BAB I

PENDAHULUAN

I.1 Latar Belakang

Pada era teknologi informasi yang semakin berkembang, pengiriman data dan informasi merupakan suatu hal yang sangat penting. Apalagi dengan adanya fasilitas internet yang semakin memudahkan dalam bertukar informasi yang terhubung dengan seluruh dunia. Namun dengan adanya kemudahan seperti ini, keamanan dan kerahasiaanpun akan menjadi hal yang tidak kalah pentingnya. Karena dalam data-data atau informasi-informasi tersebut, tidak jarang terdapat hal-hal yang bersifat pribadi, baik dalam hal personal maupun kelompok atau organisasi.

Karena itu, dibutuhkan suatu cara agar data-data atau informasi-informasi tersebut aman dan terjaga dari pihak-pihak yang tidak bertanggung jawab. Salah satu cara yang sering digunakan adalah penyandian data atau enkripsi. Enkripsi merupakan suatu cara pengkodean atau penyandian data menjadi data yang tidak bisa dimengerti oleh pihak yang tidak diinginkan. Sehingga data rahasia yang dikirim hanya dapat dimengerti oleh pihak-pihak tertentu yang dapat mendekripsikan data hasil enkripsi menjadi data sebenarnya. Ilmu tentang enkripsi dan dekripsi data ini disebut dengan kriptografi.

Pada zaman terdahulu, algoritma kriptografi dilakukan dalam basis karakter (huruf). Karena kriptografi hanya digunakan pada pesan-pesan berbentuk tulisan. Algoritma kriptografi inilah yang disebut algoritma kriptografi klasik atau

sering disebut kriptografi klasik. Tidak seperti pada zaman sekarang ini, dimana komputer adalah sarana utama untuk melakukan pertukaran data dan informasi, sehingga penggunaan algoritma kriptografipun dilakukan pada data-data komputer dalam mode bit-bit atau byte-byte data. Akibatnya kriptografi klasik telah jarang, bahkan sudah tidak digunakan lagi. Karena itulah penulis pada tugas akhir ini mengangkat kembali kriptografi klasik sebagai algoritma kriptografi dan diaplikasikan penggunaannya melalui program komputer.

Puspita (2004) menulis tentang *enkripsi dua tahap menggunakan 3-Hill Cipher dan Vigènere Cipher* yang juga membahas tentang kriptografi dengan dua tahap enkripsi. Yaitu dengan menggunakan *3-Hill Cipher* yang kemudian dilanjutkan dengan *Vigènere Cipher*. Namun penulis menemukan bahwa *3-Hill Cipher* tidak selalu dapat mendekripsi data cipherteks menjadi plainteks yang sebenarnya karena memungkinkan adanya penambahan karakter pada proses enkripsinya. Pada kasus tersebut kunci matriks (kunci *3-Hill Cipher*) yang digunakan adalah matriks-matriks tertentu. Sedangkan cipherteks yang diperoleh dari hasil enkripsi *Keyed Columnar Transposition* pasti dapat didekripsi kembali menjadi plainteks yang sebenarnya. Untuk lebih jelasnya, perbedaan antara *Keyed Columnar Transposition* dengan *3-Hill Cipher* dapat dilihat pada table (1.1).

Dari perbedaan tersebut, penulis melihat bahwa *Keyed Columnar Transposition* lebih baik dalam hal mengembalikan cipherteks menjadi plainteks sebenarnya. Karena dalam beberapa hal, data-data yang telah berubah tidak akan bisa digunakan lagi. Karena itulah pada tugas akhir ini, penulis tertarik untuk mengambil judul “Program Aplikasi Kombinasi Dua Kriptografi Klasik *Vigènere*

Cipher Dan *Keyed Columnar Transposition*" yang akan disertai dengan penyusunan program aplikasinya (perangkat lunak).

Table 1.1 Perbandingan *Keyed Columnar Transposition* dan *3-Hill Cipher*

No.	**Pembeda**	***Keyed Columnar Transposition***	***3-Hill Cipher***
1.	Kunci	Permutasi angka sesuai panjang kunci	Matriks 3×3
2.	Batasan Kunci	Panjang harus kurang atau sama dengan panjang karakter plainteks	Determinan matriks tidak boleh sama dengan nol
3.	Penambahan karakter plainteks pada proses enkripsi	Tidak	Bertambah untuk jumlah karakter plainteks yang bukan kelipatan tiga
4.	Jumlah karakter hasil enkripsi	Sama dengan plainteks	Bertambah untuk plainteks dengan jumlah karakter bukan kelipatan tiga
5.	Hasil dekripsi cipherteks	Tetap	Berubah untuk plainteks dengan jumlah karakter plainteks bukan kelipatan tiga

Pada tugas akhir yang disusun oleh Puspita, penyandian terbatas pada jumlah karakter yang digunakan, yaitu 26 karakter (huruf kapital). Sedangkan pada tugas akhir ini, penulis akan melakukan penyandian data dengan 256 karakter (*ASCII*) sehingga kemungkinan kombinasi kunci khususnya pada *Vigènere Cipher* semakin banyak.

I.2 Rumusan Masalah

Rumusan masalah dari pembuatan tugas akhir ini adalah :

1. Bagaimana merancang kriptografi klasik agar lebih sulit dipecahkan?
2. Bagaimana membuat perangkat lunak (*software*) kriptografi klasik?

I.3 Batasan Masalah

Dalam tugas akhir ini, penulis membatasi permasalahan pada *Vigènere Cipher* dan *Keyed Columnar Transposition*, di mana kedua cipher ini adalah merupakan cipher klasik dengan metode yang berbeda. *Vigènere Chiper* adalah cipher klasik dengan metode substitusi sedangkan *Keyed Columnar Transposition* adalah cipher klasik dengan metode transposisi. Metode *Keyed Columnar Transposition* yang digunakan adalah *irregular case*.

Sedangkan dalam pembuatan *software* (perangkat lunak) kriptografi ini, penulis akan menggunakan bahasa pemrograman *Delphi 7*. Pada perangkat lunak yang akan dibuat, penulis membatasi kunci *Keyed Columnar Transposition* dengan panjang 1 sampai 9. Dan file yang bisa dienkripsi adalah file teks (file dengan ekstensi txt) dan beberapa file teks tertentu seperti file dengan ekstensi html, mht, php, pas, ini, inf, reg, lrc dan beberapa jenis file lainnya.

I.4 Tujuan Penelitian

Tujuan dari pembuatan tugas akhir ini adalah:

1. Merancang kriptografi klasik agar lebih sulit dipecahkan sehingga kerahasiaannya lebih terjaga.
2. Membuat perangkat lunak kriptografi klasik dengan menuangkan algoritma-algoritma kriptografi ke dalam bahasa pemrograman Delphi.

I.5 Manfaat Penelitian

Manfaat dari penelitian ini antara lain:

1. Dapat melihat bahwa kriptografi klasik masih bisa digunakan pada masa seperti sekarang ini dan dapat diimplementasikan menjadi sebuah perangkat lunak komputer untuk menyandikan data-data dan informasi-informasi rahasia.
2. Dapat mempelajari, dan memahami konsep kriptografi-kriptografi klasik yang merupakan dasar dari kriptografi-kriptografi modern.

I.6 Metode Penelitian

Untuk menyelesaikan tugas akhir ini, dibutuhkan langkah-langkah penyelesaian sebagai berikut :

1. Studi Literatur

   Pembelajaran dan pendalaman materi dengan pencarian referensi-referensi yang berhubungan dengan penyusunan tugas akhir ini, baik melalui buku-buku referensi ataupun internet.

2. Perancangan

   Perencanaan dan perancangan beberapa proses dan algoritma yang dibutuhkan untuk membuat perangkat lunak kriptografi.

3. Pembuatan Aplikasi

   Pembuatan perangkat lunak dengan menuangkan algoritma-algoritma yang telah dirancang ke dalam bahasa pemrograman, yang dalam hal ini adalah menggunakan bahasa pemrograman *Delphi 7*.

4. Pengujian dan Revisi Aplikasi

   Pengujian dan revisi hasil pembuatan perangkat lunak untuk melihat adanya kesalahan atau tidak untuk kemudian dapat memperbaiki kesalahan-kesalahan tersebut.

5. Pengembangan Aplikasi

   Pengembangan algoritma maupun sistem yang terdapat pada perangkat lunak setelah sistem utama selesai.

6. Pembuatan laporan

   Pembuatan laporan dan dokumentasi dari proses pembuatan tugas akhir.

I.7 Sistematika Pembahasan

Buku laporan tugas akhir ini terdiri dari lima bab, yaitu:

1. BAB I (Pendahuluan) menjelaskan latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan.

2. BAB II (Landasan Teoritis) membahas teori-teori untuk menunjang penyelesaian masalah dalam pembuatan tugas akhir ini.
3. BAB III (Kombinasi *Vigènere* Cipher Dan *Keyed Columnar Transposition*) membahas tentang *Vigènere Cipher* dan *Keyed Columnar Transposition* serta kombinasi antara keduanya disertai dengan algoritma yang dibutuhkan untuk melakukan enkripsi dan dekripsi data.
4. BAB VI (Hasil Implementasi dan Uji Coba Perangkat Lunak Kriptografi Klasik *Vigènere Cipher Dan Keyed Columnar Transposition*) berisi tentang analisa dari hasil perancangan sampai pengujian perangkat lunak kriptografi.
5. BAB V (Kesimpulan Dan Saran) berisi kesimpulan dan saran-saran untuk pengembangan dan kelanjutan dari hasil yang telah diperoleh dari penelitian ini.