BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Masalah keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi. Salah satu cara pembatasan akses data bagi pihak-pihak yang tidak berhak adalah dengan enkripsi. Proses enkripsi merupakan proses untuk meng-*encode* data dalam bentuk yang hanya dapat dibaca oleh sistem yang mempunyai kunci untuk membaca data. Proses enkripsi dapat dengan menggunakan software atau hardware. Hasil enkripsi disebut *chipper*. Chiper kemudian didekripsi dengan device dan kunci yang sama tipenya (sama hardware/ softwarenya serta sama kuncinya).

Metoda enkripsi bukanlah satu-satunya solusi terbaik untuk keamanan jaringan karena kadang-kadang enkripsi juga dapat dipecahkan. Pada sistem unix, biasanya digunakan standar enkripsi *crypt* atau DES. *Data Encryption Standard* (DES) merupakan teknik enkripsi modern yang secara resmi digunakan oleh pemerintah Amerika Serikat di tahun 1977. Sedangkan *crypt* berdasarkan atas teknik enkripsi mesin Enigma Jerman (Perang Dunia II). Dari keduanya DES lebih baik.

DES merupakan blok chiper yang beroperasi dengan menggunakan blok berukuran 64-bit dan kunci berukuran 56-bit.

Guru memiliki data yang sangat penting karena di dalam data tersebut tercatat berbagai informasi dari siswa termasuk proses input nilai ulangan harian yang dikerjakan oleh siswa, tetapi masih banyak sekolah yang belum menerapkan *criptografi* dalam sistemnya. Padahal keamanan data merupakan hal yang sangat penting untuk menghidari orang -orang yang tidak berhak untuk masuk ke dalam sistem dan merubah data yang ada pada sistem.

Data guru merupakan salah satu komponen penting atau rahasia di sekolah karena di sana menyimpan data -data yang penting sehingga perlu adanya keamanan yang megamankan data-data tersebut agar tidak ada pembobolan data atau pelacakan data dari pihak yang berniat jahat.

Pada saat sekarang ini banyak lembaga-lembaga pendidikan belum mengenkripsikan datanya, padahal agar lebih aman data -data siswa tersebut perlu adanya pengenkripsian data dan data menjadi terpusat.

Berangkat dari latar belakang masalah di atas maka penulis kemudian mencoba untuk mengangkat masalah tentang pengenkripsian pada data sistem pendidikan.

1.2 Rumusan Masalah

Dari latar belakang di atas diperoleh rum usan masalah sebagai berikut :

1. Bagaimana cara mengenkripsi data yang ada pa da sistem informasi nilai sehingga, hanya yang memiliki kata kunci dan diskriptornya yang bisa membuka data tersebut.

2. Bagaimana cara penyimpanan data nilai siswa tersebut menjadi terpusat untuk mempermudah pihak guru dalam mengecek data nilai siswa .

1.3 Batasan Masalah

Atas dasar rumusan masalah yang telah disebutkan di atas maka penulis mencoba untuk membatasi ruang permasalahan yang ada sehingga lebih terarah, yaitu:

1. Hanya untuk meng-*encode*-kan data dalam bentuk yang hanya dapat dibaca oleh sistem yang mempunyai kata kunci dan enkriptor serta diskriptor yang sama.
2. Sistem ini dibuat dengan menggunakan Microsoft Web Development 2005 Express Edition.
3. Database sistem ini dibuat menggunakan Sqlexpress yang sudah tersedia di dalam Microsoft Web Development 2005 Express Edition.
4. Untuk mengenkripsi data siswa dengan sistem kriptografi simetri dan tergolong jenis *cipher* blok yang disebut juga DES *(Data Encryption Standard)* . Dengan kunci sebanyak 64 bit, begitu juga dengan deskripsinya.
5. Untuk kecepatan akses database oleh sistem ini akan lebih pelan dari sistem yang tidak menggunakan enkripsi.
6. Rancangan system

   Terdiri dari :

   1. Form login : Digunakan untuk masuk ke dalam sistem, agar dapat mengakses database sistem.

2. Form utama, terdiri dari beberapa menu, yaitu :

   a. Menu siswa : berisi tentang form siswa, yang di gunakan untuk mengisi data-data siswa.

   b. Menu tugas : berisi tentang form tugas, yang di gunakan untuk mengis i data-data tugas yang di kerjakan oleh siswa .

   c. Munu input nilai : berisi tentang form nilai, yang didapat oleh siswa .

   d. Menu laporan, isinya :

      1) Laporan siswa : laporan data siswa yang telah masuk.

      2) Laporan tugas : laporan data tugas yang telah dikerjakan oleh siswa.

      3) Laporan input nilai : laporan data nilai yang telah diperoleh siswa di setiap siswa mengerjakan tugas.

   e. Search : untuk mencari data yang akan ditampilkan atau dicari.

   f. Quit : untuk tombol keluar.

1.4 Tujuan Penelitian

Penelitian ini bertujuan :

1. Untuk mengamankan data guru agar lebih aman.
2. Mengubah penyimpana n data pada sistem yang biasa menjadi terenkripsi.
3. Membantu pengguna dalam penyimpanan data -data penting agar orang lain tidak dapat mengaksesnya.

1.5 Manfaat Penelitian

Hasil penelitian ini diharapkan dapat digunakan sebagai langkah awal dalam pengembangan keamanan data, dan dapat bermanfaat bagi:

1. Instansi
   a. Mengetahui sampai sejauh mana mahasiswa mengimplementasikan materi yang telah didapat.
   b. Salah satu produk untuk mempromosikan institusi di masyarkat .
2. Ilmu Pengetahuan
   a. Sebagai pustaka untuk pengembangan sistem yang merupakan hasil dari penerapan keamanan komputer dibidang kriptografi.
3. Mahasiswa
   a. Membatu mahasiswa mengenali bagaimana meng -enkripsi suatu data.
   b. Sebagai contoh hasil dari keamanan komputer d alam bidang kriptografi.
   c. Acuan untuk mahasiswa dalam meng embangkan keamanan data.

1.6 Metode Penelitian

1. Sifat Penelitian

   Penelitian yang penulis laksanakan dalam perancangan sistem ini menggunakan Microsoft Web Development 2005 Express Edition dengan database Sqlexpress dengan menggunakan algoritma DES *(Data Encryption Standard)*

2. Metode Pengumpulan Data

Penulis dalam melakukan penelitian menggunakan Metode pengumpulan data sebagai berikut :

a. Observasi

Pengumpulan data dengan melihat dan mengamati langsung terh adap apa yang diamati, sehingga diperoleh keamanan data yang akurat dan sesuai, yaitu mengamati saat peng-inputan data dan bagaimana menge nkripsi saat data disimpan.

b. Studi Pustaka

Metode ini dilakukan dengan cara meneliti literatur -literatur yang ada secara langsung ataupun tidak langsung untuk mendukung informasi yang diperlukan serta diperlukan sebagai landasan dalam penyusunan karya tulis ini. Adapun penulis mencari data -data dari buku-buku yang berkaitan, artikel - artikel serta jurnal-jurnal yang menduku ng informasi yang diperlukan.

3. Alat Yang digunakan dalam penelitian

Komputer dengan spesifikasi minimal pentium 3 kecepatan prosesor 1 Ghz, memory 256 Mb, kapasitas kosong pada hardisk 1,3 Gb dan menggunakan sistem operasi Windows XP. Software yang digunakan, yaitu Microsoft Web Development 2005 Express Edition.

4. Bahasa pemrograman

Sistem ini dibuat dengan menggunakan Microsoft Web Development 2005 Express Edition .

1.7 Jadwal Penelitian

Tabel 1.1 Jadwal Kegiatan

No	Target Output	Maret				April					Mei				Target Output
		2	3	4	1	2	3	4	5	1	2	3	4	
1.	Identifikasi Masalah													Mengidentifikasi kebutuhan sistem
2.	Analisi Kebutuhan													Menganalisa Hardware dan software sesuai kebutuhan
3.	Perancangan Sistem													Merancang DAD dan ERD
4.	Perancangan Program													Membuat desain form
5.	Implementasi													Pembuatan semua form sesuai desain
6.	Uji Coba													

1.8 Sistematika Penulisan

Agar penyusunan karya tulis ini memenuhi persyaratan sebagai suatu karya ilmiah yang siste matis, maka perlu diuraikan sistematika penyusunan laporannya.

Adapun sistematika penyusunan laporan karya tulis adalah sebagai berikut:

Bab 1 : Pendahuluan

Dalam bab ini diuraikan tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penulisan karya tulis, metode pengumpulan data , jadwal kegiatan dan sistematika penulisan.

Bab 2 : Tinjauan Pustaka

Berisi tentang ringkasan jurnal -jurnal yang sudah ada dan mendukung dalam peyusunan karya tulis ini serta berisi semua landasan teori yan g selanjutnya digunakan dalam pembahasan.

Bab 3 : Analisa dan Perancangan Sistem

Berisi tentang model pemrograman Microsoft Visual Basic. Net 2005 Express Edition yang digunakan untuk membangun sistem perbankan ini dengan menggunakan keamanan data atau kr iptografi dengan algoritma DES.

Bab 4 : Hasil Penelitian

Pada bab ini diuraikan tentang spesifikasi program dan cara pengoperasian program.

Bab 5 : Penutup

Dalam bab ini berisi tentang kesimpulan dan saran -saran yang dibutuhkan.