BAB I

PENDAHULUAN

1.1 Latar Belakang

Metode kriptografi digunakan untuk mengamankan data yang bersifat rahasia agar tidak diketahui oleh orang lain. Metode kriptografi yang dapat digunakan untuk mengamankan data. Ada bermacam-macam metode kriptografi. Setiap metode memiliki kelebihan dan kekurangannya masing-masing. Namun, masalah utamanya adalah bagaimana mengetahui dan memahami cara kerja atau algoritma dari metoda kriptografi tersebut. Penulis memilih pembelajaran metode kriptografi IDEA karena menurut Bruce Schneier metode IDEA ini merupakan algoritma *block cipher* yang terbaik dan teraman yang disediakan untuk publik.

Metode IDEA ini menggunakan *confusion* dan *diffusion*. Berbeda dari metode *block cipher* lainnya,metode IDEA menggunakan operasi aljabar yang tidak kompatibel yaitu XOR, penambahan modulo 2^{16}, perkalian modulo $2^{16} + 1$.

1.2 Rumusan Masalah

Dari latar belakang di atas, maka akan dibuat suatu aplikasi "Pembelajaran Metoda Kriptografi IDEA (*International Data Encryption Algorithm*)" yang dapat digunakan oleh user untuk mempelajari bagaimana proses pembentukan kunci, proses enkripsi dan proses dekripsi dengan menggunakan metoda Kriptografi IDEA.

1.3 Ruang Lingkup

Agar penulisan ini dapat mencapai sasaran dan tujuan yang diharapkan maka diberikan batasan masalah sebagai berikut:

1. Perangkat lunak akan mengolah tahap – tahap perhitungan dalam bentuk bilangan biner dan heksadesimal.
2. *Input* data berupa karakter (*string*).
3. Perangkat lunak tidak dapat mengolah input berupa gambar.
4. Perangkat lunak tidak menampilkan tahap – tahap konversi bilangan ke dalam bilangan biner.
5. Jumlah karakter untuk kunci harus 16 karakter, untuk plainteks dan chiperteks 8 harus karakter.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk merancang suatu perangkat lunak pembelajaran untuk membantu pemahaman metoda kriptografi IDEA. Selain itu di harapkan perangkat lunak dapat digunakan sebagai fasilitas pendukung dalam proses belajar mengajar.