BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada pada era modernisasi ini, keberadaan Ilmu Pengetahuan dan Teknologi (IPTEK) menjadi tolok ukur yang mampu mengubah sistem manual menjadi terkomputerisasi. Yang artinya mengubah pola sistem komunikasi *analog* menjadi *digital*. Seiring dengan laju perkembangan teknologi informasi dan komunikasi yang beraneka ragam, diperlukan peningkatan mutu dan mekanisme pelayanan di bidang komputerisasi yang tepat guna, sehingga Sumber Daya Manusia (SDM) yang diciptakan dapat berperan aktif dalam membangun dunia informasi berdasarkan kemampuan yang dimilikinya.

Perkembangan teknologi informasi yang sangat pesat ini, turut memajukan media komunikasi sebagai media penyampaian informasi dari satu tempat ke tempat lainnya. Salah satu media komunikasi yang banyak digunakan dalam penyampaian informasi tersebut adalah pengiriman file secara elektronik, yang disebut *electronic mail* atau *e-mail*.

E-mail merupakan layanan pengiriman surat digital yang disediakan oleh *Internet Service Provider* (ISP). ISP menyediakan *server e-mail* atau *mail server* yang berfungsi untuk melakukan pendeteksian pesan dan mengirimkannya pada *e-mail* tujuan. Sehingga memudahkan semua kalangan dalam melakukan pertukaran data dengan sangat cepat. Namun kemudahan dalam pengaksesan media komunikasi melalui *e-mail* oleh semua kalangan, akan memberikan dampak bagi keamanan informasi, file ataupun pesan yang menggunakan media komunikasi tersebut. File atau informasi menjadi sangat rentan untuk digunakan dan dimanipulasi oleh pihak-pihak yang tidak bertanggung jawab.

Kerahasiaan data menjadi suatu hal yang sangat perlu untuk diperhatikan untuk menjaga keamanan data. Data atau informasi yang tidak diproteksi atau terlindungi dengan baik, dengan mudah bisa diambil dan dimanipulasi orang yang

tidak bertanggung jawab. Sehingga dapat merugikan sipemilik dan orang yang membutuhkan informasi tersebut.

Untuk menjaga kerahasiaan dan keamanan file atau data tersebut, diperlukan suatu metode keamanan data yang baik, salah satunya dengan cara mengenkripsi atau biasa disebut dengan pengkodean data dan kemudian dapat dikembalikan atau didekripsikan informasi yang telah dienkripsi ke dalam bentuk semula (*default*). Metode ini biasa disebut dengan Kriptografi.

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Aplikasi pengamanan file ini, dibangun dengan menerapkan algoritma *Rivest Code* 5. Algoritma *Rivest Code* 5 merupakan algoritma enkripsi menggunakan metode simetrik dan pengolahan dalam bentuk blok *cipher*, jadi kata kunci yang sama digunakan untuk proses enkripsi dan dekripsi. *Rivest Code* 5 merupakan algoritma *cipher block* yang mempunyai ukuran blok yang variabel (32 bit, 64 bit atau 128 bit), panjang kuncinya yang variabel antara 0 samapai 2040 bit dan jumlah putaran yang variabel antara 0 sampai 255.

Untuk lebih mengamankan proses enkripsi dan dekripsi, diperlukan suatu protokol pertukaran kunci (*key exchange*). Protokol ini dibutuhkan karena algoritma simetris mempunyai kelemahan yaitu memakai kunci yang sama dalam melakukan enkripsi dan dekripsi sehingga jika kunci tersebut dipertukarkan pada saluran yang tidak aman, akan membuat pihak lain yang berhasil menyadap kunci tersebut akan dapat mendekripsi data yang dipertukarkan. Salah satu algoritma pertukaran ini adalah Algoritma *Diffie-Hellman*. Tujuan dari algoritma ini adalah untuk memungkinkan dua pengguna saling bertukar kunci secara aman, kemudian dapat digunakan untuk enkripsi dan dekripsi pesan berikutnya.

Berdasarkan uraian di atas tersebut, maka penulis membuat proposal skripsi ini dengan judul **"Implementasi Protokol *Diffie–Hellman* dan Algoritma Kriptografi *Rivest Code* 5 (RC5) untuk Enkripsi dan Dekripsi dalam Pengamanan File Pada *Electronic Mail*".**

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan di atas, maka dapat dirumuskan permasalahan sebagai berikut:

1. Bagaimana menerapkan Aplikasi Implementasi Algoritma *Rivest Code* 5 melalui protokol *Diffie-Hellman* untuk mengamankan file?
2. Bagaimana proses pembentukan dan pertukaran kunci protokol *Diffie-Hellman* dan Algoritma *Rivest Code* 5 untuk mengenkripsi dan mendekripsikan file?

1.3 Batasan Masalah

Adapun batasan masalah pada sistem yang akan dibangun adalah sebagai berikut:

1. Protokol pembentukan atau pertukaran kunci (*key exchange protocol*) yang digunakan adalah protokol *Diffie-Hellman* dan Algoritma *Rivest Code* 5 sebagai enkripsi dan dekripsi.
2. Data yang diproses meliputi file-file yang berekstensi : *xls*, *doc* dan *pdf* .
3. *Account e-mail* sebanyak dua user, yaitu satu *account* pengirim dan satu *account* penerima file.
4. *Account e-mail* digunakan hanya untuk mengirim dan menerima file enkripsi (*Ciphertext*).
5. Enkripsi dilakukan pada sisi pengirim dan dekripsi file dilakukan pada sisi penerima.
6. Jaringan yang digunakan adalah *Wireless Fidelity* atau biasa disebut jaringan Internet.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini sebagai berikut :

1. Membuat aplikasi kriptografi untuk enkripsi dan dekripsi melalui protokol *Diffie-Hellman* dan algoritma *Rivest Code* 5 untuk menjaga kerahasiaan data pada file.
2. Mengimplementasikan Protokol *Diffie-Hellman* dan Algoritma *Rivest Code* 5 untuk menjaga keamanan data agar tidak dapat diketahui dan dibaca oleh orang lain, kecuali yang berhak.

1.5 Manfaat Penelitian

Adapun manfaat dalam aplikasi yang akan dibangun adalah sebagai berikut:

1. Didapatkan hasil berupa pengamanan data file dengan baik karena kunci hanya diketahui oleh pengirim dan penerima file.
2. Dihasilkannya sebuah perangkat lunak yang mampu mengamankan file menggunakan Protokol *Diffie-Hellman* dan Algoritma *Rivest Code* 5, sehingga pengirim dan penerima file tidak merasa khawatir isi file dimanipulasi dan disalahgunakan oleh pihak yang tidak bertanggung jawab.

1.6 Relevansi

Penulis berharap penelitian ini dapat memberi manfaat dan kontribusi dalam Ilmu Pengetahuan dan Teknologi, khususnya bidang Komunikasi dan Informatika, sehingga dapat direalisasikan oleh pengguna/*user* untuk menjaga kerahasiaan data dan informasi yang dilakukan dalam pertukaran data melalui media surat elektronik atau *electronic mail* (*e-mail*).