

# BAB I PENDAHULUAN

## 1.1 Latar Belakang

Perkembangan teknologi mengalami kemajuan yang pesat dan canggih. Salah satu teknologi yang berkembang dengan pesat tersebut adalah teknologi penyandian data yang saat ini banyak digunakan untuk pengamanan data yang ada didalam komputer adalah Kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat lagi dimengerti lagi maknanya (Munir, 2004). Salah satunya algoritma kriptografi untuk pengamanan informasi atau data adalah Algoritma Skipjack.

Algoritma Skipjack merupakan salah satu algoritma kriptografi untuk penyandian data file dengan multi format. Algoritma Skipjack adalah algoritma kriptografi *block cipher* yang menggunakan 64 bit *block* data dan 8 bit kunci. Dalam hal keamanan skipjack lebih aman dibanding dengan DES (*Data Encryption Standard*) yang juga merupakan sistem sandi data, karena pada skipjack digunakan 8 bit kunci dan dibagi 10 bagian sub kunci serta dilakukan proses iterasi 32 langkah untuk menghasilkan data sandian (*ciphertext*).

Untuk meningkatkan keamanan data maka dibutuhkan sebuah algoritma skipjack. Berdasarkan pengamatan yang sudah dilakukan, masalah yang sering terjadi adalah penyimpanan suatu data atau pengiriman data menggunakan media digital membutuhkan suatu proses yang harus menjaga keamanan dan keutuhan dari sebuah data misalnya saja file dengan multi format. File harus tetap bersifat rahasia selama proses pengirimannya hingga sampai ke tempat tujuan karena sangat rentan untuk diganti dan dimanipulasi keasliannya karena dapat jatuh ke tangan yang salah melalui penyadapan untuk dimanfaatkan dan disalahgunakan orang lain.

Dalam penelitian ini akan menerapkan algoritma skipjack pada aplikasi berbasis web untuk penyandian data file multi format agar lebih meningkatkan keamanan suatu data file atau informasi yang memang bukan untuk konsumsi publik. Proses kerja dari algoritma ini adalah dengan mentransformasi data atau informasi yang asli (*Plaintext*) melewati proses enkripsi sehingga menghasilkan data atau informasi yang disandikan (*Chipertext*) yang dilakukan pada sisi pengirim, kemudian untuk memperoleh kembali data atau informasi yang asli,

maka data atau informasi yang telah disandikan harus melalui proses dekripsi sehingga akan menghasilkan kembali data atau informasi yang asli.

## **1.2 Perumusan Masalah**

Berdasarkan uraian latar belakang tersebut, dapat dirumuskan permasalahannya yaitu Bagaimana menerapkan Algoritma Skipjack dalam penyandian data file serta proses enkripsi dan dekripsi pada aplikasi berbasis web.

## **1.3 Tujuan Penelitian**

Penelitian ini bertujuan untuk menghasilkan sebuah aplikasi yang dapat digunakan dalam penyandian data dengan memanfaatkan algoritma skipjack sehingga dapat mencegah potensi kebocoran informasi yang jatuh kepada pihak ketiga.

## **1.4 Pembatasan Masalah**

Batasan masalah dibuat agar sistem tidak menyimpang dari perencanaan sehingga tujuan utama dari pembuatan sistem ini dapat tercapai. Adapun batasannya sebagai berikut:

1. Dapat mengenkripsikan segala jenis file dengan ukuran dibawah 5MB.
2. Tidak membahas algoritma kompresi dan dekompresi.
3. Untuk melihat enkripsi dan dekripsi file diharuskan download file tersebut.
4. Tidak membahas tentang keamanan jaringan.
5. Aplikasi yang dibangun berbasis website.

## **1.5 Sistematika Penulisan**

Adapun sistematika dalam penulisan skripsi yang akan dibuat ada lima bab yang terdiri dari Bab I Pendahuluan, Bab II Landasan Teori, Bab III Metodologi Penelitian, Bab IV Hasil dan Analisis, serta Bab V Kesimpulan dan Saran.

### **BAB I Pendahuluan**

Pada Bab ini dijelaskan mengenai latar belakang permasalahan, rumusan masalah, maksud dan tujuan, pembatasan masalah, dan sistematika penulisan.

## BAB II Landasan Teori

Pada Bab ini dijelaskan mengenai tinjauan pustaka, dasar-dasar teori, rujukan, metode yang berhubungan dengan judul dan uraian sistematis tentang hasil-hasil penelitian yang didapat oleh penelitian terdahulu.

## BAB III Metodologi Penelitian

Pada Bab ini membahas tentang alat-alat penelitian, metode penelitian, analisis sistem dan perancangan aplikasi penyandian data menggunakan algoritma skipjack.

## BAB IV Hasil dan Analisis

Pada Bab ini berisi hasil penelitian yang telah dilakukan dan hasil pengujian terhadap kinerja dari aplikasi yang telah dibangun.

## BAB V Kesimpulan dan Saran

Pada bagian ini memaparkan kesimpulan yang didapatkan dari aplikasi yang dibangun dan saran untuk mengembangkan aplikasi.