Vol.10 No. 2 OKTOBER 2014

ISSN 1907-0837

JURNAL ILMIAH

RealTech

Teknik Informatika | Teknik Industri | Teknik Elektro

Fakultas Teknik
Universitas Katolik De La Salle Manado

Realtech	Vol. 10	No. 2	Hal 1-99	Manado Oktober 2014	ISSN 1907-0837

ISSN 1907-0837

Jurnal Realtech

Volume 10 Nomor 2 Oktober 2014

Alamat Sekretariat / Redaksi :

Sekretariat Jurnal Realtech

Fakultas Teknik

Universitas Katolik De La Salle Manado

Kairagi I Kombos Manado 95000

Telp. 0431-877512, 871971, 871957

E-mail: realtech_dlsu@yahoo.com

Jurnal Realtech merupakan jurnal ilmiah sebagai bentuk pengabdian dalam hal pengembangan bidang Teknologi Informasi, Teknik Elektro dan Teknik Industri dan bidang terkait lainnya.

Jurnal Realtech diterbitkan oleh Fakultas Teknik Universitas Katolik De La Salle Manado. Redaksi mengundang para profesional dari dunia usaha, pendidikan dan peneliti untuk menulis mengenai perkembangan ilmu di bidang yang berkaitan dengan Teknologi Informasi, Teknik Elektro dan Teknik Industri.

Jurnal Realtech diterbitkan 2 (dua) kali dalam 1 tahun pada bulan April dan Oktober. Edisi pertama terbit Juli 2005. Harga berlangganan Rp. 25.000,-/eksemplar dan Rp. 35.000,-/eksemplar (untuk luar Pulau Sulawesi).

ISSN 1907-0837

JurnalRealtech

Volume 10 Nomor 2 Oktober 2014

Daftar Isi Kumulatif

Volume 10 Nomor 2

APLIKASI PENGAMANAN DATA MENGGUNAKAN ALGORITMA RABIN

Enjelin Fitria Tangon[1], Rinaldi Munir[2], Debby Paseru[3]
Program Studi Teknik Informatika - Universitas Katolik De La Salle Manado[1,3], Institut Teknologi Bandung[2]
Email : enjelintangon@gmail.com[1], rinaldi@informatika.org[2], bydeb_raul@yahoo.com[3]

Abstract

Data security has become an important need in an organization, agency, company and individual. This need arises from the increasing number of threats to data security such as a problem accessing the confidential data by unauthorized parties. Of course the illegal data access is detrimental to the data owner or party which associated with data access.

Crptography is a technique that uses a secure data encryption and decryption for data confidentiality. Cryptographic method being used in this study is the method of public key cryptography. This method uses an asymmetric algorithm (public key algorithm). This algorithm uses different keys for encryption and decryption, and is commonly used to secure the data to be exchanged.

Rabin algorithm being used in this research is included in the asymmetric cryptographic algorithm. The methodology being used in the application development process is Extreme Programming (XP) along with Unified Modeling Language (UML) version 2.0 as the tools to describe the application. The application is built by Borland Delphi 7.0.

After passing implementation phase, the application has been tested and the test results indicate that the application works properly, and can encrypt and decrypt any type of file with different file size.

Keywords: Data security, public key cryptography, encryption – decryption, Rabin algorithm

Abstrak

Keamanan data telah menjadi kebutuhan yang penting dalam suatu organisasi, instansi atau perusahaan maupun pribadi. Kebutuhan ini timbul karena semakin banyaknya ancaman terhadap keamanan data seperti masalah pengaksesan data rahasia oleh pihak – pihak yang tidak berhak dan tidak berkepentingan atas data rahasia tersebut. Tentunya pengaksesan data secara illegal ini merugikan pihak pemilik data atau pihak – pihak yang terkait dengan pengaksesan data.

Kriptografi merupakan teknik pengamanan data yang menggunakan proses enkripsi dan dekripsi untuk menjaga kerahasiaan data. Metode kriptografi yang digunakan pada penelitian ini adalah metode kriptografi kunci publik. Algoritma ini menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi, dan umumnya digunakan untuk mengamankan data yang akan dipertukarkan.

Algoritma Rabin yang dipakai dalam penelitian ini termasuk dalam algoritma kriptografi asimetri. Metodologi yang dipakai dalam proses pengembangan aplikasi ini adalah *Extreme programming* (XP) dengan kakas yang digunakan adalah *Unified Modeling Language* (UML). Pemrograman perangkat lunak menggunakan *Borland Delphi 7.0*.

Setelah melalui tahap implementasi, aplikasi telah diuji dan hasil pengujian menunjukkan bahwa aplikasi berjalan dengan baik, dan dapat mengenkripsi dan mendekripsi semua jenis *file* dengan ukuran *file* yang berbeda – beda.

Kata kunci: Pengamanan data, kriptografi kunci publik, enkripsi – dekripsi, algoritma Rabin

1. PENDAHULUAN

Perkembangan teknologi komputer dan kemajuan di bidang telekomunikasi telah memungkinkan seseorang, organisasi dan instansi untuk menyimpan dan mempertukarkan data dan informasi yang penting dan berharga dalam bentuk *file* di dalam komputer. Kerahasiaan dan keamanan merupakan aspek penting dari suatu data. Aspek tersebut harus dijaga pada saat pengiriman maupun penyimpanan data, karena dapat menimbulkan resiko jika data tersebut diakses, dibaca, kemudian dimanfaatkan oleh orang-orang yang tidak berhak.

Untuk mencegah agar hal tersebut tidak terjadi, maka diperlukan suatu teknik pengamanan data.

Kriptografi merupakan salah satu teknik yang dapat digunakan dalam pengamanan data. Kriptografi melakukan proses enkripsi dan dekripsi. Proses enkripsi melakukan pengacakan dan penyandian pada suatu data agar tidak dapat dipahami orang lain. Data yang sudah diacak dan disandikan disebut dengan *ciphertext*. Proses dekripsi mengembalikan kembali *ciphertext* tersebut ke bentuk aslinya (*plaintext*) agar data tersebut dapat dibaca kembali. Untuk melakukan enkripsi dan dekripsi diperlukan suatu algoritma atau fungsi matematika. Dahulu keamanan kriptografi ditentukan dengan menjaga kerahasiaan algoritma dan hal tersebut sudah tidak cocok lagi. Untuk itu kriptografi modern mengatasi masalah ini dengan penggunaan kunci untuk melakukan proses enkripsi dan dekripsi.

Keamanan suatu metode kriptografi modern bergantung pada kerahasiaan kunci yang digunakan saat melakukan proses enkripsi dan dekripsi. Dalam buku Kriptografi [6] menjelaskan bahwa ada dua tipe dasar dari metode kriptografi yaitu kriptografi kunci rahasia (*private/secret key cryptography*) dan kriptografi kunci publik (*public key cryptography*). Pada metode kriptografi kunci rahasia setiap pengguna yang ingin bertukaran data menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Kedua belah pihak harus menjaga kerahasiaan kunci tersebut. Satu masalah kritis di dalam sistem kriptografi kunci-simetri adalah cara mendistribusikan kunci. Saluran pengiriman kunci melalui saluran publik (melalui telepon, internet, dan sebagainya) jelas tidak aman, karena penyadap dapat menyadap kunci selama transmisi.

Masalah ini kemudian dipecahkan dengan menggunakan metode kriptografi kunci publik. Setiap pengguna yang ingin bertukaran data menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi. Kunci untuk enkripsi dinamakan kunci publik karena dapat diumumkan ke publik. Kunci untuk proses dekripsi dinamakan kunci privat karena sifatnya rahasia. Algoritma kunci publik adalah algoritma yang digunakan pada metode kriptografi ini.

Algoritma Rabin termasuk dalam algoritma kunci publik. Algoritma ini pertama kali diperkenalkan tahun 1979 oleh Michael Rabin. Dari segi keamanan, algoritma Rabin mengandalkan kekuatan sulitnya memfaktorkan bilangan besar dan mencari *square roots* modulo suatu bilangan gabungan [5]. Kecepatan proses pembangkitan kunci dan proses enkripsi dengan menggunakan algoritma Rabin jika dibandingkan dengan menggunakan algoritma kunci publik lain prosesnya cepat karena menggunakan komputasi sederhana [2].

Berdasarkan uraian di atas, maka dalam penelitian ini penulis membuat aplikasi pengamanan data menggunakan algoritma Rabin. Aplikasi ini diharapkan dapat membantu menjaga kerahasiaan dan keamanan data yang disimpan dan dipertukarkan dari pihak yang tidak berkepentingan.

Batasan masalah dari penelitian ini adalah sebagai berikut:

1. Aplikasi hanya dapat melakukan proses dekripsi pada *file* yang dienkripsi oleh aplikasi ini.
2. Aplikasi tidak membahas mengenai mekanisme pemecahan cipherteks menjadi plainteks semula tanpa memiliki akses ke kunci yang digunakan (kriptanalisis).

2. STUDI PUSTAKA

2.1 Data

Kata "data" yang kita kenal sekarang, diambil dari bahasa Inggris. Akan tetapi, kata data tersebut awal mulanya berasal dari bahasa Yunani yaitu *datum* yang berarti fakta [7]. Data adalah rekaman mengenai fakta yang ada atau yang terjadi. Data mengenai organisasi harus direkam dan dikelola secara baik sehingga dapat dipakai/diakses secara efisien sehingga efektif mendukung operasi dan pengendalian organisasi [3]. Makna kata data pada komputer adalah segala sesuatu yang bisa dikodekan, disimbolkan, atau dilambangkan dengan kode, simbol, ataupun lambang yang telah disediakan pada setiap komputer. Data komputer juga dikenal sebagai bentuk data yang dihasilkan oleh aplikasi yang dijalankan oleh komputer [7].

2.2 Keamanan dan Pengamanan Data

Keamanan merupakan komponen yang vital dalam komunikasi data elektronis. Masih banyak yang belum menyadari bahwa keamanan (*security*) merupakan sebuah komponen penting yang tidak murah. Teknologi kriptografi sangat berperan dalam proses komunikasi, yang digunakan untuk melakukan enkripsi (pengacakan) data yang ditransaksikan selama perjalanan dari sumber ke tujuan dan juga melakukan dekripsi (menyusun kembali) data yang telah teracak tersebut [8].

Pengamanan data secara administratif harus dilakukan untuk menjaga dari kemungkinan gangguan keamanan data yang datang dari dalam maupun dari luar organisasi [7].

2.3 Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain [1].

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematis yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data, dan autentikasi data. Kriptografi tidak hanya memberikan keamanan informasi saja, namun lebih ke arah teknik-tekniknya [8].

Komponen kriptografi terdiri dari beberapa komponen [1], seperti:

1. Enkripsi: cara pengamanan data yang dikirimkan dengan mengubah pesan asli (*plaintext*) menjadi kode-kode yang tidak dimengerti.
2. Dekripsi: merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya.
3. Kunci: adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi, yaitu kunci rahasia (*private key*) dan kunci umum (*public key*).
4. *Plaintext*: sering disebut dengan *cleartext*.
5. *Ciphertext*: merupakan suatu pesan yang telah melalui proses enkripsi. Pesan yang ada pada teks-kode ini tidak bisa dibaca karena berupa karakter-karakter yang tidak mempunyai makna (arti).
6. Pesan: dapat berupa data atau informasi yang dikirim atau yang disimpan di dalam media perekaman (kertas, *storage*, dsb).
7. *Cryptanalysis*: Suatu ilmu untuk mendapatkan teks-asli tanpa harus mengetahui kunci yang sah secara wajar.

2.4 Algoritma Kriptografi

Dalam buku Pengantar Ilmu Kriptografi [1] kata algoritma dalam bahasa Arab *algorism* mempunyai arti proses perhitungan. Algoritma berasal dari nama penulis buku Arab yang terkenal, yaitu Abu Ja'far Muhammad Ibnu Musa al-Khuwarizmi. Kata *algorism* lambat laun berubah menjadi *algorithm*.

Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut. Algoritma kriptografi dibagi menjadi tiga bagian berdasarkan kunci yang dipakainya:

1. Algoritma Simetri: algoritma ini menggunakan satu kunci untuk enkripsi dan dekripsinya
2. Algoritma Asimetri: algoritma ini menggunakan kunci yang berbeda untuk enkripsi dan dekripsi
3. *Hash Function.*

2.5 Algoritma Rabin

Algoritma Rabin pertama kali diperkenalkan tahun 1979 oleh Michael O. Rabin. Algoritma Rabin merupakan termasuk dalam **algoritma kriptografi kunci publik (kriptografi asimetri)** yang kemampuan sekuritasnya dibuktikan secara matematik mengingat metode pemfaktoran bilangan secara cepat sampai saat ini belum terpecahkan [2].

2.5.1 Dasar Matematika Algoritma Rabin

Banyak dasar matematika yang menjadi dasar pembangunan algoritma kriptografi. Dalam penelitian ini akan ditampilkan beberapa dasar matematika yang berhubungan dengan algoritma Rabin dalam implementasi dan analisisnya. Dalam bukunya, Munir [6] menjelaskan konsep dasar matematika yang mendasari pembangunan algoritma Rabin, sebagai berikut:

a. Aritmetika Modulo
b. Kekongruenan
c. Algoritma Euclidean
d. *Chinese Remainder Problem*

2.5.2 Perumusan dan Perhitungan Algoritma Rabin

Pada algoritma Rabin terdapat 3 langkah utama yaitu pembangkitan kunci (*key generation*), enkripsi dan dekripsi. Kunci pada Rabin mencakup dua buah kunci yaitu kunci publik untuk melakukan enkripsi dan kunci privat untuk melakukan dekripsi. Menezes, et al. [5] dalam buku Handbook of Applied Cryptography menjabarkan langkah-langkahnya sebagai berikut:

a. Pembangkitan kunci

Algoritma pembangkitan kuncinya adalah sebagai berikut:

1. Pilih dua buah bilangan prima p dan q secara acak dan mengikuti persamaan:
   $p \equiv q \equiv 3 \pmod 4$

Ket:

Kedua bilangan prima p dan q ini adalah kunci privat.

2. Hitung:

$n = p.q$

Hasil dari $n = p.q$ merupakan kunci publik.

b. Enkripsi

Proses enkripsi menggunakan algoritma Rabin dituliskan sebagai berikut:

1. Ambil kunci publik (n) dari penerima pesan.
2. Representasikan pesan *plaintext* sebagai suatu integer m sedemikian sehingga nilai m berada pada selang (0, 1, ..., n - 1). Artinya pesan m dibagi dalam blok – blok numerik yang nilainya lebih kecil dari nilai kunci publik (n).
3. Enkripsi dilakukan dengan menggunakan rumus:

   $c = m^2 \bmod n$

   Keterangan :

   c : cipherteks,

   m : plainteks

   n : kunci publik
4. Kirim cipherteks (c) ke penerima pesan.

c. Dekripsi

Proses untuk mencari plainteks (m) didapat dengan menggunakan langkah – langkah sebagai berikut:

1. Dengan menerapkan algoritma Euclidean Diperpanjang (*Extended Euclidean*) cari dan hitung integer a dan integer b, sehingga:

   $ap + bq = 1$
2. Dicari $\sqrt{C}$ modulo p dan $\sqrt{C}$ modulo q dengan rumus:

   $m_p = C^{(p+1)/4} \bmod p$

   $m_q = C^{(q+1)/4} \bmod q$
3. Dihitung empat akar kuadrat hasil operasi $m = \sqrt{c} \bmod n$, disimbolkan dengan m_1, m_2, m_3, m_4 yang merupakan empat kemungkinan hasil dekripsi:

   $m_1 = (a.p.m_q + b.q.m_p) \bmod n$

   $m_2 = n - m_1$

   $m_3 = (a.p.m_q - b.q.m_p) \bmod n$

   $m_4 = n - m_3$

   Ketika kita telah menemukan keempat hasil, m_1, m_2, m_3, m_4, pesan plainteks (m) yang asli adalah salah satu dari keempat hasil tersebut.

2.5.3 Keamanan Algoritma Rabin

Keamanan algoritma Rabin sama seperti algoritma RSA dimana mengandalkan kesulitan pemfaktoran bilangan besar. Hasil enkripsi menggunakan dengan algoritma Rabin terbilang cukup baik karena memiliki tingkat keamanan yang relatif tinggi [4]. Untuk proses dekripsi kekuatan dari algoritma Rabin adalah sulitnya mencari *square roots* modulo suatu bilangan gabungan (composite number). Skema enkripsi dan dekripsi menggunakan algoritma kunci publik Rabin terbukti lebih aman dalam menghadapi serangan-serangan yang bersifat pasif seperti serangan faktorisasi, terlebih lagi jika menggunakan ukuran kunci yang besar [5]. Algoritma Rabin sangat tidak aman dalam menghadapi serangan berupa *chosen-ciphertext attack* [5].

2.5.4 Kelebihan dan Kekurangan Algoritma Rabin

Kelebihan algoritma Rabin dibandingkan dengan algoritma kunci publik lainnya seperti RSA dan Elgamal adalah sebagai berikut [2]:

1. Proses enkripsi dengan algoritma Rabin lebih sederhana dibandingkan dengan algoritma RSA dan Elgamal.
2. Kecepatan proses pembangkitan kunci dengan algoritma Rabin lebih cepat dibandingkan dengan algoritma RSA dan Elgamal. Karena proses pembangkitan kuncinya tidak terlalu rumit, maka komputasinya juga tidak terlalu lama.

Sedangkan kelemahan algoritma Rabin yaitu mudah diserang dengan teknik *chosen-ciphertext attack.*

3. ANALISIS DAN PERANCANGAN

Tahap analisis menggunakan tahapan yang ada pada metodologi pengembangan *Agile* dengan *Extreme Programming* (XP).

3.1 Analisis Aplikasi Yang Akan Dibangun

Aplikasi pengamanan data yang dibangun menggunakan algoritma kriptografi asimetri – Rabin dalam melakukan proses enkripsi dan dekripsi *multiple file* dengan berbagai jenis *file.* Aplikasi yang akan dirancang ini sangat cocok digunakan untuk proteksi data rahasia yang dikirimkan kepada pihak lain.

3.1.1 Analisis Data

Data yang akan dienkripsi pada aplikasi adalah semua jenis data yaitu:

1. Data dokumen teks misalnya data yang berekstensi .doc, .txt, .xls, .ppt, .docx.

2. Data dokumen *digital* misalnya data yang berekstensi .pdf
3. Data gambar misalnya data yang berekstensi .bmp, .gif, .jpg, .png, .psd.
4. Data multimedia misalnya data yang berekstensi .mp3, .wmv, .avi.
5. Data sistem misalnya data yang berekstensi .exe.
6. Data video ponsel misalnya data yang berekstensi .3gp dan .mp4.
7. Data arsip misalnya data yang berekstensi .zip, .rar.

3.1.2 Analisis Pengguna

Latar belakang pengguna yang akan memakai program aplikasi yang akan dibuat, terbagi menjadi dua pengguna yaitu pengirim pesan dan penerima pesan, serta memiliki kriteria pengguna sebagai berikut:

1. Memiliki kemampuan dasar dalam pengoperasian komputer.
2. Mengenal sistem kriptografi.

3.1.3 Spesifikasi Persyaratan Sistem

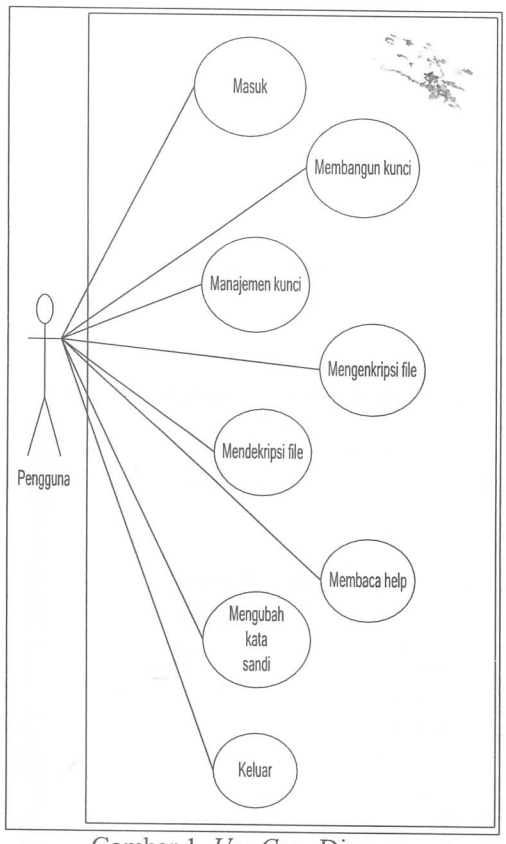
Berikut ini merupakan kelompok fitur yang disediakan oleh aplikasi.

Tabel 1. Spesifikasi Kebutuhan Perangkat Lunak

Fitur Pada Aplikasi	Deskripsi
Generate Key	Menangani fungsi untuk membangun kunci publik dan kunci privat.
Import Key	Menangani fungsi untuk meng-*import public key* dari pengguna yang lain (penerima data) untuk keperluan pengenkripsian *file* yang akan dikirim ke pengguna tersebut.
Export Key	Fitur untuk meng-*export* kunci publik penerima data yang dihasilkan dari proses pembangkitan kunci untuk dikirim kepada pengirim data.
Delete Key	Menangani fungsi untuk menghapus kunci yang dihasilkan dari proses pembangkitan kunci maupun kunci yang di-*import* ke dalam penyimpanan kunci.
Encryption	Menangani fungsi untuk mengenkripsi *file*.
Decryption	Menangani fungsi untuk mendekripsi *file*.

3.1.4 Pembuatan Model *Use Case*

Pemodelan *use case* adalah untuk melihat bagaimana sistem seharusnya berperilaku dan berinteraksi dengan pengguna. Berikut adalah *use case* diagram untuk setiap fungsi dari sistem yang akan dibangun.



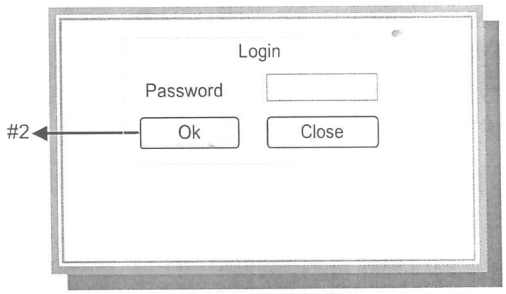
Gambar 1. *Use Case* Diagram

3.2 Perancangan

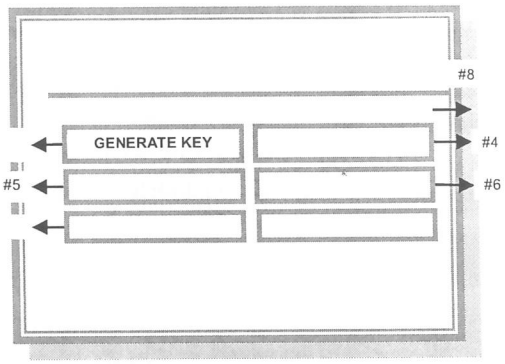
Perancangan merupakan tahap lanjutan dari analisis, dimana pada perancangan digambarkan rancangan sistem yang akan dibangun.

3.2.1 Perancangan Antarmuka

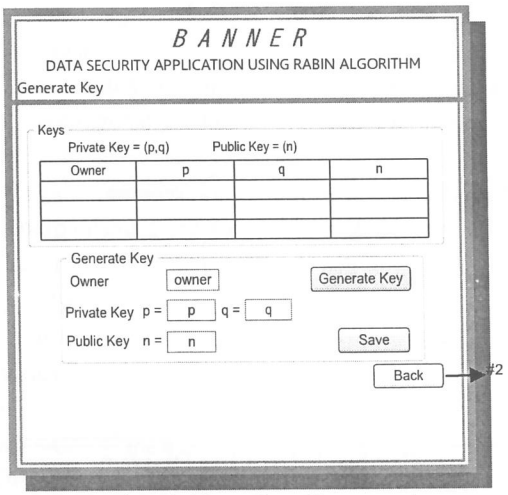
Tahap perancangan antarmuka akan menyediakan contoh halaman dan *storyboard*.



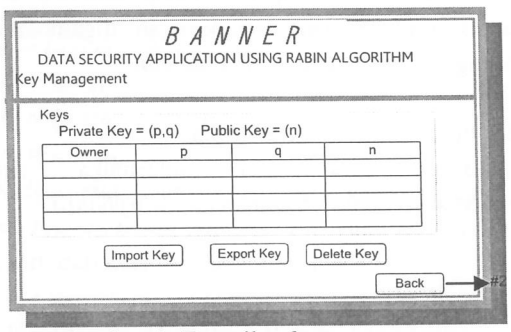
Gambar 2. Tampilan halaman login



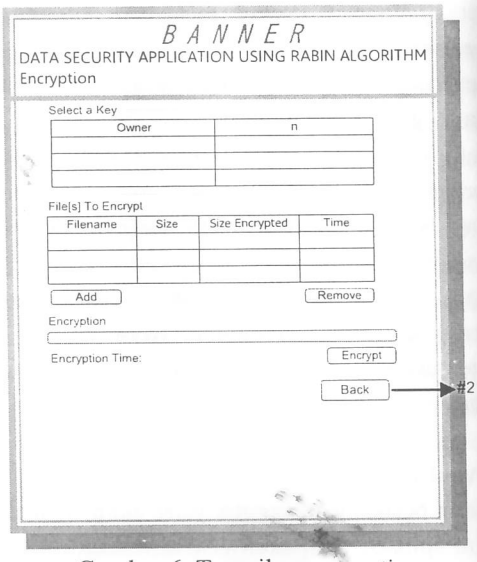
Gambar 3. Tampilan menu utama



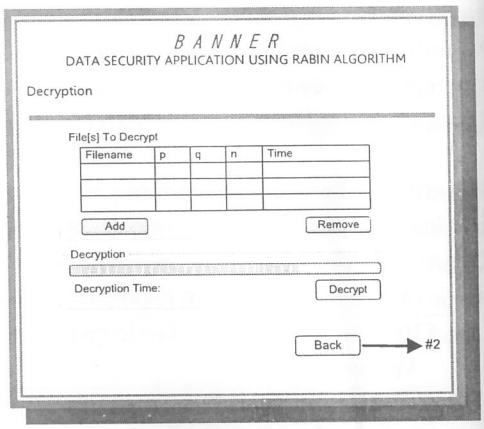
Gambar 4. Tampilan *Generate key*



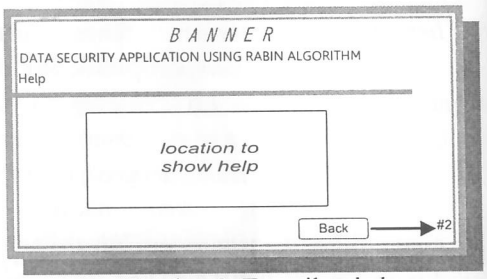
Gambar 5. Tampilan *key management*



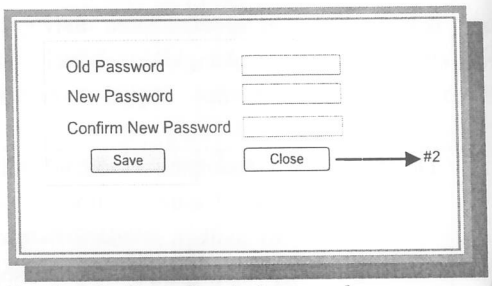
Gambar 6. Tampilan *encryption*



Gambar 7. Tampilan *decryption*



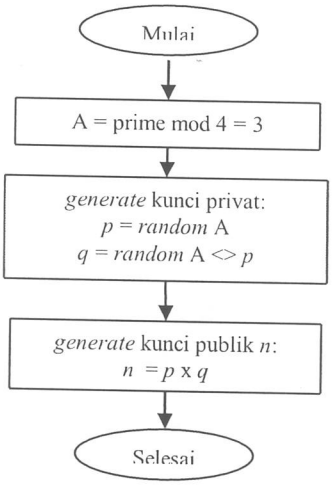
Gambar 8. Tampilan *help*



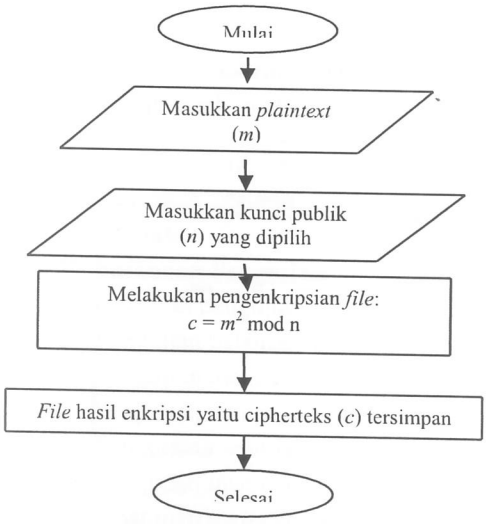
Gambar 9. Tampilan halaman *change password*

3.2.2 Perancangan Algoritma

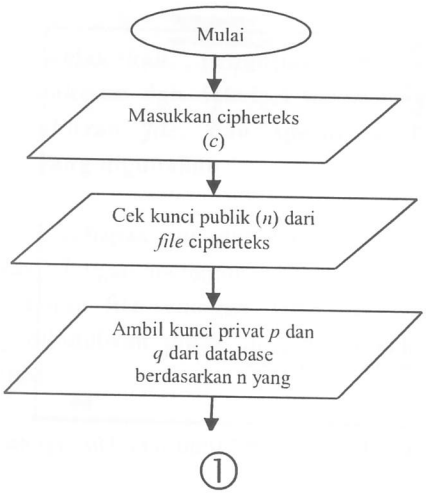
Penggambaran notasi algoritma menggunakan diagram alir (*flowchart*).



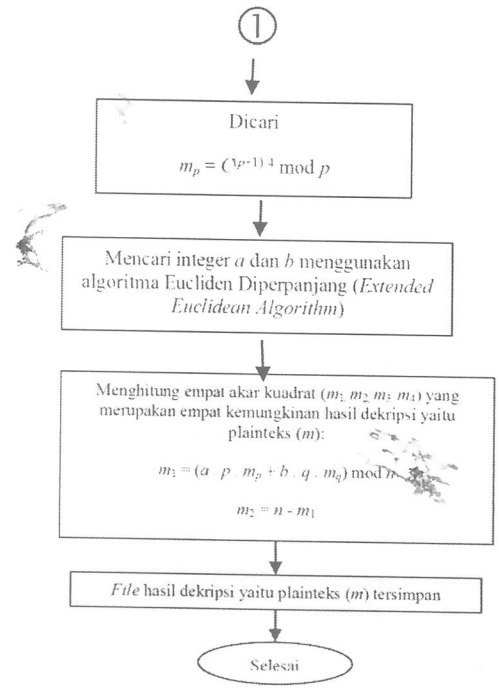
Gambar 10. *Flowchart Generate Key*



Gambar 11. *Flowchart* Enkripsi *File*



Gambar 12. *Flowchart* Dekripsi *File*



4. IMPLEMENTASI DAN PENGUJIAN

Tujuan dari tahap ini untuk menunjukkan *hardware* dan *software* yang digunakan. Selain itu, pengujian *prototype* yang telah dibangun apakah telah sesuai spesifikasi analisis dan perancangan.

4.1 Lingkungan Implementasi

A. Spesifikasi perangkat keras

Tabel 2. Spesifikasi Kebutuhan Perangkat Keras

Nama	Rekomendasi
Processor	*Intel Pentium* 4 (2.0 *Ghz*) atau versi lebih tinggi
Memory (RAM)	*1Gb* atau lebih tinggi
Harddisk	Minimal 20 Gb
CD-ROM	*CD-R / CD-RW / DVD-R / DVD-RW*
Mouse dan *keyboard*	Standard

B. Spesifikasi perangkat lunak

Tabel 3. Spesifikasi Kebutuhan Perangkat Lunak

Nama	Fungsi
Borland Delphi 7	Perangkat lunak utama dalam membangun aplikasi ini
Adobe Photoshop CS	Perangkat lunak yang digunakan dalam penggambaran dan modifikasi grafik 2D

Nama	Fungsi
Microsoft Office Word 2007	Digunakan untuk penulisan laporan
Microsoft Visio 2003	Digunakan untuk menggambarkan diagram UML

4.1.1 Pengkodean Program

Berikut ini adalah kode program untuk pembangkitan kunci, proses enkripsi dan dekripsi.

***Coding* memilih bilangan prima *p* dan *q* sebagai kunci privat dan menghitung bilangan n sebagai kunci publik**

```
Randomize;
repeat
repeat
  Result.p := prime[(Random(MAXD)
  mod   idxPrime) + 1];
until Result.p > 0;
repeat
  Result.q := prime[(Random(MAXD)
  mod   idxPrime) + 1];
until (Result.p <> Result.q) and
  (Result.q > 0);
  Result.n := Result.p *     Result.q;
until (Result.n > high(word)) and (Result.n
<=  high(longword));
```

***Coding* proses enkripsi algoritma Rabin**

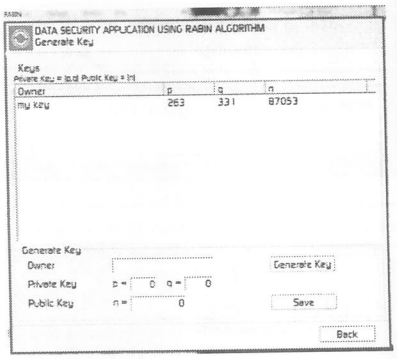
```
function Encrypt(n :      longword;  m  :
byte) :   longword;
begin
   Result :=          modular_pow(m,2,n);
end;
```

***Coding* proses dekripsi dengan algorita Rabin**

```
function Decrypt(a, b : integer; p, q, c :
longword) : byte;
var
  mp, mq: longword;
  n : longword;
  pp, qq : longword;
  m1,m2,m3,m4 : integer;
begin
  pp := (p+1) div 4;
  qq := (q+1) div 4;
  mp := modular_pow(c,pp,p);
  mq := modular_pow(c,qq,q);
  n := p * q;
  m1 := (a * p * mq + b * q * mp) mod n;
  if m1 < 0 then begin
    m1 := n + m1;
end;
m2 := n - m1;
m3 := (a * p * mq - b * q * mp) mod n;
if m3 < 0 then begin
  m3 := n + m3;
end;
m4 := n - m3;
result := 0;
if m1 <= high(byte) then
  Result := m1
else
if m2 <= high(byte) then
  Result := m2
else
if m3 <= high(byte) then
  Result := m3
else
if m4 <= high(byte) then
  Result := m4;
end;
```

4.1.2 Implementasi Antarmuka

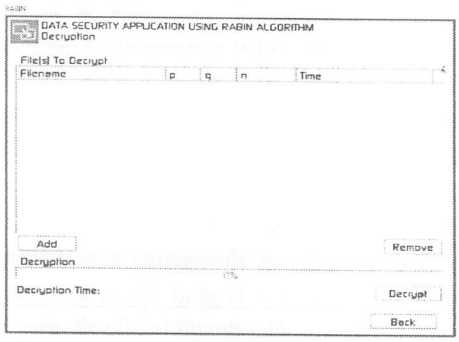
Berikut ini merupakan beberapa tampilan halaman aplikasi.



Gambar 13. Tampilan Menu *Generate Key*

Gambar 14. Tampilan Menu *Key Management*

Gambar 15. Tampilan Menu *Encryption*



Gambar 16. Tampilan Menu *Decryption*

4.2 Pengujian

4.2.1 Pelaksanaan Pengujian

Pelaksanaan pengujian meliputi:

a. Pengujian halaman *login*
b. Pengujian menu utama
c. Pengujian menu *generate key*
d. Pengujian menu *key management*
e. Pengujian menu *encryption*
f. Pengujian menu *decryption*
g. Pengujian menu *help*
h. Pengujian menu *change password*

4.2.2 Melakukan pengujian waktu proses enkripsi dan dekripsi terhadap jenis *file*, ukuran *file*, dan spesifikasi komputer yang digunakan

Tahapan ini digunakan untuk menguji aplikasi dengan menggunakan berbagai jenis file dan ukuran file sehingga dapat diketahui waktu yang dibutuhkan untuk melakukan enkripsi dan dekripsi.

Tabel 4. Analisis Waktu Proses Enkripsi dan Dekripsi Terhadap Jenis *File*, Ukuran *File*, dan Spesifikasi Komputer

Nama *File*	Ukuran *File*	Waktu Proses Enkripsi (*mili second*)	Waktu Proses Dekripsi (*mili second*)
Windows 7 Ultimate *Processor: Intel® Core i3-370M processor* *Memory : 2 GB DDR3 Memory*			
ROHANI.mp3	2.797 Mb	30997 ms	34133 ms
project_komgraf.avi	4.875 Mb	33384 ms	36005 ms
Wildlife.wmv	25.631Mb	279788 ms	194954 ms
OSI.gif	13 Kb	203 ms	109 ms
Tulips.jpg	607 Kb	6552 ms	7415 ms
Newspic.psd	282 Kb	1919 ms	2138 ms
Goldenly.png	235 Kb	2574 ms	2747 ms
bg.bmp	1.604 Mb	17285 ms	21903 ms
Software_Engineering.pdf	6.823 Mb	46597 ms	49109 ms
Eclipse.doc	7.076 Mb	76597 ms	51605 ms
summer.txt	1.31 Kb	32 ms	15 ms
cover.docx	175 Kb	1856 ms	1248 ms
xampp.exe	34.560 Mb	387413 ms	388759 ms
kbbi-offline.zip	3.297 Mb	22059 ms	23993 ms
Windows 7 Ultimate *Processor : Intel® Core™ 2 Duo* *Memory* (RAM) *: 2 GB Memory*			
ROHANI.mp3	2.797 Mb	61860 ms	127203 ms
project_komgraf.avi	4.875 Mb	120281 ms	232640 ms
Wildlife.wmv	25.631Mb	898156 ms	766329 ms
OSI.gif	13 Kb	297 ms	594 ms
Tulips.jpg	607 Kb	13375 ms	19078 ms
Newspic.psd	282 Kb	6235 ms	13234 ms
Goldenly.png	235 Kb	5203 ms	10203 ms
bg.bmp	1.604 Mb	35344 ms	39203 ms
Software_	6.823	205407	295625

Nama *File*	Ukuran *File*	Waktu Proses Enkripsi (*mili second*)	Waktu Proses Dekripsi (*mili second*)
Engineering.pdf	Kb	ms	ms
Eclipse.doc	7.076 Mb	230141 ms	299438 ms
summer.txt	2 Kb	94 ms	93 ms
cover.docx	175 Kb	3844 ms	7062 ms
xampp.exe	34.560 Mb	1418266 ms	1381016 ms
kbbi-offline.zip	3.297 Mb	104610 ms	144062 ms

4.2.3 Analisis Hasil Pengujian

Dari hasil pengujian proses enkripsi dan dekripsi di atas diperoleh hasil yang berbeda terhadap waktu proses enkripsi dan waktu proses dekripsi suatu *file*. Dari pengujian tersebut dapat dikatakan bahwa semakin besar ukuran *file* semakin lama proses enkripsi/dekripsinya, dan begitupun sebaliknya. Untuk ukuran minimum *file* yang dapat dienkripsi tidak dibatasi, untuk maksimum ukuran *file* yang dapat dienkripsi tergantung dari ukuran kapasitas penyimpanan *disk* serta sistem *file* yang digunakan.

Kecepatan proses enkripsi/dekripsi juga dipengaruhi oleh spesifikasi komputer yang digunakan, dimana semakin tinggi spesifikasi komputer yang dipakai maka proses enkripsi/dekripsi suatu *file* akan semakin cepat prosesnya.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan pengujian yang telah dilakukan maka dapat ditarik kesimpulan bahwa:

1. Aplikasi pengamanan data menggunakan algoritma Rabin dapat membantu pengguna dalam menjaga kerahasiaan dan keamanan data yang disimpan dan dipertukarkan.
2. Aplikasi pengamanan data menggunakan algoritma Rabin dapat mengenkripsi dan mendekripsi semua jenis *file* dengan ukuran *file* yang berbeda – beda.
3. Waktu untuk proses enkripsi dan dekripsi berbanding lurus dengan penambahan ukuran *file* dan dipengaruhi oleh spesifikasi komputer yang digunakan.

5.2 Saran

Saran untuk pengembangan aplikasi adalah aplikasi dapat dikembangkan lebih lanjut dengan menambahkan fitur untuk mengenkripsi direktori *folder*.

6. DAFTAR PUSTAKA

1. Ariyus, D. (2008). *Pengantar Ilmu Kriptografi: Teori, Analisis dan Implementasi*. Yogyakarta: Andi.
2. Caroline, ML. (2011). *Perbandingan Algoritma Kriptografi Kunci Publik RSA, Rabin, dan Elgamal*. Institut Teknologi Bandung. Diakses di http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2010-2011/Makalah2/Makalah2-IF3058-Sem2-2010-2011-029.pdf [3 Maret 2012].
3. Hariyanto, B. (2008). *Dasar Informatika & Ilmu Komputer: Disertai aksi-aksi praktis*. Yogyakarta: Graha Ilmu.
4. Laba, GL. (2011). *Penerapan algoritma RSA dan Rabin dalam Digital Signature*. Institut Teknologi Bandung. Diakses di http://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2011-2012/Makalah2011/Makalah-IF2091-2011-085.pdf [1 Juni 2012].
5. Menezes, A., van Oorschot, P., dan Vanstone, S. (1996). *Handbook of Applied Cryptography*. CRC Press. Diakses di http://www.cacr.math.uwaterloo.ca/hac/ [3 Maret 2012].
6. Munir, R. (2006). *Kriptografi*. Bandung: Informatika.
7. Sanusi, M. (2010). *The Genius: Hacking Sang Pembobol Data*. Jakarta: PT Elex Media Komputindo.
8. Wahana Komputer. (2010). *The Best Encryption Tools*. Jakarta: PT Elex Media Komputindo.