BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Kita ketahui bahwa zaman abad 21 sudah menjadi era digital. Hal tersebut dapat dilihat dengan banyaknya orang yang menggunakan internet dari penggunaan *e-mail*, media sosial, jual beli *online*, dan masih banyak lagi. Orang-orang berkomunikasi atau bertukar informasi menggunakan jaringan internet. Karena sifat jaringan komputer yang menggunakan konsep sistem terbuka, maka orang lain dapat dengan mudah masuk ke jaringan tersebut, sehingga pengiriman pesan menjadi tidak aman dan dapat dimanfaatkan oleh orang lain untuk mengambil atau mengubah informasi pesan tersebut di tengah jalan.

Keamanan merupakan aspek penting dalam pengiriman pesan melalui jaringan, terlebih lagi untuk pesan – pesan yang bersifat rahasia atau penting. Misalnya untuk mengirimkan soal Ujian Nasional (UN) dari pusat ke daerah akan lebih cepat dan efisien jika menggunakan *e-mail*. Supaya pesannya tidak mengalami kebocoran maka diperlukan suatu kode agar pesan tersebut masih bersifat rahasia.

Ilmu yang membuat kode atau sandi yaitu Kriptografi. Kriptografi berasal dari bahasa Yunani: *cryptos* dan *graphein*. *Cryptos* artinya rahasia, sedangkan *graphein* artinya tulisan. Jadi, kriptografi berarti tulisan rahasia. Sedangkan definisi kriptografi adalah suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, integritas suatu data, serta otentifikasi data (Menezes,1996 : 4). Menurut (Kromodimoeljo,2009 : 5) kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi data yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Proses enkripsi

dilakukan menggunakan suatu algoritma dengan beberapa parameter. Secara garis besar, proses enkripsi adalah proses pengacakan pesan yang dapat dibaca "naskah asli" (*plaintext*) menjadi pesan yang sulit dibaca "naskah acak" (*ciphertext*). Tentunya naskah acak harus dapat didekripsi oleh seseorang yang mempunyai kunci dekripsi untuk mendapatkan kembali pesan asli. Orang yang tidak memiliki kunci dekripsi akan sulit mendapatkan kembali pesan asli yang telah diubah menjadi naskah acak.

Dalam kriptografi klasik, teknik enkripsi yang digunakan adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi. Untuk *public key cryptography*, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif dibandingkan enkripsi simetris, karena enkripsi asimetris menggunakan bilangan-bilangan yang sangat besar.

Pada skripsi ini akan digunakan kriptografi *caesar cipher* dan *affine cipher* yang merupakan kriptografi sandi simetris. *Caesar cipher* dan *affine cipher* adalah kriptografi sederhana. Dengan pengenkripsian satu kali pada pesan asli tidak cukup untuk membuat pesan itu menjadi aman sehingga pesan tersebut akan mudah dipecahkan oleh orang ketiga. Salah satu cara agar pesan menjadi sulit dipecahkan yaitu dengan cara mengkomposisikan kedua *cipher*. Dengan dua kali enkripsi sederhana dari *caesar cipher* dan *affine* cipher akan meningkatkan keamanan (membuat enkripsi menjadi kuat / sulit dipecahkan). Karena menggunakan dua *cipher* maka ada dua cara mengenkripsiannya, yaitu diawali dengan *caesar cipher* terlebih dahulu kemudian diikuti dengan *affine cipher* atau sebaliknya yaitu mengenkripsi pesan dengan *affine cipher* terlebih dahulu kemudan dilanjut dengan enkripsi *caesar cipher*. Peneliti sebelumnya sudah melakukan kombinasi caesar dan *affine cipher*. Mereka memperoleh bahwa kombinasi *caesar cipher* dan *affine cipher* dapat membantu meningkatkan keamanan data.

Berkaitan dengan kriptografi *caesar cipher* dan *affine cipher* tersebut, penulis tertarik untuk membuat program aplikasi dari komposisi kriptografi klasik dengan memperhatikan konsep matematika yang berhubungan dengan kriptografi tersebut. Berdasarkan hal tersebut, judul skripsi ini adalah "Kriptografi dengan Komposisi *Caesar Cipher* dan *Affine Cipher* untuk Mengubah Pesan Rahasia".

1.2 Rumusan Masalah

Atas dasar latar belakang pada bagian sebelumnya, maka diambillah perumusan masalah sebagai berikut :

1. Bagaimana cara mengenkripsi dan mendekripsi pesan dengan kriptografi komposisi *caesar cipher* dan *affine cipher*?
2. Konsep matematika apa saja yang terdapat pada kriptografi komposisi *caesar cipher* dan *affine cipher*?
3. Bagaimana cara membuat program kriptografi komposisi *caesar cipher* dan *affine cipher*?

1.3 Batasan Masalah

Untuk mempermudah penyusunan program kriptografi komposisi *caesar cipher* dan *affine cipher* akan digunakan *software* pemrograman Delphi 7 dan penyandian teks menggunakan 95 karakter (ASCII).

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah tersebut, tujuan dari penelitian ini adalah sebagai berikut :

1. Mengetahui cara mengenkripsi dan mendekripsi kriptografi komposisi *caesar cipher* dan *affine cipher*.
2. Mengetahui konsep matematika apa saja yang dipakai pada kriptografi komposisi *caesar cipher* dan *affine cipher*.
3. Mengetahui cara membuat aplikasi program kriptografi komposisi *caesar cipher* dan *affine cipher* menggunakan Delphi 7.

1.5 Manfaat Peneltian

Adapun manfaat dari penelitian ini yaitu :

1. Bagi penulis

   Mengetahui cara penggunaan komposisi, *caesar cipher* dan *affine cipher* dengan memanfaatkan teori yang telah didapat selama menuntut ilmu di FPMIPA UPI serta mengembangkan diri dalam membuat aplikasi komputer.

2. Bagi Jurusan Pendidikan Matematika

   Menambah khasanah pengetahuan matematika pada topik kajian kriptografi *caesar cipher* dan *affine cipher*.

1.6 Metodologi Penelitian

Untuk menyelesaikan skripsi ini, dibutuhkan langkah-langkah penyelesaian sebagai berikut:

1. Studi Literatur

   Pembelajaran dan pendalaman materi dengan pencarian buku referensi ataupun internet yang berhubungan dengan penyusunan skripsi ini.

2. Perancangan Program Aplikasi Kriptografi

   Perancangan dan perencanaan yang mendukung, mulai dari algoritma sampai antar muka yang dibutuhkan untuk membuat program aplikasi ini.

3. Pembuatan Program Aplikasi Kriptografi

   Pembuatan program dengan algoritma yang telah dirancang dan dikembangan ke dalam bahasa pemrograman dengan menggunakan bahasa pemrograman Delphi 7

4. Pengujian Program Aplikasi Kriptografi

   Setelah program aplikasi selesai dibuat apakah program ini sesuai dengan apa yang diinginkan dengan cara menguji dan menganalisis progam. Selanjutnya dirangkum dalam kesimpulan dan saran.

1.7 Sistematika Penulisan

Penelitian ini disusun dalam sebuah skripsi yang terangkum dalam empat bab, yaitu sebagai berikut :

BAB I PENDAHULUAN, meliputi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan skripsi ini.

BAB II LANDASAN TEORI, membahas teori-teori untuk menunjang penyelesaian masalah dalam penulisan skripsi ini.

BAB III KOMPOSISI *CAESAR CIPHER* DAN *AFFINE CIPHER*, menjelaskan tentang *caesar cipher* dan *affine cipher* dan komposisi keduanya serta diskusi dan pembahasan matematika.

BAB IV PROGRAM APLIKASI KRIPTOGRAFI KOMPOSISI *CAESAR CIPHER* DAN *AFFINE CIPHER*, menjelaskan perancangan, implementasi dan pengujian program aplikasi kriptografi.

BAB V PENUTUP, menjelaskan kesimpulan dan saran yang diperoleh dalam pembuatan program aplikasi kriptografi.