# Perbandingan Kriptografi RSA dengan Base64

**Natalia Florida Ginting[1] , Misalina Ginting[2]**
[1]Teknik Informatika Unika St. Thomas S.U; Jln. Setia Budi No.479-F Medan, 061-8210161
[2]Teknik Informatika Unika St. Thomas S.U; Jln. Setia Budi No.479-F Medan, 061-8210161
e-mail : natalia7@gmail.com; [2]misalina@gmail.com

***Abstrak***

*Kriptografi mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut. Sampai saat ini belum ada penyerangan terhadap RSA yang efektif. Namun apabila pemilihan parameter dan implementasi yang tidak tepat terhadap RSA dapat merupakan titik lemah sistem RSA sehingga rentan untuk diserang. Kriptografi transformasi Base64 banyak digunakan didunia internet sehingga media data format untuk mengirimkan data, ini dikarenakan hasil dari Base64 berupa plainteks maka data ini akan jauh lebih mudah dikirim, dibandingkan dengan format data yang berupa bineri. Sistem yang akan dibangun peneliti dalam pengamanan teks menggunakan algoritma RSA dan Base64, dimana kedua algoritma tersebut akan dibandingkan ukran dan waktu prosesnya untuk mencari yang mana algotitma terbaik.*

***Kata kunci** : Kriptografi, RSA, Base64*

***Abstract***

*Cryptography studies mathematical techniques related to the security aspects of information, such as data confidentiality, data validity, data integrity, and data authentication. The cryptographic algorithm is a logical step how to hide messages from unauthorized people over the message. Until now there has been no effective attack on RSA. However, if the selection of parameters and improper implementation of the RSA can be a weak point of the RSA system so vulnerable to attack. Base64 transformation cryptography is widely used in the world of the Internet so that the data format media to transmit data, this is because the result of Base64 in the form of plaintext then this data will be much easier to send, compared with the format of data in the form of binaries. The system that the researcher will build in text security uses RSA and Base64 algorithm, where the two algorithms will compare the ukran and the process time to find which one is the best algorithm.*

***Keywords:** Cryptography, RSA, Base64*

## 1. PENDAHULUAN

Kriptografi merupakan bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi maupun dekripsi. Teknik ini digunakan untuk mengkonversi data kedalam bentuk kode-kode tertentu sehingga menjadi susunan huruf acak yang terurut dan tidak dapat dibaca. Algoritma yang di gunakan dalam penelitian ini adalah algoritma RSA dan base 64. Untuk mengetahui kinerja kedua algoritma tersebut harus dilakukan pengujian yang mengarah pada kecepatan dalam proses mengenkripsi atau mendekripsi data dan besaran ukuran file yang dihasilkan. Dari kedua algoritma kriptografi tersebut akan diketahui kelemahan dan

kelebihan dalam hal penanganan proses enkripsi maupun dekripsi, maka diperlukan analisis untuk mengetahui kerja program melalui uji validitas kecepatan dan besaran ukuran file yang dihasilkan dari tiap proses eksekusi. Algoritma yang efisien ialah algoritma yang meminimumkan kebutuhan ruang dan waktu dalam proses enkripsi dan dekripsi.

Maksud dari penelitian ini yaitu untuk mengetahui perbandingan kecepatan dan ukuran file yang akan dihasilkan dari algoritma RSA dan Base64. Adapun tujuan dari penelitian ini berdasarkan rumusan masalah diatas adalah membuat aplikasi enkripsi maupun dekripsi data menggunakan algoritma RSA dan algoritma base64, membandingkan kinerja aplikasi enkripsi maupun dekripsi data menggunakan algoritma RSA dan algoritma base64 dalam hal kecepatan proses enkripsi maupun dekripsi dan besaran ukuran file yang di hasilkan

## 2. METODOLOGI PENELITIAN

### *2.1 Definisi Kriptografi*

Menurut Muhammad, Fitriyani dan Nurul (2015) Kriptografi (*cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Sehingga Kriptografi dapat diartikan sebagai ilmu yang mempelajari tentang penyembunyian huruf atau tulisan sehingga membuat tulisan tersebut tidak dapat dibaca oleh orang yang tidak berkepentingan. Kriptografi mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Algoritma kriptografi merupakan langkah-Iangkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut.

Algoritma kriptografi terdiri dari tiga fungsi dasar, yaitu:

1. Enkripsi: merupakan hal yang sangat penting dalam kriptografi. Merupakan pengamanan data yang dikirimkan agar terjaga kerahasiaannya. Pesan asli disebut *plaintext*, yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan *cipher* atau kode. Sama halnya dengan kita tidak mengerti akan sebuah kata maka kita akan melihatnya di dalam kamus atau daftar istilah. Beda halnya dengan enkripsi. untuk mengubah teks-asli ke bentuk teks-kode kita menggunakan algoritma yang dapat mengkodekan data yang kita inginkan.
2. Dekripsi: merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (teks-asli), disebut dengan dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma yang digunakan untuk enkripsi.
3. Kunci: yang dimaksud di sini adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, kunci privat (*private key*) dan kunci umum (*public key*).

### *2.2 Algoritma RSA*

Menurut Muhammad, Fitriyani dan Nurul (2015) Dari banyak algoritma kriptografi asimetris yang ada, algotirma yang paling populer adalah RSA. Algortima RSA dibuat oleh tiga orang peneliti dari MIT (*Massachussets Institute of Technology*) pada tahun 1976. Nama RSA merupakan singkatan dari nama tiga orang penemunya, yaitu Rivest, Shamir, dan Adleman. Algoritma RSA melakukan pemfaktoran bilangan yang sangat besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci privat.

Algoritma RSA memiliki besaran-besaran sebagai berikut:

1. p dan q bilangan prima (rahasia)
2. $n = p \cdot q$ (tidak rahasia)
3. $\phi(n) = (p - 1)(q - 1)$ (rahasia)
4. e (kunci enkripsi) (tidak rahasia)
5. d (kunci dekripsi) (rahasia)

6. m (plainteks) (rahasia)
7. c (chiperteks) (tidak rahasia)

### *2.3 Algoritma Base64*

Menurut Febrian, Adriana dan Febry (2015) Transformsi Base64 merupakan salah satu algoritma untuk Encoding dan Decoding suatu data ke dalam format ASCII, yang di dasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metoda yang di gunkan untuk melakukan Encoding (penyandian) terhadap data binary. Karakter yang di hasilkan pada transformasi Base64 ini terdiri dari A..Z, a..z, dan 0..9, serta ditambah dengan dua karakter terakhir yang bersimbol yaitu + dan / serta satu buah karaker sama dengan (=) yang digunakan untuk penyesuaian dan menggenapkan data binary atau istilahnya disebut sebagai pengisi pad. Arakter simbol yang akan di hasilkan akan tergantung dari proses algoritma yang berjalan.

Menurut Ariyus dalam Febrian, Adriana dan Febry (2015) Teknik encoding Base64 sebnarnya sederhana, jka ada satu (string) bytes yang akan di sandikan ke Base64 maka caranya adalah :

1. Pecah *string bytes* tersebut ke per-3 bytes.
2. Gabungkan 3 bytes menjadi 24 bit. Dengan catatan 1 bytes = 8 bit, sehingga 3 x 8 = 24 bit.
3. Lalu 24 bit yang disimpan di-buffer (disatukan) dipecah-pecah menjadi 6 bit, maka akan menghasilkan 4 pecahan.
4. Masing-masing pecahan di ubah ke dalam nilai decimal, dimana maksimal nilai 6 bit adalah 63
5. Terakhir jadikan nilai-nilai desimal tersebut menjadi indeks untuk memilih karakter penyusun dari Base64 dan maksimal adalah 63 atau indeks ke 64.

Dan seterusnya sampai akhir string bytes yang mau kita konversikan. Jika ternyata dalam proses encoding terdapat sisa pembagi, maka tambahkan sebagai penggenap sisa tersebut karakter =. Maka terkadang pada *Base64* akan muncul satu atau dua karakter = ().

## 3. HASIL DAN PEMBAHASAN

### *3.1. Form Utama*


**Gambar 1.** Tampilan Form Utama

Dapat dilihat terdapat 6 (enam) buah menu pada form utama, yaitu menu ciptakan kunci, enkripsi, dekripsi, penulis, bantuan dan keluar. Serta dua buah submenu, yaitu submenu RSA dan Base64 yang terdapat pada menu enkripsi dan dekripsi.

### *3. 2. Ciptakan Kunci*

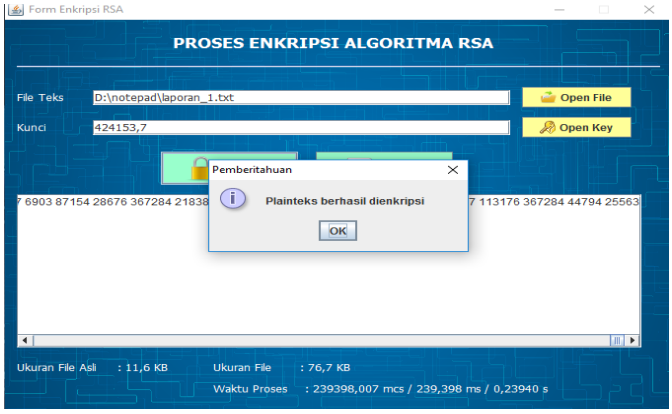
Form ciptakan kunci berfungsi untuk menciptakan kunci publik dan kunci privat yang akan digunakan pada algoritma RSA. Kunci publik digunakan untuk melakukan proses enkripsi

dan kunci privat digunakan untuk melakukan proses dekripsi. Tampilan form ciptakan kunci dapat dilihat pada Gambar 2.


**Gambar 2.** Tampilan Form Kunci

### *3. 3 Form Enkripsi RSA*

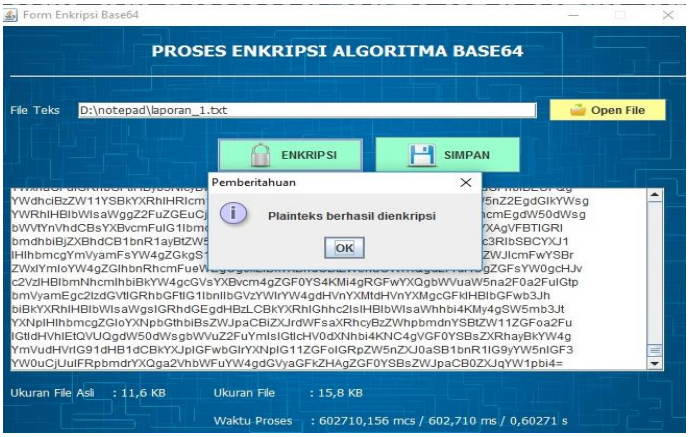
Form enkripsi RSA digunakan untuk melakukan proses enkripsi file teks. User harus menginput terlebih dahulu pesan yang akan dienkripsi dengan cara mencari file teks menggunakan tombol open file. Kemudian menginput kunci publik yang sudah di ciptakan. Selanjutnya user dapat mengklik tombol enkripsi maka pesan akan berubah menjadi cipherteks dan ukuran file dan waktu proses akan tampil pada form tersebut. Setelah proses enkripsi selesai, maka user dapat menyimpan hasil enkipsi dengan cara mengklik tombol simpan. Tampilam form enkripsi RSA dapat dilihat pada Gambar 3.




**Gambar 3** Painteks Berhasil Dienkripsi

### *3.4. Form Enkripsi Base64*

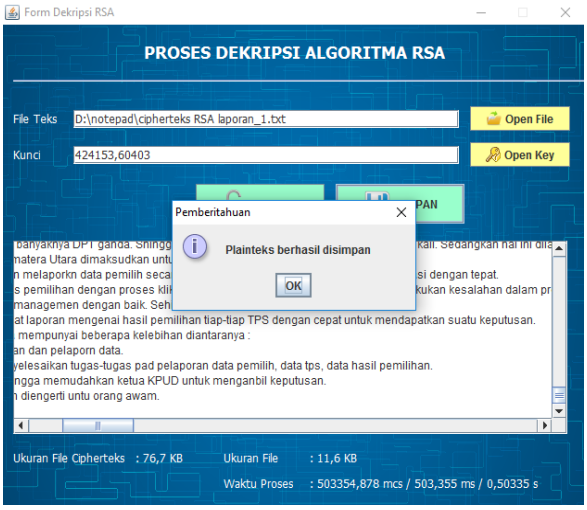
Form enkripsi Base64 digunakan untuk melakukan proses enkripsi file teks. User harus menginput terlebih dahulu pesan yang akan dienkripsi dengan cara mencari file teks menggunakan tombol open file. Selanjutnya user dapat langsung mengklik tombol enkripsi maka pesan akan berubah menjadi cipherteks dan ukuran file dan waktu proses akan tampil pada form tersebut. Setelah proses enkripsi selesai, maka user dapat menyimpan hasil enkipsi dengan cara mengklik tombol simpan. Tampilam form enkripsi Base64 dapat dilihat pada Gambar 4.




**Gambar 4** Tampilan Form Enkripsi Base64

*3. 5 Form Dekripsi RSA*

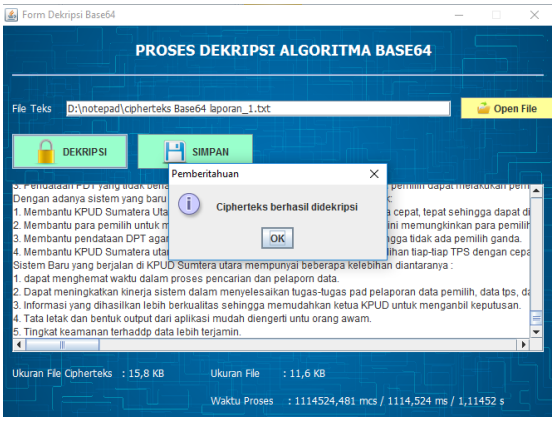
Form dekripsi RSA digunakan untuk melakukan proses dekripsi. User harus menginput terlebih dahulu pesan yang akan didekripsi dengan cara mencari file teks menggunakan tombol open file. Kemudian menginput kunci privat yang sudah di ciptakan. Selanjutnya user dapat mengklik tombol dekripsi maka pesan akan berubah menjadi teks asli (plainteks) dan ukuran file dan waktu proses akan tampil pada form tersebut. Setelah proses dekripsi selesai, maka user dapat menyimpan hasil dekripsi dengan cara mengklik tombol simpan. Tampilam form dekripsi RSA dapat dilihat pada Gambar 5




Gambar 5 Tampilan Form Dekripsi RSA

*3.6 Form Dekripsi Base64*

Form dekripsi Base64 digunakan untuk melakukan proses dekripsi. User harus menginput terlebih dahulu pesan yang akan didekripsi dengan cara mencari file teks menggunakan tombol open file. Selanjutnya user dapat mengklik tombol dekripsi maka pesan akan berubah menjadi teks asli (plainteks) dan ukuran file dan waktu proses akan tampil pada form tersebut. Setelah proses dekripsi selesai, maka user dapat menyimpan hasil dekripsi dengan cara mengklik tombol simpan. Tampilam form dekripsi Base64 dapat dilihat pada Gambar 6.




Gambar 6 Tampilan Form Dekripsi Base64

## 4. KESIMPULAN

Berdasarkan hasil pengujian yang telah dilakukan maka penulis memperoleh beberapa kesimpulan, yaitu :

1. Berdasarkan aplikasi yang telah dibangun pada proses enkripsi algoritma Base64 lebih cepat prosesnya jika di bandingkan dengan algoritma RSA. Sedangkan pada proses dekripsi algoritma RSA lebih cepat jika dibandingkan dengan algoritma Base64.
2. Berdasarkan hasil ukuran dari proses enkripsi bahwa algoritma Base64 lebih sedikit dibandingkan algoritma RSA.
3. Dari proses enkripsi dan dekripsi algoritma RSA maupun Base64 berdasarkan dua laptop yang digunakan bahwa laptop Acer lebih cepat dibandingkan dengan laptop Lenovo.

## 5. SARAN

Adapun saran yang dapat penulis berikan untuk pengembangan lebih lanjut yaitu:

1. Dengan menambahkan jenis file yang berbeda seperti doc dan pdf.
2. Penelitian dapat di kembangkan dengan meningkatkan ukuran file dari yang telah diuji penulis.

## DAFTAR PUSTAKA

[1] Arief.M,: Fitriyani, dan Nurul.I, 2015. Kriptografi RSA pada Aplikasi File Transfer Client – Server Based, Jurnal Ilmiah Teknologi Informasi Terapan. Vol.1 No.3

[2] Rifki Sadikin. 2012. Kriptografi untuk Keamanan Jaringan. Penerbit Andi. Yogyakarta

[3] C.Febrian.Wahyu.; Adriana.P.R. dan Febry de fretes, 2015. Penerapan Algoritma Gabungan RC4 dan Base64 pada Sistem Keamanan *E-Commerce*, Seminar Nasional Aplikasi Teknologi Informasi.