BAB I
PENDAHULUAN

1.1 Latar Belakang

Beberapa tahun ini perkembangan teknologi komunikasi semakin pesat. Telepon seluler merupakan salah satu hasil dari perkembangan teknologi komunikasi. Telepon seluler mempermudah orang untuk berkomunikasi satu sama lain. Dengan adanya teknologi ini dunia terasa sempit karena seseorang dapat berkomunikasi dengan orang lain yang jaraknya jauh. Di dalam telepon seluler ini ada beberapa fungsi komunikasi yang dapat digunakan antara lain telepon, *video call, SMS, MMS, chatting*, internet, dan lain-lain. Di antaranya layanan komunikasi tersebut, *SMS* tidak menjamin integritas dan keamanan pesan yang akan disampaikan. Pesan yang bersifat personal atau rahasia tidak dijamin sampai ke penerima tanpa dicuri informasinya oleh orang lain.

Ada beberapa resiko yang dapat mengancam keamanan pesan pada layanan *SMS* antara lain *SMS spoofing*, *SMS snooping*, dan *SMS interception*. *SMS spoofing* merupakan pengiriman sms di mana nomor pengirim yang tertera bukanlah nomor pengirim yang sebenarnya. Mekanisme *SMS spoofing* ini dimungkinkan karena lemahnya proteksi koneksi (*Short Message Service Center*) *SMSC gateway*. Penyusup dapat merekam *login* dan pasword dari pesan yang berasal dari SMS gateway menuju *SMSC*. Walaupun tak terlalu mudah namun ini dapat dilakukan dalam beberapa kasus. Dalam hal ini penyusup mengatur sebuah gateway palsu yang berlaku seperti gateway sesungguhnya. *Gateway* palsu ini dapat mengirim semua jenis pesan pendek kepada user *MS* melalui *SMSC*. Pada

teknik *spoofing* ini pesan dikirim dengan memanipulasi nomor (*Mobile Subscriber Integrated Services Digital Network Number*) MSISDN asal (originate) pada field yang disediakan sehingga pesan akan tampak datang dari nomor pengirim lainnya. Kemungkinan *spoofing* yang lain adalah dengan membuat simulator *SMSC* yang berlaku seperti *SMSC* asli. Dengan cara ini gateway akan kebanjiran pesan, sebagai contoh aplikasi bank menggunakan *gateway* dapat dengan mudah diperoleh informasi *account* bahkan dapat digunakan untuk transaksi bank tanpa proses *authorisasi*.

Ancaman *SMS* lainnya adalah *SMS snooping*. *SMS snooping* lebih sering terjadi karena kelalaian pengguna telepon seluler. Contohnya ketika seseorang meminjamkan telepon selulernya pada orang lain untuk menggunakan telepon selulernya. Pada saat itu orang tersebut dapat dengan sengaja atau tidak membuka isi pesan yang ada pada *inbox SMS*. Pesan yang bersifat personal atau rahasia dapat dibaca dengan mudah oleh orang lain melalui cara ini.

Celah keamanan terbesar pada layanan komunikasi *SMS* adalah pada saat *SMS* tersebut sedang dikirim melalui jaringan *SMS* tersebut. *SMS* bekerja pada jaringan nirkabel yang memungkinkan terjadinya pencurian isi pesan SMS ketika dalam proses transmisi dari pengirim ke penerima. Kasus ini disebut *SMS interception.* Dibutuhkan sebuah sistem keamanan pada layanan *SMS* yang mampu menjaga integritas dan keamanan isi pesan untuk menutupi celah keamanan *SMS* (terutama untuk *SMS snooping* dan *SMS interception*).

Agar isi pesan hanya dapat dibaca maknanya oleh pengirim dan penerima, isi pesan sebelum dikirim melalui *SMS* harus dienkripsi terlebih dahulu dengan

algoritma kriptografi, misalnya *Vigenere Cipher*. Penerima dapat membaca makna dari pesan tersebut dengan melakukan dekripsi isi pesan tersebut menggunakan kunci yang sama yang digunakan oleh pengirim. Apabila ada orang lain yang mencuri isi pesan tersebut, orang tersebut tidak akan mampu membaca makna pesan tersebut. Pesan yang dicurinya tidak akan memiliki makna karena dalam kondisi terenkripsi. Dengan adanya sistem keamanan ini isi pesan yang bersifat personal atau rahasia dapat tersampaikan secara aman.

1.2 Perumusan Dan Batasan Masalah

Identifikasi masalah yang ditemukan ialah sebagai berikut:

1. Bagaimana merancang dan membangun aplikasi enkripsi *SMS Android* menggunakan Algoritma *vigenere cipher* dengan menggunakan *code* ASCII?
2. Bagaimana menerapkan enkripsi pada *SMS Android* menggunakan Algoritma *vigenere cipher* dengan menggunakan *code* ASCII?

Adapun batasan masalah dalam penelitian ini adalah sebagai berikut :

1. Pembuatan aplikasi pengirim pesan enkripsi ini menggunakan algoritma *vigenere cipher* dengan menggunakan *code* ASCII.
2. Pada aplikasi ini, yang akan dienkripsi adalah berupa karakter teks pada *SMS*.
3. Perancangan aplikasi ini dibuat berbasis *Android.*
4. Tidak membahas kelemahan dan kelebihan algoritma *vigenere cipher* dan *code* ASCII.
5. Kunci yang digunakan berupa angka dengan panjang maksimal 10 karakter.
6. Aplikasi berjalan pada platform *android* minimal versi 3.0 atau honeycomb.
7. Tidak membahas tentang penyampaian kunci pada enkripsi.

1.3 Tujuan Penelitian

Adapun yang menjadi tujuan penelitian ini berdasarkan rumusan masalah diatas adalah :

1. Merancang dan membagun aplikasi enkripsi *SMS Android* menggunakan algoritma *vigenere cipher* dengan menggunakan *code* ASCII.
2. Menerapkan enkripsi dengan menggunakan algoritma *vigenere cipher* dengan menggunakan *code* ASCII pada aplikasi *SMS Android*.

1.4 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Meningkatkan keamanan terhadap pesan *SMS*, sehingga keamaanan pesan tersebut menjadi relative aman.
2. Menanggulangi penyadapan terhadap pesan *SMS*.
3. Memberikan kemudahan bagi pengguna telepon seluler berbasis *Android* untuk mengirimkan informasi rahasia melalui *SMS*.