BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada zaman teknologi informasi sekarang, data atau informasi merupakan suatu aset yang sangat berharga dan harus dilindungi. Hal ini juga diikuti oleh kemajuan teknologi komputer. Kemajuan teknologi komputer membantu semua aspek kehidupan manusia. Dari hal kecil sederhana sampai hal yang sangat rumit sekalipun bisa dikerjakan komputer. Keunggulan dari aplikasi komputer ini selain memberi kemudahan terhadap berbagai kegiatan pengolahan data dan informasi di berbagai bidang kehidupan, misalnya penggunaan komputer dalam bidang pemerintahan, organisasi social, militer, bank, pendidikan, transportasi, perdagangan, industri, dan lain sebagainya.

Dengan adanya kemajuan dalam teknologi informasi, komunikasi dan komputer maka kemudian muncul masalah baru, yaitu masalah keamanan data dan informasi dalam hal ini akan membuka peluang bagi orang-orang yang tidak bertanggung jawab untuk menggunakannya sebagai tindak kejahatan. Dan tentunya akan merugikan pihak tertentu.dalam kesempatan ini penulis akan mencoba menjelaskan berbagai macam ancaman keamanan data dan cara mengatasi ancaman tersebut.

Untuk menjaga keamanan dan kerahasiaan pesan, data, atau informasi dalam suatu jaringan komputer maka diperlukan suatu sistem keamanan data yang salah satu caranya dengan enkripsi guna membuat pesan, data, atau informasi agar tidak dapat dibaca atau dimengerti oleh sembarang orang, kecuali oleh penerima yang berhak. Pengamanan pesan, data, atau informasi tersebut selain bertujuan untuk meningkatkan keamanan, juga berfungsi untuk:

1. Mengamankan pesan, data, atau informasi agar tidak dapat dibaca oleh orang-orang yang tidak berhak agar kerahasian data suatu perushaan tetap terjamin kerahasiannya.
2. Mencegah agar orang-orang yang tidak berhak, menyisipkan atau menghapus pesan, data dan atau informasi. Salah satu hal yang penting

dalam komunikasi menggunakan komputer dan dalam jaringan komputer untuk menjamin kerahasiaan informasi tersebut maka harus membagun sistem keamanan data tersebut, salah satunya dengan cara enkripsi**.**

Jenis ancaman yang terjadi dalam keamanan data tersebut yaitu:

1. Kebocoran (Leakage) : pengambilan informasi oleh penerima yang tidak berhak
2. Tampering : pengubahan informasi yang tidak legal atau tanpa sepengetahuan dari pihak penerima.
3. Perusakan (Vandalism) : adalah gangguan dari sistem operasi tertentu dimana si perusak tidak mengharapkan keuntungan apapun dari perusakan tersebut.

Seperti pada RSUD Dr. H. Selamet Martodjo, sistem pengolahan data-nya masih sangat buruk, dimana data hanya tersimpan pada Microsoft Office Excel, Microsoft Office word dan Microsoft Office power poin Komputer tertentu yang loginnya telah di set username dan password.

Data yang disimpan di dalam suatu database yang dibangun dalam sistem informasi, data tersebut harus dijamin aman dari campur tangan dari pihak yang tidak diinginkan bahkan seorang adminpun tidak boleh merubah data tersebut, karena kemungkinan untuk di bajak oleh orang yang tidak berkepentingan dan pihak yang tidak memiliki wewenang sangatlah tinggi. Oleh karena itu, dalam aplikasi client-server terutama sistem informasi RSUD Dr. H. Selamet Martodjo keamanan datanya tidak boleh tergantung oleh satu orang misalkan administrator database server, tetapi puncak keamanan tertinggi dalam hal pengaman data terutama kerahasiaan data terletak pada nasabah atau anggota koperasi tersebut. Dengan demikian diperlukan suatu mekanisme sistem pengamanan data dengan menggunakan metodeAlgoritma Message Digest 5 (MD5).

Maka berdasarkan latar belakang yang ada, maka dibutuhkan sebuah aplikasi Sistem Pengaman Data dengan Menggunakan Metode MD5 pada Aplikasi Document berbasis client server untuk menghasilkan

data yang ter-enkripsi yang tersimpan dalam database sehingga data yang tersimpan lebih aman.

1.2 Rumusan Masalah.

Berdasarkan latar belakang yang telah di paparkan diatas, dapat di rumuskan permasalahan sebagai berikut :

1. Bagaimana membangun system keamanan data agar data tidak terganggu serta penerapan dalam sebuah ruang lingkup aplikasi Document ?
2. Bagaimana cara mengebangkan perlindungan data dengan menggunakan Algoritma MD5 ?
3. Bagaimana merancang dan mengimplmntasikan algoritma MD5 sebagai sebuah aplikasi untuk Enkripsi/Deskripsi document ?

1.3 Tujuan penulisan

Maksud dari penulisan Proposal Tugas Ahir ini adalah memberikan sebuah solusi awal untuk keamanan data dengan menggunakan metode kriptografi. Yang dapat memfasilitasi para karyawan dalam proses dan system yang akan mendukur dan menjaga system keamanan data di RSUD Dr. H. Selamet Martodjo.

1. Merancang system keamanan data yang mampu memberikan keamanan terhadap data dan informasi di RSUD Dr. H. Selamet Martodjo.
2. Sebagai implementasikan aplikasi yang telah di buat untuk kehidupan sehari hari di lingkungan RSUD Dr. H. Selamet Martodjo.
3. Aplikasi yang mudah dan bisa dipahami oleh masyarakat agar dapat dimanfaatkan oleh msyaraka.

1.4 Batasan Masalah.

Dalam penyusunan proposal ini dapat kita simpulkan beberapa batasan masalah yaitu :

1. Aplikasi ini hanya untuk proses kemanan data dengan enkripsi/deskripsi (Metode MD5).

2. Menggunakan metode MD5.
3. Prangkat lunak yang digunakan untuk implemntasi enkripsi/deskripsi adalah netbean 7.3 karana memiliki fitur yang
4. tidak di miliki netbeans versi lainnya serta selalu bisa competibel dengan beberapa hardware.

1.5 Metodologi Penelitian.

Langkah yang dilakukan dalam penelitian rancangan ini adalah :

a. Study Pustaka

   Identifikasi masalah dilakukan dengan cara strudi pustaka pada media perpustakaan maupun internet bisa menjadi sumber yang berkaitan dengan pembuatan aplikasi tersebut.

b. Perumusan Masalah

   Merumuskan masalah menjadi hak yang wajib agar mendapatkan pokok pembahasan serta menemukan jalan keluar permasalahan.

c. Studi Literature

   Diperlukan literatur yang berhubungan dengan sistem keamanan data mrelalui studi pustaka di perpustakaan maupun di kumpulan jurnal serta media internet.

d. Perancangan System

   Perancangan sistem yang akan dirancang harus sesuai dengan yang dibutuhkan, proses, interface hingga sistem managemen database.

e. Implementasi Program

   Pada tahapan ini merupakan tahapan implementasi dari hasil rancangan sistem.

f. Penulisan Laporan

   Pada tahap ini dilakukan penyusunan Laporan yang sudah dijelskan dalam landasan teori yang telah di tulis serta hasil penelitian berupa implementasi yang telah dibuat.

1.6 Sistematika Penulisan

Sistematika penulisan laporan tugas akhir yang disusun adalah sebagai berikut:

BAB I : PENDAHULUAN

Bab ini terdiri atas latar belakang, maksud dan tujuan dari penulisan tugas akhir, metodologi penelitian yang diterapkan, batasan masalah, serta sistematika penulisan tugas akhir ini.

BAB II : LANDASAN TEORI

Bab ini membahas mengenai beberapa teori dasar yang berhubungan dengan rancangan sistem yang dibuat seperti kriptografi secara umum, enkripsi, jaringan dan algoritma Algoritma MD5.

BAB III : PERANCANGAN SISTEM

Membahas mengenai rancangan dan alur algoritma sistem yang dibuat, disaign perangkat lunah meliputi desain proses, disain antar muka, dan disain data.

BAB IV : PERANCANGAN DAN IMPLEMENTASI

Bab ini membahas mengenai rancangan algoritma enkripsi dan dekripsi yang akan diimplementasikan dalam program serta bagaimana proses enkripsi dan dekripsi yang akan dilakukan oleh program.

BAB V : IMPLEMENTASI SISTEM

Bab ini akan dijelaskan mengenai implementasi pembuatan aplikasi berdasarkan hasil rancangan yang telah dibuat sebelumnya.

BAB VI : KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari tugas akhir ini dan saran-saran untuk pengembangan dan perbaikan dari tugas akhir ini.

BAB II

DASAR TEORI

2.1 Kriptografi

Ilmu kriptografi adalah ilmu yang mempelajari tentang penyembunyian huruf atau tulisan sehingga membuat tulisan tersebut tidak dapat dibaca oleh orang yang tidak berkepentingan. Kriptografi mempunyai dua bagian yang penting, yaitu enkripsi dan dekripsi. Enkripsi adalah proses dari penyandian pesan asli menjadi pesan yang tidak dapat diartikan seperti aslinya. Dekripsi sendiri berarti merubah pesan yang sudah disandikan menjadi pesan aslinya. Pesan asli biasanya disebut plaintext, sedangkan pesan yang sudah disandikan disebut ciphertext .

Kriptografi (cryptography) berasal dari bahasa Yunani ”cryptos” artinya ”secret” (rahasia), sedangkan ”graphein” artinya ”writing” (tulisan). Jadi kriptografi berarti ”secret writing” (tulisan rahasia).

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (Bruce Schneier, 1996). Dalam kriptografi sering ditemukan istilah atau terminologi, seperti pesan (message) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah plainteks (plaintext) atau teks jelas (cleartext). Pesan dapat berupa data atau informasi yang dikirim (melalui kurir, saluran telekomunikasi, dsb) atau yang disimpan di dalam media perekaman (kertas, storage, dsb). Pesan yang tersimpan tidak hanya berupa teks, tetapi dapat berbentuk citra (image), suara (audio), dan video, atau berkas biner lainnya.

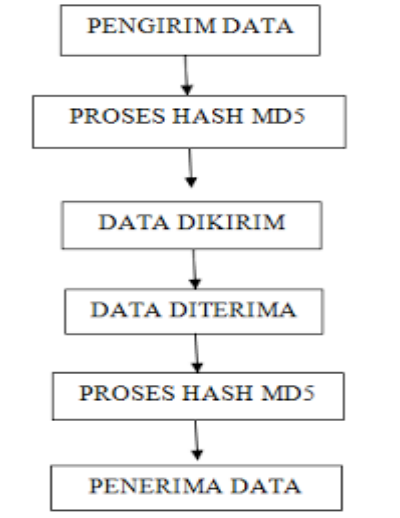
Supaya pesan tidak dapat dimengerti maknanya oleh pihak lain, maka pesan perlu disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk yang tersandi disebut ciphertext atau kriptogram yang harus bisa ditransformasikan kembali menjadi plainteks semula agar pesan yang diterima bisa dibaca. Gambar 1 memperlihatkan enkripsi dan dekripsi.

Gambar 2.1 Proses Enkripsi dan Deskripsi

2.2 Algoritma Kiptrografi MD5

MD5 adalah algoritma message digest yang dikembangkan oleh Ronald Rivest pada tahun 1991. MD5 mengambil pesan dengan panjang sembarang dan menghasilkan message digest 128 bit. Pada MD5 pesan diproses dalam blok 512 bit dengan empat round berbeda.

Message Digest 5 (MD5) ialah fungsi hash kriptografik yang digunakan secara luas dengan hash value 128-bit. Pada standart Internet (RFC 1321), MD5 telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan, dan MD5 juga umum digunakan untuk melakukan pengujian integritas sebuah file. MD5 adalah salah satu dari serangkaian algortima message digest yang didesain oleh Profesor Ronald Rivest dari MIT (Rivest, 1994). Saat kerja analitik menunjukkan bahwa pendahulu MD5-MD4- mulai tidak aman, MD5 kemudian didesain pada tahun 1991 sebagai pengganti dari MD4 (kelemahan MD4 ditemukan oleh Hans Dobbertin) [2]. Algoritma Metode MD5, setiap pesan yang akan di-enkripsi, terlebih dahulu dicari berapa banyak bit yang terdapat pada pesan, anggap sebanyak b bit. Di sinib adalah bit non negative integer, b bisa saja nol dan tidak harus selalu kelipatan delapan.



Gambar 2. 2 proses alur pengiriman data

Fungsi hash yang banyak digunakan dalam kriptografi MD5 dan SHA. Dalam artikel ini fungsi hash yang digunakan algoritma MD5. MD5 menerima masukan berupa pesan dengan ukuran sembarang dan menghasilkan message digest yang panjangnya 128 bit.

2.3 Enkripsi

Suatu proses dimana system yang metode untuk megubah suatu informasi sehingga tidak dapat dilihat tanpa membuka kunci pembukanya. Metode ini adalah metode paling efektif untuk menamankan data. Untuk membaca data yang telah di-encrip, dan kita harus mempunyai kunci untuk men-dekrip pesan atau data tersebut.

2.4 Fungsi Hash

Hash function atau fungsi hash adalah suatu cara menciptakan "fingerprint" dari berbagai data masukan. Hash function akan mengganti atau mentranspose-kan data tersebut untuk menciptakan fingerprint, yang biasa disebut hash value. Hash value biasanya digambarkan sebagai suatu string pendek yang terdiri atas huruf dan angka yang terlihat random (data biner yang ditulis dalam notasi heksadesimal). Suatu hash function adalah sebuah fungsi matematika, yang mengambil sebuah panjang variabel string input, yang disebut pre-image dan mengkonversikannya ke sebuah string output dengan panjang yang tetap dan biasanya lebih kecil, yang disebut message digest5. Hash function digunakan untuk melakukan fingerprint pada pre-image, yaitu menghasilkan sebuah nilai yang dapat menandai (mewakili) pre-image sesungguhnya. Fungsi hash satu arah (one-way hash function) adalah hash function yang bekerja satu arah, yaitu suatu hash function yang dengan mudah dapat menghitung hash value dari pre-image, tetapi sangat sukar untuk menghitung pre-image dari hash value. Sebuah fungsi hash satu arah, H(M), beroperasi pada suatu pre-image pesan M dengan panjang sembarang, dan mengembalikan nilai hash h yang memiliki panjang tetap. Dalam notasi matematika fungsi hash satu arah dapat ditulis sebagai:

h = H(M), dengan h memiliki panjang b

Ada banyak fungsi yang mampu menerima input dengan panjang sembarang dan menghasilkan output dengan panjang tetap, tetapi fungsi hash satu arah memiliki karakteristik tambahan yang membuatnya satu arah :

Diberikan M, mudah menghitung h.

Diberikan h, sulit menghitung M agar H(M) = h.

Diberikan M, sulit menemukan pesan lain, M', agar

H(M) = H(M').

Dalam dunia nyata, fungsi hash satu arah dikembangkan berdasarkan ide sebuah fungsi kompresi. Fungsi satu arah ini menghasilkan nilai hash berukuran n bila diberikan input berukuran b. Input untuk fungsi kompresi adalah suatu blok pesan dan hasil blok teks sebelumnya. Sehingga hash suatu blok M, adalah :

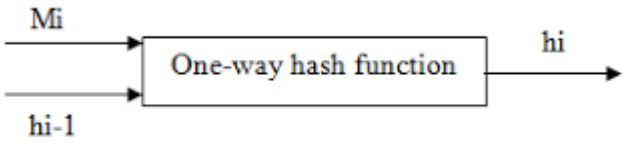
hi = f(Mi,hi-1)

dengan

hi = hash value saat ini.

Mi = blok pesan saat ini.

hi-1 = hash value blok teks sebelumnya.



Fungsi hash satu arah

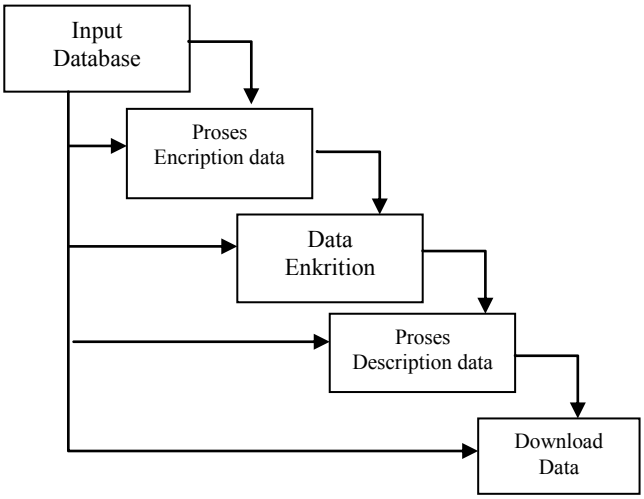
Gambar 2.3 Fungsi hash satu arah

Fungsi hash sangat berguna untuk menjaga integritas sebuah data. Sudah banyak algoritma hash function yang diciptakan, namun hash function yang umum digunakan saat ini adalah MD5 dan SHA (Secure Hash Algorithm). Algoritma hash function yang baik adalah yang menghasilkan sedikit hash collision.

BAB III

METODE PERANCANGAN SYSTEM

Metode pengembangan sistem dalam penelitian ini menggunakan metode Waterfall yang dipopulerkan oleh Summerville.

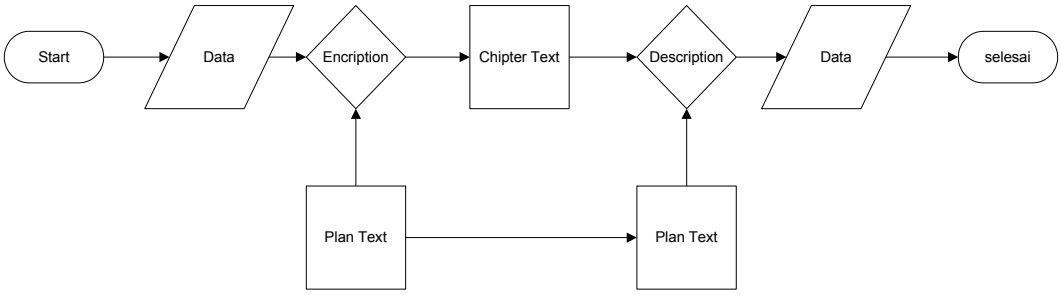


Gambar 1.4 Pemodelan waterfall

Tahap-tahap metode waterfall dapat dilihat pada Gambar 1.4. Setelah menentukan pengembangan sistem yang akan digunakan maka dilakukan perancangan sistem dengan menggunakan UML (Unified Modelling Language), meliputi use case, ctivity diagram, class diagram dan sequence diagram. Desain pada perancangan sistem dibuat flowchart sebagai analisis awal.

Pada sistem tersebut data yang akan di-input ke database, portal akan memberikan pilihan, true atau false. Jika true maka data melalui class private key yang kemudian data menjadi chipertext 1. kemudian yang selanjutnya akan diproses dalam class MD5 yang nantinya akan dihasilkan chipertext dua dan di-update tabel lalu disimpan dalam database. Data yang ada dalam database akan kembali dengan kondisi masih dalam terenkripsi dan membutuhkan proses dekripsi untuk menjadikan plaintext kembali dan kembali ke data awal. Jika false data yang di update tabel tidak melalui proses dekripsi. Portal on atau portal off

digunakan untuk membuktikan data yang tersimpan dalam database terenkripsi atau tidak.

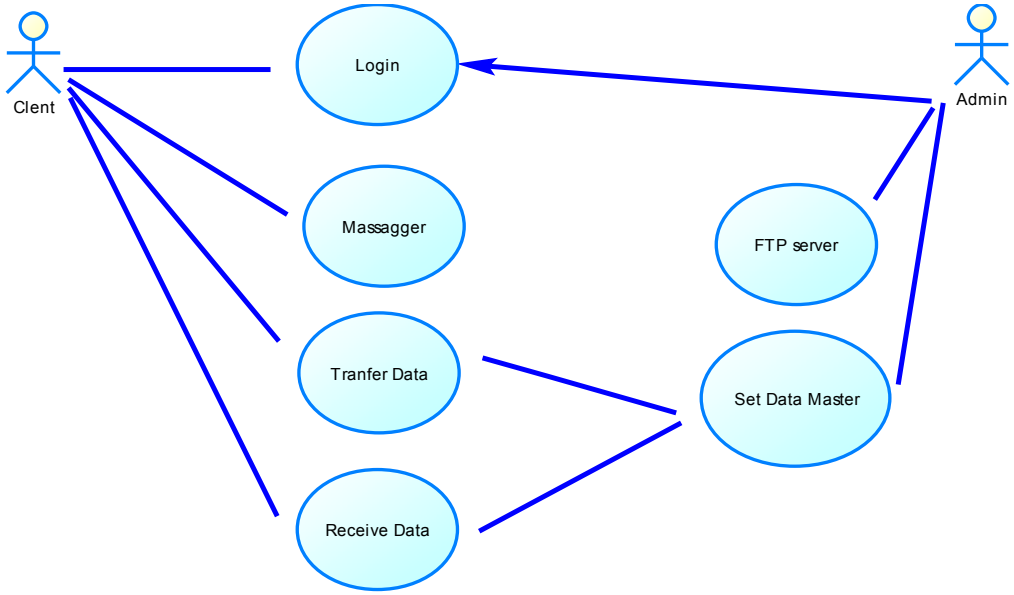


Gambar . 1.5 Encrip/Descript document dengan MD5

Pertama data yang masuk ditambah private key yang diperoleh dari class private key yang kemudian menghasilkan sebuah chipertext satu. Setelah itu chipertext satu diproses oleh enkripsi class MD5 yang akan diperoleh data chipertext dua.

3.1 Use Case

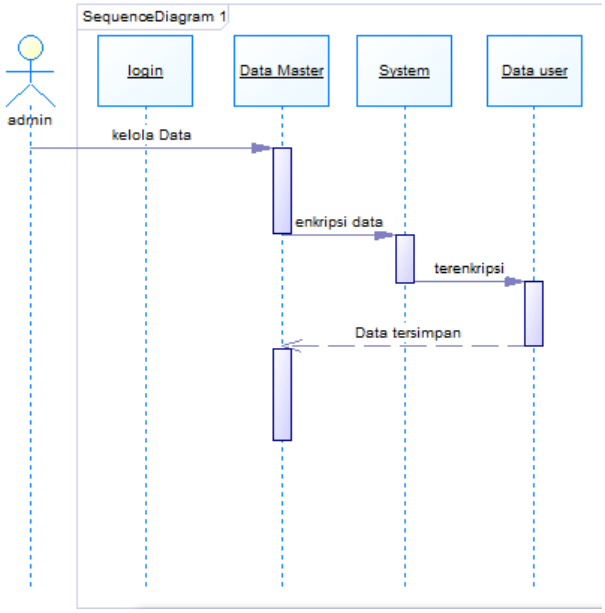
Use case adalah gambaran fungsionalitas dari suatu sistem, sehingga customer atau pengguna system paham dan mengerti mengenai kegunaan sistemyang akan dibangun [3].



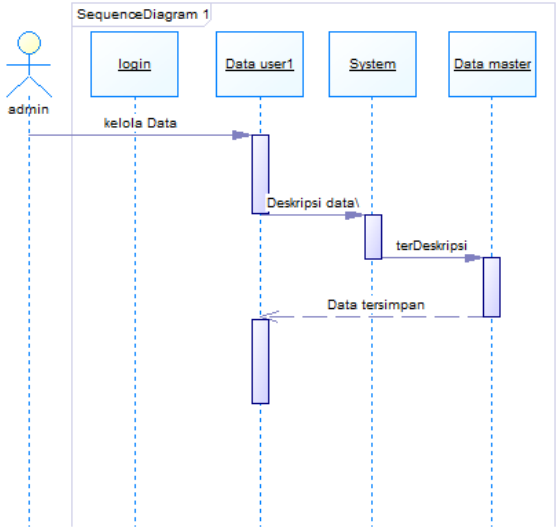
Gambar 2.1 Use Case Admin dan Client

3.2 Sequence Diagram

Sequence Diagram menejelaskan interaksi objek yang disusun dalam suatu urutan tertentu. Sequence diagram memperlihatkan tahap demi tahap apa yang seharusnya terjadi untuk menghasilkan sesuatu di dalam use case.



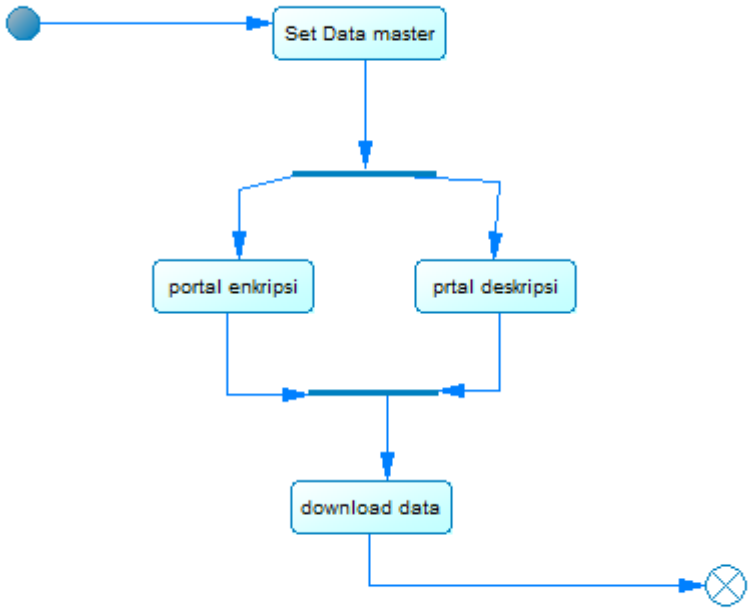
Gambar 2.3 Sequence Diagram enkripsi data



Gambar 2.4 Sequence Diagram deskripsi data

3.3 Activity Diagram

Activity diagram memodelkan alur kerja (workflow) sebuah proses bisnis dan urutan aktivitas dalam suatu proses. Diagram ini sangat mirip dengan sebuah flowchart karena kita dapat memodelkan sebuah alur kerja dari satu aktifias ke aktifitas lainnya atau dari satu aktifitas kedalam keadaan sesaat (state).



Gambar 3.4 Activity Diagram Admin

JADWAL KEGIATAN

Jadwal kegiatan merupakan jadwal waktunya (mulai dari persiapan, pengumpulan data, pengolahan data sampai dengan menyusun laporan) dalam penyusunan usulan Tugas Akhir ini.

No	Kegiatan	Bulan 1				Bulan 2				Bulan 3				Bulan 4			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Studi Literatur																
2	Perancangan Perangkat Lunak																
3	Pembuatan Program																
4	Uji Coba Perangkat Lunak																
5	Pembuatan Laporan hasil dan pengerjaan proyek Tugas Akhir																

DAFTAR PUSTAKA

1. Kurniawan, Yusuf, 2004. Kriptografi Keamanan Internet dan Jaringan Komunikasi, Bandung: Informatika.
2. Munir, R., 2006. Kriptografi, Bandung: Informatika.
3. Stalling, W., 1985. Data and Computer Communication, Fourth Edition, USA: Prentice Hall.
4. Sofwan, Aghus., Budi. Agung, Susanto. Toni, dkk. 2006. Aplikasi Kriptografidengan Algoritma Message Digest 5 (MD5). Jurnal Teknik Elektro.
5. Sadikin Rifki. 2003. Kriptografi untuk keamanan jaringan, Yogyakarta : Andi
6. Mukhtar Harun. 2007. Penerapan Kriptografy Untuk Keamanan Data . Junal Teknik Komputer