BAB I

PENDAHULUAN

1.1 Latar Belakang

E-mail atau surat elektronik adalah sarana kirim mengirim surat melalui jalur jaringan komputer (misalnya internet). *E-mail* merupakan salah satu fasilitas atau aplikasi internet yang paling banyak digunakan dalam hal surat-menyurat. Hal ini dikarenakan e-mail merupakan alat komunikasi yang murah, cepat, dan efisien. Menggunakan e-mail memungkinkan kita untuk mengirimkan pesan dalam bentuk surat ke seluruh dunia dalam waktu yang sangat cepat dan biaya yang murah. *E-mail* yang dikirimkan akan sampai ke alamat yang dituju sesaat *e-mail* tersebut dikirimkan.

Untuk mengirim *e-mail* kita memerlukan suatu program *mail-client*. *E-mail* yang kita kirim akan melalui beberapa poin sebelum sampai di tujuan. Mulai dari e-mail dikirim → Internet → POP3 server penyedia *e-mail* penerima → *e-mail client* (di komputer penerima) → *e-mail* dibaca si penerima. Terlihat *e-mail* yang terkirim hanya melalui 5 poin (selain komputer pengirim dan penerima). Sebenarnya lebih dari itu sebab setelah *e-mail* meninggalkan POP3 Server maka akan melalui banyak server-server lainnya. Tidak tertutup kemungkinan pesan *e-mail* dan *attachment* yang dikirim dapat disadap orang lain. Oleh karena itu dikembangkan cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi.

Dalam kriptografi terdapat dua konsep yaitu enkripsi dan dekripsi. Enkripsi adalah mengubah pesan asli (*plaintext*) menjadi pesan tersandi (*chipertext*). Proses enkripsi akan menghasilkan pesan yang tersandi yang hanya bisa dibuka oleh pihak yang memiliki kunci(*key*). Dekripsi adalah mengembalikan pesan tersandi(*chipertext*) menjadi pesan asli. Enkripsi dan dekripsi dilakukan dengan menggunakan algoritma kunci simetri. Berdasarkan besar data yang diolah dalam satu kali proses, maka algoritma

kriptografi dapat dibedakan menjadi dua yaitu algoritma *block cipher* dan algoritma *stream cipher*.

Pada kriptografi modern mengunakan penerapan fungsi XOR. Fungsi XOR berasal dari kata *Exclusive OR.* Fungsi ini berjalan pada mode bit, keluaran fungsi ini bernilai 1 jika nilai masukannya mempunyai keadaan yang berbeda. Fungsi *XOR* bertujuan untuk menghasilkan nilai logika benar (*true)* , dan salah (*false)* jika kedua masukan bernilai salah atau kedua masukan bernilai benar.

Berdasarkan uraian yang dijabarkan diatas, penulis mencoba untuk membuat sebuah kriptografi yang memanfaatkan fungsi XOR dan algoritma *block cipher* untuk mengamankan pesan *e-mail.* Sehingga pesan yang terkirim pada *e-mail* adalah pesan yang tersandi (enkripsi).

Dengan pesan yang tersandi maka keamanan pengguna *e-mail* dalam bertukar data menjadi lebih aman, dan menjaga keaslian data yang di kirim oleh pengguna

1.2 Rumusan masalah

Berdasarkan latar belakang diatas, maka permasalahan yang akan dibahas dalam tugas akhir ini yaitu :

1. Bagaimana tingkat *Confidentiality* (Kerahasiaan) penggunaan algoritma *block cipher* dan fungsi XOR pada pengiriman pesan dan *attachment e-mail* ?
2. Bagaimana tingkat data *integrity* (keutuhan data) penggunaan algoritma *block cipher* dan fungsi XOR pada pengiriman pesan dan *attachment e-mail* ?

1.3 Batasan masalah

Penulis akan membatasi permasalahan sebagai berikut :

1. Informasi yang digunakan berupa teks.

2. Pengimplementasian enkripsi dan dekripsi pada aplikasi yang dibangun.
3. File *attachment* (lampiran) yang digunakan berformat doc,docx, dan txt.

1.4 Tujuan

1. Menjaga kerahasiaan data (*Confidentiality)* yang dikirim pada pesan dan *attachment e-mail.*
2. Menjaga keutuhan data (data *integrity)* yang dikirim pada pesan dan *attachment e-mail.*

1.5 Manfaat

Memberikan keamanan bagi user dalam penggunaan *e*-mail karena pesan dan dokumen yang dikirim melalui *e-mail* akan tersandi sehingga keaslian pesan dan dokumen lebih terjaga.