PENERAPAN KEAMANAN BASIS DATA DENGAN TEKNIK ENKRIPSI

Hari Purwanto,
Manajemen Informatika, Fakultas Teknologi Industri, Universitas Suryadarma

Abstrak : *Suatu sistem kriptografi (kriptosistem) bekerja dengan cara menyandikan suatu pesan menjadi suatu kode rahasia yang dimengerti oleh pelaku sistem informasi saja. Pada dasarnya mekanisme kerja semacam ini telah dikenal sejak jaman dahulu. Bangsa Mesir kuno sekitar 4000 tahun yang lalu bahkan telah mempraktekkannya dengan cara yang sangat primitif. Dalam era teknologi informasi sekarang ini, mekanisme yang sama masih digunakan tetapi tentunya implementasi sistemnya berbeda. Teknologi basis data dan teknik enkripsi yang lebih canggih lagi digunakan untuk menyimpan hasil enkripsi agar lebih aman. Teknologi enkripsi digunakan semata-mata untuk meningkatkan keamanan data, salah satu penerapannya yang cukup mudah adalah mengintegrasikannya dengan suatu aplikasi,khususnya pada modul login. Modul ini mempunyai peran cukup penting dalam hal keamanan, karena apabila seseorang dapat membuka database dan melihat secara utuh database yang belum di enkripsi, maka akan sangat berbahaya sekali. Oleh karena itu, teknik enkripsi saat ini terus dikembangkan mengingat semakin tingginya ancaman dan gangguan yang datang.*

Kata kunci : *enkripsi, dekripsi, cipher, kriptografi, plaintext, ciphertext, kriptosistem*

1. Pendahuluan

Berbagai organisasi, perusahaan, atau pun pihak – pihak lain telah memanfaatkan teknologi basis data untuk menyimpan dan mengelola data organisasi atau perusahaannya. Saat ini, keamanan terhadap data yang tersimpan dalam basis data sudah menjadi persyaratan mutlak. Pengamanan terhadap jaringan komputer yang terhubung dengan basis data sudah tidak lagi menjamin keamanan data karena kebocoran data dapat disebabkan oleh "orang dalam" atau pihak – pihak yang langsung berhubungan dengan basis data seperti administrator basis data. Hal ini menyebabkan pengguna basis data harus menemukan cara untuk mengamankan data tanpa campur tangan administrator basis data.

Kriptografi dapat digunakan untuk mengamankan data. Oleh karena itu, pengguna basis data membutuhkan bantuan untuk memenuhi kebutuhan keamanan akan data yang disimpannya. Penerapan kriptografi pada Penelitian ilmiah ini akan difokuskan bagaimana kriptografi dapat mengamankan data sampai pada level baris (*row*) dan kolom (*field*) dengan tetap memperhatikan integritas data dan kewenangan setiap pengguna basis data. Algoritma kriptografi yang akan digunakan ialah algoritma kriptografi simetris dan bersifat *stream cipher* sehingga data hasil enkripsi (cipherteks) mempunyai ukuran yang sama dengan data asli (plainteks). Teknik kriptografi simetris dipilih karena diharapkan dengan algoritma ini proses enkripsi – dekripsi data dapat dilakukan dengan waktu yang lebih cepat dibandingkan dengan algoritma kriptografi kunci publik (asimetris).

Berdasarkan latar belakang masalah diatas, identifikasi masalahnya adalah bagaimana merancang suatu perangkat lunak pengenkripsian basis data pada data login yang dapat membantu keamanan aplikasi program dan database.

Adapun tujuan dari penulisan ini adalah

a. Untuk membuat sistem keamanan login aplikasi program dengan menggunakan enkripsi.
b. Mempelajari teknik pengamanan enkripsi sebagai lanjutan dari mata kuliah kriptografi sekuriti.

Adapun batasan masalah dalam penulisan penelitian ilmiah ini :

a. Perancangan program enkripsi pada login aplikasi program ini menggunakan software visual basic 6.0 dengan memanfaatkan menu *.dll.
b. Perancangan data login yang diterima adalah tidak ditentukan dan berbentuk karakter tidak numerik.

Metode yang digunakan dalam pengumpulan data adalah :

a. Wawancara
   Metode ini dilakukan dengan mewancarai pakar yang mengerti tentang keamanan suatu aplikasi program misalnya programer. Metode ini digunakan untuk mengetahui tentang bentuk-bentuk sistem keamanan dengan menggunakan enkripsi
b. Peninjauan dan Pengamatan
   Pengamatan dengan langsung terjun kelapangan. Metode ini digunakan untuk mengetahui aplikasi ilmu yang diperoleh dibangku kuliah dengan aplikasi dalam praktek yang nyata.
c. Penelitian Kepustakaan
   Merupakan cara untuk mendapatkan landasan teori dengan mempelajari dan mencatat literatur dan catatan-catatan kuliah dan penambahan catatan untuk penganalisaan kerusakan dan perbaikan sepeda motor yang erat hubungannya dengan penulisan Penelitian ilmiah ini.

2. TINJAUAN TEORI

2.1 Kriptografi dan Sistem Informasi

Keamanan telah menjadi aspek yang sangat penting dari suatu sistem informasi. Sebuah informasi umumnya hanya ditujukan bagi segolongan tertentu. Oleh ka-rena itu sangat penting untuk mencegahnya jatuh kepada pihak-pihak lain yang tidak berkepentingan. Untuk melaksanakan tujuan tersebutlah dirancang suatu sistem keamanan yang berfungsi melindungi sistem informasi.

Salah satu upaya pengamanan sistem informasi yang dapat dilakukan adalah kriptografi. Kriptografi sesungguhnya merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi, antara lain seperti kerahasiaan, interitas data, otentikasi, dan ketiadaan penyangkalan. Keempat aspek tersebut merupakan tujuan fundamental dari suatu sistem kriptografi.

1. Kerahasiaan (*confidentiality*)
   Kerahasiaan adalah layanan yang digunakan untuk menjaga informasi dari setiap pihak yang tidak berwenang untuk mengaksesnya. Dengan demikian informasi hanya akan dapat diakses oleh pihak-pihak yang berhak saja.

2. Integritas data (*data integrity)*
   Integritas data merupakan layanan yang bertujuan untuk mencegah terjadinya pengubahan informasi oleh pihak-pihak yang tidak berwenang. Untuk meyakinkan integritas data ini harus dipastikan agar sistem informasi mampu mendeteksi terjadinya manipulasi data. Manipulasi data yang dimaksud di sini meliputi penyisipan, penghapusan, maupun penggantian data.

3. Otentikasi (*authentication*)
   Otentikasi merupakan layanan yang terkait dengan identifikasi terhadap pihak-pihak yang ingin mengakses sistem informasi (*entity authentication*) maupun keaslian data dari sistem informasi itu sendiri (*data origin authentication*).

4. Ketiadaan penyangkalan (*non-repudiation*)
   Ketiadaan penyangkalan adalah layanan yang berfungsi untuk mencegah terjadinya penyangkalan terhadap suatu aksi yang dilakukan oleh pelaku sistem informasi.

2.2 Mekanisme Kriptografi

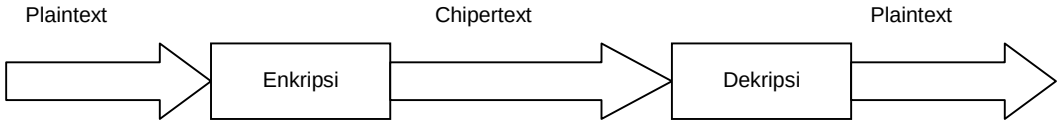
Sebelum membahas lebih jauh mekanisme kriptografi modern, berikut ini di-berikan beberapa istilah yang umum di-gunakan dalam pembahasan kriptografi.

1. *Plaintext*
   Plaintext (message) merupakan

pesan asli yang ingin dikirimkan dan dijaga keamanannya. Pesan ini tidak lain dari informasi tersebut.

2. *Chipertext*
   Chipertext *merupakan pesan yang telah dikodekan (disandikan) sehingga siap untuk dikirimkan.*
3. *Chiper*
   Chiper merupakan algoritma matematis yang digunakan untuk proses penyandian plaintext menjadi ciphertext.
4. *Enkripsi*
   Enkripsi (*encryption*) merupakan proses yang dilakukan untuk menyandikan plaintext sehingga menjadi chipertext.
5. *Dekripsi*
   Dekripsi (*decryption*) merupakan proses yang dilakukan untuk memperoleh kembali plaintext dari chipertext.
6. *Kriptosistem*
   Kriptosistem merupakan sistem yang dirancang untuk mengamankan suatu sistem informasi dengan meman-faatkan kriptografi.

Urutan-urutan proses kriptografi dapat digambarkan sebagai berikut.



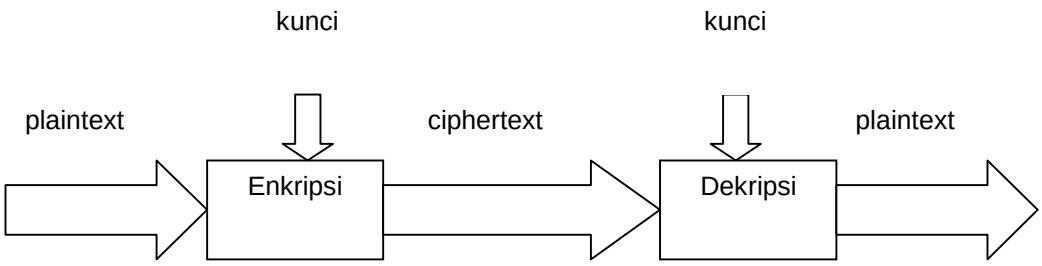
Gambar 2.1. Mekanisme kriptografi

Prosesnya pada dasarnya sangat sederhana. Sebuah plaintext (m) akan dilewatkan pada proses enkripsi (E) sehingga menghasilkan suatu ciphertext (c). Kemudian untuk memperoleh kembali plaintext, maka ciphertext (c) melalui proses dekripsi (D) yang akan menghasilkan kembali plaintext (m). Secara matematis proses ini dapat dinyatakan sebagai,

$$E(m) = c$$
$$D(c) = m$$
$$D(E(m)) = m$$

Kriptografi sederhana seperti ini menggunakan algoritma penyandian yang disebut *cipher*. Keamanannya bergantung pada kerahasiaan algoritma penyandian tersebut, karena itu algoritmanya harus dirahasiakan. Pada kelompok dengan jumlah besar dan anggota yang senantiasa berubah, penggunaannya akan menimbulkan masalah. Setiap ada anggota yang meninggalkan kelompok, algoritma harus diganti karena anggota ini dapat saja membocorkan algoritma.

Kriptografi modern selain memanfaatkan algoritma juga menggunakan kunci (*key*) untuk memecahkan masalah tersebut. Proses enkripsi dan dekripsi dilakukan dengan menggunakan kunci ini. Setiap anggota memiliki kuncinya masing-masing yang digunakan untuk proses enkripsi dan dekripsi yang akan dilakukannya. Dengan demikian ada sedikit perubahan yang harus dilakukan pada mekanisme yang digambarkan pada gambar 2.1 menjadi seperti gambar 2.2 berikut ini.



Gambar 2.2 Kriptografi berbasis kunci

Mekanisme kriptografi seperti ini dinamakan kriptografi berbasis kunci. Dengan demikian kriptosistemnya akan terdiri atas algoritma dan kunci, beserta segala plaintext dan ciphertextnya.
Persamaan matematisnya menjadi seperti berikut,

$$E_e(m) = c$$
$$D_d(c) = m$$
$$D_d(E_e(m)) = m$$

dengan,
e = kunci enkripsi
d = kunci dekripsi

2.3 Kriptografi Simetrik

Kriptografi simetrik (*symmetric cryptography*) atau dikenal pula sebagai kriptografi kunci rahasia (*secret-key cryptography*), merupakan kriptografi yang menggunakan kunci yang sama baik untuk proses enkripsi maupun dekripsi. Secara matematis dapat dinyatakan bahwa :

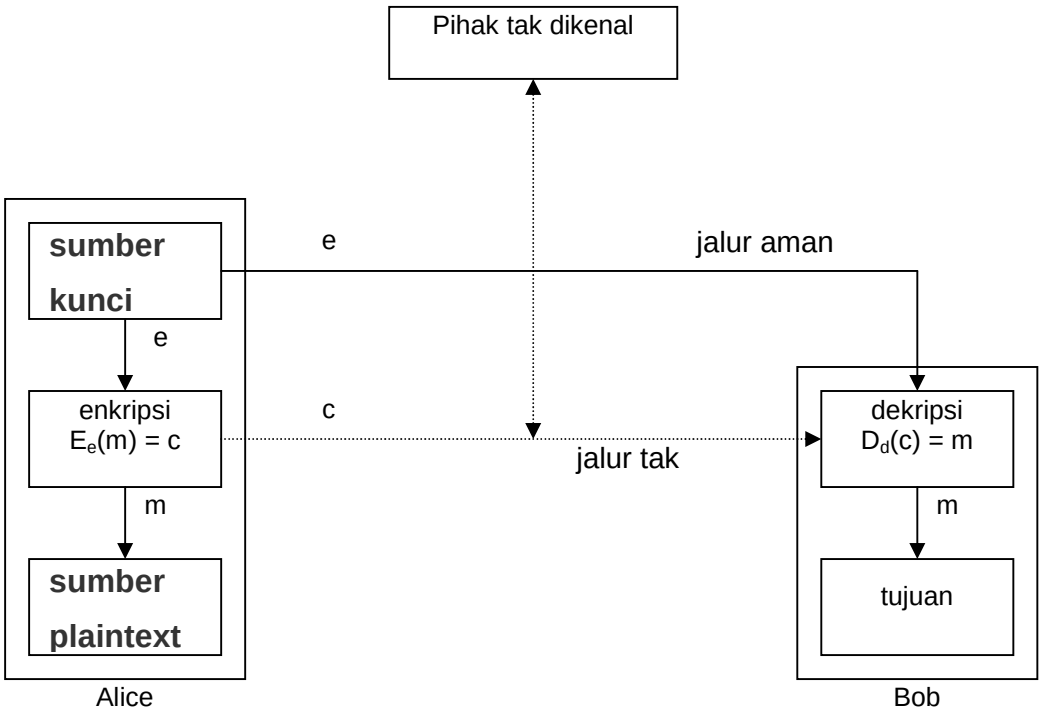
$$e = d = k$$
$$E_k(m) = c$$
$$D_k(c) = m$$

Kriptografi simetrik sangat menekankan pada kerahasiaan kunci yang digunakan untuk proses enkripsi dan dekripsi. Oleh karena itulah kriptografi ini dinamakan pula sebagai kriptografi kunci rahasia.

Mekanisme kerja kriptografi simetrik antara dua pelaku sistem informasi, Alice dan Bob, adalah sebagai berikut,

1. Alice dan Bob menyetujui algoritma simetrik yang akan digunakan.
2. Alice dan Bob menyetujui kunci yang akan dipakai.
3. Alice membuat pesan plaintext yang akan dikirimkan kepada Bob, lalu melakukan proses enkripsi dengan menggunakan kunci dan algoritma yang telah disepakati sehingga menghasilkan ciphertext.
4. Alice mengirimkan ciphertext tersebut kepada Bob.
5. Bob menerima ciphertext, lalu melakukan dekripsi dengan menggunakan kunci dan algoritma yang sama sehingga dapat memperoleh plaintext tersebut.

Gambar berikut memberikan ilustrasi mekanisme kriptografi simetrik ini.



Gambar 2.3 Mekanisme kriptografi simetrik

Dari gambar 2.3 dapat dilihat bahwa harus ada jalur aman (*secure channel*) dahulu yang memungkinkan Bob dan Alice melakukan transaksi kunci. Hal ini menjadi masalah karena jika jalur itu memang ada, tentunya kriptografi tidak diperlukan lagi dalam hal ini. Masalah ini dikenal sebagai masalah persebaran kunci (*key distribution problem*). Kelemahan lainnya adalah bahwa untuk tiap pasang pelaku sistem informasi diperlukan sebuah kunci yang berbeda. Dengan demikian bila terdapat n pelaku sistem informasi, maka agar tiap pasang dapat melakukan komunikasi diperlukan kunci sejumlah total n (n – 1) / 2 kunci. Untuk jumlah n yang sangat besar, penyediaan kunci ini akan menjadi masalah, yang dikenal sebagai masalah manajemen kunci (*key management problem*).

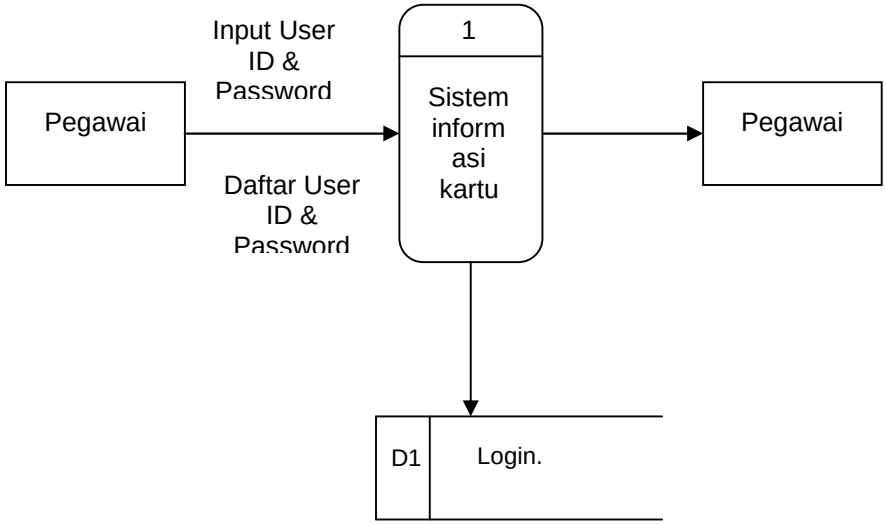
Namun di samping kelemahan tersebut, kriptografi simetrik memiliki keuntungan juga. Keuntungan menggunakan kriptografi simetrik ini adalah kecepatan operasinya yang sangat baik. Dibandingkan dengan kriptografi asimetrik, kriptografi simetrik memiliki kecepatan operasi yang jauh lebih cepat.

3. DESAIN SISTEM

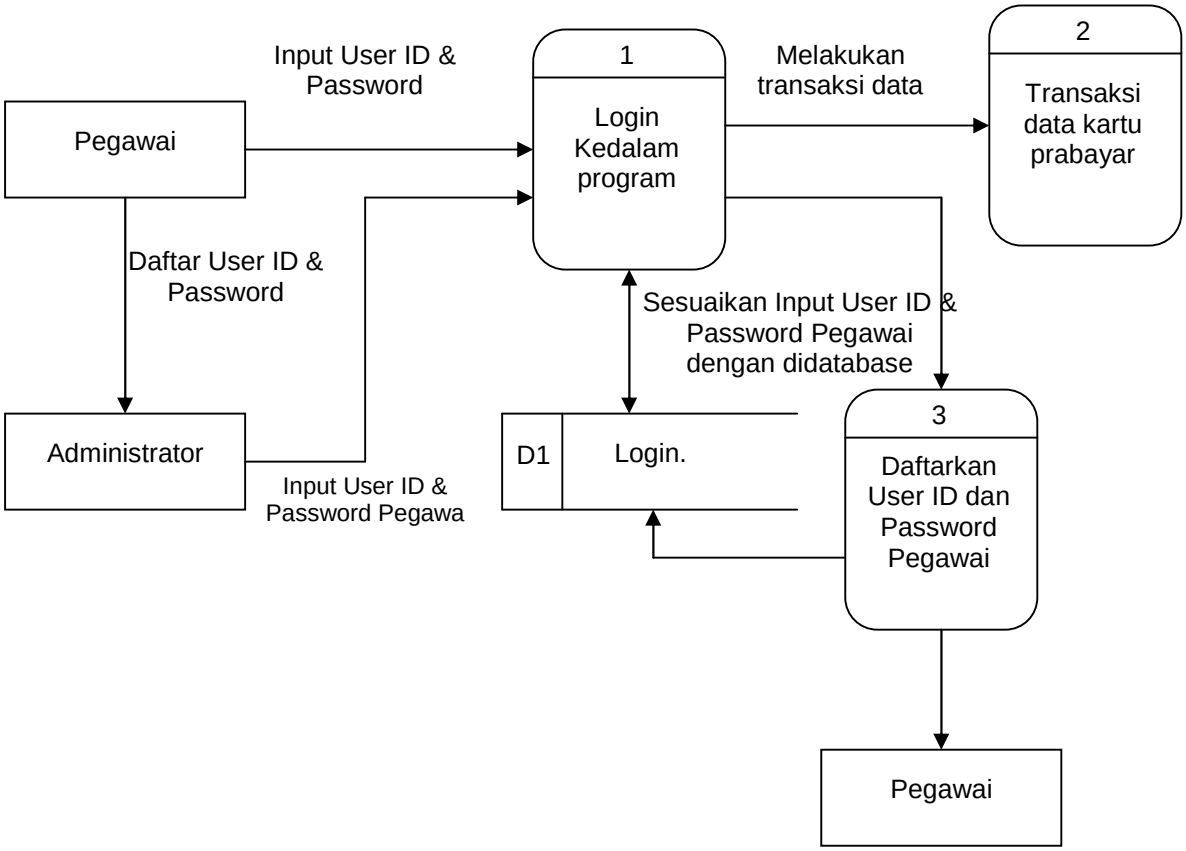
Analisa sistem yang sedang berjalan pada sebuah program distribusi kartu pada sebuah perusahaan telekomunikasi di Medan menunjukkan bahwasanya dalam akses keamanan dalam program distribusi kartu tersebut sangat tidak terjamin dan semua pegawai ataupun orang lain dapat menggunakan program tersebut sehingga yang nantinya akan mengakibatkan kesalahan data dan kerusakan dalam program kerja dimana laporan-laporan yang akan dihasilkan tidak sesuai dengan fakta yang terjadi di lapangan. Misalnya jika ada pegawai atau orang luar yang dapat menggunakan program tersebut maka dia dapat melakukan transaksi permintaan kartu yang fiktif dari sebuah toko distributor maka data transaksi tersebut akan masuk kedalam laporan dan pihak perusahaan akan membuat laporan tersebut ataupun laporan permintaan tersebut langsung akan direalisasikan dan perusahaan akan mengirim barang permintaan toko distributor dan ketika diantar bahwasanya

toko tidak pernah memesan barang tersebut.

Dari hasil penganalisaan penulis, titik kelemahan dari program distribusi kartu tersebut adalah pada menu login. Pada menu login terlihat user name dan password-nya tidak terenkripsi sehingga memudahkan orang yang tidak bertanggung jawab mudah masuk menggunakan user name dan password untuk melakukan hal-hal yang merusak kinerja sistem peru-sahaan.



Gambar 3.1. Diagram aliran data fisik sistem yang sedang berjalan

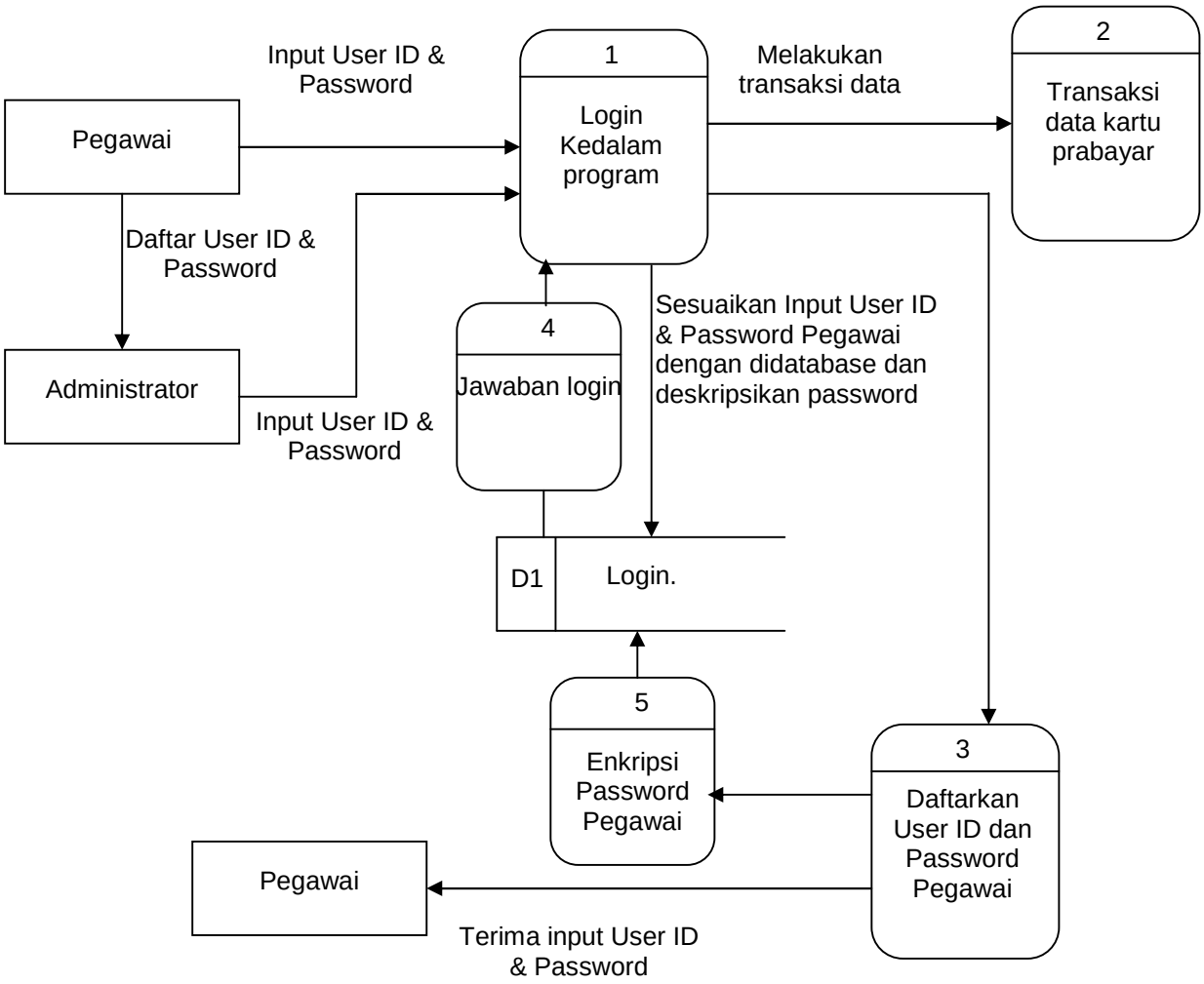


Gambar 3.2. Diagram aliran data logis sistem yang sedang berjalan

3.1. Sistem Yang Diusulkan

Karena lemahnya sistem keamanan dan kerahasian data setelah penulis analis pada sistem yang sedang berjalan, maka sehingga perlu dikembangkan lagi bentuk keamanan dan kerahasian data dengan melakukan pengenkripsian menu password tersebut sehingga orang dapat tidak dapat melakukan login dengan menggunakan user id dan password yang terdaftar karena walaupun orang tersebut dapat menembus dan masuk kedalam database login tetapi ketika orang yang dapat menembus database login program ini tetapi dia tidak akan menemukan password dari user-user id dan hanya akan terlihat user id saja karena isi dari passwordnya telah berubah bentuk karena telah terenkripsi pada saat melakukan pendaftaran user id dan password.

Bentuk pengenkripsian terotomatis pada saat pendaftaran user id dan password pertama sekali.



Gambar 3.3. Diagram aliran data logis sistem diusulkan

Terlihat pada gambar diatas setiap pengguna/pegawai yang akan melakukan kegiatan menggunakan sistem informasi kartu harus melakukan input user id dan password. Setelah user id dan password program otomatis akan mengecek apakah user id dan password terdapat didalam database dan menco-

cokkannya. Saat pengguna selesai mengisi user id dan password dan meng-enter ok otomatis program akan mendeskripsikan password didalam database. Jika user id dan password cocok maka pengguna dapat menggunakan program sistem informasi kartu dan jika tidak cocok maka pengguna diharuskan mengulang pengisian user id dan password.

Dan bagi pengguna yang belum memiliki user id dan password harus menghubungi super admin atau meminta kepada yang sudah memiliki user id dan password untuk mendaftarkan user id dan passwordnya kedalam database. Untuk mendaftar dan mengubah password digunakan menu user account. Pada saat pendaftaran user id dan password program otomatis akan mengenkripsikan password kedalam bentuk enkripsi didalam database login.

3.2. Perancangan Basis Data

Adapun disini penulis hanya menampilkan bentuk struktur data tampilan rancangan basis data login.

Data Login

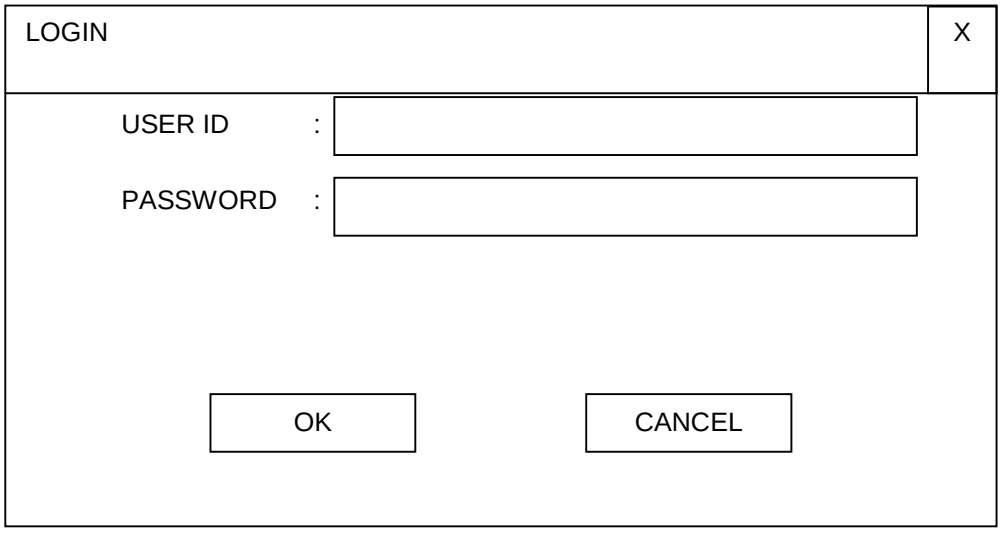
Tabel 3.1. Data login

Field Name	Type Field	Width	Keterangan
UserId	Text	8	Untuk menyimpan user name pengguna
Pass	Text	10	Untuk menyimpan password pengguna
Status	Text	15	Untuk menyimpan status pengguna

3.4. Perancangan Program Enkripsi

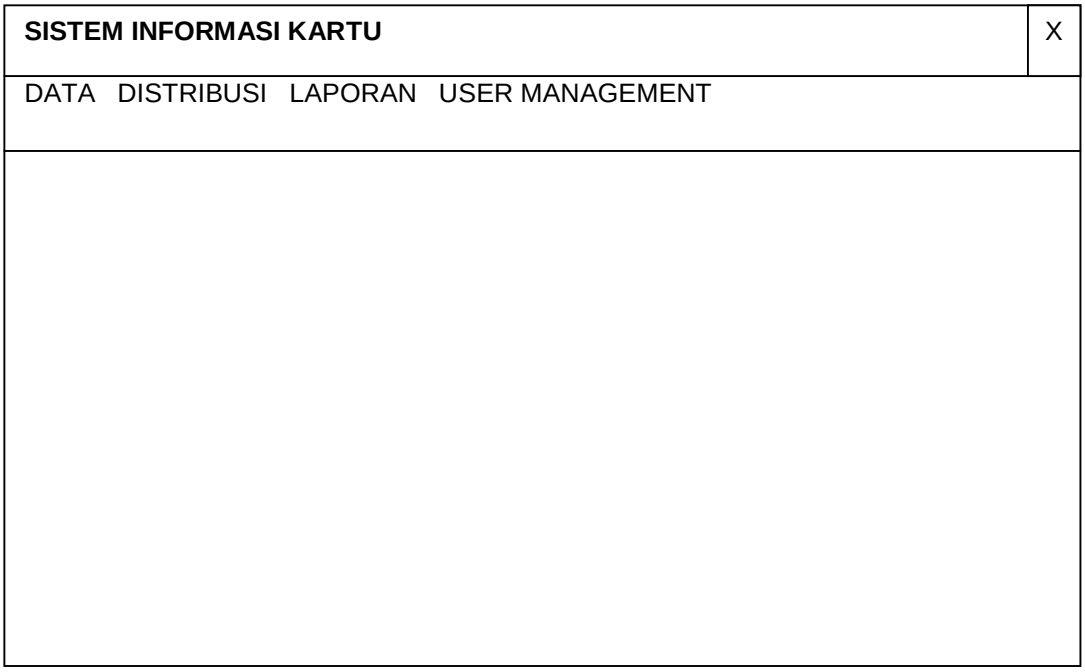
Perancangan program enkripsi ini digunakan untuk membantu pengamanan database login pada program sistem informasi kartu.

3.4.1. Perancangan Form



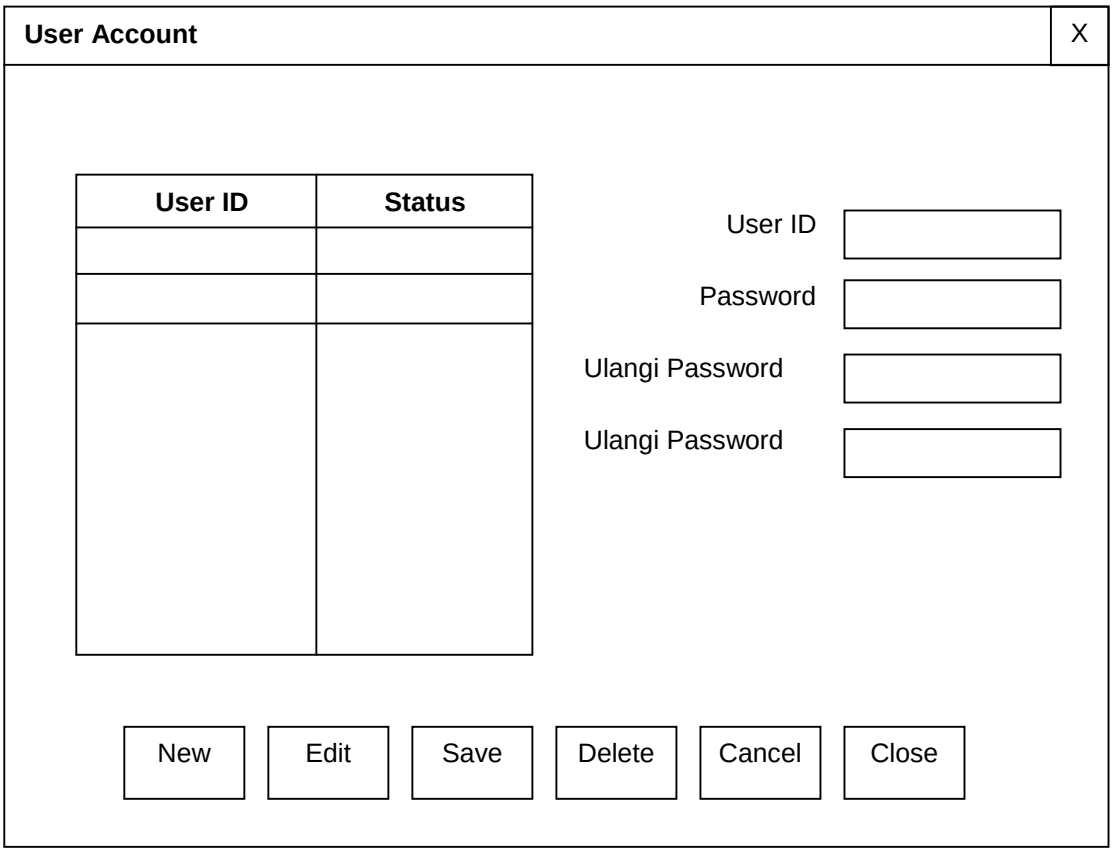
Gambar 3.4. Perancangan form login

Sebelum masuk kedalam program terdapat menu yang pertama yaitu menu login. Jadi setiap pengguna yang akan menggunakan program sistem informasi kartu ini harus melakukan login. Dalam menu login ini pengguna harus mengisikan user id dan password.



Gambar 3.5. Perancangan menu utama sistem informasi kartu

Form menu utama merupakan induk dimana penginputan data, transaksi-transaksi serta laporan-laporan diletakkan disini (dimulai dari sini).



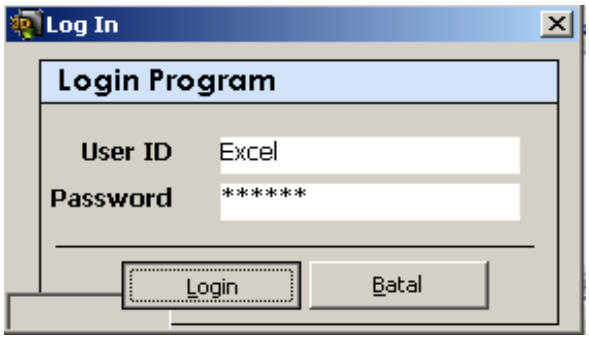
Gambar 3.6. Perancangan form user account

Pada menu user account ini digunakan untuk mendaftarkan pengguna yang akan menggunakan program sistem informasi kartu dan bila pengguna yang ingin mengganti password yang lama.

Implementasi Program

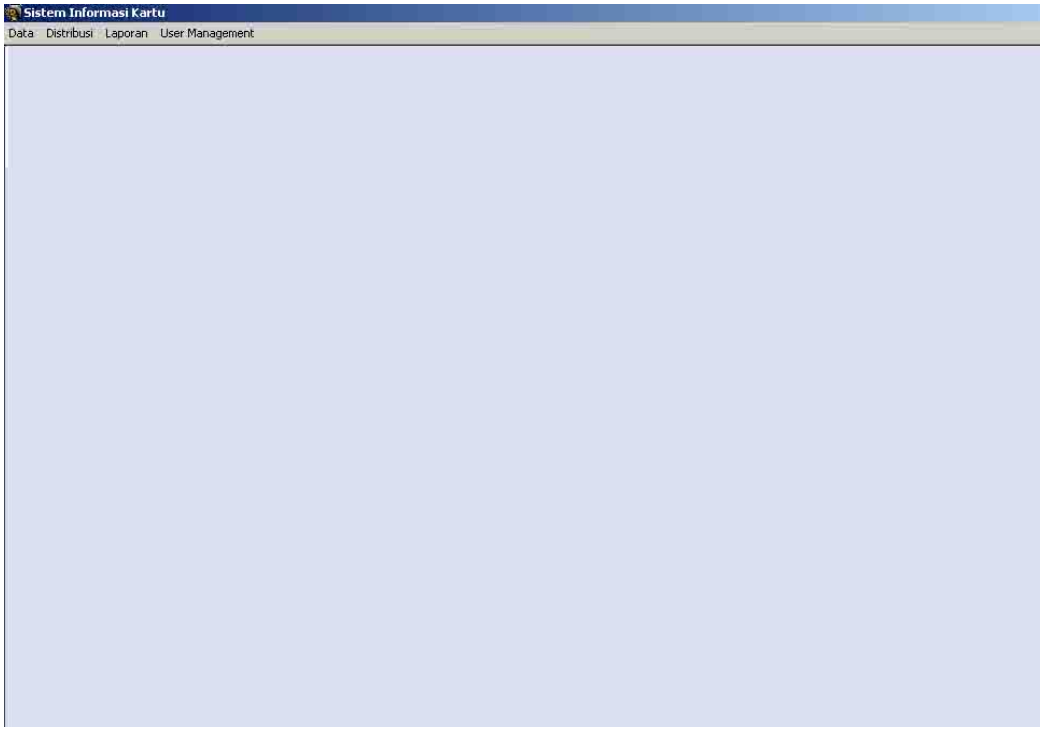
Pada tahap implementasi ini penulis mencoba melakukan percobaan pengamanan database login pada sebuah program distribusi barang dengan menggunakan enkripsi pada data password pengguna sehingga pengguna yang berhak saja yang dapat menggunakan program sistem informasi kartu tersebut.

Untuk dapat masuk ke dalam menu program sistem informasi kartu setiap pengguna harus melakukan login program dengan memasukkan User ID dan Password bila User ID dan Password sudah terdaftar dan sesuai dengan yang ada didatabase maka program sistem informasi kartu dapat terbuka (digunakan). Jika User ID dan Password tidak terdaftar dan salah maka program sistem informasi kartu tidak dapat digunakan (terbuka). Terlihat pada gambar berikut menu login untuk masuk ke dalam program sistem informasi kartu.

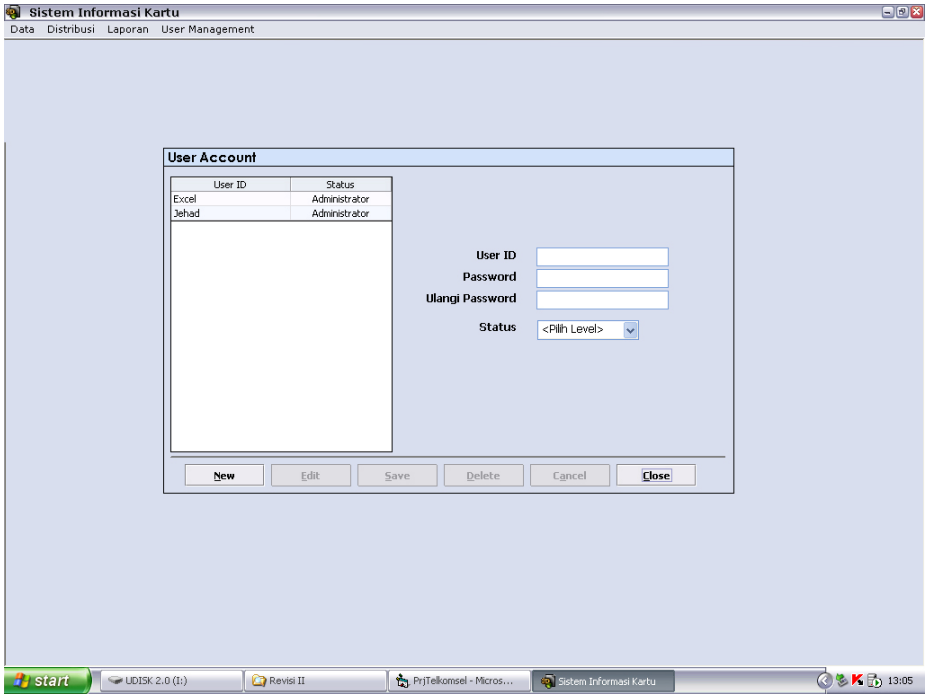


Gambar 3.7. Menu login

Untuk melakukan login pengguna harus memasukkan User ID selanjutnya memasukkan passwordnya kemudian tekan login. Dan bila pengisian User ID dan Password anda ada yang salah dapat menekan tombol batal. Setelah tombol login ditekan dan User ID dan password sesuai dengan didatabase maka pengguna dapat melihat menu utama program sistem informasi kartu seperti pada gambar 3.8. berikut.:

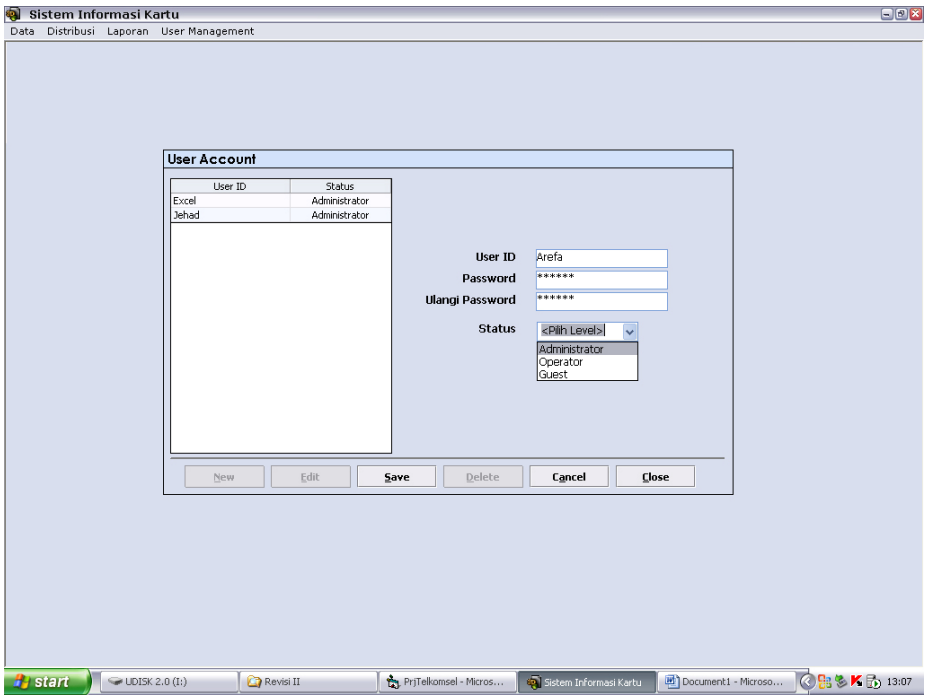


Bagi pengguna yang ingin mendaftar atau mengubah password lamanya dapat menggunakan user manangement kemudian pilih user account.



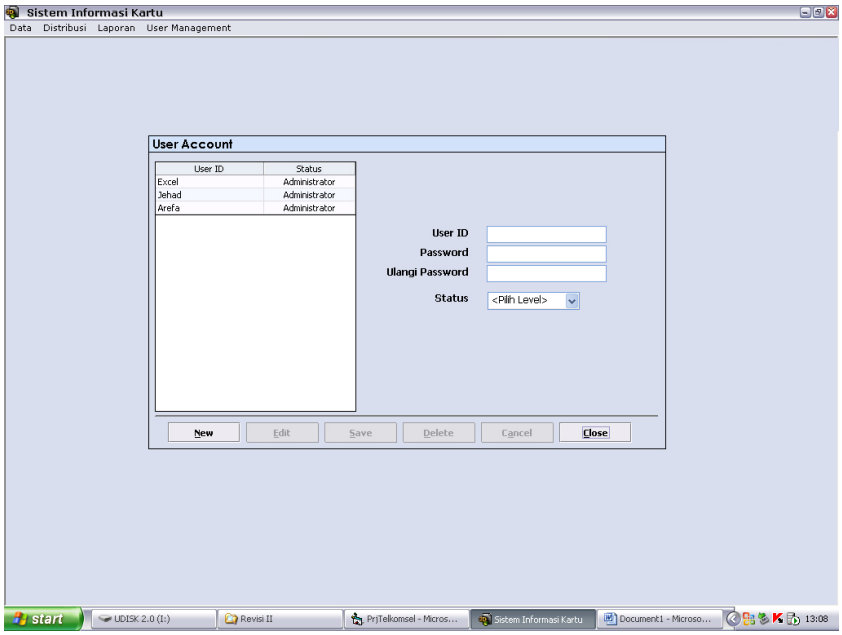
Gambar 3.9. Menu user account

Setelah masuk kedalam menu user account. Bagi pengguna yang mendaftar dapat mengklik tombol new kemudian isikan User ID dan Password dan isi ulang Password dan pilih statusnya. Pada gambar 4.0. ditampilkan contoh pengisian user account yang baru.



Gambar 4.0. Tampilan pengisian user account

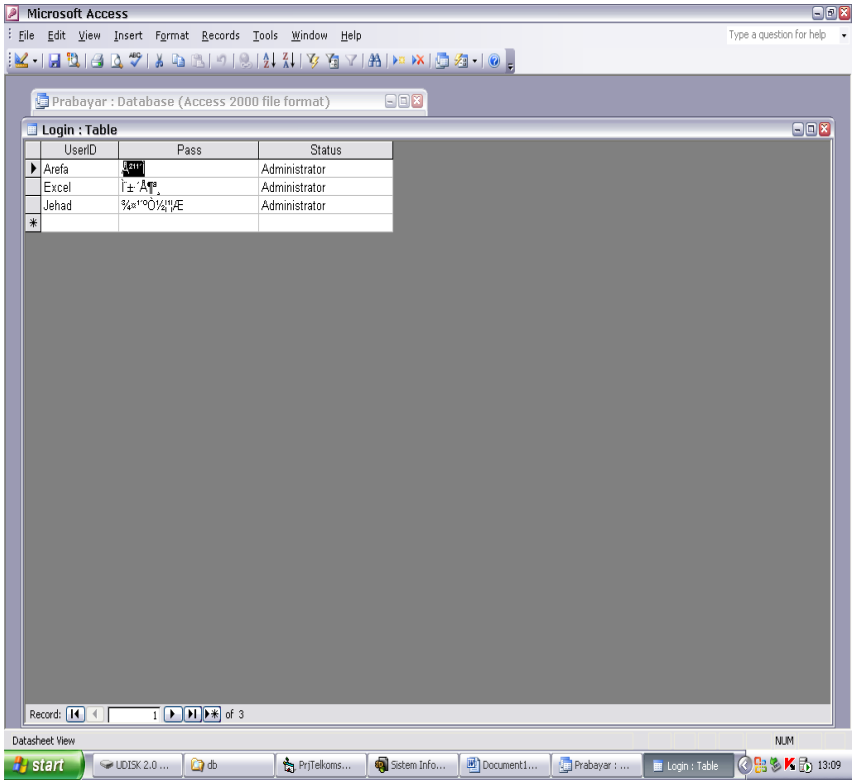
Setelah seluruh inputan diisi maka dilanjutkan untuk menyimpan atau bila anda ada merasa ragu dengan User ID ataupun pengisian password dan ulangi password ataupun salah dalam memilih status dapat menekan tombol cancel. Dan untuk keluar dari program user account dapat mengklik tombol close.



Gambar 4.1. Bentuk pengisian user account

Setelah data-data yang harus diisi telah penulis isi dan penulis telah menyimpannya maka data penulis tampak pada tabel user id didalam user account dimana ditampilkan pada tabel tersebut seluruh pengguna yang telah terdaftar dengan statusnya.

Selanjutnya kita dapat melihat bentuk basisdata pengenkripsian dari pengisian data-data pada menu user account pada tabel database login seperti yang ditunjukkan pada gambar 4.2. berikut.



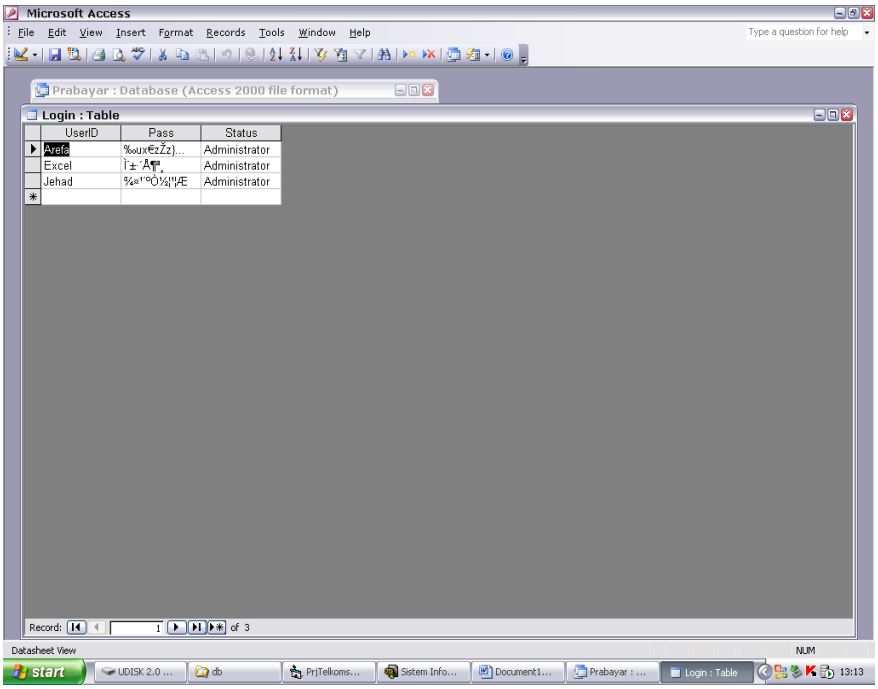
Gambar 4.2. Tabel database login

Pada gambar diatas terlihat bentuk pengenkripsian daripada database dimana yang dienkripsi adalah data password dari user id. Dengan pengenkripsian tersebut seseorang yang ingin menggunakan program sistem informasi kartu tidak dapat menggunakan user id yang lain untuk masuk ke dalam program sistem informasi kartu karena data passwordnya telah terenkripsi.

Disini penulis mencoba untuk menggganti password lamanya dengan password baru. Dalam pergantian password ini pengguna harus mengisi data-data User ID dan password lama serta statusnya. Setelah data-data tersebut diisi maka tekan tombol lanjut.

Setelah tombol lanjut ditekan maka akan muncul pengisian data-data untuk pengisian data-data baru anda seperti halnya pada gambar 4.2. Setelah data-data baru penulis isi kemudian penulis menyimpannya.

Berikut penulis tampilkan database dari data-data penulis yang baru seperti pada gambar 4.3 berikut.



Gambar 4.8. Bentuk database login

4. KESIMPULAN DAN SARAN

4.1. Kesimpulan

Setelah penulis menguraikan semuanya tentang perancangan dan implementasi dari enkripsi data login ini, maka penulis mengambil beberapa kesimpulan yaitu :

1. Dengan pengenkripsian database pada sebuah program dapat membantu pengamana program dari pengguna yang tidak bertanggung jawab.
2. Banyaknya bentuk-bentuk algoritma untuk metode enkripsi dan deskripsi sebagai pengembangan ilmu pengetahuan tentang kriptografi sekuriti sistem.
3. Salah satu upaya pengamanan sistem informasi yang dapat dilakukan adalah dengan kriptografi sekuriti sistem.

4.2. Saran

Adapun saran-saran yang penulis kemukakan adalah sebagai berikut :

1. Kiranya dalam pengajaran mata kuliah kriptografi dan sekuriti dapat dianjarkan tentang implementasi dari kriptografi tersebut.
2. Aplikasi enkripsi yang penulis kerjakan kiranya dapat dikembangkan kedalam bentuk pengamanan yang lebih baik lagi.

DAFTAR PUSTAKA

[1]. Rahmani, *Implementasi Teknik Kriptografi Blowfish untuk Pengamanan Basis Data*, Tesis Magister Departemen Teknik Informatika, ITB, 2003.

[2]. Silberschatz, H. F. Korth. Dan S. Sudarshan, *Database System Concepts, 4th Edition*, McGraw – Hill, 2002.

[3]. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition,*John Wiley & Sons, Inc, 1996.

[4]. Sukmawan, *RC4 Stream Cipher*, 1998.

[5]. Trower, *Crypt Data Packaging*, Trantor Standard Systems Inc.

[6]. Fathansyah, *Basis Data*, Informatika, Bandung, 1999.

[7]. R. Munir, *Bahan Kuliah IF5054 Kriptografi*, Departemen Teknik Informatika, ITB, 2004.

[8]. T. Marcus, A. Prijono dan J.Widiadhi, *DELPHI DEVELOPER dan SQL Server 2000*, Informatika, Bandung, 2004.