BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Dengan perkembangan teknologi informasi komunikasi sudah berkembang sangat pesat. Hampir di setiap bidang kehidupan telah menggunakan teknologi ini sebagai saran pendukung maupun sarana utama. Sehubungan dengan hal tersebut, aspek keamanan dalam teknologi informasi dan komunikasi tentunya tidak bisa diabaikan. Dalam kegiatan kirim-terima pesan, aspek keamanan yang perlu diperhatikan antara lain kerahasiaan, integritas data, dan otentikasi. Dalam aspek keamanan hal diatas dapat memanfaatkan kriptografi.

Berdasarkan penggunaan kuncinya, algoritma kriptografi bisa dibagi menjadi dua, yakni kriptografi kunci-simetri dan kriptografi kunci-asimetri. Kriptografi kunci-simetri menggunakan kunci yang sama (*private key*) untuk melakukan enkripsi dan dekripsi. Sedangkan kriptografi kunci-asimetrik menggunakan kunci yang berbeda untuk melakukan enkripsi dan dekripsi. Pada kriptografi kunci-asimetri, enkripsi dilakukan dengan kunci publik, sedangkan dekripsi dilakukan dengan kunci privat. karena itu, kriptografi kunci-asimetrik disebut juga kriptografi kunci-publik.

Untuk itu perlu keamanan yang tepat untuk memberikan keamanan sehingga dengan solusi ini *e-mail* dapat diandalkan dalam pertukaran informasi saat ini. Karena fitur keamanan informasi dan data standar browser seperti secure email belum cukup untuk melindungi keamanan informasi dari pihak yang tidak mempunyai kepentingan. Karena masih bisa diretas dengan memanfaatkan software *keylogger*. Maka dari itu penggunaan perangkat lunak yang memanfaatkan kriptografi, kunci-simetri maupun kunci-asimetri, sangatlah memudahkan pengguna untuk menjaga keamanan komunikasi ataupun data.dengan memanfaatkan perangkat lunak GNUPG, pengguna bisa melakukan enkripsi, tanda tangan digital, ataupun otentifikasi data. Salah satu perangkat lunak yang memanfaatkan kriptografi adalah GNU *Privacy Guard* (biasa disingkat menjadi GNUPG atau GPG).

GNUPG kebanyakan digunakan di lingkungan sistem operasi yang open source seperti Linux dan FreeBSD, kode program GNUPG juga bisa digunakan di lingkungan Windows. Adapun GNUPG versi Windows, dinamakan Gpg4win. Gpg4win ini merupakan bundel program yang dikemas untuk Windows yang mencakup GNUPG, pengelola kunci (*WinPT dan GPA*), plugin untuk enkripsi email (*Kleopatra*), plugin untuk tambahan (*Enigmail*), dan program email client (*Claws Mail*).

Dengan menggunakan GNUPG versi Windows, atau Gpg4win dan latar belakang tersebut diatas, di buatlah makalah komprehensif yang diberi judul:

"**SISTEM KEAMANAN EMAIL DENGAN GNUPG DI THUNDERBIRD**"

1.2 Identifikasi Masalah

Berdasarkan latar belakang masalah serta ruang lingkup permasalahan yang timbul berkenaan dengan sistem keamanan email , maka masalah dapat diidentifikasikan, sebagai berikut :

1. Keamanan dalam pengiriman informasi belum cukup untuk melindungi keamanan informasi
2. Fitur pengamanan standar broswer belum cukup untuk melindungi kerahasiaan informasi atau data karena masih bisa di retas

1.3 Batasan Masalah

Ruang masalah yang dibuat dalam pembahasan Komprehensif hanya seputar kegiatan yang berhubungan dengan :

1. Penggunaan GNUPG sebagai perangkat lunak pengamanan pengiriman informasi dan data dalam email
2. Sistem menggunakan enkripsi agar informasi atau pesan tidak dapat dibaca sembarang orang kecuali penerima asli dengan public key atau private key

1.4 Perumusan Masalah

Berdasarkan identifikasi masalah serta ruang lingkup permasalahan seperti tersebut diatas, maka dapat dirumuskan masalahnya, sebagai berikut: " Bagaimana untuk menjaga agar pesan (informasi) yang berhubungan dengan kerahasiaan, keaslian, pengakuan, dan kontrol integritas tetap aman dalam pengiriman dan penerimaan E-Mail melalui Internet?"

1.5 Tujuan Penulisan

Tujuan dari penulisan Komprehensif ini, adalah :

1. Menjaga keamanan informasi dari pihak yang tidak berkepentingan.
2. Mengertahui pentingnya kerahasiaan dan keamanan pertukaran informasi melalui E-mail

1.6 Manfaat Penulisan

Manfaat dari penulisan komprehensif ini, adalah:

1. Solusi dalam menjaga keamanan dan kerahasian dalam pengiriman informasi atau data dengan email
2. Acuan bagi mahasiswa di lingkungan Universitas Negeri Jakarta, untuk menambah wawasan berpikir serta bahan acuan untuk penulisan-penulisan ilmiah lainnya kearah yang lebih baik
3. Menerapkan kemampuan penulis dalam melakukan pembuatan sistem keamanan email selama mengenyam pendidikan di Universitas Negeri Jakarta.