

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Perkembangan teknologi dalam sistem informasi dan jaringan komputer saat ini berkembang dengan sangat pesat. Hal ini menuntut agar setiap perusahaan selalu memahami bahwa kebutuhan terhadap keamanan data sangatlah diperlukan di masa ini atau di masa yang akan datang. Dalam menjalankan tugas dari perusahaan dituntut untuk adanya suatu keamanan jaringan komputer yang dapat mengamankan data dalam tujuan tertentu.

Komunikasi data merupakan pertukaran data antara dua perangkat melalui beberapa bentuk media transmisi seperti kabel kawat. Untuk terjadinya data komunikasi, perangkat harus berkomunikasi menjadi sebuah bagian dari sistem komunikasi, yang terdiri dari kombinasi dari *hardware* (peralatan fisik) dan perangkat lunak (*software*). Efektifitas sistem komunikasi data tergantung pada empat karakteristik yang mendasar antara pengiriman, akurasi, ketepatan waktu maupun kedatangan keterlambatan paket tersebut. Pada PT. Pharos Indonesia itu sendiri mengalami kesulitan dalam mengatasi keamanan data dalam pertukaran data tersebut, karena data-data tersebut bisa dengan mudah dibaca oleh pihak yang tidak bertanggung jawab di perusahaan tersebut. Saat ini diperlukan suatu cara untuk mengamankan data dan informasi. Salah satu cara untuk mengamankan data adalah dengan cara merubah data tersebut ke dalam bentuk data yang lain

yang tidak dapat dimengerti oleh pihak lain, yaitu dengan cara penyandian atau dengan enkripsikan data pada perusahaan tersebut. Dalam kriptografi terdapat beberapa algoritma yang dapat menyandikan data.

Algoritma yang akurat adalah algoritma DES (*Data Encryption Standard*). DES ditetapkan sebagai standard untuk melindungi data dan informasi. Tetapi, DES dianggap sudah tidak aman lagi, karena dengan perangkat keras khususnya kuncinya dapat ditemukan dalam waktu beberapa hari. Kemudian IBM (*International Business Machines*) yang membuat algoritma DES mengembangkan DES menjadi 3DES (*Tripple Data Encryption Standard*). 3DES juga banyak digunakan dan penggunaannya lebih aman dibandingkan DES. Jika dilihat dari permasalahan yang ada diperusahaan, Serta mencoba memberikan suatu usulan yang penulis susun dalam tugas akhir ini.

Penerapan keamanan data merupakan solusi dari masalah yang ada diperusahaan dibutuhkan sebuah sistem yang menunjang kegiatan perusahaan untuk menekan resiko yang besar, dari penyampaian informasi dan tingkat keamanan yang lemah untuk data-data penting perusahaan PT. Pharos Indonesia tersebut. Hal tersebut dilakukan agar dapat menyediakan keamanan data yang tidak mudah dilihat orang tidak bertanggung jawab serta memberikan layanan yang aman kepada pengguna, maka judul yang peneliti ambil adalah “**Analisa Proteksi file Menggunakan Algoritma 3DES (studi kasus PT. Pharos Indonesia)**”

## 1.2 Perumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas, maka dapat dirumuskan masalah dalam penelitian ini adalah bagaimana proses enkripsi dan dekripsi suatu data, serta besaran file dengan menggunakan Algoritma 3DES di PT. Pharos Indonesia akan lebih aman menyangkut kerahasiaan dan keamanan data terjamin.

## 1.3 Pembatasan Masalah

Agar dalam analisis ini tidak menyimpang dari pembahasan, maka penulis membatasi pembahasan atau batasan masalah yaitu,

- a Bentuk yang akan di enkripsi dan dekripsi hanya file text dokumen, bukan file gambar, audio, video dan perbandingannya yang terdapat di PT. Pharos Indonesia.
- b Sistem enkripsi dekripsi menggunakan Algoritma 3DES
- c Aplikasi berjalan hanya pada sistem operasi *Windows*.

## 1.4 Tujuan dan Manfaat Penulisan

### 1.4.1 Tujuan Penulisan

Berdasarkan dari latar belakang dan masalah yang diteliti maka tujuan dari penelitian ini adalah

- a Bagaimana untuk mengetahui proses enkripsi dan dekripsi menggunakan Algoritma 3DES.
- b Penerapan aplikasi sistem proteksi file untuk sebagai keamanan data.

### 1.4.2 Manfaat Penulisan

Manfaat dari penelitian ini adalah:

- a Memberikan jaminan keamanan menyangkut kerahasiaan dan keamanan data.
- b Mengetahui tentang konsep terhadap komunikasi data menggunakan enkripsi dan dekripsi Algoritma 3DES.
- c Bertambahnya wawasan dan pengalaman penulis tentang ilmu keamanan data dengan menggunakan algoritma dan hal lainnya yang berkaitan dengan metodologi penulisan ini.

### 1.5 Sistematika Penulisan

Secara garis besar sistematika penulisan dibagi beberapa bab yang secara ringkas dapat di jabarkan sebagai berikut:

#### **BAB I PENDAHULUAN**

Bab ini berisi pendahuluan yang terdiri dari latar belakang dan perumusan masalah, pembatasan masalah, tujuan dan manfaat penulisan, dan sistematika penulisan

#### **BAB II LANDASAN TEORI**

Dalam bab ini berisikan teori yang berupa pengertian dan definisi yang diambil dari kutipan buku yang berkaitan dengan penyusunan laporan skripsi serta beberapa *literature review* yang berhubungan dengan penelitian.

### **BAB III METODE PENELITIAN**

Dalam bab ini berisikan waktu dan tempat penelitian, metode pengumpulan data, metodologi penelitian, analisa kebutuhan, usulan pemecahan masalah, dan kerangka berfikir.

### **BAB IV ANALISA DAN PERANCANGAN**

Bab ini menguraikan desain perancangan sistem yang akan di buat dari rancangan sistem sampai dengan interfacenya

### **BAB V HASIL DAN IMPLEMENTASI**

Bab ini berisi hasil implimentasi dasar dan spesifikasi khusus yang menyangkut sistem enkripsi dan dekripsi algoritma 3DES yang hasilnya dijadikan bahan referensi dalam mengimplementasikan untuk mengetahui berjalannya optimal sejak dari tahapan uji coba sampai penarikan kesimpulan.

### **BAB VI KESIMPULAN DAN SARAN**

Pada bab ini penulis menguraikan kesimpulan dari hasil uji coba sistem dan saran- saran mengembangkan sistem ke depannya.