BAB 1

PENDAHULUAN

1.1 Latar Belakang

Penyimpanan data dalam suatu perusahaan atau instansi dapat dibuat dalam berbagai macam cara mulai dari penggunaan berkas dan formulir hingga penggunaan media penyimpanan dan penanganan data elektronik yang berkembang tingkat kecanggihannya seiring perkembangan dunia komputer. Salah satu cara yang paling lazim digunakan saat ini adalah dengan menggunakan format basis data. Program basis data yang dirancang dengan baik akan memiliki tingkat efisiensi dan efektivitas yang tinggi dalam proses pemasukan dan pencarian serta penanganan data, kemampuan menangani pertukaran data dalam suatu jaringan, dan tingkat keamanan yang tinggi.

Dalam lingkungan perusahaan atau instansi lainnya yang terdiri dari beberapa orang dalam beberapa posisi dan tingkat kewenangan yang berbeda, maka tidak pelak lagi basis data akan dirancang untuk dapat digunakan oleh beberapa orang dengan hak akses yang berbeda-beda. Untuk menghindarkan data jatuh ke tangan yang salah, maka sistem pengamanan data harus dibuat dengan baik. Umumnya, data penting tidak dibagi-bagikan melainkan disimpan di satu tempat (*server*) dan setiap pengguna dapat mengaksesnya baik dengan

mengoperasikan komputer *server* maupun dari komputer lain yang terhubung dalam jaringan.

Saat ini, PT Universal Bina Insan Mandiri yang bergerak di bidang pendidikan anak usia dini dan lebih dikenal dengan nama Cambridge Child Development Centre memiliki permasalahan dalam penanganan basis data siswa dan guru. Sistem basis data Cambridge Child Development Centre ini berada dalam kondisi kacau. Data penting tersebut diletakkan dalam komputer *server* yang terhubung dalam jaringan. Jika data tersebut tidak dimasukkan dalam *shared directory* maka hanya dapat dilihat melalui komputer *server* tersebut atau ditanyakan secara lisan atau melalui email intranet kepada administrator. Padahal data yang terdapat di dalamnya berguna untuk pihak-pihak lain seperti guru kelas dan/atau orang tua murid yang mungkin membutuhkan nama teman sekelas anaknya untuk diundang ke pesta ulang tahun atau sebagainya. Tentunya dengan keadaan ini akan sangat memakan waktu. Masalah juga muncul jika basis data yang ada saat ini dimasukkan dalam *shared directory* dengan kondisi saat ini, karena tindakan ini mengakibatkan seluruh pengguna komputer yang terhubung ke jaringan dapat mengakses bahkan mengubah data yang ada termasuk data-data rahasia seperti gaji guru dan alamat atau nomor telepon murid tertentu.

Guna mengatasi masalah seperti di Cambridge Child Development Centre ini, maka disusunlah suatu program aplikasi yang lebih teratur dan aman. Para pengguna akan dibagi menjadi tingkatan yang membatasi hak akses mereka yang meliputi hak untuk melihat *field* tertentu dan mengubahnya dan seluruh pengguna akan memiliki kata sandi yang mereka pilih sendiri untuk

menghindarkan hal-hal yang tidak diinginkan seperti pengubahan data dengan menggunakan nama pengguna lain.

Informasi yang tersimpan dalam sistem basis data yang akan dirancang ini juga dilindungi terhadap orang-orang yang mungkin akan mencoba membongkarnya tanpa memiliki hak akses. Perlindungan ini akan menggunakan sistem penyandian informasi (*cryptosystem*) yang menggunakan algoritma *Multi Layered User Dependant cipher* yang merupakan modifikasi dan kombinasi beberapa algoritma enkripsi yang semakin terlindungi dengan memasukkan unsur pengguna (dalam hal ini kata kunci yang dipilih pengguna, dijelaskan lebih lanjut pada Bab 3) sebagai salah satu kunci penyandian sehingga data yang disandikan hampir tidak mungkin dapat dibongkar karena memiliki kemungkinan yang sangat banyak.

1.2 Ruang Lingkup

Ruang lingkup perancangan sistem basis data siswa dan guru Cambridge Child Development Centre Disertai Program Perlindungan Data Menggunakan Algoritma Kriptografi *Multi Layered User Dependant Chiper* ini adalah sebagai berikut:

- Dirancang untuk dapat diimplementasikan di Cambridge Child Development Centre.
- Memanfaatkan beberapa algoritma enkripsi yang sudah ada ditambah dengan prosedur enkripsi tambahan untuk mengembangkan algoritma baru. Algoritma enkripsi yang digunakan merupakan varian dari vigenere cipher dengan menggunakan matriks sebagai pengganti vektor dan fungsi linear

sebagai pengganti angka kunci. Varian dari *vigenere cipher* ini kemudian akan dienkripsi sekali lagi menggunakan transposition cipher yang diterapkan secara terbatas pada bagian-bagian tertentu dari pesan (bukan keseluruhan) di mana penentuan bagian ini diambil dari kata sandi yang dimiliki user yang melakukan *entry* atau perubahan pada data ditambah unsur lainnya.

- Dibatasi untuk menerima masukan sesuai dengan yang dibutuhkan oleh Cambridge Child Development Centre dalam kaitannya dengan besar *field* yang akan dibuat.
- Dibatasi untuk menerima masukan hanya dari *keyboard* karena *keyboard* merupakan sarana satu-satunya untuk memasukkan data pada Cambridge Child Development Centre.
- Dibatasi pada penggunaan sistem operasi Microsoft Windows 95 dan variannya (Windows 98 dan 98 *Second Edition*, Windows ME, Windows XP). Program tidak diuji cobakan pada sistem operasi Microsoft Windows NT dan 2000 tetapi dapat dengan aman disimpulkan bahwa program dapat dijalankan pada sistem operasi ini sebagai varian Microsoft Windows.

1.3 Perumusan Masalah

Merancang suatu program aplikasi berbasiskan sistem operasi Microsoft Windows yang dapat menggantikan dan memecahkan masalah yang dihasilkan sistem saat ini di Cambridge Child Development Centre yaitu penggunaan berkas tertulis yang merepotkan dan *sharing* informasi yang memungkinkan terjadinya penyalahgunaan informasi tersebut karena tidak adanya pengamanan.

1.4 Tujuan dan Manfaat

Tujuan perancangan sistem basis data siswa dan guru pada Cambridge Child Development Centre adalah menghasilkan program untuk menangani sistem basis data dan disertai perlindungan menggunakan penyandian data menggunakan algoritma kriptografi *Multi Layered User Dependant Cipher*.

Manfaat perancangan sistem basis data siswa dan guru Cambridge Child Development Centre Disertai Program Perlindungan Data Menggunakan Algoritma Kriptografi *Multi Layered User Dependant Cipher* ini adalah:

1. Bagi penulis ini juga untuk keperluan penyusunan skripsi jenjang pendidikan strata 1 di Universitas Bina Nusantara.
2. Bagi penulis adalah sebagai tugas kerja dari PT Universal Bina Insan Mandiri yang lebih dikenal dengan sebutan Cambridge Child Development Centre yang merupakan tempat kerja penulis saat penyusunan.
3. Bagi Cambridge Child Development Centre adalah untuk mendapatkan sistem informasi yang handal dan aman.
4. Bagi para akademisi adalah sebagai bahan acuan dan pelajaran baik dalam bidang perancangan sistem basis data maupun dalam bidang kriptografi terutama karena algoritma enkripsi yang digunakan merupakan hasil kreativitas penulis.
5. Bagi khalayak ramai adalah untuk mendapatkan algoritma enkripsi yang sulit dipecahkan.

1.5 Metodologi Penelitian

Metode yang digunakan untuk penyusunan skripsi ini adalah sebagai berikut:

- Metode Analisis

  Dilakukan terhadap sistem yang berjalan saat ini di Cambridge Child Development Centre dengan tujuan mendapatkan gambaran sistem informasi yang ada dan kekurangan-kekurangan yang perlu diperbaiki termasuk juga masalah-masalah yang telah pernah terpecahkan.

- Metode Studi Kepustakaan

  Dilakukan untuk mendapatkan informasi mengenai penyusunan sistem basis data, kriptografi, serta penerapannya.

- Metode Perancangan Sistem Informasi

  Untuk menerapkan penelitian tentang sistem basis data dan algoritma enkripsi yang dikembangkan dalam satu program sistem informasi.

1.5 Sistematika Penulisan

Bab 1 : Pendahuluan

Pada bab ini dibahas mengenai latar belakang penulisan skripsi ini, ruang lingkup, perumusan masalah yang ada pada saat ini di instansi bersangkutan, tujuan dan manfaat penulisan dan perancangan, metodologi penelitian, dan sistematika penulisan yaitu bagian ini.

Bab 2 : Landasan Teori

Pada bab ini dibahas teori-teori dasar yang sudah ada dan teori-teori pengembangan yang dihasilkan penulis yang digunakan penulis sebagai landasan untuk merancang aplikasi sistem informasi pada Cambridge Child Development Centre.

Bab 3 : Perancangan

Bab ini berisi sejarah organisasi Cambridge Child Development Centre, gambaran umum perancangan, algoritma yang digunakan, rancangan basis data, rancangan tampilan program pada layar, rancangan basis data, spesifikasi modul, *pseudocode*, bagan alir aplikasi, dan bagan transisi.

Bab 4 : Implementasi

Bab ini berisi penerapan sistem informasi yang dirancang pada Cambridge Child Development Centre yang meliputi kebutuhan perangkat keras dan lunak serta pengoperasian program yang dirancang dan evaluasi.

Bab 5 : Kesimpulan dan Saran

Bab ini berisi kesimpulan penulis tentang penyusunan skripsi ini dan saran untuk mengembangkan lebih jauh lagi tentang basis data dan kriptografi.