# BAB I

# PENDAHULUAN

## 1.1 Latar belakang masalah

Berkembangnya teknologi informasi saat ini, membuat semua orang di dunia ini mudah melakukan pertukaran data atau informasi di antara kelompok maupun individu, baik jarak jauh maupun jarak dekat, melalui perangkat *mobile* khususnya *handphone*. Dalam hal ini, perangkat *handphone* merupakan salah satu bagian dari teknologi *wireless* yang berfungsi untuk membantu semua orang dalam melakukan proses pertukaran data atau informasi. Perangkat *handphone* saat ini, telah berkembang dengan banyak fitur yang dimilikinya, salah satunya adalah fitur s*hort message service(*SMS*)* yang banyak diminati oleh pengguna *handphone* sebagai cara alternatif lain dalam berkomunikasi. Karena mudah digunakan dan biaya dari penggunaan fitur tersebut relatif murah.

Tetapi di sisi lain, aspek keamanan menjadi salah satu faktor terpenting dalam proses pertukaran data dan informasi. Karena aspek keamanan merupakan salah satu hal yang sangat penting dalam menjaga kerahasian data yang berisi informasi sensitif yang hanya boleh diketahui oleh pihak yang berhak atau berwenang saja, apabila proses pengiriman data atau informasi di

lakukan melalui jaringan publik. Jika data dan informasi yang di kirimkan tidak diamankan terlebih dahulu, maka akan mudah disadap dan diketahui isi informasinya oleh pihak-pihak yang tidak berwenang. Salah satu cara yang digunakan untuk mengamankan data dan informasi adalah memamfaatkan sistem kriptografi yang dapat mengubah isi informasi (*plaintext*) yang dienkripsi menjadi *ciphertext*, dan untuk memperoleh kembali informasi yang asli, maka dilakukan proses dekripsi, dan disertai dengan kata kunci yang sesuai.

Adanya permasalahan disisi keamanan dalam proses pengiriman dan penerimaan data dan informasi, maka penulis berkeinginan untuk membangun aplikasi keamanan data, yang berbasis pada algoritma kriptografi. Dalam hal ini, metode yang digunakan untuk mengenkripsi dan mendekripsi teks pada SMS adalah metode s*hift cipher* dan c*ipher block chaining.* Karena kedua metode ini memiliki kelebihan masing-masing dalam mengenkripsi dan mendekripsi teks pada SMS. Metode s*hift cipher* memiliki kelebihan dalam mengenkripsi data atau informasi berdasarkan model matematis, karena menggunakan operasi modulus dengan mengubah huruf-huruf menjadi angka. Sedangkan metode c*ipher block chaining* memiliki kelebihan dalam mengenkripsi data atau informasi dengan menggunakan

operasi c*ipher block* yang menerapakan umpan balik pada sebuah blok. Dengan demikian, kedua metode ini dikombinasikan maka, akan memberikan keamanan yang cukup kuat pada data atau informasi yang berbentuk SMS.

## 1.2 Rumusan masalah

Berdasarkan latar belakang masalah diatas, maka dapat dibuat sebuah rumusan adalah sebagai berikut :

Bagaimana mengimplementasikan algoritma s*hift cipher* dan c*ipher block chaining* untuk pengamanan teks SMS.

## 1.3 Ruang lingkup masalah

Dalam membangun aplikasi ini, meliputi beberapa batasan masalah yaitu :

1. Aplikasi dibangun dengan menggunakan bahasa pemrograman *J2ME* .
2. Dalam aplikasi ini, terdapat *menu* tulis pesan, pesan masuk , *help*, dan *about*.
3. Proses enkripsi dan dekripsi dilakukan dengan menggunakan metode s*hift cipher* dan c*ipher block chaining.*
4. Aplikasi mengenkripsi dan mendekripsi pesan berupa teks SMS.
5. Panjang *ciphertext* yang bisa dikirim maksimal 160 karakter.
6. Pengujian adalah para penguna *handphone Nokia, dan Samsung,* .

7. Aplikasi ini hanya bisa diinstal pada *handphone* yang memiliki fitur *java*.

## 1.4 Tujuan penelitian

Tujuan dari penelitian ini adalah membangun aplikasi enkripsi teks SMS menggunakan kombinasi metode s*hift cipher* dan c*ipher block chaining* pada perangkat *mobile*.