



KILAT

JURNAL KAJIAN ILMU DAN TEKNOLOGI

Alhara Yuwanda

POTENSI KOMPOSIT SERAT BAMBU UNTUK MENGGANTI MATERIAL KAYU GEROBAK DITINJAU DENGAN UJI ELASTISITAS

Anindya Khrisna Wardhani

PENERAPAN ALGORITMA *PARTITIONING AROUND MEDOIDS* UNTUK MENENTUKAN KELOMPOK PENYAKIT PASIEN (STUDI KASUS : PUSKESMAS KAJEN PEKALONGAN)

*Efy Yosrita;
Rakhmat Arianto*

PENENTUAN PENERIMAAN MAHASISWA TERHADAP APLIKASI MENGHITUNG INVERS MATRIK ORDO 3X3 DAN 4X4 DENGAN PENDEKATAN *USER ACCEPTANCE TEST*

*Gita Puspa Artiani;
Fajar Eka Surya*

PERBEDAAN PELAKSANAAN TERHADAP PERENCANAAN DAN CARA MENGATASINYA PADA PROYEK KONSTRUKSI

Abdul Haris

SISTEM PENCATAT KWH METER TERINTEGRASI KOMPUTER UNTUK MENINGKATKAN LAYANAN PADA PELANGGAN

Hendra Jatnika

PENERAPAN METODE *ENTERPRISE ARCHITECTURE PLANNING (EAP)* DALAM PERENCANAAN PROGRAM SERTIFIKASI (STUDI KASUS LABORATORIUM ITCC STT-PLN)

Marliana Sari

IMPLEMENTASI PEMBATAHAN AKSES PEMAKAI KOMPUTER MENGGUNAKAN *GROUP POLICY OBJECT* DI WINDOWS SERVER 2012 R2

*Moch. Alfian Ichsan;
Windarto*

IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA, KOMPRESI DATA HUFFMAN, DAN STEGANOGRAFI EOF PADA MEDIA VIDEO UNTUK KEAMANAN DATA DI PT SELARAS CITANUSA WISATA

Rizqia Cahyaningtyas

APLIKASI *MONITORING SMARTLAB* MENGGUNAKAN ALGORITMA ENIGMA BERBASIS ANDROID (STUDI KASUS : LABORATORIUM KOMPUTER DASAR STT-PLN)

*Ranti Hidayawanti;
Irma Wirantina K.;
Endah Lestari*

UPAYA PENGELOLAAN SAMPAH DI KAMPUS STT-PLN DENGAN TEKNOLOGI ANAEROBIK DIGESTER

*Sarwati Rahayu;
Vera Yunita;
Umniy Salamah*

IMPLEMENTASI APLIKASI PEMBELAJARAN MATEMATIKA BANGUN DATAR BAGI SISWA SEKOLAH DASAR BERBASIS ANDROID

*Mellia Nur Indah Susanti;
Yessy Asri*

PERBANDINGAN HASIL BELAJAR SISWA SD DI PERKOTAAN DAN DI PEDESAAN MELALUI MEDIA PEMBELAJARAN BERBASIS MULTIMEDIA *FLASH FLIP BOOK* PENDIDIKAN KEWARGANEGARAAN

ISSN 2089-1245



9 772089 124519

SEKOLAH TINGGI TEKNIK - PLN (STT-PLN)

KILAT	VOL.6	NO.1	HAL. 1 - 80	APRIL 2017	ISSN 2089 - 1245
-------	-------	------	-------------	------------	------------------

IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA, KOMPRESI DATA HUFFMAN, DAN STEGANOGRAFI EOF PADA MEDIA VIDEO UNTUK KEAMANAN DATA DI PT SELARAS CITANUSA WISATA

¹Moch. Alfian Ichsan; ²Windarto

¹²Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260

Telp. (021) 5853753 ext 303, Fax. 5853489

E-mail: ¹alfian.ichsan25@gmail.com, ²windarto@budiluhur.ac.id

ABSTRACT

The rapid development of technology and information has an impact on the process of delivering data which can be done through a variety of media one of which is an e-mail. Of course, the security of the data and information which is transmitted is necessary and can not be ignored in order to maintain the confidentiality of such data. As a company engaged in the field of travel agency, PT Selaras Citanusa Wisata also uses information and communication technology to produce several documents that must be kept from unauthorized persons, one of which is the manifest of Hajj and Umrah pilgrims. To deal with the problems occurred in PT Selaras Citanusa Wisata concerning the security of the data it needs a data security application to secure manifest of Hajj and Umrah pilgrims' data. By applying RSA (Rivest Shamir Adleman), a cryptographic algorithm, Huffman compression algorithm combined with End of File steganography algorithms, the application is built in Java programming language, desktop based. This application can secure and maintain the confidentiality of PT Selaras Citanusa Wisata data so as to prevent from theft and data manipulation by parties who do not have the authority.

Keywords: Cryptography, RSA, Huffman, Steganography, End of File.

ABSTRAK

Dengan perkembangan teknologi dan informasi yang semakin pesat proses pengiriman data dapat dilakukan dengan mudah melalui berbagai macam media salah satunya adalah e-mail. Tentunya keamanan akan data dan informasi yang dikirimkan sangatlah diperlukan dan tidak dapat diabaikan demi menjaga kerahasiaan data tersebut. Sebagai perusahaan yang bergerak di bidang travel agency PT Selaras Citanusa Wisata juga menggunakan teknologi informasi dan komunikasi serta menghasilkan beberapa dokumen yang harus dirahasiakan, salah satunya adalah data manifest jamaah haji dan umrah. Untuk menangani permasalahan mengenai keamanan data yang ada di PT Selaras Citanusa Wisata maka diperlukan suatu aplikasi keamanan data yang dapat mengamankan data manifest jamaah haji dan umrah. Dengan menerapkan algoritma kriptografi RSA (Rivest Shamir Adleman), dan algoritma kompresi Huffman yang dikombinasikan dengan algoritma steganografi EoF (End of File), aplikasi ini dibangun dengan bahasa pemrograman Java berbasis desktop. Aplikasi ini dapat mengamankan dan menjaga kerahasiaan data pada PT Selaras Citanusa Wisata sehingga dapat mencegah pencurian dan manipulasi data oleh pihak yang tidak memiliki wewenang.

Kata kunci: Kriptografi, RSA, Huffman, Steganografi, End of File.

1. PENDAHULUAN

Pada era teknologi informasi seperti sekarang ini, keamanan dalam penyimpanan data atau informasi adalah hal yang sangat penting dan tidak dapat diabaikan. Terlebih jika data yang tersimpan tersebut bersifat rahasia. Salah satu dampak negatif dalam perkembangan teknologi informasi saat ini adalah pencurian data. Dengan adanya pencurian data maka aspek keamanan dalam pertukaran data dianggap penting, karena suatu komunikasi jarak jauh belum tentu aman dari pencurian.

PT Selaras Citanusa Wisata merupakan perusahaan yang bergerak dibidang *travel agency* yang terletak di Jl. Ciputat Raya, Jakarta Selatan. PT Selaras Citanusa Wisata juga menggunakan teknologi informasi dan komunikasi serta menghasilkan

beberapa dokumen penting yang harus dirahasiakan, salah satunya adalah data *manifest* jamaah haji dan umrah.

Salah satu cara untuk mengatasi permasalahan ini yaitu dengan menggabungkan metode kriptografi algoritma *Rivest Shamir Adleman* (RSA), metode kompresi Huffman, dan metode algoritma *End of File* (EoF). Sehingga kombinasi metode tersebut dinilai lebih aman dalam penyimpanan data *manifest* jamaah haji dan umrah yang dirahasiakan oleh PT Selaras Citanusa Wisata.

2. METODE PENELITIAN

2.1. Kriptografi

Kriptografi (*Cryptography*) berasal dari bahasa Yunani yang terdiri dari dua buah kata yaitu *crypto* dan *graphia*. Kata *crypto* berarti rahasia sedangkan *graphia* berarti tulisan. Secara umum makna dari kata kriptografi adalah tulisan rahasia. Orang yang melakukan penyandian ini disebut *cryptographer*, sedangkan orang yang mendalami ilmu dan seni dalam membuka atau memecahkan suatu algoritma kriptografi tanpa harus mengetahui kuncinya disebut *cryptanalysis* (Meidina, 2013).

Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara himpunan, yang berisi elemen – elemen *ciphertext*. Tingkat keamanan suatu algoritma dalam kriptografi seringkali diukur dari kuantitas proses yang dilakukan dalam suatu fungsi, baik itu fungsi enkripsi maupun fungsi dekripsi. Proses tersebut juga dapat dihubungkan dengan sumber data yang dibutuhkan, menunjukkan semakin kuat algoritma kriptografi tersebut.

2.2. Algoritma RSA (Rivest Shamir Adleman)

Algoritma RSA (*Rivest Shamir Adleman*) dibuat oleh 3 peneliti dari MIT (*Massachusetts Institute of Technology*) pada tahun 1977, yaitu Ron Rivest, Adi Shamir, dan Len Adleman. Huruf RSA sendiri berasal dari inisial nama mereka (*Rivest-Shamir-Adleman*), (Adianson dkk, 2015).

Berikut adalah contoh perhitungan manual algoritma RSA dari sebuah kata yaitu "SELARAS". Langkah pertama adalah pembentukan kunci, yaitu sebagai berikut:

- 1) Dipilih dua bilangan prima sembarang yang besar, p dan q . nilai p dan q harus dirahasiakan. Misal $p = 13$ dan $q = 31$.
- 2) Dihitung $n = p \cdot q$ besaran n tidak perlu dirahasiakan. $n = 13 \cdot 31 = 403$.
- 3) Dihitung $\phi(n) = (p-1)(q-1)$ untuk mencari nilai totient dari $\phi(n)$ dan n . $\phi(n) = (13-1)(31-1) = 12 \cdot 30 = 360$.
- 4) Untuk mendapatkan nilai e dimana $1 < e < \phi(n)$. $\gcd(e, \phi(n)) = 1$, dimana bilangan e bilangan relative prima terhadap $\phi(n)$ misalkan $e = 7$, karena $\gcd(7, 360) = 1$.
- 5) Tentukan bilangan bulat d dengan rumus $(d \cdot e) \bmod \phi(n) = 1$. Misalkan $d = 103$, maka $(103 \cdot 7) \bmod 360 = 1$.

Hasil dari algoritma tersebut adalah:

- 1) Kunci publik adalah pasangan $(e, n) = (7, 403)$.
- 2) Kunci privat adalah pasangan $(d, n) = (103, 403)$.

Ketika kunci sudah selesai dibuat, maka selanjutnya proses enkripsi terhadap kata "SELARAS" bisa berjalan, namun setiap huruf pada kata tersebut diubah kedalam bentuk desimal terlebih dahulu.

$S = 83$, $E = 69$, $L = 76$, $A = 65$, $R = 82$, $A = 65$, $S = 83$.

kemudian untuk enkripsinya secara berurutan konversikan masing – masing blok – blok pl_1 , pl_2 , pl_3 , ... pl_n ke rumus $c = p^e \bmod n$.

$$S = 837 \bmod 403 = 73$$

$$E = 697 \bmod 403 = 121$$

$$L = 767 \bmod 403 = 236$$

$$A = 657 \bmod 403 = 234$$

$$R = 827 \bmod 403 = 173$$

$$A = 657 \bmod 403 = 234$$

$$S = 837 \bmod 403 = 73$$

Kata "SELARAS" setelah dienkripsi menjadi: 7312123623417323473.

Kemudian jika ingin mengembalikan seperti kata semula yaitu melalui proses dekripsi RSA dengan menggunakan rumus secara berurutan konversikan masing – masing blok – blok pl_1 , pl_2 , pl_3 , ... pl_n ke rumus $pl = c^d \bmod n$.

$$73^{103} \bmod 403 = 83$$

$$121^{103} \bmod 403 = 69$$

$$236^{103} \bmod 403 = 76$$

$$234^{103} \bmod 403 = 65$$

$$173^{103} \bmod 403 = 82$$

$$234^{103} \bmod 403 = 65$$

$$73^{103} \bmod 403 = 83$$

Maka akan menjadi kata seperti semula: "SELARAS".

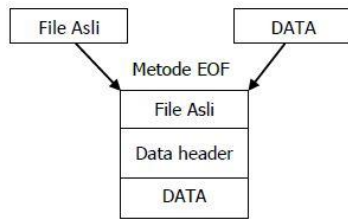
2.3. Steganografi

Steganografi sudah dikenal oleh bangsa Yunani. Penguasa Yunani dalam mengirimkan pesan rahasia menggunakan kepala budak atau prajurit sebagai media. Dalam hal ini, rambut budak dicukur habis, lalu pesan rahasia ditulis di kulit kepala budak tersebut. Ketika rambut budak tumbuh, budak tersebut diutus untuk membawa pesan rahasia di kepalanya.

Lain halnya dengan bangsa Yunani, bangsa Romawi mengenal steganografi dengan menggunakan tinta tak tampak untuk menuliskan pesan. Tinta tersebut dibuat dari campuran sari buah, susu dan cuka. Jika tinta digunakan untuk menulis maka tulisannya tidak tampak. Tulisan di atas kertas tersebut dapat dibaca dengan cara memanaskan kertas tersebut (Amal dkk, 2015).

2.4. End of File (EoF)

Secara umum teknik steganografi menggunakan *redundant bits* sebagai tempat menyembunyikan pesan pada saat dilakukan kompresi data, dan kemudian menggunakan kelemahan indera manusia yang tidak sensitif sehingga pesan tersebut tidak ada perbedaan yang terlihat atau yang terdengar. Teknik *End of File* merupakan salah satu teknik yang digunakan dalam steganografi. Teknik ini digunakan dengan cara menambahkan data atau pesan rahasia pada akhir *file*. Teknik ini dapat digunakan untuk menambahkan data yang ukurannya sesuai dengan kebutuhan. Perhitungan kasar ukuran *file* yang telah disisipkan data sama dengan ukuran *file* sebelum disisipkan data ditambah ukuran data rahasia yang telah diubah menjadi *encoding file* (Matono, 2013). Secara umum media steganografi memiliki struktur seperti pada gambar 1.



Gambar 1: Struktur File Steganografi EoF.
(Martono, 2013)

EOF mempunyai kekurangan yaitu tidak dapat menyisipkan *file* yang berukuran besar karena dapat membuat *file* citra dicurigai karena ada perubahan pada citra tersebut. Metode EoF (*End Of File*). Misalnya pada sebuah citra skala keabuan 6x6 piksel disisipkan pesan yang berbunyi "SELARAS". Kode ASCII dari pesan tersebut adalah:

83 69 76 65 82 65 83

Misalkan matriks tingkat derajat keabuan citra sebagai berikut:

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

Pada akhir data gambar akan diberikan suatu penanda data gambar dan pesan, dalam contoh tanda sebagai berikut:

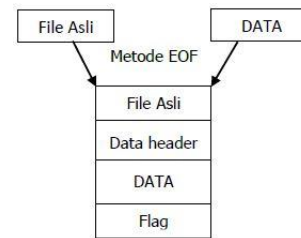
196	10	97	182	101	40
67	200	100	50	90	50
25	150	45	200	75	28
176	56	77	100	25	200
101	34	250	40	100	60
44	66	99	125	190	200
255	255	255	255	255	

Kode ASCII pesan disisipkan di akhir citra yang telah diberikan penanda, sehingga 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
255	255	255	255	255	
83	69	76	65	82	65 83

Penandaan data header atau flag akan diletakkan di awal atau akhir file, dimana tidak ada looping yang digunakan untuk mencarinya. Pada beberapa file seperti exe dan zip, penempatan flag di awal file asli tidak akan menjadi masalah, namun untuk jenis file lain semisal JPG, BMP, dan DOC, penempatan flag di awal file akan merusak file asli karena mengganggu isi file asli dan merusak file tersebut. Maka dari itu penempatannya akan ditempatkan di akhir file sehingga tidak merusak file asli meskipun menggunakan berbagai jenis file

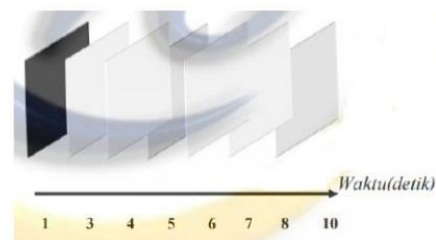
(Matono, 2013). Ini juga sesuai dengan konsep EoF pada gambar 2.



Gambar 2: Struktur File Steganografi EoF Disertai Flag. (Matono, 2013)

2.5. Video

Video merupakan gabungan gambar – gambar yang tidak bergerak dibaca berurutan dalam suatu waktu dengan kecepatan tertentu. Gambar – gambar yang digabung tersebut dinamakan *frame* dan kecepatan pembacanya gambar disebut dengan *frame rate*, dengan satuan fps (*frame per second*). Karena dinamakan dalam kecepatan yang tinggi maka tercipta ilusi gerak yang halus, semakin besar nilai *frame rate* maka akan halus pergerakan yang ditampilkan. (Kusmindar, 2015)



Gambar 3: Aliran Frame. (Kusmindar, 2015)

2.6. Kompresi Data

Kompresi adalah pengubahan data kedalam bentuk yang memerlukan *bit* yang lebih sedikit, biasanya dilakukan agar data dapat disimpan atau dikirim dengan lebih efisien. Kebalikan dan proses kompresi, yaitu dekompresi. Dekompresi merupakan proses untuk mengembalikan data baru yang telah dihasilkan oleh proses kompresi menjadi data awal. Dekompresi yang menghasilkan data sama persis dengan data aslinya sebelum dikompresi, maka kompresi tersebut disebut dengan *lossless compression*. Sebaliknya, jika hasil dekompresi tersebut tidak sama dengan data aslinya sebelum dikompresi, karena ada data yang dihilangkan karena dirasa tidak terlalu penting tetapi tidak mengubah informasi yang dikandungnya, maka disebut dengan *loosy compression* (Prasetyo, dkk 2013).

2.7. Algoritma Kompresi Huffman

Algoritma kompresi Huffman dinamakan sesuai dengan nama penemunya yaitu David Huffman, seorang professor di MIT (*Massachusetts Institute of Technology*) (Prasetyo, dkk 2013).

Kompresi Huffman merupakan algoritma kompresi *lossless* dan ideal untuk mengkompresi teks atau *file* program. Ini yang menyebabkan mengapa algoritma ini banyak dipakai dalam

program kompresi. Kompresi Huffman termasuk dalam algoritma keluarga dengan *variable codeword length*. Ini berarti symbol individual (karakter dalam sebuah file teks sebagai contoh) digantikan oleh urutan *bit* yang mempunyai suatu panjang yang nyata (*distinct length*). Jadi simbol yang muncul cukup banyak dalam file akan memberikan urutan yang pendek sementara simbol yang jarang dipakai akan mempunyai urutan *bit* yang lebih panjang (Prasetyo, dkk 2013).

Adapun bentuk algoritma Huffman dalam membentuk sebuah pohon biner adalah sebagai berikut (Prasetyo, dkk 2013):

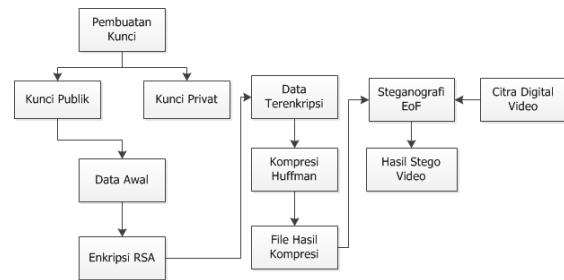
- 1) Dimulai dengan penyusunan frekuensi symbol sebagai frekuensi dari pohon.
- 2) Jika terdapat lebih dari satu pohon:
 - a) Carilah dua pohon dengan jumlah *weight* yang paling kecil.
 - b) Gabungkan dua pohon tersebut menjadi satu dan mempunyai nilai setara dengan jumlah hasil pengkodean symbol hipotesis untuk menandai tiap blok.
- 3) Symbol hipotesis dari Huffman code itu anggap C.
- 4) Kode symbol ke-l dari blok k adalah C_k^{-1} digabungkan dengan symbol ke-l dari Huffman code blok pertama.

2.8. Analisa Masalah

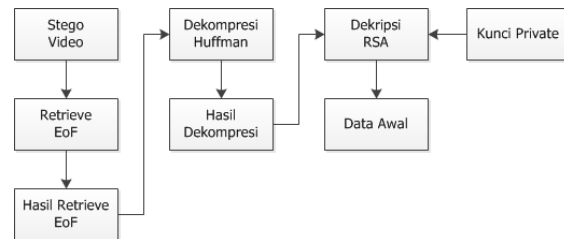
PT Selaras Citanusa Wisata menggunakan teknologi informasi dan komunikasi yang menghasilkan beberapa dokumen yang harus dirahasiakan, salah satunya adalah data *manifest* jamaah haji dan umrah. Seiring berkembangnya perusahaan ini, semakin banyak juga pelanggan yang melaksanakan ibadah haji dan umrah melalui PT Selaras Citanusa Wisata. Dengan demikian semakin banyak data yang disimpan dan perlu dilakukan pengamanan.

Saat ini pengamanan data *manifest* jamaah haji dan umrah di PT Selaras Citanusa Wisata sudah dilakukan akan tetapi pengamanan tersebut belumlah terbilang aman karena pihak perusahaan hanya menyembunyikan data tersebut di file tertentu saja dan diberikan kepada karyawan yang mempunyai wewenang yang mengetahui lokasi data *manifest* tersebut. Jika lokasi data *manifest* tersebut diketahui oleh pihak yang tidak memiliki wewenang untuk membukanya, data *manifest* tersebut bisa saja dicuri atau dimanipulasi isinya. Untuk itu PT Selaras Citanusa Wisata membutuhkan suatu aplikasi pengamanan data agar data yang tersimpan terjamin keamanannya.

2.9. Skema Proses Encoding dan Decoding



Gambar 3: Skema Proses Encoding



Gambar 4: Skema Proses Decoding

2.10. Perancangan Program

Pada perancangan program ini, pembuatan rancangan layar dan flowchart dengan menggunakan *software pencil* yang terdiri dari 7 form, yaitu form *MenuLogin*, form *MainMenu*, form *MenuGenerate*, form *MenuEncode*, form *MenuDecode*, form *MenuHelp*, form *MenuAbout*. Sebelum menggunakan aplikasi, user harus login terlebih dahulu dengan menginput *username* dan *password* agar dapat masuk ke form *MainMenu*, setelah itu user dapat memilih fitur – fitur yang ada.

2.11. Rancangan Layar Form MenuGenerate

Form *MenuGenerate* merupakan form yang berfungsi untuk membuat *public key* dan *private key*. Pasangan kunci ini nantinya digunakan pada saat melakukan proses *encoding* dan *decoding file*. Pada form *MenuGenerate* terdapat berapa komponen yaitu *textbox*, *image*, dan *button*. Rancangan layar form *MenuGenerate* dapat dilihat pada gambar 5 dibawah ini.

Gambar 5: Rancangan Layar Form Menu Generate

2.12. Rancangan Layar Form MenuEncode

Form *MenuEncode* adalah form yang berfungsi untuk melakukan proses *encoding file*. Untuk melakukan proses *encoding* terlebih dahulu memilih file yang akan di amankan lalu, memilih cover berupa media video, selanjutnya memilih kunci publik yang

sebelumnya sudah dibuat, lalu memilih lokasi tempat penyimpanan hasil proses *encoding*, setelah itu memulai proses encoding dengan menekan *button process*. Untuk rancangan layar form *MenuEncode* dapat dilihat pada gambar 6 dibawah ini.

Gambar 6: Rancangan Layar Form *MenuEncode*

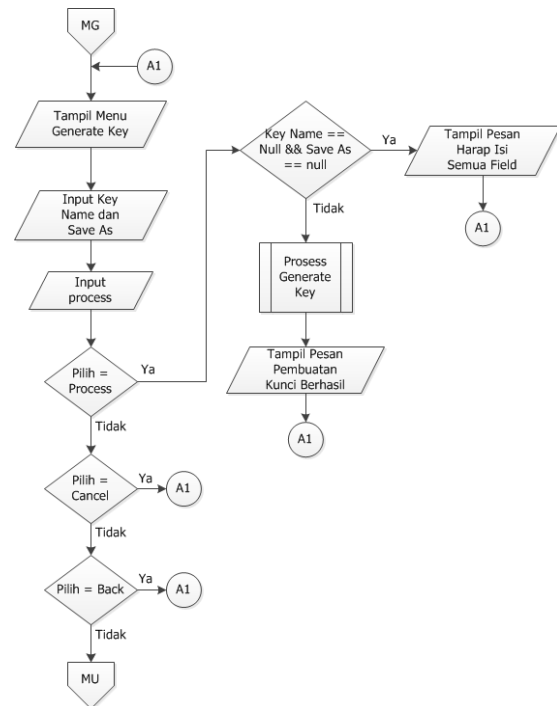
2.13. Rancangan Layar Form *MenuDecode*

Form *MenuDecode* adalah form yang berfungsi untuk melakukan *decoding file*, yaitu mengembalikan file seperti semula. Untuk melakukan proses *decoding* terlebih dulu memilih media video yang sudah disisipi pesan rahasia, setelah itu memilih lokasi penyimpanan hasil *encoding*, lalu memilih *private key*, selanjutnya melakukan proses *encoding file* dengan cara menekan *button process*. Untuk rancangan layar form *MenuDecode* dapat dilihat pada gambar 7 dibawah ini.

Gambar 7: Rancangan Layar Form *MenuDecode*

2.14. Flowchart *MenuGenerate*

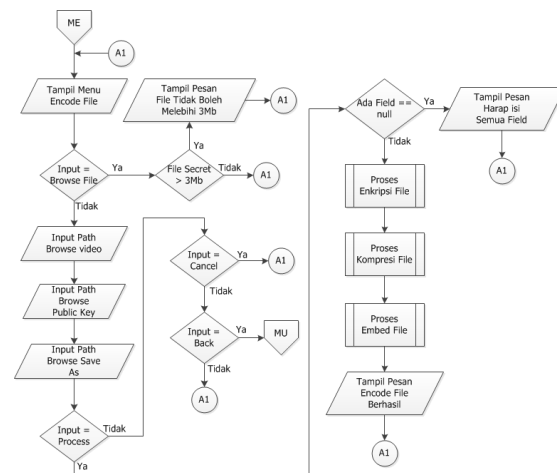
Flowchart form *MenuGenerate* pada gambar 8 menjelaskan alur proses dari form *MenuGenerate*.



Gambar 8: Flowchart *MenuGenerate*

2.15. Flowchart *MenuEncode*

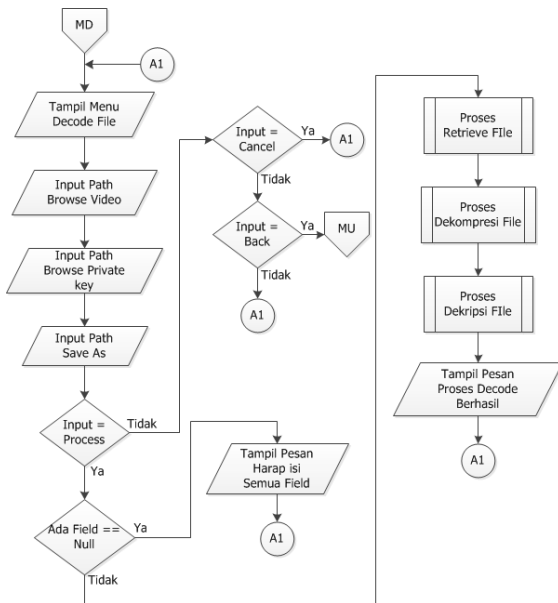
Flowchart form *MenuEncode* pada gambar 9 menjelaskan alur proses dari form *MenuEncode*.



Gambar 9: Flowchart *MenuEncode*

2.16. Flowchart *MenuDecode*

Flowchart form *MenuDecode* pada gambar 10 menjelaskan alur proses dari form *MenuDecode*.



Gambar 10: Flowchart MenuDecode

2.17. Algoritma MenuGenerate

1.	Masuk halaman MG
2.	Tampil menu <i>Generate Key</i>
3.	Input <i>Key Name</i> dan <i>Save As</i>
4.	Input <i>process</i>
5.	If pilih = <i>Process</i>
6.	If <i>Key Name</i> == null && <i>Save As</i> == null then
7.	Tampil pesan harap isi semua field
8.	Kembali ke baris 2
9.	Else
10.	Proses <i>Generate Key</i>
11.	Tampil pesan pembuatan kunci berhasil
12.	Kembali ke baris 2
13.	End if
14.	Else if pilih = <i>Cancel</i> then
15.	Kembali ke baris 2
16.	Else if pilih = <i>Back</i> then
17.	Kembali ke halaman MU
18.	Else
19.	Kembali ke baris 2
20.	End if

2.18. Algoritma MenuEncode

1.	Masuk halaman MG
2.	Tampil menu <i>Encode File</i>
3.	If input = <i>browse file</i> then
4.	If <i>file secret</i> > 3MB then
5.	Tampil pesan File Tidak Boleh Melebihi 3MB
6.	Kembali ke baris 2
7.	Else
8.	Kembali ke baris 2
9.	End if
10.	Input path <i>browse video</i>
11.	Input path <i>browse public key</i>
12.	Input path <i>browse save as</i>
13.	If input = <i>process</i>

15.	If ada <i>field</i> == null then
16.	Tampil pesan Harap Isi Semua Field
17.	Kembali ke baris 2
18.	Else
19.	Proses enkripsi file
20.	Proses kompresi file
21.	Proses embed file
22.	Tampil pesan Encode File Berhasil
23.	Kembali ke baris 2
24.	End if
25.	Else if input = <i>cancel</i> then
26.	Kembali ke baris 2
27.	Else if input = <i>back</i> then
28.	Kembali ke halaman MU
29.	Else
30.	Kembali ke baris 2
31.	End if

2.19. Algoritma MenuDecode

1.	Masuk halaman MD
2.	Tampil menu <i>Decode File</i>
3.	Input path <i>browse video</i>
4.	Input path <i>browse private key</i>
5.	Input path <i>save as</i>
6.	If input = <i>process</i> then
7.	If ada <i>field</i> = null then
8.	Kembali ke baris 2
9.	Else
10.	Proses <i>retrieve file</i>
11.	Proses dekompresi file
12.	Proses dekripsi file
13.	Tampil pesan Proses Decode Berhasil
14.	Kembali ke baris 2
15.	End if
16.	Else if input = <i>cancel</i> then
17.	Kembali ke baris 2
18.	Else if input = <i>back</i> then
19.	Kembali ke halaman MU
20.	Else
21.	Kembali ke baris 2
22.	End if

3. HASIL DAN PEMBAHASAN

3.1. Tampilan Layar

Tampilan layar program berguna untuk mengetahui program yang telah dibuat dapat berjalan secara maksimal atau bahkan terjadi kesalahan – kesalahan yang tidak diinginkan. Berikut ini adalah tampilan program beserta penjelasan penggunaan program di masing – masing tampilan program yang ada pada aplikasi ini.

3.2. Tampilan Layar MenuGenerate

Form *MenuGenerate* merupakan form yang berfungsi untuk membuat sepasang kunci yaitu *public key* dan *private key* untuk proses enkripsi dan dekripsi. Pada form ini terdapat nama kunci dan lokasi penyimpanan kunci yang harus diisi oleh user. Gambar 11 dibawa ini merupakan tampilan layar dari form *MenuGenerate*.

Gambar 11: Tampilan Layar MenuGenerate

3.3. Tampilan Layar MenuEncode

Form MenuEncode adalah form yang berfungsi untuk melakukan proses encoding data. Pada form ini user harus memilih file, memilih media penampung berupa video, memilih kunci publik, dan memilih lokasi penyimpanan. Gambar 12 dibawah ini merupakan tampilan layar dari form MenuEncode.

Gambar 12: Tampilan Layar MenuEncode

3.4. Tampilan Layar MenuDecode

Form MenuDecode adalah form yang berfungsi untuk melakukan decoding data. Pada form ini user diharuskan memilih file berupa video yang telah dilakukan proses encoding sebelumnya, memilih lokasi penyimpanan hasil decoding, dan memilih private key sebagai kunci untuk melakukan proses dekripsi. Gambar 13 dibawah ini merupakan tampilan layar dari form MenuDecode.

Gambar 13: Tampilan Layar MenuDecode

3.5. Tabel Pengujian

Tabel 1: Data Uji Coba

No	Nama File	Jenis File	Ukuran File
1.	Manifest Tgl. 22 Dec'15.docx	Word Document (.docx)	24Kb
2.	Manifest Tgl. 28 Dec'15.xlsx	Excel Document (.xlsx)	20Kb
3.	Manifest Tgl. 01 Apr'16.pdf	File PDF (.pdf)	274Kb
4.	tes1.mp4	Video (.mp4)	13,815Kb
5.	test2.mp4	Video (.mp4)	10,687Kb
6.	test3.mp4	Video (.mp4)	11,209Kb

Tabel 2: Pengujian Proses Encode File

Nama File	Ukuran File	Ukuran File Hasil Enkripsi	Nama Video	Ukuran Video	Ukuran Video Setelah di-Encode	Waktu Proses Encode (Detik)	Status
Manifest Tgl. 22 Dec'15.docx	24Kb	41Kb	tes1.mp4	13,815 Kb	13,913Kb	1,778 Detik	Sukses
Manifest Tgl. 28 Dec'15.xlsx	20Kb	35Kb	test2.mp4	10,687 Kb	10,770Kb	1,608 Detik	Sukses
Manifest Tgl. 01 Apr'16.pdf	274Kb	508Kb	test3.mp4	11,209 Kb	12,425Kb	1,915 Detik	Sukses

Tabel 3: Pengujian Proses Decode File

Nama Video Hasil Encode	Nama File	Ukuran Video Hasil Encode	Ukuran File Hasil Decode	Waktu Decode (Detik)	Status
test1.mp4	Manifest Tgl. 22 Dec'15.docx	13,913Kb	24Kb	3.828 Detik	Sukses
test2.mp4	Manifest Tgl. 28 Dec'15.xlsx	10,770Kb	20Kb	7.848 Detik	Sukses
test3.mp4	Manifest Tgl. 01 Apr'16.pdf	12,425Kb	274Kb	20.253 Detik	Sukses

3.6. Evaluasi Program

Setelah dilakukan pengujian program terhadap program aplikasi ini, didapatkan beberapa kelebihan dan kekurangan dari aplikasi ini, yaitu sebagai berikut:

Kelebihan Program

- 1) Memberikan sistem pengamanan kunci yang baik.
- 2) Memberikan pengamanan ganda kepada file agar lebih aman.
- 3) Jika hasil video dari proses encode dengan sebelum encode dijalankan, maka tidak akan terlihat bedanya, karena proses encode ini tidak akan merusak kualitas dari video itu sendiri.
- 4) File penampung menggunakan video, sehingga hasil ukuran file encode dengan file sebelum di-encode tidak terlihat jauh perbedaannya. Hal ini dikarenakan ukuran dari video itu sendiri sudah besar jadi tidak terlalu terlihat beda ukurannya sehingga meminimalkan kecurigaan pada pihak lain.
- 5) Aplikasi yang dibuat dapat mengembalikan isi file seperti semula tanpa adanya pengurangan atau penambahan.

Kekurangan Program

- 1) Semakin besar file yang digunakan, maka semakin lama proses encode ataupun decode file.

- 2) Proses *encoding* dan *decoding* dengan ukuran *file* yang besar diharapkan dapat berjalan lebih cepat dengan *hardware* yang lebih baik.
- 3) Satu media penampung hanya bisa menyisipkan satu *file* saja.

4. KESIMPULAN DAN SARAN

4.1. Kesimpulan

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

- a. Aplikasi ini mampu mengamankan *file* rahasia dengan baik.
- b. Dengan adanya aplikasi ini, pihak perusahaan tidak perlu khawatir lagi tentang permasalahan keamanan data *manifest* jamaah haji dan umrah.
- c. Satu kunci publik dan privat dapat digunakan lebih dari satu kali untuk proses *encode*.
- d. Dengan menggunakan kunci yang berbeda saat *encoding* dan *decoding* maka keamanan data rahasia semakin terjaga dan aman.
- e. Proses *decode* dengan menggunakan kunci yang sesuai akan mengembalikan data seperti semula tanpa mengalami perubahan sedikitpun.

4.2. Saran

Adapun saran yang mungkin diperlukan untuk membuat aplikasi ini dapat berjalan lebih baik lagi antara lain:

- a. Ukuran *file* hasil enkripsi dan dekripsi diharapkan menjadi lebih kecil lagi dengan menggunakan algoritma kompresi yang lebih baik
- b. Proses *encoding* dan *decoding* dengan ukuran *file* yang besar diharapkan dapat berjalan lebih cepat dengan *hardware* yang lebih baik

DAFTAR PUSTAKA

- Adianson, Niko, Yupati, & Adhadi Kurniawan. (2015). "Analisa Perbandingan Performansi RSA (Rivest Shamir Adleman) dan ECC (Elliptic Curve) Pada Protokol Secure Socket Layer (SSL)". Jurnal Media Infotama. Vol. 11, No. 1.
- Amal, Viki, Miyagina, Alfa Ryano, Yohannis. (2015). "Aplikasi Steganografi Pada Citra Digital Menggunakan Algoritma Discrete Cosine Transform". KALBIScientia Jurnal Sains dan Teknologi.
- Amin, M. Miftakul. (2014). "Image Steganography Dengan Metode Least Significant Bit (LSB)". Computer Science Research and Its Development Journal (CSRID). Vol. 6, No. 1, Hal. 53-62.
- Azhari, A Ihsan, Hidayatno, Achmad, Isnanto, R Rizal. (2012). "Aplikasi Steganografi Pada Berkas Video MP4 Dengan Menggunakan Bahasa Pemrograman Java".
- Cahyadi, Tri. (2012). "Implementasi Steganografi LSB dengan Enkripsi Vigenere Cipher pada Citra JPEG, TRANSIENT". ISSN: 2302-9927, 282.
- Harahap, Muhammad, Khoiruddin. (2016). "Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher dan One Time PAD". Jurnal Nasional Informatika dan Teknologi Jaringan. E-ISSN: 2540-7600, P-ISSN: 2540-759.
- Kusminandar, Taufan. (2015). "Aplikasi Steganografi Untuk Menyembunyikan Teks Dalam Video Menggunakan Metode Least Significant Bit (LSB) Dengan Enkripsi Vigenere Cipher".
- Lubis, Muhammad, Safri, Mohammad Andri, Biduman, Karina Lolo, Manik. (2013). "Penggunaan Algoritma RSA Dengan Metode The Sieve of Eratosthenes dalam Enkripsi dan Deskripsi Pengiriman Email". Seminar Nasional Aplikasi Teknologi Informasi (SNATI).
- Martono, Irawan. (2013). "Penggunaan Steganografi dengan Metode End of File (Eof) pada Digital Watermarking". Jurnal TICOM. Hal. 229-235, Vol. 2, No. 1.
- Meidina. (2013). "Visualisasi Algoritma RSA Dengan Menggunakan Bahasa Pemrograman Java". Depok: Universitas Gunadarma.
- Musril, Hari, Antoni. (2012). "Studi Komparasi Metode Arithmetic Coding dan Huffman Coding Dalam Algoritma Entrophy Untuk Kompresi Citra Digital". Jurnal Teknologi Informasi & Pendidikan. ISSN: 2086-4981, Vol. 5, No. 2.
- Pabokory, F Nandar, Astuti, I Fitri, Kridalaksana, A Warsa. (2015). "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard". Jurnal Informatika Mulawarman. Vol. 10 No. 1, ISSN 1858 – 4853.
- Prasestyo, Bagus, Galang, Santoso, Edy, Marji. (2013). "Kompresi File Audio Wave Menggunakan Algoritma Huffman Shift Coding". Malang: Universitas Brawijaya.
- Sembiring, Sandro. (2013). "Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan teks Pada Gambar Dengan Metode End of File". Pelita Informatika Budi Dharma. Vol. 4, No. 2.
- Zelvina, Anandia, Efendi, Syahril, Arisandi, Dedi. (2012). "Perancangan Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal Untuk Mahasiswa". Jurnal Dunia Teknologi Informasi. Vol. 1, No. 1, ISSN 2337-3415.