BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Dunia teknologi saat ini mengalami perkembangan yang pesat hingga sekarang. Teknologi yang saat ini berkembang pesat justru membuat *cybercrime* menjadi lebih agresif dalam melakukan tindak kejahatan terutama di dunia maya. Tentu kejahatan dalam dunia maya merupakan hal yang sangat merugikan baik bagi pengguna internet maupun penyedia jasa internet. Banyak informasi penting baik yang dipublikasikan maupun yang bersifat rahasia. Namun kenyataannya banyak kasus pencurian data atau penyadapan data yang sangat rahasia bisa dibobol oleh pihak yang tidak bertanggung jawab yang biasa dikenal sebagai *cybercrime*. Untuk mengamankan data penting yang berupa informasi tersebut dibutuhkan suatu kriptografi.

Teknologi pada jaman sekarang banyak dilingkupi oleh kriptografi. Mulai dari percakapan telepon genggam, akses internet, sampai aktivitas transaksi di ATM telah menggunakan kriptografi. Oleh karena itu sangat penting kriptografi untuk keamanan informasi, sehingga jika berbicara mengenai masalah keamanan yang berkaitan dengan penggunaan komputer, maka tidak akan bisa dipisahkan dari kriptografi. Ilmu kriptografi juga telah mengalami perkembangan yang cepat, hal ini dikarenakan perkembangan teknologi informasi yang juga semakin cepat terutama pada aspek keamanan data.

Email merupakan layanan terpenting yang diberikan internet. Mayoritas masyarakat menggunakan internet untuk membaca dan mengirim *email*. *Email* mengubah mekanisme komunikasi sehingga orang-orang dapat berkomunikasi jarak jauh dalam waktu yang relatif singkat.

Kriptografi juga digunakan dalam proses pengiriman *email*. Jika *email* dikirim melewati jaringan *public* maka tingkat keamanannya sangat beresiko. Teknik-teknik pencurian informasi dari sebuah *email* ini semakin canggih dari hari ke hari. Salah satunya adalah serangan *Man-In-The Middle*. Kriptografi akan sangat membantu memberikan keamanan informasi *email* kita, walaupun *attacker* atau *Man-In-The Middle* berhasil mendapatkan teks yang kita kirim namun tidak bisa mendapatkan informasi yang akurat karena teks yang didapat sudah ter-enkripsi sebelumnya. Sedangkan *Chiperteks* yang didapat hanya bisa dibuka oleh pihak yang memiliki kunci *private* (Kunci untuk dekripsi).

Masalah yang sampai saat ini marak terjadi yaitu kasus *phishing mail*. *Email phising* adalah upaya memperoleh atau "mengelabui" informasi agar pelaku kejahatan di dunia maya dapat mencuri uang atau identitas seseorang (*target phising*). *Email* tersebut terlihat sama dengan *email* asli dari perusahaan ternama seperti paypal, bank, web olshop, game, bahkan sosial media. Cara pelaku melakukan aksinya dengan mengirimkan informasi ke target yang berisi notifikasi berupa alasan akan memperbarui informasi pribadi atau mengkonfirmasi sandi target *phising*.

Permasalahan tersebut dapat diatasi dengan proses enkripsi. Salah satu enkripsi yang cukup dikenal adalah dengan metode enkripsi AES (*Advanced Encryption Standar*). Metode enkripsi AES ini akan memberikan *private key* yang digunakan dalam proses enkripsi dan dekripsi. Aplikasi enkripsi *email* ini dibangun dengan berbasis web. Sehingga diharapkan aplikasi ini dapat menjaga kerahasiaan informasi-informasi penting dan dapat diakses dengan mudah oleh penggunanya.

Berdasarkan permasalahan tersebut, maka penulis mengangkat skripsi dengan judul "**Aplikasi Enkripsi dan Dekripsi Email menggunakan Algoritma Advanced Encryption Standar berbasis Web**".

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan, maka perlu dirumuskan suatu masalah yang akan dipecahkan/diselesaikan pada penelitian/perancangan ini. Adapun pokok permasalahan dalam penelitian ini adalah bagaimana membuat aplikasi enkripsi dan dekripsi berbasis web yang mengimplementasikan algoritma kriptografi AES dalam melindungi pesan maupun dokumen yang dikirim melalui *email*.

1.3 Batasan Masalah

Agar masalah yang diteliti tidak menyimpang maka diperlukan suatu batasan masalah. Adapun batasan masalah pada penelitian ini adalah sebagai berikut :

1. Aplikasi ini dibangun dengan berbasis web.
2. Aplikasi ini menggunakan algoritma kriptografi AES dalam proses enkripsi dan dekripsi pesan dan dokumen.
3. Inputan pada aplikasi berupa teks tertulis dan dokumen.
4. Sistem operasi yang digunakan dalam pembuatan aplikasi ini menggunakan windows 7.
5. Pembuatan program pendukung aplikasi kriptografi AES menggunakan bahasa pemrograman HTML, CSS, Javascript dan PHP.
6. Pesan dapat dienkripsi/didekripsi jika user sama-sama menggunakan aplikasi ini.
7. Akun *email* yang dapat digunakan dalam aplikasi ini hanya akun gmail.

1.4 Maksud dan tujuan penelitian

Untuk menunjang penguasaan ilmu yang telah diberikan oleh lembaga pendidikan Universitas AMIKOM Yogyakarata, yang berorientasi pada Teknologi Informasi dan Komputerisasi. Adapun maksud dan tujuan yang ingin dicapai dari penelitian ini adalah :

1.4.1 Internal

Pengertian tujuan internal yang dimaksud adalah dilihat dari sisi penulis. Dalam hal ini penulis sebagai mahasiswa Universitas Amikom Yogyakarta adalah sebagai berikut:

1. Sebagai persyaratan untuk memperoleh gelar Strata-1 Jurusan Teknik Informatika dan Komputer Universitas AMIKOM Yogyakarta.
2. Menerapkan ilmu teoritis yang didapat selama mengikuti pendidikan di Universitas AMIKOM Yogyakarta.
3. Sebagai tolak ukur sejauh mana ilmu yang didapat diperkuliahan dapat diterapkan kedalam lingkungan permasalahan yang sebenarnya dengan cara terlibat langsung dalam proses pembuatan aplikasi.
4. Memperluas serta meningkatkan kemampuan mahasiswa sebagai bekal untuk memasuki dunia kerja.

1.4.2 Eksternal

Bagi masyarakat luas dan dunia pendidikan pada umumnya penelitian ini mempunyai tujuan sebagai berikut:

1. Adanya implementasi dan hasil analisa yang mampu ditunjukkan sebagai bukti bahwa algoritma kriptografi AES mampu digunakan sebagai aplikasi yang bisa merahasiakan pesan *email* dan dokumen yang sulit dipecahkan dengan perhitungan tanpa bantuan komputer.
2. Menghasilkan sebuah aplikasi berbasis web yang berfungsi untuk mengenkripsi dan dekripsi pesan *email* serta dokumen dengan algoritma kriptografi AES berbasis web.
3. Sebagai bahan penelitian yang dapat dikembangkan dan diperbaiki pada penelitian berikutnya.

1.5 Manfaat Penelitian

Manfaat yang akan didapat dari penelitian ini adalah sebagai berikut :

1. Dapat memberikan perlindungan terhadap informasi pesan maupun dokumen agar tidak mudah untuk diakses oleh pihak-pihak yang tidak bertanggung jawab.
2. Pengguna aplikasi tidak perlu khawatir lagi terhadap *email phising* yang sengaja ingin mencuri data dan informasi penting.
3. Dapat digunakan sebagai bahan kajian untuk mengembangkan teknologi informasi terutama faktor yang berhubungan dengan keamanan.

1.6 Metode Penelitian

Penulis melakukan beberapa metode penelitian dan mengumpulkan data untuk memperoleh jawaban atas permasalahan yang penulis ungkapkan. Adapun metode-metode yang penulis lakukan adalah sebagai berikut :

1.6.1 Metode Pengumpulan data

Metode pengumpulan informasi dan data yang digunakan dalam penelitian ini diantaranya :

1.6.1.1 Metode Studi Kepustakaan

Untuk mendukung perancangan aplikasi penulis menggunakan metode studi kepustakaan sebagai referensi. Pustaka yang digunakan antara lain buku-

buku literatur, dokumen, catatan kuliah atau penelitian sebelumnya yang berkaitan dengan penelitian ini.

1.6.1.2 Metode *Browsing*

Metode *browsing* yaitu teknik pengumpulan rujukan yang bersumber dari internet dengan mengunjungi situs yang berhubungan dengan penelitian ini.

1.6.2 Metode Analisis

Metode analisis yang digunakan dalam penelitian ini adalah analisis SWOT.

1.6.2.1 Analisis SWOT

Analisi SWOT adalah singkatan dari (*Strengths, Weakness, Opportunities, Threats*) yaitu menganalisa kekuatan, kelemahan, peluang dan ancaman dalam hasil penelitian ini.

1.6.2.2 Analisis Kebutuhan Sistem

Analisis kebutuhan sistem adalah beberapa kebutuhan dalam sistem untuk mendukung jalannya proses pembuatan dan kinerja aplikasi yang dibuat.

1.6.2.3 Analisis Kelayakan Sistem

Analisis kelayakan adalah untuk menentukan layak tidaknya aplikasi dibuat. Anilisis kelayakan yang digunakan adalah dari segi teknologi, operasional, dan hukum.

1.6.3 Metode Perancangan

Metode perancangan yaitu dengan menggunakan perancangan UML (*Unified Modelling Language*), *flowchart*, dan *User Interface*.

1.7 Sistematika Penulisan

Sistematika laporan disusun menggunakan dasar-dasar penulisan karya ilmiah. Metode ini dilakukan agar dalam penyusunan laporan menjadi lebih teratur dan mudah diahami. Sistematika penulisan laporan pada skripsi adalah sebagai berikut :

BAB I : PENDAHULUAN

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

BAB II : LANDASAN TEORI

Bab ini membahas tentang tinjauan pustaka dan dasar-dasar teori yang digunakan.

BAB III : ANALISIS DAN PERANCANGAN SISTEM

Bab ini menjelaskan tentang analisis sistem, analisis kebutuhan sistem,analisis kelayakan sistem dan perancangan sistem yang diusulkan.

BAB IV : IMPLEMENTASI DAN PEMBAHASAN

Bab ini membahas mengenai hasil program yang akan diimplementasikan ke dalam perangkat komputer.

BAB V : PENUTUP

Bab ini berisi tentang kesimpulan dari keseluruhan laporan dan saran yang membangun untuk menambah kesempurnaan aplikasi.