BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Berkembangnya teknologi komputer mengubah cara manusia dalam menyelesaikan perkerjaan dalam segala bidang. Keamanan data pada komputer menjadi hal yang penting. Kriptografi adalah ilmu yang digunakan untuk menjaga keamanan dari pihak yang tidak memiliki hak akses terhadap suatu data, baik data berupa e-mail, dokumen, maupun berkas pribadi. Kriptografi memiliki berbagai algoritma dengan kelebihan dan kekurangan masing-masing. Enkripsi dapat diartikan sebagai kode atau chiper. Sebuah sistem pengkodean menggunakan suatu tabel atau kamus yang telah didefinisikan untuk kata dari informasi atau yang merupakan bagian dari pesan, data, atau informasi yang di kirim. Sebuah *cipher* menggunakan suatu algoritma yang dapat mengkodekan semua aliran data (*stream*) bit dari suatu pesan asli (*plaintext*) menjadi *cryptogram* yang tidak di mengerti. Pertengahan tahun 1973, Pemerintah Amerika Serikat (AS) melalui *National Bureau of Standard* (NBS) mengumumkan kebutuhan akan suatu algoritma sandi yang akan digunakan sebagai standar untuk melindungi kerahasiaan dan keutuhan data-data penting baik yang sedang ditransmisikan maupun yang disimpan.

Algoritma DES dikembangkan di IBM dibawah kepemimpinan W.L. Tuchman pada tahun 1972. Algoritma ini didasarkan pada algoritma LUCIFER yang dibuat oleh Horst Feistel. Algoritma ini telah disetujui oleh *National Bureau of Standard* (NBS) setelah penilaian kekuatannya oleh *National Security Agency* (NSA) Amerika Serikat. Sampai pertengahan tahun 1974 tidak ada satupun algoritma sandi yang diusulkan. Hingga akhirnya pada tanggal 6 Agustus 1974, algoritma sandi yang didesain oleh IBM yang

bernama sistem sandi Lucifer ditawarkan kepada NBS. Kemudian setelah dilakukan evaluasi dan modifikasi dengan bantuan *National Security Agency* (NSA), pada tanggal 15 Juli 1977 NBS menetapkan algaritma Lucifer yang telah dimodifikasi tersebut dengan nama baru *Data Encryption Standard* atau lebih populer dengan sebutan sistem sandi DES.

Baitul Maal wat-Tamwil (BMT) Darunnahdhoh adalah sebuah lembaga ekonomi dan keuangan syariah yang berlokasi di Cabang Pulo Bambu, Kabupaten Bekasi. Kegiatan usahanya antara lain memberikan bantuan pinjaman berupa pembiayaan modal usaha untuk pedagang dan pengusaha kecil menengah dan menyelenggarakan jasa simpan pinjam bagi nasabahnya dengan sistem bagi hasil dan margin berdasarkan ekonomi syariah. Produk usaha yang ditawarkan BMT Darunnahdhoh antara lain berupa pembiayaan produk (pembiayaan mudharabah, murabahah, musyarakah dan lain-lain) serta simpanan (simpanan mudharabah biasa, mudharabah berjangka, dan mudharabah khusus). Sebagai sebuah lembaga keuangan mikro yang bertujuan melakukan pemberdayaan ekonomi untuk masyarakat, BMT Darunnahdhoh cukup gencar dalam mengembangkan usahanya. Jumlah nasabah yang bergabung terus meningkat. Selain itu BMT Darunnahdhoh juga menjalin kerjasama dengan berbagai lembaga keuangan lain untuk lebih meningkatkan usahanya.

Sistem informasi perbankan dewasa ini berkembang sangat pesat. Berbagai produk layanan perbankan muncul dengan berbagai variasi yang ditawarkan seperti undian berhadiah, asuransi, fasilitas-fasilitas membership, suku bunga kompetitive dan yang tak kalah penting adalah kemudahan bertransaksi yang semuanya dimaksudkan agar nasabah merasa puas terhadap kualitas pelayanan yang diberikan.

Banyak aspek yang harus diperhatikan dalam mendukung penyediaan layanan tersebut antara lain Pengembangan Sistem Perbankan (*Development of Banking System*), Pengembangan Sistem Informasi (*Development of Information System*), penyediaan

hardware yang memadai, dan tak kalah penting adalah Pengembangan Keamanan Sistem Informasi (*Development of Information Security System*), yaitu keamanan yang memberikan perlindungan baik bagi sistemnya sendiri, maupun terhadap aset Baitul Maal wat-Tamwil (BMT) berupa data yang ada meliputi data intern, data nasabah dan data transaksi. Pengamanan dan perlindungan tersebut dilaksanakan tidak hanya secara fisik tetapi juga dengan pemanfaatan kemajuan teknologi informasi. Masalah yang banyak dibicarakan dalam jaringan global adalah bagaimana memberikan keamanan tehadap data dan informasi karena menyangkut kepentingan pribadi, institusi, keamanan negara dan perusahaan. Oleh karena itu banyak negara-negara yang maju yang telah menghabiskan dana berjuta-juta untuk menangani dengan serius keamanan komunikasi yang sangat rahasia, terutama informasi yang menyangkut tentang kekuatan agen rahasia negara atau hal-hal yang menyangkut rahasia orang yang melakukan aktifitas di jaringan komputer global. Oleh karena itu perlu adanya metode yang memberikan keamanan terhadap data dan informasi dari kebocoran terhadap orang lain yang tidak mempunyai wewenang untuk mengetahuinya.

Salah satu metode yang digunakan untuk mengamankan data dan informasi dari tindakan orang yang tidak berwenang untuk mengetahui informasi tersebut adalah metode enkripsi (Kriptografi). Dalam tugas akhir ini akan dibahas tentang kriptografi dengan metode DES (*Data Encryption Standard*). Kriptosistem penting bagi organisasi yang besar seperti pemerintah atau militer juga keperluan individu. Sebagai contoh, jika nomor kartu kredit dikirim lewat jaringan komputer, diharapkan nomor tersebut hanya bisa dibaca oleh penerima yang diharapkan.

1.2 RUMUSAN MASALAH

Dalam Tugas Akhir ini, masalah yang akan dibahas adalah :

1. Bagaimana membuat perangkat lunak enkripsi dan deskripsi untuk menjaga keamanan data nasabah BMT?
2. Bagaimana menerapkan metode DES (*Data Encryption Standard*) untuk mengenkripsi data nasabah BMT?

1.3 TUJUAN

Laporan Tugas Akhir yang akan ditulis ini, memiliki beberapa tujuan :

1. Bagaimana memahami kriptografi dan hubungannya dengan keamanan data (*security*) dengan menjelaskan apa dan bagaimana kriptografi jika diterapkan untuk keamanan data nasabah BMT.
2. Setelah memahami point satu selanjutnya akan dipilih dan dianalisa terhadap salah satu metode yang ada dalam kriptografi yaitu metode DES (*Data Encryption Standard*).
3. Hasil analisa yang diperoleh dari metode tersebut akan diimplementasikan dengan program aplikasi sederhana menggunakan bahasa pemrograman java.

1.4 BATASAN MASALAH

Batasan masalah dibuat agar tugas akhir yang akan kita rancang dan kita buat, lebih terarah. Berikut ruang lingkup pembahasan, diantaranya :

1. Aplikasi ini menggunakan metode DES (*Data Encryption Standard*).
2. Plainteks yang akan di enkripsi dan dekripsi hanya terbatas dari beberapa nama anggota nasabah BMT Darunnahdhoh.

3. Hasil enkripsi (C*iphertext*) dan dekripsi adalah bilangan *hexa*.
4. Metode *Rational Unified Process* (RUP) yang digunakan pada tugas akhir ini terdiri dari tiga tahap yaitu : *Inception*, *Elaboration*, dan *Construction*.

1.5 METODOLOGI

Metodologi yang digunakan pada tugas akhir ini, terdiri dari metode berikut, yaitu :

1. Metode Pengumpulan Data

Tahap pengumpulan data, terdiri dari :

a. Tinjauan Pustaka

Metode ini bertujuan untuk mendapatkan pemahaman yang cukup mengenai konsep *Enkrispi dan Dekripsi*, *management BMT*, dan *data nasabah BMT*, dengan menggunakan beberapa referensi dari buku, Tugas Akhir, paper dan situs internet. Pemahaman ini nantinya menjadi tolak ukur atau pondasi dalam menyelesaikan Tugas Akhir yang dibuat.

b. Observasi (pengamatan)

Teknik pengumpulan data dengan mengadakan penelitian dan peninjauan langsung terhadap permasalahan yang diambil.

c. Interview (wawancara)

Yaitu teknik pengumpulan data dengan mengadakan tanya jawab secara langsung yang ada kaitannya dengan topik yang diambil.

2. Metode Pengembangan Perangkat Lunak

Metode pengembangan perangkat lunak yang digunakan dalam penelitian ini adalah *Rational Unified Process* (RUP). *Rational Unified Process* (RUP) merupakan suatu metode rekayasa perangkat lunak yang dikembangkan dengan mengumpulkan berbagai *best practises* yang terdapat dalam industri pengembangan perangkat lunak. Ciri utama

metode ini adalah menggunakan *use-case driven* dan pendekatan iteratif untuk siklus pengembangan perangkat lunak. RUP menggunakan konsep *object oriented*, dengan aktifitas yang berfokus pada pengembangan model dengan menggunakan *Unified Model Language* (UML). (Suryana, Taryana. 2007).

Metode *Rational Unified Process* (RUP) merupakan metode pengembangan kegiatan yang berorientasi pada proses. Dalam metode ini, terdapat tahapan-tahapan pengembangan perangkat lunak yaitu:

1. *Inception*

Pada tahap ini pengembang mendefinisikan batasan kegiatan, melakukan analisis kebutuhan user, dan melakukan perancangan awal perangkat lunak (perancangan arsitektural dan *use case*). Pada akhir fase ini, prototipe perangkat lunak versi *Alpha* harus sudah dirilis

2. *Elaboration*

Pada tahap ini dilakukan perancangan perangkat lunak mulai dari menspesifikasikan fitur perangkat lunak hingga perilisan prototipe versi *Betha* dari perangkat lunak.

3. *Construction*

Pengimplementasian rancangan perangkat lunak yang telah dibuat dilakukan pada tahap ini. Pada akhir tahap ini, perangkat lunak versi akhir yang sudah disetujui administrator dirilis beserta dokumentasi perangkat lunak.

1.6 SISTEMATIKA PENULISAN

Sistematika penulisan tugas akhir yang dibuat penulis adalah sebagai berikut :

- BAB I PENDAHULUAN

  Pada Bab ini akan dijelaskan tentang latar belakang penulisan tugas akhir, rumusan masalah, tujuan, batasan masalah penelitian, metode penelitian yang digunakan, serta sistematika penulisan yang menggambarkan urutan penyajian yang digunakan dalam penyusunan tugas akhir ini.

- BAB II LANDASAN TEORI

  Bab ini berisi tentang materi pendukung diantaranya teori aljabar (fungsi), teori bilangan (*number theory*) yang digunakan selama melakukan penelitian dan penyusunan tugas akhir.

- BAB III ANALISIS DAN PERANCANGAN SISTEM

  Bab ini akan menjelaskan tentang kriptografi, analisa metode DES dan algoritmanya dalam proses enkripsi atau deskripsi terhadap data nasabah BMT. Perancangan mengenai deskripsi sistem, *rule* bagan alir informasi, serta rancangan antar muka atau *interface* yang digunakan.

- BAB IV IMPLEMENTASI DAN PENGUJIAN

  Bab ini berisi realisasi dan implementasi dalam proses enkripsi atau deskripsi, dari rancang bangun *software*, yang terdapat dalam bab sebelumnya.

- BAB V PENUTUP

  Berisi kesimpulan dan saran terhadap *aplikasi* yang dibangun dan dikembangkan lebih lanjut.