PENGGUNAAN FUNGSI LINEAR CONGRUENTIAL GENERATOR DAN OPERATOR GENETIK UNTUK ENKRIPSI DATA TEKS

Tugas Akhir

Oleh

Popy Febrian
NIM. 22053958

Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Tahun 2011

PENGGUNAAN FUNGSI LINEAR CONGRUENTIAL GENERATOR DAN OPERATOR GENETIK UNTUK ENKRIPSI DATA TEKS

Tugas Akhir

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

Disusun oleh :

Popy Febrian
NIM. 22053958

Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Tahun 2011

PERNYATAAN KEASLIAN TUGAS AKHIR

Saya menyatakan dengan sesungguhnya bahwa tugas akhir dengan judul :

PENGGUNAAN FUNGSI LINEAR CONGRUENTIAL GENERATOR DAN OPERATOR GENETIK UNTUK ENKRIPSI DATA TEKS

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 tugas akhir ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia menerima sanksi berupa pencabutan gelar kesarjanaan saya.

Yogyakarta, 28 April 2011

(**POPY FEBRIAN**)
22 05 3958

HALAMAN PERSETUJUAN

Judul	**: PENGGUNAAN FUNGSI LINEAR CONGRUENTIAL GENERATOR DAN OPERATOR GENETIK UNTUK ENKRIPSI DATA TEKS**
Nama	**: POPY FEBRIAN**
NIM	**: 22 05 3958**
Mata kuliah	**: Tugas Akhir**
Kode	**: T12126**
Semester	**: Genap**
Tahun akademik	**: 2010/2011**

Telah diperiksa dan disetujui
di Yogyakarta,
pada tanggal : 20 Mei 2011

Dosen Pembimbing I	Dosen Pembimbing II
(Lucia Dwi Krisnawati, S.S., M.A.)	(Antonius Rachmat. C, S.Kom., M.Cs.)

PENGGUNAAN FUNGSI LINEAR CONGRUENTIAL GENERATOR DAN OPERATOR GENETIK UNTUK ENKRIPSI DATA TEKS

Oleh : Popy Febrian / 22053958

Dipertahankan di depan dewan Penguji Tugas Akhir/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
12 Mei 2011

Yogyakarta, 20 Mei 2011
Mengesahkan,

Dewan Penguji :

1. **Lucia Dwi Krisnawati, S.S., MA.**
2. **Antonius Rachmat C, S.Kom., M.Cs.**
3. **Rosa Delima, S.Kom., M.Kom.**
4. **Budi Susanto, S.Kom., M.T.**

Dekan

(Drs. Wimmie Handiwidjojo, MIT.)

Ketua Program Studi

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

HALAMAN PERSEMBAHAN

Puji Syukur Kepada Allah Yang Maha Kuasa

Skripsi Ini Saya Persembahkan Kepada Keluarga Tercinta

Dan Teman Seperjuangan

Semoga Bermanfaat Bagi Kita Semua

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan kepada **Tuhan Yang Maha Esa** atas segala rahmat dan karunia serta pertolongan-Nya, sehingga penulis dapat meyelesaikan Tugas Akhir dengan judul Penggunaan Fungsi Linear Congruential Generator dan Fungsi Genetik Untuk Enkripsi Data Teks dengan baik dan tepat waktu.

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 program dan penyusunan laporan Tugas Akhir ini penulis telah banyak mendapatkan masukan dan bimbingan dari berbagai pihak untuk kelacaran penyelesaian penulisan Tugas Akhir ini. Untuk itu pada kesempatan ini penulis menyampaikan ucapan terima kasih kepada :

1. Ibu **Lucia Dwi Krisnawati, S.S., M.A.,** selaku dosen pembimbing I yang telah banyak meluangkan waktunya memberikan pengarahan dan saran dari awal sampai terselesaikannya Tugas Akhir ini.

2. Bapak **Antonius Rachmat C, S.Kom., M.Cs.,** selaku dosen pembimbing II yang telah banyak memberi bimbingan dan petunjuk serta masukan–masukan dalam pembuatan Tugas Akhir ini.

3. Keluarga tercinta yang telah memberikan dukungan moral, dana, doa, saran dan kasih sayangnya yang berlimpah.

4. Teman-teman seperjuangan angkatan 2005 khususnya **Apul, Wahyu, Indra, Rio, Chris, Ramos** serta semua pihak yang tidak dapat penulis sebutkan satu persatu yang telah banyak memberi dukungan dan semangat dalam menyelesaikan tugas akhir ini.

Penulis menyadari bahwa program dan laporan Tugas Akhir ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari pembaca, supaya suatu saat penulis dapat menghasilkan suatu karya yang lebih baik lagi.

Akhir kata penulis mohon maaf yang sebesar-besarnya apabila ada kesalahan selama penyusunan Tugas Akhir ini. Semoga Tugas Akhir ini dapat bermanfaat bagi kita semua.

Yogyakarta, 29 April 2011

Penulis

ABSTRAK

PENGGUNAAN FUNGSI LINEAR CONGRUENTIAL GENERATOR DAN OPERATOR GENETIK UNTUK ENKRIPSI DATA TEKS

Kriptografi merupakan salah satu cara untuk menjaga kerahasiaan data dari penyadap. Begitu pentingnya kriptografi untuk keamanan informasi (*information security*), sehingga jika berbicara mengenai masalah yang berkaitan dengan penggunaan komputer, maka orang tidak bisa memisahkannya dengan penggunaan kriptografi. Adapun permasalahan yang dilakukan sebagai bahan penelitian adalah mengimplementasikan fungsi *Linear Congruential Generator*, operator genetik mutasi dan kombinasi kedalam sebuah aplikasi kriptografi enkripsi dan dekripsi data teks. Tujuan utama penulis melakukan penelitian ini adalah mengimplementasikan fungsi *Linear Congruential Generator* dan operator yang ada dalam algoritma genetik yaitu rekombinasi dan mutasi kedalam sebuah aplikasi enkripsi dan dekripsi.

Implementasi penelitian ini adalah dengan membuat sebuah aplikasi enkripsi dan dekripsi *file* teks. Aplikasi yang dibuat mengimplementasikan penggunaan fungsi *Linear Congruential Generator*, operator mutasi dan rekombinasi untuk melakukan proses enkripsi dan dekripsi kemudian diuji dengan memasukkan beberapa buah *file* teks yang berbeda. Pengujian kemudian dilakukan dengan mencatat waktu proses, ukuran *cipherteks* dan penggunaan parameter *Linear Congruential Generator* yang digunakan.

Kesimpulan yang diperoleh dari penelitian ini adalah operator genetik mutasi dan kombinasi dapat diimplementasikan kedalam sebuah aplikasi kriptografi enkripsi dan dekripsi. *Cipherteks* yang dihasilkan enkripsi dengan operator genetik dan fungsi *linear* mempunyai ukuran yang lebih besar dibandingkan ukuran *clearteksnya* dan waktu proses enkripsi yang lebih lama dibandingkan proses dekripsinya.

Kata Kunci : Kriptografi, Fungsi Genetik, Fungsi Linear Congruential Generator.

DAFTAR ISI

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Masalah keamanan (*security*) pada komputer menjadi isu penting pada era teknologi informasi saat ini. Kejahatan yang terjadi didalam keamanan komputer pun semakin maju dan beranekaragam. Pelaku kejahatan memanfaatkan celah keamanan yang ada untuk dimasuki dan melakukan manipulasi.

Kriptografi merupakan salah satu cara untuk menjaga kerahasiaan data dari penyadap. Kriptografi sudah digunakan hampir disegala bidang yang terkait dengan penggunaan jaringan komputer. Begitu pentingnya kriptografi untuk keamanan informasi (*information security*), sehingga jika berbicara mengenai masalah yang berkaitan dengan penggunaan komputer, maka orang tidak bisa memisahkannya dengan penggunaan kriptografi.

Akan tetapi dengan adanya perkembangan teknologi khususnya komputer membuat beberapa algoritma enkripsi data sudah tidak efektif lagi. Hal ini tentu saja mengharuskan penggunaan algoritma kriptografi yang efektif dan efesien. Penggunaan algoritma yang efektif tentu saja akan mempercepat proses enkripsi dan dekripsi selain itu juga akan mempersulit penyerang untuk mendapatkan informasi yang disembunyikan.

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah diatas, penulis akan membangun aplikasi enkripsi dan dekripsi dengan mengimplementasikan operator yang ada pada algoritma genetik. Masalah yang akan diteliti yaitu:

1. Bagaimana pengaruh fungsi *Linear Congruential Generator* terhadap proses enkripsi dan dekripsi ?

2. Bagaimana mengukur ukuran *cipherteks* yang dihasilkan dari proses enkripsi?
3. Bagaimana mengukur kecepatan dari enkripsi dan dekripsi data teks dengan fungsi *Linear Congruential Generator*, operator rekombinasi dan mutasi?

1.3 Batasan Masalah

Mengingat kompleksnya sistem yang akan dibuat, penulis membatasi perumusan masalah sebagai berikut :

1. *File* yang akan digunakan untuk proses enkripsi dan dekripsi berupa *plain text*.
2. Menggunakan fungsi *Linear Congruential Generator*, operator rekombinasi dan mutasi.
3. Parameter fungsi linier yang digunakan berupa bilangan bulat positif dengan nilai minimal 255 dan maksimal 2^{31}-1 (2147483647).
4. Representasi biner pada proses rekombinasi dan mutasi menggunakan 32 bit bilangan biner.

1.4 Hipotesis

Dengan menggunakan fungsi *Linear Congruential Generator* dan operator yang ada pada algoritma genetik yaitu operator rekombinasi dan mutasi dapat digunakan untuk melakukan proses enkripsi dan dekripsi.

1.5 Tujuan Penelitian

Tujuan utama penulis melakukan penelitian ini adalah mengimplementasikan fungsi *Linear Congruential Generator* dan operator yang ada dalam algoritma genetik yaitu rekombinasi dan mutasi kedalam sebuah aplikasi enkripsi dan dekripsi.

1.6 Metode Penelitian

Metode yang digunakan dalam penyusunan tugas akhir ini antara lain :

1. Pengumpulan data yang dilakukan dengan mencari referensi baik berupa buku maupun tulisan ilmiah lainnya.
2. Pembuatan sistem yang disesuaikan dengan tugas akhir ini yaitu penggunaan fungsi *Linear Congruential Generator*.
3. Evaluasi terhadap sistem yang telah dibuat sehingga dapat diperoleh sebuah kesimpulan.

1.7 Sistematika Penulisan

Sistematika penulisan laporan tugas akhir ini dibagi menjadi beberapa bab.

Bab 1 berupa PENDAHULUAN, berisi latar belakang masalah yang akan diteliti dan rencana penelitian yang akan dilakukan. Bab 2 merupakan TINJAUAN PUSTAKA yang memuat uraian dari konsep-konsep atau teori-teori yang digunakan sebagai dasar pembuatan tugas akhir ini. Bab 3 merupakan PERANCANGAN SISTEM, yang berisi tahapan dalam perancangan dan pembangunan sistem, termasuk aliran data dan rancangan antarmuka *form* masukan *(input)* dan *form* hasil *(output)* beserta kegunaannya. Bab 4 merupakan IMPLEMENTASI dan ANALISIS SISTEM, membahas tentang implementasi perancangan sistem pada bab 3 beserta analisis dan hasil *capture* dari sistem yang dibuat. Bab 5 merupakan KESIMPULAN dan SARAN, berisi kesimpulan dari hasil penelitian yang dilakukan serta memberikan saran untuk pengembangan penelitian yang telah dilakukan.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil analisis dan ujicoba yang dilakukan seperti yang dituliskan dalam bab 4. Maka dapat diambil kesimpulan seperti yang berikut ini :

1. Fungsi *Linear Congruential Generator* sangat berpengaruh terhadap proses enkripsi dengan metode ini hal ini disebabkan karena nilai acak yang dihasilkan dipengaruhi oleh parameter linier yang digunakan. Pemilihan parameter linier menentukan baik tidaknya proses enkripsi, penentuan nilai yang tidak bisa sembarang ini membuat metode enkripsi ini tidak efektif.
2. Waktu proses dekripsi lebih cepat karena proses dekripsi lebih sederhana daripada proses enkripsi.
3. Ukuran *file cipherteks* yang diperoleh dari enkripsi lebih besar bila dibandingkan dengan *clearteks* yang digunakan. Ukuran yang besar disebabkan karena *file cipherteks* menyimpan angka yang ukurannya paling tidak dua kali ukuran *cleartek*snya

5.2 Saran

Sebagai saran terhadap penelitian berikutnya adalah:

1. Perlu diuji lagi tingkat keamanan penggunaan fungsi *Linear Congruential Generator* dan operator genetik ini untuk enkripsi data teks.
2. Metode enkripsi dan dekripsi yang digunakan perlu dikembangkan sehingga tidak hanya melakukan enkripsi dekripsi terhadap *file* teks yang berupa ASCII tetapi juga terhadap jenis *file* lainnya.

DAFTAR PUSTAKA

Al-Husainy, M, A.F. (2006). Image Encryption Using Genetic Algorithm. *Asian Network for Scientific Information*, 5(3), 516-519.

Menezes, A.J., Oorschot, P.C.V & Vanstone,S.A.(1996). *Handbook of Applied Cryptography*. Ontario: CRC Press.

Munir, R.(2006). Kriptografi. Bandung: Informatika.

Nalini, N. & Rao, R .(2004). *A New Encryption And Decryption Algorithm. Combining The Featrures Of Genetic Algorithm (GA) And Cryptography*. Diakses 10 Juni 2010 dari : http://www.niitcrcs.com/iccs/iccs2004/Papers/290%20Nalini%20Niranjan.pdf

Padhy, N.P.(2005). *Artificial Intelligence and Intelligent Systems*. New York: Oxford.

Pakereng, M.A.I. (2008). Kriptosistem Menggunakan Algoritma Genetik Pada Data Citra. *Jurnal Informatika*, 9(2), 137 – 149.

Som, S., Madal, J.K , & Basu, S .(2009). A Genetic Functions Based Cryptosystem. *International Journal of Computer Science and Network Security*, 9(9), 310-315.

Stallings, W.(2005). *Cryptography and Network Security Principles and Practices (4th ed.)*. London : Prentice Hall.

Suyanto. (2008). *Evolutionary Computation*. Bandung: Informatika.