

IMPLEMENTASI KRIPTOGRAFI MODERN DENGAN METODE RSA PADA DATA CITRA DIGITAL

Zeyan Zico Deskiva

STMIK Kristen Neumann Indonesia
Jl. Letjen Jamin Ginting KM. 10,5 Medan
zeyn.zhe@gmail.com

Program Studi Teknik Informatika

ABSTRAK

Perkembangan teknologi pada saat ini telah sangat membantu manusia dalam berbagai bidang, khususnya dalam bidang komunikasi, yang hanya memerlukan waktu yang singkat dalam bertukar informasi. Informasi-informasi tersebut tersimpan dalam bentuk format digital, seperti teks, citra, video, audio, dan multimedia lainnya. Khususnya terkait dengan citra digital, banyak sekali terdapat aplikasi untuk mengubah gambar dengan mudah. Penelitian ini memiliki tujuan untuk membuat sebuah aplikasi yang dapat digunakan untuk mengamankan gambar-gambar tersebut khususnya dalam citra digital, dan salah satu metode yang dapat digunakan adalah kriptografi. Kriptografi adalah sebuah seni dalam menjaga kerahasiaan sebuah data. Untuk menjaga kerahasiaan data tersebut kriptografi mengubah data yang memiliki makna (plaintext) menjadi bentuk yang tidak diketahui maknanya (ciphertext). Ciphertext inilah yang akan dikirim kepada penerima. Metode yang dipakai pada kasus ini adalah metode asimetris dengan algoritma Rivest Shamir Adleman (RSA). Kesulitan dalam pemfaktoran bilangan-bilangan menjadi faktor prima adalah letak keamanan dari algoritma RSA, yang bertujuan untuk mendapatkan kunci publik dan private.

Kata Kunci: Kriptografi, RSA, Enkripsi, Dekripsi, Citra Digital,

PENDAHULUAN

Perkembangan teknologi informasi saat ini telah mengalami perkembangan yang sangat pesat yang telah mampu menciptakan sesuatu yang dapat mendukung perkembangan dari teknologi informasi tersebut.

Informasi tersebut saat ini telah dapat disajikan dan tersimpan berbentuk digital dan memiliki beberapa bentuk seperti teks, citra, video, audio, dan multimedia. Dalam hal ini, khususnya citra digital banyak sekali terdapat aplikasi yang dapat memanipulasi citra tersebut dengan mudah oleh oknum-oknum yang kurang bertanggung jawab dengan memberikan kesan-kesan negatif dalam citra tersebut. Hal tersebut menimbulkan kekhawatiran pada berbagai pihak dalam melakukan interaksi baik secara individu maupun kelompok.

Berdasarkan permasalahan tersebut, dibutuhkan cara dalam melindungi data tersebut untuk menghindari penggunaan data yang bersifat negatif oleh pengguna yang tidak bertanggung jawab. Maka dari

itu, dikembangkanlah sistem pengamanan data yang berbasis pada ilmu penyandian yang disebut dengan “Kriptografi”.

Kriptografi merupakan sebuah seni dalam menyandikan suatu pesan dengan mengubah data yang semula memiliki makna yang jelas menjadi data yang tidak dapat diketahui maknanya.

Algoritma kriptografi yang dibahas dalam penelitian ini adalah Algoritma Kriptografi dengan metode Asimetris dengan Algoritma RSA (Rivest Shamir Adleman). Algoritma RSA memiliki dua kunci, yaitu publik dan rahasia.

Beberapa peneliti telah melakukan penelitian tentang Algoritma Kriptografi RSA (Rivest Shamir Adleman), diantaranya:

1. Hanes dan Rin Rin Meilani Salim (2014), melakukan penelitian tentang “Penerapan Algoritma RSA Untuk Pengamanan Password Pada Aplikasi Desktop”.
2. Lisda Juliana Pangaribuan (2014), melakukan penelitian tentang “Kriptografi Modern Kunci Asimetris

Dengan Metode RSA Untuk Keamanan Pesan Dalam E-Mail”.

Berdasarkan latar belakang tersebut, maka yang menjadi rumusan masalah pada penulisan penelitian ini adalah:

1. Bagaimana menyandikan suatu gambar dengan metode RSA.
2. Bagaimana algoritma RSA bekerja dalam penyandian data citra digital.
3. Bagaimana menerapkan algoritma RSA dengan citra digital untuk menyandikan gambar.

Tujuan dari penelitian ini adalah:

1. Mengetahui teknik penyandian suatu gambar dengan metode RSA.
2. Mengetahui Algoritma RSA bekerja dalam penyandian data Citra Digital.
3. Penerapan Algoritma RSA dalam Citra Digital untuk menyandikan gambar.

Pengertian Kriptografi

Kata Kriptografi (*cryptography*) berasal dari bahasa Yunani: "*cryptos*" artinya "*secret*" (rahasia), sedangkan "*gráphein*" artinya "*writing*" (tulisan). Jadi kriptografi berarti "*secret writing*" (tulisan rahasia) (Munir, 2006:2).

Buku-buku lama mengatakan bahwa kriptografi adalah sebuah ilmu dan seni dalam menjaga kerahasiaan suatu pesan dengan mengubahnya ke dalam bentuk yang maknanya tidak dapat diketahui lagi.

Algoritma Kriptografi RSA

Algoritma RSA diperkenalkan oleh tiga orang profesor MIT (*Massachusetts Institute of Technology*) yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1978. Nama RSA sendiri diambil dari inisial nama penemunya yakni Rivest, Shamir dan Adleman.

Kesulitan dalam pemfaktoran bilangan ke dalam bentuk prima adalah titik kekuatan dari algoritma ini untuk mendapatkan kunci private. Algoritma RSA tergolong ke dalam kriptografi asimetri, yaitu kriptografi yang menggunakan dua kunci: kunci publik (*public key*) dan kunci pribadi (*private key*).

Proses kriptografi algoritma RSA terdiri dari 3 tahapan yaitu :

1. Pembangkitan Kunci
 - a. Tentukan nilai p dan q sebagai dua bilangan prima sembarang.
 - b. Hitung $n = p \times q$ (sebaiknya p tidak sama dengan q).
 - c. Hitung $m = (p - 1)(q - 1)$.
 - d. Tentukan kunci publik, e , yang relatif prima terhadap m ($\text{gcd}(e, m) = 1$).
 - e. Cari d , sehingga $e \cdot d = 1 \text{ mod } (m)$, atau $d = (1 + nm)/e$ untuk bilangan besar
2. Proses Enkripsi
 - a. Ambil kunci publik penerima pesan, e , dan modulus n .
 - b. Nyatakan plaintext P menjadi blok-blok P_1, P_2, \dots , sehingga setiap blok menampilkan nilai di dalam selang $[0, n - 1]$.
 - c. Tiap blok P_i di enkripsi menjadi blok C_i dengan rumus

$$C_i = P_i^e \text{ mod } n$$

3. Proses Dekripsi
Setiap blok ciphertexts c_i di dekripsi kembali menjadi blok P_i dengan rumus

$$P_i = C_i^d \text{ mod } n$$

Citra Digital

Citra adalah suatu gambaran, kemiripan, atau imitasi dari sebuah objek. Citra terbagi 2 yaitu ada citra yang analog dan ada citra yang digital. Citra analog yaitu citra yang bersifat kontinu. Sedangkan citra digital adalah citra yang dapat diolah oleh komputer (T, Sutoyo *et al.* 2009: 9).

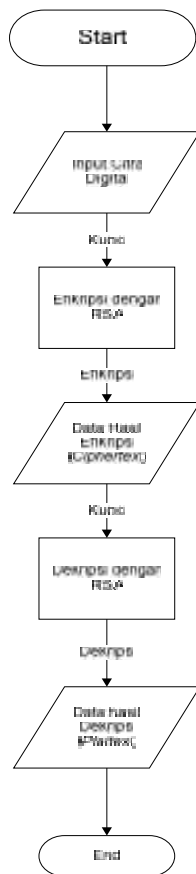
METODE PENELITIAN

Tujuan pembuatan sistem ini adalah menerapkan algoritma RSA dalam mengamankan data citra digital dimana disini penulis mengamankan data dalam bentuk gambar sehingga data ataupun gambar tersebut tidak dapat dilihat lagi. Langkah pertama dalam proses aplikasi ini yaitu melakukan enkripsi pada data citra digital dan melakukan dekripsi pada gambar tersebut.

Dalam proses awal sistem ini, akan dimulai dengan proses memasukkan gambar

ke dalam sistem sebagai *plaintext*. Setelah proses gambar selesai maka selanjutnya melakukan proses enkripsi pada gambar sesuai aturan yang sudah ditetapkan. Dari proses tersebut kita akan mendapatkan hasil dari enkripsi berupa *ciphertext* yang akan dikirim ke penerima. Setelah mendapatkan ciphertext maka selanjutnya dapat dilakukan proses dekripsi pada *ciphertext* yang telah di dapatkan untuk mendapatkan kembali gambar yang telah terenkripsi sebelumnya sehingga dapat melihat gambar seperti *plaintext* semula.

Berikut ini merupakan *flowchart* sistem untuk enkripsi dan dekripsi data citra digital.



HASIL DAN PEMBAHASAN

Hasil Pembahasan

Setelah program aplikasi dirancang, tahap selanjutnya yaitu tahap hasil dari perancangan. Hasil perancangan ini dilakukan dengan tujuan untuk mengetahui apakah berhasil atau tidak dan sesuai dengan yang dirancang. Aplikasi yang dihasilkan hanya melakukan proses enkripsi dan dekripsi citra digital atau gambar.

Tampilan Menu Utama

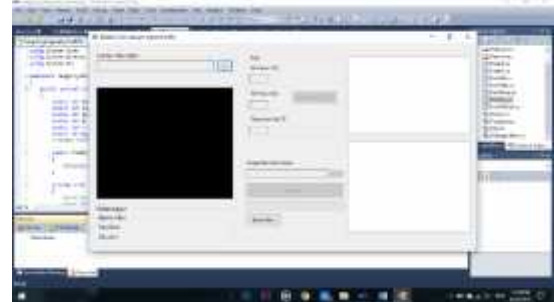
Form menu utama adalah form tampilan awal aplikasi saat pertama di buka atau di jalankan seperti tampilan gambar dibawah ini.



Gambar 1. Tampilan Utama Aplikasi
 Dalam tampilan awal tersebut, terdapat dua menu pilihan yaitu menu "RSA Algorithm" dan menu "Exit". Pada menu *RSA Algorithm* terdapat dua menu pilihan yaitu menu *encrypt* dan menu *decrypt*.

Tampilan Menu Enkripsi

Tampilan berikut adalah tampilan untuk melakukan load atau memasukkan gambar untuk proses enkripsi.



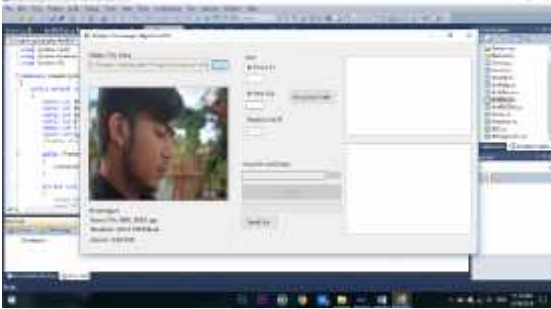
Gambar 2. Tampilan Load Gambar

Proses memasukkan gambar untuk proses enkripsi dilakukan dengan menekan tombol yang berwarna biru pada *layout* seperti gambar diatas. Setelah itu, pilihlah gambar yang untuk proses enkripsi seperti tampilan gambar dibawah ini.



Gambar 3. Form pilih gambar untuk proses enkripsi

Setelah berhasil memasukkan gambar, maka gambar tersebut akan tampil pada aplikasi.

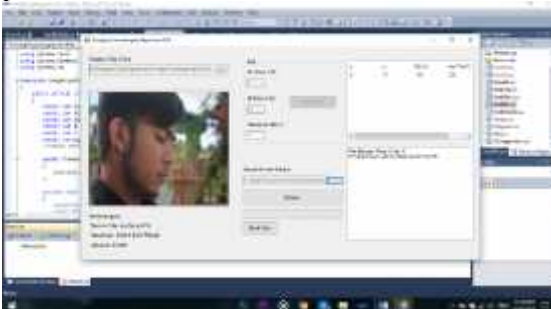


Gambar 4. Form Setelah Load Gambar

Setelah berhasil memasukkan gambar, proses selanjutnya adalah memasukkan bilangan prima pada kolom bilangan prima 1 dan 2 yang telah disediakan untuk melakukan pembangkitan kunci yaitu untuk mencari nilai n dan m dengan menekan tombol “Hitung” pada aplikasi. Masukkan juga nilai e yang merupakan bilangan yang relatif prima terhadap nilai m , dimana nilai ini bersifat rahasia.

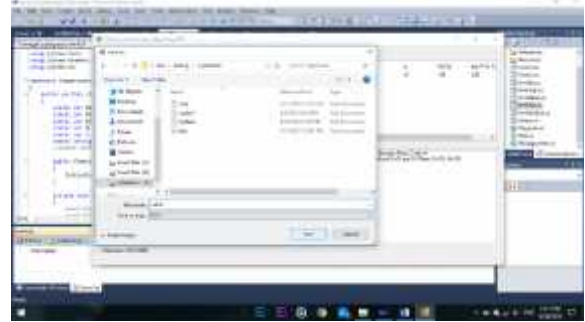
Tampilan Proses Enkripsi

Setelah berhasil melakukan load gambar, maka proses selanjutnya adalah memasukkan bilangan prima p dan q secara acak untuk melakukan proses pembangkitan kunci untuk proses enkripsi dan dekripsi, dimana bilangan tersebut tidak boleh sama. Dan juga masukkan nilai e yang relatif prima terhadap m hasil perhitungan dua bilangan prima.



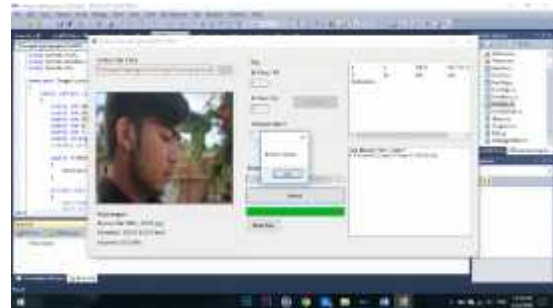
Gambar 5. Masukkan nilai p , q , dan e

Setelah berhasil melakukan proses diatas, selanjutnya tentukan dimana file hasil enkripsi nantinya akan disimpan agar lebih mudah dalam mencari kembali file hasil enkripsi ditemukan untuk diberikan kepada penerima.



Gambar 6. Tentukan dimana hasil enkripsi akan disimpan

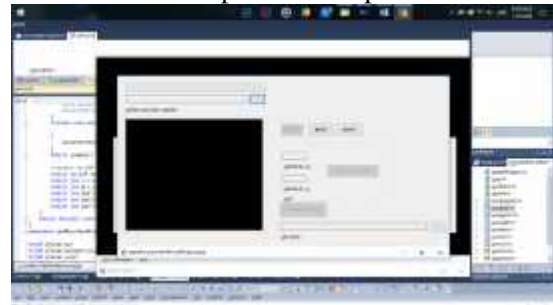
Setelah itu, tekan tombol “Enkripsi” pada aplikasi untuk melakukan proses enkripsi, dan akan muncul pesan jika proses telah selesai seperti gambar dibawah.



Gambar 7. Tampilan berhasil melakukan proses enkripsi

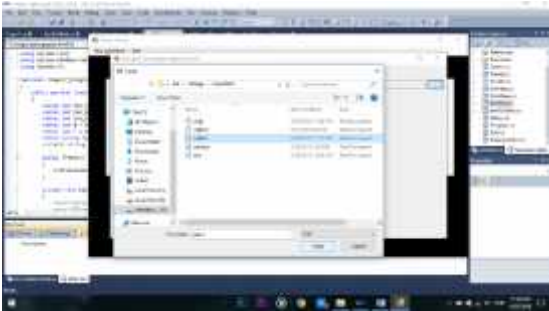
Tampilan Menu Dekripsi

Tampilan berikut adalah tampilan untuk melakukan proses dekripsi.



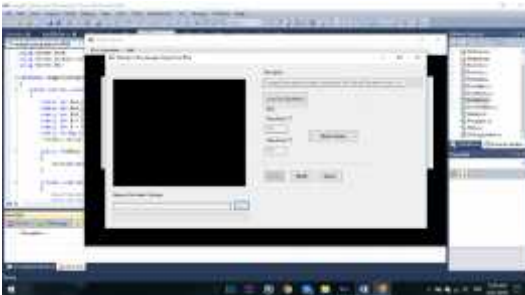
Gambar 8. Tampilan Menu Dekripsi

Untuk melakukan proses dekripsi, terlebih dahulu kita load cipherteks yang telah kita simpan saat melakukan proses enkripsi. Setelah menentukan file yang akan di dekripsi, tekan tombol “Load File” untuk melakukan load pada file.



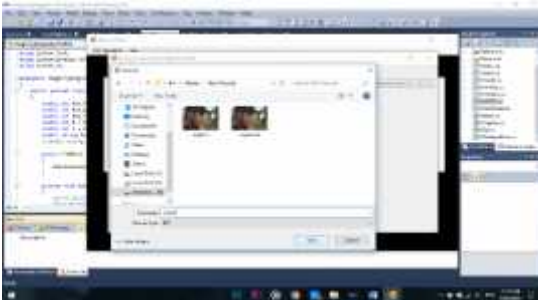
Gambar 9. Load File *Ciphertext*

Setelah itu, masukkan nilai d dan n untuk proses dekripsi yang telah di dapatkan pada proses enkripsi sebelumnya lalu tekan tombol “Hitung” dan masukkan nilai d dan n kembali untuk memvalidasi nilai yang dimasukkan sudah benar dan tekan tombol “Set Details” untuk melakukan verifikasi kunci.



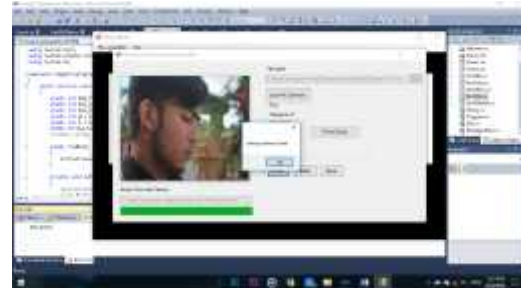
Gambar 10. Masukkan Nilai d dan n

Setelah itu, tentukan dimana file hasil dekripsi akan di simpan dan tentukan nama file sesuai dengan keinginan.



Gambar 11. Tentukan Tempat Penyimpanan File

Untuk menjalankan proses dekripsi, tekan tombol “Dekripsi” pada aplikasi dan tunggu hingga proses selesai dan akan muncul pesan jika proses tersebut telah selesai dan gambar hasil dekripsi akan tampil pada kolom yang telah ditentukan.



Gambar 12. Hasil Proses Dekripsi

KESIMPULAN

Berdasarkan pembahasan mengenai penerapan algoritma RSA pada data citra digital dapat disimpulkan sebagai berikut :

1. Algoritma kriptografi RSA dapat diimplementasikan pada penyandian data citra digital dengan mengubah citra menjadi bentuk nilai *pixel-pixel*.
2. Dalam membuat kunci publik dan kunci privat, ada beberapa faktor yang perlu dipertimbangkan, yaitu ukuran kunci, penentuan nilai p dan q agar sukar dibobol.
3. Data yang tersimpan berupa *ciphertext* yang merupakan hasil enkripsi menggunakan algoritma kriptografi RSA, sehingga pihak lain tidak dapat melihat gambar atau citra yang akan dikirim kepada penerima.
4. Berdasarkan hasil pengujian terhadap implementasi algoritma RSA, proses enkripsi dan dekripsi membutuhkan waktu sesuai dengan ukuran *pixel* gambar, dimana semakin besar jumlah *pixel* gambar tersebut maka akan semakin lama proses enkripsi dan dekripsi selesai.
5. Citra berwarna terdiri dari 3 layer matriks yaitu R-Layer, G-Layer, dan B-Layer untuk menentukan nilai suatu *pixel*

DAFTAR PUSTAKA

- [1] Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi*. Yogyakarta. Andi Offset
- [2] Ariyus, Dony. 2005. *Computer Security*. Yogyakarta. Andi Offset
- [3] Ginting, R. R. Isnanto, and I. P. Windasari, "Implementasi Algoritma

Kriptografi RSA untuk Enkripsi dan Dekripsi Email," Jurnal Teknologi dan Sistem Komputer, vol. 3, no. 2, pp. 253-258, Apr. 2015.

<https://doi.org/10.14710/jtsiskom.3.2.2015.253-258>

- [4] Hanes., Rin Rin, M.S. 2014. Penerapan Algoritma RSA Untuk Pengamanan Password Pada Aplikasi Desktop. Prosiding KeTIK 2014. ISBN: 979-458-766-4
- [5] Lisda, J.P.2014. Kriptografi Modern Kunci Asimetris Dengan Metode RSA Untuk Keamanan Pesan Dalam E-Mail. Prosiding KeTIK 2014. ISBN: 979-458-766-4
- [6] Munir, Rinaldi. 2006. Definisi Kriptografi. *Diktat Kuliah Kriptografi*. Program Studi Teknik Informatika. Sekolah Teknik Elektro dan Informatika. Institut Teknologi Bandung.
- [7] Putra, Darma. 2010. *Pengolahan Citra Digital*. Yogyakarta. Andi Offset
- [8] T. Sutoyo. 2009. *Teori Pengolahan Citra Digital*. Yogyakarta. Andi Offset