ANALISIS DAN IMPLEMENTASI ALGORITMA KRIPTOGRAFI KUNCI SIMETRI RABBIT UNTUK KASUS PENYANDIAN DATA MULTIMEDIA

Gadis Aprilianti[1], M. Zuliansyah[2], Vera Suryani[3]

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

Abstrak

Dengan seiring berjalannya kemajuan teknologi, banyak file multimedia yang harus diamankan dalam pendistribusiannya. Salah satunya adalah dengan teknik kriptografi dengan algoritma Rabbit. Rabbit merupakan algoritma baru yang sedang mengikuti proyek pemilihan untuk algoritma stream cipher standar baru.

Pada Tugas Akhir ini yang dilakukan adalah mengimplementasikan pengamanan data multimedia dengan algoritma Rabbit. Dari percobaan yang telah dilakukan, didapatkan data bahwa algoritma ini dapat mengenkripsi data multimedia dengan kecepatan mencapai 3,5 MB/detik. Algortima ini juga memiliki nilai avalanche effect yang baik.

Maka hasil akhir yang didapat yaitu algoritma rabbit dapat diimplementasikan untuk mengamankan data multimedia.

Kata Kunci : rabbit, stream cipher, kriptograpfi, multimedia.

Abstract

Due to the technology improvement, many multimedia files have to be secured on its distribution. One of the techniques to secure the data is to encrypt them with cryptographic algorithm such as Rabbit. Rabbit is a new cryptography algorithm which now still participates in a project to search a new standard of stream cipher algorithm.

The goal of this final task is to make an implementation of multimedia data security by encrypting the data using Rabbit algorithm. From the experiment that have been conducted, it is found that this algorithm can encrypt a multimedia data with the speed up to 3,5 MB/second. This algorithm is also has a good value of avalanche effect.

So, now we can conclude that Rabbit algorithm can be implemented for securing multimedia data.

Keywords : rabbit, stream cipher, cryptography, multimedia.

1. Pendahuluan

1.1 Latar Belakang

Kriptografi merupakan ilmu untuk mengamankan data. Kehidupan sehari-hari sebenarnya sangat berdekatan dengan kriptografi. Mulai dari transaksi di ATM, kartu kredit, bank, percakapan di telepon genggam, hingga pengaksesan internet semua menggunakan teknik kriptografi. Banyak sekali algoritma kriptografi yang dapat diaplikasikan untuk mencapai keamanan informasi. Seiring berjalannya waktu telah banyak berkembang algoritma baru yang merupakan hasil dari berbagai perbaikan dari algoritma-algoritma yang terdahulu dan diperkirakan dapat menggantikan algoritma-algoritma tersebut saat penggunaannya nanti tidak lagi dianggap aman.

Dengan seiring berjalannya kemajuan teknologi, semakin banyak pula data yang harus diamankan. Salah satunya adalah file multimedia yang pada saat ini sangat banyak dipakai untuk berbagai tujuan. Tingkat pengaksesan file multimedia yang tinggi mendorong berkembangnya pula teknik keamanan pengiriman data. File multimedia yang pada umumnya memiliki ukuran file yang besar memerlukan sistem kriptografi yang dapat mengamankan data dengan cepat. Maka itu sangat diperlukan teknik pengamanan yang sesuai untuk file multimedia.

eSTREAM adalah sebuah proyek yang diadakan oleh *European Network of Excellence for Cryptology* (ECRYPT) untuk mencari algoritma *stream cipher* baru yang memungkinkan untuk diadaptasi secara luas (*widespread adoption*) dan bertujuan untuk mendapatkan algoritma yang sesuai untuk berbagai profil aplikasi *hardware* dan *software*.

Rabbit merupakan salah satu algoritma kriptografi *stream cipher* yang ikut bersaing pada proyek ini. Saat ini Rabbit telah mencapai tahap akhir pemilihan bersama 8 kandidat lainnya. Menurut referensi [2] disebutkan bahwa Rabbit memiliki proses key setup dan enkripsi yang baik sehingga cocok untuk semua aplikasi yang memerlukan pengenkripsian data dengan jumlah yang besar seperti enkripsi pada *server*, enkripsi multimedia, enkripsi *hard-disk*, dan enkripsi pada sumberdaya yang terbatas.

1.2 Perumusan Masalah

Rabbit merupakan algoritma kriptografi kunci simetri yang termasuk dalam kategori *stream cipher*. Permasalahan yang dijadikan objek penelitian dan pengembangan tugas akhir ini adalah:

1. Bagaimana mengamankan data multimedia dengan menggunakan algoritma kriptografi Rabbit.
2. Mengetahui bagaimana performansi algoritma Rabbit dalam mengenkripsi data multimedia berdasarkan parameter waktu enkripsi/dekripsi, *avalanche effect* dan besar file input dan output.

Pada tugas akhir ini akan dibatasi oleh beberapa batasan masalah , yaitu:

1. File yang akan menjadi input merupakan file multimedia yang dibagi dalam 3 kategori yaitu image, audio dan video. Pada file image bentuknya dibatasi

hanya pada format JPEG dan GIF, file audio dengan format WAV dan MP3 dan file video dengan format AVI dan RMVB dengan berbagai ukuran. Pemilihan format file yang menjadi batasan masalah ini dilatarbelakangi oleh karena file-file tersebut merupakan format yang umum dipakai serta mudah dalam pencarian data yang diperlukan untuk proses analisis.
2. Parameter yang menjadi ukuran untuk menganalisa performansi algoritma Rabbit adalah waktu enkripsi/dekripsi, *avalanche effect* serta besar file input dan output.
3. Tidak melakukan kriptanalisis.

Hipotesa awal adalah algoritma kriptgrafi Rabbit memiliki performansi yang baik dalam mengenkripsi data multimedia bila dilihat dari parameter waktu enkripsi/dekripsi, *avalanche effect* dan besar file input dan output.

1.3 Tujuan

Dengan tugas akhir ini, diharapkan tercapainya hal-hal sebagai berikut :
1. Terbentuknya sebuah aplikasi yang merupakan implementasi pengamanan data multimedia dengan algoritma Rabbit.
2. Memberikan hasil analisa dan kesimpulan tentang performansi algoritma kriptografi Rabbit berdasarkan parameter waktu, *avalanche effect* dan besar input data dalam mengamankan data multimedia.

1.4 Metodologi Penyelesaian Masalah

Metode yang digunakan dalam penyelesaian tugas akhir ini adalah :
1. Studi Literatur dengan mempelajari literatur-literatur yang relevan dengan permasalahan yang meliputi studi pustaka dan referensi tentang:
   a. Ilmu kriptografi dan proses pengamanan data secara umum.
   b. Konsep desain dari algoritma kriptografi Rabbit.
   c. Data multimedia.
2. Melakukan perancangan perangkat lunak dengan menggunakan analisa kebutuhan sistem dan desain prosedural.
3. Melakukan implementasi berdasarkan analisa dan desain sistem yang telah dibuat.
4. Melakukan pengujian perangkat lunak yang telah dibangun.
5. Melakukan analisa proses pengamanan data multimedia dengan algoritma Rabbit dengan perangkat lunak yang telah dibangun berdasarkan parameter yang telah ditentukan.
6. Penyusunan tugas akhir dan kesimpulan akhir.

1.5 Sistematika Penulisan

Struktur Pembahasan Tugas Akhir ini disusun sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah, perumusan masalah, batasan masalah, tujuan pembahasan, metodologi pemecahan masalah dan sistematika penulisan.

BAB II LANDASAN TEORI

Membahas dasar teori yang berhubungan dengan pengertian umum kriptografi, pengamanan data menggunakan algoritma kriptografi Rabbit dan jenis-jenis *file* multimedia

BAB III PERANCANGAN PERANGKAT LUNAK

Bab ini akan membahas proses perancangan aplikasi pengamanan data multimedia dengan menggunakan algoritma kriptografi Rabbit.

BAB IV IMPLEMENTASI DAN ANALISIS HASIL UJI COBA

Membahas tentang analisis dari hasil pengujian ataupun percobaan pada implementasi algoritma kriptografi Rabbit.

BAB V KESIMPULAN & SARAN

Pada bab ini akan menjelaskan kesimpulan dan saran sebagai hasil dari analisa dan implementasi Tugas Akhir.

5. Kesimpulan dan Saran

5.1 Kesimpulan

1. Algoritma Rabbit dapat diimplementasikan untuk mengamankan data multimedia memiliki rata-rata kecepatan waktu enkripsi sebesar 3.678.812,036 byte/detik (3,5 MB/detik) dan waktu dekripsi sebesar 3.772.332,001 byte/detik (3,5 MB/detik).
2. Besar file input dan output setelah proses enkripsi tidak mengalami perubahan karena algoritma Rabbit merupakan algoritma *stream cipher* yang tidak menggunakan *padding* pada prosesnya
3. Format file yang digunakan tidak berpengaruh pada proses enkripsi maupun dekripsi yang dilakukan karena seluruh file diperlakukan sebagai file biner.
4. Algoritma Rabbit memiliki nilai *avalanche effect* sebesar 50,3907% untuk kasus berbeda kunci dan 55,1564 % untuk kasus berbeda plainteks.

5.2 Saran

Saran-saran yang dapat diberikan jika dilakukan pengembangan terhadap TA ini adalah sebagai berikut:

1. Untuk mengimplementasikan penyandian algoritma Rabbit dalam kondisi real-time yaitu pada jaringan.
2. Untuk menganalisis algoritma Rabbit dari sisi keamanan (kriptanalisis).

Daftar Pustaka

[1] Boesgaard, M., Vesterager, M., Christiansen, J., Zenner, E. *The Stream Cipher Rabbit*. Cryptico A/S.

[2] Boesgaard, M., Vesterager, M., Zenner, E. *A Description of the Rabbit Stream Cipher Algorithm*. Cryptico A/S. May 2006.

[3] Boesgaard, M., Vesterager, M., Pedersen, T., Christiansen, J., Scavenius, O. *Rabbit: A New High-Performance Stream Cipher*. Cryptico A/S. FSE 2003.

[4] Furht, B., Socek, D., Eskicioglu, A.M. *Fundamentals of Multimedia Encryption Techniques*.

[5] Heryanto, Imam dan Raharjo, Budi. *Pemrograman Borland C++ Builder*. Penerbit Informatika. Bandung. 2006.

[6] Munir, Rinaldi. *Kritografi*. Penerbit Informatika. Bandung. 2006.

[7] *Rabbit Stream Cipher, Algorithm Specification*. Cryptico A/S.12 May 2005.

[8] *Rabbit Stream Cipher - Performance Evaluation*. Cryptico A/S.20 December 2005.

[9] Schneier, B. *Applied Crytography Second Edition*. John Wiley & Sons, Inc. 1996.