

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.

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. Ada beberapa algoritma enkripsi yang terbuka untuk dipelajari dan digunakan dalam proses keamanan data, seperti *Data Encryption Standard (DES)*, *RC-4*, *TwoFish*, *RC-5*, *CAST*, *IDE*, *DSA* dan lain-lain.

Metode enkripsi yang dibahas adalah *RC-4* dan *DSA*. Algoritma *RC-4* merupakan salah satu algoritma kunci simetris yang berbentuk stream chipper.

Sedangkan DSA merupakan dalam algoritma kriptografi asimetri menggunakan pembangkitan kunci. Dalam kenyataannya sebuah algoritma kriptografi yang sudah ada sulit untuk dipelajari oleh seorang pemula.

Dalam perancangan aplikasi ini penulis menggunakan program bahasa Java dengan *software* Eclipse. Dipilih *software* tersebut karena akan dibuat dalam bentuk *mobile* dengan platform android sehingga memudahkan dalam penggunaannya.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, maka permasalahan yang dapat didefinisikan adalah Bagaimana merancang aplikasi kriptografi RC-4 dan DSA sebagai pendukung belajar ilmu kriptografi?

1.3 Batasan Masalah

Untuk menghindari terlalu melebarnya objek penelitian, maka di butuhkan batasan masalah, antara lain :

1. Algoritma Kriptografi yang digunakan adalah RC-4 dan DSA.
2. Input data berupa teks.
3. Aplikasi dibuat menggunakan bahasa Java dengan *software* Eclipse.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah :

1. Memudahkan mempelajari kriptografi dalam bentuk aplikasi.
2. Membantu memahami sebuah algoritma kriptografi dengan mudah dan dapat dipergunakan dengan mudah.
3. Sebagai bahan belajar yang menarik untuk belajar kriptografi bagi pemula.

4. Menganalisis kelebihan dan kekurangan dari aplikasi kriptografi simetris RC-4 dan kriptografi asimetris DSA.

1.5 Manfaat Penelitian

Dalam perancangan perangkat aplikasi kriptografi terdapat beberapa manfaat yang dapat digunakan dalam pembelajaran ilmu kriptografi. Adapun berbagai manfaat dari perancangan perangkat lunak yaitu:

1. Diharapkan dari perancangan ini dapat memperkaya literatur mengenai ilmu kriptografi.
2. Aplikasi ini dibuat guna membantu pemula yang ingin belajar ilmu kriptografi.

1.6 Metodologi Penelitian

Langkah - langkah dalam melakukan penelitian yang berjudul "Perancangan aplikasi kriptografi RC4 dan DSA sebagai media belajar kriptografi berbasis mobile" ini adalah sebagai berikut :

1. Pengumpulan data
 - a. Metode Kepustakaan

Metode pengumpulan data yang dilakukan dengan cara membaca, mempelajari, mencari bahkan menulis dari sebuah buku, artikel, jurnal ilmiah, majalah baik dari media cetak maupun media elektronik yang berkaitan dengan topik yang dibahas dalam pembuatan aplikasi.

b. Metode *browsing*

Metode *browsing* yaitu teknik pengumpulan rujukan yang bersumber dari internet dengan mengunjungi situs yang berhubungan dengan penelitian ini.

2. Analisis data

Melakukan analisis data yang telah dikumpulkan untuk penyusunan laporan kemudian merancang dan membuat aplikasi. Analisis data dalam penelitian meliputi :

a. Analisis kebutuhan fungsional

Merupakan pendefinisian fungsi sistem yang harus disediakan, bagaimana reaksi sistem terhadap input dan apa yang harus dilakukan sistem pada situasi khusus.

b. Analisis kebutuhan non fungsional

Menganalisis kebutuhan pendukung bagi sistem.

3. Perancangan aplikasi

Perancangan aplikasi meliputi perancangan antarmuka.

4. *Testing*

Pada tahap ini dilakukan *testing* dan penyesuaian (jika belum sesuai) pada aplikasi yang telah dibuat.

5. Implementasi aplikasi

Mengimplementasikan aplikasi yang telah dibuat.

1.7 Sistematika Penulisan

Dalam penyusunannya, laporan ini disusun secara sistematis dalam 5 bab, adapun sistematika penulisan pada penelitian ini adalah :

BAB I PENDAHULUAN

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

BAB II LANDASAN TEORI

Bab ini menjelaskan landasan Teori menjelaskan tentang teori-teori yang digunakan oleh penulis sebagai dasar penelitian, pada bab ini juga disampaikan tentang tools atau software yang digunakan dalam pembuatan aplikasi untuk keperluan penelitian.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini menjelaskan tentang gambaran umum objek penelitian, analisis, rancangan implementasi, dan proses pembuatan aplikasi.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

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

BAB V PENUTUP

Bab ini berisi tentang kesimpulan dan saran yang digunakan dalam pengembangan perangkat lunak di masa depan yang diharapkan dapat bermanfaat bagi seluruh pihak yang terlibat.