BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Saat ini ilmu pengetahuan berkembang semakin pesat, menciptakan sebuah era yang modern, dimana untuk mengirim surat cukup menggunakan *email*, untuk berbelanja suatu barang cukup memesan secara *online*, dan untuk mengirim dana cukup dengan menggunakan layanan *online* yang disediakan oleh setiap bank. Namun dalam penggunaan internet tersebut, memungkinkan pihak ketiga untuk mencuri data-data penting, seperti *email*, informasi kartu kredit, *password* akun media sosial, dan lain sebagainya. Oleh karena itu pihak penyedia layanan perlu mengamankan pesan tersebut dengan mengubahnya ke dalam bentuk pesan yang tidak dapat dimengerti oleh orang lain sehingga saat pesan tersebut dicuri, pesan tersebut akan tetap aman. Ilmu yang berhubungan dengan masalah tersebut adalah kriptografi. Kriptografi adalah seni menulis dan memecahkan suatu kode (*Concise Oxford Dictionary*, 2006).

Konsep kriptografi telah digunakan sejak zaman dahulu oleh Julius Caesar dan terus berkembang sampai saat ini. Berdasarkan era-nya kriptografi terbagi menjadi dua bagian, yaitu kriptografi klasik dan kriptografi modern. Persamaan dari keduanya adalah sama-sama menggunakan konsep matematika dalam teknik pembuatan dan pemecahan suatu pesan. Tetapi dalam kriptografi klasik, konsep matematika yang dipakai masih sangat sederhana, seperti substitusi, permutasi dan transpos. Sedangkan dalam kriptografi modern konsep matematika yang digunakan sudah tidak sederhana lagi, seperti polinom, bilangan prima, grup, ring dan lapangan. Kelebihan dari kriptografi klasik adalah kemudahannya dalam mengenkripsi pesan, tetapi beberapa teknik pengenkripsiannya juga memiliki kelemahan yang cukup fatal yaitu sangat mudah untuk dipecahkan. Contoh kriptografi klasik yang sangat mudah dibuat dan dipecahkan adalah Caesar *Cipher* yang hanya memiliki kunci yang mungkin sebanyak 26 buah. Caesar *Cipher* termasuk kedalam enkripsi *Substitution Cipher*, dimana kode atau naskah acak didapatkan dengan mengganti setiap karakter pada naskash asli. Algoritma enkripsi klasik yang baik adalah algoritma yang tahan terhadap

known plaintext attack dan analisa statistik sehingga pencarian kunci harus dilakukan dengan *brute force search* (Kromodimoeljo. 2010). Contoh algoritma enkripsi kriptografi klasik yang baik adalah *Row Transposition Cipher* yang memiliki kunci yang mungkin sebanyak n! (n faktorial). *Row Transposition Cipher* termasuk ke dalam enkripsi *Transposition Cipher*, dimana naskah acak didapatkan dengan mengubah urutan karakter pada *plaintext* dengan permutasi tertentu.

Dari latar belakang tersebut, akan dikembangkan suatu teknik enkripsi kriptografi klasik dalam hal ini Caesar *Cipher* menggunakan penggabungan dengan metode enkripsi *Row Transposition Cipher*. *Row Transposition Cipher* dipilih karena memiliki keamanan dalam pengenkripsian yang baik. Sehingga pengenkripsian gabungan antara enkripsi Caesar *Cipher* dan *Row Transposition Cipher* dapat memenuhi kriteria pengenkripsian kriptografi klasik yang baik sebab jumlah kunci yang mungkin dari pengenkripsiannya lebih banyak dari enkripsi *Row Transposition Cipher* sendiri. Selanjutnya, setelah pengenkripsian Caesar *Cipher* ditingkatkan keamanannya, metode pengenkripsian tersebut akan diterapkan dalam program aplikasi pengirim *email*. Aplikasi pengirim *email* dipilih agar dapat mengantisipasi pembobolan akun *email* yang marak terjadi, dengan aplikasi pengirim *email* ini diharapkan pesan dalam akun *email* pengguna lebih aman walaupun *hacker* atau peretas berhasil membobol akun *email* pengguna, sebab *email* yang dikirimkan merupakan pesan yang sudah diacak yang hanya dapat dibaca oleh pemilik kunci enkripsi. Berdasarkan pemaparan tersebut, maka judul dari penelitian ini adalah "Aplikasi Pengirim *Email* dengan Penerapan Enkripsi Caesar *Cipher* yang Telah Ditingkatkan Keamanannya Menggunakan Enkripsi *Row Transposition Cipher*".

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang yang dipaparkan pada subbab sebelumnya, rumusan masalah yang diajukan pada penelitian ini adalah:

a. Bagaimana cara meningkatkan keamanan pengenkripsian *Caesar Cipher* menggunakan enkripsi *Row Transposition Cipher* sehingga memenuhi

kriteria pengenkripsian kriptografi klasik yang baik dan kuat terhadap serangan *brute force search*?

b. Bagaimana mengkontruksi program aplikasi untuk pengiriman *email* berupa *ciphertext* yang telah dienkripsi dengan Caesar *Cipher* yang telah ditingkatkan keamanannya?

1.3 Tujuan

Berdasarkan rumusan masalah di atas, maka tujuan dari penelitian ini adalah sebagai berikut:

a. Mengetahui cara meningkatkan keamanan pengenkripsian Caesar *Cipher* menggunakan enkripsi *Row Transposition Cipher* sehingga memenuhhi kriteria pengenkripsian kriptografi klasik yang baik dan kuat terhadap serangan *brute force search.*
b. Mengkontruksi program aplikasi untuk pengiriman *email* berupa *ciphertext* yang telah dienkripsi dengan Caesar *Cipher* yang telah ditingkatkan keamanannya.

1.4 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

a. Saat proses enkripsi menggunakan program aplikasi, spasi, angka dan tanda baca akan dihapus, sehingga karakter yang dapat dienkripsi adalah huruf alphabet a-z dan A-Z. Tetapi, untuk huruf a-z, program aplikasi akan mengubahnya ke huruf kapital.
b. Dalam program aplikasi pengirim *email*, penggunaannya masih terbatas hanya bagi pengguna layanan *email* yang dapat mengizinkan pihak ketiga untuk mengirimkan *email*. Penyedia layanan *email* yang mengizinkan pihak ketiga untuk mengirim *email* adalah Yahoo Mail dan Google Mail.

1.5 Struktur Organisasi

Berikut ini struktur organisasi dari skripsi ini:

Bab I Pendahuluan, berisi latar belakang dari permasalahan yang diambil, rumusan masalahnya, tujuan serta manfaat dari penelitian yang dilakukan.

Bab II Kajian Pustaka/ Landasan Teoretis, membahas teori-teori yang berkaitan dengan permasalahan dan penyelesaian yang akan diambil.

Bab III Metode Penelitian, membahas langkah-langkah yang diambil untuk menyelesaikan permasalahan.

BAB IV Penerapan Enkripsi Caesar Cipher Yang Telah Ditingkatkan Keamanannya Pada Aplikasi Pengirim Email, mengkaji tentang penyelesaian dan pembahasan dari masalah yang diambil.

Bab V Kesimpulan, Implikasi dan Rekomendasi, membahas mengenai kesimpulan dan implikasi yang didapatkan selama penyelesaian permasalahan serta rekomendasi untuk kedepannya.