

**IMPLEMENTASI ALGORITMA ELGAMAL UNTUK
ENKRIPSI DAN DEKRIPSI PADA FILE CITRA**

Skripsi



oleh
IGNATIUS ADHITYA PURNOMO
22104880

**PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2015**

IMPLEMENTASI ALGORITMA ELGAMAL UNTUK ENKRIPSI DAN DEKRIPSI PADA FILE CITRA

Skripsi



Diajukan kepada Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh

IGNATIUS ADHITYA PURNOMO
22104880

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2015

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

IMPLEMENTASI ALGORITMA ELGAMAL UNTUK ENKRIPSI DAN DEKRIPSI PADA FILE CITRA

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 sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 15 Desember 2014



IGNATIUS ADHITYA PURNOMO
22104880

HALAMAN PERSETUJUAN

Judul Skripsi : IMPLEMENTASI ALGORITMA ELGAMAL
UNTUK ENKRIPSI DAN DEKRIPSI PADA FILE
CITRA

Nama Mahasiswa : IGNATIUS ADHITYA PURNOMO

N I M : 22104880

Matakuliah : Skripsi (Tugas Akhir)

Kode : TIW276

Semester : Gasal

Tahun Akademik : 2014/2015

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 15 Desember 2014

acc pendadaran

Dosen Pembimbing I


Jurius Karel, M.T.

Dosen Pembimbing II


Kristian Adi Nugraha, S.Kom., M.T.

HALAMAN PENGESAHAN

**IMPLEMENTASI ALGORITMA ELGAMAL UNTUK ENKRIPSI DAN
DEKRIPSI PADA FILE CITRA**

Oleh: IGNATIUS ADHITYA PURNOMO / 22104880

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal 7 Januari 2015


Yogyakarta, 14 Januari 2015
Mengesahkan,

Dewan Penguji:

1. Junius Karel, M.T.
2. Kristian Adi Nugraha, S.Kom., M.T.
3. Nugroho Agus Haryono, M.Si
4. R. Gunawan Santosa, Drx. M.Si.

Dekan

Ketua Program Studi


(Budi Susanto, S.Kom., M.T.)


(Gloria Virginia, Ph.D.)

KATA PENGANTAR

Pertama – tama, puji dan syukur penulis ucapkan kepada Tuhan Yang Maha Esa, yang karena rahmat dan karunianya, penulis dapat menyelesaikan tugas akhir ini dengan baik dan tepat waktu. Ucapan syukur ini tidak lepas dari segala penyertaannya dalam menyertai penulis dalam setiap langkah yang harus ditempuh untuk menyelesaikan tugas akhir ini. Pada akhirnya, penulis dengan syukur dan bangga dapat mempersembahkan tugas akhir dengan judul “Implementasi Algoritma ElGamal untuk Enkripsi dan Dekripsi pada *File Citra*” ini ke dalam kemuliannya yang lebih besar.

Tugas akhir ini merupakan salah satu persyaratan untuk mendapatkan gelar Strata 1 dalam Program Studi Teknik Informatika pada Universitas Kristen Duta Wacana, yaitu gelar Sarjana Komputer. Mata kuliah ini merupakan mata kuliah wajib dengan bobot yang lumayan besar, yang menurut penulis dapat memberi manfaat sekaligus dorongan untuk terus belajar hal baru, karena penelitian pada tugas akhir ini merupakan hal yang baru bagi penulis.

Terlepas dari segala suka dan duka pada saat penulisan tugas akhir ini, tentu penulis tidak lupa mengucapkan terima kasih yang sebesar-besarnya kepada para pribadi maupun kelompok yang telah membantu penulis baik secara teknis maupun semangat dalam menyelesaikan tugas akhir ini:

1. Bapak Junius Karel, M.T. dan Bapak Kristian Adi Nugraha, S. Kom., M.T. selaku dosen pembimbing yang dengan baik hati selalu membantu untuk setiap permasalahan dalam penulisan tugas akhir ini.
2. Kepada bapak dan ibu penulis yang mulai dari penulis lahir sampai dengan saat ini, selalu menemani dan memberi pelajaran yang paling berharga dalam hidup penulis, yang besar kasihnya tidak akan bisa disetarakan oleh banyaknya kalimat pada tugas akhir ini.
3. Kepada kedua adik penulis yang setiap saat memberi semangat dengan cara mereka sendiri, dengan menjadi dorongan untuk tidak mau kalah dari mereka, dan keinginan untuk selalu menjadi motivasi untuk mereka.
4. Teman-teman penghuni DWTC, dimana menyelesaikan tugas akhir disana terasa menyenangkan, dan juga kepada Bapak Abet selaku dosen di DWTC, yang pada bagian akhir memberi saran dan banyak membantu penulis.

5. Teman-teman Duta Wacana Photographie Club, organisasi yang selama empat tahun ini menjadi tempat yang nyaman untuk penulis, tempat untuk belajar hal-hal di luar kegiatan akademis, tempat untuk belajar *soft-skill* yang sangat penulis rasakan manfaatnya.
6. Teman-teman *Yogyakarta Kampoeng Field School*, yang memberi pengalaman baru dalam dunia kemasyarakatan, sekaligus bersosialisasi dengan budaya dan kultur baru.
7. Kepada Bapak Taher ElGamal - meskipun penulis belum pernah berjumpa dengan beliau, seseorang yang sudah memberi inspirasi dan menciptakan algoritmanya untuk akhirnya penulis dapat menyelesaikan tugas akhir ini dengan lancar dan baik.

Pada akhirnya, penulis berharap agar segala hal yang penulis teliti di dalam tugas akhir ini dapat menjadi manfaat bagi orang lain dan bagi penulis sendiri. Semoga tugas akhir ini dapat menjadi referensi ilmiah untuk penelitian masalah keamanan komputer, khususnya untuk peneliti yang mempelajari algoritma ElGamal.

Yogyakarta, 16 Desember 2014

Ignatius Adhitya Purnomo

Abstrak

Kemajuan pada dunia teknologi saat ini mempunyai keuntungan dan kerugian. Salah satu keuntungannya adalah kemudahan bagi pengguna untuk mengakses informasi yang ada pada dunia ini. Pengaksesan data yang saat ini dirasa semakin mudah, menyebabkan banyak orang untuk mulai mencoba mengakses data yang bukan miliknya. Informasi yang mengandung nilai penting seperti citra digital contohnya, dapat dimanfaatkan untuk hal negatif bila jatuh ke tangan orang yang salah.

Tulisan dalam penelitian ini bertujuan untuk mengamankan informasi tersebut, khususnya informasi dalam citra digital. Algoritma ElGamal digunakan untuk melindungi informasi yang terkandung pada citra, sehingga pada akhirnya, hanya pengirim dan penerima pesan saja yang bisa mengakses informasi tersebut.

Keseluruhan sistem dapat dengan baik melakukan enkripsi dan dekripsi pada citra, citra hasil enkripsi menjadi acak dan tidak jelas, sedangkan citra hasil dekripsi dapat kembali ke citra awal dengan kemiripan yang mendekati sempurna. Tetapi tentu saja, sistem ini perlu dikembangkan untuk penelitian yang lebih lanjut.

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN SAMPUL DALAM	ii
PERNYATAAN KEASLIAN SKRIPSI.....	iii
HALAMAN PERSETUJUAN.....	iv
HALAMAN PENGESAHAN	v
KATA PENGANTAR	vii
ABSTRAK.....	ix
BAB 1	1
PENDAHULUAN	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	3
1.5 Metodologi Penelitian	3
1.5.1 Studi pustaka dan literatur	3
1.5.2 Perancangan sistem.....	3
1.5.3 Pembangunan sistem.....	3
1.5.4 Pengujian dan Analisis.....	4
1.6 Sistematika Penulisan.....	4
BAB 2	6
TINJAUAN PUSTAKA	6
2.1 Tinjauan Pustaka	6
2.2 Landasan Teori.....	9
2.2.1 Kriptografi.....	10

2.2.2	Citra Digital	10
2.2.3	Kriptografi Asimetris	13
2.2.4	Algoritma ElGamal	13
2.2.5	MSE (Mean Square Error)	15
BAB 3		17
ANALISIS DAN PERANCANGAN SISTEM		17
3.1	Analisis Kebutuhan	17
3.1.1	Analisis Data	17
3.1.2	Analisis Kebutuhan Perangkat Lunak	18
3.1.3	Analisis Kebutuhan Perangkat Keras	18
3.2	Rancangan Sistem	18
3.2.1	Use Case	18
3.2.2	Diagram Alir (<i>Flowchart</i>)	20
3.2.3	Perancangan Antarmuka Sistem	28
BAB 4		33
IMPLEMENTASI DAN ANALISIS SISTEM		33
4.1	Implementasi Sistem	33
4.1.1	Antarmuka Program	33
4.1.2	Implementasi <i>Input</i> dan <i>Output</i> Sistem	37
4.2	Analisis Sistem	44
4.2.1	Analisis Pengaruh Luas dan Jenis Citra Terhadap Kecepatan Enkripsi dan Dekripsi	44
4.2.2	Analisis Pengaruh Luas dan Jenis Citra Terhadap Ukuran <i>File</i> Citra Setelah Enkripsi dan Dekripsi	48
4.2.3	Analisis Pengaruh Jenis Citra Terhadap Besar Kecilnya Nilai MSE pada Citra Awal dan Citra Setelah Dekripsi	52
4.3	Analisis Implementasi Algoritma ElGamal untuk Enkripsi dan Dekripsi pada Citra	55

BAB 5	57
KESIMPULAN DAN SARAN.....	57
5.1 Kesimpulan.....	57
5.2 Saran.....	58
DAFTAR PUSTAKA	59

©UKDW

Gambar 2.1 Perbandingan <i>Ciphertext</i> yang Dihasilkan dengan Variabel k yang Berbeda	6
Gambar 2.2 <i>Plaintext</i> Citra	8
Gambar 2.3 Hasil Enkripsi, Kunci <i>Share a</i>	8
Gambar 2. 4 Hasil Enkripsi, Kunci <i>Share b</i>	9
Gambar 2.5 Alur Enkripsi dan Dekripsi	10
Gambar 2.6 Perbedaan Tingkat Keabuan	11
Gambar 2.7 Representasi CMYK dan RGB	12
Gambar 3.1 <i>Usecase</i> Sistem	19
Gambar 3.2 <i>Flowchart</i> Sistem	21
Gambar 3.3 <i>Flowchart Generate Key</i>	23
Gambar 3.4 <i>Flowchart</i> Enkripsi	25
Gambar 3.5 <i>Flowchart</i> Dekripsi	28
<i>Gambar 3.6</i> Tampilan Awal Sistem	29
<i>Gambar 3.7</i> Tampilan <i>Form</i> Dekripsi Citra	31
<i>Gambar 3.8</i> Tampilan <i>Form</i> Komparasi Citra	32

BAB 1

PENDAHULUAN

1.1 Latar Belakang Masalah

Pada buku *Applied Cryptography* karya Bruce Schneier, beliau memberikan pengantar berupa analogi tentang keamanan sebagai berikut: Jika saya mengambil surat, menguncinya dalam sebuah brankas, dan menyembunyikan brankas itu di suatu tempat di New York dan menyuruh anda untuk membaca surat itu, maka hal itu bukan keamanan, melainkan ketidakjelasan. Di sisi lain, jika saya menyimpan surat itu dalam sebuah brankas, dan memberikan kepada anda brankas tersebut beserta spesifikasi desain dan ratusan brankas serupa dengan kombinasi kuncinya masing-masing, sehingga anda dan para ahli pembuka brankas dapat mempelajari mekanisme kunci brankas tersebut, tetapi anda tetap tidak dapat membuka brankas tersebut dan membaca surat itu, inilah yang disebut dengan keamanan. (Schneier, 1996).

Keamanan dalam bidang teknologi informasi, dibahas lebih lanjut dalam kriptografi. Kriptografi adalah bidang studi dari *cryptosystem* dimana privasi dan autentikasi sebuah data dipastikan dapat terjaga (Rhee, 1994). Dalam kriptografi sendiri, sebuah pesan yang sudah dienkripsi (*ciphertext*) akan mempunyai bentuk yang sangat berbeda dengan pesan aslinya (*plaintext*). Hal inilah yang membuat sebuah data yang akan ditransmisikan sangat aman, karena pihak lain selain pengirim dan penerima yang dimaksud tidak akan mengetahui isi pesan asli tersebut. Contoh kasus dalam dunia nyata yaitu keamanan dalam penyimpanan data ke *cloud storage*. Hal ini akan mencegah adanya *hacker* untuk melihat data yang tidak diinginkan, dengan menyediakan proteksi ganda walaupun *hacker* sudah bisa membobol *password* pengguna.

Pada tugas akhir ini, akan dibuat sebuah aplikasi enkripsi dan dekripsi suatu citra menggunakan algoritma ElGamal. Algoritma ini sebenarnya merupakan algoritma yang biasa digunakan untuk tanda tangan digital (*digital signatures*). Pengertian tanda tangan *digital* di sini bukanlah tanda tangan yang di-dijitasi dengan *scanner*, tetapi suatu nilai kriptografis

yang bergantung pada pesan dan pengirim pesan (Nurhasanah & Sulaiman, 2013). Algoritma ini dipilih karena algoritma ini merupakan salah satu algoritma asimetris yang bekerja dengan baik untuk enkripsi (Schneier, 1996). Selain itu, algoritma ElGamal sendiri mempunyai tingkat keamanan yang tinggi karena cara kerjanya bergantung pada kesulitan dari menghitung logaritma diskrit dalam sebuah *finite field* $GF(p)$ dimana p merupakan bilangan prima (Rhee, 1994).

1.2 Rumusan Masalah

Berdasar latar belakang, maka permasalahan yang diteliti dirumuskan sebagai berikut:

- a. Bagaimana sistem mampu mengaplikasikan algoritma ElGamal untuk proses enkripsi dan dekripsi pada *file* citra?
- b. Bagaimana sistem mampu melakukan pengembalian citra, yaitu mendekripsi hasil enkripsi citra kembali ke bentuk awal sebelum enkripsi?

1.3 Batasan Masalah

Dalam penelitian ini, permasalahan dibatasi sebagai berikut:

- a. Selain melakukan enkripsi dan dekripsi, sistem juga dapat menghitung selisih *error* antara citra awal sebelum enkripsi (*plaintext*) dengan citra setelah dekripsi menggunakan MSE (*Mean Square Error*).
- b. Kunci p , g , y , dan x di *generate* oleh sistem.
- c. Sistem hanya menerima masukan berupa citra, dengan ekstensi standar *.jpg*.
- d. Citra yang dienkripsi dan didekripsi mempunyai kedalaman warna 24 bit, dengan resolusi panjang atau lebar maksimum sebesar 1800 piksel.
- e. Citra sampel yang digunakan untuk penelitian sebanyak 30 buah, merupakan gabungan antara citra berwarna dan citra hitam putih.

1.4 Tujuan Penelitian

Tugas akhir ini bertujuan untuk mengaplikasikan algoritma ElGamal dalam mengenkripsi suatu *file* citra secara efisien dan terjaga kemanannya, dengan tetap memperhatikan proses dekripsi agar citra bisa kembali ke bentuk semula. Penelitian ini juga diharapkan dapat digunakan sebagai salah satu sumber referensi penelitian tentang enkripsi dan dekripsi citra menggunakan algoritma lain.

1.5 Metodologi Penelitian

Proses yang dilakukan pada penelitian ini disusun melalui beberapa tahapan-tahapan yang berbeda satu sama lain, sehingga penelitian menjadi lebih sistematis. Tahapan-tahapan pendekatan pada penelitian ini akan dijabarkan lebih lanjut pada sub-bab berikut.

1.5.1 Studi pustaka dan literatur

Studi pustaka dilakukan dengan mencari dan mempelajari sumber-sumber pustaka yang berkaitan dengan enkripsi dan dekripsi algoritma asimetris, dasar-dasar pengolahan citra, dan algoritma ElGamal itu sendiri.

1.5.2 Perancangan sistem

Tahap ini berisi perancangan antar muka yang akan dibangun beserta dengan perancangan alur bekerja sistem.

1.5.3 Pembangunan sistem

Tahap ini merupakan tahap pembuatan program untuk mengenkripsi dan mendekripsi citra. Pada tahap awal, sistem akan membentuk kunci publik dan kunci privat. Kunci publik tersebut digunakan untuk melakukan skripsi pada citra awal. Setelah selesai mengenkripsi, hasil enkripsi dikirimkan kepada penerima citra. Penerima citra kemudian akan melakukan

deskripsi menggunakan sistem yang sudah dibangun sehingga pesan dapat dikenali oleh si penerima citra.

1.5.4 Pengujian dan Analisis

Tahap ini merupakan tahap pengujian sistem yang telah dibuat dan menganalisis perubahan piksel R , G , dan B pada citra untuk hasil enkripsi dan dekripsi yang dilakukan. Analisis perubahan piksel akan ditampilkan menggunakan perhitungan MSE (*Mean Square Error*). Selain itu, akan dicatat pula waktu yang dibutuhkan untuk proses enkripsi dan dekripsi citra dan perubahan ukuran *file* citra dalam byte.

1.6 Sistematika Penulisan

Sistematika penulisan tugas akhir ini terdiri dari lima bagian. Bab pertama menjabarkan latar belakang masalah, rumusan masalah, batasan masalah, tujuan penulisan, metode penulisan dan sistematika penulisan tugas akhir ini.

Pada bab kedua akan dijelaskan tentang landasan teori yang digunakan dalam penulisan tugas akhir ini, yaitu pengantar mengenai dunia keamanan komputer, dilanjutkan dengan pengertian algoritma kunci publik (asimetris), pengertian tentang citra digital, lalu algoritma yang digunakan untuk enkripsi dan dekripsi pada penelitian ini, yaitu algoritma ElGamal.

Analisis dan perancangan sistem akan dijabarkan pada bab ketiga. Bab ketiga berisi uraian mengenai kebutuhan sistem, rancangan alur kerja sistem, dan rancangan antar muka sistem. Selain itu akan dijelaskan pula rancangan pengujian sistem dan metode analisis data yang digunakan dalam tugas akhir ini.

Hasil analisa dari perancangan sistem yang dibuat di bab ketiga akan dibahas pada bab keempat. Bab ini secara lebih spesifik akan membahas perbedaan *pixel* citra hasil denkripsi dengan citra asli. Untuk bab kelima terdiri atas dua bagian, yaitu kesimpulan tentang tugas akhir ini serta beberapa saran pengembangan yang dapat digunakan untuk penelitian yang lainnya.

BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan pada pembahasan dan analisa penulis terhadap sistem yang telah diuji pada bab 4, maka penulis dapat menarik kesimpulan sebagai berikut:

1. Algoritma ElGamal dapat diimplementasikan dengan cukup baik pada citra digital.
2. Jenis citra tidak berpengaruh terhadap lama waktu proses enkripsi dan dekripsi, lama waktu proses enkripsi dan dekripsi berbanding lurus dengan luas citra, semakin besar luas (resolusi) citra, semakin lama pula waktu yang diperlukan oleh sistem untuk melakukan proses enkripsi dan dekripsi.
3. Algoritma ElGamal dapat diimplementasikan untuk citra dengan resolusi yang cukup tinggi dengan waktu enkripsi dan dekripsi yang tidak terlalu lama.
4. Ukuran *file* citra hasil enkripsi tidak hanya membengkak dua kali lipat dari citra asli. Begitu juga dengan citra hasil dekripsi, yang mengalami pembengkakan pada hasil akhirnya. Hal ini menandakan bahwa implementasi algoritma ElGamal untuk *file* citra tidak cocok untuk ditransmisikan melalui media kirim berkecepatan rendah.
5. Algoritma ElGamal dapat mengembalikan citra hasil enkripsi ke citra awal dengan nilai MSE rendah, yang berarti, citra awal dan citra setelah mengalami pemrosesan enkripsi dekripsi hanya mengalami sedikit pergeseran nilai piksel.

5.2 Saran

Berikut adalah beberapa saran yang dapat digunakan untuk penelitian dan pengembangan sistem kedepannya:

1. Menambahkan sistem kompresi terhadap algoritma ini agar ukuran *file* yang besar dapat dikompresi menjadi *file* dengan ukuran lebih kecil, sehingga *file* dapat ditransmisikan dengan cepat.
2. Menggunakan citra dengan ekstensi lain selain .jpeg untuk penelitian.
3. Melakukan penelitian tambahan terhadap keamanan citra terhadap serangan – serangan yang biasa dilakukan peretas.

©UKDW

DAFTAR PUSTAKA

- Fauzan, A. (2012). Kriptografi Visual dengan Memanfaatkan Algoritma ElGamal untuk Citra Berwarna. *Makalah IF3058 Kriptografi – Sem. II Tahun 2012/2013*.
- Ifanto, M. (2009). METODE ENKRIPSI DAN DEKRIPSI DENGAN MENGGUNAKAN. *MAKALAH IF2091 STRUKTUR DISKRIT*.
- Jolfaei, A., & Mirghadri, A. R. (2010). An Image Encryption Approach Using Chaos and Stream Cipher. *Journal of Theoretical and Applied Information Technology*.
- Moenandar Male, G., Wirawan, & Setijadi, E. (2012). ANALISA KUALITAS CITRA PADA STEGANOGRAFI UNTUK APLIKASI e-GOVERNMENT. *Prosiding Seminar Nasional Manajemen Teknologi XV*.
- Nurhasanah, F., & Sulaiman, R. (2013). PEMBUATAN TANDA TANGAN DIGITAL MENGGUNAKAN DIGITAL SIGNATURE ALGORITHM. *MATHunesa*.
- Rhee, M. Y. (1994). *Cryptography and Secure Communications*. Seoul: McGRAW-HILL BOOK CO.
- Rochmat, N., Isnanto, R. R., & Sumantri, M. (2012). IMPLEMENTASI ALGORITMA KRIPTOGRAFI ELGAMAL UNTUK KEAMANAN PESAN (MESSAGE SECURITY). *TRANSIENT, VOL. 1, NO. 3, SEPTEMBER 2012, ISSN: 2302-9927, 83*.
- Sachs, J. (1996). *Digital Image Basics*. Digital Light & Color.
- Schaefer, E. (2010). *An Introduction to Cryptography and Cryptanalysis*.
- Schneier, B. (1996). *Applied Cryptography*. Canada: John Wiley & Sons, Inc.
- Tamam, M. T., Dwiono, W., & Hartanto, T. (2010). Penerapan Algoritma Kriptografi ElGamal untuk Pengaman File Citra. *Jurnal EECCIS Vol. IV, No. 1*.
- Xiang, T., Wong, K.-w., & Liao, X. (2007). Selective Image Encryption Using a Spatiotemporal Chaotic System. *Chaos Volume 17*.