BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Teknologi merupakan sesuatu yang tidak bisa kita pungkiri pengaruhnya terhadap perubahan zaman. Sudah banyak kegiatan kita sehari-hari yang membutuhkan bantuan teknologi. Salah satu teknologi yang dibutuhkan dewasa ini adalah internet, karena penggunaanya yang praktis dan luas dapat digunakan di mana saja dan kapan saja, tentu dengan bantuan teknologi elektronik yang memadai. Internet menjadi sebuah kebutuhan sekarang ini, banyaknya penggunaan internet seperti media sosial, media komunikasi, media pemasaran dan masih banyak lagi menunjukkan bahwa internet merupakan teknologi yang perkembangannya sangatlah pesat. Internet yang bisa digunakan dalam bertukar informasi dengan mudah dan cepat keamanan menjadi aspek yang penting dalam menjaga informasi yang dikirim atau diterima. Jaringan komputer menggunakan konsep sistem terbuka, maka orang lain dapat masuk ke jaringan tersebut, sehingga pengiriman informasi menjadi tidak aman dan dapat dimanfaatkan oleh orang lain untuk mengubah atau mengambil informasi tersebut di tengah jalan. Agar tidak terjadi kebocoran maka diperlukan sandi agar informasi tersebut bersifat rahasia.

Ilmu yang mempelajari 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 di mana 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 "teks asli" (*plaintext*) menjadi pesan yang sulit dibaca "teks sandi" (*ciphertext*). Tentunya *ciphertext* harus dapat didekripsi oleh seseorang yang mempunyai kunci dekripsi untuk mendapatkan kembali *plaintext*. Orang yang tidak memiliki kunci dekripsi akan sulit mendapatkan kembali *plaintext* yang telah diubah menjadi *ciphertext*.

Pada saat perang dunia II pemerintah Jerman Nazi menggunakan mesin Enigma untuk mengubah pesan yang akan dikirim kepada pasukannya menjadi sandi sebagai salah satu strategi mereka agar tidak dapat diketahui oleh lawan. Mesin Enigma merupakan mesin yang merubah pesan menjadi sandi menggunakan metode kriptografi klasik yang digunakkan untuk menyembunyikan pesan koordinasi atau target yang akan mereka serang. Sulitnya pemecahan sandi yang digunakkan pemerintah Jerman Nazi menjadikan mereka tidak mudah untuk dikalahkan. Sampai akhirnya Britania dan Perancis berhasil membuat mesin pemecah Enigma dan dapat meruntuhkan pemerintahan Jerman Nazi. Bagaimana jika pada saat itu pemerintah Jerman Nazi menggunakan mesin enigma untuk menyandikan pesan yang sudah disandikan? Mungkin perang dunia II akan berlangsung lebih lama.

Menurut Sadikin (2012) algoritma kriptografi dapat diklasifikasikan menjadi menjadi dua jenis berdasarkan perkembangannya, yaitu algoritma kriptografi klasik dan algoritma kriptografi modern. Algoritma kriptografi klasik umumnya merupakan teknik penyandian dengan kunci simetrik, sedangkan algoritma kriptografi modern menggunakan kunci asimetris di mana kunci dekripsi berbeda 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. Metode yang digunakan dalam algoritma kriptografi klasik merupakan metode subtitusi (perpindahan / pergantian huruf) atau metode transposisi (pertukaran posisi huruf). *One time*

pad cipher merupakan salah satu jenis algoritma klasik yang menggunakan metode subtitusi. *One time pad cipher* merupakan salah satu algoritma kriptografi klasik yang kerahasiaannya mencapai sempurna karena menggunakan kunci yang tidak membentuk barisan yang berulang dan panjang kunci sama dengan panjang teks yang akan dirahasiakan. Dikarenakan menggunakan teknik tersebut *one time pad cipher* menjadi tidak efisien, karena membutuhkan waktu yang lama untuk menentukan kunci yang sama panjang dengan panjang teks yang akan dirahasiakan. *Affine cipher* juga merupakan salah satu algoritma kriptografi klasik yang menggunakan metode subtitusi. $aP + b$ adalah formula dari *affine cipher* yang merupakan dasar dari semua algoritma kriptografi klasik yang menggunakan metode subtitusi di mana a dan b sebagai kunci dan P adalah *plaintext*, misalnya *one time pad cipher* menggunakan formula *affine cipher* dengan nilai a dan b yang berbeda disetiap hurufnya.

Algoritma kriptografi klasik yang hanya memiliki satu kunci untuk memecah dekripsi dan enkripsi memiliki tingkat keamanan yang lebih lemah dibandingkan dengan algoritma kriptografi modern yang memiliki kunci berbeda untuk mengenkripsi dan mendekripsi. Sehingga algoritma kriptografi klasik mudah dipecahkan oleh pihak ketiga yang ingin mengetahui informasi yang dikirimkan. Namun demikian bukan berarti algoritma kriptografi klasik kurang bagus untuk digunakan dalam sistem keamanan, banyak cara agar algoritma kriptografi klasik dapat menjadi lebih aman. Salah satu cara agar algoritma kriptografi klasik menjadi lebih aman adalah dengan mengkomposisikan dua jenis algoritma kriptografi klasik, sehingga pengekripsian menjadi lebih rumit untuk didekripsi. Dengan mengkomposisikan dua algoritma kriptografi klasik artinya dua kali mengenkripsi pesan atau informasi, $f(g(x))$ atau $g(f(x))$. Misalnya pertama mengenkripsikan pesan dengan *affine cipher* sehingga menghasilkan *cipher text*, lalu *cipher text* kembali dienkripsi dengan *one time pad cipher* atau sebaliknya sehingga pesan akan semakin sulit untuk dipecahkan bagi orang yang tidak memiliki kunci untuk mendekripsinya.

Pada skripsi ini penulis tertarik untuk melakukan percobaan mengubah agar kunci dari *one time pad cipher* menjadi lebih sederhana dan mengkomposisikan dua jenis kriptografi kunci simetri yaitu *one time pad cipher* dan *affine cipher*. Berdasarkan hal tersebut, skripsi ini diberi judul "Aplikasi Kriptografi Komposisi *One Time Pad Cipher* dan *Affine Cipher*"

1.2 Rumusan Masalah

Berdasarkan latar belakang pada bagian sebelumnya, maka diambil perumusan masalah sebagai berikut :

1. Bagaimana mengkonstruksi kunci *one time pad cipher* agar lebih sederhana?
2. Bagaimana cara mengenkripsi dan mendekripsi pesan dengan kriptografi *one time pad cipher* komposisi *affine cipher* dan sebaliknya?
3. Bagaimana mengkonstruksi progam aplikasi kriptografi komposisi *one time pad cipher* dan *affine cipher*?

1.3 Batasan Masalah

Batasan masalah yang terdapat dalam skripsi ini adalah pengkonstruksian program mengunakan aplikasi Borland Delphi 7.0 dan penyandian teks menggunakan 95 karakter (ASCII).

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah tersebut, maka tujuan penulisan pada skripsi in adalah:

1. Mengkonstruksi kunci *one time pad cipher* yang sederhana.
2. Mengetahui cara menenkipsi dan mendekripsi pesan dengan kriptografi *one time pad cipher* komposisi *affine cipher* dan sebaliknya.
3. Membuat program kriptografi komposisi *one time pad cipher* dan *affine cipher*.

1.5 Manfaat Penelitian

Manfaat penulisan skripsi ini diharapkan dapat memperluas ilmu kriptografi di departemen pendidikan matematika. Sedangkan bagi penulis

penulisan skripsi ini membuat penulis mengetahui banyak konsep matematika yang digunakan untuk kriptografi.

1.6 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, sistematika penulisan skripsi ini.

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

BAB III METODE PENELITIAN, membahas mengenai metode penelitian yang dilakukan dalam penulisan skripsi ini secara garis besar.

BAB IV PEMBAHASAN, menjelaskan pengkonstruksian kunci *one time pad cipher*, kriptografi komposisi *one time pad cipher* dan *affine cipher* dan pembuatan program aplikasi kriptografi komposisi *one time pad cipher dan affine cipher*.

BAB V PENUTUP, menjelaskan kesimpulan dan saran yang diperoleh dalam pengkonstruksian kunci *one time pad cipher* dan pembuatan program aplikasi kriptografi komposisi *one time pad cipher* dan *affine cipher*.