BAB I

PENDAHULUAN

I.1. Latar Belakang

Perkembangan teknologi mendorong perubahan yang cukup besar terhadap kebutuhan manusia secara luas. Kebutuhan untuk saling bertukar informasi secara lebih mudah, cepat, dan aman menjadi hal yang sangat penting. Oleh karena itulah, begitu penting peranan suatu aplikasi yang dapat memenuhi kebutuhan manusia tersebut. Agar lebih mudah mengakses, mengirim, atau bertukar informasi baik secara pribadi maupun untuk kepentingan perusahaan atau instansi [5].

Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi suatu kode yang tidak dapat dimengerti oleh pihak lain [2].

Sampai sejauh ini perkembangan teknologi informasi semakin pesat. Dalam perkembangan informasi yang paling banyak didapatkan oleh masyarakat umum adalah melalui internet. Dengan memanfaatkan jaringan internet ataupun dengan *Local Area Network* (LAN), kini pertukaran informasi bukan menjadi hal yang sulit lagi [5].

Email merupakan layanan terpenting yang diberikan oleh internet. Hampir 90% masyarakat menggunakan internet untuk membuka, membaca, dan

mengirimkan email. Email mengubah mekanisme komunikasi sehingga orang-orang dapat berkomunikasi jarak jauh dalam waktu yang relatif singkat.

RC4 merupakan salah satu jenis stream cipher, yaitu memproses unit atau input data, pesan atau informasi pada satu saat. Unit atau data pada umumnya sebuah byte atau bahkan kadang kadang bit (byte dalam hal RC4). Dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada panjang yang variabel. Algoritma ini tidak harus menunggu sejumlah input data, pesan atau informasi tertentu sebelum diproses, atau menambahkan byte tambahan untuk mengenkrip [3].
Oleh karena itulah, penulis terdorong dan berinisiatif untuk mengambil judul "**Rancang Bangun Aplikasi Kriptografi Email Gmail Menggunakan Algoritma Rc4**".

I.2. Ruang lingkup Permasalahan

Adapun beberapa tahap yang dilakukan dalam membuat ruang lingkup permasalahan adalah :

I.2.1. Identifikasi Masalah

Berdasarkan penelitian penulis sehubungan dengan materi yang penulis diangkat dalam skripsi ini, penulis menemukan beberapa masalah antara lain :

1. Rentannya keamanan data pada email gmail yang bersifat pribadi, sehingga perlu dicari pemecahannya. Pemecahan masalah ini dapat dipecahkan dengan membangun aplikasi kriptgrafi dengan menggunakan algoritma RC4.
2. Belum adanya jaminan jika sewaktu-waktu pengguna yang tidak diinginkan akan membuka isi dari email gmail tersebut.
3. Belum diketahui kehandalan algoritma RC4 dalam mengamankan informasi pada email.

I.2.2. Rumusan Masalah

Berikut rumusan masalah yang akan dicari pemecahannya melalui penulisan skripsi ini :

1. Bagaimana membuat sebuah aplikasi kriptografi yang dapat mengenkripsi dan mendekripsi file menggunakan algoritma RC4 ?
2. Bagaimana membuat sebuah aplikasi email gmail yang dapat mengirim dan menerima pesan menggunakan javascript ?
3. Bagaimana membuat sebuah aplikasi email gmail yang dapat menyisipkan file untuk dikirim serta bersama pesan di email tersebut ?

I.2.3. Batasan Masalah

Adapun batasan masalah yang penulis berikan dalam pembuatan skripsi ini adalah sebagai berikut :

1. Aplikasi kriptografi email gmail yang digunakan adalah algoritma RC4.
2. Perangkat lunak yang di bangun tidak menggunakan aplikasi database tetapi menggunkan Google drive.
3. Enkripsi gmail tidak bisa mengirim file folder, rar atau zip dikarenakan hanya berbentuk text.
4. Bahasa pemrograman yang digunakan untuk membuat aplikasi yaitu Javascript.
5. Pemodelan sistem dilakukan dengan UML 2.0.

I.3. Tujuan Dan Manfaat

Tujuan dan manfaat yang penulis peroleh dari penelitian skripsi ini adalah sebagai berikut :

I.3.1. Tujuan

Tujuan yang ingin dicapai melalui penulisan skripsi ini adalah sebagai berikut:

1. Merancang suatu aplikasi untuk menganalisa proses kebutuhan atau pun perubahan email pada gmail.
2. Membuat aplikasi ini dapat melakukan kemanan pada email tersebut.
3. Dapat menganalisa hasil keluaran dari email yang berupa kecepatan dari proses aplikasi yang dibuat.

I.3.2. Manfaat

Manfaat yang diharapkan dari penulisan skripsi ini adalah :

1. Pemahaman bagi pembaca dan pihak – pihak yang berkecimpung dalam aplikasi kriptografi email.
2. Memberikan keamanan pada email dapat disimpan diperangkat komputer yang dimiliki, sehingga tidak perlu khawatir kehilangan.
3. Peningkatan kemananan email yang signifikan karena *chipper* yang dihasilkan oleh algoritma RC4 sangat rumit untuk diproses.

I.4. Metodologi Penelitian

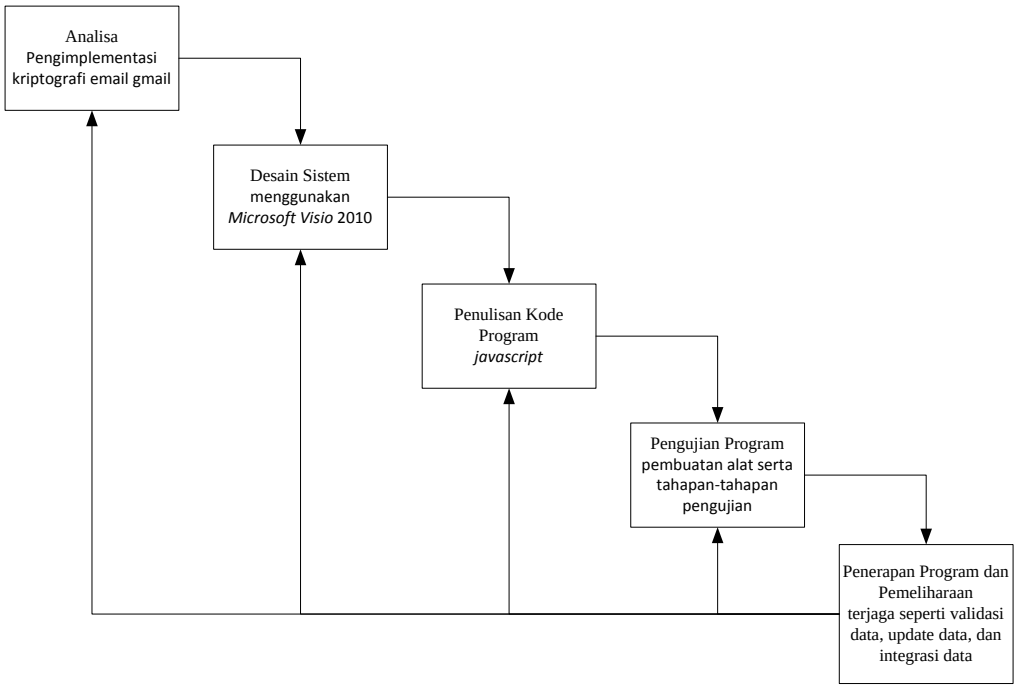
Berisikan metoda/cara/prosedur yang digunakan dalam melaksanakan penelitian serta menyelesaikan masalah yang telah didefenisikan pada poin 3 (Permasalahan). Mulai dari pengumpulan data sampai kepada terselesaikannya masalah. Ada beberapa prosedur yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Prosedur Perancangan

Merupakan tata cara dan langkah-langkah yang diperlukan untuk mencapai tujuan perancangan yang dilakukan. Langkah-langkahnya adalah:

a. Menganalisis permasalahan keamanan yang ada dalam aplikasi kriptografi.
b. Merancang sistem yang baru dengan menggunakan model UML (*Unified Modeling Language*).
c. Membuat aplikasi dengan bahasa pemrograman Javascript.

Berikut adalah skema dalam melaksanakan penelitian :



Gambar I.1. Perancangan Sistem berbentuk *Waterfall*

Pada gambar prosedur perancangan sistem di atas dapat diuraikan ke dalam beberapa tahap yaitu Tujuan Penelitian, tahap Analisa (*Analisys*), Spesifikasi, tahap Perancangan (*Design*) dan tahap Penerapan (Implementasi), Verifikasi serta tahap Validasi. Dan kegiatan yang dilakukan pada tiap-tiap tahap adalah sebagai berikut:

1. Analisis Kebutuhan

Sesuai penyelesaian masalah yang akan dilakukan, kebutuhan pokok yang harus ada pada "Perancangan Aplikasi Kriptografi Dengan Algoritma RC4*"* adalah sebagai berikut :

a. Mengimplementasikan penggunaan *Javascript* dalam membuat aplikasi Perancangan Aplikasi Kriptografi Dengan Algoritma RC4.
b. Memberikan kemudahan dan solusi cepat dalam kriptografi.

2. Desain Sistem

Setelah jelas selanjutnya dilakukan pembuatan desain aplikasi dengan menggunakan UML memanfaatkan masing-masing program. Untuk mengetahui apakah pemanfaatan masing-masing komponen sudah dapat bekerja dengan baik perlu dilakukan uji coba sementara dengan melakukan implementasi tahap awal.

3. Penulisan Pemrograman

Secara umum "*Rancang Bangun Aplikasi Kriptografi Dengan Algoritma RC4*", yang dirancang memiliki spesifikasi sebagai berikut :

a. Di bangun dengan menggunakan *Javascript* sebagai *tools* pemrogramannya.
b. Aplikasi yang dibuat dapat digunakan pada komputer, dengan *hardware* minimum adalah *processor* setara Pentium IV dan Memori 512 MB, dengan sistem operasi *Microsoft Windows XP SP3/Vista/7.*

4. Pengujian

Selanjutnya dilakukan verifikasi terhadap aplikasi yang telah masuk ke tahap implementasi tahap awal sehingga data-data yang menggunkan algoritma RC4 yang terintegrasi benar-benar telah sesuai dengan prinsip kerja aplikasi dan apa yang menjadi tujuan penulis. Dengan demikian bila ada kesalahan atau kekurangan dapat diperbaiki terlebih dahulu sebelum dirangkai menjadi kesatuan aplikasi yang utuh dan siap pakai.

5. Pemeliharaan

Pada tahap ini dilakukan pengujian aplikasi secara menyeluruh, meliputi pengujian fungsional dan pengujian ketahanan sistem. Pengujian fungsional dilakukan untuk mengetahui bahwa aplikasi dapat bekerja dengan baik sesuai dengan prinsip kerjanya. Pengujian ketahanan berkaitan dengan kemampuan aplikasi untuk dapat berjalan

I.5. Keaslian Penelitian

Sebagai bukti penelitian yang akan dibuat, maka penelitian akan dibandingkan terhadap penelitian sejenis yang pernah dilakukan perbandinganya dapat dilihat pada tabel I.1 dibawah ini :

Tabel I.1. Keaslian Penelitian

No	Materi Perbandingan	Instrumen
Penelitian pertama : Perancangan Dan Implementasi Cryptography Dengan Metode Algoritma Rc4 Pada Type File Document Menggunakan Bahasa Pemrograman Visual Basic 6.0 Hasil : Algoritma RC4 mampu melakukan proses enskripsi dan deskripsi data, dan sekaligus mampu melakukan pengompresan data sehingga data dienskripsi tersebut terdapat perubahan		
1.	Algoritma yang digunakan	RC4
2.	Penelitian	Implementasi *Cryptography Type File Document* .
3.	Basis Aplikasi	Desktop
4.	Perangkat Lunak	VB, SQL Server
Penelitian kedua : Aplikasi Kriptografi Dengan Algoritma Message Digest 5 (Md5). Hasil : Hasil pengujian digambarkan dengan tabel hasil pengujian, yang kemudian dijabarkan dengan grafik hasil uji coba terhadap file yaitu Grafik kecepatan aplikasi terhadap besar file, Grafik rerata waktu eksekusi terhadap besar file dan Tabel perbandingan kecepatan maksimum dengan kecepatan rerata terhadap besar file.		
1.	Algoritma yang digunakan	Message Digest 5 (Md5)
2.	Penelitian	Kriptografi
3.	Basis Aplikasi	Tidak Diketahui
4.	Perangkat Lunak	Tidak digunakan
Penelitian yang akan dibuat : *Rancang Bangun Aplikasi Kriptografi Email Gmail*		

Menggunakan Algoritma Rc4		
1.	Algoritma/Metode yang digunakan	RC4
2.	Penelitian	Kriptografi.
3.	Basis Aplikasi	Dekstop.
4.	Perangkat Lunak	Algoritma RC4, Java script

I.6. Sistematika Penulisan

Adapun sistematika penulisan yang diajukan dalam Skripsi ini adalahsebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metode penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan tentang teori-teori dan metode yang berhubungan dengan topik yang dibahas atau permasalahan yang sedang dihadapi.

BAB III : ANALISA DAN DESAIN SISTEM

Pada bab ini mengemukakan tentang analisa sistem yang sedang berjalan, evaluasi sistem yang berjalan dan desain sistem secara detail.

BAB IV : HASIL DAN UJI COBA

Pada bab ini menerangkan hasil dan pembahasan program yang dirancang serta kelebihan dan kekurangan sistem yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan penulisan dan saran dari penulis sebagai perbaikan di masa yang akan datang untuk sistem.