BAB I

PENDAHULUAN

1.1 Latar Belakang

Pesatnya teknologi saat ini menuntut masyarakat untuk selalu beradaptasi terhadap perkembangan teknologi yang ada. Kebutuhan untuk berbagi informasi secara mudah terus dikembangkan teknologinya hingga saat ini. Banyaknya aplikasi pengiriman pesan secara instan dan gratis memberikan kemudahan yang sangat bermanfaat bagi masyarakat untuk saling berbagi informasi. Salah satu metode pengiriman pesan yang banyak digunakan oleh masyarakat hingga saat ini adalah pengiriman pesan melalui *e-mail*.

E-mail (*Electronic Mail*) merupakan surat elektonik yang digunakan sebagai sarana menerima dan mengirim surat melalui jalur internet atau bisa juga diartikan surat dengan format digital (ditulis dengan menggunakan komputer atau *gedget* yang telah mendukung aplikasi *e-mail*) dan dikirimkan melalui jaringan Internet. Namun kemanan pesan yang dikirimkan secara terbuka (tanpa adanya pengubahan/enkripsi) menjadikan beberapa pesan yang seharusnya dirahasiakan menjadi mudah untuk diartiakan sebagai suatu tujuan atau kalimat yang sesungguhnya.

Menjadi sebuah kerugian jika suatu informasi yang sangat penting bisa diketahui oleh pihak-phak yang tidak berkepentingan, hal itu pernah tejadi pada sebuah perusahaan besar di Indonesia. Pada tahun 2012 terjadi sebuah kasus

pembobolan *email* pada grup Bakrie Tbk. Kasus yang pernah diselidiki oleh kepolisian Indonesia ini diduga dilakukan dengan sengaja oleh *hacker* untuk mencuri suatu informasi, menurut Karopenmas Polri Brigjen Boy Rafli Umar, kasus tersebut sudah ditangani oleh tim *cyber* Polda. "Dari laporan awal yang diterima sepertinya ada dugaan tindak pidana ITE (Informasi dan Transaksi Elektronik), sebagaimana diatur UU 11/2008, saat ini sedang ditelusuri," ujar Boy, kepada wartawan, Rabu (12/12/2012).[1]

Oleh karena itu pada penelitian kali ini peneliti akan mencoba untuk merancang suatu aplikasi yang mendukung enkripsi kriptografi pada pengiriman pesan melalui *e-mail*. Pada penelitian ini peneliti akan mencoba membuat sebuah aplikasi enkripsi pesan email dengan menerapkan dua algoritma yaitu Vigenere dan RSA (Rivest, Shamir, Adleman), diharapkan hasil dari penelitian ini dapat mendukung keamanan komunikasi yang menggunakan fasilitas *email* sebagai media pengirimnya.

1.2 Rumusan Masalah

Berdasar latar belakang yang telah peneliti buat maka dari itu rumusan masalah pada penelitian ini adalah : Bagaimana merancang dan menggabungkan dua algoritma kriptografi yaitu Vigenere dan RSA pada sebuah aplikasi pengiriman pesan *e-mail* ?

1.3 Batasan Masalah

Batasan masalah yang diterapkan pada aplikasi enkripsi pesan e-mail dengan algoritma kriptografi Vigenere dan RSA adalah sebagai berikut :

1. Algoritma yang diterapkan pada aplikasi untuk enkripsi adalah Vigenere Chiper dan RSA.
2. Aplikasi hanya mendukung untuk pengiriman pesan melalui *e-mail*.
3. Karakter emotikon hanya akan menggantikan bentuk dari huruf dan angka.
4. Pengujian bilangan prima yang dipakai adalah *Fermat's Little Theorem*.
5. Aplikasi ini dibangun dengan bahasa pemrograman *Java Script* dan PHP.

1.4 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut :

1. Merancang sebuah aplikasi pengiriman pesan *e-mail* dengan enkripsi kriptgrafi
2. Mencoba untuk mengkombinasikan dua algoritma kriptografi yaitu algoritma RSA dan Vigenere.
3. Mencoba untuk memodifikasi hasil enkripsi pesan pada algoritma Vigenere chiper dengan emotikon

1.5 Manfaat Penelitian

Adapun manfaat yang ingin dicapai dari penelitian ini adalah sebagai berikut :

1. Menambah pengetahuan peneliti pada bidang kriptografi khususnya pada algoritma Vigenre dan RSA.
2. Membuat inovasi baru pada bidang kriptografi.
3. Menjadi referensi untuk penelitian selanjutnya pada bidang kriptografi.
4. Dengan adanya aplikasi untuk enskripsi pesan berbasis *e-mail* ini diharapkan pengguna dapat menerapkanya untuk meningkatkan penjagaan dan kerahasiaan pesan yang akan dikirmkan.

1.6 Metode Penelitian

Berikut adalah tahapan yang dilakukan dalam penelitian ini :

1. Studi Literatur

   Sebelum memulai penelitian ini terlebih dahulu peneliti akan mencoba untuk mempelajari literatur melalui buku, jurnal, artikel, makalah maupun situs internet yang membahas tentang kriptografi dengan algoritma Vigenere dan juga RSA.

2. Analisis dan Perancangan Sitem

   Pada tahap ini peneliti akan melakukan analisis sistem dengan metode SWOT terhadap aplikasi sesuai dengan batasan masalah dan tujuan yang akan dicapai dari pengujian aplikasi kriptografi dengan algoritma Vigenere dan juga RSA, setelah itu dilakukan perancangan *flowchart*

serta *interface* dan perancangan sistem yang dapat menerapkan enkripsi gabungan sesuai dengan algoritna RSA dan Vigenere yang telah dimodifikasi.

3. Implementasi Sistem

   Pada tahap ini akan dilaksanakan pengkodean (*coding*) dengan merancang interface *website* terlebih dahulu menggunakan HTML dan CSS dan proses sistem dengan Java Script dan PHP pada aplikasi untuk meng-enkripsi pesan e-mail.

4. Pengujian Sistem

   Pada tahap pengujian sistem, peneliti akan mencoba aplikasi yang telah dibangun apakah sudah sesuai dengan algoritma yang diterapkan yaitu penggabungan algoritma Vigenere dan RSA.

5. Dokumentasi

   Dalam tahap ini dilakukan penyusunan laporan hasil dari analisis dan perancangan aplikasi dalam format penulisan penelitian.

1.7 Sistematika Penulisan

Sistematika penulisan skripsi ini terdiri atas bagian-bagian berikut :

BAB I : PENDAHULUAN

Bab ini menjelaskan tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian yang akan diterapkan dan sistematika penulisan serta rencana kegiatan dari skripsi ini.

BAB II : LANDASAN TEORI

Bab ini menjelasakan landasan teori dari penelitian yang dilakukan. Teori yang diangkat yaitu kriptografi dan keamanannya, algoritma Vigenere Chiper dan algoritma RSA (*Rivest, Shamir, Adleman*).

BAB III : ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini akan dijelaskan analisis terhadap proses enkripsi kriptografi gabungan dengan algoritma Vigenere dan RSA yang diterapkan pada aplikasi dan dilakukan analisis terhadap tingkat keamanan yang dihasilkan dari gabungan kedua algoritma tersebut.

BAB IV : IMPLEMENTASI SISTEM

Pada bab ini akan menguraikan hasil pengujian aplikasi yang telah dibuat serta dan hasil enrkripsi dari algoritma gabungan Vigenere dan RSA.

BAB V : KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang didapat dari hasil pengujian yang dilakukan serta saran-saran yang diberikan untuk penelitian selanjutnya.