

BAB I

PENDAHULUAN

I.1. Latar Belakang

Pada saat ini perkembangan teknologi komputer telah memberikan kemudahan bagi banyak orang, dari perangkat keras atau perangkat lunak yang dapat dengan mudah didapat dan digunakan. Semakin berkembangnya aplikasi yang telah komputersasi yang banyak mendukung pada banyak perangkat baik komputer maupun *mobile phone*. Salah satu bentuk aplikasi yang mengikuti perkembangan komputer adalah aplikasi pengiriman *email*. Aplikasi pengiriman *email* sangat bermanfaat bagi setiap orang. Dimana penggunaannya dapat dilakukan dengan jarak jauh, pengiriman email pesan teks, kutipan, *video* ataupun juga mengirim *file* penting lainnya.

Keamanan adalah aspek yang paling menantang di internet dan jaringan aplikasi. Internet dan jaringan aplikasi yang berkembang sangat cepat, sehingga pentingnya dan nilai data yang dipertukarkan melalui internet atau jenis media lainnya meningkat. Oleh karena itu pencarian solusi terbaik untuk menawarkan perlindungan yang diperlukan terhadap serangan penyusup data bersama dengan menyediakan layanan ini dalam waktu adalah salah satu mata pelajaran yang paling menarik dalam masyarakat keamanan terkait. Kriptografi adalah salah satu kategori utama keamanan komputer yang mengkonversi informasi dari bentuk normal ke dalam bentuk terbaca. Dua karakteristik utama yang mengidentifikasi dan membedakan algoritma enkripsi satu dari yang lain adalah kemampuannya

untuk mengamankan data yang dilindungi terhadap serangan dan kecepatan dan efisiensi dalam melakukannya. Dengan itu pada perancangan aplikasi ini penulis berinisiatif mengangkat perancangan ini dengan judul “**Perancangan Aplikasi Pengiriman Email Dengan Implementasi Keamanan Menggunakan Algoritma *Triple DES***”

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Adapun identifikasi masalah pada perancangan yang penulis lakukan adalah sebagai berikut :

1. Masih berkurangnya suatu aplikasi keamanan dalam pengiriman *file* pada *email* dengan algoritma *Triple DES*.
2. Masih seringnya terjadi manipulasi data yang dilakukan oleh pihak-pihak yang tidak terjadi bertanggung jawab.
3. Kurangnya perancangan aplikasi dalam pengamanan data dengan menggunakan pemrograman Java.

I.2.2. Perumusan Masalah

Berdasarkan identifikasi masalah di atas, penulis merumuskan masalah dalam suatu perumusan. Adapun perumusan masalah yang penulis rangkum dalam penulisan skripsi ini adalah :

1. Bagaimana perancangan dengan implementasi keamanan dalam pengiriman email dengan penerapan metode Triple DES?

2. Bagaimana mengembangkan pemrograman Java ke dalam aplikasi keamanan data dalam pengiriman email?
3. Bagaimana proses yang terjadi pengiriman email dengan penerapan algoritma Triple DES?

I.2.3. Batasan Masalah

Agar memperoleh hasil yang maksimal dan terfokus maka penulis membatasi permasalahan pada perancangan aplikasi ini antara lain :

1. Perancangan aplikasi ini hanya sebatas pada pengiriman email.
2. Perancangan aplikasi pengiriman email menggunakan algoritma *Triple DES*.
3. Menjelaskan secara detail konsep kerja dari aplikasi dengan implementasi algoritma *Triple DES*.
4. Bahasa pemrograman yang digunakan adalah *Java* dengan *SDK Java* Versi 1.7, *tools editor Netbeans 7.1* sebagai alat bantu pengerjaan *Coding*, dan *algoritma Triple DES* sebagai media *Eclipse*.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Adapun tujuan dari perancangan aplikasi ini adalah sebagai berikut :

1. Untuk membangun aplikasi pengiriman email dengan pengkodean pada sebuah perangkat.

2. Untuk mengimplementasikan aplikasi dalam meningkatkan kenyamanan pengiriman email sehingga *file* yang dikirim lebih nyaman.
3. Untuk mengetahui tingkat penyandian yang terjadi dengan penerapan *Triple DES*.

I.3.2. Manfaat

Manfaat yang diharapkan dari penulisan skripsi ini adalah :

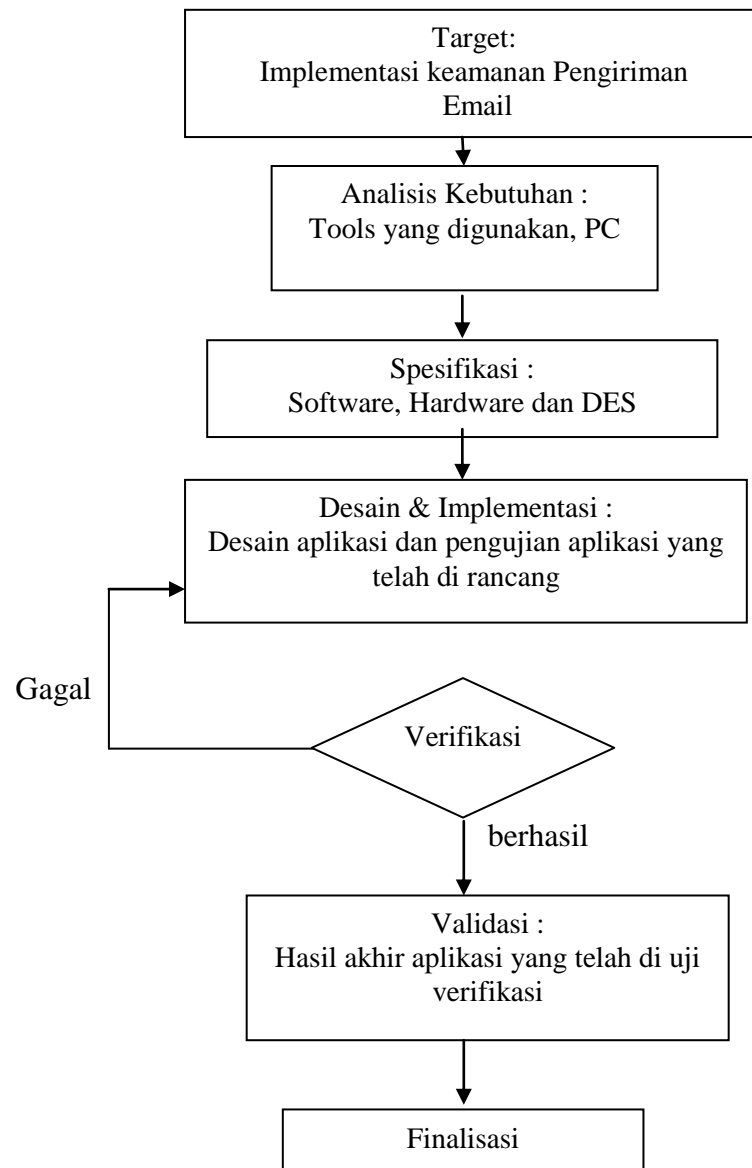
1. Memberikan informasi pengiriman email dengan penyandian atau pengkodean.
2. Mengetahui tingkat keamanan dengan penerapan kriptografi algoritma *Triple DES* .
3. Menyediakan aplikasi kriptografi dalam pengiriman email dengan kriptografi algoritma *Triple DES*.

I.4. Metodologi Penelitian

Pengumpulan data yang dilakukan penulisan terdiri dari beberapa tahapan, yaitu sebagai berikut :

1. Penelitian ini bersifat teoritis dengan cara memperoleh informasi dalam buku bacaan, jurnal, artikel yang berhubungan dengan masalah yang akan dibahas Terutama yang berkaitan dengan pengiriman email dengan implementasi keamanan menggunakan bahasa pemrograman *Java* untuk mengembangkan algoritma *Triple DES*.
2. Adapun prosedur perancangan aplikasi yang dibuat terdiri dari beberapa

tahapan, yaitu sebagai berikut :



Gambar 1.1. Prosedur Perancangan

- a. Target penelitian ini yaitu membuat Perancangan Aplikasi Pengiriman *Email* Dengan Implementasi Keamanan Menggunakan Algoritma *Triple DES*.
- b. Analisis kebutuhan, pada tahapan ini menentukan kebutuhan apa saja

untuk perancangan dan pengembangan, yaitu sebagai *tools* dalam perancangan dengan bahasa pemrograman *Java*, edisi *Java* yang digunakan adalah J2SE, SDK *Android* untuk aplikasi yang berjalan pada perangkat *PC* untuk pengembangan aplikasi Algoritma *Triple DES*.

- c. Spesifikasi dan Desain, untuk membangun dan menguji Aplikasi yang dirancang membutuhkan beberapa komponen.
- d. Hardware, komputer minimum sekelas dengan *Intel Pentium Core 2 Duo, Mouse, Keyboard, Monitor*.
- e. Implementasi dan Verifikasi, selanjutnya dilakukan pembuatan aplikasi dengan memanfaatkan masing-masing komponen. Untuk mengetahui apakah pemanfaatan masing-masing komponen sudah dapat bekerja dengan baik. Bila ada kesalahan atau kekurangan dapat diperbaiki.
- f. Validasi, Pada tahap ini dilakukan pengujian aplikasi secara menyeluruh, meliputi pengujian fungsional dan pengujian ketahanan sistem.

I.5. Keaslian Penelitian

Setiap penelitian yang dilakukan memiliki bukti keaslian, dimana keaslian tersebut juga dibandingkan dengan penelitian-penelitian yang akan dirancang. Untuk lebih jelasnya perbandingan-perbandingan tersebut dapat dilihat pada tabel I.1 sebagai berikut:

Tabel 1.1. Keaslian Penelitian

NO	Peneliti/Tahun	Judul	Hasil
1	Mandeep Singh Narula (2014)	<i>Implementation of Triple Data Encryption Standard using Verilog.</i>	Implementasi yang diusulkan dari DES dan TDES memberikan kinerja kecepatan tinggi dengan implementasi perangkat keras yang sangat kompak . Dengan membahas prosedur penuh menerapkan algoritma DES dan Triple DES menggunakan tingkat tinggi Verilog bahasa deskripsi hardware .
2	Jawahar Thakur (2011)	<i>AES, DES and Blowfish : Symetric Key Cryptography Algoritms Simulation Based Perfomance Analysis</i>	Hasil simulasi disajikan menunjukkan bahwa Blowfish memiliki kinerja yang lebih baik dari algoritma enkripsi umum lain yang digunakan . Karena Blowfish memiliki tidak ada keamanan yang kurang baik sejauh ini,. AES menunjukkan hasil kinerja yang kurang baik dibandingkan dengan algoritma lainnya karena memerlukan pemrosesan yang lebih. Menggunakan mode CBC telah menambahkan waktu pemrosesan tambahan , tapi secara keseluruhan itu relatif diabaikan terutama untuk aplikasi tertentu yang membutuhkan enkripsi yang lebih aman untuk blok data yang relatif besar . OFB menunjukkan kinerja yang lebih baik dari ECB dan CBC tetapi membutuhkan waktu pemrosesan lebih dari CFB.

I.6. Sistematika Penulisan

Secara garis besar skripsi ini terdiri dari 5(lima) bab dan beberapa lampiran. Adapun setiap bab terdiri dari sub sub dan sistematika penulisan skripsi ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini secara ringkas diterangkan mengenai latar belakang, identifikasi masalah, batasan masalah, tujuan penelitian dan manfaat penelitian, metodologi penyelesaian masalah, serta sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Bab ini membahas tentang teori yang berkaitan dengan pembuatan, desain dan tampilan Perancangan Aplikasi Pengiriman Email Dengan Implementasi Keamanan Menggunakan Algoritma *TripleDES*, serta teori-teori yang mendukung analisa penelitian.

BAB III : ANALISA DAN PERANCANGAN PROGRAM

Bab ini berisi tentang analisa dan perancangan aplikasi, yang meliputi analisa masalah, perancangan *interface*, perangkat yang digunakan, algoritma serta ketentuan penggunaan.

BAB IV : HASIL DAN PEMBAHASAN

Bab ini berisi tentang tampilan hasil impelentasi program, beserta pembahasannya, serta kelebihan dan kekurangan sistem yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Dalam bab ini diuraikan kesimpulan dan saran yang dapat diberikan untuk pengembangan aplikasi yang dirancang.