BAB I

PENDAHULUAN

1.1 Latar Belakang Pemilihan Judul

Dalam sebuah masalah kerahasian data, data yang rahasia harus diamankan terlebih dahulu dengan berbagai macam cara, salah satunya adalah dengan menggunakan metoda kriptografi. Agar data / informasi yang dikirim tidak diketahui oleh orang lain yang tidak berkepentingan. Metoda kriptografi yang digunakan untuk mengamankan data ada bermacam – macam. Masing – masing metoda memiliki kelebihan dan kekurangan. Salah satu metoda kriptografi yang dianggap sebagai algoritma *block cipher* yang terbaik dan teraman yang tersedia untuk publik sampai saat ini adalah metoda kriptografi IDEA (*International Data Encryption Algorithm*).

Metoda IDEA diperkenalkan pertama kali oleh Xuejia Lai dan James Massey pada tahun 1990 dengan nama PES (*Proposed Encryption Standard*). Setelah Biham dan Shamir mendemonstrasikan *cryptanalysis* yang berbeda, sang penemu memperkuat algoritma mereka dari serangan dan algoritma hasil pengubahan tersebut dan diberi nama IPES (*Improved Proposed Encryption Algorithm*). Kemudian pada tahun 1992, IPES diganti namanya menjadi IDEA (*International Data Encryption Algorithm*).

Metoda IDEA ini menggunakan beberapa operasi dasar, seperti operasi logika *XOR* (*Exclusive – OR*), operasi perkalian mod $2^{16} + 1$ (*multiplication*

modulo 2^{16} + 1) dan operasi penambahan mod 2^{16} (*addition modulo* 2^{16}). Metoda ini terdiri dari 8 putaran (*round*) dan menggunakan 64 *bit plaintext* dengan panjang kunci sebesar 128 *bit*.

Berdasarkan uraian di atas, penulis bermaksud untuk mengambil tugas akhir (skripsi) dengan judul " Pengamanan Data dengan Metoda Kriptografi IDEA ".

1.2 Perumusan Masalah

Yang menjadi permasalahan dalam menyusun tugas akhir (skripsi) ini adalah bagaimana merancang perangkat lunak pembelajaran metoda kriptografi IDEA yang telah dikembangkan dengan inputan *plaintext* lebih kecil dan lebih besar dari 64 bit (32 bit dan 128 bit).

1.3 Tujuan dan Manfaat

Tujuan penyusunan tugas akhir (skripsi) ini adalah untuk merancang suatu perangkat lunak pembelajaran untuk membantu pemahaman metoda kriptografi IDEA dan mengembangkan inputan *plaintext* lebih kecil dan lebih besar dari 64 bit (32 bit dan 128 bit)..

Manfaat dari penyusunan tugas akhir (skripsi) ini yaitu untuk membantu pembelajaran metoda kriptografi IDEA dan perangkat lunak dapat digunakan sebagai fasilitas pendukung dalam proses belajar mengajar.

1.4 Pembatasan Masalah

Pembatasan permasalahan dalam merancang perangkat lunak ini adalah :

1. Perangkat lunak akan menampilkan tahap – tahap perhitungan dalam bentuk bilangan biner.
2. *Input* data berupa bilangan biner, desimal, heksadesimal dan karakter (*string*).
3. *Input* data / plainteks dengan jumlah bit 32, 64,dan 128 bit.
4. Perangkat lunak tidak menampilkan tahap – tahap konversi bilangan ke dalam bilangan biner.
5. Perangkat lunak menyediakan teori – teori dasar dari metoda IDEA.

1.5 Sistematika Penulisan

Sistematika penulisan dari skripsi ini terdiri dari beberapa bagian utama sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini akan menjelaskan mengenai latar belakang pemilihan judul skripsi "Pengamanan Data dengan Metoda Kriptografi IDEA", rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Bab ini akan membahas mengenai tinjauan pustaka yang berkaitan dengan definisi kriptografi, sejarah kriptografi, jenis kriptografi, operasi matematika yang berhubungan dengan kriptografi, Enkripsi dan Dekripsi pada Algoritma IDEA.

BAB 3 METODOLOGI PENELITIAN

Bab ini membahas mengenai pendefinisian lingkup sistem dan pemodelan pada pengamanan data menggunakan metode IDEA.

BAB 4 ANALISIS DAN PERANCANGAN SISTEM

Bab ini berisi implementasi dari Pengamanan Data dengan Mtoda Kriptografi IDEA dan pengujian sistem secara manual.

BAB 5 KESIMPULAN dan SARAN

Bab ini akan memuat kesimpulan isi dari keseluruhan uraian bab-bab sebelumnya dan saran-saran dari hasil yang diperoleh yang diharapkan dapat bermanfaat untuk pengembangan selanjutnya.