BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi yang semakin berkembang dan semakin canggih merupakan kemajuan yang paling pesat didunia ini. Salah satu contoh dalam hal kemajuan teknologi adalah komunikasi yang bisa dibilang luar biasa perkembanganya dan menjadi salah satu kebutuhan yang penting untuk sekarang. Terutama dalam hal pengiriman pesan penting. Keamanan sistem komunikasi menjadi syarat yang harus dipenuhi oleh semua pihak yang terlibat di dalam sistem tersebut. Pertukaran pesan atau informasi membutuhkan tingkat keamanan yang tinggi, karena pengamanan pesan atau informasi berfungsi melindungi pesan atau informasi agar tidak dapat dibaca oleh kriptanalisis, serta mencegah kriptanalisis memodifikasi pesan atau informasi. Di dunia internet banyak perbuatan yang negatif seperti pencurian informasi maraknya kriminalitas seperti itu bisa menjadi opsi untuk menentukan keamanan untuk salah satu media informasi atau media komunikasi. Informasi yang terandung didalamnya pun bisa saja berubah sehingga menyebabkan salah penafsiran oleh penerima. Hal yang penting dalam komunikasi menggunakan komputer adalah untuk menjamin kerahasian data/informasi, salah satunya dengan menggunakan enkripsi.

Kriptografi sebelum pada termodernisasi merupakan sinonim dari "enkripsi", konversi dari kalimat-kalimat yang dapat dibaca menjadi kelihatan tidak masuk akal. Pembuat dari pesan enkripsi membagi teknik pemecahan sandi yang dibutuhkan untuk mengembalikan informasi asli jika hanya dengan penerima yang diinginkan, sehingga dapat mencegah orang yang tidak diinginkan melakukan hal yang sama. Kriptografi modern sangat didasari pada teori matematis dan aplikasi komputer algoritma kriptografi didesain pada asumsi ketahanan komputasional, membuat algoritma ini sangat sulit dipecahkan oleh musuh atau pencuri. Membangun sebuah keamanan komputer diperlukan suatu sistem pengamanan data yang mengamankan data tersebut. Berdasarkan paparan ini penulis mencoba untuk membuat rancangan pengiriman pesan

menggunakan algoritma *Affine Cipher*, dengan mengambil judul "Perancangan perangkat lunak untuk keamanan pengiriman pesan menggunakan *Affine Cipher*".

1.2 Perumusan Masalah

Rumusan masalah yang dapat didefinisikan dalam penelitian ini diantaranya adalah sebagai berikut :

1. Bagaimana mengamankan data pesan menggunakan proses dekripsi dan proses enkripsi dengan menggunakan algoritma kriptografi *Affine Cipher* ?.
2. Bagaimana hasil penerapan algoritma kriptografi *Affine Cipher* pada aplikasi pengiriman pesan?.

1.3 Tujuan Penelitian

Tujuan dari penelitian dengan algoritma kriptografi *Affine Cipher* dalam keamanan jaringan adalah :

1. Melindungi data pesan yang dianggap penting menggunakan algoritma kriptografi *Affine Cipher.*
2. Memperoleh informasi hasil enkripsi berupa *ciphertext* yang tidak terbaca karena bukan *plaintext* dan *ciphertext* yang dihasilkan berhasil masuk ke *database* sebagai pengganti pesan *plaintext* yang dikirim.

1.4 Manfaat Penelitian

Manfaat dari penelitian dengan algoritma kriptografi *Affine Cipher* dalam keamanan jaringan adalah :

1. Mengamankan pesan yang dikirim melalui pengiriman pesan dengan menggunakan metode *Affine Cipher.*
2. Menghasilkan perangkat lunak untuk berkirim pesan teks berbasis *web* atau pengiriman pesan dengan menggunakan metode *Affine Cipher.*

1.5 Batasan Masalah

Batasan Masalah dari penelitian dengan algoritma kriptografi *Affine Cipher* dalam keamanan jaringan adalah Penelitian ini difokuskan untuk pengiriman pesan dengan penggunaan huruf.Tanda baca yang bisa masuk kedalam sistem ini adalah (titik, koma,

space, tanda seru, tanda pagar, tanda persen, bintang, tanda kurung, sama dengan, tambah, kurang, tanda tanya, koma, garis miring, tanda petik, tanda titik koma).