rate* yang ada (dalam *frame* per *second*). Jika *frame rate* cukup tinggi, mata manusia tidak dapat melihat gambar atau *frame*, melainkan melihatnya sebagai rangkaian yang kontinu/berlanjut (video)[1].

2.7. Moving Picture Experts Group (MPEG-4)

Sebuah video digital terdiri dari *frame by frame* yang mana *frame by frame* tersebut dijadikan sebuah *file* yang hanya dapat dijalankan menggunakan sebuah perangkat lunak *multimedia player*. Berdasarkan bentuk-bentuk *file* video digital tersebut, banyak format-format video digital yang dapat digunakan oleh *user* dengan kelebihan dan kekurangannya masing-masing. Salah satu contoh format video digital adalah MP4. MPEG-4 Bagian 14 atau MP4 format *file*, secara resmi ISO / IEC 14496-14:2003, adalah sebuah format *multimedia container* yang ditetapkan sebagai bagian dari MPEG-4. Hal ini paling sering digunakan untuk menyimpan video digital dan digital *stream audio*, terutama yang didefinisikan oleh MPEG. Seperti format paling modern, MPEG4 *Part* 14 telah memungkinkan *streaming* melalui dunia maya. *Track* petunjuk terpisah digunakan untuk menyertakan informasi dalam *streaming file*. *Filename extension* resmi untuk MPEG-4 *Part* 14 *file* adalah MP4, sehingga format sering disebut sebagai MP4[1].

2.8. Metode End Of File

End Of File (EOF) adalah salah satu metode steganografi. Metode ini melakukan proses *embed* dengan cara dengan menyisipkan data/informasi pada akhir *file*. Sehingga, tidak merusak kualitas *file* penampung yang akan disisipkan pesan. Namun, setelah disisipkan pesan rahasia ukuran *file* akan bertambah. Sebab, ukuran *file* penampung akan ditambah dengan ukuran *file* yang disisipkan. Metode EOF menggunakan karakter yang berbeda sebagai penanda awal penyisipan pesan rahasia dan penanda akhir penyisipan pesan rahasia. Metode EOF memanfaatkan kelemahan indera manusia yang tidak sensitif sehingga seakan-akan tidak ada perbedaan yang terlihat antara sebelum atau sesudah pesan rahasia disisipkan[1].

Pada EOF pesan rahasia yang akan disisipkan pada media penampung akan di-*convert* kedalam nilai desimal berdasarkan tabel ascii. Kode ASCII (*American Standart Code for Informatian Interchange*) merupakan representasi *numeric* dari karakter- karakter yang akan digunakan, dengan ketentuan huruf a-z, A-Z, 0-9 dan simbol standar pada *keyboard*[1].

Contohnya ada pada sebuah citra gambar grayscale 6x6 *pixel* disisipkan pesan yang berbunyi "aku". Untuk menandai akhir pesan digunakan karakter yang tidak sering digunakan, misalnya karakter #. Sehingga pesan yang dimaksud adalah "#aku"[1]. Kode ASCII dari pesan diberikan sebagai berikut:

97 107 117 35

Misalkan sebuah citra gambar grayscale dengan kode warna:

196	**10**	**97**	**182**	**101**	**40**
67	**200**	**100**	**50**	**90**	**50**
25	**150**	**45**	**200**	**75**	**28**
176	**56**	**77**	**100**	**25**	**200**
101	**34**	**250**	**40**	**100**	**60**
44	**66**	**99**	**125**	**190**	**200**

Nilai desimal pesan rahasia berdasarkan tabel ascii disisipkan diakhir citra gambar, sehingga citra gambar menjadi:

196	**10**	**97**	**182**	**101**	**40**
67	**200**	**100**	**50**	**90**	**50**
25	**150**	**45**	**200**	**75**	**28**
176	**56**	**77**	**100**	**25**	**200**
101	**34**	**250**	**40**	**100**	**60**
44	**66**	**99**	**125**	**190**	**200**
97	**107**	**117**	**35**		

Metode EOF tidak mengubah isi awal dari *file* yang dijadikan media penampung. Sebagai contoh, jika pengguna menyisipkan sebuah pesan kedalam sebuah dokumen/teks, isi dari dokumen/teks tidak akan berubah. Hal ini yang menjadi salah satu keunggulan metode EOF dibandingkan dengan metode *steganografi* lain. Karena disisipkan pada akhir *file*, pesan yang disisipkan tidak akan bersinggungan dengan isi *file*, hal ini menyebabkan integrasi data dari *file* media penampung tetap terjaga[1].

3. ANALISIS MASALAH DAN PERANCANGAN SOLUSI

3.1. Analisis Permasalahan

Setiap instansi memiliki informasi yang sangat penting dan tentunya pihak yang boleh mengetahui isi informasi tersebut. Hanya pihak yang tertentu yang diperbolehkan untuk mengola data atau informasi tersebut. Informasi yang dimaksud bisa berupa data soal ujian serta dokumen-dokumen penting lainnya. Karena hal itu sendiri ada beberapa di hadapi oleh setiap instansi mengenai keamanan data. Tanpa pengamanan data, dokumen bisa disadap dan diambil oleh pihak yang tidak berhak isi dokumen. Namun saat ini keamanan data atau informasi sering terancam kerahasiannya oleh pihak yang tidak bertanggung jawab yang mencari data atau informasi untuk kepentingan pribadi. Oleh karena itu, demi menjaga kerahasiaan data atau informasi tersebut maka pada penelitian ini dibuatlah sistem pengaman data dokumen dengan cara mengacak isi dokumen

tersebut dan menyisipkannya kedalam suatu media video.

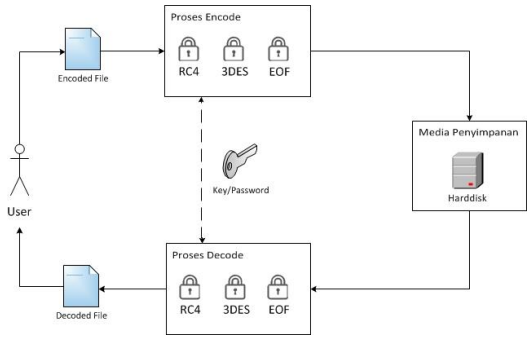
3.2. Penyelesaian Masalah

Dari permasalahan tersebut, maka diperlukan sebuah aplikasi yang berguna menjaga kerahasiaan informasi atau data berupa *file* teks atau gambar. Aplikasi tersebut nantinya bisa mengubah sebuah *file* teks atau gambar menjadi *file* yang isinya tidak dapat dibaca dan menyisipkannya ke *file* video agar terjaga kerahasiaannya. Dalam mengimplementasikan pengamanan informasi atau data tersebut penulis menggunakan teknik kriptografi dan steganografi.

Aplikasi kriptografi dan steganografi ini dibuat berbasis *desktop* dengan bahasa pemograman *java*. Dalam hal pembuatan aplikasi ini menggunakan metode algoritme kriptografi *Rivest Code* 4 (RC4) dan *Triple Data Encryption Standard* (3DES) serta metode steganografi *End of File* (EOF). Dengan dibuatnya aplikasi ini diharapkan mampu memenuhi aspek keamanan sehingga terjaga kerahasiaan informasi/data tersebut.

3.3. Perancangan Program

Aplikasi kriptografi dan steganografi yang akan dibuat memiliki 6 buah menu yaitu menu *login*, menu *home*, menu *encode*, menu *decode*, menu *help* dan menu *about*. menu *login* adalah tampilan awal dimana program ini dijalankan dan menu *home* adalah menu utama pada program. Pada menu *encode* ada 4 pilihan *form* yaitu *form* pilih *file*, *form* pilih video, *form* penyimpanan dan *form password* dan di dalam menu *decode* ada 3 pilihan *form* yaitu *form* pilih video, *form* penyimpanan dan *form password*. Menu *Help* adalah menu yang akan memberikan informasi kepada *user* tentang penggunaan aplikasi tersebut, *help* memiliki 2 menu yaitu *encode* dan *decode*. Dan menu *about* akan memuat informasi tentang pembuat aplikasi. Berikut skema arsitektur program:



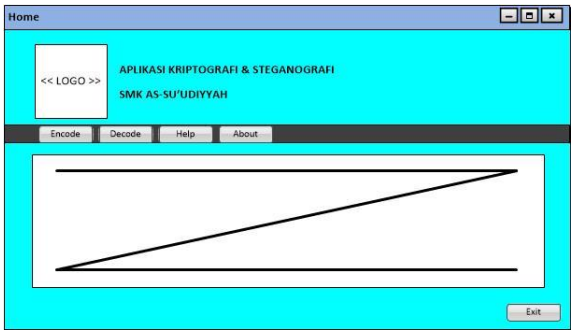
Gambar 6. Skema Arsitektur Program

Keterangan:

Gambar arsitektur kerja aplikasi ini merupakan alur jalannya program yang akan dibuat dengan menggunakan algoritma kriptografi *Rivest Code* 4 (RC4), *Triple Data Encryption Standard* (3DES) dan steganografi *End of File* (EOF).

3.4. Rancangan Layar Halaman *Home*

Fungsi Halaman *Home* berfungsi sebagai halaman awal yang memberikan akses kepada *user* dan menjadi *form* pertama yang ditampilkan pada saat *user* menggunakan aplikasi pengamanan data ini. Didalam layar halaman home terdapat beberapa pilihan menu yaitu *form encode*, *form decode*, *form about*, *form help* dan *form exit* seperti Gambar 7 berikut ini.



Gambar 7. Rancangan Layar Halaman Home

4. IMPLEMENTASI DAN UJI COBA SOLUSI

4.1. Implementasi Perangkat Keras dan Perangkat Lunak

Agar aplikasi pengamanan data ini dapat berjalan dengan baik dan bekerja sesuai dengan keinginan, spesifikasi perangkat keras dan perangkat lunak yang dipakai untuk implementasi aplikasi ini juga harus mendukung. Berikut spesifikasi yang dapat mendukung aplikasi ini, diantaranya adalah:

4.1.1. Perangkat Keras (*Hardware*)

Perangkat keras (*hardware*) yang digunakan untuk implementasi aplikasi ini adalah sebagai berikut:

1) *Processor*: Intel®Core™ i5-4210 CPU @1.70GHz 2.40GHz
2) *Memory*: 4 GB
3) *Monitor*: 14" (1366 x 768)
4) Penyimpanan: 500 GB

4.1.2. Perangkat Lunak (*Software*)

Perangkat lunak (*software*) yang digunakan untuk implementasi aplikasi ini adalah sebagai berikut:

1) Sistem Operasi Windows 10
2) Bahasa Pemrograman Java dengan Editor NetBeans IDE 8.2
3) JDK 1.8
4) Microsoft Office Visio Standard 2010
5) Hex Editor Neo 6.44

4.2. Tabel Pengujian

Dalam pengujian akan dibahas mengenai perbandingan antara proses *encode* dan *decode file*.

File yang diuji meliputi *file* yang berformat **.docx*, **.xlsx*. Pengujiannya yaitu antara lain perbandingan antara ukuran *file* asli dan ukuran *file* hasil *encode* serta ukuran *file* video sebelum di-*encode* dan setelah di-*encode*, waktu proses pada saat *encode*, waktu proses pada saat *decode* hingga hasil yang dicapai dalam proses *encode* maupun *decode*.

Tabel 1. Tabel Pengujian Proses *Encode File*

Nama File	Ukuran File Asli	Nama Video	Ukuran Video Asli	Ukuran Video Hasil Encode	Waktu Encode
Soal-utama KKPI .docx	214 KB	MAH00481.mp4	27,8 MB	28,7 MB	13.227 detik
ADMINISTRASI TAHUN AJARAN 2017-2018 .xlsx	58 KB	MAH00491.mp4	19,1 MB	38,2 MB	5.078detik

Tabel 2. Tabel Pengujian Proses *Decode File*

Nama Video	Ukuran Video Hasil Encode	Waktu Decode	Ukuran File Hasil Decode
Embed_MAH00481.mp4	28,7 MB	48.986 detik	214 KB
Embed_MAH00491.mp4	38,2 MB	63.645 detik	58 KB

4.3. Evaluasi Aplikasi

Berdasarkan pengujian program untuk proses *encode* dan *decode* yang telah dilakukan dapat ditemukan beberapa kelebihan dan kekurangan dari aplikasi ini, yaitu sebagai berikut:

4.3.1. Kelebihan Program

a. Kualitas video seperti bentuk awal tidak rusak setelah disisipkan *file* rahasia sehingga benar-benar tidak nampak keberadaan *file* rahasia.
b. *File* yang sudah di *encode* tidak bisa dibaca atau dibuka kembali oleh siapapun sebelum di *decode* dengan *password* yang sesuai.
c. Isi *file* dari hasil *decode* tidak mengalami perubahan atau kembali seperti *file* asli

4.3.2. Kekurangan Program

a. Semakin besar ukuran sebuah *file* maka akan semakin lama prosesnya.
b. Ukuran video yang dapat digunakan sebagai media penyisipan *file* hanya dibatasi sampai 50 MB.
c. Ukuran *file* yang di *encode* dibatasi hanya 5 MB.
d. Waktu yang diperlukan untuk proses *decode* masih terbilang kurang cepat jika dibandingkan dengan proses *encode*

5. KESIMPULAN

Berdasarkan perancangan, pembuatan, serangkaian uji coba dan analisa program dari aplikasi kriptografi dan steganografi ini, maka dapat diambil suatu kesimpulan antara lain:

a. Dengan adanya aplikasi kriptografi dan steganografi ini, proses penyimpanan dan pertukaran informasi menjadi lebih aman.
b. Kecepatan penggunaan aplikasi sangat tergantung pada *software*, *hardware*, dan *file* yang digunakan baik *file* rahasia ataupun *file* video yang akan di-*encode* maupun di-*decode*.
c. Proses *decode* akan mengembalikan *file* seperti semula dengan menggunakan *password* yang sesuai

DAFTAR PUSTAKA

[1] Anti, U. Ari, Kridalaksana, Harsa A., & Khairina, Marisa D. (2017). Steganografi Pada Video Menggunakan Metode Least Significant Bit (LSB) Dan End of File (EOF). *Jurnal Informatika Mulawarman*, *12*(2), 104–111.

[2] Ariyus, D. (2008). Pengantar Ilmu Kriptografi: teori, analisis dan implementasi. Yogyakarta: ANDI.

[3] Gunawan, Heru A., Arifin, Z., & Astuti, I. F. (2014). Keamanan Login Web Menggunakan Metode 3Des Berbasis Teknologi Quick Response Code, *9*(2), 18–23.

[4] Hakim, E. L., & Utami, F. H. (2014). Aplikasi Enkripsi Dan Deskripsi Data Menggunakan Algoritma Rc4, *10*(1), 1–7.

[5] Gunawan, Indra. (2017). Pengamanan Acakan Biss Menggunakan Algoritma Rsa. *Riset Sistem Informasi Dan Teknik Informatika (JURASIK)*, *2*(1), 58–63.

[6] Kurniadi, Irwansyah, F. (2015). PENERAPAN ALGORITMA RC4 UNTUK ENKRIPSI KEAMANAN DATA (Studi kasus: Dinas Pendidikan dan Kebudayaan Kota Sekayu). *Jurnal Ilmiah R & B*, (12).

[7] McLeod, R. Jr. and Jordan, E. 2002. Systems development: a project management approach, New York, NY: John Wiley and Sons, Inc.

[8] Munir, R. (2004). Sistem Kriptografi Kunci-Publik Departemen Teknik Informatika Institut Teknologi Bandung.

[9] Christanalis, Sitompul, O. S., & Tulus. (2014). KOMBINASI ALGORITMA TRIPLE DES DAN ALGORITMA AES DALAM PENGAMANAN FILE. Konferensi Nasional Ilmu Komputer (KONIK).

[10] Rifai, R. Y., Christyono, Y., & Santoso, I. (2016). Shamir Adleman, Dan Metode Steganografi Untuk Pengamanan Pesan Rahasia Pada Berkas Teks Digital. *Transient*, *5*(1).

[11] Siswanto, Feriadi, Utama, Gunawan P., Achmad, Aditya F. (2016). Pengamanan Data Dengan Menggunakan Algoritma Kriptografi Aes, Rc4 Dan Kompresi Lz77. *Seminar Nasional Telekomunikasi Dan Informatika (SELESIK 2016)*, *1*(Selisik),1.