

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan ilmu dan teknologi terutama pada perusahaan saat ini terus berkembang. Modernisasi pada perusahaan membuat segala sesuatunya menjadi lebih lancar dan mudah, beberapa faktor pendukung perusahaan adalah internet, fasilitas Wifi, dan komputer yang dijadikan sebagai penunjang kemajuan pada suatu perusahaan. Dikarenakan kemajuan teknologi tersebut, menuntut suatu perusahaan untuk menggunakan sistem informasi yang handal, untuk terus-menerus mengikuti alur perkembangan ilmu dan teknologi yang kian berkembang pesat, serta dapat memberikan informasi yang di perlukan untuk pengambilan keputusan yang dapat menentukan maju dan mundurnya suatu perusahaan dikemudian hari.

Short Message Service (SMS) merupakan sebuah revolusi teknologi komunikasi yang sangat populer. Dengan menggunakan SMS seseorang dapat saling bertukar pesan dengan orang lain. Namun, dengan adanya masalah penyadapan SMS, seseorang sudah tidak lagi mempunyai hak privasi. Sehingga pada penelitian ini, penulis mengembangkan sebuah aplikasi pada telepon selular berbasis Android yang akan merubah pesan SMS menjadi kode-kode agar isi informasi dari SMS tersebut tidak diketahui orang lain.

DES (*Data Encryption Standard*) adalah algoritma cipher blok yang populer karena dijadikan standard algoritma enkripsi kunci-simetri. DES adalah nama standard enkripsi simetri, nama algoritma enkripsinya sendiri adalah DEA (*Data Encryption Algorithm*), namun nama DES lebih populer daripada DEA. Algoritma DES dikembangkan di IBM dibawah kepemimpinan W.L. Tuchman pada tahun 1972. Algoritma ini didasarkan pada algoritma Lucifer yang dibuat oleh Horst Feistel. Algoritma ini telah disetujui oleh National Bureau of Standard (NBS) setelah penilaian kekuatannya oleh National Security Agency (NSA) Amerika Serikat. DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis *cipher blok*. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit

plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (*internal key*) atau upa-kunci (*subkey*). Kunci internal dibangkitkan dari kunci eksternal (*external key*) yang panjangnya 64 bit.

Beberapa penelitian terdahulu Penelitian R.Rumani M (2015) yang berjudul DESAIN DAN IMPLEMENTASI APLIKASI SMS (*SHORT MESSAGE SERVICE*) PADA ANDROID MENGGUNAKAN ALGORITMA AES. Menurut penelitiannya Jika pesan yang kita kirimkan merupakan pesan yang tidak boleh di lihat oleh orang lain maka akan timbul permasalahan keamanan data. Oleh karena itu di butuhkan kewanaman pesan pada *smartphone* dengan menggunakan algoritma kriptografi maka pesan dapat di enkripsi dan di dekripsi dengan baik. Metode nya menggunakan android dalam pemrograman tersebut akan di gunakan algoritma AES.^[1] Penelitian Fuasan, Defi Akhsan Nur (2014) yang berjudul IMPLEMENTASI ALGORITMA AES MODE CBC UNTUK ENKRIPSI DAN DEKRIPSI PESAN SMS BERBASIS ANDROID. Aplikasi ini dibuat menggunakan bahasa pemrograman Java dan IDE (Integrated Development Environment) Eclipse dengan metode algoritma AES. Aplikasi SMS ini memanfaatkan algoritma AES sehingga memungkinkan pengguna untuk mengirimkan pesan singkat dengan enkripsi teks dan dapat melakukan dekripsi terhadap pesan terenkripsi sehingga tingkat keamanan informasi pesan tersebut dapat ditingkatkan, penerapan kriptografi dalam aplikasi SMS ini dibutuhkan dalam menjaga kerahasiaan suatu pesan. Hasil dari implementasi ini adalah menghasilkan aplikasi SMS yang dapat mengirim pesan asli SMS maupun mengubah pesan asli SMS menjadi kode tertentu, sehingga diharapkan pesan SMS memiliki tingkat keamanan tinggi agar terhindar dari penyadapan dan hal lain yang merugikan.^[2] Penelitian Kusnadi Kusnadi, Muhammad Hatta, Nanang Sanjaya (2016) yang berjudul IMPLEMENTASI ALGORITMA BLOWFISH DAN VIGENERE CHIPER PADA APLIKASI SMS BERBASIS ANDROID. Keamanan isi pesan SMS diberikan untuk memberikan perlindungan pada isi pesan SMS agar tidak dapat dibaca oleh orang yang tidak dikehendaki atau hanya dapat dibaca oleh orang tertentu saja. Diperlukan pengamanan isi pesan untuk menjaga kerahasiaan isi pesan. Pengamanan isi pesan SMS melalui aplikasi ponsel dengan cara melakukan

penyandian (enkripsi) dengan algoritma blowfish dan vigenere chiper. Dengan aplikasi enkripsi dan dekripsi pesan ini diharapkan mampu memaksimalkan pengamanan isi pesan terhadap ancaman terhadap pembacaan isi pesan oleh orang yang tidak diinginkan atau tidak memiliki hak dalam pembacaan isi pesan.^[3] Penelitian Heliza Rahmania Hatta dkk (2017) tentang APLIKASI KRIPTOGRAFI PESAN SHORT MESSAGE SERVICE PADA SMARTPHONE BERBASIS ANDROID DENGAN METODE PLAYFAIR CIPHER, Penelitian ini bertujuan untuk membangun suatu aplikasi kriptografi pesan SMS (*Short Messsage Service*) pada smartphone berbasis android dengan metode *playfair cipher*, yang dapat mengirim kriptografi pesan SMS dan menerima pesan teks terenkripsi yang kemudian didekripsi. Aplikasi ini melakukan kriptografi pada teks berupa huruf. Kunci yang digunakan berupa huruf. Hasil dari penelitian ini adalah berupa aplikasi berbasis android yang dapat melakukan pengiriman pesan SMS yang telah terenkripsi menggunakan metode *playfair cipher*, sehingga kerahasiaan dari pesan tersebut dapat terjaga keamanannya.^[4] Penelitian Ari Amir Alkodri, R. Burham Isnanto F, 2014, Prototype aplikasi untuk mengetahui tata letak ATM di Pangkalpinang pada smartphone android, Program Studi Teknik Informatika, STMIK Atmaluhur, Pangkalpinang. Jurnal teknologi dan Sistem Komputer, Vol.1, No.1, September 2014, ISSN 2406-7962, Pada penelitian ini penulis menemukan masalah yaitu sulitnya bagi masyarakat Bangka Belitung dan Masyarakat luar kota untuk mengetahui letak ATM yang ada Di pangkalpinang. Hasil dari penelitian ini adalah aplikasi ini dapat membantu masyarakat sangat mempermudah transaksi perbankan dengan mudah mengetahui posisi ATM yang terdekat dimana pada aplikasi untuk mengetahui tata letak ATM di Pangkalpinang pada smartphone android hampir semua Bank ada di Pangkalpinang Kepulauan Bangka Belitung.^[5]

Berdasarkan permasalahan diatas penulis membuat solusi dengan penelitian yang berjudul **“PEMANFAATAN ALGORITMA BLOK CHIPER DES (*DATA ENCRYPTION STANDARD*) UNTUK MENGENKRIPSI SMS (*SHORT MESSAGE SERVICES*) PADA PLATFORM ANDROID”**.

1.2 Rumusan Masalah

Berikut merupakan permasalahan yang penulis temukan angkat dalam penelitian ini :

1. Bagaimana cara kerja kriptografi dengan metode DES?
2. Bagaimana cara membuat dan menerapkan metode kriptografi DES pada android?

1.3 Batasan Masalah

Pada penelitian ini dibuat suatu batasan masalah agar pembahasan tidak meluas, adapun batasan masalahnya adalah sebagai berikut :

1. Perancangan aplikasi ini menggunakan Android Studio.
2. Aplikasi hanya dapat berjalan di sistem operasi android.

1.4 Tujuan dan Manfaat Penelitian

Adapun tujuan dan manfaat penelitian yang akan dicapai dari aplikasi ini adalah :

1. Agar dapat membuat dan menerapkan aplikasi enkripsi SMS berbasis android.
2. Dapat mengimplementasikan aplikasi enkripsi SMS berbasis android.
3. Dapat menganalisis cara kerja Algoritma DES.
3. Membantu pengguna mengamankan pesannya dari penyadapan.

1.5 Sistematika Penulisan

Sistematika penulisan laporan Skripsi ini bertujuan agar proses dokumentasi pembuatan laporan secara terstruktur sehingga mudah dipahami. Adapun sistematika dalam penulisan laporan ini terdiri dari 5 (lima) bab yaitu sebagai berikut :

BAB I

PENDAHULUAN

Bab ini awal yang mengemukakan latar belakang, rumusan masalah , batasan masalah yang akan dibahas, metodologi

penelitian, tujuan dan manfaat penelitian, dan sistematika penulisan.

BAB II

LANDASAN TEORI

Pada bab ini berisi tinjauan pustaka, menguraikan teori-teori yang mendukung judul, dan mendasari pembahasan secara detail. Landasan teori dapat berupa definisi-definisi atau model yang langsung berkaitan dengan ilmu atau masalah yang diteliti

BAB III

METODOLOGI PENELITIAN

Bab Metodologi Penelitian terdiri dari 3 bagian utama yaitu model pengembangan perangkat lunak, metode penelitian, dan *tools* (alat bantu dalam analisis dan merancang Aplikasi).

BAB IV

HASIL DAN PEMBAHASAN

Bab ini berisi antara lain: Tinjauan umum yang menguraikan tentang gambaran umum objek penelitian, yang dipergunakan untuk memecahkan masalah-masalah yang dihadapi, berkaitan dengan kegiatan penelitian. Bab ini point utamanya adalah analisis masalah, perancangan, dan implementasi sistem.

BAB V

PENUTUP

Pada Bab ini berisi tentang kesimpulan dan saran yang memaparkan hasil-hasil dari tahapan penelitian, dari tahap analisis, desain, implementasi desain, hasil testing dan implementasinya.