BAB I
PENDAHULUAN

1.1 Latar Belakang

Informasi merupakan suatu yang sangat penting dan standar dalam berbagai aspek kehidupan. Dahulu informasi dikirim dengan cara memberikan kode asap, ada juga yang menggunakan peluit dengan kode-kode tertentu, hingga mengirim informasi dengan membuat surat dan dikirim menggunakan burung. Seiring dengan perkembangan teknologi yang tiada habisnya yang memungkinkan manusia untuk dapat berkomunikasi dan saling bertukar informasi pada jarak yang dekat ataupun dengan jarak yang jauh sekalipun. Untuk jarak jauh misalnya antar kota, antar wilayah, antar Negara bahkan hingga antar Benua. Dengan jarak yang jauh bukan merupakan suatu kendala lagi dalam melakukan komunikasi.

Saat ini banyak layanan yang membantu dalam proses pengiriman informasi seperti *E-Mail (Electronic Mail)* dan *SMS (Short Messaging Service)* untuk *E-Mail* menggunakan internet dalam proses pengiriman informasinya sedangkan untuk *SMS* dikirim melalui jaringan telekomunikasi pada telepon selular. *SMS* merupakan yang layanan pengiriman informasi yang paling banyak digunakan dikarenakan hampir semua orang di dunia ini memiliki telepon selular. Dan juga dikarenakan biaya yang murah dibandingkan dengan menelepon langsung. Informasi yang dikirim dengan menggunakan layanan *SMS* bisa saja merupakan informasi penting/rahasia yang tidak boleh diketahui oleh orang lain. Misal informasi bisnis antar Perusahaan, informasi pertahanan Negara. Untuk menjaga kerahasian pesan tersebut dikembangkanlah suatu ilmu yang mempelajari tentang cara pengamanan informasi/pesan yang dikenal dengan istilah kriptografi.

Kriptografi merupakan suatu ilmu yang berfungsi untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Pesan yang akan dikirim tersebut di enkripsi menjadi suatu *cipher text* atau suatu kalimat yang tidak beraturan susunan hurufnya sebelum dikirim. Setelah sampai ke tujuan *cipher text* tersebut di dekripsi menjadi pesan seperti awal. Algoritma kriptografi ini ada yang simetri dan asimetri. Disebut algoritma simetri dikarenakan kunci yang digunakan

untuk me-enkripsi dan mendekripsi pesan nilainya sama sedangkan algoritma asimetri kunci enkripsi dan dekripsi nilainya berbeda.

Pada kategori kunci simetri modern beroperasi dalam mode bit dan dapat dikelompokkan menjadi 2 kategori yaitu *cipher* aliran (*stream cipher*) dan *cipher* blok (*block cipher*). Hampir semua algoritma *cipher* blok bekerja dalam model *Feistel*. Model *Feistel* ini ditemukan oleh Horst Feistel tahun 1970. Model ini juga banyak dipakai dalam algoritma kriptografi seperti *DES*, *LOKI*, *GOST*, *Lucifer*, dll.

Andi Kurniawan Dwi (2012) pernah membuat aplikasi kriptografi pada *SMS* berbasis android dengan menggunakan metode Vigenere Cipher dan menyimpulkan bahwa dengan dengan aplikasi *SMS* yang dibuat dapat meningkatkan keamanan pada layanan *SMS* seperti *snooping* maupun *interception*, namun pada aplikasi ini memiliki kelemahan dengan adanya karakter yang berulang dan user yang akan dikirimi pesan harus mengetahui kunci yang digunakan[7]. Becik Gati Anjari (2012) juga membuat aplikasi enkripsi *SMS* pada telepon selular berbasi android dengan menggunakan metode yang sama dengan Andi Kurniawan Dwi (2012) yaitu metode Vigenere Cipher namun pada aplikasi yang dibuat oleh Becik Gati Anjari (2012) metode Vigenere Cipher sudah dimodifikasi dan diberi *Key* tambahan dengan metode tersebut dapat menghilangkan kelemahan metode vigenere yaitu adanya karakter yang berulang. selain itu juga dengan memberikan kunci tambahan keamanan dan privasi pengguna lebih terjamin[6]. Chandra Ari Wijaya dan Willya Triana (2011) mengimplementasikan algoritma *Twofish* untuk enkripsi dan dekripsi pesan pada ponsel berbasis android menyimpulkan bahwa dengan menggunakan algoritma *Twofish* pengiriman pesan dapat tergjaga keamanannya namun apabila pesannya panjang maka proses pengenkripsiannya akan lama[10].

Vigenere Cipher masih lemah terhadap *avalanche attack* maka dari itu diperlukan langkah untuk meningkatkan *avalance affect* yang disebut *confusion*. Salah satu langkah *confusion* yaitu menambah *feedback* pada pemrosesan algoritmanya. Struktur *feedback* untuk *confusion* yang sering digunakan adalah struktur *Feistel*. Berdasarkan latar belakang diatas maka penulis memiliki inisiatif untuk membuat aplikasi untuk mengamankan pesan menggunakan algoritma kriptografi model *Feistel* dengan Kunci nomor handphone pengguna dan tujuan untuk memenuhi syarat *authentication* pada platform android. Selain itu juga pada

algoritma ini ditambahkan permutasi dimana permutasi ini merupakan proses untuk mengacak setiap karakter agar tidak pada posisi yang sama sehingga dapat menigkatkan *avalanche effectnya*.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka dirancang suatu perangkat yang mencakup permasalah-permasalahan berikut :

1. Bagaimana merancang aplikasi enkripsi dan dekripsi pesan pada *SMS* di Android yang menggunakan algoritma struktur *Feistel*.
2. Bagaimana implementasi kriptografi pada handphone berbasis android dengan menggunakan metode blok cipher *Feistel*
3. Bagaimana performansi dalam pengenkripsian dan pendekripsian data *SMS* yang didapat dari hasil pengujian.

1.3 Batasan Masalah

Pengembangan aplikasi mengamankan pesan menggunakan algoritma kriptografi model *Feistel* terbatas pada hal-hal sebagai berikut.

1. Aplikasi ini dibuat menggunakan eclipse dan SDK sehingga hanya dapat digunakan pada perangkat android
2. Algoritma yang dipakai dalam aplikasi ini menerapkan algoritma *cipher* blok model *Feistel*.
3. Tidak membahas algoritma kriptografi yang lain.
4. Tidak membahas proses pengiriman dan penerimaan *SMS* yang terjadi di luar aplikasi ini.
5. Kunci yang digunakan pada aplikasi ini berupa angka.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini yang mengacu pada rumusan masalah adalah sebagai berikut.

1. Merancang aplikasi enkripsi dan dekripsi pesan pada *SMS* di Android menggunakan *cipher* blok model *Feistel.*
2. Mengimplementasikan algortima Kriptografi pada aplikasi yang berbasis Android.
3. Mengetahui perfomansi sistem yang dirancang.

1.5 Metode Penelitian

Tujuan yang ingin dicapai dalam penelitian ini yang mengacu pada rumusan masalah adalah sebagai berikut.

1. Merancang aplikasi enkripsi dan dekripsi pesan pada *SMS* di Android menggunakan *cipher* blok model *Feistel.*
2. Mengimplementasikan algortima Kriptografi pada aplikasi yang berbasis Android.
3. Mengetahui perfomansi sistem yang dirancang.

1.6 Sistematika Penulisan

Adapun sistematika penulisan laporan hasil penelitian tugas akhir ini adalah sebagai berikut :

1. **BAB I Pendahuluan**

   Pada BAB ini membahas mengenai latar belakang masalah, perumusan masalah dan batasan masalah, tujuan, metodologi penelitian, serta sistematika penulisan dari kegiatan tugas akhir ini.

2. **BAB II Landasan Teori**

   Pada BAB ini akan membahas mengenai teori dasar yang berhubungan dengan aplikasi yang akan dibangun.

3. **BAB III Analisis dan Perancangan Sistem**

   BAB ini berisi analisa terhadap seluruh sistem yang dibuat untuk menentukan kebutuhan apa saja yang harus dipenuhi dan pengembangannya disesuaikan dengan keterbatasan yang dimiliki oleh sumber daya telepon selular.

4. **BAB IV Implementasi dan Analisis Hasil Sistem**

   Pada bagian ini dibahas tentang implementasi dan pengujian terhadap aplikasi yang dikembangkan serta analisis aplikasi.

5. **BAB V Kesimpulan dan Saran**

   Pada BAB ini berisi kesimpulan dan saran dari seluruh kegiatan penelitian tugas akhir ini yang bisa digunakan sebagai masukan untuk pengembangan lebih lanjut.