

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Saat ini perkembangan teknologi informasi sudah memasuki hampir di setiap aktifitas manusia. Tingkat mobilitas seseorang sudah mulai bergantung pada kecanggihan teknologi yang bersifat praktis dan efisien. Teknologi *smartphone* menjadi pilihan yang mayoritas diminati untuk mendukung aktifitas keseharian. Android merupakan sistem informasi yang dipasang pada *smartphone* yang dewasa ini menduduki tingkat penjualan terbanyak [1]. Kebutuhan fitur pun ikut mengalami evolusi, dari kebutuhan perangkat yang diterapkan pada dekstop menjadi kebutuhan perangkat *mobile*.

Selain keuntungan yang diperoleh dari kemajuan teknologi, tapi juga aspek negatifnya banyak terjadi seperti kejahatan komputer, yang meliputi pencurian penipuan, pemerasan, kompetitif, sampai jatuhnya informasi ke pihak yang tidak berhak [2]. Cara mencegah permasalahan keamanan tersebut, diperlukan suatu metode keamanan data. Data atau informasi tidak hanya berupa data teks, tetapi juga dapat berupa data citra (*image*), data suara (*audio*), dan video. Metode yang sering digunakan adalah kriptografi [3]. Kriptografi adalah salah satu kategori utama terhadap keamanan komputer yang dapat mengubah suatu informasi yang dapat dikenali menjadi informasi yang tidak dapat dimengerti [4].

Salah satu algoritma yang dapat digunakan adalah algoritma twofish yang merupakan algoritma kriptografi kunci simetri dengan memanfaatkan 128 block

bit dalam proses enkripsi dan dekripsi data. Tahun 1998 diadakan suatu kompetisi untuk menetapkan metode algoritma enkripsi standar di amerika. Kompetisi itu memperoleh lima finalis yaitu *Rijindael*, *Serpent*, *Twofish*, *MARS* dan *RC6*. Diantara semua metode, algoritma *twofish* dianggap sebagai algoritma yang memiliki tingkat keamanan yang tinggi dan metodenya bebas digunakan [3].

Algoritma *twofish* menggunakan desain yang mudah dan kunci tidak lemah[4]. Desain yang mudah akan mempengaruhi kecepatan proses enkripsi dan dekripsi sehingga algoritma ini cocok untuk keamanan file yang membutuhkan proses yang cepat. Sementara itu, dengan kunci tidak lemah maka kunci apapun yang menjadi masukan oleh pengguna, akan tetap sama tingkat keamanannya. Berdasarkan uraian diatas, maka dilakukan penelitian yang bertujuan untuk merancang dan mengimplmentasikan aplikasi kriptosistem file berbasis android menggunakan algoritma *twofish*.

1.2 Rumusan Masalah

Dari uraian latar belakang diatas, maka dapat dirumuskan masalah sebagai berikut:

1. Bagaimana cara membuat aplikasi kriptosistem file berbasis android menggunakan algoritma *twofish*?
2. Bagaimana membuat aplikasi kriptosistem file untuk mengamankan berbagai jenis data, berupa data text, citra (image), suara (audio), video atau berbagai extensi file.

1.3 Batasan Masalah

Ada beberapa batasan masalah dengan tujuan agar pembahasan tidak melebar dan lebih terperinci. Adapun ruang lingkup permasalahan antara lain:

1. Aplikasi kriptosistem file dijalankan pada sistem operasi android mulai versi 4.1.1 (jelly bean), kapasitas minimal RAM 512 Mb
2. Aplikasi kriptosistem file dapat melakukan enkripsi data text (doc dan pdf), gambar (JPG dan PNG), suara (mp3), dan video (mp4, dan mkv).
3. Algoritma yang digunakan adalah *Twofish*
4. Software yang digunakan untuk membangun aplikasi adalah Android studio 1.5

1.4 Maksud dan Tujuan

Penelitian ini memiliki maksud dan tujuan sebagai berikut:

- a. Menghasilkan sebuah aplikasi yang bisa menjadi sarana keamanan data dan informasi
- b. Penulis mendapat pengetahuan mengenai pembuatan aplikasi kriptosistem file
- c. Menambah koleksi skripsi di Amikom Research Center (AMC) tentang perancangan dan implementasi aplikasi kriptosistem file berbasis android serta memberikan referensi kepada mahasiswa STMIK Amikom yang menyelesaikan tugas akhir dan skripsi
- d. Penulis mampu mengembangkan dan penerapkan ilmu yang telah diperoleh selama mengikuti perkuliahan di STMIK Amikom Yogyakarta

- e. Sebagai salah satu syarat untuk mendapatkan gelar sarjana Strata-1 pada jurusan Teknik Informatika STMIK Amikom Yogyakarta

1.5 Metode Penelitian

Penelitian menjabarkan cara – cara memperoleh data – data yang digunakan untuk kebutuhan penelitian. Metode penelitian yang penulis gunakan dalam penyusunan skripsi adalah sebagai berikut:

1.5.1 Metode Pengumpulan Data

Penulis menggunakan metode studi pustaka dalam pengumpulan data yang dimaksudkan untuk mendapatkan konsep – konsep teoritis menggunakan buku, jurnal, serta sumber lainnya yang berhubungan dengan masalah yang diteliti, sehingga dapat digunakan untuk landasan teori dalam penelitian maupun dalam menganalisa data yang ada.

1.5.2 Metode Analisis

Metode analisis menggunakan analisis kebutuhan, analisis sumber daya manusia dan analisis kelayakan.

1.5.3 Metode Perancangan

Metode perancangan penulis menggunakan diagram UML (*unified Modelling language*) untuk menentukan alur dari aplikasi yang dibuat.

1.5.4 Metode Pengembangan

Metode pengembangan penulis menerapkan tahapan-tahapan sebagai berikut:

- a. Perancangan aset interface aplikasi

- b. Pembuatan aplikasi
- c. Pengujian aplikasi
- d. Implementasi aplikasi

1.5.5 Metode Testing

Metode testing penulis menggunakan beberapa jenis testing, yaitu sebagai berikut:

a. *White Box Testing*

Aplikasi di uji dengan cara pengecekan terhadap detail perancangan, menggunakan struktur kontrol dari desain program secara procedural.

b. *Black Box Testing*

Aplikasi di uji dengan menjalankan atau mengeksekusi unit atau modul, kemudian diamati apakah apakah hasil dari unit atau modul, sesuai dengan proses yang diinginkan

c. *Compability Testing*

Aplikasi di uji ke beberapa hardware yang berbeda, dan jenis versi android yang berbeda.

1.6 Sistematika Penulisan

Sistematika penulisan laporan yang merupakan laporan analisa hasil penelitian terdiri atas:

BAB I PENDAHULUAN

Bab ini memuat latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini menjelaskan konsep dasar aplikasi, sistem file, kriptografi, android, dan uraian penjelasan tentang algoritma *twofish*, serta konsep dasar UML (*Unified Modelling Language*).

BAB III ANALISA DAN PERANCANGAN

Bab ini membahas mengenai analisa kebutuhan sistem, analisis sumber daya manusia, analisis kelayakan, perancangan sistem, dan perancangan interface aplikasi.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini membahas aplikasi secara keseluruhan, dari tahap penelitian sampai pembuatan aplikasi, serta hasil testing dan implementasi dari aplikasi yang dibuat.

BAB V PENUTUP

Bab ini menjelaskan mengenai kesimpulan dari hasil penelitian dan sebagai bahan peninjauan selanjutnya.

DAFTAR PUSTAKA