SISTEM INFORMASI PENGAMANAN BASIS DATA MENGGUNAKAN TEKNIK ENKRIPSI BAGIAN TATA USAHA LEMBAGA SANDI NEGARA

NUNU KUSTIAN
kustiannunu@gmail.com
Teknik Informatika, Fakultas Teknik dan MIPA Univesitas Indraprasta PGRI Jl. Nangka No. 58C Tanjung Barat Simatupang, Jagakarsa, Jakarta 12530 Indonesia

Abstrak. Lembaga Sandi Negara sebagai salah satu lembaga pemerintah non-departemen dibentuk karena diperlukannya pelaksanaan tugas pemerintah dibidang persandian sesuai dengan ketentuan peraturan perundang-undangan yang berlaku *(keputusan presiden RI nomor 103 tahun 2001*. Mengingat bahwa berita rahasia Negara yang dikirim melalui sarana komunikasi perlu dilindungi dari kebocoran-kebocoran, maka penyelenggaraan sistem informasi yang menggunakan teknologi komputer dalam pemberitaan rahasia Negara yang disalurkan dengan sistem persandian, pelaksanaannya dikoordinasi oleh Lembaga Sandi Negara. Beberapa kendala yang dialami oleh karyawan Bidang Tata Usaha Lembaga Sandi Negara (*user*) dalam mengatasi administrasi dapat mengakibatkan terbengkalainya pekerjaan yang dilakukan oleh *user* yang mengalami gangguan tersebut. Untuk mengatasi hal tersebut, terdapat beberapa alternatif pemecahan masalah yang dapat dilakukan untuk mengatasi permasalahan yang ada dengan membuat sistem keamanan login aplikasi program menggunakan enkripsi berbasis program PHP dan MySQL dengan implementasi MD5 pada saat login dalam membantu kegiatan bagian Tata Usaha Lembaga Sandi Negara.

Kata Kunci: Lembaga Sandi Negara, Sistem Informasi, Enkripsi, MD5, PHP, MySQL

PENDAHULUAN

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.

Untuk dapat menjamin keamanan rahasia Negara dari kebocoran-kebocoran yang memanfaatkan sistem informasi dengan teknologi komputer dibutuhkan suatu sistem pengamanan yang handal serta tenaga operasional atau staf yang mempunyai integritas dan loyalitas, karena adanya kecerobohan pengguna dalam memperlakukan jaringan komputernya, sehingga terdapat celah-celah yang dapat dimanfaatkan oleh pihak-pihak yang tidak berhak untuk mengambil keuntungan tertentu. 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 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 *(chiperteks)* 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).

METODE

Penelitian ini menggunakan metode *Grounded theory*. *Grounded Theory* adalah salah satu jenis metode kualitatif karena analisanya tidak menggunakan angka. Objek penelitiannya adalah suatu fenomena yang ada dalam konteksnya yang alamiah dan dimengerti sesudah data lapangan diperoleh, entah melalui wawancara atau observasi, diinterpretasi.
Dalam metode ini koleksi data, analisis, dan teori satu dengan lain sangat berhubungan (Strauss dan Corbin, 1008 dalam Bryman, 2001). Ada dua hal yang sentral sebagai ciri utama *grounded theory* yang berkenaan dengan perkembangan teori berdasarkan data dan pendekatan *iterative* atau *recursive,* yang artinya koleksi data dan analisis secara bersamaan timbal balik pengaruh mempengaruhi. Tidak cukup *grounded theory* hanya dikembangkan bersumber dari data, karena mencakup perangkat prosedur tertentu.

Adapun metode yang digunakan adalah:

1. 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
2. Observasi
   Pengamatan dengan langsung terjun kelapangan. Metode ini digunakan untuk mengetahui aplikasi ilmu yang diperoleh dibangku kuliah dengan aplikasi dalam praktek yang nyata.
3. Studi Pustaka
   Merupakan teknik pengumpulan data yang dilakukan dengan membaca atau menganalisis catatan-catatan, arsip-arsip, dokumen-dokumen serta penelitian literature untuk teori dan penelitian sebelumnya yang sesuai dan berhubungan dengan permasalahan yang diteliti.

Secara garis besar proses kegiatan kerja Tata Usaha Lembaga Sandi Negara adalah sebagai berikut:

1. Prosedur Penerimaan Surat
   Surat dari instansi A ditujukan kepada Kepala Lembaga, setelah diterima dan diagendakan oleh satuan kerja Persuratan dan Kearsipan. Tetapi surat yang ditujukan selain untuk Kepala dan SU, maka surat tersebut langsung diagendakan oleh satuan kerja tujuan surat.
2. Surat Keluar
   Mengagendakan surat yang dikirimkan keluar instansi lembaga.
3. Kepegawaian
   Penginputan data pegawai Lembaga Sandi Negara. Terdapat dua aktifitas, yaitu *input* data pegawai dan *edit* data pegawai.

Langkah-langkah Pengembangan Sistem

Adapun langkah-langkah pengembangan sistem sebagai berikut:

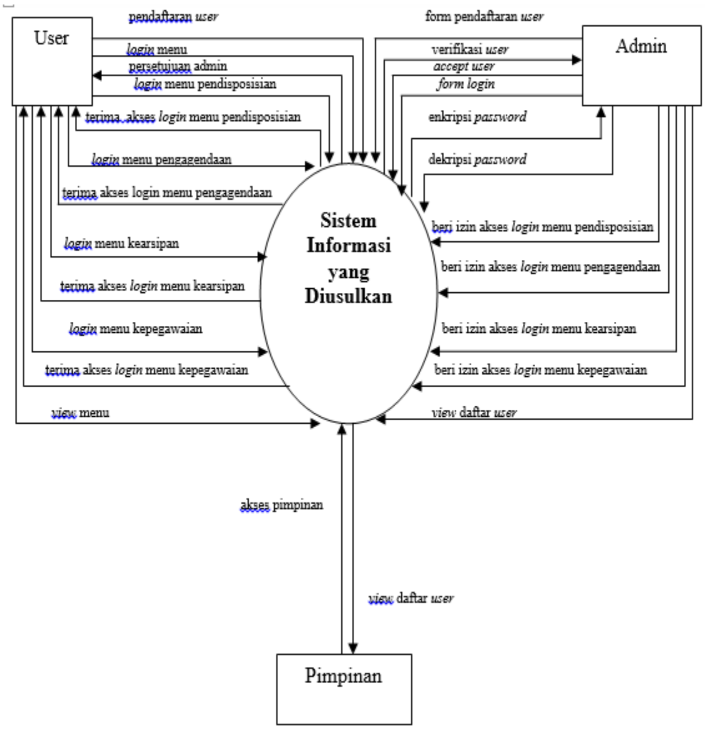
a. Analisa Kebutuhan
   Bertujuan untuk mendapatkan data-data yang akan digunakan sebagai masukan dari sistem (perangkat lunak) dan memperoleh data yang berhubungan dengan Proposal Skripsi ini. Proses pembuatan perancanaan program menggunakan PHP, MySQL, dan Xampp server dan didukung peralatan lainnya. Sebelum merancang kita harus mengetahui apa saja kebutuhan pengguna inginkan dan bagaimana mereka melakukan cara memenuhi keinginannya.

Faktor Exacta 7(2): 188-199, 2014
ISSN: 1979-276X

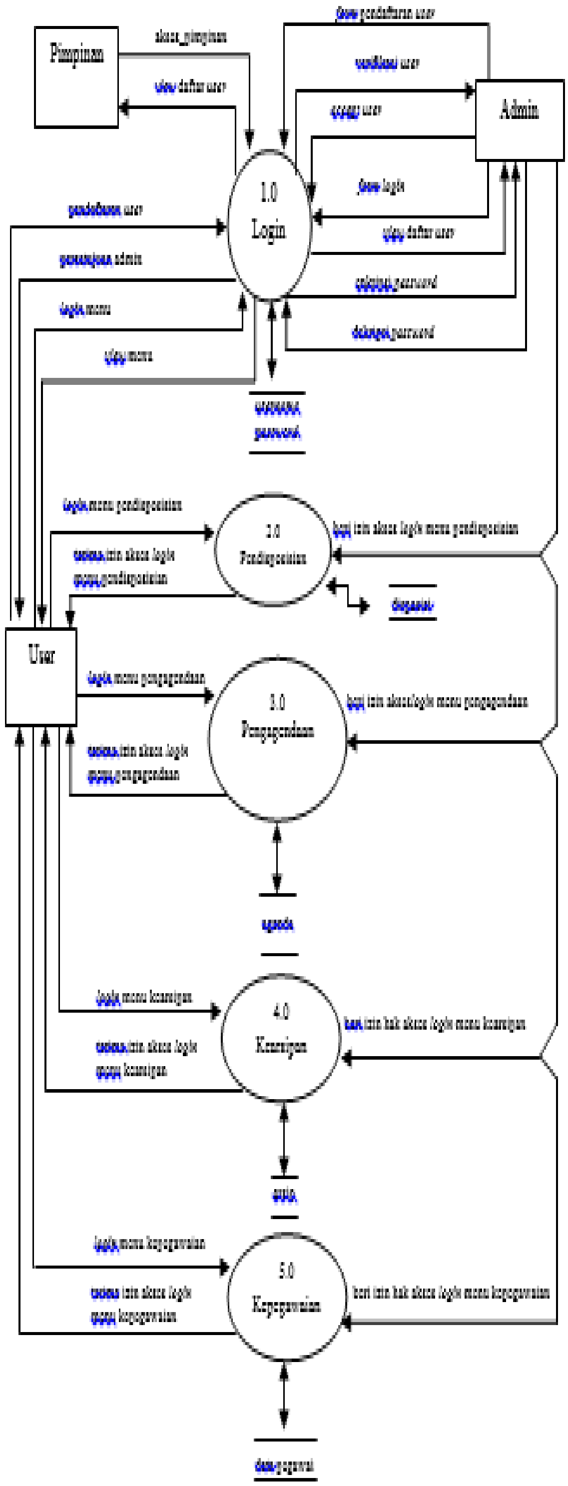
b. Perancangan Sistem
   Bertujuan untuk merancang sistem yang akan dibuat agar dapat diimplementasikan dengan kebutuhan pengguna.
c. Pengkodean
   Pengkodean adalah proses menterjemah dokumen hasil desain baris-baris, perintah bahasa pemrograman komputer. Semakin baik hasil analisis dan desain yang dilakukan, maka proses pengkodean ini akan mudah dilakukan.
d. Pengujian
   Pengujian adalah proses untuk memastikan apakah semua fungsi sistem bekerja dengan baik, dan mencari apakah masih ada kesalahan pada sistem. Pengujian sangat penting untuk dilakukan pengujian ini, bertujuan untuk menjamin kualitas software dan juga menjadi peninjauan terakhir spesifikasi, desain dan pengkodean.
e. Implementasi
   Menerapkan atau memperkenalkan suatu sistem baru dengan melakukan dua cara yaitu langsung pelaksanaan dan menjalankan secara paralel. Namun dalam sistem informasi ini melakukan pelaksanaan secara langsung agar diketahui dengan cepat kesalahan

HASIL DAN PEMBAHASAN

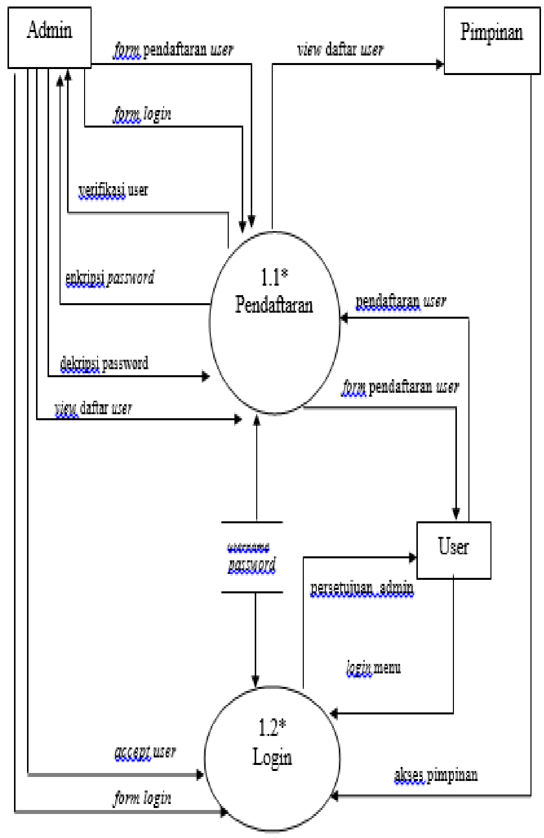
Diagram Konteks



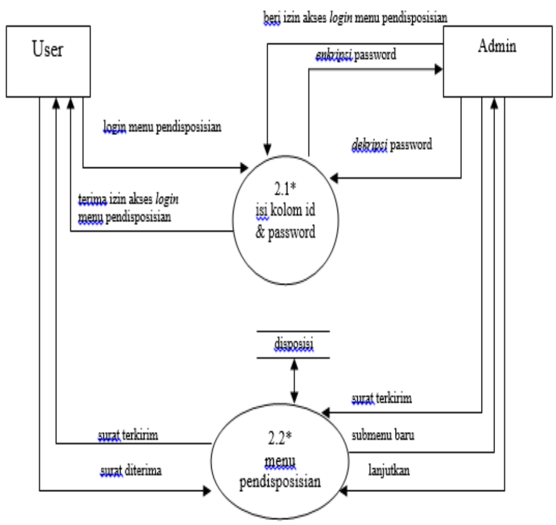
Gambar 1. Diagram Konteks yang diusulkan



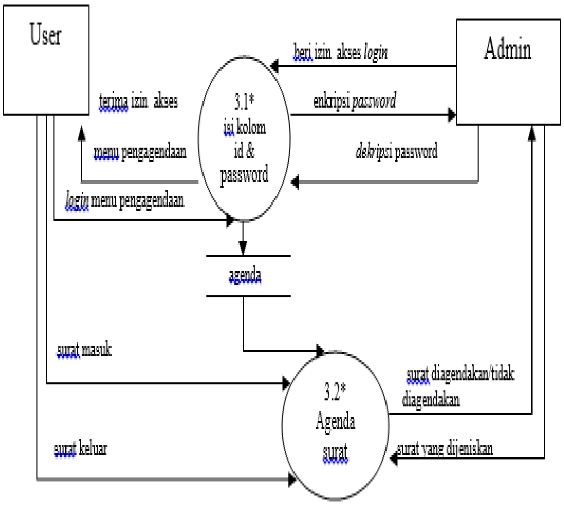
Gambar 2. Diagram Nol yang Diusulkan



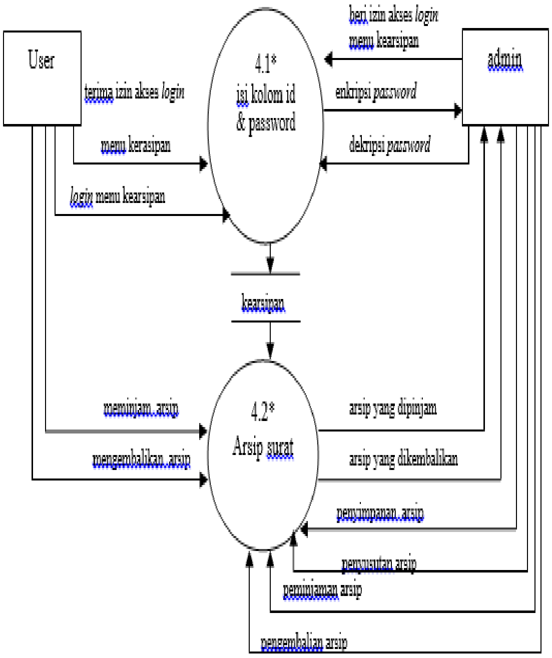
Gambar 3. Diagram Proses Login yang Diusulkan



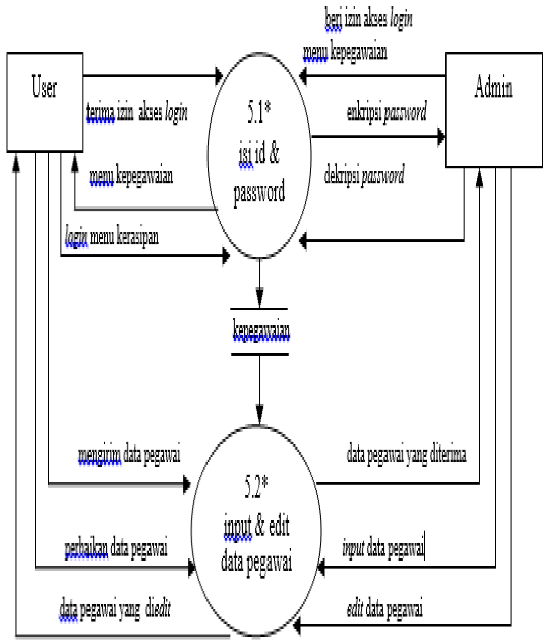
Gambar 4. Diagram Rinci Proses Pendisposisian yang Diusulkan



Gambar 5. Diagram Rinci 3.0
Proses Pengagendaan yang Diusulkan

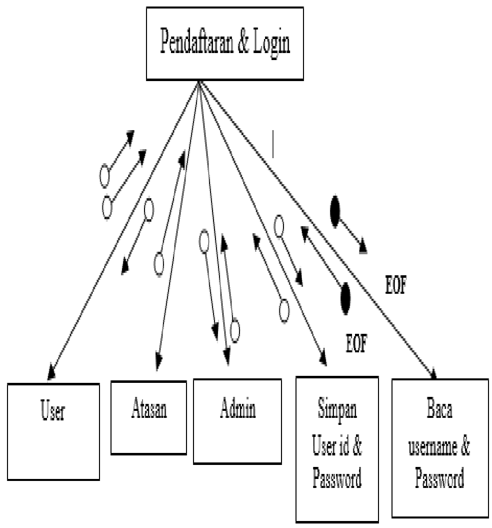


Gambar 6. Diagram Rinci 4.0 Proses Kearsipan yang Diusulkan

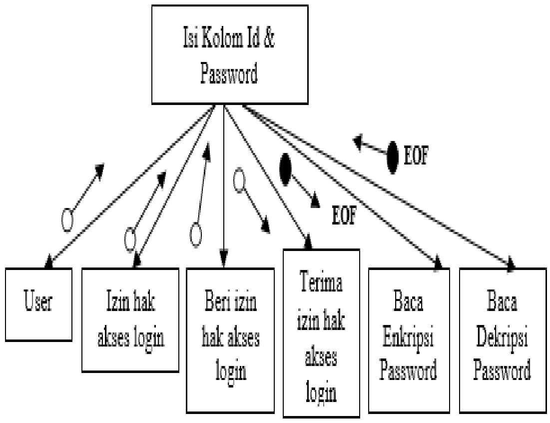


Gambar 7. Diagram 5.0 Proses Proses Kepegawaian yang Diusulkan

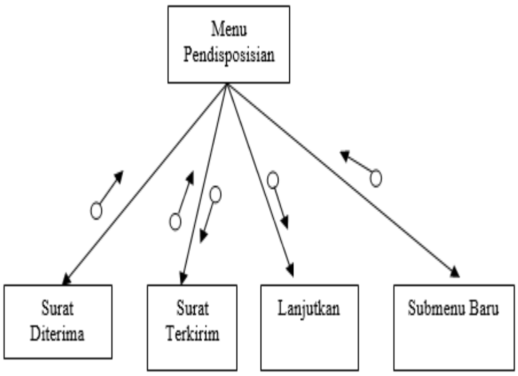
Bagan Terstruktur Sistem yang Diusulkan



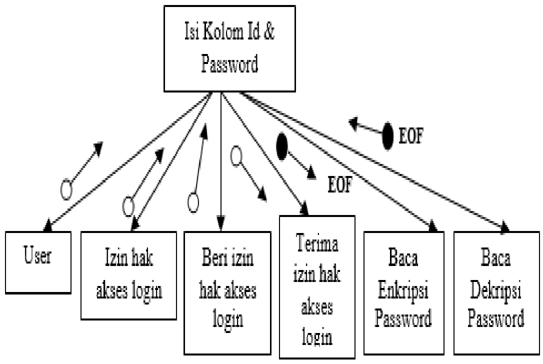
Gambar 8. Bagan Terstruktur Diagram Rinci 1.1



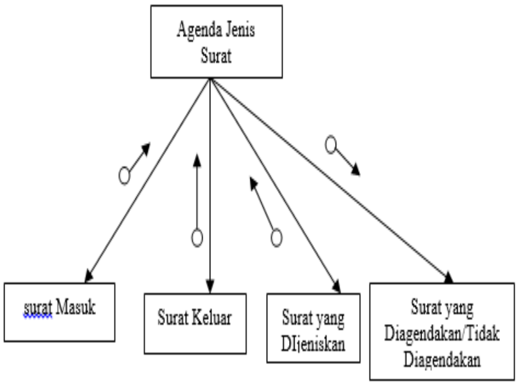
Gambar 9. Bagan Terstruktur Diagram Rinci 2.1



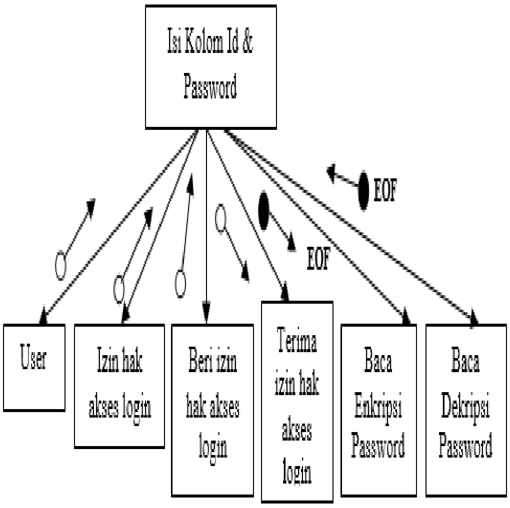
Gambar 10. Bagan Terstruktur Diagram Rinci 2.2



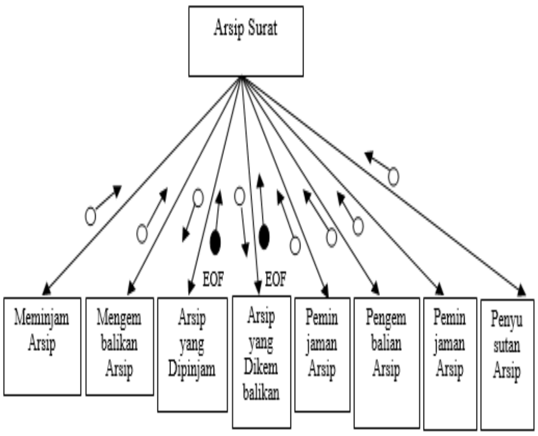
Gambar 11. Bagan Terstruktur Diagram Rinci 3.1



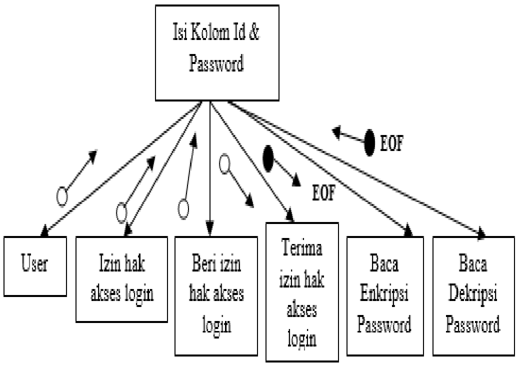
Gambar 12. Bagan Terstruktur Diagram Rinci 3.2



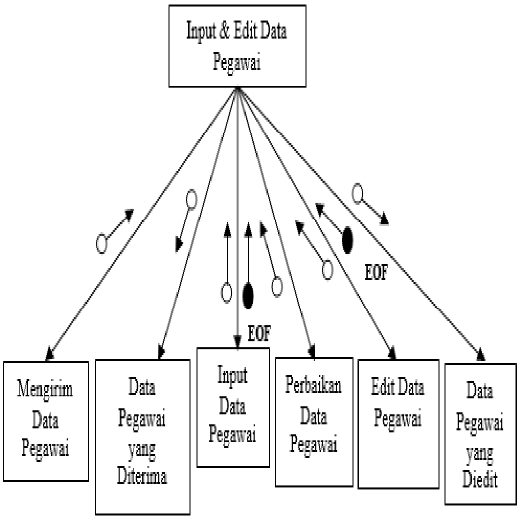
Gambar 13. Bagan Terstruktur Diagram Rinci 4.1



Gambar 14. Bagan Terstruktur Diagram Rinci 4.2



Gambar 15. Bagan Terstruktur Diagram Rinci 5.1



Gambar 16. Bagan Terstruktur Diagram Rinci 5.2

Rancangan Tampilan Layar, Rancangan Tampilan *Form* Masukan Data, dan Rancangan Tampilan *Form* Keluaran

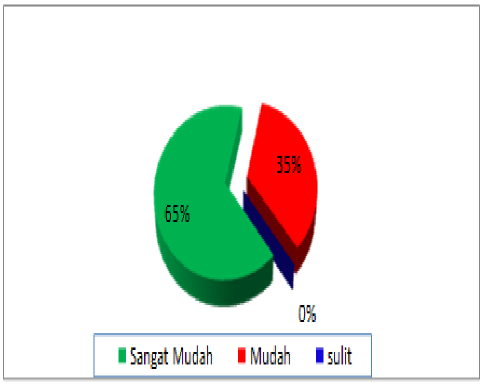
Rancangan antar muka atau dialog layar merupakan rancang bangun percakapan antara pemakai dengan komputer yang terdiri dari proses memasukkan data ke sistem kemudian menampilkan kembali output informasi kepada user.

Pembahasan

Sistem yang dibuat oleh penulis sudah diujicobakan di Lembaga Sandi Negara dengan beberapa karyawan yang bekerja di Bagian Tata Usaha pada bulan maret 2012.

Berdasarkan hasil uji coba tentang kemudahan mengakses informasi diperoleh data sebagai berikut: 65% responden menjawab sangat mudah, 35% responden menjawab mudah dan responden tidak ada yang menjawab sulit. Dari hasil uji coba yang telah dilakukan di komputer dapat dikemukakan bahwa:

1. Gambar yang ditampilkan dapat dimodifikasi setiap saat**.**
2. Data yang ditampilkan dapat dimodifikasi setiap saat dengan *notepad*
3. Aplikasi menampilkan tentang hal-hal yang mengenai berbagai macam kerusakan.



Gambar 17. Grafik Hasil Uji Coba

Kelebihan sistem
Kelebihan dari sistem ini, *software* yang digunakan *free* atau gratis, sistem oprasinya dapat digunakan dimanapun dan kapanpun untuk diakses. Serta *user* dapat mengetahui secara dini tentang kerusakan yang terjadi dan sebagai rekomendasi apabila hendak menanganinya.

Kelemahan sistem
Keamanan untuk *enkripsi* data masih kurang baik karena sistem *enkripsi* data masih menggunakan *md5* pada *MYSQL*.

PENUTUP

Simpulan

Berdasarkan hasil pengolahan data serta analisis yang telah dilakukan, maka dapat diperoleh beberapa kesimpulan sebagai berikut:

1. Dengan pengenkripsian *database* pada sebuah program dapat membantu pengamanan program dari pengguna yang tidak bertanggung jawab.
2. Meningkatkan kinerja pegawai khususnya bagian Tata Usaha agar pegawai lebih dapat efisiensi dan efektif dalam aktivitas yang dilakukannya.
3. Penggunaan teknologi komputerisasi dengan kriptografi *security* sistem proses pelayanan semakin meningkat.

Saran

Adapun saran-saran yang penulis kemukakan adalah sebagai berikut:

1. Agar dalam pengajaran mata kuliah kriptografi dan *security* dapat dianjurkan tentang implementasi dari kriptografi tersebut.
2. Apikasi enkripsi yang penulis kerjakan kiranya dapat dikembangkan kedalam bentuk pengamanan yang lebih baik lagi.

UCAPAN TERIMA KASIH

Puji syukur atas Kehadirat Tuhan Yang Maha Esa, atas rahmatnya penelitian ini dapat terlaksana dengan baik. Penulis juga ucapkan terima kasih yang sebesar-besarnya kepada para staf Lembaga Sandi Negara dan LP2M Universitas Indraprasta PGRI yang memberikan kesempatan penulis untuk menjalankan penelitian ini. Semoga Tuhan Yang Maha Esa membalas semua amalan baik kalian semua.

DAFTAR PUSTAKA

Charles P. Pfleeger. 1993. **Computer Basic Data**. Erlangga, Jakarta.

Demarco dan Gene Sarson. 1979. **Metodologi Struktur Analis dan Sistem Informasi.** PT. Gramedia, Jakarta.

Icove, David. 1993. **Sistem Keamanan Komputer**. PT. Gramedia, Jakarta.

Ir. Betha Sidik. 2001. **Pemograman Web dengan PHP.** Andi Yogyakarta, Yogyakarta.

Ir. MT. Bambang Hariyanto. **Perangkat Lunak Web Server.** Informatika, Bandung.

J. S. Badudu dan Sutan Mohammad Zain, 1996. **Strategi dan Pengelolaan Basis Data**. Erlangga, Jakarta.

Kadir, Abdul. 2001. **Dasar-Dasar Pemograman Web Dinamis Menggunakan PHP**. Andi Yogyakarta, Yogyakarta, 2001.

Gustiono, Booby. 2006. **Programmer Sejati PHP**. Solusi Media, Jakarta.

Peranginangain, Kasiman. 2006. **Aplikasi Web dengan PHP dan MySQL**. Andi.: Yogyakarta.

Rahmani. 2003. **Keamanan Sistem Kriptografi**. PT. Gramedia, Jakarta.

Riyanto, S. Kom., 2006. **Desain dan Implementasi Sistem Informasi. Erlangga**, Jakarta.

R. Munir. 2004. **Enkripsi Menggunakan Teknik Kriptografi.** Erlangga, Jakarta.

Sutabri, Tata S. Kom., 1998. **Sistem Informasi Manajemen Database Mysql server.** PT Gramedia, Jakarta.

Yahdi Kusnadi S. Kom dan Yasni Djamin S. Kom., 1998. **Pengenkripsian Basis Data dan Struktur Sistem Informasi**. PT. Gramedia, Jakarta.

Annisa Dini Handayani. 2009. **Tinjauan Matematis Fungsi *Well Pairing* pada Skema Enkripsi Berbasis Identitas (EBI).** Jurnal Sandi dan Keamanan Informasi.