

BAB I

PENDAHULUAN

1.1 Latar Belakang

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting. Bagi suatu perusahaan, organisasi, instansi, dan lainnya telah memanfaatkan teknologi berbentuk file dokumen *portable document format* (PDF) baik berupa pesan, data, atau informasi. Dalam hal ini sangat terkait dengan betapa pentingnya pesan, data, atau informasi tersebut oleh pihak atau orang yang berkepentingan. Keamanan terhadap data yang disimpan dalam file dokumen PDF sudah sangat dibutuhkan. Salah satu cara mengamankan sebuah data adalah dengan menggunakan kriptografi. Kriptografi adalah ilmu dan seni penyimpanan pesan, data, atau informasi secara aman.

Salah satu metode keamanan yang digunakan adalah algoritma RC4. RC4 merupakan algoritma kriptografi kunci simetris dan bersifat *stream cipher* sehingga panjang karakter hasil enkripsi (*cipherteks*) mempunyai panjang karakter yang sama dengan data asli (*plaintext*). Teknik kriptografi simetris ini dipilih karena dengan algoritma ini proses enkripsi dan dekripsi data dapat dilakukan dengan waktu yang lebih cepat dibandingkan dengan algoritma kriptografi asimetris.

Berdasarkan pada informasi yang dipaparkan, peneliti akan membuat sebuah penerapan enkripsi dan dekripsi dengan menggunakan metode algoritma RC4 pada file dokumen PDF dengan mengenkripsi dan mendeskripsi data. Untuk

mengamankan file dokumen PDF dengan metode yang berbeda, yaitu algoritma RC4 dengan membatasi pengenkripsian 3 file dalam 1 kali proses untuk mempermudah pengguna dalam mengamankan data. Berdasarkan latar belakang diatas, maka akan dibuat “Aplikasi Keamanan Data Berbentuk File Dokumen *Portable Document Format* (PDF) dengan menggunakan Algoritma RC4”.

1.2 Identifikasi Masalah

Berdasarkan penjelasan pada latar belakang diatas, maka identifikasi masalah dalam penelitian ini adalah bagaimana algoritma RC4 diimplementasikan dalam aplikasi keamanan data yang digunakan untuk mengamankan data file dokumen PDF.

1.3 Rumusan Masalah

Perumusan masalah yang dapat dirumuskan dari permasalahan diatas adalah sebagai berikut ini:

1. Bagaimana merancang dan membuat aplikasi keamanan data berbentuk file dokumen PDF dengan menggunakan metode algoritma RC4?
2. Bagaimana menerapkan metode algoritma RC4 pada proses enkripsi dan dekripsi pada file dokumen PDF?
3. Apakah dengan menggunakan algoritma RC4 ini dapat menjaga keamanan file dokumen PDF dengan baik?

1.4 Batasan Masalah

Untuk mengatasi permasalahan yang ada diatas, maka cakupan masalah akan dibatasi, yaitu sebagai berikut:

1. Aplikasi yang akan dibangun menggunakan metode algoritma RC4 dengan kunci simetris.
2. File yang dienkripsi hanya berbentuk file dokumen PDF.
3. Membatasi pengenkripsian file dokumen PDF 3 file dalam satu kali proses.

1.5 Tujuan Penelitian

Tujuan dari penelitian ini yaitu membuat aplikasi keamanan yang dapat mengamankan data file dokumen PDF dengan menggunakan algoritma RC4.

1.6 Manfaat Penelitian

Adapun manfaat dari penelitian ini, yaitu diharapkan dengan adanya aplikasi keamanan data menggunakan algoritma *RC4* adalah :

1. Memberikan kemudahan pada pengguna aplikasi untuk mengamankan data berbentuk file dokumen PDF.
2. Pengguna dapat mengirimkan file dokumen PDF yang bersifat rahasia dengan aman.