BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada era digital, komunikasi melalui jaringan komputer memegang peranan penting. Melalui komunikasi elektronik, seseorang dapat melakukan transaksi atau komunikasi dengan sangat cepat dan praktis. Hal ini merupakan pengaruh dari perkembangan yang sangat signifikan dalam teknologi informasi yaitu dengan *bandwidth* internet yang semakin besar dan biaya akses yang semakin murah. Konsekuensinya adalah resiko dalam keamanan data semakin meningkat. Keamanan data merupakan perlindungan data pada suatu sistem dari serangan seperti modifikasi data, otorisasi yang tidak sah, atau perusakan data itu sendiri.

Salah satu cara yang dapat digunakan untuk melindungi kerahasiaan data adalah dengan menerapkan ilmu kriptografi. Kriptografi berasal dari bahasa Yunani, "*kryptós*" yang berarti tersembunyi dan "*gráphein*" yang berarti tulisan. Sehingga kata kriptografi dapat diartikan berupa frase "tulisan tersembunyi". Pada dasarnya, kriptografi berkaitan dengan informasi, baik disimpan sebagai data atau dikomunikasikan dengan orang lain[1]. Salah satu algoritma yang digunakan untuk proses kriptografi adalah algoritma RC4. Algoritma ini merupakan salah satu algoritma *stream cipher* paling populer dan dianggap sebagai algortima *stream cipher* tercepat dan termudah untuk diterapkan [2]. Namun, disamping kemudahan dalam penggunaannya, sejumlah serangan ditemukan pada algoritma

ini. Salah satu serangan yang paling populer adalah *Bit Flipping Attack*. Guna menanggulangi serangan yang didapatkan, maka dilakukan modifikasi pada algoritma RC4 [3]. *Bit Flipping Attack* adalah serangan yang bertujuan untuk mengetahui sebagian atau keseluruhan *plaintext* dari *ciphertext* tanpa harus mengetahui kunci.

Salah satu komunikasi yang dilakukan melalui jaringan komputer, adalah pertukaran pesan melalui *email*. Proses penerimaan dan pengirimaan *email* dilakukan melalui jalur publik. Pada proses tersebut pesan yang dikirimkan berbentuk asli tanpa adanya perlindungan. Jika pesan tersebut bersifat rahasia atau bersifat pribadi yang tidak boleh diketahui oleh pihak lain, maka diperlukan pengamanan dari serangan-serangan yang dapat merugikan.

Saat ini, Gmail merupakan aplikasi *email* yang banyak digunakan. Sebagai perusahaan peyedia layanan Gmail, Google LLC sebuah perusahaan multinasional Amerika Serikat yang berkekhususan pada jasa dan produk internet[4], mengklaim bahwa jumlah perangkat aktif dengan sistem operasi Android kini menembus lebih dari 2,5 miliar per bulan[5].

Berdasarkan kebutuhan dan kondisi yang telah disebutkan di atas maka dibutuhkan sistem pengamanan isi pesan, baik pada saat pengiriman maupun penerimaan *Gmail*. Maka dalam penyusunan tugas akhir ini, akan dibangun aplikasi kriptografi dengan mengimplementasikan algoritma *Modified RC4*. Dengan kriptografi data dapat diubah menjadi sandi-sandi yang tidak di mengerti melalui proses enkripsi, kemudian dapat dikembalikan ke bentuk semula melalui proses dekripsi.

1.2 Perumusan Masalah

Berdasarkan uraian tersebut di atas, dalam pengerjaan tugas akhir ini muncul beberapa permasalahan diantaranya adalah :

1. Bagaimana cara untuk melindungi informasi yang dikirim melalui *email* sehingga tidak dapat dibaca oleh pihak-pihak yang tidak berkepentingan?
2. Bagaimana menerapkan algoritma *Modified RC4* untuk mengamankan isi pesan pada saat pengiriman dan penerimaan *email*?

1.3 Tujuan dan Manfaat

Adapun tujuan dari tugas akhir ini adalah sebagai berikut :

1. Mengimplementasikan metode *Modified RC4* untuk mengenkripsi dan dekripsi data dan informasi terhadap media *email* berbentuk teks.
2. Memahami proses algoritma *Modified RC*

Sedangkan manfaat dari tugas akhir ini adalah sebagai pencegahan dari serangan-serangan terhadap pesan rahasia atau pribadi oleh pihak yang tidak berkepentingan.

1.4 Ruang Lingkup

Adapun ruang lingkup yang dibahas pada tugas akhir ini adalah :

1. Aplikasi dibuat berdasarkan *web based* dan *responsive* sehingga memungkinkan untuk diakses baik melalui komputer pribadi ataupun

smartphone (*handphone* atau tablet) dengan tampilan yang akan menyesuaikan.

2. Data yang akan dienkripsi dan dekripsi berbentuk teks
3. Metode algoritma kriptografi yang digunakan adalah *Modified RC4*
4. Bahasa pemrograman yang digunakan adalah ASP.NET
5. Layanan *Email* yang akan diimplementasikan kriptografi adalah Gmail.
6. Kriptografi diimplementasikan pada *body emaill*
7. Data *email* dari *inbox* dan *sent items* yang akan ditampilkan sebanyak sepuluh pesan per halaman. Pembatasan data yang tampilkan ini untuk memercepat proses *loading* halaman.

1.5 Metodologi

Cara atau metode pendekatan yang dilakukan untuk penyelesaian tugas akhir ini adalah sebagai berikut :

a. Studi Literatur

Pada tahapan ini dilakukan studi terhadap hasil karya ilmiah yang berhubungan dengan kriptografi secara umum, perkembangan kriptografi pada dari masa ke masa, pengkodean teks menjadi data biner, protokol untuk menerima dan mengirimkan *email*, alat dan teknologi yang digunakan, serta algortima yang diimplementasikan untuk membangun aplikasi kriptografi tersebut.

b. Analisis

Pada tahapan ini dilakukan identifikasi kebutuhan dan persyaratan sistem serta dilakukan pemodelan hasil analisis. Model analisis dibuat menggunakan pendekatan berorientasi objek dengan menggunakan notasi UML. Notasi yang digunakan diantaranya yaitu *Class Diagram*, *Use Case Diagram*, *Sequence Diagram*, dan *Activity Diagram*.

c. Perancangan

Pada tahap perancangan maka akan dilakukan pemodelan rancangan berupa perancangan arsitektur, perancangan navigasi menu, perancangan antar muka serta perancanan algortima.

d. Implementasi

Pada tahapan ini dilakukan pengimplementasian hasil rancangan menjadi kode dalam bahasa pemrograman ASP .Net. Pada bagian ini dijelaskan bagaimana mengimplementasikan algoritma, struktur data, serta antarmuka hasil rancangan menjadi kode program dalam sintaks bahasa pemrograman tertentu.

e. Pengujian

Pada tahapan ini dilakukan pengujian terhadap kesesuaian implementasi program terhadap kebutuhan yang telah ditentukan. Pengujian yang ditempuh melalui metode *white box* dengan meggunakan *tools* NUnit pada framework .Net , serta metode *black box* testing dengan meguji hasil teks enkripsi dan dekripsi yang tampil pada layar antar muka.

1.6 Sistematika Penulisan

Untuk memudahkan dalam memahami isi laporan, maka dibuatlah sistematika penulisan yang terbagi menjadi enam bab sebagai berikut :

BAB I : PENDAHULUAN

Dalam bab ini diuraikan mengenai latar belakang masalah, perumusan masalah, tujuan dan manfaat, ruang lingkup pembahasan, metoda penelitian serta sistematika penulisan.

BAB II : LANDASAN TEORI

Dalam bab ini diuraikan mengenai landasan-landasan yang akan digunakan untuk pendukung pengerjaan tugas akhir. Di dalamnya memuat pengertian dan sifat yang diperlukan untuk pembahasan di bab berikutnya.

BAB III : ANALISA DAN PERANCANGAN

Bab ini akan membahas secara rinci mengenai identifikasi kebutuhan dan persyaratan sistem beserta pemodelannya serta membahas secara rinci mengenai perancangan aplikasi yang meliputi rancangan arsitektur, rancangan menu, rancangan antar muka, serta rancangan algoritma.

BAB IV : IMPLEMENTASI DAN PENGUJIAN

Bab ini berisikan penjelasan mngenai implementasi algoritma, struktur data, serta antarmuka hasil rancangan menjadi kode program dalam sintaks bahasa pemrograman tertentu. Kemudian setelah pembahasan implementasi, selanjutnya akan dibahas mengenai pengujian terhadap aplikasi yang dibuat.

BAB V : PENUTUP

Bab ini berisi kesimpulan yang diambil setiap tahap pengembangan perangkat lunak dan saran-saran yang dapat digunakan untuk pengembangan dan perbaikan di kemudian hari.