ANALISA PERBANDINGAN ENKRIPSI DAN DEKRIPSI ALGORITMA KRIPTOGRAFI GOST DAN SERPENT UNTUK PENYANDIAN DATA

Nanda Sabrina[1], Setyorini[2], Dr.yusuf Kurniawan [3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Keamanan merupakan hal yang sangat penting pada era perkembangan teknologi informasi ini. Pertukaran informasi dipastikan tidak jatuh kepada pihak yang tidak mempunyai hak atas informasi tersebut oleh karena itu dibutuhkan sebuah keamanan informasi untuk menjaganya. Salah satu caranya adalah dengan menggunakan metode kriptografi.

Metode kriptografi merupakan seni dan ilmu menjaga keamanan informasi(data) dari pihak yang tidak berhak. Seseorang dapat mengubah data asli (plainteks) menjadi data yang tidak dapat dibaca (cipherteks) dan mengembalikan cipherteks menjadi plainteks semula dengan menggunakan sebuah kunci (password).

Dalam tugas akhir ini dibuat suatu perangkat lunak dengan menggunakan Borland Delphi 7 dan menganalisa perbandingan enkripsi dan dekripsi antara algoritma Gost yang memiliki kemudahan dalam implementasi nya sehingga mempunyai waktu proses yang cepat, dengan algoritma Serpent yang memiliki tingkat keamanan yang tinggi namun mempunyai waktu proses yang kurang cepat. Parameter yang dibandingkan antara lain waktu proses enkripsi dan dekripsi, nilai avalance effect, dan tingkat keamanan

Kata Kunci : kriptografi, kunci, Gost, dan Serpent.

Abstract

Security is very important thing in this information technology development. Exchange information must be prevented to fall to unauthorized user, therefore needed an information security to take care it. One of this way is using a cryptography method.

Cryptography method represent science and art of keeping information (data) secure from unauthorized user. A person can change original data (plainteks) become a data that can not be read (cipherteks) and return cipherteks into plainteks with use a key (password).

In this final task is made an implementation by using Borland Delphi 7 and analysis encryption and decryption comparison between Gost algorithm that easy to implementation so that has quick processing time, and Serpent algorithm that has high security but less in processing time. The parameters that will be compared are encryption and decryption processing time, avalance effect, and security.

Keywords : cryptography, key, Gost, and Serpent.

1. Pendahuluan

1.1 Latar Belakang

Perkembangan suatu organisasi, perusahaan, maupun negara ditentukan oleh informasi, karena hal itu merupakan suatu hal yang sangat penting. Informasi tersebut mengalami pertukaran seperti contohnya semakin mudah para pelaku kejahatan memanfaatkannya dengan memasuki maupun memanipulasi informasi. Oleh karena itu dibutuhkan sebuah keamanan pada sistem informasi untuk menanggulanginya.

Banyak hal yang dapat dilakukan untuk menanggulangi masalah keamanan informasi tersebut, salah satunya adalah dengan kriptografi. Tanpa kita sadari, kehidupan kita sudah dikelilingi oleh kriptografi, antara lain transaksi di mesin ATM, kartu kredit, mengakses internet, pembicaraan melalui telepon genggam. Sehingga kita sulit untuk memisahkan diri dari kriptografi.

Dalam kriptografi mempunyai banyak algoritma untuk menyelesaikan setiap permasalahan. Akan tetapi setiap algoritma mempunyai prinsip yang sama yaitu mengubah data jelas (*plainteks*) menjadi data sandi (*ciphertext*). Plaintext akan dikirimkan melalui saluran telekomunikasi maupun media lain. Agar data tersebut tidak dapat dimengerti oleh pihak lain, plainteks akan diubah (disandikan) dalam bentuk lain yang tidak dapat dimengerti oleh orang lain. Penyandian plainteks menjadi cipherteks biasa dinamakan *enkripsi*. Sedangkan untuk dapat membaca kembali sebuah cipherteks maka harus ditransformasikan kembali sehingga menjadi plainteks semula. Transformasi itu dinamakan *dekripsi*.

Contoh algoritma kriptografi adalah algoritma Gost dan algoritma Serpent yang mempunyai kelebihan dan kekurangan masing-masing. Algoritma Gost, *Gosudarstvenny Standart*, dikembangkan pada tahun 1970 oleh pemerintah Soviet untuk penyandian pemerintahan. Gost dibangun menggunakan jaringan Feistel dengan mempunyai panjang kunci 256 bit, beroperasi pada blok pesan dengan panjang 64-bit dan 32 putaran dengan masing putaran mempunyai 8 kunci internal. Belum adanya publikasi mengenai kripanalisis dari algoritma Gost ini memperlihatkan ketahanan algortima ini yang baik. Algoritma Serpent dipublikasikan pada tahun 1998 pada perlombaan enkripsi AES dan menduduki peringkat kedua. Serpent beroperasi dengan 128-bit dan panjang kunci 128, 192, dan 256 bit dengan 32 putaran yang mempunyai 32 kunci internal. Serpent dirancang untuk menyediakan cipher yang aman dan tahan terhadap semua jenis serangan cipher.

Tugas Akhir ini akan dibuat sebuah perangkat lunak yang dapat membandingkan algoritma Gost dan Serpent. Kedua algoritma ini mempunyai perbedaan tahun yang cukup jauh, akan tetapi keduanya mempunyai ketahanan yang mendekati, dan mempunyai putaran kunci yang sama. Tugas akhir ini akan menganalisa dengan menggunakan parameter waktu proses, *avalance effect*, dan tingkat keamanan, yang dibutuhkan untuk melakukan enkripsi dan dekripsi dari algoritma Gost dan Serpent.

1.2 Perumusan masalah

Perumusan masalah dalam Tugas Akhir ini adalah sebagai berikut :

1. Bagaimana membangun suatu perangkat lunak menggunakan algoritma Gost dan Serpent.
2. Bagaimana menganalisa perbandingan algoritma kriptografi Gost dan Serpent dengan parameter waktu proses, *avalance effect*, dan tingkat keamanan yang dibutuhkan untuk enkripsi dan dekripsi.

Ruang lingkup yang menjadi batasan Tugas Akhir ini adalah:

1. Perangkat lunak akan menghitung waktu proses untuk enkripsi dan dekripsi serta *avalance effect* pada algoritma Gost dan Serpent.
2. Parameter tingkat keamanan diselesaikan dengan uji statistik.
3. Mode Operasi yang digunakan adalah *Electronic Code Book* (ECB).
4. Ukuran kunci yang digunakan adalah 256 bit.

1.3 Tujuan Penulisan

Adapun Tujuan dari Tugas Akhir ini ialah :

1. Membangun perangkat lunak dengan menggunakan algoritma Gost dan Serpent
2. Menghitung waktu proses untuk enkripsi dan dekripsi serta *avalance effect* dari algoritma Gost dan Serpent.
3. Menganalisa kekurangan dan kelebihan dari algoritma Gost dan Serpent dengan membandingkan parameter waktu proses, *avalance effect*, dan tingkat keamanan.

1.4 Metodologi penyelesaian masalah

Metodologi yang digunakan dalam menyelesaikan Tugas Akhir ini adalah :

1. Studi Literatur dan pustaka yang bertujuan untuk mempelajari dan memahami algoritma Gost dan Serpent serta materi lain yang mendukung Tugas Akhir ini, antara lain :
   a. Pemahaman tentang sejarah dan prinsip-prinsip dasar kriptografi.
   b. Literatur mengenai prinsip dasar, *source code*, implementasi dan hal-hal lain yang berhubungan dengan algoritma Gost dan Serpent.
   c. Literatur-literatur lain yang mendukung Tugas Akhir ini.
2. Melakukan analisis terhadap materi yang didapat, antara lain :
   a. Mencari perbedaan antara algoritma Gost dan Serpent untuk dilakukan perbandingan (sebagai permasalahan dalam Tugas Akhir ini, yaitu mengenai waktu yang dibutuhkan, *avalance effect*, dan tingkat keamanan).
   b. Menganalisis kebutuhan dan spesifikasi yang dibutuhkan dalam membangun perangkat lunak.
3. Merancang perangkat lunak yang didapat dari hasil analisis sebelumnya, antara lain :
   a. Perancangan perangkat lunak dengan menggunakan Data Aliran Diagram, spesifikasi proses, dan kamus data.

4. Membangun perangkat lunak dengan menggunakan Borland Delphi 7 untuk algoritma Gost dan Serpent.
5. Melakukan pengujian dan menganalisis perangkat lunak yang telah dibangun berdasarkan waktu yang dibutuhkan untuk enkripsi dan dekripsi data dan *avalance effect*
6. Membuat laporan Tugas Akhir dan kesimpulan.

1.5 Sistematika Penulisan

Tugas Akhir ini disusun dengan sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Bab ini menjelaskan latar belakang penelitian, perumusan masalah yang dibahas serta ruang lingkup yang menjadi batasan masalah, tujuan yang ingin dicapai, metode penyelesaian masalah, dan sistematika penulisan.

BAB II DASAR TEORI

Bab ini membahas teori yang mendukung penyusunan Tugas Akhir ini, yaitu : pengenalan sistem kriptografi, algoritma kriptografi, mode operasi, dasar matematis, pengenalan algoritma Gost dan Serpent.

BAB III ANALISA DAN PERANCANGAN SISTEM

Bab ini menjelaskan hasil analisis dari kebutuhan sistem dan perancangan algoritma Gost dan Serpent dengan menggunakan Data Aliran Diagram.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini menjelaskan hasil implementasi dan pengujian perangkat lunak dari perbandingan algoritma Gost dan Serpent.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari hasil penelitian Tugas Akhir ini serta saran-saran untuk pengembangan lebih lanjut.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Kesimpulan yang diperoleh dari perbandingan dua algoritma tersebut adalah sebagai berikut:

a. Waktu proses enkripsi pada algoritma Serpent lebih lama dibandingkan pada algoritma Gost. Hal ini dikarenakan pada algoritma Serpent terdapat tiga buat tahap selain menggunakan kotak-S, dimulai dari permutasi awal, transformasi linear, dan permutasi akhir. Sedangkan pada algoritma Gost hanya mempunyai satu tahap yaitu dengan penggunaan kotak-S.
b. Waktu proses dekripsi pada algoritma Serpent lebih lama dibandingkan pada algoritma Gost karena pada algoritma Serpent menggunakan fungsi pembalik (*invers*) sedangkan pada algoritma Gost menggunakan urutan yang berbalik dibandingkan proses enkripsinya.
c. Nilai *Avalance Effect* (AE) pada algoritma Serpent lebih besar dibandingkan pada algoritma Gost, sehingga tingkat keamanan algoritma Serpent lebih baik dibandingkan algoritma Gost. Akantetapi, kedua algoritma ini mempunyai tingkat keamanan yang cukup baik karena pada pengujiannya mendapat nilai AE mendekati 50%

5.2 Saran

Saran yang diberikan untuk pengembangan algoritma Gost dan Serpent adalah

a. Dalam proses enkripsi dan dekripsi dapat menggunakan mode operasi *Cipher Block Chaining*, *Cipher Feed Back*, dan *Output Feed Back*.
b. Untuk mendapatkan sebuah kunci selain dengan menggunakan proses *padding*, dapat juga dilakukan dengan *hashing function*, maupun fungsi MAC yang menggunakan kunci rahasia dalam pembangkitan nilainya

DAFTAR PUSTAKA

[1] http://en.wikipedia.org/wiki/Avalance_Effect , Avalance Effect, diambil tanggal 1 Oktober 2009

[2] http://en.wikipedia.org/wiki/GOST, *GOST*, diambil tanggal 10 Agustus 2008

[3] Anderson, Ross dkk, 2000, *Serpent : A Proposal for the Advanced Encryption Standart*, http://www.cl.cam.ac.uk/ftp/users/rjal14/serpent.pdf didownload tanggal 28 Agustus 2008

[4] Amin, Aulia Rahman, , *Studi Block Cipher Serpent dan Rijndael*, Bandung : Institut Teknologi Bandung

[5] BORA, Piotr dan Tomasz CZAJKA, 2000, *Implementation of the Serpent Algoritm Using Altera FPGA Devices*

[6] Budiyono, Avon, 2004, *Enkripsi Data Kunci Simetris dengan Algoritma Kriptografi LOKI97*, Bandung : Institut Teknologi Bandung

[7] Felix. Fidens, 2005, *Dasar Kriptografi* http://www.ilmukomputer.com/2006/08/20/dasar-kriptografi diambil tanggal 12 Agustus 2008

[8] Jaya, 2004, *SSH-Agent*, http://www.jogja.linux.or.id diambil tanggal 10 Oktober 2009

[9] Kelsey. John, Schneier. Bruce, Wagner. David, 1996, *Key-Schedule Crypanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES* http://www.schneier.com/paper-key-schedule.pdf diambil tanggal 10 Agustus 2008

[10] Kurniawan. Yusuf, 2004, *Kriptografi Keamanan Internet dan Jaringan Komunikasi*, Informatika, Bandung

[11] Kurniawan. Yusuf, 2008, *Keamanan Sistem*, Institut Teknologi Telkom, Bandung *Slide matakuliah Keamanan Sistem 2008*

[12] Mulya. Megah, 2008, *Diktat Kuliah Kriptografi*, Universitas Sriwijaya, Palembang

[13] Munir. Rinaldi, 2004, *Sistem Kriptografi Kunci-Publik*, Institut Teknologi Bandung, Bandung

[14] Munir. Rinaldi, 2006, *GOST* http://www.informatika.org/~rinaldi/kriptografi/2006-2007 diambil tanggal 12 Agustus 2008

[15] Munir. Rinaldi, 2006, *Kriptografi*, Informatika, Bandung

[16] Peterson. Larry L, Bruce S. Davie, 2003, *Computer Network A System Approad, 3th edition*, Morgan Kaufhann Publishers, San Fransisco

[17] Sajuthi, Satria Putra, , *Kriptanalisis pada Block Cipher*, Institut Teknologi Bandung, Bandung

[18] Schneier. Bruce, 1996, *Applied Cryptography 2nd Edition*, John Wiley & Sons Inc, New York

[19] Sukmawan. Budi, 1999, Metode Enkripsi GOST http://www.bimacipta.com/gost.htm diambil tanggal 15 Agustus 208

[20] Suryana. Aulya, Santoso. Dewi Santi, Wiryadi. I Gede Arya, Sukamto. Fenny, 2007, Enkripsi, STIKOM, Bali

[21] Wikipedia, 2006, *Kriptografi* , http://id.wikipedia.org/wiki/kriptografi didownload pada tanggal 18 Agustus 2008