BAB I
PENDAHULUAN

1.1 Latar Belakang

Kehidupan manusia saat ini tanpa disadari dilingkupi oleh teknologi informasi, salah satu unsur didalamnya adalah kriptografi. Mulai dari transaksi di mesin ATM, transaksi di bank, transaksi dengan kartu kredit, percakapan melalui telepon genggam dan mengakses internet. Begitu pentingnya kriptografi untuk keamanan informasi, sehingga jika berbicara mengenai masalah keamanan informasi, maka tidak dapat memisahkannya dengan dunia kriptografi.

Perkembangan teknologi informasi saat ini membawa cara berkomunikasi yang beragam bagi manusia dengan munculnya berbagai macam media komunikasi untuk bertukar informasi. Telepon seluler merupakan media berkomunikasi yang umum digunakan manusia sekarang ini karena memberikan kemudahan bagi penggunanya dalam berkomunikasi lisan maupun tulisan [1]. Teknologi pada telepon seluler terus mengalami perkembangan yang dahulu hanya dapat digunakan untuk melakukan panggilan dan mengirim pesan (SMS) kini dapat digunakan untuk berbagai macam hal seperti *chatting, browsing, video call,* dan lain lain.

Salah satunya adalah SMS yang merupakan fasilitas yang disediakan ponsel untuk melakukan pengiriman data berupa pesan singkat yang tidak memerlukan koneksi internet dan dalam waktu yang lebih cepat pengirimannya. Tetapi dengan perkembangan teknologi saat ini muncul permasalahan yang berhubungan dengan tingkat keamanan layanan tersebut. Kemudahan pertukaran informasi melalui SMS disalahgunakan oleh sebagian orang dengan berbagai cara mencoba untuk mencuri informasi karena belum dilengkapi dengan sistem yang dapat menjamin kerahasiaan isi SMS sehingga orang yang tidak berhak juga dapat mengetahui isi dari SMS tersebut. Pesan yang dikirimkan adalah berupa plainteks, data plainteks seperti ini dapat dicegat dijalan oleh siapa saja yang memiliki akses ke sistem SMS. Celah keamanan pada komunikasi via SMS adalah pesan yang dikirimkan akan disimpan di SMSC (Pusat Layanan Pesan Singkat), yaitu tempat dimana SMS

disimpan sebelum dikirim ke tujuan. SMSC merupakan salah satu pihak yang dapat mengambil data ini. Pesan yang sifatnya teks biasa ini dapat disadap oleh siapa saja yang berhasil memiliki akses ke dalam SMSC.

Maka dari itu, untuk mengurangi resiko pada layanan SMS maka dibutuhkan sebuah sistem keamanan pada layanan SMS yang mampu menjaga integritas dan keamanan isi pesan. Enkripsi dan dekripsi pesan dapat digunakan sebagai faktor keamanan tambahan pada layanan SMS. Dengan menerapkan algoritma kriptografi pada pesan yang dikirim, maka isi SMS menjadi sulit untuk dimengerti karena telah dienkripsi sehingga hanya dapat dibaca dengan menggunakan kunci enkripsi.

Untuk menjaga keamanan pesan yang bersifat rahasia, terdapat beberapa cara dan teknik tertentu yang dapat digunakan. Salah satunya dengan kriptografi yang berfungsi untuk menyamarkan pesan menjadi bentuk pesan tersandi. *Caesar cipher* merupakan salah satu algoritma *cipher* tertua dan merupakan salah satu jenis *cipher* substitusi yang membentuk *cipher* dengan cara melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama.

Dari uraian permasalahan di atas maka akan diterapkan suatu sistem keamanan berbasis android pada aplikasi pesan singkat yang berjudul "**Kriptografi *Short Message Service* Menggunakan Metode *Caesar Cipher* Berbasis Android**".

Terdapat beberapa penelitian terdahulu yang melakukan penelitian terkait dengan kriptografi *Short Message Service* berbasis android seperti berikut ini:
Pertama, penelitian [2] oleh Dian Rachmawati dan Ade Candra, 2015 yang berjudul "Implementasi Kombinasi *Caesar* dan *Affine Cipher* untuk Keamanan Data Teks". Penelitian kedua [3] yang berjudul "Enkripsi dan Dekripsi *Short Message Service* Menggunakan Algoritma *Caesar Cipher*" oleh Imbana Saputra, 2015. Penelitian ketiga oleh [4] Aditi Saraswat dkk, 2016 yang berjudul "*An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication*". Keempat, penelitian [5] yang berjudul "Pembuatan Aplikasi *Notes* Menggunakan Algoritma Kriptografi *Polyalphabetic Substitusion Cipher* Kombinasi Kode ASCII Dan Operasi XOR Berbasis Android" oleh Rizqi Sukma Kharisma dan Muhammad Aziz Fatchu Rachman, 2017. Penelitian kelima [6] oleh Benni Purnama dan Hetty Rohayani.AH, 2015 yang berjudul *A New Modified Caesar Cipher Cryptography*

Method with Legible Ciphertext from A Message to Be Encrypted. Penelitian keenam [7] oleh Ana Wahyuni, 2016 yang berjudul Kriptografi Dengan Algoritma *Grass Caesar*. Penelitian ketujuh [8] oleh Yusuf Triyuswoyo ST, dkk, 2014 yang berjudul Implementasi Algoritma Caesar, Cipher Disk dan Scytale pada Aplikasi Enkripsi dan Dekripsi Pesan Singkat, LumaSMS. Penelitian kedelapan [9] oleh Damai Subimawanto, dkk, 2014 yang berjudul Implementasi Algoritma Kriptografi Kode Caesar, Vigenere dan Transposisi untuk Sistem Proteksi Penggunaan Pesan Singkat (SMS) Pada *Smartphone* Android. Penelitian kesembilan [10] oleh Bonifacius Vicky Indriyono, 2016 yang berjudul Implementasi Sistem Keamanan File dengan Metode Steganografi EOF dan Enkripsi Caesar Cipher. Penelitian kesepuluh [11] oleh Muhammad Usman Rosyidi, 2017 yang berjudul Implementasi Algoritma Kriptografi RC4 Pada Aplikasi SMS Berbasis Java.

1.2 Rumusan Masalah

Dari latar belakang diatas, maka dapat kita ketahui bahwa kegiatan pada aplikasi pesan singkat adalah menyediakan kemampuan untuk mengirimkan pesan singkat. Maka dengan ini dapat disimpulkan, rumusan masalah yang dibahas adalah:

1. Bagaimana melakukan pengamanan informasi atau pesan pada media SMS berbasis android?
2. Bagaimana mengimplementasikan metode *caesar cipher* sehingga pesan teks SMS tersebut terjaga keamanannya saat terkirim?

1.3 Tujuan dan Manfaat Penelitian

1.3.1 Tujuan Penelitian

Berdasarkan perumusan masalah di atas, maka tujuan yang dicapai adalah membangun aplikasi kriptografi (enkripsi dan dekripsi) data SMS dengan metode *caesar cipher*, sehingga pesan yang penting atau rahasia tetap terlindungi saat dikirim dan tidak dapat dicuri atau dibaca oleh orang lain.

1.3.2 Manfaat Penelitian

Adapun manfaat dalam penelitian ini adalah sebagai berikut:

1. Membantu pengguna SMS khususnya yang menggunakan perangkat *mobile* berbasis android dalam mengamankan konten SMS antar pengirim dan penerima.
2. Menanggulangi penyadapan terhadap pesan SMS.

1.4 Batasan Masalah

Supaya penelitian ini lebih terarah dan memudahkan dalam pembahasan maka perlu adanya batasan masalah, adapun batasan masalah dalam penelitian ini adalah:

1. Algoritma kriptografi yang digunakan adalah algoritma *Caesar Cipher*.
2. Aplikasi yang dibangun difokuskan pada pengiriman SMS dan penerimaan SMS.
3. Aplikasi ini hanya dapat mengenkripsi dan mendekripsikan pesan berupa teks (SMS).
4. Enkripsi dan dekripsi pesan menggunakan alfabet Bahasa Indonesia.
5. Karakter petik satu (′) dan karakter at (@) tidak digunakan dalam enkripsi dan dekripsi.
6. Panjang kunci yang digunakan hanya 2 karakter.
7. *Hardware* yang digunakan adalah *smartphone* berbasis android.

1.5 Sistematika Penulisan

Sistematika dari penulisan laporan penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang masalah, rumusan masalah yang dihadapi, tujuan dan manfaat dilakukannya penelitian, batasan masalah, serta sistematika penulisan laporan.

BAB II LANDASAN TEORI

Bab landasan teori merupakan tinjauan pustaka, menjelaskan mengenai konsep dasar dan teori-teori dari penelitian yang digunakan serta untuk menjelaskan dan menyelesaikan permasalahan yang akan dikaji.

BAB III METODOLOGI PENELITIAN

Bab metodologi penelitian terdiri dari 3 bagian utama yaitu model pengembangan sistem, metode pengembangan sistem, dan *tools* pengembangan sistem (alat bantu dalam analisis dan merancang aplikasi).

BAB IV PEMBAHASAN

Bab ini berisi tentang Analisis Masalah, Analisis Kebutuhan, Analisis Sistem Berjalan, Perancangan Sistem, Identifikasi Sistem Usulan, Rancangan Sistem, Rancangan Layar, Implementasi, Tampilan Layar dan Pengujian.

BAB V PENUTUP

Bab ini menjelaskan kesimpulan dari penulisan disertai dengan saran-saran untuk meningkatkan kenyamanan dalam berkomunikasi melalui pesan singkat.