BAB I
PENDAHULUAN

1.1.LATAR BELAKANG MASALAH

Perkembangan teknologi telekomunikasi yang ada pada saat ini mampu menciptakan berbagai macam perangkat keras yang dapat digunakan untuk mengirim atau menerima informasi dengan cepat dan mudah. Salah satu perangkat keras yang cukup banyak digunakan pada saat ini adalah telepon selular. Banyak merk dan jenis telepon selular beredar di pasaran, bahkan sudah banyak beredar telepon selular yang mempunyai kamera terintegrasi di dalamnya.

Dengan adanya penambahan fungsi pada telepon selular berupa kamera terintegrasi, penggunaan telepon selular tidak hanya digunakan untuk komunikasi suara maupun pesan teks. Namun, berkembang fungsinya sehingga dapat mengirim pesan berupa pesan multimedia khususnya *image* (*image*). Setiap pesan multimedia dapat ditransmisikan dengan berbagai media transmisi. Media transmisi tersebut dapat berupa jalur komunikasi *Global System for Mobile Communication* (GSM), *bluetooth*, *infrared*, maupun media lainnya.

Seperti halnya pesan teks, pesan yang berupa *image* juga memiliki nilai informasi yang membutuhkan pengamanan. Nilai informasi tersebut bisa menjadi informasi rahasia dan hanya pihak berwenang yang dapat mengakses informasi berupa *image* tersebut. Sebagai contoh dalam dunia intelijen, ketika seorang intelijen melakukan pengumpulan informasi rahasia yang membutuhkan pengambilan gambar dengan menggunakan telepon selular. *Image* tersebut kemudian dikirimkan kepada pimpinan melalui *Multimedia Message Service* (MMS), karena pentingnya informasi tersebut, *image* harus dienkripsi terlebih dahulu sebelum dikirimkan.

Saat ini fitur layanan MMS belum memiliki standar keamanan yang baik, karena pada implementasinya, pihak operator selular selaku penyedia layanan MMS masih dapat mengetahui isi pesan yang dikirimkan oleh pelanggan. Permasalahan lain muncul dari sisi *human error* yaitu terjadi kesalahan penulisan nomor tujuan pesan. Hal-hal tersebut menyebabkan kurang terjaminnya kerahasiaan pesan yang dikirim.

Penerapan kriptografi dengan cara penyandian pesan merupakan salah satu solusi yang dapat digunakan untuk memenuhi aspek kerahasiaan. Pesan yang dikirim tersebut hanya dapat dibaca oleh penerima yang memiliki hak untuk mengetahui isi pesan tersebut dengan menggunakan kunci rahasia. Menurut Liu, mayoritas algoritma enkripsi yang umum seperti DES, AES, IDEA tidak cocok untuk penyandian data berupa *image*.[1] Sedangkan menurut Shuihua, alasan pertama karena kecepatan proses enkripsi yang lambat. Hal ini terkait data berupa *image* memiliki ciri – ciri khusus seperti kapasitas besar, redudansi tinggi, dan korelasi antar *pixel* yang tinggi. Alasan kedua adalah dekripsi *ciphertext* harus sama dengan *original text*. Akan tetapi, persyaratan ini tidak terlalu berlaku pada *image*. Sebuah hasil dekripsi dari *cipher image* akan mengakibatkan adanya sedikit distorsi yang masih dapat diterima karena persepsi manusia.[2] Suatu distorsi merupakan nilai yang menunjukkan perbedaan antara *plain image* dengan hasil dekripsi dari *cipher image*. Perbedaan ini terjadi karena algoritma enkripsi khusus untuk *image* akan melakukan pengefektifan dalam proses enkripsinya, sehingga nilai – nilai pixel yang kurang berkorelasi akan dihilangkan tetapi tidak akan mengubah konten dari gambar tersebut. Nilai distorsi suatu *image* dapat dilihat dari nilai entropi dan korelasi antara *plain image* dan hasil dekripsi dari *cipher image*nya.

---

[1] Liu, Shubo., Sun, Jing., Xu, Zhengquan.2009. *An Improved Image Encryption Algorithm based on Chaotic System*. Wuhan University,China.Journal of Computers.

[2] Shuihua, Han., Shuangyuan, Yang.2005. *An Asymmetric Image Encryption Based on Matrix Transformation*. ECTI Transaction on Computer and Information Technologi.

Menurut Ratnasari, nilai entropi ini memberikan batasan minimum banyaknya bit yang diperlukan untuk mengkodekan keluaran sumber informasi tersebut. Sedangkan nilai korelasi merupakan salah satu teknik statistik yang digunakan untuk mencari hubungan antara (*measure of association*) dua variabel atau lebih yang sifatnya kuantitatif. Misalkan terdapat dua variabel x dan y, kita bisa menguji hubungan antara dua variabel tersebut apakah hubungannya berbanding lurus atau terbalik atau bahkan tidak mempunyai hubungan sama sekali. Dalam enkripsi *image*, dua variabel yang diuji adalah *plain image* dengan hasil dekripsi *cipher image*. Semakin rendah nilai korelasi yang dihasilkan maka algoritma tersebut semakin bagus.

Masalah lainnya muncul apabila diimplementasikan pada telepon selular. Menurut Soplanit, adanya keterbatasan kemampuan telepon selular untuk mempertahankan format dalam bentuk *image* sehingga untuk penerapan pada telepon selular yang memiliki keterbatasan kecepatan prosesor dan kapasitas memori, dibutuhkan suatu metode enkripsi yang khusus.

Menurut David Ruslim, dalam tugas akhir yang berjudul Kriptografi MMS pada Aplikasi Java menggunakan Algoritma AES , dalam pengiriman pesan yang dilakukan pengguna Mobile untuk sekarang ini, penulis berpendapat bahwa masih kurangnya keamanan akan pengiriman pesan ataupun data informasi yang akan dikirimkan, kemungkinan penyadapan pesan atau data informasi cukup relatif besar. Berdasarkan perkembangan dalam messaging services tersebut, maka dalam tugas akhir ini penulis mengkhususkan sistem yang di kriptografikan yaitu Multimedia Message Services (MMS). Sistem mengenkripsikan pesan atau data informasi berupa MMS pengirim kemudian diterima oleh penerima setelah itu penerima melakukan dekripsi pada MMS yang telah dikirim. Dari analisa yang dilakukan, diketahui bahwa ukuran besar MMS sangat

mempengaruhi proses enkripsi dan dekripsi MMS. Semakin besar ukuran MMS semakin lama waktu proses.

Menurut Yudi Prayudi dan Idham Halik dalam penulisan tugas akhir yang berjudul Studi dan Analisis Algoritma RIVEST CODE 6(RC6) mengatakan bahwa dari hasil analisis untuk enkripsi dan dekripsi data algoritma RC6 merupakan algoritma enkripsi yang lebih simple, fast, and secure.

Berdasarkan uraian diatas, penulis mencoba mengimplementasikan algoritma RC6 dan enkripsi citra pada mms dalam bentuk aplikasi perangkat lunak RCCRYPT dan menjadikannya sebagai bahan untuk penelitian skripsi dengan judul **"IMPLEMENTASI ALGORITMA RC6 UNTUK ENKRIPSI CITRA PADA MMS DENGAN MENGGUNAKAN J2ME"**

1.2.RUMUSAN MASALAH

Berdasarkan latar belakang masalah yang telah diuraikan sebelumnya, maka pokok permasalahan pada penelitian Skripsi ini adalah sebagai berikut:

1. Bagaimana mengimplementasikan algoritma enkripsi *RC6* pada J2ME?
2. Bagaimana membangun perangkat lunak untuk enkripsi *image* berbasis *RC6* pada J2ME?
3. Bagaimana propagasi *error* hasil dekripsi *cipher image* berdasarkan nilai korelasi dan entropi?

1.3.BATASAN MASALAH

Agar penelitian ini dapat dilakukan lebih mendalam dan tidak meluas maka penulisan Skripsi ini hanya akan difokuskan pada :

1. Citra yang dienkripsi hanya yang berformat JPEG.
2. Pengiriman gambar melalui *Multimedia Message Service* (MMS).
3. Diasumsikan tidak ada *error transmision*.

4. Aplikasi yang dibangun tidak menangani pengiriman kunci enkripsi ataupun dekripsi.
5. Algoritma *RC6* menggunakan satu kunci untuk enkripsi dan dekripsi (simetri)
6. Penelitian ini tidak membahas mengenai distribusi kunci publik.

1.4.TUJUAN PENELITIAN

Tujuan penelitian yang akan dilakukan pada Skripsi ini adalah sebagai berikut:

1. Mengetahui cara mengenkripsi gambar menggunakan algoritma *RC6*.
2. Mengetahui arsitektur MMS pada telepon selular.
3. Membuat perangkat lunak untuk enkripsi *image* berbasis *RC6* pada telepon selular.
4. Mengetahui propagasi *error* pada enkripsi *image* menggunakan *RC6*

1.5.MANFAAT PENELITIAN

Manfaat dari penelitian ini yaitu :

1. Secara teoritis penelitian ini diharapkan dapat menambah khasanah kepustakaan pendidikan, terutama menyangkut pengamanan pengiriman *image* pada telepon selular.
2. Secara praktisi penelitian ini diharapkan dapat memberikan solusi terhadap pengamanan pengiriman *image* pada telepon selular terkait keterbatasan kecepatan prosesor dan kapasitas memori yang ada pada telepon selular.

1.6.SISTEMATIKA PENULISAN

Secara keseluruhan Skripsi ini terdiri dari 5 bab, yaitu :

BAB I PENDAHULUAN

Pada bab ini akan dijelaskan mengenai latar belakang permasalahan, pokok permasalahan, metode penelitian, tujuan dan manfaat penulisan, kerangka berfikir serta sistematika penulisan Skripsi.

BAB II LANDASAN TEORI

Bab ini berisi tentang teori – teori yang mendasari penulisan Skripsi, antara lain : Algoritma RC6, JPEG dan bahasa pemprograman J2ME.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini menjelaskan mengenai analisis terhadap masalah – masalah pokok yang mendasari dalam penelitian Skripsi ini.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Deskripsi mengenai pengujian dan analisis performa aplikasi perangkat lunak CryptRC6

BAB V PENUTUP

Bab ini berisi simpulan yang berkaitan dengan hal-hal yang telah disampaikan sebelumnya, serta saran yang dapat dimanfaatkan untuk pengembangan lebih lanjut.

1.7.JADWAL PELAKSANAAN KEGIATAN

NO	Kegiatan	Target Output	Oktober				November				Desember				Januari				Februari			
			1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Studi Literatur	1. Menentukan Permasalahan																				
		2.Memahami cara kerja Algoritma RC6																				
		3.Mengumpulkan landasan teori permasalahan..																				
2	Perancangan Sistem	1.Menetukan software yang akan digunakan.																				
		2.Menganalisa masalah perancangan.																				
		3.Membuat perancangan sistem.																				
3	Uji Coba Rancangan	1.Simulasi & Analisa uji coba rancangan.																				
		2.Rancangan yang optimal.																				
4	Implementasi	1.Mempelajari masalah implementasi.																				
		2.Implementasi rancangan ke dalam sistem.																				
5	Uji Coba Sistem	1.Simulasi uji coba sistem																				
		2.Analisa sistem																				
6	Penyusunan Laporan	1.Dokumentasi penelitian secara lengkap.																				
		2.Laporan Skripsi																				