Jurnal Ilmiah Teknologi - Informasi dan Sains (TeknoIS)
Volume 9 Nomor 1 Bulan Mei 2019 Hal. 1-9
p-ISSN : 2087-3891 dan e-ISSN : 2597-8918

Aplikasi Keamanan Data Gambar Menggunakan Algoritma RSA (*Rivest Shamir Adleman*) Berbasis Desktop

Muhamad Andra Fahreza[1], Arif Harbani[2]
Program Studi Teknik Informatika
STIKOM Binaniaga Bogor.
Email: arifharbani@gmail.com

ABSTRACT

A common way to do when data communication is the exchange of information in the form of photos, images. Exchange of data must be confidential because in the picture there are various kinds of important information, so that the contents of the messages sent are still confidential and unknown to other parties. and Decryption by applying the RSA Algorithm. The RSA algorithm is a highly advanced algorithm in the field of public key cryptography (public key cryptography) that is very popular and is still used today. In this study the author can produce an application to secure image data through the process of Encryption and Decryption which uses a key / password so that the information contained in the image is kept confidential. From the questionnaire with the number of respondents 91 students the percentage of eligibility obtained was 84.1%. then it can be categorized into the interpretation that is "very feasible".

Keywords*: Cryptography, RSA Algorithm, Encryption, Decryption*

ABSTRAK

Cara yang umum dilakukan pada saat komunikasi data yaitu pertukaran informasi berupa foto, gambar. Pertukaran data harus bersifat rahasia dikarenakan dalam gambar terdapat berbagai macam informasi penting, agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain.Untuk penerapan keamanan data gambar dapat menggunakan kriptografi, maka dari itu perlunya suatu algoritma untuk mempersulit keamanan tersebut melalui proses Enkripsi dan Dekripsi dengan penerapan Algoritma RSA. Algoritma RSA adalah algoritma yang sangat maju dalam bidang kriptografi kunci public (kriptografi public key) yang sangat popular dan masih digunakan sampai saat ini. Pada penelitian ini penulis dapat menghasilkan Aplikasi untuk mengamankan data gambar dengan melalui proses Enkripsi dan Dekripsi yang menggunakan kunci/password agar informasi yang terdapat pada gambar tetap terjaga kerahasiaannya. Dari kuesioner dengan jumlah responden 91 mahasiswa presentase kelayakan yang didapat sebesar 84.1%. maka dapat dikategorikan kedalam interpretasi yang ***"Sangat layak".***

Kata Kunci*: Kriptograpi, Algoritma RSA, Enkripsi, Dekripsi*

PENDAHULUAN

Komunikasi data merupakan teknologi komunikasi yang secara khusus berkenaan dengan transmisi atau pemindahan data dan informasi antara komputer melalui media komunikasi data. Perkembangan teknologi semakin pesat, media komunikasi pun saat ini banyak yang menyediakan kemudahan untuk berbagi informasi. Informasi yang mudah diakses akan menjadi rentan untuk disalahgunakan oleh pihak yang tidak bertanggung jawab.

Informasi merupakan kumpulan data atau fakta yang diolah menjadi bentuk yang berguna bagi penerima informasi. Suatu informasi harus dilindungi dengan baik, keamanan data menjadi hal penting agar data tersebut tidak disalahgunakan oleh pihak yang tidak bertanggung jawab sehingga perlu penerapan keamanan kriptografi.

Penerapan keamanan data menggunakan kriptografi diperlukan suatu algoritma untuk mempersulit keamanan tersebut agar tidak mudah untuk disadap oleh pihak yang tidak bertanggung jawab. Algoritma RSA adalah algoritma dalam bidang kriptografi kunci public (*kriptografi public key*) yang

sangat popular dan masih digunakan sampai saat ini. RSA merupakan algoritma yang paling cocok untuk *digital signature* seperti halnya enkripsi. Algoritma RSA masih digunakan secara luas dalam *protocol electronic commerce* dan dalam pengamanan dengan kunci yang sangat panjang. Algoritma RSA menggunakan kunci publik karena kunci enkripsi dapat dibuat publik. Keamanan algoritma RSA terletak pada kunci enkripsi yang berbeda dengan kunci untuk dekripsinya. Keamanan enkripsi dan dekripsi terletak pada kesulitan untuk memfaktorkan modulus n yang sangat besar.

Tingkat kesulitan kekuatan algoritma RSA terletak dalam memfaktorkan bilangan menjadi faktor primanya yaitu memfaktorkan n menjadi p dan q. Ketahanan algoritma RSA terletak pada bentuk serangan, terutama serangan *brute force*. Kompleksitas dekripsinya dapat ditentukan secara dinamis dengan cara menentukan nilai p dan q yang besar pada proses pembangkitan pasangan kunci, sehingga dihasilkan sebuah *key space* yang besar. Tetapi ukuran kunci privat yang terlalu besar akan mengakibatkan proses dekripsi yang cukup lambat, terutama untuk ukuran pesan yang besar. Oleh karena itu, RSA umumnya digunakan untuk mengenkripsi pesan berukuran kecil seperti kata kunci dari enkripsi simetris seperti DES dan AES yang kemudian kunci tersebut dikirim secara bersamaan dengan pesan utama.

Rumusan masalah :

1. Apakah keamanan file gambar penting untuk menjaga kerahasiaan file tersebut ?
2. Apakah diperlukan aplikasi untuk mengamankan file gambar tersebut ?
3. Bagaimana penerapan algoritma RSA untuk keamanan file gambar dalam bentuk aplikasi pengamanan?

Identifikasi Masalah

1. Pengamanan file gambar yang belum terjaga kerahasiaannya
2. Belum adanya aplikasi pengamanan file gambar

Pernyataan Masalah

Pada penelitian ini terdapat suatu permasalahan mengenai keamanan file gambar, setelah dilakukan penyebaran kuesioner kepada mahasiswa dengan sampel responden 91 mahasiswa dari 118 mahasiswa maka diambil kesimpulan perlunya sebuah aplikasi pengamanan file gambar.

Tujuan Pengembangan

1. Mengamanan kerahasiaan file gambar dengan menggunakan kunci
2. Menerapkan algoritma RSA dalam aplikasi pengamanan file gambar

Spesikasi Produk yang diharapkan

1. Dapat mempermudah penggunaan
2. Bekerja dengan semestinya
3. Dapat merahasiakan informasi pada file gambar agar keamanan terjaga
4. Mengenkripsi dan mendekripsi file gambar dengan baik sehingga tidak mengubah makna dan informasi yang terkandung didalamnya

Keterbatasan Penelitian

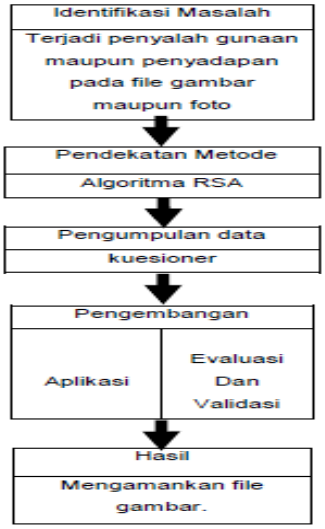
1. File yang dapat di enkripsi yaitu file gambar dengan format .jpg
2. Ukuran file gambar yang terlalu besar akan mengakibatkan proses enkripsi dekripsi yang cukup lambat (ukuran file 100 kb memerlukan waktu 5 menit lebih)
3. Metode yang digunakan adalah Algoritma RSA

METODE

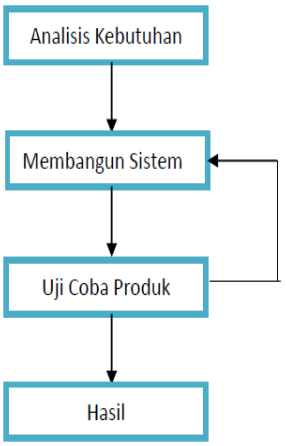
Kerangka Pemikiran

Saat komunikasi data berlangsung kemungkinan data dapat disadap oleh pihak yang tidak bertanggung jawab sangat besar, oleh karena itu perlunya keamanan kriptografi. Pendekatan atau metode penelitian yang digunakan dalam proses pengamanan data file gambar adalah Algoritma *Blowfish*. Data yang diperlukan yaitu dengan cara observasi secara langsung yang berupa data gambar, maupun foto. Model pengembangan dari penelitian ini adalah pembuatan aplikasi desktop dimana data file berupa

gambar akan di enkripsi dan kemudian akan didekripsikan oleh penerima dengan tingkat keamanan menggunakan password. Kerangka pemikiran pada penelitian ini dapat digambarkan pada gambar 1.



Gambar 1. Kerangka pemikiran



Gambar 2. Prosedur Pengembangan

Penjelasan tentang kerangka pemikiran pada gambar 1 diatas, yaitu:

1. Identifikasi masalah yaitu untuk menetapkan tujuan masalah pada penelitian ini
2. Dengan menggunakan Algoritma RSA dapat digunakan untuk mengamankan data gambar.
3. Pengumpulan data berdasarkan kebutuhan pengguna, pada pengumpulan data digunakan 2 kuesioner, yang terdiri dari 1 kuesioner untuk menentukan permasalahan dan 1 kuesioner lagi setelah penerapan penelitian dilakukan agar mengetahui presentase kelayakan aplikasi pengamanan file gambar berbasis desktop.
4. Pada tahap Pengembangan yang dilakukan yaitu pembuatan aplikasi berbasis desktop dan kemudian dilakukan evaluasi dan validasi berdasarkan dari aplikasi yang dibuat
5. Hasil yang diharapkan yaitu aplikasi pengamanan data gambar yang dapat mengamankan dengan baik

Model Pengembangan

Dalam penelitian ini metode yang digunakan adalah eksperimen, artinya bahwa penelitian yang dilakukan untuk melakukan uji coba terhadap permasalahan tertentu dengan penggunaan teori tertentu sehingga didapatkan hasil pengujian yang tepat antara permasalahan yang diambil dengan teori yang digunakan.

Prosedur Pengembangan

Prosedur pengembangan dalam penelitian yang dilakukan dapat digambarkan pada gambar 2 diatas, dengan mendefinisikan prosedur pengembangan yaitu:

1. Analisa kebutuhan, yaitu pengumpulan data-data yang diperlukan untuk digunakan sebagai dasar dari pengembangan sistem.
2. Membangun sistem, yaitu penerapan metode yang sudah sesuai dengan kebutuhan.
3. Uji Coba Produk, yaitu menguji produk apakah sudah sesuai dengan kebutuhan. Apabila uji produk belum berhasil maka akan diulang terus sampai hasil yang didapat sesuai.
4. Hasil, hasil yang diharapkan sesuai dengan kebutuhan yaitu aplikasi yang dapat digunakan untuk mengamankan suatu data gambar dengan baik.

HASIL DAN PEMBAHASAN

OBJEK PENELITIAN

Responden dalam penelitian ini adalah mahasiswa STIKOM Binaniaga yang pada umumnya yaitu mahasiswa teknik informatika. Dari penelitian diawal menyatakan pentingnya keamanan gambar

dalam pertukaran data. Pertukaran data harus bersifat rahasia agar isi pesan yang dikirimkan tetap terjaga kerahasiaannya dan tidak diketahui pihak lain. Pentingnya keamanan data gambar dinyatakan dalam sebuah aplikasi, yang tentunya aplikasi tersebut dapat mengamankan gambar dengan baik menggunakan kunci atau password yang sifatnya rahasia.

HASIL PENGEMBANGAN

Analisa kebutuhan

Yaitu pengumpulan data-data untuk digunakan sebagai dasar dari pengembangan sistem.

a. Kebutuhan Pengguna

1. Aplikasi yang mudah digunakan
2. Dapat menjaga kerahasiaan Gambar
3. Menggunakan kunci untuk pengamanan
4. Proses Enkripsi dan Dekripsi cepat

b. Kebutuhan Sistem

Tabel 1 Kebutuhan Sistem

Fitur Aplikasi	Keterangan
Enkripsi	Untuk mengenkrip Gambar menjadi file txt
Dekripsi	Untuk mendekripsikan atau mengembalikan kebentuk semula dari file txt ke Gambar
Password	Untuk memasukan kunci pada file yang akan di Enkripsi atau Dekripsi

c. Kebutuhan Aplikasi

1. Hardware :

Tabel 2 Kebutuhan Aplikasi Hardware

Item Hardware	Spesifikasi
PC / Laptop	Intel dual core, RAM 2 GB, 500GB HDD
Smartphone	RAM 2 GB, 32GB Memori

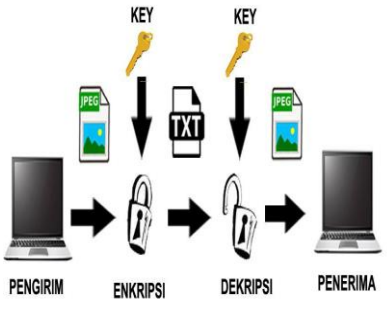
2. Software :

Tabel 3 Kebutuhan Aplikasi Software

Item Software	Spesifikasi
Sistem Operasi	Windows XP, Windows 7, Windows 8, Windows 10
Software	VB.NET

3. Skema pertukaran data pada umumnya

Gambar 3 Skema Pertukaran Data Gambar



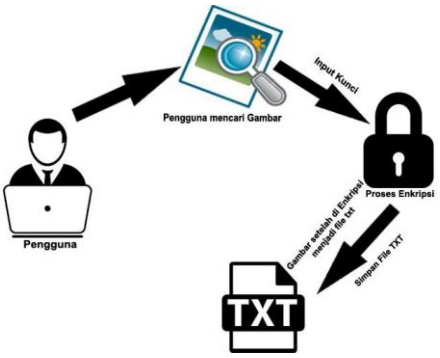
Gambar 4 Skema Pertukaran Data Setelah diterapkan Algoritma

Dari gambar diatas terlihat skema pengiriman gambar sebelum diterapkannya Algoritma.

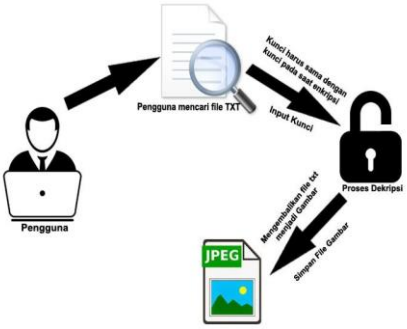
4. Skema Pertukaran data Setelah di terapkan Algoritma
   Dari gambar diatas terlihat skema pertukaran data setelah diterapkan algoritma. Pada proses diatas data gambar akan di enkripsi menjadi data text dengan memasukan kunci, kemudian

data text akan dirubah kembali menjadi data gambar melalui proses dekripsi dengan memasukan kunci yang sama pada proses enkripsi.

5. Skema Enkripsi pada tahapan algoritma



Gambar 5 Skema Enkripsi pada tahapan algoritma



Gambar 6 Skema Dekripsi pada tahapan algoritma

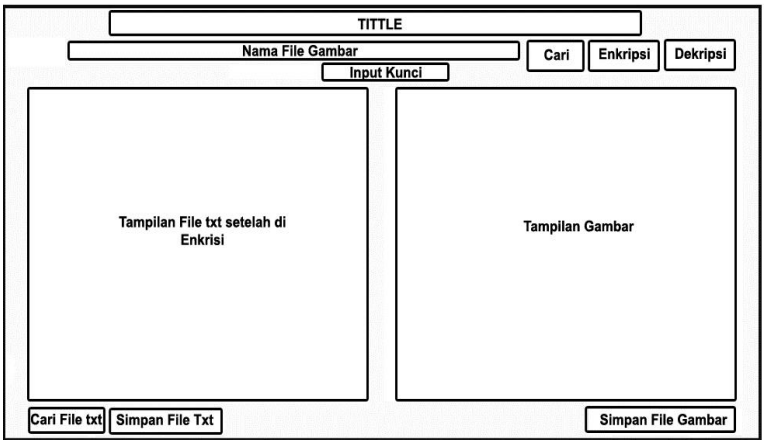
Pada Gambar 5 diatas menjelaskan skema enkripsi pada aplikasi keamanan Gambar, pengguna terlebih dahulu mencari gambar yang akan diamankan kemudian input kunci. Proses Enkripsi ini merubah gambar menjadi file txt.

6. Skema Dekripsi Pada Tahapan Algoritma
   Pada Gambar 6 diatas menjelaskan skema dekripsi pada aplikasi keamanan gambar, pengguna mencari file txt hasil dari proses enkripsi kemudian input kunci yang sama. Proses Dekripsi ini mengembalikan file txt menjadi gambar.

2. Membangun Sistem

Penerapan metode yang sudah sesuai dengan kebutuhan.

a. Pada penelitian ini menerapkan Metode Algoritma RSA (Rivest Shamir Adleman)
b. Rancangan tampilan Aplikasi Keamanan Gambar



Gambar 7 Rancangan Tampilan Aplikasi Keamanan Gambar

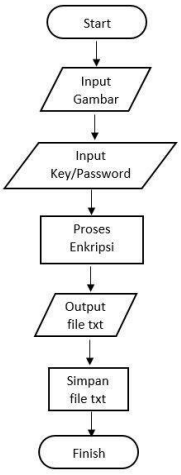
Pada Gambar 7 diatas adalah Rancangan tampilan Aplikasi yang terdiri dari Tittle, Textbox Nama file gambar, Tombol cari gambar, Tombol enkripsi, Tombol dekripsi, Input Kunci, Tampilan File txt, Tampilan Gambar, Tombol cari file txt, Tombol Simpan File Txt, Tombol Simpan Gambar. Pada Tombol Enkripsi dan Tombol Dekripsi terdapat Penerapan metode Algoritma RSA.

c. Flowchart Enkripsi

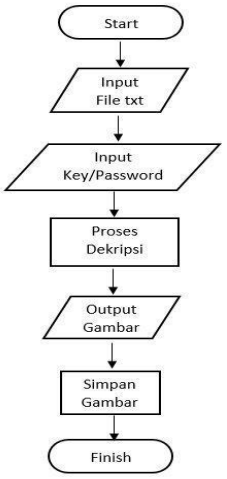
Gambar 8 Mendefinisikan Flowchart proses Enkripsi yaitu :

1. Tahap Pertama yaitu Start untuk memulai proses Enkripsi.
2. Tahap Kedua yaitu menginputkan Gambar

3. Tahap Ketiga yaitu menginputkan Key/Password sebelum melakukan proses Enkripsi. Key/password yang diinputkan harus sama dengan key/password pada proses dekripsi.
4. Tahap Keempat yaitu proses Enkripsi, pada proses Enkripsi menerapkan base64 dan Algoritma RSA.
5. Tahap Kelima yaitu menghasilkan file txt yang merupakan Ouput dari proses Enkripsi
6. Tahap Keenam yaitu menyimpan file txt
7. Tahap Ketujuh yaitu Finish berarti proses Enkripsi telah selesai



Gambar 8 Flowchart Enkripsi



Gambar 9 Flowchart Dekripsi

d. Flowhchart Dekripsi

Pada gambar 9. mendefinisikan Flowchart proses Dekripsi yaitu :

1. Tahap Pertama yaitu Start untuk memulai proses Dekripsi.
2. Tahap Kedua yaitu menginputkan File txt
3. Tahap Ketiga yaitu menginputkan Key/Password sebelum melakukan proses Dekripsi. Key/password yang diinputkan harus sama dengan key/password pada proses Enkripsi.
4. Tahap Keempat yaitu proses Dekripsi, pada proses Dekripsi menerapkan base64 dan Algoritma RSA.
5. Tahap Kelima yaitu menghasilkan file gambar yang merupakan Ouput dari proses Dekripsi
6. Tahap Keenam yaitu menyimpan file gambar
7. Tahap Ketujuh yaitu Finish berarti proses Dekripsi telah selesai

Tampilan desain pada aplikasi keamanan data gambar

a. Tampilan awal desain sebelum dimasukan gambar

Gambar 10 Tampilan awal

Gambar 11 Tampilan desain setelah dilakuan pencarian gambar

Pada Gambar 10 diatas terlihat tampilan awal sebelum dimasukan gambar dengan tampilan tombol cari untuk mencari gambar yang akan dienkripsi,Input kunci,Tombol Enkripsi,Tombol Dekripsi, Tampil Gambar, Tampil File txt, Tombol Cari File txt, Tombol Simpan File txt dan Tombol Simpan Gambar.

b. Tampilan desain setelah dilakuan pencarian gambar

Pada Gambar 11 diatas menunjukan tampilan setelah dilakukan pencarian gambar untuk di Enkripsi.

c. Tampilan setelah di Enkripsi

Gambar 12 Proses Enkripsi

Gambar 13 Proses Enkripsi

Pada Gambar 12 diatas menunjukan setelah proses Enkripsi selesai dan mendapatkan file txt. Sebelum proses Enkripsi dilakukan harus menginput kunci dan kemudian simpan file txt.

d. Tampilan setelah proses Dekripsi

Pada Gambar 13 diatas menunjukan setelah dilakukan proses Dekripsi mengembalikan file txt menjadi gambar, sebelum proses Dekripsi dilakukan cari file txt yang telah di Enkripsi kemudian tekan tombol Dekripsi untuk prosesnya lalu gambar hasil Dekripsi tersebut disimpan.

PEMBAHASAN

Aplikasi ini dilihat dan digunakan oleh pengguna untuk menilai apakah sistem ini sudah sesuai atau sudah layak digunakan untuk mengamankan file gambar, adapun penilaian yang dilakukan adalah dengan cara penyebaran kuesioner kepada pengguna.

Kuesioner Pengguna

Tabel 4. Kuesioner Pengguna

No	Pertanyaan	Jawaban				
		SS	S	RG	TS	ST
1.	Aplikasi keamanan informasi membantu menjaga keahasiaan infomasi					
2.	Aplikasi dapt digunakan dengan mudah					
3.	Proses enkripsi dan dskripsi oleh aplikasi keamanan cepat					
4.	Saya merasa puas dengan aplikasi yang dibuat					
5.	Informasi dikarenakan adanya password					
6.	Aplikasi keamanan informasi sangat membatu dalam komunikasi data					
7.	Dengan adanya algoritma RSA sangat membantu dalam keamanan informasi					
8.	File yang di enkripsi tidak dapat dibuka tanpa aplikasi keeamanan informasi dan password yang dipakai					
9.	Saran					

Uji Coba Produk

Aplikasi dilihat, dicoba dan digunakan oleh pengguna untuk melihat apakah sistem ini sudah sesuai atau sudah layak digunakan untuk menghitung ketepatan jawaban soal essay di STIKOM Binaniaga Bogor, adapun penilaian yang dilakukan adalah dengan cara penyebaran kuesioner kepada pengguna dan ahli sistem dapat dilihat pada tabel 7.

Tabel 5 Uji Kelayakan Pengguna

Responden	Pertanyaan								Jumlah	Jumlah Tertinggi
	Aplikasi keamanan informasi membantu menjaga keahasiaan	Aplikasi dapat digunakan dengan mudah	Proses enkripsi dandskripsi oleh aplikasi keamanan cepat	Saya merasa puas dengan aplikasi yang dibuat	Informasi dikarenakan adanya password	Aplikasi keamanan informasi sangat membatu dalam komunikasi data	Dengan adanya algoritma RSA sangat membantu dalam keamanan informasi	File yang di enkripsi tidak dapat dibuka tanpa aplikasi keeamanan informasi dan password yang dipakai		
R1	5	5	4	4	4	4	5	5	**36**	**40**
R2	5	5	4	5	5	5	5	5	**39**	**40**
R3	4	4	3	4	4	4	4	4	**31**	**40**
R4	4	5	3	4	5	4	5	5	**35**	**40**
R5	4	4	4	4	4	4	4	4	**32**	**40**
R16	4	5	4	4	5	4	1	5	**32**	**40**
R17	4	4	3	4	4	4	4	4	**31**	**40**
R18	5	5	4	5	5	5	5	4	**38**	**40**
R19	5	4	4	5	4	5	5	4	**36**	**40**
R20	4	4	3	4	4	4	4	4	**31**	**40**

Responden	Pertanyaan								Jumlah	Jumlah Tertinggi
	Aplikasi keamanan informasi membantu menjaga keahasiaan	Aplikasi dapat digunakan dengan mudah	Proses enkripsi dandskripsi oleh aplikasi keamanan cepat	Saya merasa puas dengan aplikasi yang dibuat	Informasi dikarenakan adanya password	Aplikasi keamanan informasi sangat membatu dalam komunikasi data	Dengan adanya algoritma RSA sangat membantu dalam keamanan informasi	File yang di enkripsi tidak dapat dibuka tanpa aplikasi keeamanan informasi dan password yang dipakai		
...	...	...	...	...	...	...	...	...	...	...
R85	5	4	3	4	5	4	4	5	**34**	**40**
R86	4	4	3	4	4	4	4	4	**31**	**40**
R87	4	3	3	4	4	4	4	4	**30**	**40**
R88	4	5	4	4	4	4	4	4	**33**	**40**
R89	4	4	3	4	4	5	5	5	**34**	**40**
R90	5	3	4	3	4	4	4	4	**31**	**40**
R91	4	3	3	3	4	4	4	4	**29**	**40**

$$\textit{Persentase Kelayakan (\%)} = \frac{36+39+31+35+32+\cdots}{40+40+40+40+40+...} \times 100\%$$

$$\textit{Persentase Kelayakan (\%)} = 30613640 \times 100\%$$

$$\textit{Persentase Kelayakan (\%)} = 84.1\%$$

SIMPULAN DAN SARAN

Simpulan

Berdasarkan hasil penelitian dapat ditarik kesimpulan :

1. Algoritma RSA dapat diterapkan sebagai metode untuk pengamanan data gambar
2. Aplikasi pengamanan data gambar dengan algoritma RSA mendapatkan presentasi kelayakan 84.1% berarti penelitian ini dikatakan sangat layak

Saran

Dalam jangka waktu kedepan penelitian ini dapat dikembangkan lagi, antara lain :

1. Data gambar yang di enkripsi dan dekripsi bisa dalam bentuk lain seperti png dan bmp.
2. Enkripsi maupun dekripsi dapat diterapkan dengan alternatif lain seperti menggunakan pengkodean php maupun java
3. Penelitian selanjutnya dapat digabungkan dengan Algoritma selain RSA.

DAFTAR RUJUKAN

Arikunto, Suharsimi. 2007. Prosedur Penelitian Suatu Pendekatan Praktik Edisi Revisi. Jakarta: Rineka Cipta.

Ariyus, D., 2008. Pengantar Ilmu Kriptografi Teori Analisis Dan Implementasi. Bandung : Penerbit Informatika.

Diarse, Ngakan Nyoman. Kristoforus. 2016. Penerapan Algoritma RSA Pada Sistem Kriptografi File Audio Mp3. Palembang

Roger S. Pressman. (2005). Software Engineering Fifth Edition

R. Munir, Kriptografi, Bandung: Informatika Bandung, 2006.

Sadikin, R., 2012. Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java. Yogyakarta: Penerbit ANDI.

Sugiyono. (2012). Metode Penelitian kuantitatif, kualitatif dan kombinasi (mixed methods). Bandung: Alfabeta