BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

E-mail atau *electronic mail* merupakan suatu layanan yang digunakan oleh setiap orang di masa kini untuk bertukar informasi dengan orang lain. Informasi tersebut dapat berupa pesan, tulisan, gambar, suara, maupun file dokumen lainnya. Sebelum ada layanan email masyarakat umum yang ingin mengirimkan pesan maupun dokumen harus menggunakan suatu jasa pos maupun pengiriman barang. Namun seiring dengan perkembangan teknologi, informasi-informasi tersebut dapat dikirimkan kepada orang lain secara mudah, gratis dan aman menggunakan layanan email.

Informasi-informasi yang akan dikirimkan pasti ada suatu informasi penting tidak ingin diketahui oleh orang selain penerima pesan tersebut. Meskipun dengan tingginya sistem keamanan yang digunakan pada layanan email pasti ada kemungkinan informasi-informasi penting tersebut terkena suatu penyadapan atau pembajakan dari pihak yang tidak bertanggungjawab. Oleh karena itu diperlukan suatu metode pengamanan data didalam aplikasi email yang dapat digunakan untuk menyandikan informasi tersebut menjadi suatu informasi yang sangat sulit untuk dimengerti oleh pihak lain selain penerima pesan tersebut.

Ilmu dalam dunia komputer yang mempelajari tentang penyandian suatu informasi disebut dengan ilmu kriptografi. Dengan diimplementasikannya ilmu kriptografi didalam aplikasi email pada penulisan skripsi ini, informasi-informasi

yang akan dikirimkan ke server layanan email akan dienkripsi, sehingga pihak luar yang tidak memiliki aplikasi emaisssl yang tidak sama dengan pengirim email akan sangat sulit untuk membaca informasi yang ada didalam email tersebut.

Metode atau algoritma kriptografi yang akan digunakan pada penulisan skripsi ini merupakan pengkombinasian dua algoritma kriptografi modern tingkat tinggi yaitu algoritma RSA dan AES. Algoritma RSA dan AES sama-sama menggunakan kunci yang berbeda dalam melakukan enkripsi dan dekripsi pesan yang dinamakan dengan kunci privat dan kunci public. Dengan menggunakan dua kunci yang berbeda untuk melakukan enkripsi dan dekripsi, maka proses untuk kriptanalisis atau pembongkaran dan pembajakan informasi juga akan semakin sulit.

1.2 Rumusan Masalah

Untuk mempermudah dalam penyusunan skripsi ini maka penulis merumuskan permasalahan sebagai berikut :

1. Bagaimana membuat aplikasi desktop menggunakan Visual Studio 2015 yang memiliki kompatibilitas tinggi pada semua sistem operasi Windows?
2. Bagaimana agar pengguna bisa mengirimkan dan menerima pesan maupun file dokumen menggunakan berbagai penyedia *email*?
3. Bagaimana membuat aplikasi *email* agar dapat digunakan untuk mengirim dan menerima pesan dan berkas dokumen yang bersifat rahasia tanpa diketahui oleh pihak lain yang tidak berwenang menggunakan algoritma RSA dan AES?

1.3 Batasan Masalah

Dari rumusan masalah yang diuraikan diatas, agar hasil dari penulisan ini lebih tepat sasaran, maka permasalahan yang ada dibatasi pada pengembangan aplikasi ini secara umum menggunakan Visual Studio 2015. Sedangkan batasan pada perancangan dan pembuatan aplikasi ini adalah :

1. Aplikasi ini adalah aplikasi yang mampu mengenkripsi dan dekripsi pesan maupun file dokumen yang dibuat dengan software Visual Studio 2015.
2. Aplikasi ini mampu mengirimkan dan menerima pesan maupun file dokumen melalui beberapa penyedia *email* (*google, yahoo, microsoft*) yang dapat berfungsi dengan baik di PC desktop yang menggunakan sistem operasi *Windows*.
3. Proses pengiriman pesan email memanfaatkan *library* yang sudah ada pada C# Visual Studio 2015.
4. Proses penerimaan pesan email memanfaatkan *library* yang disediakan secara gratis oleh *Mailkit*.
5. Proses enkripsi dan dekripsi pesan maupun file menggunakan algoritma RSA dan AES dengan memanfaatkan algoritma yang sudah ada pada *library C# Visual Studio 2015*.
6. Seluruh data pada aplikasi ini tidak disimpan dalam *database* melainkan disimpan disuatu file dengan format *XML file*.

1.4 Maksud dan Tujuan Penulisan

Maksud dan tujuan yang ingin penulis capai dalam pembuatan skripsi ini adalah :

1. Menghasilkan aplikasi *E-Mail Client* yang dapat digunakan untuk menerima dan mengirimkan *E-Mail* menggunakan beberapa penyedia *email*.
2. Mengenkripsi dan dekripsi pesan maupun file lampiran *E-mail* yang akan dikirim atau *E-mail* yang sudah diterima dari pengirim *E-mail*.

1.5 Manfaat Penulisan

Manfaat yang ingin penulis capai dalam penulisan skripsi ini adalah :

1. Bagi Penulis :

   Menerapkan dan mengembangkan ilmu yang sudah dipelajari dan didapatkan saat mengikuti perkuliahan di Universitas AMIKOM Yogyakarta.
2. Bagi Masyarakat :

   Menjaga kerahasiaan dan keamanan pesan *Email* yang mungkin bersifat rahasia dan pribadi agar aman dari pencurian informasi maupun penyadapan dari pihak yang tidak bertanggungjawab.

1.6 Metode Penulisan

Metode penulisan yang digunakan penulis pada penulisan skripsi ini adalah metode SDLC atau *System Development Life Cycle*. Model SDLC yang penulis gunakan sebagai prosedur penyusunan penulisan skipsi ini adalah model *waterfall.*

1.6.1 Metode Pengumpulan Data

1.6.1.1 Metode Kepustakaan

Metode yang penulis gunakan untuk memperoleh data-data informasi dengan membaca buku-buku literatur, dokumen, jurnal dan catatan kuliah sebagai referensi dan sumber informasi yang berhubungan dengan permasalahan dalam penulisan skripsi ini

1.6.1.2 Metode Studi Literatur

Metode yang penulis gunakan untuk memperoleh data-data informasi dengan mencari informasi di berbagai situs web yang memiliki konten yang dapat dipercaya dan berkaitan dengan permasalahan dalam penulisan skripsi ini

1.6.2 Metode Analisis

Merupakan tahapan menganalisis sistem maupun aplikasi yang akan dibangun pada penulisan skripsi ini. Adapun analisis yang dimaksud adalah sebagai berikut

1.6.2.1 Analisis Kebutuhan Sistem

Analisis kebutuhan sistem terdiri dari analisis kebutuhan fungsional dan analisis kebutuhan non-fungsional dari sistem yang akan dibangun pada penulisan skripsi ini.

1.6.2.2 Analisis Kelayakan Sistem

Analisis kelayakan sistem terdiri dari analisis kelayakan teknologi, analisis kelayakan operasional, analisis kelayakan ekonomi, dan analisis kelayakan hukum.

1.6.3 Metode Perancangan

Pada tahap perancangan sistem akan dilakukan perancangan UML (*Unified Modeling Language*) untuk memvisualisasikan sistem yang akan dibuat. Setelah melakukan perancangan UML melakukan perancangan *interface* atau antarmuka aplikasi.

1.6.4 Pembuatan Aplikasi

Pada tahap pembuatan aplikasi, yang akan dilakukan adalah menerjemahkan perancangan UML dan *interface* aplikasi ke dalam bahasa pemrograman C# menggunakan software Visual Studio 2015.

1.6.5 Pengujian Sistem

Pada tahap pengujian sistem ada dua jenis pengujian yang dapat penulis lakukan, yaitu pengujian per modul (*white box*) dan pengujian sistem secara terintegrasi (*black box*).

1.7 Sistematika Penulisan

Metode penulisan laporan dan sistematika laporan bertujuan untuk mempermudah dalam penyusunanlaporan. Adapun sistematika penulisan yang digunakan dalam penulisan skripsi ini terbagi dalam beberapa pokok bahasan, adalah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini akan diuraikan mengenai latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penulisan, manfaat penulisan, metode penulisan dan sistematika penulisan.

BAB II : LANDASAN TEORI

Bab ini merupakan tinjuan pustaka yang menguraikan teori-teori yang mendukung judul dan mendasari pembahasan secara detail. Landasan teori dapat berupa definisi-definisi atau model yang langsung berkaitan dengan ilmu atau masalah yang diteliti. Pada bab ini juga akan disampaikan tentang *tools* atau *software* yang digunakan dalam pembuatan aplikasi untuk keperluan penulisan.

BAB III : ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini berisi tentang tinjauan umum yang menguraikan tentang analisa kebutuhan pada aplikasi enkripsi email dan perancangan perangkat lunak dengan menggunakan *Visual Studio 2015*.

BAB IV : IMPLEMENTASI DAN PEMBAHASAN

Pada bab ini berisi tentang implementasi dan pengujian dari perangkat lunak yang telah dibuat beserta analisis hasilnya.

BAB V : PENUTUP

Pada bab ini berisi kesimpulan dan saran. Kesimpulan digunakan untuk mengemukakan kembali masalah penulisan, menjawab pertanyaan di rumusan masalah, dan menarik kesimpulan apakah hasil yang didapat layak untuk diimplementasikan.