

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Telepon seluler merupakan alat komunikasi yang sudah dipakai oleh orang banyak. Telepon seluler juga mempunyai banyak layanan yang disediakan untuk memudahkan para pengguna. Bahkan sekarang ada telepon seluler cerdas dimana telepon seluler dapat bekerja seperti layaknya komputer. Salah satu pengembang telepon seluler pintar menggunakan sistem operasi Android.

Android adalah *system* operasi berbasis linux untuk telepon seluler. Dengan adanya android banyak sekali layanan tambahan seperti mendengarkan *music*, *video*, pengecekan *email*, pencarian data dengan internet, pertukaran data dan lain-lainnya

Pertukaran data bisa dalam bentuk teks, gambar, audio, dan multimedia. Dalam melakukan pertukaran data bisa terjadi serangan oleh orang lain dengan cara penyadapan frekuensi radio (khan, 2005). Jika pertukaran data berupa gambar maka gambar tersebut jatuh pada orang yang tidak berhak, dan gambar tersebut diedit dengan aplikasi editing gambar sehingga membuat citra seseorang jelek dimata orang lain.

Hal ini tentu saja akan mengganggu pemilik gambar, ataupun pihak yang ingin berkomunikasi dalam rangka bertukar informasi baik dalam kepentingan pribadi maupun kelompok. Sehingga perlindungan gambar merupakan kebutuhan saat ini. Untuk itu dibutuhkan suatu usaha pengamanan data dan kerahasiannya.

Perlindungan data tersebut dapat dilakukan dengan berbagai cara salah satunya dengan kriptografi menggunakan metode enkripsi terhadap gambar. Enkripsi adalah proses mengubah data asli menjadi sesuatu yang tidak memiliki makna. Dan untuk mengembalikan data menjadi dalam bentuk asli disebut proses dekripsi.

Salah satu metode enkripsi yang menggunakan dua buah kunci yang sama untuk enkripsi dan deskripsi. Metode ini lebih dikenal dengan sebutan *simetris*, contoh dari algoritma *simetris* adalah algoritma RC6

Algoritma RC6 adalah salah satu algoritma kriptografi *block cipher* yang dirancang oleh Ronald L. Rivest, Matt J.B Robshaw, Ray Sidney, dan Yuqin Lisa Yin dari RSA laboratories. Algoritma RC6 merupakan algoritma dengan parameter penuh, algoritma RC6 dispesifikasikan dengan notasi RC6-w/r/b, dimana W adalah ukuran dari word dalam bit, karena pada RC6 menggunakan 4 buah register maka word adalah ukuran blok dibagi 4. R adalah jumlah iterasi, dimana r tidak boleh negative, dan B adalah panjang kunci dalam bytes.

Kelebihan Algoritma RC6 dari algoritma RC2, RC4, RC5 yaitu algoritma RC6 yang paling aman, rumit dan sederhana, karena melibatkan *confussion*, *diffusion*, jaringan feistel dan panjang *block* dan kunci yang besar (Safrina Rika, 2006). Sedangkan jika dibandingkan dengan algoritma lain seperti *blowfish* maka algoritma RC6 lebih unggul dari dalam proses enkripsi ( Brianca Widodo Reza, 2011).

Tugas akhir ini merupakan pengembangan dari tugas akhir terdahulu yaitu enkripsi SMS (*short message service*) dengan menggunakan algoritma RC6 pada Sistem Operasi Android ( Rahmanto Arif, 2012). Pada tugas akhir ini enkripsi dilakukan pada gambar yang akan dikirim sehingga dapat terhindar dari kejahatan-kejahatan yang dapat menyalahgunakan gambar oleh orang yang tidak berkepentingan.

## **1.2 Rumusan Masalah**

Berdasarkan latar belakang masalah tersebut dapat suatu rumusan masalah yaitu “Bagaimana menerapkan algoritma RC6 pada gambar berbasis android.”

## **1.3 Batasan Masalah**

Agar fokus penelitian ini terjaga, diberikan beberapa batasan sebagai berikut :

1. Tidak membahas kecepatan dalam proses enkripsi dan dekripsi.
2. Extensi dilakukan khusus pada gambar yang berekstensi \*.JPEG dan PNG

## **1.4 Tujuan**

Tujuan dari penulisan tugas akhir ini adalah menghasilkan:

1. Melakukan enkripsi pada gambar.
2. Mengimplementasikan konsep enkripsi dengan menggunakan algoritma RC6.
3. Membangun aplikasi Android untuk pengamanan gambar menggunakan metode RC6.

## **1.5 Sistematika Penulisan**

Sistematika penulisan tugas akhir ini terdiri dari enam bagian, penjelasan dari keenam bagian ini yaitu:

### **BAB I PENDAHULUAN**

Membahas mengenai latar belakang permasalahan, rumusan masalah, batasan masalah, tujuan pembahasan, metodologi penelitian dan sistematika penulisan.

### **BAB II LANDASAN TEORI**

Membahas teori-teori pendukung. Teori yang diangkat yaitu mengenai kriptografi, pengertian kriptografi, *block cipher*, citra digital, algoritma RC6, pembangkit kunci internal, proses enkripsi dan dekkripsi RC6, pengertian Android, versi Android, arsitektur Android, perangkat Android, market Android, UML, *use case diagram*, dan *sequence diagram*.

### **BAB III METODOLOGI PENELITIAN**

Membahas tentang cara-cara atau hal-hal yang dilakukan dalam menyelesaikan kasus tugas akhir ini tahapan penelitian.

## **BAB IV ANALISIS DAN PERANCANGAN**

Membahas tentang teknik pengiriman menggunakan enkripsi pada perangkat android dengan menggunakan algoritma RC6 serta perancangan Algoritma dan prototype aplikasi yang akan dibangun.

## **BAB V IMPLEMENTASI DAN PENGUJIAN**

Membahas mengenai implementasi aplikasi enkripsi bergambar dengan menggunakan algoritma enkripsi RC6 serta melakukan pengujian dengan menggunakan metode *blackbox*, dan pengujian keamanan terenkripsi.

## **BAB VI PENUTUP**

Bab ini berisi kesimpulan dari tugas akhir yang dibuat dan menjelaskan saran-saran penulis kepada pembaca agar penerapan enkripsi menggunakan algoritma enkripsi RC6 pada sistem operasi Android dapat dikembangkan lagi.