BAB I

PENDAHULUAN

I.1 Latar Belakang

Electronic Mail atau biasa yang disebut Email merupakan salah satu jenis service yang tidak bisa dilepaskan dari segala aktivitas yang terjadi di dunia maya, penggunaan email bukan hanya untuk bisnis semata tapi juga untuk social network, pengiriman pesan secara cepat, pengiriman file yang penting dan hal lainnya yang berkaitan dengan proses transfer informasi. *Microsoft Outlook* dan *Mozilla Thunderbird* merupakan aplikasi yang di khususkan untuk pengiriman dan penerimaan email dari pihak ketiga, kemudahan pengiriman dan penerimaan email sehingga bisa dibaca offline tanpa harus terhubung ke internet.

Proses pengiriman dan penerimaan email merupakan hal yang sangat penting terutama dalam hal kecepatan penerimaan dan kemudahan pengaksesan ketika offline, *Microsoft Outlook* dan *Thunderbird* sudah menerapkan penerimaan email tetapi aplikasi tersebut sangat selektif dalam pemilihan attachment email sehingga tidak semua attachment dapat dibaca

Service Mail Transfer Protocol (SMTP) merupakan layanan yang ada pada setiap sistem operasi terutama sistem operasi *Windows*, kegunaan SMTP yang ada pada *service* digunakan untuk mengirimkan email secara langsung dari windows tanpa harus menggunakan *software* khusus, pengiriman email bisa dilakukan via *Telnet* dan FTP dari *command prompt* dan biasanya prosesnya lebih cepat karena tidak membutuhkan banyak pemeriksaan, SMTP pada dasarnya sudah ada pada

sistem operasi windows dan sangat jarang dipergunakan bahkan sangat sedikit *user* yang mengetahui *service* ini ada di sistem operasi windows dan bagaimana cara penggunaannya.

Email server Adalah perangkat lunak yang berguna untuk mengatur proses pengiriman serta penerimaan email yang ada di internet. Biasanya *email server* sudah tersedia dalam layanan hosting yang ditawarkan *provider internet*, dalam pembuatan skripsi ini penulis menggunakan layanan email dari google yang bernama Yahoo mail, penggunaan yahoo mail dikarenakan layanan ini memberikan hak akses untuk proses POP3 diluar layanan aplikasi sehingga bisa berkomunikasi dengan email client pihak ketiga dalam hal ini adalah aplikasi yang penulis buat.

Yahoo mail atau dikenal juga dengan layanan email berbasis web yang disediakan oleh Google secara gratis. Layanan ini diluncurkan pada tanggal 21 Maret 2004 dan sempat membuat heboh banyak kalangan karena langsung menyediakan kapasitas email 1 GB yang pada saat itu sangat tidak wajar. Dan untuk pendaftarannya tidak terbuka untuk umum tetapi harus melalui undangan dari orang yang sebelumnya sudah mendapatkan account yahoo mempunyai beberapa kelebihan dibandingkan penyedia email lainnya diantaranya Perlindungan dari Spam, Mudah melakukan pencarian terhadap email-email Anda, Lebih mudah mengikuti diskusi, karena dibantu layout topik/*thread* yang tersusun dengan baik, Fasilitas *chatting* yang terintegrasi, Pengelompokan email dengan cara *filtering*/penyaringan, pemberian label dan bintang yang tidak

terbatas, Dapat diakses dengan ponsel (*mobile device*), Kapasitas yang besar – dan makin besar dan juga gratis.

Pengiriman pesan email pada dasarnya tidak di enkripsi hanya pengiriman emailnya yang di amankan menggunakan SSL (Secure Socket Layer) yang sudah di sediakan penyedia layanan email, tidak diamankannya pesan email tersebut menjadi salah satu masalah yang penulis bahas pada penelitian ini, untuk mengamankan pesan penulis menggunakan algoritma one time pad untuk melakukan enkripsi sehingga pesan email aman dari pihak yang tidak bertanggung jawab jika pesan email tersebut berhasil disadap.

Berdasarkan uraian di atas, penulis tertarik untuk mengajukan tugas akhir yang berjudul : **"Aplikasi Kriptografi Pada Keamanan Pesan Email Dengan Menggunakan Algoritma One Time Pad".**

I.2. Ruang Lingkup Permasalahan

Adapun Ruang Lingkup permasalahan yang akan dibahas dalam penulisan pengerjaan skripsi ini adalah sebagai berikut:

I.2.1 Identifikasi Masalah

Adapun identifikasi masalah yang ada yaitu sebagai berikut:

1. Pentingnya sebuah aplikasi kriptografi agar pesan yang penting tidak bisa dibaca oleh pihak yang tidak bertanggung jawab
2. Pengamana pesan email tersebut dibuat dengan menggunakan algoritma one time pad agar data tersebut tidak mudah diganggu isi aslinya dari seseorang yang tidak di ijinkan.

I.2.2. Rumusan Masalah

Berdasarkan uraian latar belakang terhadap masalah di atas, maka yang menjadi perumusan masalah adalah :

1. Bagaimana mengamankan pesan email dengan menggunakan algoritma kriptografi one time pad?
2. Bagaimana mengkombinasikan aplikasi pengiriman email dengan kriptografi one time pad?
3. Bagaimana mengimplementasikan algoritma one time pad pada pesan email?

I.2.3. Batasan Masalah

Mengingat keterbatasan waktu dalam penulisan dan pengumpulan data maka penulis memberikan batasan masalah untuk mempermudah penyusunan laporan yang sistematis agar mudah di pahami oleh pembaca yaitu :

1. Enkripsi hanya dilakukan pada pesan email
2. Pada implementasi perangkat lunak pesan email di enkripsi terlebih dahulu baru dikirimkan
3. Perangkat lunak yang dirancang hanya menggunakan akun google mail untuk pengiriman pesan email.
4. Algoritma kriptografi yang digunakan adalah algoritma one time pad.
5. Bahasa pemrograman yang digunakan adalah Visual Basic.Net 2010

I.3. Tujuan dan Manfaat Penelitian

Adapun yang menjadi tujuan penulisan dalam penyusunan skripsi adalah sebagai berikut :

1. Untuk mengamankan pesan dengan menggunakan kriptografi
2. Untuk mengimplementasi kriptografi dengan algoritma one time pad pada pengiriman pesan email
3. Untuk mengetahui proses pengiriman email dengan menggunakan *Service Mail Transfer Protocol*.

Sedangkan manfaat dari penulisan ini adalah sebagai berikut:

1. Menjadikan salah satu aplikasi yang bisa mengamanan pesan email dengan menyediakan fitur enkripsi dengan algoritma *one time pad*.
2. Dapat menghasilkan suatu sistem enkripsi untuk pesan email serta menerapkan ilmu tersebut dalam dunia informatika komputer, juga memberikan pengetahuan baru tentang algoritma *one time pad*.

I.4. Metode Penelitian

Dalam pelaksanaan tugas akhir ini aktivitas yang dilakukan didalamnya yaitu mengadakan eksplorasi terhadap perangkat dan konsep yang akan digunakan dalam pembangunan sistem ini, melakukan analisis terhadap permasalahan yang ada, melakukan perancangan sistem berdasarkan hasil analisis tersebut, melakukan implementasi sistem tersebut dengan perangkat yang telah ditentukan dan yang terakhir adalah mengadakan testing terhadap sistem tersebut.

Langkah-langkah yang digunakan dalam penelitian ini adalah:

1. observasi

   Pada tahap ini dilakukan eksplorasi terhadap beberapa perangkat dan konsep yang akan digunakan dalam membuat tugas akhir ini. Eksplorasi dilakukan pada beberapa perangkat yang akan digunakan untuk membangun sistem

dalam tugas akhir ini seperti *Visual Basic.Net 2010*. Eksplorasi konsep dilakukan dengan cara studi literatur yaitu dengan studi dari berbagai macam buku teks, jurnal dan skripsi.

2. Analisis Sistem.

   Pada tahap ini dilakukan analisis terhadap rumusan masalah dan batasan yang ada dalam tugas akhir ini.

3. Perancangan Sistem.

   Pada tahap ini dilakukan proses perancangan sesuai hasil analisis. Pada tahap perancangan ini dilakukan beberapa perancangan yaitu perancangan arsitektur sistem, perancangan antarmuka, perancangan modul lainnya yang akan berintegrasi dalam suatu sistem.

4. Implementasi Sistem.

   Pada tahap ini dilakukan implementasi sesuai dengan hasil perancangan. Implementasi ini dilakukan dengan menggunakan perangkat yang sudah dieksplorasi pada tahap sebelumnya. Pada proses implementasi ini dilakukan pembuatan modul-modul dalam bahasa pemrograman tertentu.

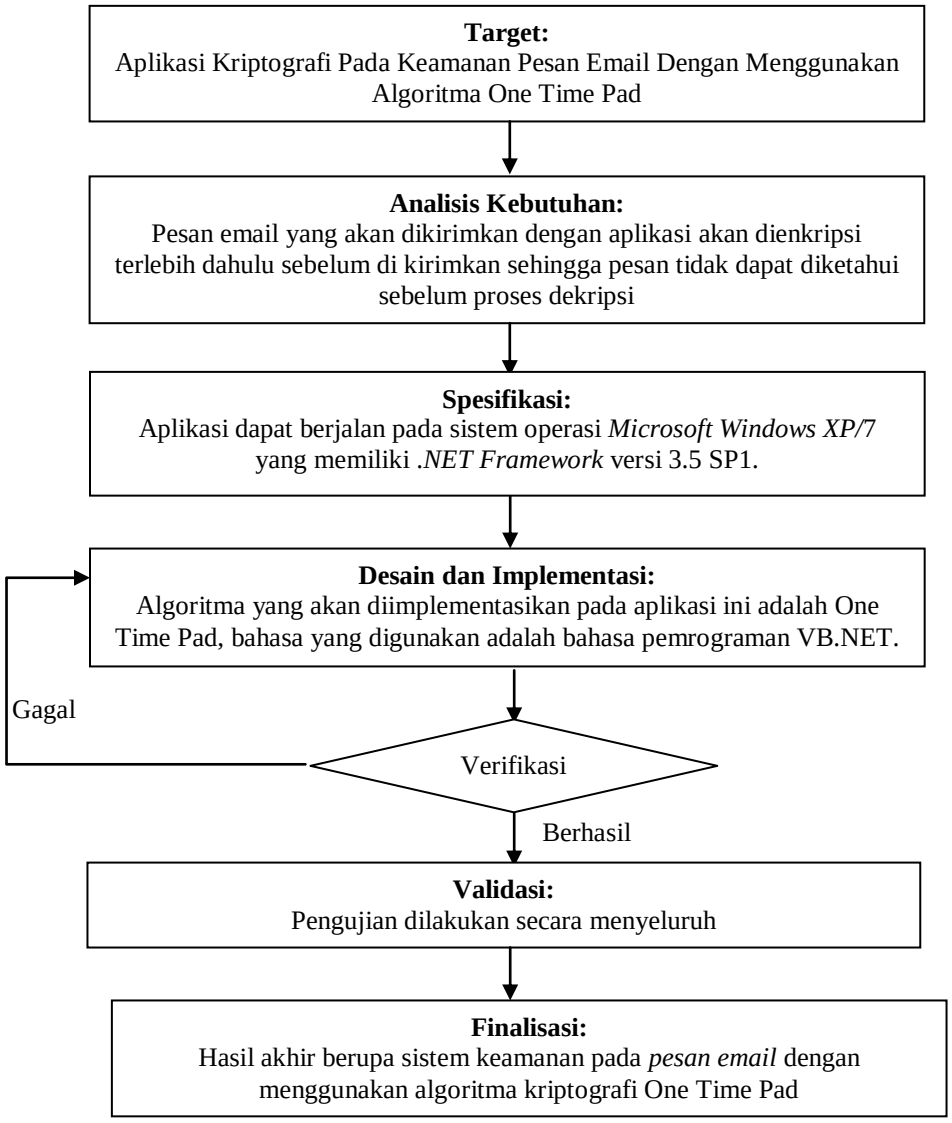
5. Testing Sistem

   Pada tahap ini dilakukan beberapa tes terhadap sistem yang telah diimplementasikan. Testing dilakukan dengan memasukkan data pengujian tertentu, untuk melihat kesiapan sistem di dunia nyata.

Selain itu juga terdapat beberapa prosedur pembuatan system sebagai berikut:

1. Prosedur Perancangan

Penelitian yang dilakukan berkaitan dengan desain dan implementasi aplikasi adalah sebagai berikut



Gambar I.1 Prosedur Perancangan

Adapun penjelasannya sebagai berikut:

1. Observasi, pada proses ini penulis melakukan survey terhadap penggunaan email terutama pada proses pengiriman email.

2. Studi Pustaka, pada tahapan ini penulis melakukan pencarian referensi dengan menggunakan buku atau pun jurnal yang penulis dapat dari berbagai sumber
3. Analisa Kebutuhan, pada tahapan ini menulis menganalisa kebutuhan data untuk sistem yang akan dirancang
4. Perancangan, pada tahapan ini penulis melakukan pembuatan sistem berdasarkan analisa kebutuhan yang sudah dirancang
5. Desain program email, penulis membuat satu bagian aplikasi untuk mengirimkan email
6. Desain program kriptografi, penulis membuat sistem menggunakan bahasa pemrograman visual basic.Net 2010 untuk melakukan enkripsi
7. Pengujian sistem, pada tahapan ini dilakukan pengujian sistem untuk memeriksa apakah sistem dapat berjalan dengan baik dan tepat atau tidak.
8. Validasi, tahapan ini dilakuakn evaluasi sistem apakah perlu dilakukan pengembangan atau tidak.

I.4.1 Keaslian Penelitian

Sebagai bukti penelitian yang akan dibuat, maka penelitian akan dibandingkan dengan penelitian sebelumnya yang memiliki kemiripan.

1. Halasson Gultom, Penyandian Email Menggunakan Algoritma Kriptografi Wake (Word Auto Key Encryption)
2. Reza Fahlevi, Perancangan Aplikasi Email - Recaiver Dengan Menerapkan metode Secure Socket Layer

3. Hengky Mulyono, Implementasi Algoritma One Time Pad Pada Penyimpanan Data Berbasis Web
4. Sugeng Sutrisno, Rancang Bangun Aplikasi Pesan Menggunakan Algoritma Vigenere Cipher Dan One Time Pad.
5. Firman Rickson Saragih, Penggunaan Kriptografi One Time Pad (Algoritma Vernam) dalam Pengamanan Informasi

Untuk detail penjelasan dari penelitian yang sudah disebutkan dapat dilihat pada tabel dibawah ini:

Tabel I.1 Tabel Perbandingan

No.	Peneliti	Judul	Hasil
1.	Halasson Gultom (2013)	Penyandian Email Menggunakan Algoritma Kriptografi Wake (Word Auto Key Encryption)	Berdasarkan penelitian yang penulis lakukan ini dapat ditarik beberapa kesimpulan antara lain 1) Proses penyandian email berupa plainteks dapat dilakukan dengan teknik enkripsi deskripsi dengan menggunakan algoritma kriptografi WAKE (Word Auto Key Encryption) sehingga pihak-pihak yang tidak bertanggung jawab tidak dapat mengetahui isi email dengan mudah. 2) Dalam penerapan metode WAKE (Word Auto Key Encryption) pada penyandian email berupa plainteks, pengirim dan pernerima harus menggunakan kunci dan jumlah rotasi kunci yang sama. 3) Penyandian email menggunakan algoritma kriptografi WAKE (Word

			Auto Key Encryption) dapat dilakukan dengan menggunakan bahasa pemograman visual basic 6.0
2.	Reza Fahlevi (2014)	Perancangan Aplikasi Email - Recaiver Dengan Menerapkanmetode Secure Socket Layer	Pada penelitian yang dibahas penulis dapat diambil kesimpulan sebagai berikut 1) Program ini dapat berjalan dengan baik sesuai dengan prosedur penerimaan email dengan Post office Protokol dan secure socket layer, penggunaan secure socket layer yang merupakan metode untuk kriptografi email dalam hal ini adalah secure socket layer Google bisa di integrasikan dengan aplikasi sehingga penerimaan email lebih aman. 2) Program dirancang dengan GUI yang menarik dan mudah dalam pengoperasiannya serta mudah digunakan dan ringan dalam penggunaan memori. 3) Program email client bisa dibuat dengan menggunakan bahasa pemrograman visual basic.net 2008 dengan ditambahkannya library net mail dan network library
3.	Hengky Mulyono (2013)	Implementasi Algoritma One Time Pad Pada Penyimpanan Data Berbasis Web	Berdasarkan pada analisis hasil pengujian terhadap implementasi algoritma One Time Pad pada aplikasi penyimpanan data dan informasi dapat di ambilkesimpulan bahwa aplikasi penyimpanan data

			dan informasi dengan mengimplementasikan algoritma OneTime Pad ini dapat menjaga keamanan dan kerahasiaan data atau informasi yang tersimpan didalamnya dan dapat memastikan bahwa user yang mengakses data maupun informasi pada sistem tersebut adalah user yang benar-benar memiliki wewenang dalam hal ini adalah pihak yang memiliki kunci dari data atau informasi yang disimpan.

I.5. Sistematika Penulisan

Langkah-langkah ataupun tahapan yang ditempuh dalam menyelesaikan penulisan skripsi ini adalah :

BAB I : PENDAHULUAN

Bab ini menjelaskan tentang Latar belakang ruang lingkup permasalahan, Tujuan dan Manfaat, Metodologi Penelitian, Lokasi Penelitian dan Sistematika Penulisan.

BAB II : TINJAUAN PUSTAKA

Bab ini menjelaskan tentang teori-teori yang berhubungan dengan program yang dirancang seperti pengertian sistem informasi, alat bantu perancangan sistem, database dan bahasa pemrograman yang digunakan.

BAB III : ANALISA DAN DESAIN SISTEM

Bab ini mengemukakan tentang analisa sistem yang sedang berjalan, evaluasi sistem yang sedang berjalan dan desain sistem yang diusulkan.

BAB IV : HASIL DAN UJI COBA

Bab ini menjelaskan tentang tampilan hasil imlementasi sistem yang diusulkan , pembahasan hasil uji coba sistem, serta kelebihan dan kekurangan sistem yang dirancang.

BAB V : KESIMPULAN

Bab ini berisi kesimpulan penulisan dan saran dari penulis sebagai referensi perbaikan dimasa yang akan datang.