

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Surat adalah sarana komunikasi untuk menyampaikan informasi tertulis oleh suatu pihak kepada pihak lain. Fungsinya mencakup lima hal yaitu sarana pemberitahuan, permintaan, buah pikiran, dan gagasan; alat bukti tertulis; alat pengingat; bukti historis; dan pedoman kerja. Pada umumnya, dibutuhkan perangko dan amplop sebagai alat ganti bayar jasa pengiriman. Semakin jauh tujuan pengiriman surat maka nilai yang tercantum di perangko harus semakin besar juga.

Semakin berkembangnya teknologi, dunia kini lebih mengenal *Electronic Mail*. *E-mail* adalah surat dalam bentuk elektronik. *E-mail* merupakan salah satu fasilitas atau aplikasi internet yang paling banyak digunakan dalam hal surat-menyurat. Hal ini dikarenakan *e-mail* merupakan alat komunikasi yang murah, cepat, dan efisien. Menggunakan *e-mail* memungkinkan kita untuk mengirimkan pesan dalam bentuk surat ke seluruh dunia dalam waktu yang sangat cepat dan biaya yang murah. *E-mail* yang dikirimkan akan sampai ke alamat yang dituju sesaat *e-mail* tersebut dikirimkan. Biaya yang dikeluarkan pun hanyalah biaya untuk mengakses internet pada saat kita mengirimkan/membuka untuk menerima *e-mail* tersebut. Komunikasi menggunakan *e-mail* dilakukan dengan cara mengaktifkan

pesan yang akan kita kirim pada software yang dikhususkan untuk keperluan ini, misalnya *Microsoft Outlook*.

Selain memberikan keuntungan dan kemudahan, ada beberapa hal yang perlu di perhatikan mengenai keamanan *e-mail*. Selama *e-mail* masih menggunakan jaringan internet sebagai media penghantarnya, maka *e-mail* juga sangat rentan terhadap celah keamanan seperti yang terjadi pada jaringan internet. Berbagai macam jenis ancaman dapat terjadi pada *e-mail*. *Salah satu contoh rentannya keamanan pada e-mail adalah terjadinya penyadapan e-mail. Penyadapan pada e-mail terjadi karena pengiriman email menggunakan protokol SMTP (Simple Mail Transport Protocol). Jika kita berada pada satu jaringan yang sama dengan orang yang mengirim e-mail, atau yang dilalui oleh email, maka kita bisa menyadap email dengan memantau port 25, yaitu port yang digunakan oleh SMTP. Demikian pula untuk mengambil e-mail yang menggunakan protokol POP (Post Office Protocol). Protokol yang menggunakan port 110.*

Agar e-mail aman dari penyadapan maka perlu digunakan enkripsi untuk mengacak isi dari e-mail. Header dari e-mail tetap tidak dapat dienkripsi karena nanti akan membingungkan MTA (Mail Transfer Agent). Dengan menggunakan algoritma kriptografi seperti Caesar Cipher, Vigenere Cipher dan Base64, penulis akan merancang sebuah aplikasi yang mampu merubah isi dari e-mail ke bentuk ciphertext.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka permasalahan yang dapat dirumuskan adalah bagaimana cara merancang aplikasi Z-Mail menggunakan algoritma Caesar Cipher, modifikasi vigenere cipher dan base64 berbasis desktop?

1.3 Batasan Masalah

Batasan masalah dibuat agar pembahasan dalam perancangan aplikasi Z-Mail berbasis desktop ini tidak menyimpang dari fokus penelitiannya, berikut adalah beberapa batasan masalah yang perlu dibuat, yakni:

1. Aplikasi berbasis desktop.
2. Deskripsi adalah suatu proses dimana ciphertext di ubah ke plaintext (teks yang asli sebelum di rubah ke ciphertext).
3. Modifikasi pada judul artinya adalah merubah kembali chipertext dari Caesar Cipher ke Vigenere Cipher dan Base64 (super enkripsi).
4. Pesan yang di Enkripsi dan di Deskripsi berupa text.
5. Sistem operasi yang digunakan saat perancangan adalah Windows 10.
6. Aplikasi ini bersifat umum, dalam arti siapa saja dapat menggunakannya.
7. Aplikasi belum bisa mengenkripsi berupa media, baik itu gambar, suara dan video.
8. Pengguna hanya bisa login menggunakan account google yang sudah di setting "less secure".
9. Software yang digunakan peneliti dalam membuat aplikasi ini yaitu Micrisoft VisualStudio 2015.

1.4 Tujuan Penelitian

Tujuan dari dibuatnya aplikasi ini adalah sebagai berikut:

1. Sebagai salah satu syarat penulis untuk menyelesaikan studi dan mendapatkan gelar Sarjana.
2. Merancang suatu aplikasi yang dapat men-enkripsi suatu pesan.
3. Menghasilkan suatu aplikasi yang dapat mengenkripsi dan mendeskripsi isi *e-mail*.

1.5 Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat mencegah atau meminimalkan tindakan penyadapan yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab, sehingga pengguna *e-mail* yang merasa isi pesan yang dikirimkan penting tidak perlu resah.

1.6 Metode Penelitian

Adapun metode penelitian yang dilakukan untuk perancangan Z-mail menggunakan algoritma caesar cipher, modifikasi vigenere cipher dan base64 berbasis desktop adalah sebagai berikut:

1.6.1 Metode Pengumpulan Data

Metode kepustakaan adalah metode pengumpulan data yang dilakukan dengan cara membaca, mempelajari, mencari bahkan menulis dari sebuah buku, artikel, jurnal ilmiah, majalah baik dari media cetak maupun media elektronik yang berkaitan dengan topik yang dibahas dalam pembuatan aplikasi.

1.6.2 Metode Analisis Data

Metode analisis data bertujuan untuk melakukan analisis data yang telah dikumpulkan untuk penyusunan laporan kemudian merancang dan membuat aplikasi. Analisis data dalam penelitian meliputi:

1. Analisis kebutuhan fungsional
Merupakan pendefinisian fungsi sistem yang harus disediakan, bagaimana reaksi sistem terhadap input dan apa yang harus dilakukan sistem pada situasi khusus.
2. Analisis kebutuhan non-fungsional
Menganalisis kebutuhan pendukung bagi sistem.

1.6.3 Metode Perancangan Aplikasi

Metode perancangan aplikasi meliputi perancangan antarmuka dan perancangan algoritma yang digunakan dalam aplikasi yang akan dibuat.

1.6.4 Metode Implementasi Aplikasi

Metode ini adalah mengimplementasikan aplikasi yang sudah dirancang, yaitu implementasi menggunakan perangkat lunak menulis baris kode atau disebut *programming* untuk menghasilkan aplikasi yang akan diinginkan.

1.6.5 Metode Testing

Aplikasi yang sudah dibuat masuk dalam metode testing, metode ini digunakan untuk mendapatkan diantaranya data-data dan hasil yang diinginkan. Pada metode ini menghasilkan dokumentasi-dokumentasi dari aplikasi yang buat untuk digunakan sebagai panduan penggunaan aplikasi.

1.7 Sistematika Penulisan

Untuk memperoleh gambaran yang komprehensif dan mudah dimengerti mengenai isi penulisan skripsi ini secara umum, maka dapat dilihat dari sistematika penulisan skripsi dibawah ini:

BAB I PENDAHULUAN

Bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab landasan teori merupakan tinjauan pustaka, berisi dasar-dasar teori yang digunakan dalam penyusunan skripsi. Pada bab ini juga berisi tentang software atau tools yang digunakan dalam pembuatan aplikasi.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini menjelaskan tentang analisis terhadap kasus yang diteliti dan perancangan aplikasi yang dibuat.

BAB IV IMPLEMETASI DAN PEMBAHASAN

Bab ini memaparkan hasil-hasil dari tahapan penelitian, mulai dari analisis, desain, implementasi desain, hasil testing dan implementasi.

BAB V PENUTUP

Bab ini berisi tentang kesimpulan, saran dan kekurangan, yang diharapkan bermanfaat untuk pengembangan pembuatan program aplikasi kemana data dan informasi selanjutnya.