BAB I

PENDAHULUAN

I.1. Latar Belakang

Teknologi sangat diperlukan dalam kehidupan, dimana teknologi dapat membantu untuk mempermudah aktifitas manusia baik dalam berbagi infoemasi berbentuk citra ataupun pesan teks. Namun, seringnya terjadi pengalian pesan atau informasi yang kita kirim ataupun pesan tersimpan yang dilakukan oleh pihak yang tidak bertanggung jawab. Hal ini memungkinkan perlunya menyediakan aplikasi yang dapat mengamankan pesan tersebut untuk menghindari campur tangan pihak luar. Saat ini masih perlunya suatu perhatian dalam tiap data atau *file*. Beberapa algoritma kriptografi pengamanan file teks diantaranya triangel chain dan RC4 (Rivest Shamir Adleman 1987) merupakan algoritma kriptogarfi yang bersifat *One Time Pad* algoritma kriptografi ini dikemukakan oleh Ronald linn Rivest pada tahun 1987. hal ini sesuai dengan nama yang diberikan pada algoritma kriptografi tersebut yang merupakan singkatan dari nama penemunya. Algoritma Kriptografi Triangel Chain merupakan algoritma yang difungsikan untuk melakukan pengenkripsi file, sebuah data input data ASCII dapat dijaga kerahasian dari sebuah file teks.

Algoritma kriptografi *Triangel Chain* atau umumnya dikenal dengan sebutan rantai segitiga merupakan *cipher* yang ide awalnya dari algoritma kriptografi *One Time Pad*, yaitu kunci yang dibangkitkan secara *random* dan

panjang kunci sepanjang plainteks yang akan dienkripsi. Tetapi pada algoritma kriptogarfi rantai segitiga pembangkitan kunci-kunci tersebut secara otomatis dengan teknik berantai. Algoritma rantai segitiga ini memiliki aturan substitusi berdasar pada caesar *cipher* yaitu dengan pergeseran huruf-huruf. Begitu juga dengan algoritma RC4 yang merupakan algoritma enkripsi *stream cipher* dan *symmetric key*, dimana algoritma RC4 ini melakukan proses enkripsi/diskripsi menggunakan kunci yang sama. Salah satu bidang ilmu pengetahuan yang digunakan untuk mengamankan data proses enkripsi data. Dimana cara yang digunakan untuk melakukan enkripsi ialah dengan cara melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti enkripsi dapat diartikan sebagai sebuah kode atau *cipher*.

Selama ini telah banyak yang memanfaatkan algoritma Triangel Chain atau RC4, baik itu untuk pengamanan *file*, citra, atau bahkan pesan SMS, dengan menjadikan pesan atau file yang tersimpan menjadi sebuah pengkodean yang tidak dipahami oleh pihak yang tidak bersangkutan. Dengan itu, dalam perancangan dan penulisan skripsi ini penulis berinisiatif mengembangkan algoritma RC4 serta *Triangel Chain* sehingga masyarakat luas memahami penggunaan algoritma tersebut. Dari latar belakang diatas penulis berencana memberikan judul pada penulisan skripsi ini dengan **"Implementasi Pengamanan File Teks Dengan Metode Triangel Chain dan RC4"**.

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Identifikasi yang penulis temukan dalam penulisan skripsi ini ada beberapa masalah yang disimpulkan yaitu sebagai berikut :

1. Masih sedikit penelitian mengenai pengamanan file teks dengan Triangel Chain dan RC4 .
2. Dibutuhkan penelitian dan pengembangan sebuah aplikasi pengamanan file teks yang memberikan informasi dari algoritma kriptografi pengamanan file teks.
3. Masih kurangnya aplikasi pembelajaran RC4 untuk pengamanan *file* teks.

I.2.2. Rumusan Masalah

Rumusan masalah dalam pembahasan dan permasalahan yang akan dihadapi dalam perancangan aplikasi ini :

1. Bagaimana mengimplementasikan algoritma Triangel Chain serta RC4 dalam pengamanan pesan teks?
2. Bagaimana menyajikan suatu aplikasi yang dapat digunakan untuk pengamanan file teks dengan algoritma Triangel Chain dan RC4 dalam mengamankan suatu pesan teks?
3. Bagaimana mengimplementasikan dalam pengamanan pesan teks dengan menggunakan metode triangel chain serta algoritma RC4 yaitu dengan pengembangan menggunakan pemrograman algoritma kriptografi?

I.2.3. Batasan Masalah

Dalam penulisan skripsi ini penulis membatasi permasalah agar pembahasan tidak rancu dari penelitian, yaitu sebagai berikut :

1. Dalam perancangan penulis membatasi pada pembangunan pengamanan pesan teks.
2. Perancangan aplikasi pengamanan pesan teks menggunakan algortima triangel chain dan RC4.
3. Aplikasi pengamanan pesan teks dengan implementasi algoritma triangel chain serta RC4 dengan pengembangan menggunakan pemrograman *Java*.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan Penelitian

Adapun tujuan dari penelitian penulis ini adalah :

1. Untuk membangung aplikasi pengkodean dengan algoritma *triangel chain* dan *RC4* sebagai pengamanan pesan teks.
2. Untuk mengimplementasikan pemrograman *Java* dengan aplikasi enkripsi pesan teks.
3. Untuk memberikan pehamanan algortima *triangel chain* dan *RC4* kapada pihak umum.

I.3.2. Manfaat Penelitian

Adapun manfaat dari penulisan tugas akhir ini adalah sebagai berikut:

1. Memberikan hasil analisa dan implementasi pengamanan file teks kepada pengguna.
2. Memberikan aplikasi yang dapat melakukan penyandian *file* untuk menghindari manipulasi data oleh pihak. yang tidak bertanggung jawab.
3. Mempermudah pengguna dalam mengamankan pesan teks untuk pencegahan penyalahgunaan oleh pihak yang tidak bertanggungjawab.

I.4. Metodologi Penyelesaian Masalah

Adapun teknik-teknik pengumpulan data yang dilakukan penulisan adalah sebagai berikaut :

1. Penelitian ini bersifat teoritis dengan cara memperoleh informasi dalam buku bacaan, jurnal, artikel seperti algoritma RC4 dan algoritma Triangel Chain, serta yang berhubungan dengan masalah yang akan dibahas yang berasal dari akedemik ataupun dari luar akedemik, terutama yang berkaitan dengan prosedur, implementasi bahasa pemrograman *Java.*
2. Analisa Permasalahan.

   Tahapan ini berupa proses pembelajaran lebih lanjut mengenai permasalahan yang ada menggunakan analisa sebab akibat sebagai dasar penentuan analisa kebutuhan.
3. Analisa Kebutuhan

   Pada tahapan ini dilakukan analisa sehingga dapat didefinisikan kebutuhan-kebutuhan sistem meliputi *input*, *output*, operasi, dan *resources* sehingga dapat terbentuk suatu sistem baru yang lebih handal.
4. Analisa Keputusan

   Tahapan ini bertujuan untuk menentukan solusi yang paling layak di dalam memecahkan permasalahan yang ada. Dalam hal ini berkaitan dengan perangkat keras dan perangkat lunak yang akan digunakan.
5. Desain Sistem

   Tahapan ini meliputi desain model, desain basis data, desain masukan dan keluaran, dan desain dialog antarmuka pengguna.
6. Pembuatan Sistem

Berdasarkan desain yang telah dibuat pada tahap sebelumnya dilakukan proses pembuatan sistem menggunakan perangkat yang telah ditentukan pada tahapan analisa keputusan.

7. Implementasi Sistem

   Tahapan ini tidak akan dikerjakan seluruhnya, hanya tahap pengujian program. Hal ini disebabkan oleh keterbatasan waktu.

I.5. Sistematika Penulisan

Susunan dan sistematika penulisan skripsi ini terdiri dari beberapa sub bab dapat dilihat sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini secara ringkas diterangkan mengenai latar belakang, identifikasi masalah, batasan masalah, tujuan penelitian dan manfaat penelitian, metodologi penyelesaian masalah, serta sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Sub bab ini tentang teori yang berkaitan dengan pembuatan, desain dan tampilan rancangan aplikasi implementasi pengamanan pesan teks serta teori-teori yang mendukung analisa penelitian.

BAB III : ANALISA DAN PERANCANGAN PROGRAM

Berisi tentang analisa dan perancangan aplikasi, yang meliputi analisa masalah, perancangan *interface*, perangkat yang digunakan, metode serta ketentuan penggunaan.

BAB IV: HASIL DAN PEMBAHASAN

Berisi tentang tampilan hasil impelentasi program, beserta pembahasannya, serta kelebihan dan kekurangan sistem yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Dalam bab ini diuraikan kesimpulan dan saran yang dapat diberikan untuk pengembangan aplikasi yang dirancang.