BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Kemajuan dan perkembangan teknologi informasi dewasa ini berpengaruh pada hampir semua aspek kehidupan manusia, terutama dalam hal berkomunikasi. Komunikasi mengandung sebuah informasi yang bersifat rahasia maka keamanan informasi menjadi faktor utama yang harus dipenuhi. Berbagai hal telah dilakukan untuk mendapatkan jaminan keamanan untuk informasi rahasia ini. Salah satu cara yang digunakan adalah dengan menyandikan isi informasi menjadi suatu kode yang tidak dimengerti sehingga apabila disadap maka akan kesulitan untuk mengetahui isi informasi yang sebenarnya. [1]

Keamanan kriptografi modern hanya dengan merahasiakan knci yang dimiliki dari orang lain, tanpa harus merahasiakan algoritma itu sendiri. Kunci berfungsi sama seperti *password*. Jika keseluruhan dari keamanan algoritma tergantung pada kunci yang dipakai maka, algoritma ini dapat dpublikasikan dan dianalisis oleh orang lain. Jika algoritma yang telah dipublikasikan bisa dipecahkan dalam waktu singkat oleh orang lain maka, algoritma tersebut belum aman untuk digunakan.[2]

Untuk menyandikan sebuah informasi yang bersifat rahasia diperlukan sebuah algoritma kriptografi yang dapat mengamankan integritas data atau informasi. Dengan menggunakan teknik enkripsi terhadap integritas data maka

suatu informasi tidak bisa dibaca oleh orang yang tidak berkepentingan. Pada perkembangannya kriptografi mengalami pengembangan, buktinya dengan munculnya beberapa algoritma kriptografi baru yang dapat menambah perbendaharaan ilmu dalam bidang kriptografi.[3]

Dalam perancangan aplikasi ini digunakan program bahasa Java dengan software Android Studio IDE. Software di pilih karena aplikasi akan dibuat berbasis mobile dengan sistem operasi android.

1.2 Rumusan Masalah

Berdasarkan analisis latar belakang masalah maka perumusan masalah adalah sebagai berikut :

1. Bagaimana perancangan aplikasi media pembelajaran kriptografi sebagai pendukung materi belajar algoritma kriptografi ?
2. Apakah aplikasi dapat memberikan contoh hasil dari enkripsi dan dekripsi dari metode yang dipakai?

1.3 Batasan Masalah

Dengan uraian rumusan masalah supaya hasil tepat seperti yang diinginkan maka batasan pada perancangan dan pembuatan aplikasi adalah :

1. Metode kriptografi yang digunakan adalah AES dan RSA.
2. Input merupakan *string* yang dirubah menjadi *ciphertext*.
3. Aplikasi dibuat menggunakan bahasa JAVA dengan software IDE Android Studio.
4. Aplikasi hanya terbatas untuk telepon seluler yang menggunakan sistem operasi android.

5. Algoritma enkripsi aplikasi dibuat menurut pengetahuan pakar dan buku yang telah dipilih.

1.4 Maksud Dan Tujuan Penelitian

Tujuan dari penelitian ini adalah :

1. Membantu memudahkan belajar kriptografi dengan menggunakan sebuah aplikasi.
2. Dapat mengerti dan menggunakan sebuah algoritma kriptografi dengan mudah.
3. Menjadi referensi materi belajar yang menarik bagi para pengguna.

Menganalisis kelebihan dan kekurangan algoritma kriptografi simetris AES dengan algoritma asimetris RSA.

1.5 Manfaat Penelitian

Dalam perancangan aplikasi ada beberapa manfaat yang diambil dalam pembelajaran algoritma kriptografi. Beberapa contoh manfaat penelitian adalah :

1. Dengan adanya penelitian in dapat menambahkan kepustakaan terutama dalam bidang algoritma kriptografi.
2. Dengan menggunakan aplikasi yang dibangun dalam penelitian ini akan membantu pengguna yang ingin belajar ilmu kriptografi.

Hasil penelitian dapat menjadi referensi bagi pembaca yang ingin mengetahui langkah dan proses enkripsi data, dan membagi pengetahuan di bidang ilmu kriptografi.

1.6 Metode Penelitian

Metode pengumpulan data yang dugunakan untuk penelitian ini adalah ;

1. Metode studi kepustakaan

   Studi kepustakaan ure yaitu teknik pengumpulan data yang dilakukan dengan pengamatan terhadap literatur – literatur, buku – buku pendukung, catatan, dan berbagai laporan yang bersangkutan dengan bahan penelitian.

2. Metode Browsing

   Merupakan pengumpulan bahan yang bersumber dari internet dengan mengunjungi situs yang menyediakan bahan penelitian.

1.7 Sistematika Penulisan

Laporan ini telah disusun secara sistematis dalam 5 bab, berikut adalah sistematika penulisan penelitian ini :

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metodologi penelitian dan sistematika penelitian.

BAB II LANDASAN TEORI

Bab ini menjelaskan teori – yang digunakan oleh penulis untuk memulai penelitian. Pada bab ini juga dituliskan tentang alat dan perangkat yang digunakan untuk keperluan penelitian dan pembuatan aplikasi.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini akan dijelaskan konsep umum objek penelitian analisis, rancangan, dan proses pembuatan aplikasi.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini menjelaskan tentang implementasi dan pengujian aplikasi yang telah dibuat beserta analisis hasilnya.

BAB V PENUTUP

Bab ini berisi tentang kesimpulan yang diambil dan saran yang diberikan dalam pengembangan aplikasi untuk kedepannya yang diharapkan dapat lebih bermanfaat bagi pihak – pihak yang terlibat.