PENYANDIAN CITRA DENGAN KRIPTOGRAFI RSA

SKRIPSI

Disusun oleh :

Terry Dumania Manurung

NIM. 2205 3933

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS KRISTEN DUTA WACANA

YOGYAKARTA

2012

PENYANDIAN CITRA DENGAN KRIPTOGRAFI RSA

TUGAS AKHIR

Diajukan kepada Fakultas Teknologi Informasi
Program Studi Teknik Informatika
Universitas Kristen Duta Wacana Yogyakarta
sebagai salah satu syarat dalam memperoleh gelar
Sarjana Komputer

Disusun oleh :

Terry Dumania Manurung
NIM. 2205 3933

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
YOGYAKARTA
2012

PERYATAAN KEASLIAN TUGAS AKHIR

Saya menyatakan dengan sungguh-sungguh bahwa Tugas Akhir dengan judul:

PENYANDIAN CITRA DENGAN KRIPTOGRAFI RSA

Yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan sarjana Program Studi Teknik Informatika, Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di perguruan tinggi atau instansi manapun, kecuali bagian yang bersumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia untuk menerima sanksi.

Yogyakarta, 25 Juli 2012

(Terry Dumania Manurung)

22 05 3933

HALAMAN PERSETUJUAN

Judul	: **Penyandian Citra menggunakan metode Kriptografi RSA**
Nama	: **Terry Dumania Manurung**
Nim	: **220533933**
Mata kuliah	: Tugas Akhir
Kode	: TIW276
Semester	: Genap
Tahun	: 2011/2012

Selesai diperiksa dan
Disetujui di Yogyakarta
Pada tanggal:

Dosen Pembimbing I	Dosen Pembimbing II
(Willy Sudiarto R. S.Kom., M.Cs.)	(Restyandito. S.Kom., MSIS.)

HALAMAN PENGESAHAN

SKRIPSI

PENYANDIAN CITRA DENGAN KRIPTOGRAFI RSA

oleh : Terry Dumania Manurung / 22 05 3933

Dipertahankan didepan Dewan Penguji Tugas Akhir
Fakultas Teknologi Informasi Program Studi Teknik Informatika
Universitas Kristen Duta Wacana Yogyakarta
dan dinyatakan diterima untuk memenuhi sebagai
syarat-syarat guna memperoleh gelar Sarjana Komputer
Pada tanggal:

Yogyakarta,
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto R. S.Kom., M.Cs. ----------
2. Restyandito. S.Kom,. MSIS ----------
3. Budi Susanto., S.Kom., M.T. ----------
4. Theresia Herlina R., S.Kom., M.T ----------

Dekan,

(Drs. Wimmie Handiwidjojo, MIT)

Ketua Program Studi,

(Nugroho Agus. H, S.Si, M.Si)

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa yang telah melimpahkan rahmat dan anugerahnya, sehingga penulis dapat menyelesaikan tugas akhir dengan judul penyandian citra dengan kritografi RSA dengan baik.

Penulisan laporan ini merupakan kelengkapan dan pemenuhan dari salah satu syarat dalam memperoleh gelar sarjana komputer. Selain itu bertujuan melatih mahasiswa untuk dapat menghasilkan suatu karya yang dapat dipertanggungjawabkan secara ilmiah, sehingga dapat bermanfaat bagi penggunanya.

Dalam menyelesaikan pembuatan program dan laporan tugas akhir ini, penulis telah menerima bimbingan dan saran dan masukan serta semangat dari berbagai pihak, baik secara langsung maupun secara tidak langsung. Untuk itu dengan segala kerendahan hati, pada kesempatan ini penulis menyampaikan ucapan terimakasih kepada :

1. Bpk. Willy Sudiarto R, S.Kom., M.Cs. selaku dosen pembimbing I yang sabar dan seksama memberikan bimbingan dan dukungan moril secara langsung maupun secara tidak langsung.
2. Bpk. Restyandito, S.Kom., MSIS. Selaku dosen pembimbing II atas bimbingan, petunjuk dan masukan yang diberikan selama pengerjaan tugas akhir ini sejak awal hingga akhir.
3. Keluarga tercinta yang tak hentinya memberi dukungan doa dan semangat (mama, bapa, kak Vina, abang Juventus, adik Irin, Intan dan Bunga)
4. Sahabatku dalam perkuliahan maupun diluar perkuliahan yang selalu menjaga dan memberi ion positif dalam hidupku (Masku Yona, Tien, Corry, Lia, abang Son, kak Yenni, mas David, Lumut Crew, CG Yoka, CM UKDW, Euronet Tim, Mr. Reza)
5. Seluruh dosen pengajar selama masa perkuliahan penulis di Universitas Kristen Duta Wacana, serta dosen favorit yang sangat penulis kagumi

(Pak Yuan, Pak Hendro, Bu Widi, Bu Lucia, Bu Rosa, Pak Karel, Pak Gani, Pak Gun, Pak Katon, Pak Anton, Pak JJS, Pak Sri, Pak Petrus, Pak Joko, Pak Sri dan Pak BudSus)

6. Seluruh pihak yang membatu selama penulis berkuliah di Universitas Kristen Duta Wacana (Mas Roni, Mba Dhian, Mas Dave, Bpk/Ibu Dokter Poliklinik UKDW)
7. Semua kawan-kawanku yang sangat berjasa mengatasi setiap kegalauanku dengan setiap inspirasi yang sangat membuka otak kiri dan kanan pada saat membuat program, *I can not survive without you all, thankyou...*

Penulis menyadari bahwa program dan laporan tugas akhir ini masih jauh dari sempurna. Oleh karena itu, saran dan kritik merupakan salah satu penunjang untuk pengembangan dari program pada tugas akhir ini.

Akhir kata penulis memohon maaf atas kesalahan baik dalam penyusunan laporan maupun dalam kehidupan sehari-hari hingga penyelesaian tugas akhir ini. Kiranya laporan tugas akhir ini dapat berguna bagi kita semua.

Yogyakarta, 25 Juli 2012

Penulis

MOTTO

"Segala perkara dapat kutanggung di dalam Dia yang memberi kekuatan kepadaku …"

(Filipi 4:13)

"Berpeganglah pada didikan, janganlah melepaskannya, peliharalah dia, karena dialah hidupmu"

(Amsal 4:13)

ABSTRAK

Keamanan data merupakan hal terpenting dalam melakukan pengiriman sebuah data.Data yang dikirmkan dapat berupa data teks, suara, maupun data gambar atau citra. Keberhasilan sebuah proses pengamanan pada sebuah citra adalah dimana citra asli dan citra hasil pengamanan tidak mengalami perubahan yang signifikan. Salah satu pengamanan yang dapat dilakukan padas ebuah data adalah dengan metode kriptografi, yakni menyandikan data menjadi sebuah data baru. Kriptografi RSA dapat membantu dalam proses penyandian citra, dimana citra asli diamankan dengan kunci umum penerima dan penerima dapat mengembalikan citra yang telah disandikan dengan kunci rahasia. Implementasi metode kriptografi RSA pada penyandian citra dengan kunci yang tepat dapat menghasilkan citra yang bersifat lossless terhadap data citra yang asli.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB 1
PENDAHULUAN

1.1. Latar Belakang Masalah

Kriptografi merupakan suatu seni dimana sebuah data diamankan melalui proses penyandian. Pada permulaannya kriptografi digunakan untuk mengamankan sebuah data berupa teks. Bermacam-macam algoritma yang digunakan dalam mengamankan sebuah data diantaranya adalah DES, RC5, IDEA, RSA dan masih banyak lagi algoritma kriptografi lainnya. Pada proses pembuatan tugas akhir ini data yang akan diamankan adalah berupa data gambar yang berekstensi bitmap.

Data gambar merupakan data yang dapat digolongkan sebagai data pribadi. Salah satu cara mengamankan data gambar adalah dengan algoritma kriptografi. Pada tugas akhir ini algoritma kriptografi yang dipakai adalah algoritma RSA. Pengamanan data gambar dengan kriptografi memiliki perbedaan yang dapat menjadikan kesulitan tersendiri. Dengan adanya permasalahan tersebut maka dalam tugas akhir ini dilakukan pengujian pengamanan data gambar dengan algoritma RSA.

1.2. Rumusan Masalah

Keamanan dalam berkomunikasi adalah salah satu aspek terpenting dari kehidupan bersosialisasi. Seseorang memberikan informasi hanya kepada pihak yang berhak menerima informasi tersebut. Penyandian pada data yang akan ditujukan dapat memberikan kemananan terhadap data. Adapun rumusan masalah yang akan dibahas pada penulisan tugas Akhir ini adalah:

a. Bagaimana menyandikan data gambar menggunakan algoritma RSA?

b. Apakah data gambar setelah proses dekripsi mengalami perubahan yang signifikan?

1.3. Batasan Masalah

Dengan adanya keterbatasan yang dimiliki oleh penulis maka sistem ini dibuat memiliki keterbatasan, diantaranya:

a. Program ini berbasis desktop

b. Program ini menggunakan algoritma RSA dalam proses penyandian data gambar

c. Pembuatan program menggunakan bahasa Delphi

d. Pada Proses Pembuatan Kunci nilai dari *p* dan *q* terdapat pada *range* 1-100.

1.4. Tujuan Penelitian

Tujuan dari Tugas Akhir ini adalah untuk menghasilkan sebuah program berbasis desktop yang berfungsi untuk menyandikan data gambar.

1.5. Metodologi Penelitian

Metodologi penelitian yang digunakan dalam menyelesaikan Tugas Akhir ini adalah:

1. Studi Pustaka dengan membaca dan mengumpulkan in*form*asi dan pengetahuan tambahan mengenai Krptografi, Algoritma RSA, Pemrograman Bahasa Delphi dan pengetahuan lainnya.
2. Perancangan, pembuatan, dan pengujian program.

1.6. Sistematika Penulisan

Sistematika penulisan pada tugas akhir ini terdiri dari beberapa bagian utama sebagai berikut:

Bab 1 yang berjudul. *Pendahuluan*, berisi tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, metodologi penelitian, serta sistematika penulisan.

Bab 2. *Landasan Teori*, berisi tentang teori-teori yang menjadi landasan dalam penulisan tugas akhir yaitu kriptografi dan algoritma RSA.

Bab 3 yang berjudul *Perancangan Sistem* berisi mengenai perancangan *form* sistem, diagram alur sistem, perancangan program penyandian citra menggunakan algoritma RSA dengan bahasa pemrograman Delphi 7 yang implementasinya akan dibahas pada bab selanjutnya.

Bab 4 yang berjudul *Implementasi dan Analisis Sistem*.

Bab 5 yang berjudul *Kesimpulan dan Saran* berisi tentang kesimpulan dan saran dari keseluruhan proses pembuatan tugas akhir dan harapan untuk pengembangan program dikemudian hari.

BAB V
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Sistem yang telah dibuat dapat melakukan penyandian terhadap citra. Sistem yang telah dibangun dapat mengimplementasikan metode kriptografi RSA pada proses penyandian citra dan pembuatan kunci.

Dari hasil penelitian dan analisis yang telah dilakukan, keberhasilan pengembalian citra hasil dekripsi bersifat *lossless* jika nilai dari *p* dan *q* bernilai lebih besar dari 20. Percobaan penyandian citra yang sama dengan ragam kunci penyandi yang berbeda tetap menghasilkan hasil dekripsi yang bersifat *lossless*.

5.2. Saran

Penelitian tentang penyandian citra dapat dilakukan dengan berbagai macam metode kriptografi. Penelitian lebih lanjut tentang pemilihan kunci atau pembuatan kunci umum dan rahasia menjadi hal yang sangat perlu diteliti lebih lagi. Sistem dapat dikembangkan menjadi 2 *form* yang berbeda yakni *form* enkripsi atau pengirim dan *form* dekripsi atau penerima untuk mempermudah *user* memilih fungsi dari sistem.

DAFTAR PUSTAKA

Ali Bani Younes, Mohammad. Jantan, Aman. .(2008) . *IJCSNS International Journal of Computer Science and Network Security*

Gitaprabowo, Jonata. (1996) . Tugas Akhir: *Penerapan Encryption-Decryption dengan Algoritma ESA pada File Text*, UKDW

Hutapea, Bonggas. (2001). Tugas Akhir*: Penyandian Citra dengan metode Subtitusi dan Transposisi*. UKDW

Martina, Inge. (2004). *36 jam belajar komputer Pemrograman Visual Borland Delphi 7*

Menezes, Alfred J. Paul C. van Ourschot. Vanstone, Scott A. (1965). *Handbook of applied cryptography*

Tahun, Marthen. (1999) . Tugas Akhir*: Electronic Signature dengan Metode RSA*, UKDW

Violina, Sriyani. Junaedi, Danang. (2007). Materi perkuliahan: *Format Bitmap*

Yoenanto, Chahyo. (2007) .Tugas Akhir*: Implementasi Algoritma Kriptografi RSA pada data Text dengan private Key dienkripsi dengan Algoritma Kriptografi RC-5*. UKDW

Yusuf, Kurniawan.(2004). *Kriptografi: Keamanan internet dan jaringan komunikasi*