BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Teknologi dan informasi dari masa ke masa terus mengalami perkembangan yang sangat berpengaruh pada hampir semua aspek kehidupan manusia, salah satunya dalam hal berkomunikasi. Bagi manusia komunikasi adalah salah satu cara untuk mendapatkan informasi. Salah satu cara berkomunikasi yaitu dengan mengirim pesan berupa tulisan. Namun dengan berkembangnya teknologi seringkali pesan disadap oleh pihak-pihak yang tidak berhak mengetahui informasi tersebut. Oleh karena itu, masalah keamanan menjadi aspek terpenting dalam sebuah sistem informasi. Salah satu cara agar pesan tidak dapat disadap oleh pihak lain maka diperlukannya suatu seni atau ilmu untuk menjaga keamanan pesan di mana hanya pengirim dan penerima pesan yang mengetahui isi pesan tersebut, ilmu ini dikenal dengan Kriptografi.

Menurut Menezez dkk. (dalam Arifin & Oktaviana, 2013) definisi kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta keasliannya.

Dalam kriptografi terdapat tiga fungsi dasar, yaitu enkripsi, dekripsi dan kunci. Enkripsi yaitu mengubah pesan asli atau *plaintext* ke dalam bentuk pesan yang tidak dimengerti yaitu *ciphertext.* Dekripsi merupakan kebalikan dari enkripsi, yaitu mengembalikan *ciphertext* ke bentuk *plaintext.* Kunci yang dimaksud di sini adalah kunci yang dipakai untuk mengenkripsi dan mendekripsi. Kunci terbagi menjadi dua bagian, yaitu kunci rahasia (*private key*) dan kunci publik (*public key*).

Berdasarkan kuncinya, algoritma kriptografi dibagi menjadi Algoritma Simetri dan Algoritma Asimetri. Ariyus (2008:44) mendefinisikan bahwa "Algoritma simetri sering disebut dengan algoritma klasik karena memakai kunci yang sama untuk kegiatan enkripsi dan dekripsi". Artinya pada algoritma simetri hanya memiliki satu kunci. "Algoritma asimetri sering juga disebut dengan algoritma kunci publik, dengan

arti kata kunci yang digunakan untuk melakukan enkripsi dan dekripsi berbeda" (Ariyus, 2008:45). Pada algoritma asimetri terdapat dua kunci, yaitu kunci publik (*public key*) untuk enkripsi dan kunci rahasia (*private key*) untuk dekripsi.

Bentuk algoritma yang akan digunakan disini adalah algoritma klasik, yaitu Vigenere *Cipher* dan algoritma asimetri, yaitu algoritma *Knapsack* Merkle-Hellman. Dalam memecahkan masalah keamanan kedua algoritma tersebut tidak lepas dari konsep-konsep matematika seperti aritmatika modulo, relatif prima dan balikan modulo.

Kedua algoritma ini dinilai sudah tidak aman lagi karena pada abad ke-19 Vigenere *Cipher* telah dipecahkan dengan menggunakan algoritma Kasiski, begitu juga dengan algoritma *Knapsack* Merkle-Hellman yang berhasil dipecahkan pada permulaan 1980. Untuk itu dalam penelitian ini akan mengkomposisikan dua algoritma ini agar proses enkripsi dan dekripsi lebih sulit dipecahkan. Kemudian hasil komposisi kedua algoritma tersebut akan dibuat program aplikasi menggunakan perangkat lunak Matlab. Berdasarkan hal tersebut, judul untuk penelitian ini adalah "Kriptografi dengan Mengkomposisikan Vigenere *Cipher* dan Algoritma *Knapsack* Merkle-Hellman".

1.2 Rumusan Masalah Penelitian

Berdasarkan uraian latar belakang di atas, maka rumusan masalah dari penelitiaan ini adalah:

1. Bagaimana mengkontruksi kriptografi yang dikembangkan dari kriptografi Vigenere *Cipher* dan algoritma *Knapsack* Merkle-Hellman?
2. Bagaimana implementasi Vigenere *Cipher* dan algoritma *Knapsack* Merkle-Hellman dalam sebuah program aplikasi?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang diuraikan, maka tujuan dari penelitian ini adalah:

1. Mengkontruksi kriptografi yang dikembangkan dari kriptografi Vigenere *Cipher* dan algoritma *Knapsack* Merkle-Hellman.

2. Mengetahui proses penyandian serta implementasi Vigenere *Cipher* dan algoritma *Knapsack* Merkle-Hellman dalam sebuah program komputer .

1.4 Manfaat Penelitian

Manfaat penulisan penelitian ini adalah mengkontruksi keamanan pesan dengan menerapkan komposisi dua algoritma kriptografi sehingga dalam pengiriman pesan lebih aman.

1.5 Struktur Organisasi Skripsi

BAB I PENDAHULUAN

Meliputi latar belakang penelitian, rumusan masalah penelitian, batasan masalah, tujuan penelitian, manfaat penelitian dan struktur organisasi skripsi.

BAB II LANDASAN TEORI

Membahas teori-teori dasar dan konsep yang berhubungan dan mendukung penulisan penelitian ini.

BAB III METODOLOGI PENELITIAN

Membahas mengenai prosedur-prosedur yang dilakukan saat penelitian.

BAB IV PEMBAHASAN

Membahas hasil dari penelitian yang telah dilakukan.

BAB V PENUTUPAN

Menjelaskan kesimpulan dan saran yang diperoleh dalam penelitian.