SISTEM PENGAMANAN GAMBAR MENGGUNAKAN ALGORITMA AES 256 BERBASISJAVA MOBILE PADA PT.ANTAR MITRA SEMBADA

Bintang Kristoper Simanjuntak[1)], Ir.Siswanto, M.M[2)]
[1]Teknik Informatika,Fakultas Teknologi Informasi, Universitas Budi Luhur
[1.2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : bintangkristoper@gmail.com[1)], siswanto@budiluhur.ac.id[2)]

Abstrak

Pada penelitian ini dibahas mengenai bagaimana suatu pengamanan file gambar dengan menggunakan algoritmaAES 256untuk proteksi keamanan terhadap suatu gambar, pengamanan dilakukan dengan cara melakukan enkripsi dan dekripsi. Pengimplementasian dari penelitian ini yaitu membuat sebuah *software* yang akan diletakkan di sisi *admin* yang berfungsi untuk menginput dokumen gambar yang diletakkan di sisi sistem. PT.Antar Mitra sembada belum memiliki sistem pengamanan terutama pada pengamanan gambar, maka dari itu dibuatlah sebuah sistem yang memiliki fasilitas untuk mengamankan sebuah gambar, untuk file gambar yang memiliki format.png,.Jpg, .Gif dengan menggunakan metode algoritma AES 256.Dengan demikian gambar dapat terjamin keamanannya. Terjaminnya keamanan sebuah gambar dapat dikatakan berhasil jika *software* berhasil mengenkripsi sebuah gambar sehingga apabila terjadi penyadapan terhadap sebuah gambar, penyadap tidak akan mengerti gambar tersebut. Kesimpulan dari penelitian ini yaitu Aplikasi yang dibuat dapat mengenkripsi dan dekripsi sebuah gambar yang dianggap rahasia dengan proses enkripsi dan dekripsi dan Aplikasi dapat mengembalikan sebuah gambar secara utuh yang sebelumnya telah di enkripsi dengan cara proses deskripsi.

Kata kunci: Pengamanan file gambar, Algoritma AES 256, Kriptografi, *Java mobile*

1. PENDAHULUAN

PT.Antar Mitra Sembada adalah sebuah perusahaan yang bergerak di bidang distributor parmasi dan alat kesehatan serta distributor untuk PT.Customer Good. Banyak file gambar perusahaan yang bersifat rahasia dan tidak boleh dirubah oleh pihak yang tidak berhak untuk merubahnya. Untuk mengamankan file gambar dapat menggunakan kriptografi. Oleh Karena itu, pengguna membutuhkan bantuan untuk keamanan akan file gambar yang disimpannya. Penerapan kriptografi pada PT. Antar Mitra Sembadaakan difokuskan pada cara bagaimana kriptografi dapat mengamankan gambar yang tersimpan menjadi aman sampai dengan gambar dibuka oleh pihak yang berhak untuk membukanya. Dalam hal ini gambar yang ingin di amankan adalah gambar yang memiliki format .png, gambar yang dimiliki perusahaan yang dianggap gambar tersebut perlu diamankan supaya tidak ada pihak lain yang dapat merubah atau mencuri gambar tersebut untuk di salah gunakan kecuali karyawan yang diberikan akses untuk mengubah gambar tersebut. Oleh karena itu di buatlah suatu sistem aplikasi pengamanan gambar yang dimaksudkan untuk mengamankan filegambar yang ada pada PT.Antar Mitra Sembada. Algoritma yang digunakan adalah algoritma AES 256, algoritma AES 256 dipilih karena dianggap algoritma AES 256 lebih cepat dalam hal eksekusi enkripsi gambar, sehingga gambar yang telah dienkripsi mempunyai tingkat keamanan tinggi terhadap pencurian data.Secara umum tujuan penelitian ini adalah untuk mengamankan data dalam bentuk gambar agar tidak bisa dicuri olehorang lain dan menghasilkan sebuah aplikasi pengamanan gambar berbasis *java mobile* yang mudah digunakan oleh pengguna. Tujuan dari penelitian ini adalah untuk mengimplementasikan algoritma AES 256 dalam enkripsi dan deskripsi sebuah gambar yang memiliki format .png, .Jpg, .Gif. Berikut ini adalah beberapa landasan teori yang di gunakan dalam penelitian ini :

Kriptografi

Kriptografi merupakan suatu ilmu atau seni untuk menjaga kerahasiaan pesan dengan cara menyadikannya ke dalam bentuk yang tidak dapat di mengerti (Wardoyo, Imanullah, & Fahrizal, 2014).

Proses menyandikan plainteks menjadi cipherteks disebut dengan enkripsiSedangkan proses mengembalikan cipherteks menjadi plainteks semula dinamakan dekripsi. Pesan yang di enkripsi atau di dekripsi dapat berupa data atau informasi yang dikirimatau disimpan di dalam sebuah media penyimpanan.Pesan yang disimpandapat berupa tekstetapi bisa jugaberbentuk gambar, suara dan video.Cipherteks harus dapat dikembalikan lagi menjadi plainteks semula agar pesan yang diterima bisa dibaca.Kriptografi mempunyai sejarah yang panjang, untuk informasi yang lengkap mengenai sejarah kriptografi dapat ditemukan di dalam buku David Kahn yang berjudul *The Codebreakers*. Buku yang tebalnya 1000 halaman ini menulis secara rinci sejarah kriptografi mulai dari penggunaan kriptografi oleh Bangsa Mesir 4000 tahun yang lalu (berupa *hieroglyph* yang terdapat pada piramid) hingga penggunaan kriptografi pada abad ke-20 (Alfred J. Menezes, Paul C. van Oorschot, 1996).Secara sejarah ada empat kelompok yang berkontribusiterhadap

perkembangan kriptografi,dimana mereka menggunakan kriptografi untuk menjamin kerahasiaan dalam komunikasi suatu pesan penting, yaitu kalangan militer, kalangan diplomatik, penulis buku harian, dan pencinta.Diantara keempat kelompok ini, kalangan militer yang memberikan kontribusi paling penting karena pengiriman pesan di dalam suasana perang membutuhkan teknik enkripsi dandekripsi yang rumit.

Kriptografi dapat di bedakan menjadi dua jenis yaitu:

1. Kriptografi Simetri

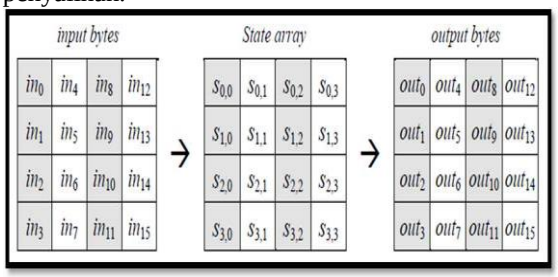
Pada kriptografi simetri, kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Keamanan sistem kriptografi simetri terletak pada kerahasiaan kunci.

2. Kriptografi Asimetri

Pada sistem kriptografi asimetri, kunci untuk proses enkripsi tidak sama dengan kunci untuk proses dekripsi. Sebab kunci untuk enkripsi tidak rahasia dan dapat diketahui oleh siapapun, sementara kunci untuk dekripsi hanya diketahui oleh penerima pesan

Algoritma AES

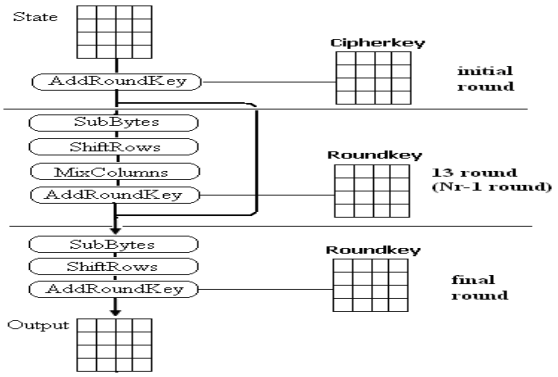
Input dan *output* dari algoritma AES terdiri dari urutan data sebesar 128 *bit*.Data yang sudah terbentuk dalam satu kelompok 128 *bit* tersebut disebut juga sebagai blok data yang nantinya akan dienkripsi menjadi *ciphertext*.*Cipher key* dari AES terdiri dari *key* dengan panjang 128 *bit*, 192 *bit*, atau256*bit*.Perbedaan panjang kunci akan mempengaruhi jumlah *round* yang akan diimplementasikan pada algoritma AES.Dibuat pada gambar 1 yang memperlihatkan jumlah *round*yang harus diimplementasikan pada masing masing panjang kunci (Yuniati, Indriyanta, & C, 2009). Pada dasarnya, operasi AES dilakukan terhadap *array of byte* dua dimensi yang disebutdengan *state*.*State* mempunyai ukuran *NROWS* X *NCOLS*. Awal enkripsi data masukan yang berupa in0, in2, in3, in4, in5, in6, in7, in8, in9, in10, in11, in12, in13, in14, in15 disalin ke dalam *array state*. *State* inilah yang nantinya dilakukan operasi enkripsi / dekripsi. Kemudian keluarannya akan ditampung ke dalam *array out*.Gambar 1 mengilustrasikan proses penyalinan.



Gambar 1. Proses Input Bytes, State Array, dan Output Bytes

a. Proses Enkripsi *Advanced Enryption Standard*

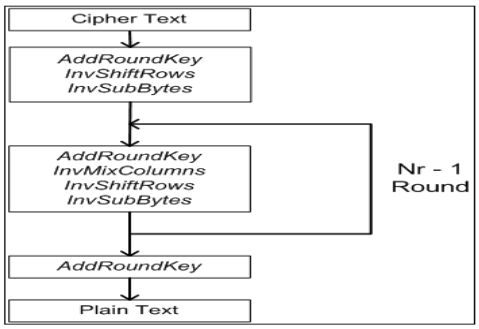
Proses enkripsi algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu *SubBytes,ShiftRows,Mixcolumns,* dan *AddRoundKey*. Pada awal proses enkripsi masukkanyang telahdi *copy*kan ke dalam *state* akan mengalami transformasi*AddRoundKey*. Setelah itu*state* akan mengalami transformasi *SubBytes,ShiftRows,MixColumns,* dan *AddRoundKey* secaraberulang-ulang sebanyak Nr. Ilustrasi proses enkripsi AES dapatdigambarkan seperti pada Gambar 2.



Gambar 2 : Ilustrasi Proses Enkripsi AES

b. Proses Dekripsi Advanced Encryption Standard

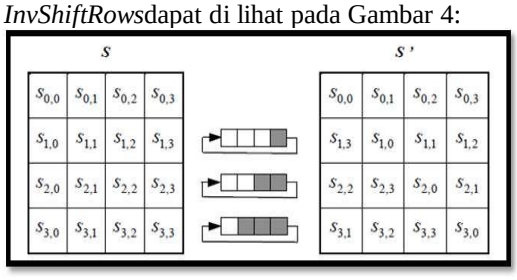
Transformasi *cipher* dapat dibalikkan dan dapat di implementasikan dalam arah yang berlawanan untukmenghasilkan *inverse cipher* yang mudah dimengerti untuk algoritma AES.Transformasi byte yangdigunakan pada *invers cipher* adalah *InvShiftRows*, *InvSubBytes*,*InvMixColumns*, dan *AddRoundKey*. Ilustrasi dekripsi Algoritma AES dapat dilihat pada gambar 3berikut:



Gambar 3 : Ilustrasi Proses Dekripsi AES

1) **InvShiftRows**

InvShiftRows merupakan transformasi byte yang berkebalikan dengan transformasi *ShiftRows*. Pada transformasi *InvShiftRows*Ilustrasi transformasi *InvShiftRows*dapat di lihat pada Gambar 4:



Gambar 4 : Transformasi InvShiftRows

2) InvSubBytes

InvSubBytes juga merupakan transformasi *bytes* yang berkebalikan dengan transformasi *SubBytes*, gambar*Inverse S-Box* dapat dilihat pada Gambar 5 :

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Gambar 5 : Tabel Inverse S-Box

3) InvMixColumns

Setiap kolom didalam *state* akan dikalikan dengan matrik perkalian dalam AES, dapat dituliskan sebagai berikut :

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

2. METODE PENELITIAN

Dalam penelitian ini, beberapa metode digunakan untuk memperoleh informasi yang diperlukan dan menyelesaikan masalah yang ditemui. Adapun metode yang di gunakan adalah *prototyping* yaitu metode yang merepresentasikan versi awal dari sistem perangkat lunak yang akan digunakan untuk menunjukan konsep, dan mengetahui lebih lanjut tentang masalah dan memberikan solusi, dengan langkah - langkah sebagai berikut :

a. Studi literature

Metode ini menggunakan pembelajaran dengan cara mengumpulkan, membaca dan memahami jurnal ilmiah, makalah serta refrensi lain guna mendapatkan informasi yang dibutuhkan dalam menunjang penelitian, peneliti juga melakukan wawancara langsung kepada pihak instansi PT.Antar Mitra Sembada.

b. Analisa Data

Metode ini yaitu menganalisa data yang di gunakan dan menganalisa algoritma yang di gunakan serta teknik teknik yang digunakan.

c. Perancangan Sistem

Merancang suatu sistem aplikasi untuk mengimplementasikan algoritma AES 256 dengan menggunakan bahasa pemrograman *Java mobile*.

d. Pengujian system

Metode pengujiannya adalah dengan cara menguji aplikasi yang telah dibuat melalui data yang di uji, dan mengamati hasil dari uji coba data tersebut.

e. Penarikan Kesimpulan

Metode ini dilakukan dengan cara Menarik kesimpulan dari program yang telah diujicoba.

3. ANALISA DAN RANCANGAN PROGRAM

3.1 Skema Proses Keseluruhan Aplikasi

Enkripsi adalah proses pengacakan sebuah *file*. Algoritma yang digunakan pada aplikasi ini adalah algoritma AES 256 yang akan mengenkripsi dan dekripsi gambar. Proses keseluruhan aplikasi ini dapat diuraikan sebagai berikut:

a. Pada tampilan awal user akan di tampilkan empat buah form yaitu form password, choose file,encrypt,decrypt.
b. Lalu user dapat memilih form *Encrypt* untuk mengenkripsi gambar dan form d*ecrypt* untuk mendekripsi gambar.
c. Masukkan password untuk melakukan enkripsi.
d. pilih gambar yang akan di enkripsi.
e. lalu klik Tombol *encrypt* untu melakukan enkripsi.
f. Lalu jika berhasil akan ada pemberitahuan “sukses Encrypt”.
g. Setelah itu file hasil enkripsi akan tersimpan dan tidak bisa untuk di buka.
h. Masukkan password untuk melakukan dekripsi.
i. Lalu pilih file hasil enkripsi yang akan di dekripsi.
j. Lalu klik tombol *decrpt* untuk melakukan dekripsi.
k. Lalu jika berhasil akan ada pemberitahuan “sukses Decrypt”.
l. Setelah itu file hasil dekripsi akan tersimpan dan kembali seperti aslinya.
m. Jika diperlukan pengenkripsian gambar kembali kita dapat mengulangi langkah C sampai dengan F.
n. Jika diperlukan pengdekripsian gambar kembali kita dapat mengulangi langkah H sampai dengan K

3.2 Perangkat yang digunakan

Perangkat yang dibutuhkan dalam membangun aplikasi ini terdiri dari perangkat keras dan perangkat lunak, yang terdiri sebagai berikut :

a). Perangat Keras

Perangak keras yang dibutuhkan dalam membanun perangkat lunak ini memiliki spesifikasi yang dapat dilihat pada tabel 3.1 sebagai berikut:

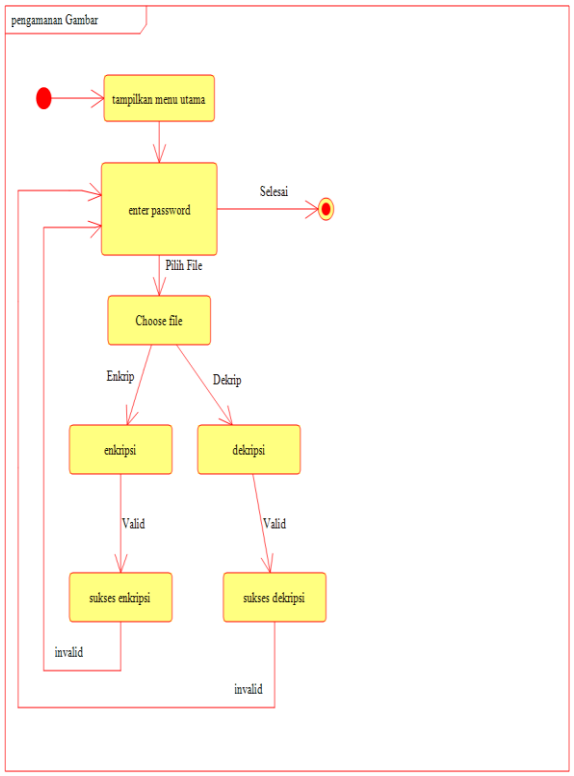
1. Cpu : Intel® Core™ i3
2. RAM : 6.00 GB
3. Keyboard :Internal Keyboard Laptop

b). Perangkat Lunak

1. Sistem Operasi :Windows 8
2.*Tools Editor* :Android Studio

3.3 State Diagram

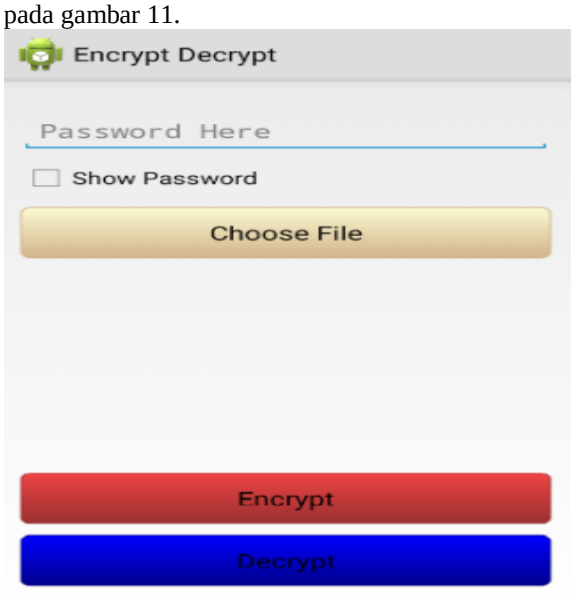
Statediagram adalah suatu diagram yang menggambarkan proses daur hidupdari sebuah objek,mulai dari awal objek tsb diinisialisasi sampai di-destroy.dapat di lihat pada gambar 10.



Gambar 10 : State Diagram

3.4*Form* Halaman Utama

Pada *form* Menu Utama terdiri dari empat *form* yang ditampilkan yaitu form insert password, form choose file, form Enkripsi dan form Deskripsi. Dapat di liht pada gambar 11.

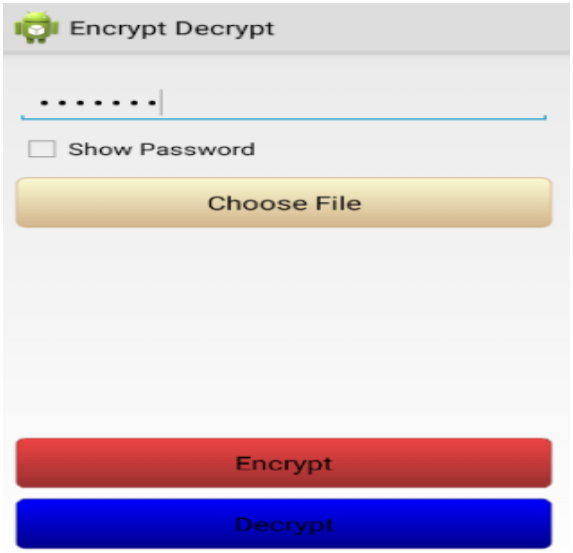


Gambar 11: Form Halaman Utama

3.5Form Insert Password

Pada *form insert passworduser* harus memasukkan password terlebih dahulu untuk melakukan proses enkrip atau dekrip, password yang di masukkan saat proses enkripsi harus sama untuk melakukan proses dekripsi.

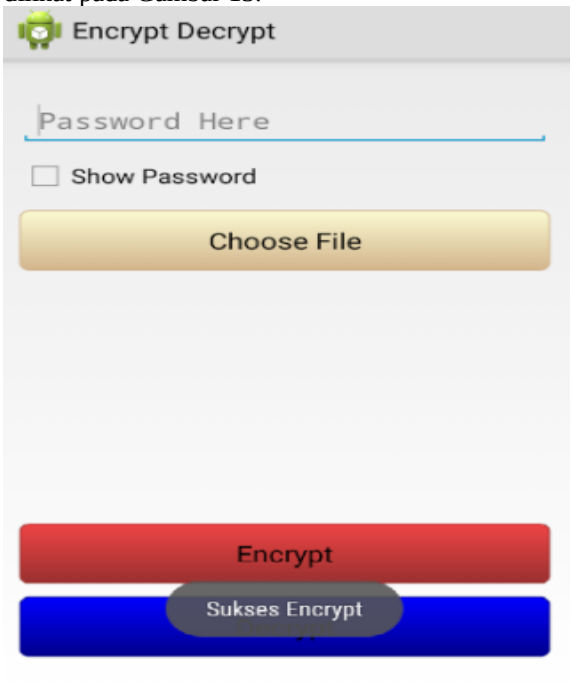
Tampilan layar dapat dilihat pada Gambar 12.



Gambar 12:Form Insert Password

3.6 Form Encrypt

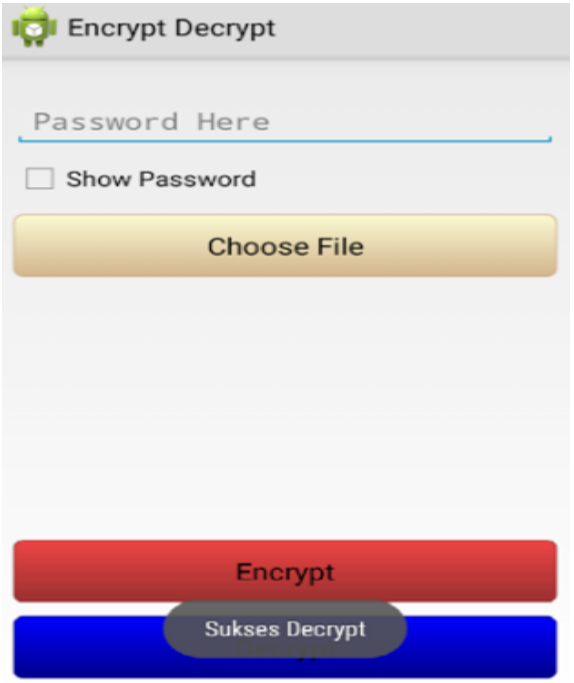
Pada *form Encrypt*, *user* dapat melakukan proses enkripsi setelah user memasukkan password untuk proses enkripsi lalu memilih gambar yang akan di enkripsi, dan jika berhasil melakukan enkripsi akan tampil pesan “Sukses encrypt”. Tampilan layar dapat dilihat pada Gambar 13.



Gambar 13.Form Enkripsi sukses

3.7 Form Decrypt

Pada *form* Decrypt, *user* dapat melakukan proses dekripsi dan jika berhasil melakukan dekripsi akan tampil pesan “Sukses decrypt”. Tampilan layar dapat dilihat pada Gambar 14.



Gambar 14 : Tampilan Layar Sukses Dekripsi

4. KESIMPULAN

Berdasarkan hasil pengamatan yang telah dilakukan terhadap aplikasi yang telah dibuat, dapat ditarik kesimpulan sebagai berikut :

a. Aplikasi yang dibuat dapat mengenkrip sebuah gambar yang dianggap rahasia.
b. Aplikasi dapat mengembalikan isi pesan secara utuh yang sebelumnya telah di *enkripsi* dengan cara proses *deskripsi*.
c. Rata-Rata waktu yang di pelukan untuk melakukan enkrip gambar adalah 4,66 ms
d. Rata-Rata waktu yang diperlukan untuk melakukan dekripsi gambar adalah 4,25

Saran –saran untuk pengembangan selanjutnya:

a. Semoga aplikasi ini bisa dikembangkan lagi untuk pencarian gambar selain format .png, .Jpg, .Gif
b. Semoga kedepannya aplikasi ini dapat mengamankan yang lain selain gambar contohnya seperti video,dokumen dll

5. DAFTAR PUSTAKA

[1]Alfred J. Menezes, Paul C. van Oorschot, S. A. V. (1996). *handbook of applied cryptography*. new york: CRC Press.

[2]Kaoru Kurosawa, G. H. (Ed.). (2013). *Public-Key Cryptography -- PKC 2013: 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, Feburary 26 -- March 1, 2013, Proceedings* (berilustra). Springer.

[3]Wardoyo, S., Imanullah, Z., & Fahrizal, R. (2014). Enkripsi Dan Dekripsi File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android. *Setrum*, *3*(1), 43–53.

[4]Yuniati, V., Indriyanta, G., & C, A. R. (2009). Enkripsi dan Dekripsi dengan Algoritma AES 256 untuk Semua Jensis File. *Journal Informatika*, *5*(1), 22–31.