BAB I

PENDAHULUAN

1.1 Latar Belakang

Dewasa ini sudah banyak cara untuk mendapatkan Informasi termasuk untuk pengiriman pesan, sudah banyak sarana untuk mengirimkan pesan sehingga kita bisa dengan mudah mengirim dan menerima pesan. Di era digital ini alat untuk mengirim pesan sudah banyak termasuk medianya seperti SMS, atau dengan IM seperti WhatssApp, Line, BBM dan sebagainya, sehingga kita bisa mengirim pesan dengan cepat begitupun sebaliknya kita bisa menerima pesan dengan cepat pula. Begitu cepat dan mudahnya kita mengirim pesan kepada orang lain meski jauh sekalipun, hanya dengan sekali klik pesan tersebut terkirim dan diterima pada saat yang sama. Dari fasilitas pengiriman pesan yang kita dapatkan ini, kita sering mengabaikan tentang keamanan pesan dari pihak ketiga. Dan salah satu yang harus benar-benar dijaga keamanan dan kerahasiaannya adalah pesan yang bersifat rahasia negara karena jika pesan itu diketahui oleh pihak ketiga dan tersebar maka akan mengancam persatuan dan keamanan negara.

Ada berbagai macam pengamanan pesan, salah satunya dengan cara meng-enkripsi pesan tersebut. Enkripsi adalah proses untuk menyamarkan isi dari pesan, sehingga orang yang tidak berkepentingan atau bahkan penyadap tidak bisa mengetahui isi dari pesan tersebut. Proses enkripsi membuat pesan yang tersamarkan isinya namun masih berbentuk tulisan oleh karena itu walau pesan itu telah di enkripsi tetap akan menimbulkan kecurigaan sehingga dapat memicu orang yang ingin tau makna pesan untuk mencari makna sebenarnya dari pesan

tersebut. Kriptografi masih bisa depecahkan oleh para Kriptanalis yang memang orang yang mempunyai kemampuan untuk memecahkan enkripsi pesan.

Berdasarkan latar belakang di atas penulis mencoba untuk menerapkan Algoritma Kriptografi AES 128 bit dimana Algoritma ini masih aman sampai saat ini dari para kriptanalis. Penelitian ini juga sebagai tugas akhir untuk menyelesaikan studi pada program S1 Teknik Informatika dengan judul **"IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES 128bit SEBAGAI PENGAMAN SMS PADA SMARTPHONE BERBASIS ANDROID".**

1.2 Rumusan Masalah

Dari latar belakang diatas dapat disimpulkan bahwa rumusan masalahnya adalah :

1. Bagaimana cara mengamankan pesan yang akan dikirimkan ?
2. Bagaimana membuat aplikasi pesan android ?
3. Bagaimana menerapkan Algoritma kriptografi AES 128bit pada aplikasi pesan android ?

1.3 Batasan Masalah

Penelitian ini memiliki batasan atau ruang lingkup seperti :

1. Software yang digunakan untuk membuat aplikasi adalah netbeans dan eclipse.
2. Pembuatan script dengan menggunakan bahasa pemrograman Java untuk mobile.
3. Software ini digunakan untuk OS android versi 4.0.4

1.4 Tujuan Penelitian

Adapun maksud dan tujuan penelitian ini adalah :

1. Penerapan algoritma kriptografi sebagai pengamanan pesan di handphone android.
2. Untuk memenuhi syarat kelulusan Strata Satu di STIMIK AMIKOM jurusan Teknik Informatika.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah :

1. Bagi penulis

   Pendalaman ilmu yang telah dipelajari pada saat kuliah khususnya Kriptografi dan sebagai syarat kelulusan program S1 Teknik Informatika STIMIK AMIKOM YOGYAKARTA.

2. Bagi STIMIK AMIKOM YOGYAKARTA

   Menambah judul karya ilmiah yang ada di STIMIK AMIKOM YOGYAKARTA dan bisa dijadikan referensi oleh mahasiswa dalam mempelajari kriptografi.

3. Bagi pembaca dan masyarakat umum

   Masyarakat bisa mengamankan pesan kepada orang yang dituju tanpa khawatir akan diketahui oleh pihak ketiga melalui perangkat Android mobile serta dapat menyadarkan bahwa keamanan pesan sangatlah penting.

1.6 Metodelogi Penelitian

1. Metode yang digunakan

Metode yang digunakan dalam penelitian ini yaitu dengan mencari solusi bagaimana cara mengamankan pesan dari penyadap.

2. Metode pengumpulan data

Metode yang digunakan dalam mengumpulkan data yaitu :

1. Observasi

   Observasi tentang bagaimana cara untuk menerapkan algoritma kriptografi pada aplikasi pesan pada android sebagai pengaman pesan.

2. Pustaka

   Referensi yang dibutuhkan dalam penelitian ini baik dari jurnal, buku, maupun internet.

3. Metode Analisa Data

Metode yang digunakan yaitu dengan menganalisa dari data yang telah diperoleh. Dari Rumusan Masalah dapat diperoleh bahwa masalahnya adalah bagaimana cara membuat aplikasi untuk mengamankan pesan supaya pesan yang kita kirim dan pihak ketiga tidak bisa membaca pesan tersebut, kemudian dari observasi dan pustaka kita dapat membuat solusinya. Setelah solusi didapat maka kita dapat membuat aplikasinya.

1.7 Sistematika Penulisan

Adapun sistematika penulisan dalam penelitian ini yaitu:

BAB I : PENDAHULUAN

Pada bab ini berisikan Latar Belakang, Rumusan Masalah, Tujuan Penelitian, Batasan variable, Metodelogi Penelitian dan Sistematika Penulisan.

BAB II: LANDASAN TEORI

Landasan Teori ini adalah kumpulan dari studi pustaka penulis yang didalamnya membahas seputar teori-teori yang mendukung dalam pembuatan penelitian ini.

BAB III: ANALISIS DAN PERANCANGAN SISTEM

Pada BAB ini membahas tentang analisis terhadap sistem yang akan dibuat seperti kebutuhan apa saja yang diperlukan untuk membuat aplikasi, UML, rancangan basis data, rancangan user interface dan rancangan tentang aplikasi yang akan dibuat.

BAB IV : IMPLEMENTASI DAN PEMBAHASAN

Pada bab ini akan di akan mengimplemantasikan hasil dari analisis dan perancangan sistem yang telah di buat.

BAB V : PENUTUP

Pada bab ini akan membahas tentang kesimpulan penelitian dan saran yang dituliskan oleh penulis.