UNPjoMath Vol. 2 No. 4 Agustus 2019
ISSN: 977 235516589 Page 61-66

Penerapan Algoritma Rivest Shamir Adleman (RSA) untuk File Citra Menggunakan Visual Basic

Yessy Nazir[#1], Arnellis[*2], Meira Parma Dewi[*3]

[#]*Student of Mathematics Department Universitas Negeri Padang, Indonesia*
[*]*Lecturers of Mathematics Department Universitas Negeri Padang, Indonesia*

[1]yessynazir@yahoo.co.id
[2]arnellis_unp@yahoo.co.id
[3]meiradaud@gmail.com

Abstract – Most images have important information or a secret message. Secret message can provoke onset of opportunity the existence of threats to change the message. The messages of the image can be done by manipulating or piracy on the image. The results of image manipulation can change the meaning the image. Such as threats can be avoided by providing a safeguard against the image. Application of Rivest Shamir Adleman (RSA) Algorithm for Image Files is one way to secure an image of piracy as well as the manipulation of images. This article discussed the application of the RSA algorithm for image files. This method can hide the image using an early form of the public key and return it to the initial form with private key. The whole process is done by using Visual Basic 6.0. On the various experiments conducted the results of his work from the encryption produces 13 imagery similar to the image of the beginning of 15 sample images. Errors may caused by the selection of keywords which is less precise.

Keywords – A Safety Of Image File, The RSA Algorithm, Encryption, Descryption

Abstract – Banyak citra (*image*) yang berisi informasi penting ataupun pesan rahasia. Pesan rahasia dapat memancing terjadinya peluang adanya ancaman perubahan pesan dan pencurian pesan. Perubahan pesan dapat dilakukan dengan memanipulasi atau pembajakan pada citra. Hasil manipulasi citra dapat mengubah makna atau pesan dari citra. Ancaman tersebut dapat dihindari dengan memberi pengamanan terhadap citra tersebut. Penerapan Algoritma Rivest Shamir Adleman untuk File Citra merupakan salah satu cara mengamankan citra dari pembajakan maupun manipulasi citra. Pada artikel ini dibahas penerapan Algoritma Rivest Shamir Adleman (RSA) untuk file citra. Metode ini dapat menyembunyikan bentuk awal citra menggunakan sebuah kunci publik dan mengembalikannya ke bentuk awal dengan kunci private. Keseluruhan proses ini dilakukan dengan menggunakan Visual Basic 6.0. Pada berbagai percobaan yang dilakukan, hasil pendekripsian dari enkripsi menghasilkan 13 citra yang mirip dengan citra awal dari 15 contoh citra. Kesalahan itu terjadi mungkin disebabkan oleh pemilihan kunci yang kurang tepat, sehingga menghasilkan pendekripsian yang salah.

Keywords – Pengaman File Citra, Algoritma RSA, Enkripsi, Dekripsi

PENDAHULUAN

Perkembangan teknologi pada saat sekarang ini sangatlah pesat, termasuk teknologi pada jaringan komputer. Teknologi ini dapat gunakan dalam pengiriman pesan. Namun pesan pada media elektronik dapat berupa data. Salah satu contoh data adalah citra (*image*). Perkembangan citra digital dalam berbagai bentuk menunjukkan semakin tingginya kesadaran masyarakat akan citra (*image*) terhadap suatu objek. Banyak citra (*image*) yang berisi informasi penting ataupun pesan rahasia. Beberapa pesan tersebut merupakan pesan yang harus dijaga rahasianya. Sehingga pesan tersebut hanya dapat dilihat oleh orang yang diinginkan oleh si pemilik citra.

Pesan rahasia dapat memancing terjadinya peluang adanya ancaman terhadap perubahan pesan dan pencurian pesan. Perubahan pesan dapat dilakukan dengan memanipulasi atau pembajakan pada citra. Memanipulasi dapat merugikan pihak yang bersangkutan. Karena hasil manipulasi citra dapat mengubah makna atau pesan dari citra. Serta pembajakan citra dapat berdampak buruk seperti, tersebarnya citra tersebut tanpa seizin pemiliknya dan berubahnya bentuk dari asli citra. Ancaman tersebut dapat dihindari dengan memberi pengamanan terhadap citra tersebut. Oleh karena itu, untuk melindungi citra

terhadap akses, perubahan dan penghalangan yang tidak dilakukan oleh pihak yang berwenang, alat keamanan citra di jaringan komputer pun harus disediakan. Banyak jenis layanan keamanan jaringan, salah satunya yaitu kerahasiaan data.

Salah satu cara menjaga kerahasiaan data berupa citra adalah dengan cara menyembunyikan bentuk dari citra. Menyembunyikan bentuk citra dapat dilakukan dengan menggunakan Algoritma Kriptografi. Algoritma kriptografi terdiri dari tiga fungsi dasar, yaitu enkripsi, Dekripsi, dan kunci. Enkripsi adalah mengubah pesan atau data menjadi kode-kode yang tidak dimengerti. Dekripsi merupakan kebalikan enkripsi yaitu mengubah kode-kode tidak dimengerti menjadi pesan atau data asli. Sedangkan yang dimaksud kunci disini adalah kunci yang digunakan untuk melakukan enkripsi dan Dekripsi. Keamanan dari kriptografi didapat dengan merahasiakan kunci yang dimiliki dari orang lain, tanpa harus merahasiakan algoritma itu sendiri [1].

Algoritma kriptografi yang digunakan pada sistem komputer adalah algoritma kriptografi modern. Berbeda dengan kriptografi kalsik yang menitikberatkan kekuatan pada kerahasiaan algoritma yang digunakan, kriptografi modern lebih menitikberatkan pada kerahasiaan kunci yang digunakan pada algoritma tersebut (oleh pemakainya) sehingga algoritma tersebut dapat saja disebarkan ke kalangan masyarakat tanpa takut kehilangan kerahasiaan para pemakainya [1]. Untuk membangkitkan kunci, digunankan Saringan Erarothenes. Saringan Erarothenes merupakan suatu cara untuk menemukan semua bilangan prima dari 1 sampai bilangan bulat yang ditentukan. Saringan ini ditemukan oleh Eratosthenes, seorang ilmuwan Yunani kuno [4]. Salah satu algoritma kriptografi modern adalah Sistem Kriptografi Rivest Shamir Adleman (RSA). Kekuatan Sistem Kriptografi RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan menjadi faktor-faktor prima. Algoritma enkripsi dan Dekripsi sistem kriptografi RSA bersandar pada asumsi fungsi satu arah (one-way function) [3]. Algoritma ini melakukan pemfaktoran bilangan yang sangat besar [1]. Sistem Kriptografi RSA ini dapat diterapkan di beberapa perangkat lunak pada komputer, salah satunya adalah Microsoft Visual Basic.

Microsoft Visual Basic merupakan perangkat lunak yang memungkinkan untuk menggunakan image atau citra, sehingga dapat digunakan untuk mengamankan data berupa citra. Microsoft Visual Basic Merupakan pengembangan dari BASIC yang dibuat sebagai bahasa pemograman yang mudah dipelajari dan digunakan [2]. Dengan menerapkan Algoritma RSA pada perangkat lunak Microsoft Visual Basic, citra yang bersifat rahasia dapat diamankan. Dimana si pemilik citra menyembunyikan bentuk asli citra. Dan si penerima yang telah mendapat kuncilah yang bisa mengubah citra tersebut ke bentuk semula. Sehingga rahasia yang ada pada citra tersebut terjaga secara aman.

METODE

Penelitian ini merupakan penelitian dasar atau teoritis. Metode yang dilakukan dalam penelitian ini adalah studi kepustakaan dan dalam penyelesaian permasalahan, langkah kerja yang dilakukan adalah sebagai berikut:

1. Membuat tahapan-tahapan dalam Penerapan Algoritma Rivest Shamir Adleman (RSA) untuk File Citra Menggunakan Visual Basic.
2. Membuat desain proses untuk setiap tahap.
3. Menerapkan desain proses dalam bentuk program komputer berbantuan program aplikasi Visual Basic 6.0.
4. Melakukan uji coba terhadap program aplikasi yang telah dibuat.
5. Menarik kesimpulan dari hasil dan pembahasan yang telah dikerjakan.

HASIL DAN PEMBAHASAN

A. *Penerapan Sistem Kriptografi Rivest Shamir Adleman (RSA) untuk File Citra*

Pada penelitian ini objek yang digunakan adalah citra digital. Citra menurut KBBI (Kamus Besar Bahasa Indonesia) adalah rupa; gambar; gambaran. Citra digital yang digunakan adalah citra dengan format jpg dengan kedalaman pixel 8 bit yang mempunyai variasi warna serta dimensi ukuran citra beragam. Citra ini merupakan citra RGB, dimana tiap komponen RGB piksel memiliki panjang 8 bit (0-255), maka sistem modulo yang dipakai dalam penyandian adalah 256.

1. *Merubah Citra menjadi Bentuk Matriks*
   a. Tampilkan citra skala RGB dengan resolusi rendah (*5 x 5*) dan kedalaman warna 8-bit.
   b. Tentukan tingkat variasi warna masing-masing piksel yang direpresentasikan dalam bentuk matriks.
2. *Menentuan Kunci Publik dan Kunci Private dengan Algoritma Pembangkit Kunci RSA*

   Penjabaran Algoritma Pembangkit Kunci RSA dengan langkah-langkah pengerjaan yang jelas seperti berikut:
   1) Mengambil secara acak 2 buah bilangan prima misal p dan q.
   2) Menentukan nilai n, dimana $n = p * q$
   3) Menentukan $\emptyset(n)$, dimana $\emptyset(n) = (p-1) * (q-1)$
   4) Menentukan nilai e, dimana $gcd(e, \emptyset(n)) = 1$ dan e berada pada $Z_{\emptyset(n)}$
   5) Menentukan nilai d, dimana $d = e^{-1}$ pada $Z_{\emptyset(n)}$
   6) Kunci Publik = (e,n) dan Kunci Private adalah (d,n)
3. *Merubah Bentuk Citra dengan Algoritma Enkripsi RSA*

Untuk menjalankan proses enkripsi, maka dibutuhkan kunci publik yang telah dibentuk sebelumnya, yaitu (e, n). Penulis akan mengambil sample nilai RGB dari

file citra sebanyak 5x5 pixel untuk mewakili citra gambar secara keseluruhan yang akan dienkripsi. Dengan menggunakan algoritma Enkripsi $C = P^e mod\ n$.

4. *Merubah Bentuk file citra seperti bentuk awal dengan Algoritma Dekripsi RSA*

Untuk menjalankan proses dekripsi, maka dibutuhkan kunci private yang telah dibentuk sebelumnya, yaitu (d, n), dengan rumus $P = C^d mod\ n$, maka diperoleh nilai dekripsi.

B. *Proses Perancangan Program Aplikasi Penerapan Sistem Kriptografi Rivest Shamir Adleman (RSA) untuk File Citra*

Pada proses ini, algoritma Rivest Shamir Adleman akan di terjemahkan kedalam bahasa Visual Basic. Algoritma Rivest Shamir Adleman dibagi menjadi beberapa proses, yang akan memiliki algoritma tersendiri. Desain proses ini dibagi menjadi proses global dan algoritma proses.

a. *Desain Proses Global*

Gambar 1. Proses desain global

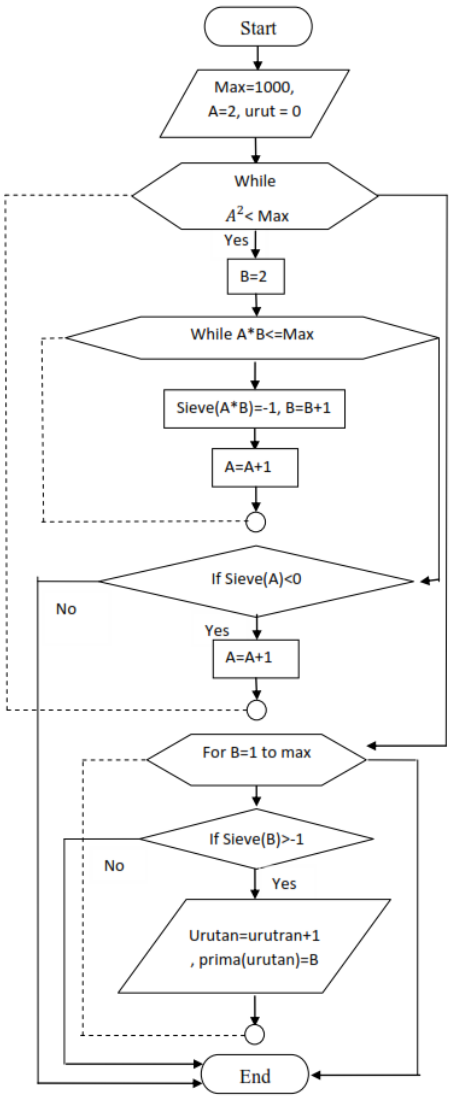
Dalam pembuatan program ini, citra yang digunakan untuk penerapan Sistem Kriptografi Rivest Shamir Adleman (RSA) diinputkan yang direpresentasikan dalam bentuk matriks. Kemudian, kita akan menentukan kunci publik dan kunci private dengan mengunakan algoritma pembangkit kunci. Untuk mengenkripsikan file citra, kita akan menggunakan hasil representasi citra dalam bentuk matriks berserta kunci publik yang telah dibentuk. Hasil dari enkripsi ini berupa matriks baru yang yang dapat di representasikan dalam bentuk citra baru. Sedangkan untuk mendekripsikan citra, kita membutuhkan matriks hasil enkripsi serta kunci private yang telah dibentuk. Hasil dekripsi ini berupa matriks ynag dapat direpresentasikan dalam bentuk citra. Citra hasil dekripsi ini akan sama dengan citra awal.

b. *Desain Algoritma Proses*

Desain algoritma proses ini dibagi menjadi 3 bagian, yaitu desain algoritma pembentukan kunci kunci publik dan private, desain algoritma pengenkripsian citra dan desain algoritma pendekripsian citra.

1) *Algoritma Pembentukan Kunci Publik dan Kunci Private*

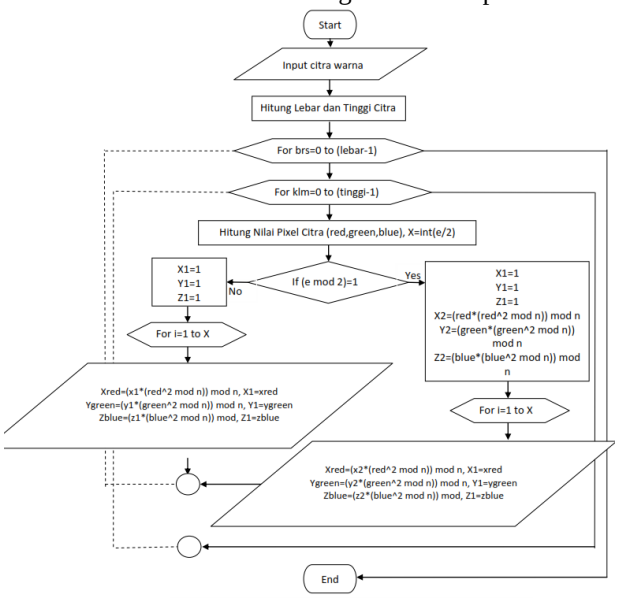
Pada desain ini, input yang digunakan alah bilangan acak. Dimana bilangan ini akan membangkitkan sebuah bilangan prima, dan mencari bilangan prima lain yang hasil perkaliannya menghampiri nilai 256. Kemudian dari hasil perkalian dan dua bilangan prima tersebut akan dicari nilai psi. Hasil dari nilai psi, akan digunakan untuk mencari pasangan kunci publik, dimana FPB pasangan kunci publik dan psi tersebut adalah 1. Setelah diperoleh kunci publik, akan dicari pasangan kunci private dengan menggunakan kunci publik dan psi. Pasangan kunci private merupakan invers dari kunci publik pada modulo psi. pembangkit kunci disini Algoritma Saringan Eratothenes.



Gambar 2. Flowchart Saringan Erarothenes

2) *Algoritma Enkripsi*

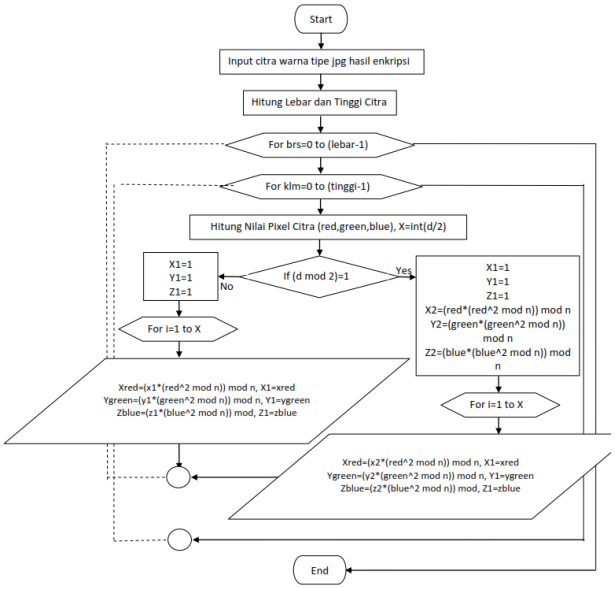
Berikut adalah desain dari algoritma enkripsi:



Gambar 3. FlowChart algoritma enkripsi

3) *Algoritma Dekripsi*

Berikut adalah desain dari algoritma dekripsi:



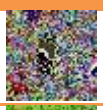
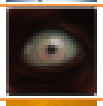
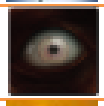
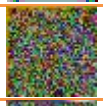
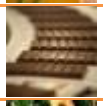
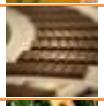
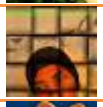
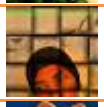
Gambar 4. FlowChart algoritma dekripsi

C. *Uji Coba, Simulasi dan Evaluasi Program*

Uji coba berserta simulasi dan evaluasi program bertujuan untuk mengetahui kemampuan dari progam dalam menentukan hasil enkripsi dan dekripsi citra, sehingga dapat diketahui tingkat keakuratan program. Uji coba ini dibutuhkan untuk menentukan hasil enkripsi dan dekripsi citra menggunakan Sistem Kriptografi Rivest Shamir Adleman (RSA).

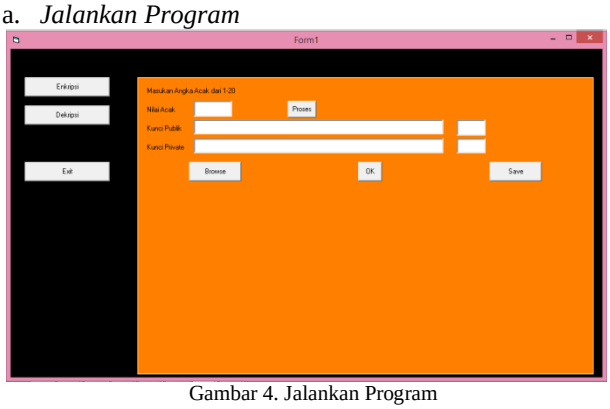
Berikut adalah beberapa contoh hasil simulasi program yang diambil pada pada skripsi [5] seperti berikut ini:

TABEL I
HASIL HASIL SIMULASI ENKRIPSI DEKRIPSI

No	Kunci Publik	Kunci Private	Citra Awal	Citra Enskripsi	Citra Dekripsi
1	**19,254**	73,254			
2	**17,221**	113,221			
3	**17,249**	29,249			
4	**17,247**	89,247			
5	**13,253**	**17,253**			
6	**13,235**	**85,235**			
7	**17,221**	**113,221**			
8	**17,203**	**89,203**			
9	**17,185**	**17,185**			
10	**17,217**	**53,217**			
11	**17,237**	**101,237**			
12	**17,253**	**15,253**			
13	**17,213**	**33,213**			
14	**17,235**	**65,235**			
15	**17,177**	**41,177**			

Proses uji coba dilakukan dengan langkah-langkah sebagai berikut:

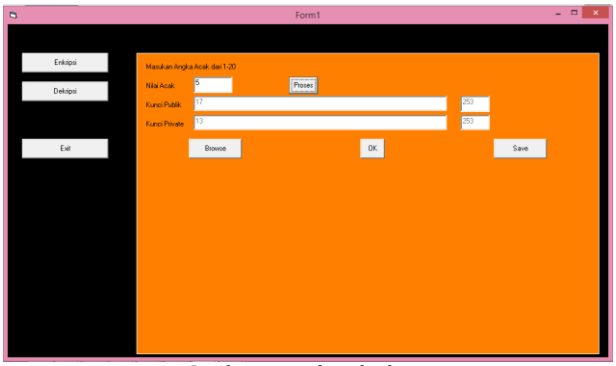
a. *Jalankan Program*



Gambar 4. Jalankan Program

b. *Masukan sebarang angka acak pada kolom Nilai Acak*

Masukan sebarang angka pada kolom nilai acak, ini berguna untuk membangkitkan sebuah bilangan prima. Kemudian, bilangan prima yang kedua akan dicari dengan menggunakan perkalian 2 bilangan prima yang hasilnya mendekati 256. Karena nilai pada setiap pixelnya hanya berkisar dari 1-256, maka modulo yang digunakan haruslah mendekati 256. Kemudian klik tombol proses



Gambar 5. Pembangkit kunci

Maka akan diperoleh kunci publik beserta kunci private pada kolom kunci publik dan kunci private. Kunci ini diperoleh dari Algoritma pembangkit kunci RSA beserta algoritma Saringan Erarothenes (Sieve Erarothenes).

c. *Pengenkripsian Citra*

Dengan mengklik tombol browse, maka akan muncul sebuah jendela tempat penyimpanan file citra. Klik open, maka citra pun telah diinputkan kedalam program. Dengan menekan tombol Ok, maka proses pengenkripsian citra pun dilakukan. Pengenkripsian citra menggunakan algoritma enkripsi, dimana pada algoritma ini dibutuhkan kunci publik yang telah dibentuk pada saat membangkitkan kunci.

Contoh hasil penerapan Algoritma RSA untuk file citra ini diambil pada skripsi [5]. Dimana Gambar 6, merupakan citra awal, dan Gambar 7 merupakan citra hasil enkripsi dimana nilai setiap pixel citra hasil enkripsi diperoleh dengan menggunakan algoritma enkripsi RSA pada setiap nilai pixel dari citra awal yang digunakan. Dengan contoh seperti berikut:

Gambar 6. Citra Awal

Gambar 7. Citra Hasil Ekripsi

d. *Pendekripsian Citra*

Pada Pendekripsian citra, kita akan memasukan kunci private yang telah kita peroleh pada saat membangkitkan kunci. Kunci ini berguna untuk tahap pendekripsian. Setelah memasukan kunci publik, maka klik tombol browse. Kemudian, akan muncul jendela baru, untuk pengambilan citra. Klik tombol open, maka gambar yang dipilih akan ditampilkan didalam program. Sama dengan proses pengenkripsian, tombol OK berfungsi untuk melakukan tahap pendekripsian. Dimana citra hasil enkripsi akan dirubah kembali menjadi citra semula menggukan kunci publik dan kunci private. Contoh hasil penerapan Algoritma RSA untuk file citra ini diambil pada skripsi [5] adalah sebagai berikut:

Gambar 8. Citra Hasil Dekripsi

D. *Keterbatasan Program*

Penelitian mempunyai beberapa keterbatasan dalam program, yaitu:

a. Jumlah piksel pada citra yang lebih dari 2500 piksel akan menyebabkan penggunaan memori yang besar dan waktu proses yang lama. Program akan menelusuri satu persaru pixel dan menentukan nilai RGB. Penentuan nilai RGB ini berfungsi untuk melakukan enkripsi dan dekripsi.

b. Bilangan acak yang dimasukan hanya untuk satu bilangan prima, sehingga untuk membangkitkan kunci, kita hanya bisa memilih 1 bilangan prima.

c. Penerapan Algoritma Rivest Shamir Adleman (RSA) untuk file citra menggunakan modulo yang menghampiri nilai 256, sehingga kunci yang dibentuk oleh pembangkit kunti tidak terlalu bervariasi.

SIMPULAN

Berdasarkan hasil pembahasan dari penelitian ini, dapat diperoleh kesimpulan sebagai berikut:

1. Pada Penelitian ini untuk membangkitkan kunci publik dan kunci private digunakan Algoritma Saringan Eratothenes, dimana dengan algoritma ini, akan dibuat barisan bilangan prima. Menggunakan barisan prima itu akan di pilih p, q, e. sehingga diperoleh kunci publik dan kunci private. Dimana modulus yang digunakan adalah menggunakan modulus perkalian 2 bilangan prima yang mendekati nilai 256.
2. Pengenkripsian Citra menggunakan rumus:
$$C = P^e mod\ n$$
Dimana C merupakan matriks hasil dari enkripsi, P merupakan matriks awal citra, e dan n merupakan nilai dari pasangan kunci publik, yang diperoleh dari algoritma pembangkit kunci.
3. Pendekripsian Citra menggunakan rumus:
$$P = C^d\ mod\ n$$
Dimana P merupakan matriks hasil dari dekripsi, C merupakan matriks hasil enkripsi citra, d dan n merupakan nilai dari pasangan kunci private, yang diperoleh dari algoritma pembangkit kunci.
4. Menggunakan program aplikasi Visual Basic 6.0, penerapan Sistem Kriptografi Rivest Shamir Adleman (RSA) memperoleh hasil citra dekripsi yang sesuai dengan citra awal. Dimana dari 15 citra yang dicobakan, hanya 3 citra yang hasil dekripsinya tidak persis dengan citra awal. Kesalahan itu terjadi mungkin disebabkan oleh pemilihan kunci yang kurang tepat, sehingga menghasilkan pendekripsian yang salah.

REFERENSI

[1] Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi*. Yogyakarta: C.V Andi Offset.

[2] Enterprise, Jubilee. 2014. *Dasar-dasar Visual Basic 2013.* Jakarta: PT. Elex Media Komputindo.

[3] Sadikin, Rifki. 2012. *Kriptografi untuk Keamanan Jaringan*. Yogyakarta: C.V Andi Offset.

[4] Wikipedia. 2015. "Saringan Eratothenes". https://id.wikipedia.org/saringan-eratothenes. Diakses 13 juni 2016.

[5] Nazir, Yessy. 2016. "Penerapan Algoritma Rivest Sahmir Adleman (RSA) untuk Pengamanan File Citra Menggunakan Visual Basic". Padang : Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Negeri Padang