BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Kerahasiaan dan keamanan saat melakukan pertukaran data adalah hal yang sangat penting dalam komunikasi data, baik untuk tujuan keamanan bersama, maupun untuk privasi individu. Mereka yang menginginkan agar datanya tidak diketahui oleh pihak-pihak yang tidak berkepentingan selalu berusaha menyiasati cara mengamankan informasi yang akan dikomunikasikannya.Perlindungan terhadap kerahasiaan datapun meningkat, salah satu caranya dengan penyandian data atau enkripsi.

Enkripsi merupakan suatu proses pengubahan pesan asal menjadi karakter yang tidak dapat dibaca. Ada beberapa algoritma enkripsi yang biasa digunakan seperti *DES*, *Triple DES*, *Blowfish, IDEA* dan sebagainya. Algoritma-algoritma tersebut begitu rumit dan sulit dimengerti dengan dalih 'faktor keamanan', katanya semakin sulit suatu algoritma dimengerti, maka semakin aman. Namun bagi para pengguna mereka tidak memikirkan seberapa sulit algoritma dan aplikasinya, yang mereka inginkan adalah menjaga

kerahasiaan data. Ada dua syarat untuk mengimplementasikan suatu sistem enkripsi yang aman. Pertama, *true random bits* (benar-benar hanya dihasilkan sekali) dan kedua, *key space* yang besar untuk algoritma enkripsi tersebut. Jika kedua syarat dipenuhi, tidak masalah seberapa kompleks algoritma enkripsinya. Bahkan semakin sederhana semakin baik, karena semakin sederhana suatu algoritma, maka akan semakin sedikit proses komputasinya dan semakin sedikit waktu yang dibutuhkan untuk mengeksekusinya. Kesederhanaan itulah yang ditawarkan oleh algoritma *One Time Pad (OTP)*, algoritma kriptografi yang secara teori dan praktek aman dari tangan-tangan penyadap, dan dikenal dengan sebutan *'unbreakable algorithm'.*

Skema enkripsi yang akan dibangun pada tugas akhir ini menerapkan teknik kriptografi, yang menganut kerahasiaan pada kunci (key), sehingga keamanan enkripsi hanya tergantung pada *key* dan tidak tergantung apakah algoritmanya diketahui orang atau tidak. Pada tugas akhir ini algoritma yang digunakan adalah OTP*(One Time Pad)* yang mana algoritma ini akan diterapkan padametode Enkripsitext

untuk SMS berbasis android. SMS adalah layanan pesan singkat (*short message service*) untuk bertukar informasi antara satu dengan yang lain. Berbagai jenis informasi dikirimkan melalui layanan tersebut setiap harinya, namun kemudahan ini sering di salah gunakan oleh beberapa pihak. Beberapa orang dengan berbagai cara mencoba mencuri informasi yang bukan hak mereka. Karena itu, dibutuhkan suatu cara untuk dapat mengamankan informasi-informasi yang sifatnya rahasia

Oleh karena itu, Penulis akan membuat sebuah aplikasi pengamanan SMS dengan metode Vigenere Cipher dan One Time Pad untuk mengenkripsikan data yang berjalan pada system operasi android.

1.2 Rumusan Masalah

Masalah yang akan di tangani pada tugas akhir ini adalah bagaimana cara mengimplementasikan algoritma *one time pad dan vigenere cipher* untuk mengamankan pesan melalui *SMS* pada system operasi android dalam mengirim dan menerima pesan yang bersifat rahasia.

1.3 Ruang Lingkup

Dalam perancangan dan implementasi, terdapat ruang lingkup kajian atau penelitian yang meliputi :

1. Aplikasi ini dibangun pada system operasi andoid.
2. Terdapat menu tulis pesan yang digunakan untuk menulis pesan yang nantinya akan di enkripsikan.
3. Terdapat pesan masuk yang digunakan untuk menyimpan pesan masuk.
4. Terdapat pesan keluar yang digunakan untuk menyimpan pesan yang telah dikirim.
5. Menggunakan metode *vigenere cipher* dan algoritma OTP (*one time pad)* untuk mengenkripsikan dan mendekripsikan pesan.
6. Aplikasi ini hanya mengenkripsikan dan mendekripsikan pesan berupa teks.
7. Dibangun dengan menggunakan karakter 64 bit.
8. Kedua belah pihak pengguna harus sama-sama menggunakan aplikasi ini.

1.4 Tujuan

Tujuan dari penulisan ini adalah untuk membangun sebuah aplikasi pengamanan SMS berbasis android, menggunakan metode *Vigenere Cipher* dan *One Time Pad* sehingga diharapkan pengguna *smartphone* android pada khususnya mendapatkan kelebihan berupa keamanan di dalam mengirim SMS.