SKRIPSI

IMPLEMENTASI ALGORITMA DATA ENCRYPTION STANDARD MENGGUNAKAN GRAF SEBAGAI PEMBANGKIT KUNCI

Ignasius David Yulianus

NPM: 2013730019

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI DAN SAINS
UNIVERSITAS KATOLIK PARAHYANGAN
2017

UNDERGRADUATE THESIS

IMPLEMENTATION OF DATA ENCRYPTION STANDARD ALGORITHM WITH GRAPH AS KEY GENERATOR

Ignasius David Yulianus

NPM: 2013730019

DEPARTMENT OF INFORMATICS
FACULTY OF INFORMATION TECHNOLOGY AND SCIENCES
PARAHYANGAN CATHOLIC UNIVERSITY

2017

LEMBAR PENGESAHAN

IMPLEMENTASI ALGORITMA DATA ENCRYPTION STANDARD MENGGUNAKAN GRAF SEBAGAI PEMBANGKIT KUNCI

Ignasius David Yulianus

NPM: 2013730019

Bandung, 18 Desember 2017

Menyetujui,

Pembimbing

Mariskha Tri Adithia, P.D.Eng

Ketua Tim Penguji	Anggota Tim Penguji
Husnul Hakim, M.T.	Chandra Wijaya, M.T.

Mengetahui,

Ketua Program Studi

Mariskha Tri Adithia, P.D.Eng

PERNYATAAN

Dengan ini saya yang bertandatangan di bawah ini menyatakan bahwa skripsi dengan judul:

IMPLEMENTASI ALGORITMA DATA ENCRYPTION STANDARD MENGGUNAKAN GRAF SEBAGAI PEMBANGKIT KUNCI

adalah benar-benar karya saya sendiri, dan saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika keilmuan yang berlaku dalam masyarakat keilmuan.

Atas pernyataan ini, saya siap menanggung segala risiko dan sanksi yang dijatuhkan kepada saya, apabila di kemudian hari ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya, atau jika ada tuntutan formal atau non-formal dari pihak lain berkaitan dengan keaslian karya saya ini.

Dinyatakan di Bandung,
Tanggal 18 Desember 2017

Ignasius David Yulianus
NPM: 2013730019

ABSTRAK

Algoritma *Data Encryption Standard* (DES) merupakan sebuah teknik enkripsi yang digunakan untuk menjaga kerahasiaan suatu data. Algoritma ini akan mengubah masukannya, sebuah plainteks menjadi bentuk yang tidak dapat dimengerti lagi oleh manusia yaitu cipherteks. Pada setiap proses enkripsi, algoritma DES akan mengubah 64 bit blok plainteks menjadi 64 blok bit cipherteks.

Algoritma *Data Encryption Standard* Berbasiskan Graf (DESBG) merupakan sebuah pengembangan dari algoritma DES. Perbedaan kedua algoritma ini terdapat pada cara pembuatan 16 buah kunci ronde. DES berbasiskan graf akan menggunakan beberapa teori seperti sirkuit Hamilton dan *graph automorphism* untuk membuat kunci ronde. Modifikasi ini bertujuan untuk meningkatkan keamanan pada algoritma DES yang telah ada.

Pada skripsi ini, sebuah perangkat lunak dibangun untuk mengimplementasikan algoritma DESBG. Input yang dipakai pada perangkat lunak ini adalah plainteks dan pemetaan graf yang dimasukan oleh pengguna. Setelah perangkat lunak dibangun, pengujian keamanan terhadap algoritma ini dilakukan untuk membandingkan tingkat ketahanan algoritma terhadap serangan *brute force*.

Berdasarkan hasil pengujian, dapat disimpulkan bahwa algoritma DESBG memiliki ketahanan yang lebih baik daripada algoritma DES pada tipe serangan *brute force*.

Kata-kata kunci: *Data Encryption Standard*, plainteks, cipherteks, sirkuit Hamilton, *graph automorphism*, *brute force*

ABSTRACT

Data Encryption Standard (DES) algorithm is an encryption technique that is used to protect the secrecy of data. This algorithm will change its input, a plaintext to an incomprehensible form called ciphertext. In every encryption, DES algorithm will change 64 bits block of plaintext to 64 bits block of ciphertext.

Graph Based Data Encryption Standard (GBDES) is an improvement from data encryption standard. The difference between this two algorithm lies in the way of making 16 round keys. a graph based DES will used some theories like Hamilton circuit and graph automorphism to build a round key.The purpose of this modification is to improve the resistance to attack from the existing DES.

A software is developed to implements the GBDES. The input of this software are plaintext and graph mapping which is given by the user. Once the software is built, some test is done on this algorithm to compare the algorithm's resistance to brute force attack.

Based on the test result, it can be concluded that GBDES algorithm have a better resistance than DES algorithm due to brute force attack.

Keywords: Data Encryption Standard, plaintext, ciphertext, Hamilton circuit, graph automorphism, brute force

Dipersembahkan untuk Tuhan Yang Maha Esa, diri sendiri, keluarga, pembimbing, para sahabat dan semua orang yang telah berperan dalam pembuatan skripsi ini.

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa karena atas berkat dan rahmat-Nya penulis berhasil menyelesaikan penyusunan skripsi yang berjudul "Implementasi Algoritma Data Encryption Standard Menggunakan Graf Sebagai Pembangkit Kunci". Penulis menyadari bahwa penyelesaian penyusunan skripsi ini tidak terlepas dari bantuan berbagai pihak. Oleh karena itu, penulis ingin mengucapkan terima kasih kepada:

- Kedua orang tua penulis yang selalu memberikan movitasi, dukungan, serta kepercayaan kepada penulis.
- Ibu Mariskha Tri Adithia, P.D.Eng selalu dosen pembimbing atas bimbingan, dukungan, dan kesabarannya selama proses penyusunan skripsi ini.
- Bapak Husnul Hakim, M.T. dan Bapak Chandra Wijaya, M.T. selaku dosen penguji yang telah memberikan saran yang membangun sehingga skripsi ini dapat diselesaikan dengan baik.
- Calvin Otot Setiadi, S.E., Engkoh Kevin Sunjaya, S.T., dan Ariadne Sipit Prawita, S. Farm. selaku sahabat penulis yang selalu mengingatkan penulis untuk mengerjakan skripsi dan memberikan dukungan selama masa perkuliahan hingga penyusunan skripsi selesai.
- Mantan pacar penulis yang telah memberi semangat dan menemani penulis ketika masih menjadi pacar penulis selama proses penyusunan skripsi.
- Seluruh rekan seperjuangan dari Jurusan Teknik Informatika UNPAR yang telah menjadi teman dan sahabat penulis selama masa perkuliahan.
- Pihak lain yang tidak dapat disebutkan satu-persatu yang telah memberikan bantuan dan dukungan dalam proses penyusunan skripsi ini.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna dan memohon maaf apabila terdapat kesalahan dan kekurangan pada skripsi ini. Semoga skripsi ini bermanfaat bagi pembaca yang sedang meneliti atau mempelajari topik yang berkaitan dengan skripsi ini.

Bandung, Desember 2017

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Kriptografi adalah gabugan dari ilmu dan seni untuk mengamankan data, dan membuatnya imun terhadap serangan dari pihak ketiga[1]. Kriptografi sendiri berfokus pada pembuatan dan analisa protokol komunikasi yang dapat memblokir pihak ketiga mengetahui isi pesan atau data. Kriptografi memiliki empat buah tujuan yaitu kerahasiaan, integritas data, otentikasi, dan nirpenyangkalan. Salah satu cara yang digunakan pada kriptografi untuk mencapai tujuan kerahasiaan yaitu mengubah pesan asli menjadi sebuah bentuk yang tidak dapat dimengerti lagi oleh manusia dan mengirimkannya melewati jaringan yang aman, yang disebut dengan enkripsi. Pesan asli yang akan diubah disebut dengan plainteks dan hasil dari enkripsi disebut dengan cipherteks. Salah satu contoh algoritma yang digunakan untuk melakukan proses enkripsi adalah algoritma *Data Encryption Standard*.

Data Encryption Standard (DES) merupakan teknik enkripsi yang dikembangkan pada tahun 1970-an oleh IBM dan resmi dipublikasikan pada tahun 1977. Cara kerja DES adalah dengan mengenkripsikan sebuah blok plainteks sepanjang 64 bit menjadi cipherteks sepanjang 64 bit dengan menggunakan kunci awal sepanjang 64 bit. Terdapat dua operasi matematika yang digunakan pada algoritma ini yaitu permutasi, penyusunan kembali suatu kumpulan objek dalam urutan yang berbeda dari urutan awalnya dan operasi XOR, sebuah operasi dengan dua buah masukan berupa benar atau salah, di mana operasi ini akan mengeluarkan nilai salah jika kedua masukan memiliki nilai yang sama dan mengeluarkan nilai benar jika kedua masukan memiliki nilai yang berbeda. Pertama-tama blok plainteks akan dipermutasi dengan permutasi awal (IP). Selanjutnya hasil permutasi awal akan dimasukkan sebagai input pada *feistel network* yang akan dilakukan sebanyak 16 kali. Pada tahap terakhir hasil dari 16 ronde *feistel network* akan dipermutasi dengan *inverse* dari permutasi awal (IP-1) untuk menghasilkan cipherteks.

Saat ini algoritma DES sudah dianggap tidak aman lagi untuk melindungi proses pengiriman informasi. Hal ini terbukti pada tahun 1998 terdapat sebuah mesin bernama *Deep Crack* yang mampu meretas algoritma DES menggunakan metode *brute force* hanya dalam waktu 56 jam saja. Oleh sebab itu diperlukan algoritma lain yang lebih sulit untuk diretas. Salah satu solusi dari permasalahan ini yaitu dengan memodifikasi algoritma DES yang telah ada menggunakan graf. Graf tersebut akan digunakan untuk membangun kunci yang digunakan dalam 16 ronde *feistel network*.

Untuk memodifikasi algoritma DES menggunakan graf, beberapa teori yang berhubungan dengan graf seperti sirkuit Hamilton, sebuah sirkuit pada graf yang mengunjungi setiap simpulnya tepat satu kali dan *graph automorphism*, bentuk simetris dari sebuah graf yang dipetakan terdahap dirinya sendiri dengan tetap menjaga ketetanggaan dari simpul-simpulnya akan digunakan. Graf yang digunakan pada algoritma ini ada 2 buah graf kubus yang saling berhubungan. Sebuah graf kubus adalah sebuah graf dengan 8 buah simpul yang masing-masing simpulnya memiliki derajat 3 sehingga dapat digambarkan menyerupai bentuk kubus. Kunci yang digunakan adalah sebuah sirkuit Hamilton pada tersebut yang telah dipetakan terhadap dirinya sendiri sehingga tidak membentuk *graph automorphism* dari graf awalnya.

Dalam skripsi ini, dibuat sebuah perangkat lunak yang dapat mengubah sebuah plainteks

menjadi cipherteks dengan menggunakan algoritma DES dan algoritma DES yang telah dimodifikasi menggunakan graf. Dengan menggunakan perangkat lunak tersebut pengguna dapat melihat perbedaan cipherteks hasil enkripsi dari DES dan DES hasil modifikasi.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, rumusan masalah penelitian ini adalah sebagai berikut:

1. Bagaimana cara memodifikasi algoritma DES menggunakan graf dalam pembangunan kunci?
2. Bagaimana cara mengimplementasikan algoritma DES yang telah dimodifikasi menggunakan graf?
3. Bagaimana perbandingan keamanan antara algoritma DES yang telah dimodifikasi dengan algoritma DES?

1.3 Tujuan

Berdasarkan identifikasi masalah, tujuan penelitian ini adalah sebagai berikut:

1. Mempelajari cara memodifikasi algoritma DES menggunakan graf sebagai pembangun kunci.
2. Mengimplementasikan algoritma DES yang telah dimodifikasi menggunakan graf.
3. Menganalisis perbandingan keamanan antara algoritma DES dan algoritma DESBG.

1.4 Batasan Masalah

Dalam penelitian ini terdapat sebuah batasan yang digunakan yaitu pemilihan sirkuit Hamilton yang digunakan untuk proses pembangunan kunci dilakukan secara otomatis oleh perangkat lunak. Hal ini dilakukan untuk memudahkan pengguna dalam menggunakan perangkat lunak yang dibuat sehingga pengguna tidak perlu membuat sebuah graf dan mencari sirkuit Hamilton dari graf tersebut.

1.5 Metodologi

Metodologi yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Melakukan studi literatur tentang kriptografi, enkripsi, dan algoritma DES.
2. Melakukan studi literatur tentang graf dan *graph automorphism*.
3. Melakukan implementasi secara manual algoritma DES yang telah dimodifikasi menggunakan graf.
4. Membuat perancangan diagram kelas perangkat lunak.
5. Mengimplementasikan hasil perancangan menggunakan bahasa pemrograman *Java*.
6. Melakukan pengujian terhadap implementasi algoritma.
7. Melakukan analisa terhadap hasil pengujian perangkat lunak.
8. Membuat kesimpulan berdasarkan hasil analisis.

1.6 Sistematika Pembahasan

Pembahasan dalam penelitian ini akan dilakukan secara sistematis sebagai berikut:

1. Bab 1 Pendahuluan
   Bab ini berisi latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi penelitian, dan sistematika pembahasan.

2. Bab 2 Landasan Teori
   Bab ini berisi dasar teori tentang kriptografi, *feistel network*, algoritma *Data Encryption Standard*, graf, sirkuit Hamilton dan *graf automorphism.*

3. Bab 3 Analisis
   Bab ini berisi analisis masalah, studi kasus, diagram aliran proses, dan rancangan diagram kelas.

4. Bab 4 Perancangan
   Bab ini perisi perancangan perangkat lunak yang akan dibangun yang meliputi kebutuhan masukan dan keluaran perangkat lunak, perancangan antarmuka, dan diagram kelas lengkap.

5. Bab 5 Implementasi dan Pengujian
   Bab ini berisi implementasi antarmuka perangkat lunak, pengujian fungsional perangkat lunak, dan pengujian eksperimental perangkat lunak.

6. Bab 6 Kesimpulan dan Saran
   Bab ini berisi kesimpulan berdasarkan penelitian yang telah dilakukan serta saran bagi pengembangan selanjutnya.