BAB I
PENDAHULUAN

1.1 Latar Belakang

Short Message Service atau yang lebih dikenal dengan SMS adalah salah satu fasilitas yang disediakan telepon seluler. Dengan SMS tersebut dapat dilakukan pengiriman data berupa pesan singkat yang mudah digunakan oleh masyarakat untuk berbagi informasi tanpa harus saling bertemu. Walaupun terlihat praktis, banyak tindakan yang tidak bertanggung jawab untuk mencuri informasi yang bersifat rahasia. Maka dari itu dibutuhkan suatu penyandian untuk melindungi kemanan dan keaslian pesan tersebut. Untuk itu dalam meningkatkan keamanan yang memerlukan kerahasiaan pesan dapat menggunakan teknik kriptografi.

Kriptografi merupakan ilmu yang mempelajari mengenai tulisan rahasia dengan tujuan menyembunyikan pesan sebenarnya. Dalam proses kriptografi diperlukan dua proses penting yaitu enkripsi dan dekripsi. Untuk melakukan enkripsi dan dekripsi pesan diperlukan algoritma yang cocok digunakan untuk dijalankan pada platform telepon seluluer. Algoritma RC4 dan Rijndael

termasuk algoritma simetris yang dapat digunakan untuk enkripsi dan dekripsi pesan teks (Ariyus, 2010).

Untuk mengetahui apakah kedua algoritma tersebut dapat dijalankan pada telepon seluler maka dilakukan penelitian serta untuk membandingan waktu yang diperlukan pada proses enkripsi dan dekripsi pesan kedua algoritma tersebut.

1.2 Rumusan Masalah

Rumusan permasalahan yang akan dikaji dalam penelitian ini adalah membandingkan waktu yang diperlukan untuk proses enkripsi dan dekripsi SMS menggunakan algoritma RC4 dan Rijndael.

1.3 Batasan Masalah

Berikut adalah batasan masalah dalam proposal penelitian ini adalah:

1. Algoritma yang digunakan pada enkripsi dan dekripsi SMS hanya algoritma RC4 dan Rijndael.
2. Penelitian ini hanya membandingkan waktu yang dibutuhkan dalam proses enkripsi dan dekripsi SMS.
3. Algoritma Rijndael yang digunakan hanya blok yang berukuran 128 *bit* dan ukuran kunci sebesar 128 *bit*.

4. Aplikasi enkripsi dan dekripsi SMS digunakan hanya pada telepon seluler yang berbasis JAVA.
5. Algoritma RC4 dan Rijndael yang digunakan pada JAVA dengan menggunakan bantuan *library Bouncy Castle.*

1.4 Tujuan

Tujuan dilaksanakan penelitian ini adalah :

1. Menggunakan Algoritma RC4 pada proses enkripsi dan dekripsi SMS.
2. Menggunakan Algoritma Rijndael pada proses enkripsi dan dekripsi SMS.
3. Membandingkan waktu kedua algoritma tersebut pada proses enkripsi dan dekripsi SMS.

1.5 Manfaat

Manfaat penelitian ini yaitu sebagai berikut:

1. Menambah pengetahuan mengenai penerapan algoritma RC4 pada enkripsi dan dekripsi SMS.
2. Menambah pengetahuan mengenai penerapan algoritma Rijndael pada enkripsi dan dekripsi SMS.
3. Menambah pengetahuan mengenai enkripsi dan dekripsi suatu data, khususnya pada SMS dengan penenerapannya dalam bahasa JAVA.

4. Mengetahui hasil perbandingan waktu proses enkripsi dan dekripsi Algoritma RC4 dan Rijndael