BAB I
PENDAHULUAN

1.1. Latar Belakang

Telepon seluler merupakan alat komunikasi yang umum dipakai oleh sebagian besar umat manusia di dunia. Telepon seluler juga menyediakan media komunikasi yang beragam, salah satunya adalah SMS. Penggunaan SMS menjadi popular di kalangan masyarakat karena dengan begitu mudahnya kita dapat saling bertukar informasi tanpa batasan jarak dan waktu. Celah keamanan terbesar pada komunikasi via SMS adalah pesan yang dikirimkan akan disimpan di SMSC (*Short Message Service Center*), yaitu tempat dimana SMS disimpan sebelum dikirim ke tujuan. Pesan yang sifatnya *plaintext* ini dapat disadap oleh siapa saja yang berhasil memiliki akses ke dalam SMSC. Akibatnya, informasi penting seperti *password*, nomer pin, dan lain-lain dapat dibaca oleh orang yang tidak berhak untuk mengetahuinya. Proyek akhir ini akan memberikan alternatif untuk menyelesaikan masalah ini.

Dengan semakin majunya teknologi pada telepon seluler, implementasi suatu algoritma menjadi mungkin dilakukan. Macam-macam algoritma enkripsi antara lain : *Vegenere*, *ROT13*, *DES*, *IDEA*, *AES*, *Vernam Cipher*, *Blowfish* dan masih banyak lagi.

One Time Pad ditemukan pada tahun 1917 oleh Mayor Joseph Mauborgne dan Gilbert Vernam. *Cipher* ini termasuk ke dalam kelompok algoritma kriptografi simetri. *Cipher* ini diimplementasikan melalui sebuah kunci yang terdiri dari sekumpulan *random* karakter-karakter yang tidak berulang. Setiap huruf kunci dijumlahkan *modulo* 26 dengan huruf pada *plaintext*. Pada *One Time Pad*, tiap huruf kunci digunakan satu kali untuk satu pesan dan tidak digunakan kembali. Panjang *stream* karakter kunci sama dengan panjang pesan. *One time pad* (*pad* = kertas *bloknot*) berisi barisan karakter-karakter kunci yang dibangkitkan secara acak. Satu *pad* hanya digunakan sekali (*one time*) saja untuk mengenkripsi pesan, setelah itu *pad* yang telah digunakan dihancurkan..

ROT13 adalah subtitusi kode dengan melakukan pergeseran sebanyak k=13. Digabungkan dengan teknik algoritma *encoding* karakter *base64*. *Base64* adalah sebuah *encoding* karakter yang mewakili data *biner* dalam format *string* ASCII dengan menerjemahkannya ke dalam representasi 64.

Dengan menggunakan kombinasi 2 algoritma yaitu *One Time Pad* dan *ROT13*, keamanan data menjadi lebih baik karena penyusup harus melewati 2 *layer* keamanan

yaitu *ROT13* dan *One Time Pad*. Dari kedua algoritma tersebut, penulis mengimplementasikannya dengan membangun sebuah aplikasi yang dapat meng-*enkripsi* teks pada SMS (*Short Message Services*) sehingga teks yang terkirim ke nomor tujuan adalah teks yang telah ter-*enkripsi*.

1.2. Rumusan Masalah

Berdasarkan uraian pada latar belakang masalah, maka dapat durumuskan suatu rumusan masalah sebagai berikut.

1. Bagaimana membuat sistem pengamanan teks SMS (*Short Message Services*) dengan menggunakan Algoritma *Vernam Cipher* dan *ROT13*.
2. Bagaimana tingkat keamanan text setelah menggunakan sistem pengamanan teks SMS (*Short Message Services*) dengan menggunakan Algoritma *Vernam Cipher* dan *ROT13*.

1.3. Batasan Masalah

Untuk memfokuskan pengerjaan tugas akhir ini, penulis akan membatasi masalah, yaitu sebagai berikut:

1. Pembahasan hanya pada pengimplementasian dan proses kerja enkripsi dan dekripsi pada SMS (*Short Message Services*).
2. Penelitian ini hanya membahas keamanan data berdasarkan aspek keamanan kriptografi yaitu *confidentiality* dan data *integrity*.
3. Library/tool yang dipakai dalam sms gateway ini menggunakan gammu lib dengan bahasa pemrograman yang dipakai Visual Basic Net 2010.
4. OS yang digunakan minimum windows 7 sp 1 yang telah mendukung *framework* 4.0.
5. Panjang kunci OTP harus sama dengan *plaintext*. Hal ini menyebabkan apabila *plaintext* semakin panjang maka keamanannya semakin berkurang. Jika sebuah kunci telah digunakan maka kita tidak boleh lagi menggunakan kunci yang sama. Seandainya kita telah menggunakan sebuah kunci maka kita tidak boleh menggunakan kunci yang sama dan jika kombinasi yang kita miliki telah kadaluarsa mau tidak mau kita tidak bisa menggunakan OTP lagi (karena jika kita tetap menggunakannya keamanan pesan menjadi berkurang dan akan hilang).

1.3 Tujuan Penelitian

Tujuan penelitian ini adalah untuk mengamankan teks yang akan dikirim melalui SMS (*Short Message Services*) dari orang-orang yang ingin membaca informasi yang terdapat pada teks tersebut dan mengukur tingkat keamanan.

1.4. Manfaat Penelitian

Tugas akhir ini diharapkan akan mampu memberikan keamanan bagi user dalam menggunakan SMS (*Short Message Services*) agar orang yang tidak berhak tidak bisa membaca informasi yang ada pada SMS (*Short Message Services*) tersebut sehingga keamanan dan kerahasiaan data yang dikirim melalui SMS (*Short Message Services*) dapat terjaga.