BAB I

PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

Teknologi semakin berkembang yang berdampak positif bagi kehidupan manusia, salah satunya dalam hal berkomunikasi jarak jauh dan bertukar informasi yang bersifat publik maupun rahasia. Namun terdapat dampak negatif dari teknologi, yaitu kerahasiaan suatu informasi atau data semakin mudah diketahui orang lain (pihak ketiga) yang dapat mengakibatkan kerugian pada pihak yang saling bertukar informasi. Salah satu upaya agar data atau informasi tersebut tidak diketahui oleh pihak ketiga, maka dilakukan penyandian data dengan kunci. Orang yang mengetahui kunci pada sandi data tersebut hanya orang yang saling bertukar informasi sehingga rahasia terjamin. Dalam dunia sains, terdapat ilmu yang mempelajari penyandian data yang disebut Kriptografi.

"Kriptografi adalah ilmu pengetahuan dengan teknik matematika yang berhubungan dengan aspek keamanan jaringan, misalnya kerahasiaan data, keutuhan data, autentikasi data dan keaslian data" (Menezes *et al*., 1996: 4). Singkatnya, kriptografi adalah ilmu menyembunyikan data atau pesan. Terdapat dua proses dalam kriptografi, yaitu enkripsi dan dekripsi. Enkripsi adalah proses untuk mengubah data awal menjadi data sandi, sedangkan dekripsi adalah kebalikan dari enkripsi, yaitu proses untuk mengubah data sandi menjadi data awal. Kedua proses tersebut membutuhkan kunci, yaitu inputan untuk proses enkripsi dan dekripsi.

Sejak jaman dahulu, kriptografi sudah digunakan untuk kepentingan pengiriman pesan saat perang (kriptografi klasik). Sistem penyandian kriptografi klasik masih berdasarkan jumlah karakter pesan yang akan disandikan. Kriptografi klasik menggunakan teknik operasi sandi menggunakan metode subtitusi (perpindahan/pergantian huruf) dan metode transposisi (pertukaran posisi).

Sandi *Vigenere* adalah kriptografi klasik dengan metode subtitusi. Sandi *Vigenere* merupakan sistem sandi poli-alfabetik yang sederhana. Misalkan pada saat mengenkripsi data sebuah teks yang terdiri dari beberapa huruf menggunakan barisan karakter kunci yang berbeda. Sandi ini menggunakan operasi *shift*, sebagaimana yang dikemukakan oleh Sadikin (2010: 40) bahwa "operasi *shift* yaitu mensubtitusi suatu huruf menjadi huruf pada daftar alfabet berada di-k sebelah kanan atau kiri huruf tersebut". Sandi dengan metode subtitusi lainnya, adalah sandi *one time pad*, sandi ini merupakan sandi yang mencapai kerahasiaan sempurna (*perfect secrecy*). Shannon (Sadikin, 2010: 55) mendefinisikan bahwa "sebuah sistem sandi mencapai *perfect secrecy* bila pasangan teks asli dan teks sandi tidak memiliki hubungan statistik sehingga sulit bagi penyerang untuk melakukan analisis sandi atau analisis statistik". Kunci yang digunakan sandi *one time pad* ini berbeda untuk setiap karakternya, dengan panjang kunci sama dengan panjang pesan yang akan dienkripsi dan kunci diberikan secara acak dan hanya digunakan sekali.

Dalam jurnal Amroodi *et al.* (2013) menjelaskan algoritma kriptografi baru berupa penggabungan konsep sandi *one time pad* dan sandi *Vigenere*. Pada sandi *one time pad*, kunci yang digunakan untuk proses enkripsi dan dekripsi mempunyai panjang yang sama dengan data awal, sedangkan dalam penggabungan konsep ini kunci sandi yang digunakan cukup memiliki panjang kunci setengah dari panjang data awal. Hal ini berguna untuk peringkasan/pemadatan data. Proses enkripsi dan dekripsi pada kriptografi modifikasi ini menggunakan operasi *bitwise* XOR. Proses enkripsi dengan meng-XOR-kan teks awal (misal: abcd) dan invers dari teks awal (misal: dcba) sehingga diperoleh teks sandi (misal: 1234). Untuk proses dekripsi yaitu meng-XOR-kan teks sandi dan kunci, teks sandi yang digunakan hanya setengah karakter pertama dari panjang teks sandi yang telah diperoleh dari proses enkripsi. Kunci yang digunakan adalah setengah karakter pertama dari panjang teks awal (misal: ab). Proses dekripsi ini menghasilkan kebalikan dari setengah karakter kedua dari panjang teks awal (misal: dc), sehingga perlu diinverskan kembali dan menghasilkan setengah karakter kedua dari teks awal (misal: cd). Teks awal

secara keseluruhan diperoleh dengan menggabungkan kunci dan hasil yang didapat dari proses dekripsi. Sehingga diperoleh teks awal secara utuh (misal: abcd). Oleh karena itu, penulis tertarik untuk membuat program aplikasi dari kriptografi klasik dengan modifikasi. Berdasarkan hal tersebut, judul skripsi ini adalah "PROGRAM APLIKASI KRIPTOGRAFI PENYANDIAN *ONE TIME PAD* MENGGUNAKAN SANDI *VIGENERE*".

1.2 RUMUSAN MASALAH

Berdasarkan uraian latar belakang di atas, maka perumusan masalah pada penulisan skripsi ini adalah:

1. Bagaimana konsep dasar matematika yang digunakan dalam penyandian *one time pad* menggunakan sandi *Vigenere*?
2. Bagaimana merancang dan membuat program aplikasi kriptografi modifikasi tersebut?

1.3 BATASAN MASALAH

Pada pembahasan skripsi ini, penulis memberikan batasan masalah, yaitu program aplikasi kriptografi yang dibuat merupakan implementasi dengan bahasa pemrograman Delphi 7 dan penyandian teks menggunakan 95 karakter (ASCII).

1.4 TUJUAN PENELITIAN

Berdasarkan rumusan masalah yang telah diuraikan, maka skripsi ini bertujuan memberikan gambaran mengenai:

1. Mengetahui konsep dasar matematika yang digunakan dalam penyandian *one time pad* menggunakan sandi *Vigenere*.
2. Mengetahui merancang dan membuat program aplikasi kriptografi modifikasi tersebut.

1.5 MANFAAT PENELITIAN

Manfaat dari penulisan skripsi ini adalah memperdalam keilmuan kriptografi di jurusan Pendidikan Matematika UPI, selain itu program aplikasi ini nantinya

dapat digunakan untuk menyandikan data-data rahasia. Untuk penulis sendiri manfaat yang didapat dalam penulisan ini adalah lebih memahami tentang kriptografi klasik, terutama sandi *Vigenere* dan sandi *one time pad* juga memperdalam pemahaman pemrograman Delphi 7.

1.6 METODOLOGI PENELITIAN

1. Studi Literatur

   Pembelajaran dan pendalaman materi dengan mempelajari literatur, buku-buku referensi, jurnal, maupun internet yang berhubungan dengan penyusunan skripsi ini.
2. Pengembangan Program Aplikasi Kriptografi

   Pengembangan meliputi perancangan segala aspek yang mendukung program aplikasi ini, mulai dari antarmuka pengguna, algoritma sistem penyandian, dan alur program aplikasi.
3. Pembuatan Program Aplikasi Kriptografi

   Pembuatan program aplikasi berdasarkan pada studi literatur dan pengembangan program yang telah dilakukan. Dalam hal ini, pembuatan program aplikasi menggunakan bahasa pemrograman Delphi 7.
4. Pengujian Program Aplikasi Kriptografi

   Setelah program aplikasi selesai dibuat, pengujian dan analisis program dilakukan apakah program telah sesuai dengan apa yang diinginkan. Selanjutnya dirangkum dalam kesimpulan dan saran.

1.7 SISTEMATIKA PENULISAN

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

BAB II LANDASAN TEORI, membahas teori-teori dasar dan konsep yang berhubungan dan mendukung penulisan skripsi ini.

BAB III PENYANDIAN *ONE TIME PAD* MENGGUNAKAN SANDI *VIGENERE*, menjelaskan sandi *Vigenere*, sandi *one time pad* dan algoritma kriptografi sandi modifikasi dari kedua sandi tersebut.

BAB IV PROGRAM APLIKASI KRIPTOGRAFI PENYANDIAN *ONE TIME PAD* MENGGUNAKAN SANDI *VIGENERE*, menjelaskan perancangan, implementasi dan pengujian program aplikasi kriptografi.

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