BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan data adalah suatu hal yang diinginkan semua orang untuk menjaga privasi dengan menyembunyikan data. Sebuah data atau pesan yang bersifat rahasia harus benar-benar dijaga. Kriptografi adalah salah satu teknik untuk pengamanan data atau pesan. Enkripsi dan dekripsi banyak digunakan untuk pengamanan data.

Enkripsi merupakan metode yang digunakan untuk mengubah kata atau data menjadi sebuah kode-kode yang tidak dimengerti oleh orang lain termasuk komputer. Untuk bisa mengetahui data yang sebenarnya diperlukan satu metode lagi yakni deskripsi. Deskripsi akan mengubah kode-kode yang tidak bisa dimengeri menjadi data yang sebenarnya (Mukhtar, 2018).

Salah satu algoritma kriptografi adalah *vigenere chiper* dan *RC4*. Algoritma *vigenere chiper* dan *RC4* termasuk kriptografi klasik yang menggunakan plainteks, cipherteks dan kunci untuk melakukan proses enkripsi dan dekripsi dalam pengamanan data. Vigenere cipher adalah salah satu jenis kriptografi simteris dan dikategorikan pula sebagai *polyalfabet cipher*. *RC4* adalah salah satu jenis *stream cipher* yang sinkron yaitu cipher yang memiliki kunci simetris dan mengenkripsi atau mendekripsi plainteks secara digit per digit atau bit per bit dengan cara mengkombinasikan secara operasi biner

Penerapan algoritma *vigenere chiper* ternyata dapat dipecahkan oleh *crypanalyst* melalui metode kasiski. Metode kaisiski sebenarnya digunakan untuk mengestimasi kemungkinan panjang kunci yang muncul. Dengan melihat hal tersebuh penulis mencoba melakukan kombinasi enkripsi menggunakan algoritma Rivest Block *4* untuk meningkatkan keamanan sebuah pesan text.

1.2 Perumusan Masalah

Rumusan masalah yang dapat didefinisikan dalam penelitian ini diantaranya adalah sebagai berikut.

1. Bagaimana merancang pengamanan pesan teks menggunakan algoritma *vigenere chiper* dan *RC4*?
2. Bagaimana mengimplementasikan teknologi enkripsi dan deskripsi pesan teks menggunakan algoritma *vigenere chiper* dan *RC4*?
3. Bagaimana menganalisa kinerja enkripsi dan deskripsi untuk pengamanan sebuah pesan teks menggunakan algoritma *vigenere chiper* dan *RC4*?

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Membangun sebuah aplikasi pengamanan pesan teks menggunakan algoritma *vigenere chiper* dan *RC4.*
2. Mengimplementasikan teknologi enkripsi dan deskripsi untuk pesan teks menggunakan algoritma *vigenere chiper* dan *RC4.*
3. Menganalisa kinerja pengamanan pesan teks menggunakan algoritma *vigenere chiper* dan *RC4.*

1.4 Manfaat penelitian

Manfaat dari penelitian ini adalah agar pengguna dapat menggunakannya sebagai media atau alat untuk pengamanan sebuah pesan teks menggunakan algoritma *vigenere chiper* dan *RC4.*

1.5 Batasan Masalah

Adapun yang menjadi batasan masalah dalam penelitian ini adalah:

1. Sistem yang dirancang hanya untuk proses enkripsi dan deskripsi pada sebuah pesan teks.
2. Metode yang digunakan adalah algoritna *vigenere chiper* dan *RC4.*

Tidak menggabungkan atau membandingkan algoritma yang digunakan.