SISTEM PENGAMANAN PESAN DENGAN METODE KRIPTOGRAFI RSA-CRT DAN METODE STEGANOGRAFI *LINEAR CONGRUENTIAL GENERATOR* PADA MEDIA CITRA DIGITAL

Diajukan Sebagai Syarat Untuk Menyelesaikan
Pendidikan Program Strata-1 Pada
Jurusan Teknik Informatika

Oleh:

M.Farid Landriandani
09021181621012

JURUSAN TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2020

LEMBAR PENGESAHAN TUGAS AKHIR

SISTEM PENGAMANAN PESAN DENGAN METODE KRIPTOGRAFI RSA- CRT DAN METODE STEGANOGRAFI LINEAR CONGRUENTIAL GENERATOR PADA MEDIA CITRA DIGITAL

Oleh :

MUHAMMAD FARID LANDRIANDANI
NIM : 09021181621012

Palembang, 19 Desember 2020

Pembimbing I

Drs. Megah Mulya, M.T.
NIP. 196602202006041001

Pembimbing II,

Kanda Januar Miraswan, M.T.
NIP. 199001092019031012

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

TANDA LULUS UJIAN SIDANG TUGAS AKHIR

Pada hari Selasa tanggal 15 Desember 2020 telah dilaksanakan ujian sidang tugas akhir oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : M. Farid Landriandani
NIM : 09021181621012
Judul : Sistem Pengamanan Pesan dengan Metode Kriptografi RSA- CRT dan Metode Steganografi *Linear Congruential Generator* Pada Media Citra Digital

1. Pembimbing I

   Drs. Megah Mulya, M.T .....
   NIP. 196602202006041001

2. Pembimbing II

   Kanda Januar Miraswan, M.T. .....
   NIP. 199001092019031012

3. Penguji I

   Alvi Syahrini Utami, M.Kom .....
   NIP. 197812222006042003

4. Penguji II

   Danny Matthew Saputram, M.Sc. .....
   NIP. 198505102015041002

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom
NIP. 197812222006042003

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	:	M. Farid Landriandani
NIM	:	09021181621012
Program Studi	:	Teknik Informatika
Judul Skripsi	:	Sistem Pengamanan Pesan dengan Metode Kriptografi RSA-CRT dan Metode Steganografi *Linear Congruential Generator* Pada Media Citra Digital.

Hasil Pengecekan Software *iThenticate/Turnitin* : 14%

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, Desember 2020

M. Farid Landriandani
NIM. 09021181621012

MOTTO DAN PERSEMBAHAN

MOTTO:

“I Must Endure”

-Omen, Valorant –

" Jika Anda tidak bisa membuat sesuatu menjadi baik, paling tidak buatlah hal itu terlihat baik."

- Bill Gates -

Kupersembahkan Karya Tulis ini kepada:

- **Keluargaku tercinta**
- **Orang-orang tersayangku**
- **Sahabat-sahabatku**
- **Fakultas Ilmu Komputer, Universitas Sriwijaya**

Message Security System with the RSA-CRT Cryptography Method and the Linear Congruential Generator Steganography Method on Digital Media Image

By :
M.Farid Landriandani
NIM : 09021181621012

ABSTRACT

Data security is an important aspect in the process of sending messages, especially for messages that are confidential. There are many methods in protecting data security in cryptography, so the RSA cryptography technique is chosen. This algorithm performs factoring of very large numbers, therefore RSA is considered safe to generate two keys, two large random prime numbers are selected. This study aims to develop software and test whether the process of adding CRT (Chinese Remainder Theorem) to the RSA cryptographic algorithm affects 3 aspects of testing when combined with LSB random steganography techniques. This study used 10 images with a resolution of 256 x 256 and text data consisting of ASCII characters stored in TXT format with a total of 10 - 50 words. The data is used in accordance with the provisions based on 3 aspects of testing. In this research, a prototype software has been made to apply the comparison between the RSA and RSA-CRT algorithms. From the results of tests that have been done with 3 aspects of testing, the use of the CRT theorem in the RSA algorithm only affects the decryption process, and there is no effect on the encryption process.

Keyword : Cryptography, LCG, RSA, RSA-CRT, Random LSB, Steganography

Palembang, 19 Desember 2020

Pembimbing I

Drs. Megah Mulya, M.T.
NIP. 196602202006041001

Pembimbing II,

Kanda Januar Miraswan, M.T.
NIP. 199001092019031012

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

Sistem Pengamanan Pesan dengan Metode Kriptografi RSA-CRT dan Metode Steganografi Linear Congruential Generator Pada Media Citra Digital

Oleh :
M.Farid Landriandani
NIM : 09021181621012

ABSTRAK

Keamanan data merupakan aspek penting dalam sebuah proses pengiriman pesan terutama untuk pesan yang bersifat rahasia. Banyaknya metode dalam melindungi keamanan data pada kriptografi, maka dipilihla teknik kriptografi RSA. Algoritma ini melakukan pemfaktoran bilangan yang sangat besar, oleh karena itu RSA dianggap aman untuk membangkitkan dua kunci, dipilih dua bilangan prima acak yang besar. Penelitian ini bertujuan untuk mengembangkan perangkat lunak dan menguji apakah proses dari penambahan CRT (*Chinese Remainder Theorem*) pada Algoritma kriptografi RSA mempengaruhi 3 aspek pengujian saat dikombinasikan dengan teknik steganografi *random* LSB. Penelitian ini menggunakan data sebanyak 10 citra dengan resolusi 256 x 256 serta data teks yang terdiri dari karakter ASCII yang disimpan dalam format TXT dengan jumlah 10 – 50 jumlah kata. Data tersebut dipakai sesuai dengan ketentuan berdasarkan 3 aspek pengujian. Pada penelitian telah dibuat perangkat lunak prototype untuk menerapkan perbandingan antara algoritma RSA dan RSA-CRT. Dari hasil pengujian yang telah dilakukan dengan 3 aspek pengujian, penggunaan teorema CRT dalam algoritma RSA hanya berpengaruh pada proses dekripsi, dan tidak ada pengaruh pada proses enkripsi.

Kata Kunci : Kriptografi, LCG, RSA, RSA-CRT, *Random* LSB, Steganografi

Palembang, 19 Desember 2020

Pembimbing I

Drs. Megah Mulya, M.T.
NIP. 196602202006041001

Pembimbing II,

Kanda Januar Miraswan, M.T.
NIP. 199001092019031012

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

KATA PENGANTAR

Puji syukur kepada Allah SWT atas berkat dan rahmat-Nya yang telah melimpahkan rahmat dan karunianya kepada Penulis sehingga mampu menyelesaikan Tugas Akhir ini dengan baik. Tugas akhir ini disusun untuk memenuhi salah satu syarat untuk menyelesaikan Pendidikan program Strata-1 pada Fakultas Ilmu Komputer Program Studi Teknik Informatika di Universitas Sriwijaya.

Dalam menyelesaikan Tugas Akhir ini, banyak pihak yang telah memberikan bantuan dan dukungan baik secara langsung maupun tidak langsung. Oleh karena itu, penulis ingin menyampaikan rasa terima kasih kepada:

1. Orang tuaku, Lendi Ansyori dan Msy. Farida Aryani yang jasanya tiada tara dan tak akan dapat tergantikan. Kakak perempuanku Serli Fatriandini, Dina Ayu Mardianti dan Indah Revika Sari, Adik laki-lakiku Iqbal Reza Riandani, serta seluruh keluarga besarku yang selalu mendoakan, menghibur, serta memberikan dukungan baik secara moril maupun materil.
2. Civitas Akademika Fakultas Ilmu Komputer Universitas Sriwijaya yang telah memberikan ilmu, serta membimbing jalan penulis dalam menghadapi perkuliahan.
3. Pembimbing Tugas Akhir, Bapak Drs Megah Mulya, M.T. dan Bapak Kanda Januar Miraswan, M.T. yang telah membimbing penulis dengan sabar dan semangat.

4. Penguji Tugas Akhir, Bapak Samsuryadi, M.Kom., Ph.D. , Ibu Alvi Syahrini Utami, M.Kom dan Bapak Danny Matthew Saputra, M.Sc. yang senantiasa memberikan masukan kepada penulis mengenai tugas akhir dan pengalaman kerja.
5. Pembimbing Akademik, Rifkie Primartha, M.T. yang telah banyak memberikan masukan kepada penulis mengenai perkuliahan.
6. Anggi Tri Rizki Ramadhani dan Satriadinata yang telah selalu ada serta menemani setiap hari dan perjuangan tugas akhir bersama penulis.
7. Teman-teman perjuangan Tugas Akhir sekaligus teman setiaku Alep, Herlan, Dika, Dedes, Dina, Irfan, Fadli, Luthfi, Ryadh, Daniel, Dendi serta seluruh anggota kelas Inforgen yang setia bersama penulis dalam perjuangan mengerjakan tugas akhir,

Penulis menyadari dalam penyusunan Tugas Akhir ini masih terdapat banyak kekurangan, oleh karena itu kritik dan saran yang membangun sangat diharapkan untuk kemajuan penelitian selanjutnya. Akhir kata semoga Tugas Akhir ini dapat digunakan sebaik-baiknya serta bermanfaat bagi kita semua.

Palembang, Desember 2020

Penulis

M. Farid Landriandani

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Pendahuluan

Pada bab ini dibahas mengenai latar belakang masalah, rumusan masalah, tujuan dan manfaat penelitian serta batasan masalah. Bab ini akan memberikan penjelasan umum mengenai keseluruhan penelitian.

1.2 Latar Belakang

Keamanan data merupakan aspek penting dalam sebuah proses pengiriman pesan terutama untuk pesan yang bersifat rahasia. Dalam aktivitas sehari-hari penggunaan internet sudah menjadi hal yang biasa saja, salah satu penggunaan internet yaitu pengiriman sebuah pesan misalnya berkomunikasi lewat media sosial, mengirimkan *e-mail*, dan jual beli secara *online*. Untuk itu diperlukan suatu sandi agar pesan tersebut dapat terjaga kerahasiaan dan keamaannya, karena keamanan data yang berada pada jaringan publik rentan terhadap serangan oleh siapapun. Layanan keamanan data diwujudkan dengan menggunakan mekanisme keamanan data. Mekanisme keamanan data pada implementasinya menggunakan teknik-teknik penyandian, yaitu kriptografi.

Banyaknya metode dalam melindungi keamanan data pada kriptografi, maka dipilihla teknik kriptografi RSA. Algoritma ini melakukan pemfaktoran bilangan yang sangat besar, oleh karena itu RSA dianggap aman untuk membangkitkan dua kunci, dipilih dua bilangan prima acak yang besar. Sistem Kriptografi RSA dapat dimodifikasi dengan menggunakan teorema *Chinese Remainder Theorem* (CRT) disebut dengan RSA-CRT. Pada dasarnya RSA-CRT

sama dengan RSA biasa namun memanfaatkan teorema CRT untuk memperpendek ukuran bit dan terbukti sistem kriptografi RSA-CRT memiliki waktu komputasi yang lebih singkat daripada sistem kriptografi RSA biasa yaitu sekitar 4 kali lebih cepat (Nasution, 2017).

Pada penelitian terkait yang menjadi rujukan utama penelitian ini, digunakan salah satu teknik yang paling efektif dalam teknik pengamanan pesan yaitu kombinasi algoritma kriptografi RSA dan steganografi LSB yang menghasilkan sistem paling aman dan kuat. Data yang disembunyikan dalam penelitian ini adalah *file* audio, dan fokus utamanya adalah mengatasi kecepatan yang lambat saat proses dekripsi pada algoritma RSA dengan menggunakan teknik RSA-CRT. Hasilnya disebutkan penambahan RSA-CRT membuat proses dekripsi menjadi lebih cepat dengan ditinjau dari waktu komputasi algoritma (Abdulameer *et al.*, 2015). Namun disisi lain penelitian penambahan CRT pada algoritma RSA menyebutkan bahwa RSA-CRT lebih banyak membutuhkan *resource memory* dibandingkan dengan RSA ketika panjang kunci lebih besar dari 2048. Hal ini dikarenakan penggunaan lebih banyak variabel pada operasi teorema CRT, oleh karena itu pemanfaatan memori oleh RSA-CRT lebih besar daripada RSA (Mantri *et al.*, 2016).

Penelitian tersebut menjadi dasar dari penelitian ini dimana akan dibandingkan algoritma RSA biasa dengan algoritma RSA yang sudah ditambahkan CRT kemudian akan dikombinasikan dengan algoritma steganografi LSB menggunakan *Linier Congruential Generator*, bedanya pada penelitian ini data yang dipakai pada proses steganografi adalah citra digital. Dengan dilakukannya

penelitian ini pengguna akan mendapatkan hasil uji dari 3 aspek yaitu aspek mutu citra steganografi yang meliputi nilai *Mean Square Error* (MSE), dan *Peak Signal to Noise Ratio* (PSNR), aspek kecepatan komputasi melalui analisis algoritma serta *access time* dari proses enkripsi dan dekripsi, dan aspek performansi kriptografi dalam keamanan pesan meliputi pengukuran *Avalanche Effect*, diharapkan dari hasil uji tersebut dapat dilakukannya pembuktian apakah proses dari penambahan CRT (*Chinese Remainder Theorem*) pada algoritma kriptografi RSA mempengaruhi 3 aspek tersebut secara signifikan.

1.3 Rumusan Masalah

Fokus permasalahan pada penelitian ini adalah apakah proses dari penambahan CRT (*Chinese Remainder Theorem*) pada Algoritma kriptografi RSA mempengaruhi 3 aspek pengujian saat dikombinasikan dengan teknik steganografi *random* LSB. Dari permasalahan tersebut selanjutnya dirumuskan pertanyaan penelitian sebagai berikut:

1. Bagaimana pengaruh dari penambahan CRT (*Chinese Remainder Theorem*) pada algoritma kriptografi RSA terhadap *Fidelity* atau mutu citra penampung setelah ditambahkan pesan saat dikombinasikan dengan teknik steganografi *random* LSB berdasarkan pengukuran nilai *Mean Square Error* (MSE), dan *Peak Signal to Noise Ratio* (PSNR) yang dihasilkan?
2. Bagaimana pengaruh dari penambahan CRT (*Chinese Remainder Theorem*) pada algoritma kriptografi RSA terhadap kecepatan komputasi melalui analisis algoritma serta *access time* dari proses enkripsi dan dekripsi?

3. Bagaimana pengaruh dari penambahan CRT (*Chinese Remainder Theorem*) pada algoritma kriptografi RSA terhadap performansi kriptografi dalam keamanan pesan meliputi pengukuran *Avalanche Effect?*

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengembangkan perangkat lunak yang mengimplementasikan penggabungan algoritma RSA-CRT dan teknik steganografi *Random* LSB: *Linear Congruential Generator*;
2. Melakukan perhitungan terhadap 3 aspek pengujian, yaitu aspek mutu citra steganografi yang meliputi nilai *Mean Square Error* (MSE), dan *Peak Signal to Noise Ratio* (PSNR), aspek kecepatan komputasi melalui analisis algoritma serta *access time* dari proses enkripsi dan dekripsi, dan aspek performansi kriptografi dalam keamanan pesan meliputi pengukuran *Avalanche Effect* sehingga dapat diketahui pengaruh dari penambahan CRT (*Chinese Remainder Theorem*) pada Algoritma kriptografi RSA saat dikombinasikan dengan teknik steganografi *random* LSB.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini sebagai berikut :

1. Menghasilkan perangkat lunak yang dapat mengimplementasikan penggabungan Algoritma RSA-CRT dan Teknik Steganografi *Random* LSB: *Linear Congruential Generator*;
2. Mempersulit orang yang tidak bertanggung jawab dalam mengambil data pada saat pengiriman dari pengirim ke penerima pesan yang

diimplementasikan dalam penggabungan Algoritma RSA-CRT dan Teknik Steganografi *Random* LSB: *Linear Congruential Generator*;

3. Mengetahui apakah proses dari penambahan CRT (*Chinese Remainder Theorem*) pada Algoritma kriptografi RSA saat dikombinasikan dengan teknik steganografi *random* LSB mempengaruhi terhadap 3 aspek pengujian, yaitu aspek mutu citra steganografi yang meliputi nilai *Mean Square Error* (MSE), dan *Peak Signal to Noise Ratio* (PSNR), aspek kecepatan komputasi melalui analisis algoritma serta *access time* dari proses enkripsi dan dekripsi, dan aspek performansi kriptografi dalam keamanan pesan meliputi pengukuran *Avalanche Effect.*

1.6 Batasan Masalah

Adapun batasan masalah yang diberikan pada penelitian ini adalah sebagai berikut:

1. Pesan yang diamankan dimuat dalam file teks berekstensi (.txt).
2. Tidak mencakup aspek keamanan pada proses pengiriman *stego image* dan kunci.
3. Pesan yang menjadi *plaintext* mempunyai panjang maksimal 5616 bit.

1.7 Sistematika Penulisan

Sistematika penulisan tugas akhir ini mengikuti standar penulisan tugas akhir Fakultas Ilmu Komputer Universitas Sriwijaya yaitu sebagai berikut.:

BAB I. PENDAHULUAN

Pada bab ini akan diuraikan mengenai latar belakang, perumusan masalah, tujuan dan manfaat penelitian, Batasan

masalah/ruang lingkup, metodologi penelitian dan sistemarika penulisan.

BAB II. KAJIAN LITERATUR

Pada bab ini akan membahas seluruh dasar-dasar teori yang digunakan mulai dari definisi sistem, informasi mengenai domain, dan semua yang digunakan pada tahapan analisis, perancangan, dan implementasi.

BAB III. METODELOGI PENELITIAN

Pada bab ini akan membahas mengenai tahap-tahap yang akan diterapkan pada penelitian. Setiap rencana dari tahapan penelitian dideskripsikan secara rinci berdasarkan kerangka kerja. Dilanjutkan dengan perancangan manajemen proyek dalam pelaksanaan penelitian.

1.8 Kesimpulan

Dari pendahuluan ini, telah dijelaskan secara umum mengenai penelitian yang akan dilakukan, meliputi latar belakang, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah serta sistematika penulisan.

DAFTAR PUSTAKA

A.Abdullah, H., A. Abdulameer, A. & F. Hussein, I. 2015. Audio Steganography and Security by using Cryptography. i-manager's Journal on Information Technology, 4(4): 17–24.

Ahmed Laskar, S. 2012. High Capacity data hiding using LSB Steganography and Encryption. International Journal of Database Management Systems, 4(6): 57–68.

Arief, A. 2016. Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging. 3(1): 46–54.

Gonzalez, R.C., Woods, R.E. & Masters, B.R. 2007. Digital Image Processing, Third Edition. (December): 976.

Kroll, P. & Kruchten, P. 2003. The Rational Unified Process Made Easy. Rational Unified Process Made Easy: A Practitioner's Guide to the RUP.

Lubis, A.A., Wong, N.P., Arfiandi, I., Damanik, V.I. & Maulana, A. 2015. Steganografi pada Citra dengan Metode MLSB dan Enkripsi Triple Transposition Vigenere Cipher. Steganografi pada Citra dengan Metode MLSB dan Enkripsi Triple Transposition Vigenere Cipher, 16(2): 125–134.

Mandal, J.K. & Das, D. 2012. Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain. IERI Procedia, 2(4): 17–24.

Mantri, A., Razaque, A., Makwana, H., Parekh, P. & Soomro, T.R. 2016. Analytical Comparison of RSA and RSA with Chinese Remainder Theorem. Journal of Independent Studies and Research - Computing, 14(1).

Menezes, A., Van, O. & Vanstones 1996. Handbook of Applied Cryptography. New York : CRC Press.

Morkel, T., Eloff, J.H.P. & Olivier, M.S. 2005. An Overview of Image Steganography. Information and Computer Security Architecture (ICSA) Research Group, 83(July): 51–107.

Mulawarman, J.I., Pabokory, F.N., Astuti, I.F., Kridalaksana, A.H., Studi, P., Komputer, I., Mulawarman, U., Teks, P. & Dokumen, I.F. 2015. IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA PADA PESAN TEKS , ISI FILE DOKUMEN , DAN FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION. 10(1).

Munir, R. 2019. Kriptografi. *2*. Informatika Bandung, hal.645.

Nasution, N.R. 2017. Kombinasi RSA-CRT dengan Random LSB untuk Keamanan Data. 5341(April): 32–42.

Pangaribuan, L.J. & Simbolon, F.H. 2017. Kriptografi Hybrida Menggunakan

Algoritma Hill Cipher Dan. I: 1–11.

Pusparani, N.A. 2009. Analisis RSA dengan Penambahan Chinese Remainder Theorem Untuk Mempercepat Proses Dekripsi.

Raju & Mohit 2015. An Improved LSB based Image Steganography for Grayscale and Color Images. International Journal of Current Engineering and Technology, 5(5): 22774106.

Sardju, E.R., Magdalena, R. & Atmaja, R.D. 2015. Implementasi Algoritma Rsa Untuk Enkripsi Dan Dekripsi Sms (short Message Service) Pada Ponsel Berbasis Android. eProceedings of Engineering, 2(2): 2435–2442.

Yovita, L.V. 2015. Perancangan Sistem Pengamanan Dan Otentikasi Pengiriman System Design of Security and Authentication Delivery Message. 2(1): 9–24.