

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Perkembangan teknologi informasi yang begitu pesat ini sangatlah membantu kehidupan manusia. Teknologi informasi saat ini semakin canggih, tuntutan akan kemudahan mencari informasi menjadi faktor penggerak pesatnya pertumbuhan teknologi informasi. Selain itu perkembangan teknologi internet juga tumbuh cukup pesat, hal ini mendukung untuk memudahkan masyarakat dalam mengakses informasi yang diinginkan.

Pemanfaatan teknologi informasi telah terbukti memudahkan kegiatan manusia untuk mengakses informasi dalam waktu yang singkat akan tetapi dikarenakan akses yang begitu luas, informasi atau data yang rahasia menjadi sangat riskan dapat diketahui oleh orang yang tidak berhak. Pada layanan komunikasi public sangat rentan terhadap ancaman pihak ketiga untuk menyadap, merusak dan mengubah informasi yang dikirimkan.

Di era globalisasi saat ini keamanan data sangat dibutuhkan pada tiap perusahaan baik perusahaan kecil maupun perusahaan besar.

Berdasarkan analisa di PT. Trisari Tigaputra Utama, data FTP sering hilang/ganda dikarenakan akses multi user. Sehingga membutuhkan pengamanan data menggunakan *Algoritma Data Encryption Standard (DES)*. Dengan menggunakan algoritma DES diharapkan dapat mengamankan data dari FTP karena data telah di enkripsi terlebih dahulu sebelum dikirimkan ke masing-masing user.

Oleh sebab itu tindakan pengamanan data mutlak diperlukan dikarenakan rentan pengambilan data karena pengguna lebih dari satu user dan bebas mengelola data, tindakan yang dilakukan biasanya dengan melakukan proses penyandian data yang biasa disebut enkripsi data. Metode ini mengkodekan suatu informasi sedemikian rupa dengan algoritma kriptografi tertentu sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak berhak mengetahuinya.

Masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem jaringan komunikasi data. Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila mengganggu jalannya sistem, seringkali keamanan dikurangi atau ditiadakan. Dalam teknologi informasi, telah dikembangkan berbagai cara untuk mengatasi keamanan data salah satunya adalah dengan algoritma kriptografi yang menggunakan transformasi data sehingga data yang dihasilkan tidak dapat dimengerti oleh pihak ketiga. Transformasi dapat menjadi solusi dalam mengatasi masalah privasi (*privacy*) dan autentikasi (*authentication*) data.

Untuk menghindari agar hal tersebut tidak terjadi, penulis menggunakan algoritma kriptografi *DES* untuk proses enkripsi dan deskripsi data pada PT. Trisari Tigaputra Utama. Kriptografi telah menjadi suatu bagian yang tidak dapat di pisahkan dari sistem keamanan jaringan, Salah satu metode enkripsi data adalah *Data Encryption Standard (DES)*. *Data Encryption Standard (DES)* merupakan algoritma *cipher* blok yang populer karena dijadikan standar algoritma enkripsi

kunci-simetri. Sebenarnya *DES* adalah nama standar enkripsi simetri, nama algoritma enkripsinya sendiri adalah *DEA (Data Encryption Algorithm)*, namun nama *DES* lebih populer dari pada *DEA*. Dari latar belakang di atas penulis mencoba untuk membuat *rancangan* keamanan data dengan menggunakan algoritma kriptografi *DES*, dengan mengambil judul “**Analisis Transmisi Data Menggunakan Algoritma *Data Encryption Standard (DES)* Pada PT. Trisari Tigaputra Utama**”.

### **1.2 Rumusan Masalah**

Berdasarkan latar belakang masalah yang telah diuraikan di atas, maka dapat dirumuskan masalah dalam penelitian ini adalah bagaimana menganalisis transmisi data menggunakan algoritma *DES (Data Encryption Standard)* pada PT. Trisari Tigaputra Utama?. Karena pada PT. Trisari Tigaputra Utama saat ini memerlukan pengamanan data.

### **1.3 Ruang Lingkup**

Agar dalam analisis ini tidak menyimpang dari pembahasan, maka penulis membatasi ruang lingkup pembahasan mengenai analisa transmisi data yaitu hanya membahas mengenai proses penyandian data yang meliputi proses enkripsi dan deskripsi data menggunakan algoritma kriptografi *DES (Data Encryption Standard)*.

### **1.4 Tujuan Dan Manfaat**

Adapun dalam penyusunan laporan penelitian ini memiliki tujuan dan manfaat sebagai berikut :

#### 1.4.1 Tujuan

Tujuan dari penulisan laporan ini yaitu :

- a. Memberikan gambaran dalam proses enkripsi dan dekripsi pesan atau informasi secara detail.
- b. Menganalisis keamanan data menggunakan algoritma kriptografi *Data Encryption Standard (DES)*

#### 1.4.2 Manfaat

Manfaat dari penulisan laporan ini yaitu :

##### 1. Manfaat Teoritis

- a. Memperkenalkan teknologi keamanan data atau informasi menggunakan metode enkripsi dan dekripsi
- b. Mengembangkan ilmu dan teori yang telah dipelajari di Universitas Satya Negara Indonesia (USNI) pada bidang teknik informatika untuk menambah ilmu pengetahuan.
- c. Melatih diri untuk berfikir kreatif, inovatif dan efektif dalam memecahkan masalah.

##### 2. Manfaat Aplikatif

- a. Bagi PT. Trisari Tigaputra Utama
  - 1) Meningkatkan keamanan terhadap file - file yang dianggap penting.
  - 2) Kerahasiaan suatu data atau informasi terjamin.
  - 3) Menanggulangi penyadapan telepon dan email.
- b. Bagi Peneliti

- 1) Dapat menambah pengetahuan dan wawasan penulis tentang kriptografi khususnya dalam hal proses enkripsi dan deskripsi didalam pengamanan dan kerahasiaan keamanan data menggunakan kriptografi *Data Encryption Standard (DES)*.
  - 2) Sebagai penerapan ilmu pengetahuan yang pernah diperoleh selama melaksanakan pembelajaran di Universitas Satya Negara Indonesia (USNI).
- c. Bagi Universitas Satya Negara Indonesia (USNI)
- 1) Sebagai bahan pertimbangan untuk penilaian bagi mahasiswa yang telah membuat penelitian ini.
  - 2) Penelitian ini diharapkan dapat dijadikan sebagai bahan referensi untuk para peneliti selanjutnya dalam melakukan penelitian baik dalam pengembangan penelitian maupun penelitian baru.

### **1.5 Sistematika Penulisan**

Untuk memahami lebih jelas laporan ini, maka materi-materi yang tertera pada penelitian ini dikelompokkan menjadi beberapa sub bab dengan sistematika penyampaian sebagai berikut :

#### **BAB I PENDAHULUAN**

Berisi tentang latar belakang, perumusan masalah, tujuan dan manfaat penelitian, luaran yang diharapkan, ruang lingkup penelitian, metodologi penelitian dan sistematika penulisan.

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

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

Bab ini berisikan waktu dan tempat penelitian, metode pengumpulan data, kerangka kerja, metode analisa sistem, perancangan sistem dan juga pengembangan sistem.

### BAB IV ANALISA HASIL DAN PEMBAHASAN

Bab ini berisikan analisis dan perancangan berupa analisis permasalahan, analisis data, analisis keamanan data, langkah-langkah penyelesaian, proses enkripsi dan deskripsi.

### BAB V KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan hasil analisa dan dalam rangka menjawab tujuan penelitian yang diajukan, serta saran-saran yang penulis berikan untuk lebih memaksimalkan kinerja system baru.