

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 kriptografi 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 <i>file</i> 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.