

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Berkat perkembangan teknologi yang begitu pesat memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi atau data secara jarak jauh. Antar kota antar wilayah antar negara bahkan antar benua bukan merupakan suatu kendala lagi dalam melakukan komunikasi dan pertukaran data.

Seiring dengan perkembangan teknologi tersebut semakin meningkat pula tingkat tingkat kriminalitas terhadap konfidensial data yang saling di pertukarkan. Adapun contoh kriminalitas dalam proses pertukaran data seperti pencurian data secara ilegal, perubahan data dalam proses pengiriman. Sedangkan contoh dalam proses komunikasi, seseorang yang berada di negara hukum namun tidak mendapatkan perlindungan hak asasi pada saat dia melakukan pelanggaran hukum dengan di-*expose*-nya semua *privacy* yang dia miliki seperti foto dan lain-lain yang secara tidak langsung dikonsumsi *public*. Oleh karena itu tuntutan akan sekuritas keamanan terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat.

Berdasarkan permasalahan diatas, maka di usulkan suatu sistem kriptografi yang diharapkan dapat membantu menangani keamanan dalam proses komunikasi dan pertukaran informasi data yang berupa gambar.

1.2 Rumusan Masalah

Berdasarkan dari latar belakang yang ada di atas, maka rumusan masalah untuk proyek akhir ini adalah :

- a) Kurangnya keamanan terhadap konfidensial data dalam proses pertukaran informasi.
- b) Maraknya pencurian data atau informasi secara ilegal.

1.2 Tujuan

Berdasarkan dari latar belakang yang ada di atas, maka tujuan untuk proyek akhir ini adalah :

- a) Melindungi data dari serangan terhadap konfidensial data.
- b) Menjaga data dari pencurian ilegal dalam proses pertukaran informasi.
- c) Membangun aplikasi enkripsi untuk meningkatkan keamanan data dalam proses pertukaran informasi.

1.4 Batasan Masalah

Berdasarkan dari latar belakang yang ada di atas, maka batasan masalah untuk proyek akhir ini adalah :

- a) *Framework* yang digunakan berbasis *Android Jelly Bean 4.1* dan *4.2*
- b) Algoritma yang dipakai untuk enkripsi dan dekripsi adalah Kriptografi *Blowfish*
- c) Format gambar yang di enkripsi dan dekripsi disesuaikan dengan format di android
- d) Ukuran gambar yg di enkripsi dan deskripsi maksimal *1Mega Byte*
- e) Pada saat proses enkripsi dan dekripsi menggunakan kunci yang sama
- f) Tidak membahas proses pengiriman data

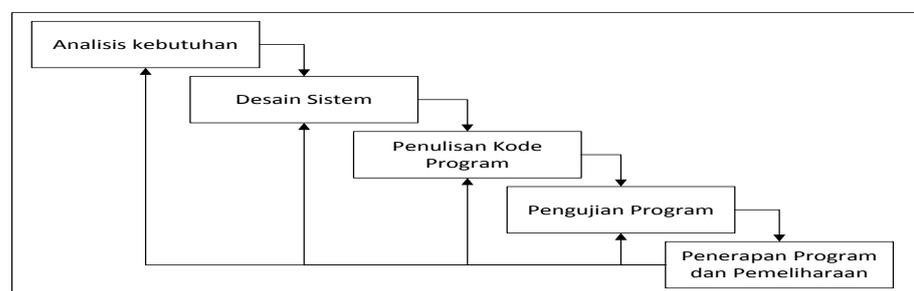
1.5 Definisi Operasional

Perancangan dan implementasi algoritma kriptografi *Blowfish* pada gambar untuk pengamanan data berbasis android merupakan suatu aplikasi yang dapat mengubah suatu pesan asli atau *plaintext* menjadi *chipertext*. Algoritma kriptografi *Blowfish* merupakan algoritma simetris yang memiliki kunci yang sama. Penggunaan algoritma *Blowfish* pada gambar adalah untuk memudahkan pengguna yang akan mengirimkan suatu gambar kepada orang lain. Gambar tersebut akan membutuhkan enkripsi apabila *file* yang dikirimkan itu merupakan suatu gambar yang bersifat rahasia. Pengamanan yang dilakukan ini untuk mengantisipasi seseorang yang tidak bertanggung jawab untuk memiliki *file* tersebut yang tentunya bukan miliknya.

Untuk sekarang ini, android merupakan operasi sistem yang banyak digunakan. Dengan fitur yang kekinian dan juga banyak aplikasi yang menunjang dalam kegiatan sehari-hari menjadikan android ini banyak digemari oleh masyarakat. Melihat kondisi ini, android menjadi pilihan yang pas apabila aplikasi ini dapat diterapkan.

1.6 Metode Pengerjaan

Metode yang dilakukan untuk mengerjakan proyek akhir ini menggunakan metode SDLC (*Systems Development Life Cycle*) dengan model *waterfall* dengan tahapan-tahapan seperti pada Gambar 1-1



Gambar 1-1
Tahapan Metode *Waterfall*

a. Analisis Kebutuhan

1. Mencari berbagai referensi mengenai metode kriptografi *Blowfish*.
2. Memahami metode kriptografi *Blowfish* dengan mengacu pada referensi yang telah diperoleh
3. Menentukan aplikasi pendukung untuk mendesain dan mengimplementasikan kriptografi *Blowfish* sebagai metode pengamanan.

b. Desain Sistem

Setelah dokumen analisa kebutuhan aplikasi telah terdefinisi dengan baik dan sesuai dengan keinginan ,maka kebutuhan aplikasi siap diimplementasikan . Membuat spesifikasi utama yaitu merancang *Diagram Flowchart* di *microsoft visio 2007*.

c. Penulisan Kode Program

Tahapan penulisan kode program dilakukan berdasarkan dokumen desain yang telah dibuat oleh desainer pada tahapan sebelumnya dan menterjemahkan kedalam bahasa pemrograman oleh *programmer*.

d. Pengujian Program

Proses pengujian dimulai dari kebenaran logika perangkat lunak.Semua fungsi-fungsi aplikasi harus diuji cobakan, agar aplikasi bebas dari *error*, dan hasilnya harus benar-benar sesuai dengan kebutuhan yang sudah direncanakan.

e. Penerapan Program dan Pemeliharaan

Perangkat lunak yang sudah disampaikan kepada masyarakat akan mengalami perubahan. Perubahan tersebut karena pelanggan membutuhkan perkembangan fungsional terhadap perangkat lunak yang disampaikan.

1.7 Jadwal Pengerjaan

Untuk jadwal pengerjaan pada proyek akhir ini dapat dilihat pada tabel 1-1

Tabel 1-1
Pengerjaan Proyek Akhir

Kegiatan	Agu-13				Sep-13				Okt-13				Nov-13				Des-13			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Pengumpulan Data																				
Analisis kebutuhan																				
Desain Sistem																				
Penulisan Kode Program																				
Pengujian Program																				
Penerapan Program dan Pemeliharaan																				
Pembuatan laporan																				