BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Dalam dunia pedidikan, komputer dapat menjadi media pembelajaran yang baru. Pembelajaran yang didapat di perkuliahan terkadang membuat mahasiswa menjadi bosan. Hal itu disebabkan penyampaian yang kurang menarik dan cenderung membosankan, sehingga membuat mahasiswa menjadi mudah lupa dengan apa yang dipelajarinya, terutama pelajaran yang bersifat teoritis. Perlu dilakukan cara lain agar pembelajaran menjadi menarik dan mahasiswa menjadi lebih mudah menerima materi yang diajarkan. Salah satu cara untuk membuat pembelajaran menjadi lebih menarik adalah dengan membuat perangkat lunak media pembelajaran menggunakan komputer.

Komputer dapat menunjang proses pembelajaran karena dengan menggunakan komputer, materi tidak hanya ditampilkan secara tertulis, tetapi juga terdapat suara ataupun animasi dan di samping itu pelajar dapat berinteraksi secara interaktif.

Untuk itu pada skripsi ini dibahas pembuatan perangkat lunak media pembelajaran yang ditujukan untuk materi Kriptografi Blowfish untuk mahasiswa sederajat. Perangkat lunak ini dibuat karena Kriptografi merupakan salah satu cabang ilmu komputer yang sangat mendasar dan sedikit sulit untuk dipahami. Dalam hal teknik pengaman data, banyak metode Kriptografi yang digunakan. Metode-metode kriptografi tersebut mempunyai teknik dan cara tersendiri. Langkah-langkah pengerjaan setiap

metode pun berbeda-beda, baik dari segi panjang maupun kerumitan. Salah satu metode kriptografi yang menarik untuk dipelajari adalah metode Blowfish.

Metode Blowfish dirancang oleh Bruce Schneier pada tahun 1993. Blowfish merupakan algoritma kunci simetri blok kode dengan panjang blok tetap 64 bit. Blowfish menerapkan teknik kunci berukuran sembarangan antara 32 bit hingga 448 bit, dengan ukuran default 128 bit. Keamanan metode inipun berada pada proses pembentukan kuncinya yang panjang dan rumit. Inti dari metode kriptografi Blowfish terletak pada proses pengekspasian kunci dan pembentukan tabel *S-Box*. Tabel S-Box dari metode ini bersifat fleksibel dan berbeda-beda setiap putaran.

Oleh karena itu, dibutuhkan perangkat lunak untuk memaparkan materi tersebut secara visual dan memberi alternatif metode belajar selain buku,yaitu belajar dengan bantuan komputer, yang diharapkan lebih menarik dan interaktif dibandingkan dengan buku biasa.

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah yang diuraikan, maka dapat diidentifikasikan masalahnya, yaitu:

1. Bagaimana membuat materi kriptografi algortima Blowfish yang mudah untuk dipahami oleh mahasiswa atau pelajar.
2. Apakah materi kriptografi algoritma Blowfish dapat dipaparkan secara visual.

3. Bagaimana merancang perangkat lunak materi kriptografi algoritma Blowfish dan bahasa pemrograman untuk mengaplikasikannya.

1.3. Batasan Masalah

Ruang lingkup pada tugas akhir ini dibatasi pada hal-hal sebagai berikut:

1. Materi pembelajaran yang dibahas adalah algoritma Blowfish.
2. Perangkat lunak pembelajaran komputer algoritma Blowfish ditujukan untuk mahasiswa Ilmu Komputer.
3. Lingkungan pengembangan aplikasi menggunakan Visual Basic, dan aplikasi dirancang untuk berjalan di atas sistem operasi Microsoft Windows.

1.4. Tujuan Penelitian

1. Sebagai salah satu syarat kelulusan program pendidikan jenjang Strata-1 pada jurusan Teknik Informatika di STMIK AMIKOM Yogyakarta.
2. Mempermudah dan membantu pemahaman kriptografi khususnya algoritma Blowfish.

1.5. Manfaat Penelitian

Adapun manfaat dari tugas akhir ini adalah:

1. Membantu memvisualisasikan proses enkripsi dan dekripsi algoritma Blowfish.
2. Dengan model pembelajaran berbantuan komputer ini dapat memotivasi pengguna belajar secara efektif dan mandiri.

1.6. Metodelogi Penelitian

Metodologi yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Tahap pengumpulan data yang digunakan dalam penelitian ini adalah sebagai berikut :
    a. Studi Literatur.

       Pengumpulan data dengan cara mengumpulkan literatur, jurnal, paper dan bacaan-bacaan yang ada kaitannya dengan metode kriptografi Blowfish.
    b. Internet.

       Teknik pengumpulan data dengan mencari data-data yang berkaitan dengan kriptografi Blowfish.
2. Tahap pembuatan perangkat lunak

   Teknik analisis data dalam pembuatan perangkat lunak menggunakan paradigma perangkat lunak secara *waterfall*

1.7. Sistematika Penulisan

Sistematika penulisan tugas akhir ini dibagi dalam lima bab, masing-masing bab diuraikan sebagai berikut :

BAB 1 PENDAHULUAN

Bab ini menjelaskan latar belakang masalah, rumusan masalah, batasan masalah, tujuan penulisan, manfaat penulisan, metode penulisan dan sistematika penulisan.

BAB 2 LANDASAN TEORI

Bab ini berisikan penjelasan pembelajaran berbantuan komputer, penjelasan tentang algoritma kriptografi Blowfish, penjelasan tentang proses kerja algoritma kriptografi Blowfish seperti proses enkripsi dan dekripsi.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini berisikan langkah-langkah penelitian yang dilakukan, serta analisis terhadap fokus permasalahan penelitian. Pada bab ini juga akan dibahas perancangan sistem yang merupakan tindak lanjut dari tahapan analisis, termasuk di dalamnya pemodelan proses dan pemodelan data yang dibangun berdasarkan pendekatan terstruktur.

BAB 4 IMPLEMENTASI DAN PEMBAHASAN

Bab ini berisi proses pembangunan perangkat lunak berdasarkan hasil perancangan pada bab sebelumnya dan pengimplementasianya ke sistem nyata.

BAB 5 PENUTUP

Bab ini berisikan kesimpulan-kesimpulan dari bab-bab sebelumnya dan saran-saran yang coba disampaikan penulis guna melengkapi dan menyempurnakan perancangan model pembelajaran berbantuan komputer untuk masa yang akan datang.