BAB I

PENDAHULUAN

I.1. Latar Belakang

Saat ini sistem komputer yang terpasang makin mudah diakses. Sistem *time sharing* dan akses jarak jauh menyebabkan masalah keamanan menjadi salah satu kelemahan komunikasi data seperti internet. Di samping itu kecendrungan lain saat ini adalah memberikan tanggung jawab sepenuhnya kepada komputer untuk mengelola aktifitas pribadi dan bisnis seperti *sistem transfer* dana elektronik yang melewatkan uang sebagai aliran bit dan lain sebagainya. Untuk itu diperlukan sistem komputer yang memiliki tingkat keamanan yang dapat terjamin, demikian pula dengan keamanan data.

Keamanan dokumen merupakan salah satu hal yang sangat penting dalam penukaran data, khusunya pertukaran data di dunia maya yang di dalamnya terdapat banyak ancaman pada saat proses itu di lakukan. Keamanan data, khususnya untuk dokumen teks bagi suatu organisasi yang mengasumsikan bahwa dokumen tersebut bernilai rahasia (*private and confidential*). Salah satu aspek keamanan dalam dokumen teks adalah keaslian, bentuk dan isinya harus sesuai dengan yang dimaksud oleh pembuat. Hingga saat ini sistem *kriptografi* merupakan salah satu solusi untuk menjamin keamanan dari suatu data yaitu dengan menyandikan *file* dokumen tersebut menjadi sulit bahkan tidak dipahami melalui proses *enkripsi* dan untuk memperoleh kembali informasi yang asli dilakukan, proses *dekripsi* disertai dengan menggunakan kunci yang benar.

Dari latar belakang di atas penulis akan mengangkat judul skripsi yang berjudul **"Implementasi Metode Stream Cipher untuk Keamanan File Dokumen Berbasis Android".**

I.2. Ruang Lingkup Permasalahan

Ruang lingkup permasalahan yang terdapat pada penelitian ini adalah sebagai berikut :

I.2.1. Identifikasi Masalah

Berdasarkan latar belakang permasalahan diatas, penulis dapat mengidentifkasikan masalah yang ada, yaitu :

1. Pertukaran data *File* dokumen sangat beresiko mengalami tindak kejahatan seperti pencurian, penyadapan, dan manipulasi data.
2. Sangat mudahnya penyalinan data oleh pihak yang tidak berhak karena tidak memiliki keamanan data membuat data pribadi dari pengguna lain dapat diakses oleh siapa saja..
3. Masih sedikitnya aplikasi yang mendukung pengamanan data file dokumen yang di implementasikan dalam android.

I.2.2. Perumusan Masalah

Rumusan masalah pada penulisan skripsi ini adalah sebagai berikut :

1. Bagaimana cara kerja dan penerapan metode *Stream Cipher* untuk keamanan data ?
2. Bagaimana mengimplementasikan metode *Stream Cipher* untuk keamanan data atau *file* dokumen ?

3. Bagaimana membangun sebuah aplikasi yang mampu mengelola dan mengamankan data atau *file* dokumen berbasis Android ?

I.2.3. Batasan Masalah

Adapun penulis memliki batasan masalah pada penulisan skripsi ini antara lain :

1. Penulisan skripsi hanya membahas tentang algoritma *stream cipher* yaitu meliputi perhitungan enkripsi dan perhitungan dekripsi.
2. Penulisan skripsi fokus untuk membangun rancangan program berbasis android.
3. Penulisan skripsi difokuskan untuk mengamankan *file* dokumen dari segi ekstensi,dan nama *file* saja.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Adapun tujuan dan target penulisan skripsi ini adalah sebagai berikut :

1. Menerapkanan metode *Stream Cipher* untuk keamanan data.
2. Mengimplementasikan metode *Stream Cipher* untuk keamanan data atau *file* dokumen.
3. Membangun sebuah aplikasi yang mampu mengelola dan mengamankan data atau *file* dokumen berbasis Android.

I.3.2. Manfaat

Adapun manfaat bagi penulis dari hasil penulisan skripsi ini adalah sebagai berikut

1. Dapat menerapkan metode *Stream Cipher* untuk keamanan data.
2. Dapat mengimplementasikan metode *Stream Cipher* untuk keamanan *file* dokumen.
3. Menghasilkan sebuah aplikasi yang mampu mengelola dan mengamankan data atau *file* dokumen berbasis Android.

I.4. Metodologi Penelitian

Pada tahap ini dilakukan dengan mempelajari teori dasar yang mendukung penelitian, pencarian dan pengumpulan data-data yang dibutuhkan. Untuk mengumpulkan data yang dibutuhkan, maka penulis memakai teknik :

1. Wawancara (*Interview*)

Penulis mewawancarai pihak-pihak terkait dengan penelitian yaitu ahli kriptografi dan peneliti terdahulu

2. Penelitian Perpustakaan (*Library Research*)

Studi kepustakaan dapat diartikan sebagai suatu langkah untuk memperoleh informasi dari penelitian terdahulu yang harus dikerjakan, tanpa memperdulikan apakah sebuah penelitian menggunakan data sekunder. Data sekunder adalah data yang diperoleh melalui data yang telah diteliti dan dikumpulkan oleh pihak lain yang berkaitan dengan permasalahan penelitian Adapun beberapa jurnal yang penulis jadikan referensi antara lain :

No	Bentuk	Penulis	Judul
1	Jurnal	F. Wiwiek Nurwiyati & Indra Yatini B (2013).	Enkripsi Dekripsi Data Menggunakan Metode *Stream* Dan *Vigenere Cipher*.
2	Jurnal	Setyaningsih E. (2013).	Implementasi System Sandi *Stream Cipher* Untuk Pengamanan Data *Image.*
3	Jurnal	Fresly Nandar Pabokory, Indah Fitri Astuti & Awang Harsa Kridalaksana (2015).	Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi *File* Dokumen, Dan *File* Dokumen Menggunakan Algoritma *Advanced Encryptio Standard.*
4	Buku	Penerbit Andi (2010).	Paling Dicari PHP *Source Code*.
5	Jurnal	Nurhadiyanto,	Algoritma Optimasi & Aplikasinya.
6	Jurnal	Syamsurizal Angga Agusta & Triyani Arita Fitri A (2016).	Implementasi Algorithma *Stream Cipher* RC4 dalam Aplikasi Pendataan Alumni STMIK Amik Riau.
7	Jurnal	Aulia Arham, (2014).	Enkripsi Selektif Audio Digital Dengan *Stream Cipher* Berbasis Fungsi Chaotik *Logistic* Map.
8	Jurnal	14. Paulus Lucky Tirma Irawan, (2015).	Implementasi Teknik Kriptografi *Stream Cipher Salsa20* Untuk Pengamanan Basis Data.
9	Jurnal	Halim Agung, Budiman, (2015).	Implementasi *Affine Chiper* Dan Rc4 Pada Enkripsi *File* Tunggal.

10	Jurnal	Muhammad Ropianto. (2016).	Pemahaman Penggunaan *Unified Modelling Language.*
11	Jurnal	Made Suarte, 2013	Rancang Bangun Aplikasi Warta Kesatuan Mahasiswa Hindu Dharma Indonesia Berbasis Android Dengan Metode Guidelines For Rapid Application Engineering (GRAPPLE)
12	Jurnal	Nathasia, N. D. (2012)	Penerapan Teknik Kriptografi Stream Cipher Untuk Pengaman Basis Data.

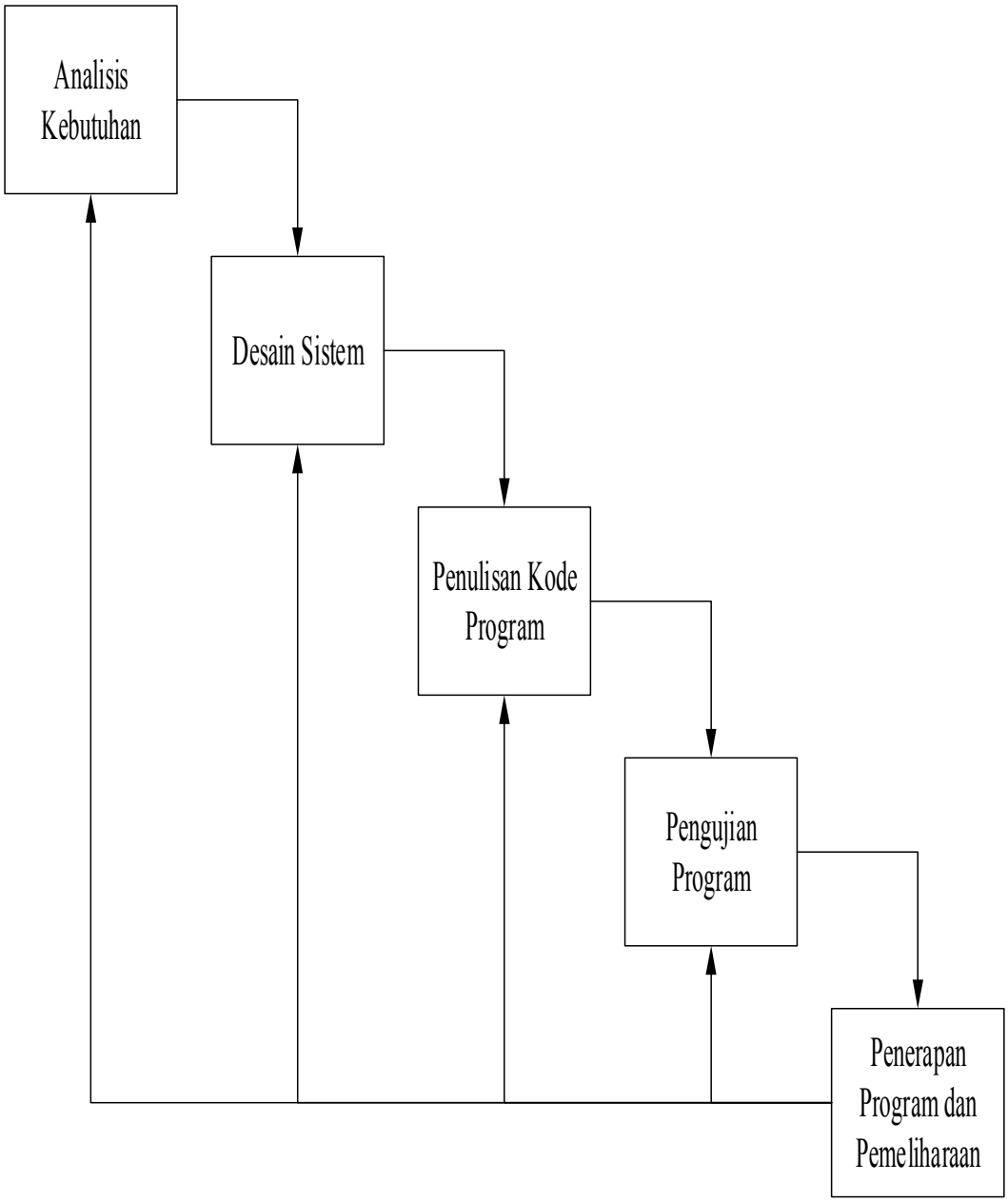
Tabel I.1. Referensi penelitian perpustakaan.

3. Sampel (*Sampling*)

Mengambil contoh data yang diperlukan untuk proses pengujian hasil program, khususnya disini penulis mengambil contoh data milik penulis sendiri. Adapun beberapa sampel contoh data yang akan digunakan antara lain :

1. *File* dokumen dalam ekstensi *document* (.doc).

Adapun model rancangan pembangunan sistem yang akan dibuat dalam beberapa tahapan yang digambarkan dalam bentuk *waterfall* seperti di gambar I.1. berikut :



Gambar I.1. Metode *Waterfall* Dalam Perancangan Sistem.

Keterangan :

1. Analisis Kebutuhan

Pada tahapan ini merupakan analisa terhadap kebutuhan yang diperlukan untuk mencapai tujuan penelitian yang akan dilakukan. Pada tahap ini dilakukan

pengumpulan kebutuhan data dan aplikasi sebagai media perancangan program yang akan dibangun. Adapun beberapa hal yang penulis butuhkan antara lain :

Berikut adalah *software* yang digunakan untuk pembuatan sistem :

a. Sistem operasi *windows* 7
b. *Ionic*
c. *Visual Studio Code*

Berikut adalah *hardware* yang digunakan untuk penerapan sistem :

a. *Laptop/ Computer*
b. Kabel *USB*
c. *Mouse*
d. *SmartPhone Android*

Berikut adalah bahan bacaan yang digunakan untuk teori :

a. Buku
b. Jurnal

2. Desain Sistem

Proses desain akan menerjemahkan syarat kebutuhan sebuah perancangan perangkat lunak yang dapat diperkirakan sebelum dibuat kode program. Proses ini berfokus kepada : struktur data, arsitektur perangkat lunak, representasi *interface*, dan *detail* (algoritma) prosedural. Pada tahap ini dilakukan desain perangkat lunak menggunakan pemodelan *UML* yaitu *use case diagram*, *class diagram*, *activity diagram* dan *sequence diagram*.

3. Penulisan Kode Program

Kode program merupakan terjemahan *design* dalam bahasa yang bisa dikenali komputer. Pada tahap ini desain sistem diimplementasikan ke dalam kode program. Pemrograman dimulai dengan bahasa pemrograman *JavaScript*.

4. Pengujian Program

Tahap pengujian adalah tahap dimana sistem yang telah dibuat dari hasil analisis masalah yang telah melalui tahap-tahap desain, lalu masuk kedalam proses pengujian sistem, sehingga akan dapat diketahui hasil kinerja sistem.

5. Penerapan Program dan Pemeliharaan

Pada tahap ini program akan diterapkan dalam sistem android. Pengguna mengklik menu *enkripsi* kemudian pada menu tersebut *file* dokumen yang akan di *enkrpsi* di upload oleh pengguna kedalam sistem kemudian pengguna mengisi kunci yang akan di gunakan untuk *enkripsi* setelah itu pengguna mengklik tombol *enkripsi file* ,setelah itu file akan otomatis terenkripsi dengan metode *stream cipher* dan pengguna dapat *mendownload file* yang sudah terenkripsi dengan mengklik tombol *download file* kemudian *file* hasil *enkripsi* akan tersimpan di perangkat di folder *Download* kemudian *folder enkripsi* .Setelah itu proses dekripsi bisa dilakukan di menu dekripsi pengguna mengupload *file* yang sudah terenkripsi tadi,kemudian pengguna memasukkan kunci yang sama pada saat *enkripsi* sebelumnya bila kunci tidak sama hasil *dekripsi* tidak akan berhasil dan *file* tidak akan terbuka setelah itu pengguna mengklik tombol *dekripsi file* sistem akan otomatis medkripsikan *file* dokumen tersebut setelah itu pengguna dapat mendownload *file* dengan cara mengkilk tombol *download file* kemudian *file* akan

tersimpan di perangkat di dalam folder Download kemudian folder *dekripsi* .bila pengguna tidak paham cara menggunkan aplikasi ini pengguna dapat mencari informasi di menu *Help* di dalam menu *Help* berisi informasi cara pemakian aplikasi yang benar dan tepat. Apabila program telah berjalan dengan baik maka program akan dilakukan pemeliharaan secara berkala.

I.5. Kontribusi Penelitian

Hasil dari penelitian ini dapat digunakan berbagai kalangan dan hasil dari penelitian ini sangat bermanfaat untuk melakukan pengamanan *file* dokumen penting. Aplikasi ini nantinya juga dapat digunakan oleh instansi swasta ataupun instansi negara untuk mengamankan *file* dokumen yang bersifat rahasia maupun penting bagi instansi tersebut.

I.6. Lokasi Penelitian

Dalam melakukan proses penulisan skripsi ini, penulis tidak melakukan penelitian pada perusahaan ataupun instansi terkait, dikarenakan dalam melakukan penelitian ini penulis cukup menggunakan *file* berkas data dokumen penulis untuk dijadikan objek penelitian.

I.7. Sistematika Penulisan

Sistematika penulisan yang diajukan dalam skripsi ini adalah sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini menjelaskan tentang ide-ide pokok permasalahan yang akan dikembangkan. Pada bab ini juga menyertakan cara pengumpulan data dan jadwal perencanaan dalam menyelesaikan penulisan skripsi. Bab ini terdiri dari latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metodologi penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini menjelaskan teori dasar yang berhubungan dengan program yang akan dirancang serta menggunakan *database* dan bahasa program yang akan digunakan. Bab ini berisi tentang studi literatur.

BAB III ANALISA DAN DESAIN SISTEM

Pada bab ini menjelaskan tentang perancangan analisa sistem dan desain tampilan sistem yang akan dibangun. Pada bab ini juga menjelaskan metode perhitungan algoritma yang akan digunakan. Bab ini terdiri dari analisis masalah, penerapan metode/algoritma, desain sistem, desain *database* dan desain *user interface*.

BAB IV HASIL DAN UJI COBA

Pada bab ini menjelaskan tentang hasil sistem/perangkat lunak yang telah selesai dibangun dengan implementasi rancangan sistem baru. Pada bab ini juga menyajikan hasil uji coba dari sistem yang sedang dirancang. Bab ini terdiri dari hasil

dan uji coba hasil. Analisa sistem dirancang untuk mengetahui kelebihan dan kekurangan sistem yang dibuat

BAB V KESIMPULAN

Pada bab ini menjelaskan tentang kesimpulan hasil akhir dari pemecahan masalah yang didefinisikan pada Bab I. Pada bab ini juga menjelaskan tentang saran yang diberikan penulis agar skripsi ini dapat lebih baik. Bab ini terdiri dari kesimpulan dan saran.