PERANCANGAN APLIKASI KEAMANAN DATA TENTANG UJIAN BERBASIS CAT DISEKOLAH AL-AZHAR MENGGUNAKAN METODE AES BERBASIS WEB

Disusun dan DiajukanUntukMemenuhiPersyaratanUjianAkhir
MemperolehGelarSarjanaKomputer Pada FakultasSains dan Teknologi
Universitas Pembangunan Panca Budi
Medan

SKRIPSI

OLEH:

NAMA	**: SAIDAH MARIAM**
NPM	**:1414370411**
PROGRAM STUDI	**: SISTEM KOMPUTER**

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCABUDI
MEDAN
2020

ABSTRAK

SAIDAH MARIAM

Perancangan Aplikasi Keamanan Data Tentang Ujian Berbasis CAT Disekolah AL-AZHAR Menggunakan Metode AES Berbasis Web

Tahun 2019

Dalam aktifitas belajar mengajar, sekolah belum sepenuhnya menerapkan sistem komputerisasi. Sehingga dalam melakukan proses belajar mengajar, membuat soal ujian, hasil ujian, data siswa membutuhkan waktu yang cukup lama dan terkadang hasilnya kurang akurat. Oleh karena itu dirancanglah suatu aplikasi berbasis web yang mampu untuk menyimpan data, menghapus data, mengubah data dan menampilkan data. Aplikasi ini mampu membantu mempermudah dan mempercepat proses pembuatan soal ujian dan memproleh hasil ujian siswa. Teknologi pengkodean komputer memggunakan PHP dan kontrol panel xampp, pemrograman basis data menggunakan MySQL. Hasil akhir dari penelitian ini adalah suatu aplikasi berbasis web yang mempermudah dan meningkatkan kinerja pada saat belajar mengajar.aplikasi ini berjalan pada lingkungan web agar mudah dioprasikan.

Kata kunci : PHP, MySQL, WEB, XAMPP

DAFTAR ISI

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan dunia teknologi saat ini mulai mempengaruhi segala lini kehidupan. Baik dalam bidang ekonomi, kesehatan, sosial, politik, bahkan pendidikan dalam skala kecil hingga besar. Manusia mulai dapat menerima perkembangan teknologi dengan baik, sehingga mendukung percepatan perkembangan teknologi dalam berbagai lini kehidupan.

Computer Assisted Test (CAT) merupakan salah satu metode seleksi atau sistem rekrutmen dengan alat bantu komputer untuk mendapatkan suatu standar minimal kompetensi dasar bagi siswa. Berdasarkan hasil evaluasi implementasi (*Computer Assisted Test*) CAT, manajemen memandang perlu dilakukan pengembangan (*Computer Assisted Test*) CAT dengan skala nasional dan memiliki aspek kepatuhan regulasi, kualitas perangkat lunak yang mengacu kepada standar internasional agar sistem pengembangan (*Computer Assisted Test*) CAT dapat dipercaya sebagai sebuah alat bantu yang handal dan layak digunakan untuk skala nasional (khusul Khotimah, 2016 : 54).

Dewasa ini ujian online dan *Computer Assisted Test* digunakan sebagai sarana evaluasi untuk mengukur pengetahuan dengan cara mengambil data peserta ujian yang memenuhi syarat dan menyimpan hasil ujian peserta dalam *Database* pusat.

Permasalahan dari aplikasi (*Computer Assisted Test*) CAT, salah satunya adalah kesulitan dalam *maintenace software,* serta perbaikan-perbaikan dibagian testing yang sesuai dengan kebutuhan peserta ujian. Berdasarkan masalah-masalah yang muncul inilah, maka penulis memberikan pemecahan masalah yang disarankan adalah dengan mengembangkan sistem aplikasi pengembangkan (*Computer Assisted Test*) CAT berbasis web dengan metode keamanan data dan *framework.Net*. Data adalah sifat rahasia tidak boleh data diubah – ubah karena itu menyangkut hasil ujian siswa yang sebenarnya oleh karena itu penulis ingin membuat suatu keamanan data dengan menggunakan metode AES sebagai pengamannya.

Dari permasalahan tersebut peneliti termotivasi dan mencoba memberikan pemecahan masalah yang dihadapi di MTS AL-AZHAR dengan merancang dan membangun aplikasi agar dapat mengamankan data dan menjaga kerahasiaan data soal ujian semester. Oleh karena itu, maka dalam penyusunan skripsi ini peneliti mengambil judul "**Perancangan Aplikasi Keamanan Data Tentang Ujian Berbasis CAT Di Sekolah AL-AZHAR Menggunakan Metode AES Berbasis WEB**". Dan teknik yang dapat digunakan adalah dengan menerapkan suatu metode kriptografi pada isi informasi. Kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut dengan melakukan pembangkitan kunci, enkripsi dan dekripsi. Kriptografi bertujuan untuk memberi layanan keamanan (yang juga dinamakan sebagai aspek-aspek keamanan). (Sholeh, et al, 2016 : 2). Dengan tersandikannya isi data dan informasi, maka seseorang yang berhasil mencuri data

dan informasi akan kesulitan untuk mengetahui isi dari data dan informasi dari Sekolah Al-Azhar.

1.2 Perumusan Masalah

Perumusan masalah yang terdapat pada penelitian ini yaitu :

1. Bagaimana merancang aplikasi keamanan Data Nilai Dan Soal ujian Sekolah Al-Azhar?
2. Bagaimana mengimplementasi aplikasi keamanan data dengan Algoritma AES?
3. Bagaimana merancang database aplikasi pengamanan Data Soal ujian?

1.3 Batasan Masalah

Agar pembahasan masalah tidak kemana-mana maka penulis membatasi masalah sebagai berikut :

1. Aplikasi hanya dapat berjalan pada sistem operasi berbasis *windows*.
2. Aplikasi pengamanan data ini menggunakan data tersembunyi yaitu Data Nilai dan Soal Semester.
3. Aplikasi ini hanya membahas masalah pengamanan data menggunakan Algoritma AES dengan bahasa pemrograman *PHP* dan menggunakan *Xampp*.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini yaitu :

1. Membangun sebuah aplikasi yang dapat mengamankan data soal ujian semester Pada MTS AL-AZHAR Medan.
2. Menerapkan metode Algoritma AES untuk pengamanan dan menjaga kerahasiaan data.
3. Menyajikan solusi keamanan data soal ujian.

1.5 Manfaat Penelitian

Manfaat penelitian ini yaitu :

1. Memudahkan pengerjaan data proses dalam membuat laporan Data Soal Semester.
2. Memudahkan *user* dalam melindungi data menjadi lebih aman dari pencurian.
3. Memudahkan *user* mengerjakan proses ujian akhir sekolah yang berlangsung secara online dalam penggunaan sistem aplikasi.

BAB II

LANDASAN TEORI

2.1 Penelitian Terdahulu

Bedasarkan penelitian yang dilakukan oleh Arisantoso, dkk (2017) mengenai Penerapan Aplikasi Pengamanan Data Dengan Metode *Enkripsi* Dan *Dekripsi* Algoritma AES Dalam Jaringan Lokal *Area*, Arisantoso, dkk menyimpulkan bahwa menerapkan aplikasi pengamanan data menggunakan bahasa pemrograman *Microsoft Visual Studio.Net*. Cara kerja pengenkripsian pada kirim dan terima data yaitu pengguna mengirimkan data melalui jaringan lokal *area* lalu penerima data menginstal, membuka *file* dengan hak aksesnya (*password*) dari pengirim. Cara mengembalikan data yang orisinal tanpa mengalami cacat yaitu dengan cara *dekripsi* artinya kapasitas *file* yang telah di*enkripsi* dan kapasitas *file* hasil *dekripsi* sama dengan *file* asli sebelum di*enkripsi*.

Bedasarkan penelitian yang dilakukan oleh Susanto, dkk (2016) mengenai Aplikasi *Enkripsi* Dan *Dekripsi* Untuk Keamanan Dokumen Menggunakan AES Dengan Memanfaatkan *field*, Susanto, dkk menyimpulkan bahwa untuk memudahkan penggunaan algoritma AES, maka dibuat suatu program algoritma AES dengan alat bantu *software* komputer yang dapat mengenkripsi dan mendekripsi data dan memanfaatkan *field* sebagai salah satu kunci dalam penggunaan aplikasi AES.

Bedasarkan penelitian yang dilakukan oleh Aulia, dkk (2016) mengenai Aplikasi *Enkripsi* Dan *Dekripsi* Menggunakan *Visual Basic* 2012 Dengan Algoritma AES, Aulia, dkk menyimpulkan bahwa untuk memudahkan penggunaan algoritma AES, maka dibuat suatu program algoritma AES dengan alat bantu *software* komputer, yaitu *android* yang dapat mengenkripsi data.

Bedasarkan penelitian yang dilakukan oleh Rahmat Tullah, dkk (2016) mengenai Metode Algoritma *Advanced Encryption Standard* (AES)dapat digunakan untuk membantu dalam proses pengamanan data dan Sistem pengiriman data dan penyimpanan data melalui media elektronik memerlukan suatu proses yang dapat menjamin keamanan dan keutuhan dari data yang dikirimkan tersebut. Data tersebut harus tetap rahasia selama pengiriman dan harus tetap utuh pada saat penerimaan di tujuan.

Bedasarkan penelitian yang dilakukan oleh Erwin Gunadhi, dkk (2015) mengenai Metode Algoritma *Advanced Encryption Standard* (AES)dapat digunakan untuk keamanan komunikasi data sms pada androiddan Sistem yang dapat memberikan pengamanan terhadap pertukaran informasi pada SMS berbasis android.

Bedasarkan penelitian yang dilakukan oleh Ana Kurniawati, dkk (2015) mengenai Metode Algoritma *Advanced Encryption Standard* (AES)dapat digunakan untuk enkripsi dan dekripsi pada dokumen teks danpengujian adalah dokumen teks jurnal – jurnal penelitian berbahasa Indonesia sebanyak 15 dokumen.

Bedasarkan penelitian yang dilakukan oleh Indra Suryanto, dkk (2017) mengenai Metode Algoritma *Advanced Encryption Standard* (AES)dapat digunakan untuk *chat messenger* dandapat berkomunikasi dengan aman tanpa takut pesan tersebut disadap atau dimanipulasi.

Bedasarkan penelitian yang dilakukan oleh Indra Saefudin, dkk (2017) mengenai Metode Algoritma *Advanced Encryption Standard* (AES)dapat digunakan untuk Enkripsi Pesan Teks danenkripsi pesan teks yang telah dibangun dapat berjalan pada ponsel dengan sistem operasi minimal gingerbread.

Bedasarkan penelitian yang dilakukan oleh Fricles Ariwisanto Sianturi (2016) mengenai Metode Algoritma *Advanced Encryption Standard* (AES)dapat digunakan untuk pengamanan data danTeknik yang dilakukan dalam pengamanan data teks ini yaitu dengan cara menerapkan metode AES kedalamnya yang bisa mengubah data teks asli ke dalam teks rahasia.

Bedasarkan penelitian yang dilakukan oleh Voni Yuniati,dkk(2015) mengenai Metode Algoritma *Advanced Encryption Standard* (AES)dapat digunakan untuk pengamanan datadokumen tek danTeknik yang dilakukan dalam pengamanan data tersebut harus tetap rahasia selama pengiriman dan harus tetap utuh pada saat penerimaan di tujuan

2.2.1. Perancangan

Berdasarkan penelitian yang di lakukan oleh Sandro (2014), perancangan adalah analisis sistem, persiapan untuk merancangan dan *implementasi* agar dapat menyelesaikan apa yang harus diselesaikan serta mengkonfigurasikan *komponen - komponen* perangkat lunak ke perangkat keras. Menurut (Adi Nugroho , 2014), menyatakan bahwa "Perancangan adalah *strategi* untuk memecahkan masalah dan mengembangkan solusi terbaik bagi permasalahan itu".

2.2.2 Aplikasi

Aplikasi merupakan rangkaian kegiatan atau perintah untuk dieksekusi oleh komputer atau suatu perangkat lunak komputer yang memanfaatkan kemampuan komputer langsung untuk melakukan suatu tugas yang diinginkan pengguna. Beberapa aplikasi yang digabung bersama menjadi suatu paket kadang disebut sebagai suatu paket atau *suite* aplikasi *(application suite)*.Aplikasi-aplikasi dalam suatu paket biasanya memiliki antar muka pengguna yang memiliki kesamaan sehingga memudahkan pengguna untuk mempelajari dan menggunakan tiap aplikasi. Seringkali, mereka memiliki kemampuan untuk saling berinteraksi satu sama lain sehingga menguntungkan pengguna. (Sitohang, 2013:2).

Aplikasi adalah penerapan dari rancang sistem untuk mengolah data yang menggunakan aturan atau ketentuan bahasa pemrograman tertentu. Aplikasi adalah Program yang dibuat oleh manusia yang berfungsi untuk menyelesaikan permasalahan-permasalahan masalah yang akan dihadapi. (Zulfauzi, 2015 : 57).

2.2.3 Kriptografi

Menurut(PatriciaHandoko,dkk2014)Kriptografi merupakan sebuah ilmu yang digunakan untuk menjaga kerahasiaan dari sebuah data, dengan menggunakan metode-metode tertentu sehingga data hanya dapat dibaca oleh orang yang berhak terhadap data tersebut. Dalam menjaga kerahasiaan data, kriptografi mengubah pesan asli (*plaintext*) menjadi pesan yang disandikan (*ciphertext*), proses ini disebut dengan enkripsi. Kemudian *ciphertext* inilah yang akan dikirim kepenerima, di pihak penerima, penerima mengubah kembali *ciphertext*menjadi *plaintext* agar pesan asli dapat dibaca kembali, proses ini disebut dengan dekripsi.

Kriptografi mempunya 4 tujuan umum yaitu;

1. Kerahasiaan

   Menjaga isi dari suatu pesan dari siapapun kecualikepada orang yang memiliki otoritas terhadap data yangdisandikan dalam bentuk kunci dekripsi.

2. Integritas Data

   Dalam kriptografi akan dilakukan prosespengecekan apakah data yang sampai di penerimamerupakan benar data yang pertama kali dikirim olehpengirim.

3. Autentikasi

   Pada proses autentikasi ini data akan dicek apakahmengalami manipulasi dalam isinya seperti penyisipan,penghapusan dan penggantian data.

4. Non-Repudiasi

   Jika seseorang sudah mengirimkan pesan, makaorang tersebut tidak dapat membantah/ menyangkalpengiriman pesan tersebut.

2.2.4 Pengamanan

Menjaga keamanan dan kerahasiaan data adalah hal yang sangat penting dan perlu adanya upaya keseriusan guna meningkatkan kesadaran keamanan informasi baik dilingkungan pemerintah, instansi dan organisasi.Salah satu teknik mengamankan data yaitu dengan teknik penyandian atau kriptografi. (Arisantoso,dkk 2017).

2.2.5 Ujian Semester

Ujian semester adalah suatu kegiatan yang dilkukan oleh Program Studi Pendidikan untuk mengetahui tingkat kemajuan belajar siswa dan merupakan proses penilaian hasil belajar siswa.

	ACAK	SOAL	JAWAB1	FILEJAWAB1	JAWAB2	FILEJAWAB2	JAWAB3	FILEJAWAB3	JAWAB4	FILEJAWAB4	JAWAB5
4		Suatu tahapan yang dilakukan untuk membangun sebuah database disebut	web database		database planning		data server		DBMS		router server
5		dibawah ini terdapat tahapan dalam membuat database, kecuali	menentukan nama database		membuat tabel yang dibutuhkan		menentukan letak tebel berdasarkan kebutuhan		menentukan item yang dibutuhkan		membuat server pada host sendiri
6		Software yang termasuk dalam pembuatan desain website, kecuali	Dreamweaver		Sublime text		notepad ++		Photoshop		Visual Studio
7		Dibawah ini terdapat nama tabal dalam pembuatan database perpustakan, kecuali	tabel user		tabel siswa		tabel RAK		tabel buku		tabel gaji

Gambar 2.1. Soal Semester

2.2.6 Algoritma AES

AES merupakan nama untuk *Federal Information Processing Standards Publication*197. AES menjelaskan mengenai algoritma kriptografi yang digunakan untuk melindungi data. Algoritma AES adalah sebuah *symmetric block cipher*yang dapat melakukan enkripsi dan dekripsi pada data. Algoritma AES dapat menggunakan kunci 128, 192 dan 256 *bit* untuk melakukan enkripsi dan dekripsi terhadap data dengan ukuran blok 128 *bit*.

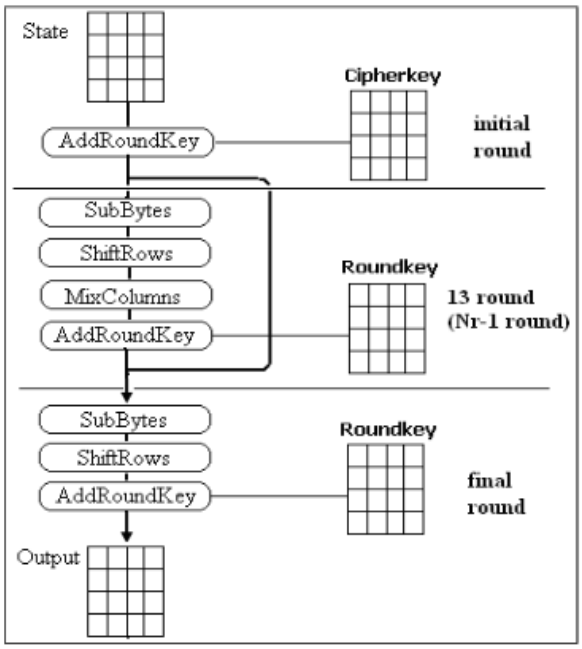
Metode AES256 merupakan salah satu metode kriptografi simetris yang mampu untuk mengenkripsi pesan sepanjang 16 karakter dengan menggunakan kunci sepanjang 32 karakter.Untuk meningkatkan keamanannya, maka kunci yang digunakan dapat dimasukkan ke dalam fungsi hash SHA1 sehingga nilai hash yang diperoleh yang digunakan sebagai kunci.

The Advanced Encryption Standard (AES) dengan metode Rijndael ini diperkenalkan oleh 2 orang kriptografer asal Belgia yaitu Joan Daemen dan Vincent Rijmen. Karena menggunakan kunci dengan ukuran 128, 192 atau 256 *bit* maka algoritma ini sering disebut dengan “AES-128”, “AES-192”, atau”AES-256” sesuai dengan kunci yang dipakai, sedangkanukuran blok yang digunakan adalah 128 *bit*.

2.2.7 Proses *Enkripsi* AES (*Advanced Enryption Standard*)

Proses enkripsi algoritma AES terdiri dari 4 jenis transformasi *bytes*, yaitu *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*. Pada awal proses enkripsi, *input* yang telah di *copy*kan ke dalam *State*akan mengalami transformasi

byteAddRoundKey. Setelah itu, *State* akan mengalami transformasi, *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES sebagai *roundfunction*. *Round* yang terakhir agak berbeda dengan *round-round* sebelumnya dimana pada *round* terakhir, state tidak mengalami transformasi *MixColumns*. Ilustrasi proses enkripsi AES dapat digambarkan seperti pada Gambar 2.3 di bawah ini (Voni Yuniati,dkk ;2014:24).



Gambar 2.2 Ilustrasi Proses Enkripsi AES
(Sumber :Voni Yuniati,dkk ;2014:24)

Pada proses enkripsi, algoritma AES menggunakan empat transformasi yang berbeda yaitu:

1. SubBytes()

Transformasi *SubBytes()* merupakan substitusi *byte* yang beroperasiterhadap setiap *byte* pada *State*dengan menggunakan tabel substitusi (*S-box*).Sebagai contoh, jika s1,1= {53} maka nilaisubstitusi diperoleh dari perpotongan antara baris “5” dengan kolom “3” pada *S-box* sehingga didapat hasilnya {ed}.

2. ShiftRows()

Transformasi *ShiftRows()* dilakukan pada 3 baris terakhir dengan melakukan geser (*shift*)memutar dengan nilai shiftyang berbeda–beda tergantung kepada barisnya. Baris pertama (r = 0) tidak dilakukan operasi *ShiftRows()*. Secara spesifik, proses transformasi *ShiftRows()* adalah s‟r,c= sr, (c + shift(r,Nb)) mod Nb ; untuk0 < r < 4 dan 0 ≤ c < Nbdimana nilai shift(r,Nb) tergantung pada nomor baris, untuk Nb=4 maka :shift(1,4) = 1; shift(2,4) = 2; shift(3,4) = 3

3. MixColumns()

Transformasi *MixColumns()* dioperasikan pada *State*secara kolom per kolom, masing–masing kolom dikalikan dengan matrik yang sudah ditentukan

4. AddRoundKey()

Pada transformasi *AddRoundKey()*, sebuah subkunciditambahkan pada *State*dengan operasi XOR. Setiap subkunci terdiri dari Nb*word* dari himpunan subkunci. Subkunci ditambahkan dengan *State* dengan cara [s‟0,c, s‟1,c, s‟2,c, s‟3,c] = [s0,c, s1,c, s2,c, s3,c] ⊕[w_{round}*Nb+c] ;untuk 0 c<Nb[wi] adalah *word* dari *key* yang bersesuaian dimana i = round*Nb+c. Transformasi*AddRoundKey* pada proses enkripsi pertama kali pada *round* = 0 untuk *round* selanjutnya *round*= *round* + 1, pada proses dekripsi pertama kali pada *round* = 14 untuk *round* selanjutnya *round* =*round* – 1 (Voni Yuniati,dkk ;2014:24).

Pada permulaan enkripsi, *input* yang berupa *plaintext*dimasukkan ke dalam *State*, pada initial *round*dilakukan transformasi AddRoundKey(State, SubKunci(0)), setelah initial *round*proses menuju pada *round function*sebanyak Nr-1 putaran (1 ≤ *round*< Nr),dimana di dalam *round function* ini dilakukan

transformasi berturut –turut yaitu *SubBytes()*, *ShiftRows()*, *MixColumns()*, dan *AddRoundKey()*. Setelah itu proses akan menuju pada putaran terakhir (*final round*) dimana pada putaran terakhir ini dilakukan transformasi *SubBytes()*, *ShiftRows()* dan *AddRoundKey()*, pada putaran terakhir ini setelah transformasi *AddRoundKey()* maka akan menghasilkan *final State*yang merupakan *output* yang disebut *ciphertext.*(Voni Yuniati,dkk ;2014:25).

2.2.8 Proses *Enkripsi* dan *Dekripsi*

Proses enkripsi adalah suatu proses yang mengubah plainteks (kode sesungguhnya) menjadi ciperteks (kode rahasia). Untuk merubah plainteks ke ciperteks digunakan fungsi matematika dan kunci (Santomo, 2016). (Santomo,2016) menyatakan bahwan Proses dekripsi adalah suatu proses yang mengubah ciperteks menjadi plainteks, dimana pesan yang sudah teracak dikembalikan ke pesan semula yang juga menggunakan fungsi matematika dan kunci. Sebelum proses (proses enkripsi maupun dekripsi) dilakukan, ada satu pengaman awal yaitu menentukan kunci sandi kunci pengaman (*key pairs*) yang terdiri dari *private key*, *public key* dan *modulo* yang digunakan untuk membuka dan mengunci *system*. Setelah *system* dapat dibuka dengan kunci pengaman, proses enkripsi maupun dekripsi dapat dilakukan, baik dilakukan dengan proses enkripsi dan enkripsi sekali saja maupun proses enkripsi dan dekripsi yang dilakukan berkali-kali agar semakin terjamin kerahasiaannnya.

Salah satu contoh soal Enkripsi dan Deskipsi

- Pesan : BUDIDARM A
- Kunci : ABCDEFGH I

Maka langkah-langkahnya seperti di bawah ini :

Tabel 2.1 Tabel Alfabert

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

- Plainteks 1(B) 20(U) 3(D) 8(I) 3(D) 0(A) 17(R) 12(M) 0(A)
- Kunci 0(A) 1(B) 2(C) 3(D) 4(E) 5(F) 6(G) 7(H) 8(I)
- ---------- +
- Hasil mod 26 1 21 5 11 7 5 23 19 8
- Chiperteks B V F L H F X T I

Jadi Chiperteks yang di hasilkan yaitu : BVFLHFXTI

Deskripsi pesan, perhatikan langkah di bawah ini :

- Chiperteks 1(B) 21(V) 5(F) 11(L) 7(H) 5(F) 23(X) 19(T) 8(I)
- Kunci 0(A) 1(B) 2(C) 3(D) 4(E) 5(F) 6(G) 7(H) 8(I)
- ---------- -
- Hasil mod 26 1 20 3 8 3 0 17 12 0
- Plainteks B U D I D A R M A

Jadi Plainteks yaitu : BUDIDARM A

2.2.9 Pengenalan *Database* dan PHP

Database merupakan kumpulan *file* yang saling berhubungan. Akan tetapi *database* tidak hanya kumpulan *file*. *Record* di dalam tiap *file* harus dapat dihubungkan dengan *record* di dalam *file* lain.

Dalam manajemen *database* relational terdapat komponen utama dalam konsep *database* :

1. *Field* adalah unit terkecil data yang disimpan dalam *database*. Unit terkecil data yang disimpan dalam *database*.
   a. *Primary key* yaitu *field* yang unik dan mengidentifikasi satu *record*. Contoh *customer number* dan *order number*.
   b. *Secondary key* yaitu *field* yang mengidentifikasi sebuah *record* atau bagian dari beberapa *record* yang terkait.
   c. *Foreign key* yaitu field yang menunjuk beberapa *record* pada *file* lain. Contoh *Order Record* berisi *foreign key customer number*.
   d. *Descriptive field* yaitu non *keyfield*.
2. *Record* adalah kumpulan *field* yang diatur dalam format yang predermined (telah ditentukan).
   a. Fixed length record structures

   Sebagian besar teknologi *database* memaksakan struktur *record fixedlength*, dalam artian setiap *instancerecord* mempunyai *field* yang sama, jumlah *field* yang sama, dan ukuran logika yang sama. Akan tetapi beberapa sistem *database*akan mengkompresi *field-field* dan nilai-nilai yang tidak digunakan untuk menghemat ruang penyimpanan disk.

b. *Variable length record structured*

Memperoleh *record-record* pada *file* yang sama memiliki *length* yang berbeda.

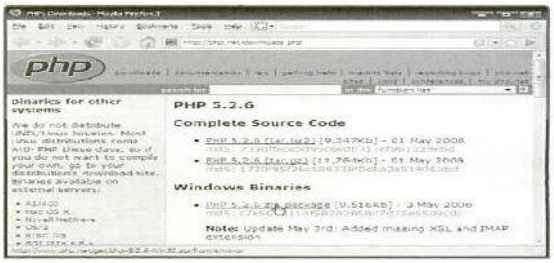
3. *Field* dan Tabel

File adalah kumpulan semua kejadian dari struktur record yang ditentukan. Tipe-tipe dari *file*yaitu :

a. File induk / master adalah *file* penting dalam sistem dan akan tetap ada selama siklus hidup sistem informasi berputar.
b. *File* transaksi adalah *file* yang digunakan untuk merekam data dari suatu transaksi yang terjadi.
c. *File* laporan adalah *file* yang berisi sistem informasi yang akan ditampilkan.
d. *File* sejarah adalah *file* yang berisi data masa lalu yang sudah tidak aktif lagi.
e. *File pelindung adalah salinan dari file*-file yang masih aktif di *database* pada saat tertentu yang digunakan bila *filedatabase* rusak.
f. *File* kerja adalah suatu proses program secara sementara karena memori komputer tidak mencukupi

Kelebihan PHP yang paling terasa adalah tersedianya PHP parser di banyak platform. Anda bisa menjalankan skrip PHP di banyak *server*, seperti Apache dan IIS dan di banyak sistem operasi.

Untuk melihat halaman download PHP dapat dilihat pada Gambar 2.1.



Gambar 2.3 Halaman PHP
(Sumber : Ali Zaki ; 2013 : 32)

2.2.10 *Database*

Database adalah sekumpulan data mentah yang disusun menurut logika tertentu dan terorganisasi dalam bentuk yang dapat disimpan dan diproses oleh komputer. Contoh *database* dapat berisi data pegawai, data penjualan, pmbayaran dan lain-lain. Data internail dari akunting, keuangan, penjualan dan bidang-bidang bisnis lainnya yang disimpan dalan suatu komputer dan disusun mnurut logika tertentu deisbut dengan *internal database*. Database seringkali disimpan dalam suatu perangkat tertntu pada komputer, seperti *hard disk*, *compacct disk*, dan sebagainya. Hubungan antar sistem *database* dan sistem *software* sangat kuat karena sistm *database* yang dipakai sangat menentukan kmudahan aksesnya data sementara *software* sendiri memunkinkan peneliti memanipulasi data untuk dianalisis. (Dermawan Wibisono : 2012).

2.2.11 Mengenal MySQL

MySQL merupakan *database server open source* yang cukup populer keberadaannya. Dengan berbagai keunggulan yang dimiliki, membuat software database ini banyak digunakan oleh para praktisi untuk membangun suatu project. Adanya fasilitas API (*Application Programming Interface*) yang dimiliki oleh MySQL, memungkinkan bermacam-macam aplikasi komputer yang ditulis dengan berbagai bahasa pemrogramman dapat mengakses basis data MySQL (Wahana Komputer ; 2010 : 2)

2.2.12 *Unified Modeling Language* (UML)

Menurut Windu Gata (2013) Hasil pemodelan pada OOAD terdokumentasikan dalam bentuk *Unified Modeling Language* (UML). UML adalah bahasa spesifikasi standar yang dipergunakan untuk mendokumentasikan, men*spesifikasi*kan dan membangun perangkat lunak.

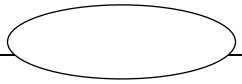
UML merupakan metodologi dalam mengembangkan sistem ber*orientasi* objek dan juga merupakan alat untuk mendukung pengembangan sistem. UML saat ini sangat banyak dipergunakan dalam dunia industri yang merupakan standar bahasa pemodelan umum dalam industri perangkat lunak dan pengembangan sistem. (Urva dan Siregar, 2015 : 93).Alat bantu yang digunakan dalam perancangan ber*orientasi* objek berbasiskan UML adalah sebagai berikut:

1. *Use Case* Diagram

Use case diagram merupakan pemodelan untuk kelakukan (*behavior*) sistem informasi yang akan dibuat. *Use case* mendeskripsikan sebuah interaksi antara

satu atau lebih aktor dengan sistem informasi yang akan dibuat. Dapat dikatakan *use case* digunakan untuk mengetahui fungsi apa saja yang ada di dalam sistem informasi dan siapa saja yang berhak menggunakan fungsi-fungsi tersebut. Simbol-simbol yang digunakan dalam *use case* diagram dapat dilihat pada tabel 2.1 dibawah ini.

Tabel 2.2. Simbol *Use Case*

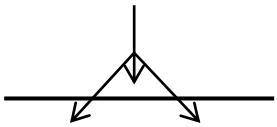
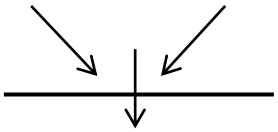
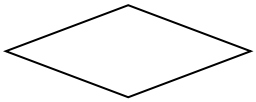
Gambar	Keterangan
	*Use case* menggambarkan fungsionalitas yang disediakan sistem sebagai unit-unit yang bertukar pesan antar unit dengan aktor, dan dinyatakan dengan menggunakan kata kerja di awal nama *use case*.
	Aktor adalah *abstraction* dari orang atau sistem yang lain yang mengaktifkan fungsi dari target sistem. Untuk mengidentifikasikan aktor, harus ditentukan pembagian tenaga kerja dan tugas-tugas yang berkaitan dengan peran pada konteks target sistem. Orang atau sistem bisa muncul dalam beberapa peran. Perlu dicatat bahwa aktor berinteraksi dengan *use case*, tetapi tidak memiliki *control* terhadap *use case*.
	Asosiasi antara aktor dan *use case*, digambarkan dengan garis tanpa panah yang mengindikasikan siapa atau apa yang meminta interaksi secara langsung dan bukannya mengidikasikan aliran data.
	Asosiasi antara aktor dan *use case* yang menggunakan panah terbuka untuk mengidinkasikan bila aktor berinteraksi secara pasif dengan sistem.
	Include, merupakan di dalam *use case* lain (*required*) atau pemanggilan *use case* oleh *use case* lain.
	Extend, merupakan perluasan dari *use case* lain jika kondisi atau syarat terpenuhi.

(Sumber : Urva dan Siregar, 2015 : 94)

2. Diagram Aktivitas (*Activity Diagram*)

Activity Diagram menggambarkan *workflow* (aliran kerja) atau aktivitas dari sebuah sistem atau proses bisnis. Simbol-simbol yang digunakan dalam *activity diagram* dapat dilihat pada tabel 2.2 dibawah ini:

Tabel 2.3. Simbol *Activity Diagram*

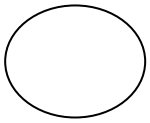
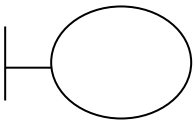
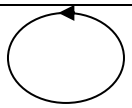
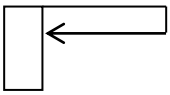
Gambar	**Keterangan**
	*Start point*, diletakkan pada pojok kiri atas dan merupakan awal aktifitas.
	*End point*, akhir aktifitas.
	*Activites*, menggambarkan suatu proses/kegiatan bisnis.
	*Fork* (Percabangan), digunakan untuk menunjukkan kegiatan yang dilakukan secara parallel atau untuk menggabungkan dua kegiatan pararel menjadi satu.
	*Join* (penggabungan) atau rake, digunakan untuk menunjukkan adanya dekomposisi.
	*Decision Points*, menggambarkan pilihan untuk pengambilan keputusan, *true*, *false.*
	*Swimlane*, pembagian activity diagram untuk menunjukkan siapa melakukan apa.

(Sumber : Urva dan Siregar, 2015 : 94)

3. Diagram Urutan (*Sequence Diagram*)

Sequence diagram menggambarkan kelakuan objek pada *use case* dengan mendeskripsikan waktu hidup objek dan pesan yang dikirimkan dan diterima antar objek. Simbol-simbol yang digunakan dalam *sequence diagram* dapat dilihat pada table dibawah ini.

Tabel 2.4. Simbol *Sequence Diagram*

Gambar	**Keterangan**
	*EntityClass*, merupakan bagian dari sistem yang berisi kumpulan kelas berupa entitas-entitas yang membentuk gambaran awal sistem dan menjadi landasan untuk menyusun basis data.
	*Boundary Class*, berisi kumpulan kelas yang menjadi *interface* atau interaksi antara satu atau lebih aktor dengan sistem, seperti tampilan formentry dan *form* cetak.
	*Control class*, suatu objek yang berisi logika aplikasi yang tidak memiliki tanggung jawab kepada entitas, contohnya adalah kalkulasi dan aturan bisnis yang melibatkan berbagai objek.
	*Message*, simbol mengirim pesan antar *class*.
	*Recursive*, menggambarkan pengiriman pesan yang dikirim untuk dirinya sendiri.
	*Activation, activation* mewakili sebuah eksekusi operasi dari objek, panjang kotak ini berbanding lurus dengan durasi aktivitas sebuah operasi.
	Lifeline, garis titik-titik yang terhubung dengan objek, sepanjang *lifeline* terdapat *activation*.

(Sumber : Urva dan Siregar, 2015 : 95)

4. *Class Diagram* (Diagram Kelas)

Merupakan hubungan antar kelas dan penjelasan detail tiap-tiap kelas di dalam model desain dari suatu sistem, juga memperlihatkan aturan-aturan dan tanggng jawab entitas yang menentukan perilaku sistem.*Class diagram* juga menunjukkan atribut-atribut dan operasi-operasi dari sebuah kelas dan *constraint* yang berhubungan dengan objek yang dikoneksikan. *Class diagram* secara khas meliputi: Kelas (*Class*), Relasi, *Associations*, *Generalization* dan *Aggregation*, Atribut (*Attributes*), Operasi (*Operations/Method*), *Visibility*, tingkat akses objek *eksternal* kepada suatu operasi atau atribut. Hubungan antar kelas mempunyai keterangan yang disebut dengan *multiplicity* atau kardinaliti yang dapat dilihat pada tabel 2.4 dibawah ini:

Tabel 2.5. *Multiplicity Class Diagram*

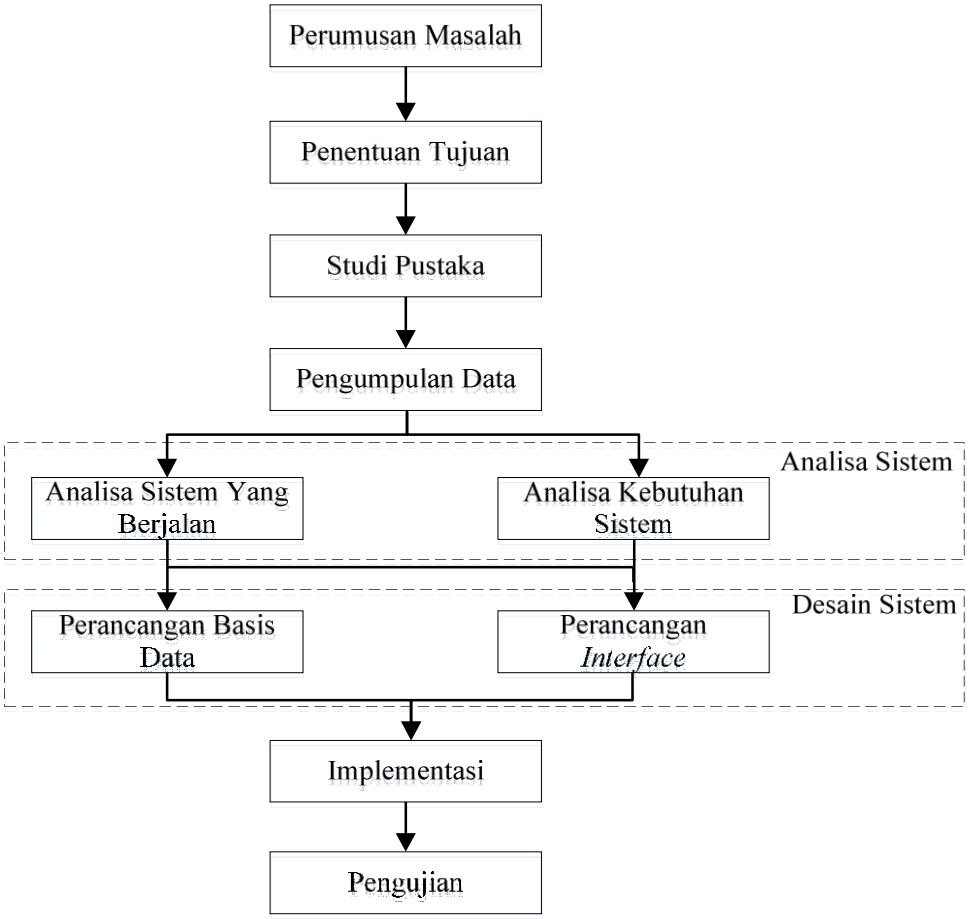
Multiplicity	**Penjelasan**
1	Satu dan hanya satu
0..*	Boleh tidak ada atau 1 atau lebih
1..*	1 atau lebih
0..1	Boleh tidak ada, maksimal 1
n..n	Batasan antara. Contoh 2..4 mempunyai arti minimal 2 maksimum 4

(Sumber : Urva dan Siregar, 2015 : 95)

BAB III

METODE PENELITIAN

3.1. Tahapan Penelitian



Gambar 3.1 Flowhart Tahapan Penelitian

3.2. Metode Pengumpulan Data

Metode pengumpulan data yang diperlukan dalam penelitian ini dilakukan dengan pendekatan sebagai berikut :

a. Wawancara Adalah komunikasi atau pembicaraan dua arah yang dilakukan oleh peneliti dan petugas statistik guna untuk mendapatkan data yang kongkret dan relevan.
b. Studi dokumentasi yaitu mempelajari data-data yang ada dalam perusahaan dan berhubungan dengan penelitian ini.

3.3. Analisis Sistem Berjalan

Analisis sistem merupakan gambaran tentang sistem yang saat ini sedang berjalan di sekolah MTS AL-AZHAR Medan permasalahan yang dihadapai oleh sekolah MTS AL-AZHAR adalah Dalam ujian semester yang sudah Berbasis Komputer disebut juga *Computer Assisted Test* (CAT) adalah sistem pelaksanaan ujian semester dengan menggunakan komputer sebagai media ujiannya. Dalam pelaksanaanya, CAT berbeda dengan sistem ujian berbasis kertas atau Paper Based Test(PBT) yang selama ini sudah berjalan. Dalam hal ini adapun permasalahan yang terjadi di MTS AL-AZHAR adalah dalam menyiapkan data soal ujian semseter yang bersifat rahasia masih belum dapat menyimpan secara aman atau dapat mencadangkan file penting yang ada dalam data soal semester dikarenakan file hanya di simpan pada folder komputer biasa sehingga sering terjadi pencurian data soal ujian dan jawaban ujian.

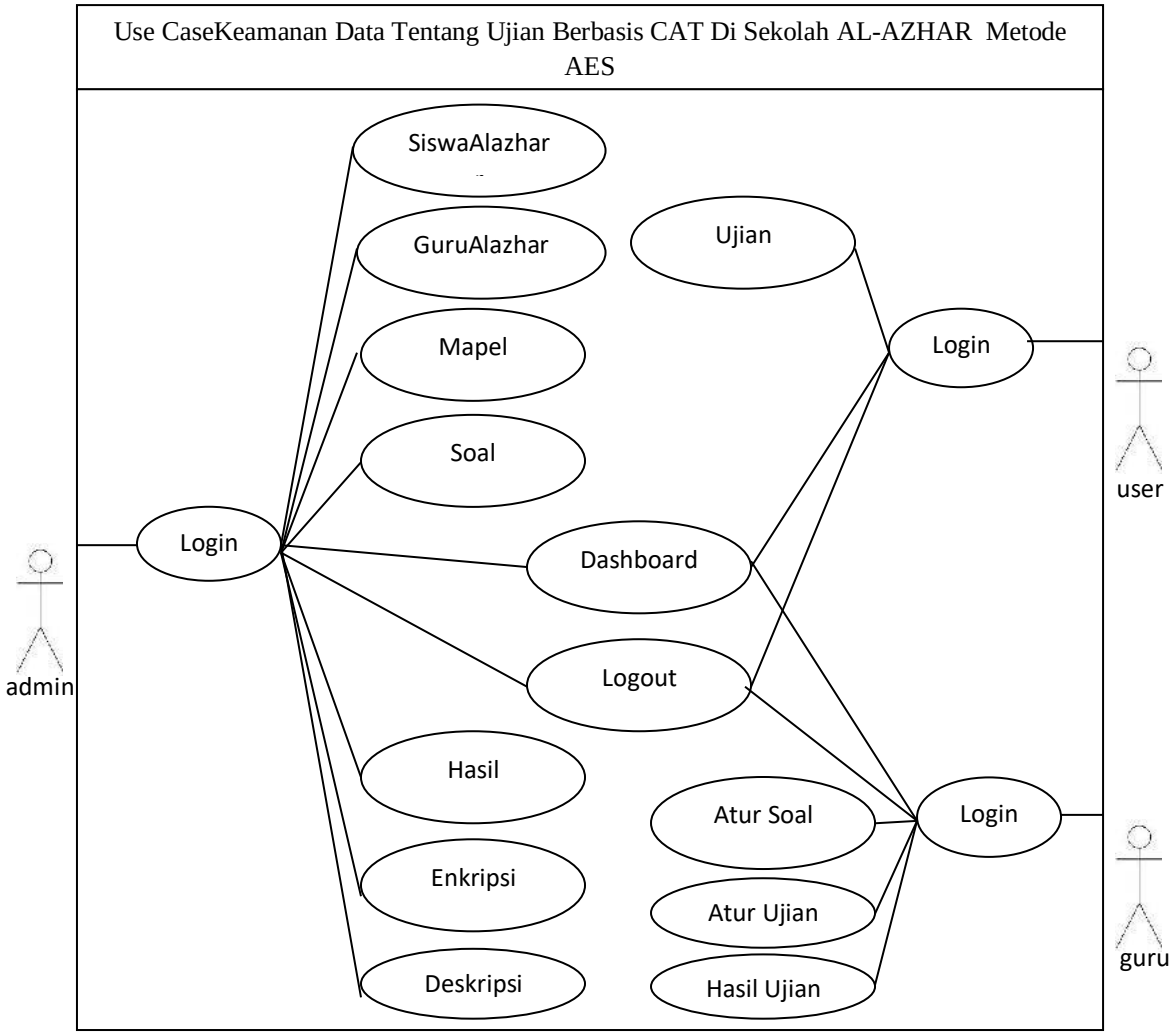
3.4. Rancangan Penelitian

3.4.1. Desain Sistem Secara Global

Desain sistem atau perancangan sistem adalah proses pengembangan spesifikasi baru berdasarkan hasil *rekomendasi* analisis sistem. Dalam tahap perancangan, diharuskan merancang *spesifikasi* yang dibutuhkan. Bentuk rancangan sistem yang penulis buat menggunakan beberapa bentuk diagram dari *Unified Modeling Language* (UML) yaitu *Use Cace Diagram, Sequence Diagram, Activity Diagram, dan Class Diagram*.

3.4.2. *Use Case Diagram*

Perancangan dimulai dari *identifikasi* aktor dan bagaimana hubungan antara aktor dan *use case* didalam sistem. Perancangan *Use Case* Diagram dapat dilihat pada gambar 3.2.



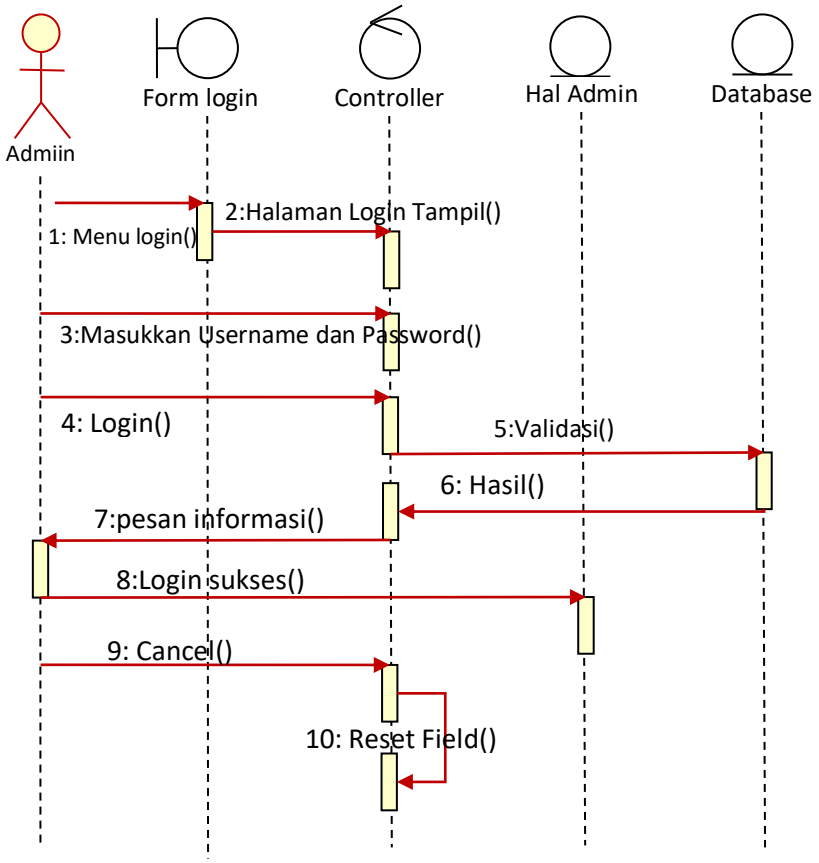
Gambar 3.2. *Use Case Diagram* Ujian CAT

3.4.3. *Sequence Diagram*

Rangkaian kerja melakukan pengamanan data nilai dan soal ujian semester dapat terlihat seperti pada gambar 3.3. berikut :

3.4.4. *Sequence Diagram Login*

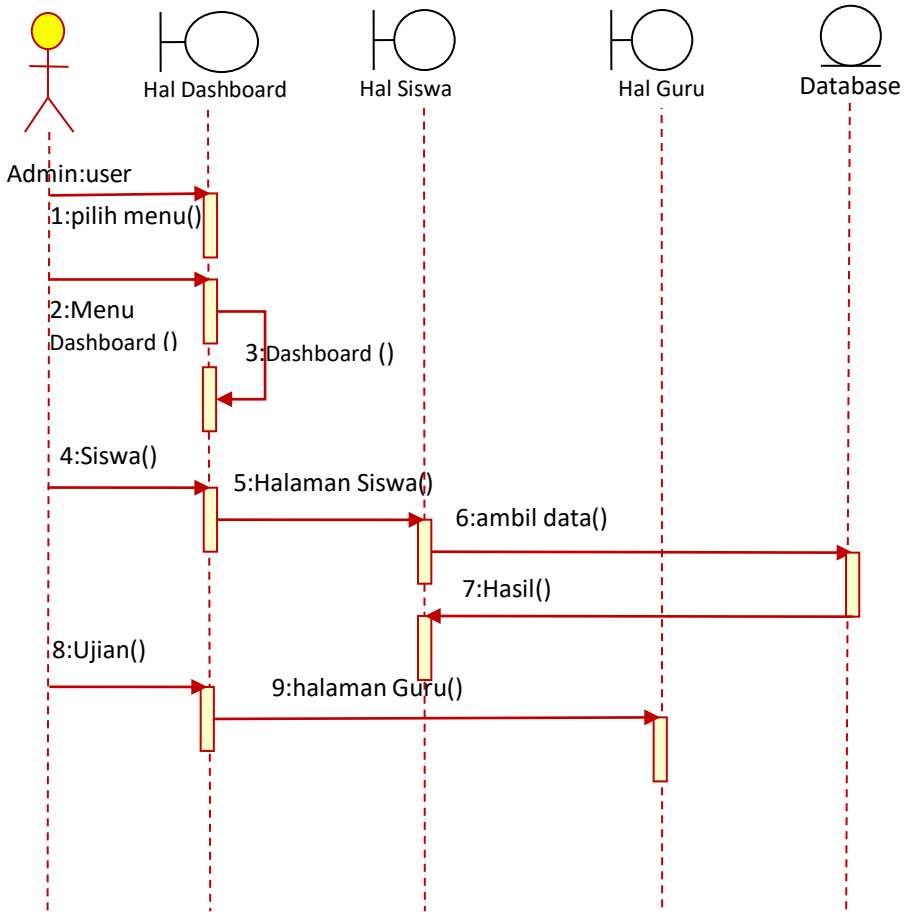
Gambar 3.3. adalah *sequence* diagram login dari Perancangan Aplikasi Keamanan Data Nilai Dan Soal Ujian Semester Dengan Implementasi Algoritma AES".



Gambar 3.3. *Sequence Diagram* Daftar *Login*

3.4.5. *Sequence Diagram* Dashboard

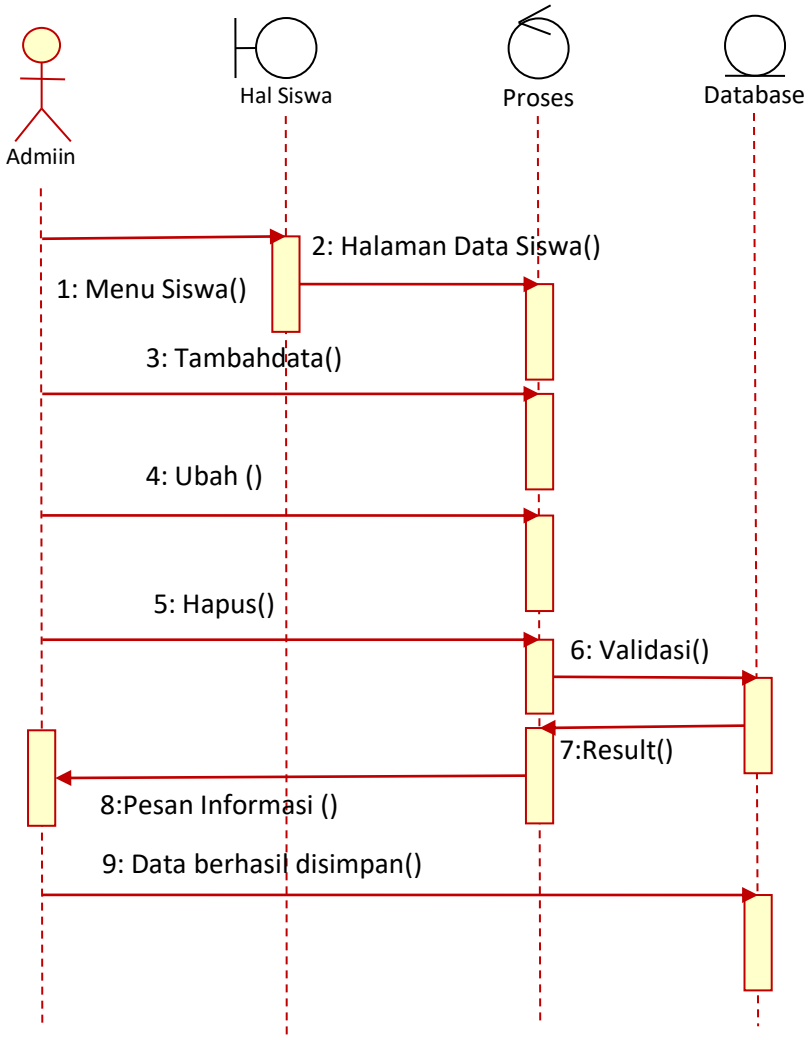
Gambar 3.4. adalah *sequence* diagram dashboard pada aplikasi ujian cat metode aes.



Gambar 3.4. *Sequence Diagram* Dashboard

3.4.6. *Sequence Diagram* Siswa

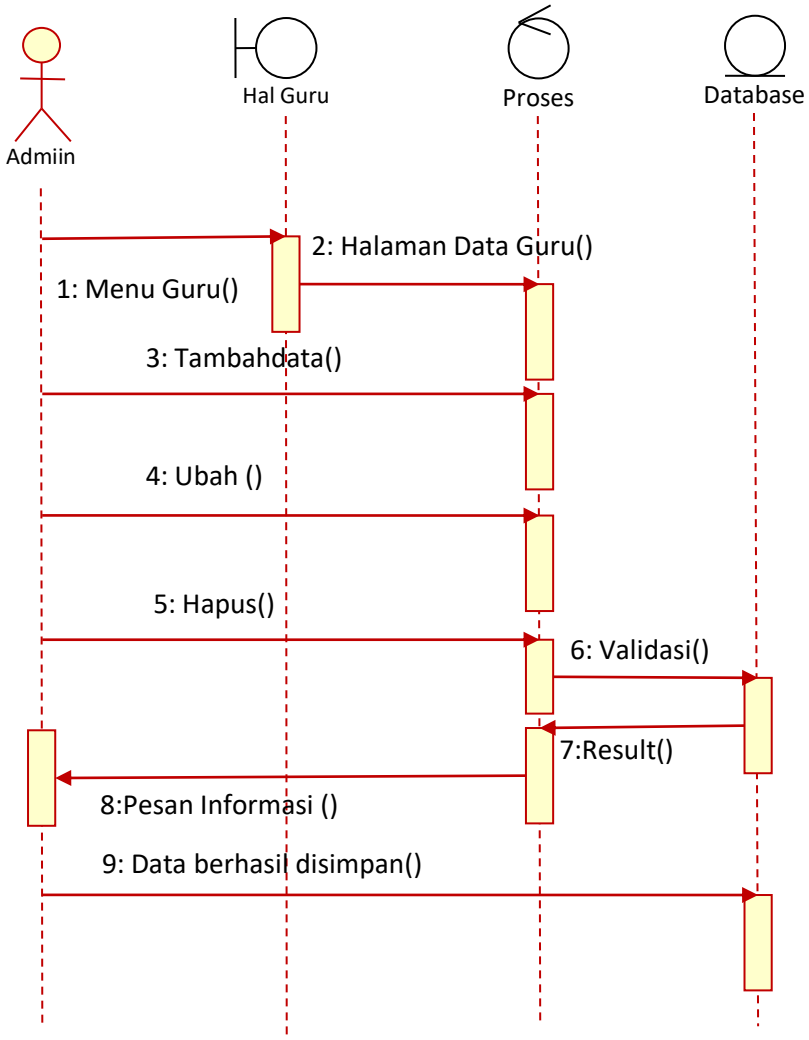
Gambar 3.5. adalah *sequence* diagram siswa pada aplikasi ujian cat metode aes.



Gambar 3.5. *Sequence Diagram* Siswa

3.4.7. *Sequence Diagram* Guru

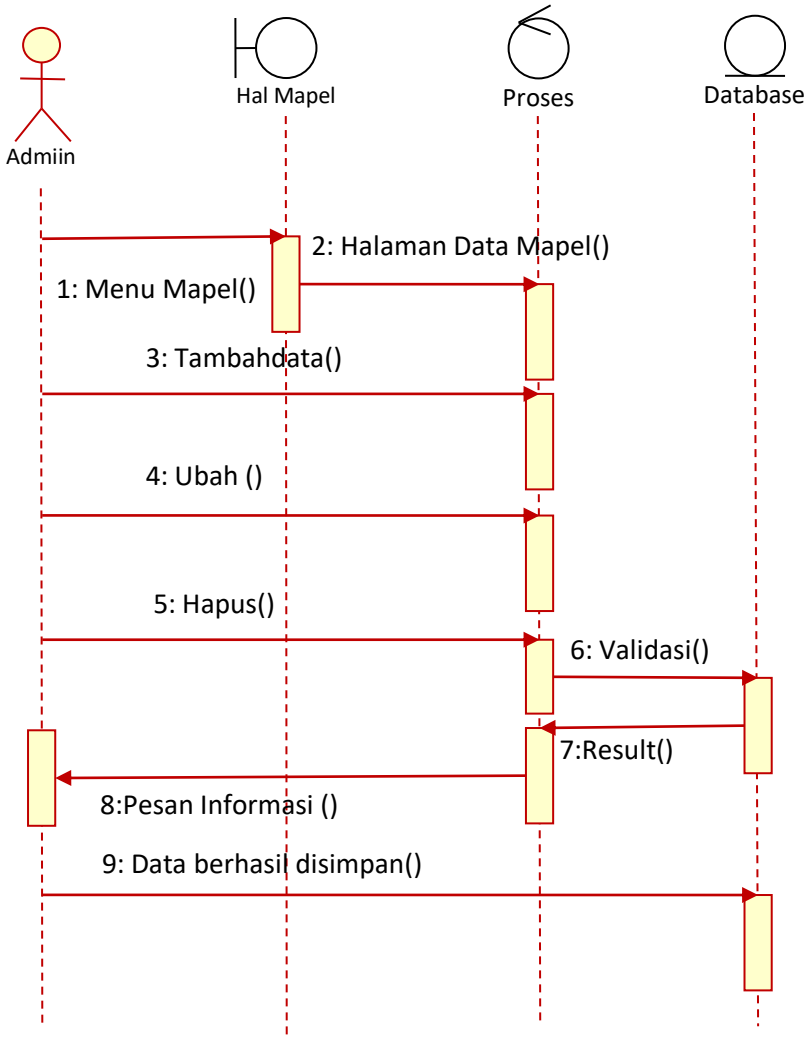
Gambar 3.6. adalah *sequence* diagram guru pada aplikasi ujian cat metode aes.



Gambar 3.6. *Sequence Diagram* Guru

3.4.8. *Sequence Diagram* Mapel

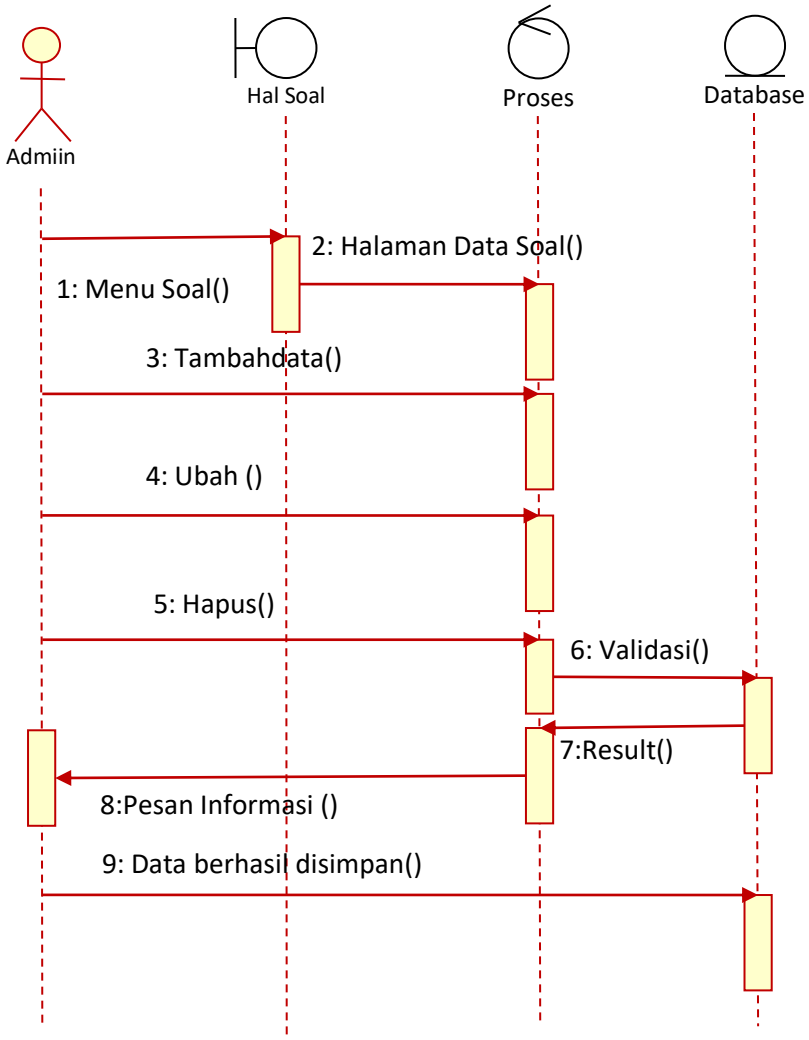
Gambar 3.7. adalah *sequence* diagram mapel pada aplikasi ujian cat metode aes.



Gambar 3.7. *Sequence Diagram* Mapel

3.4.9. *Sequence Diagram* Soal

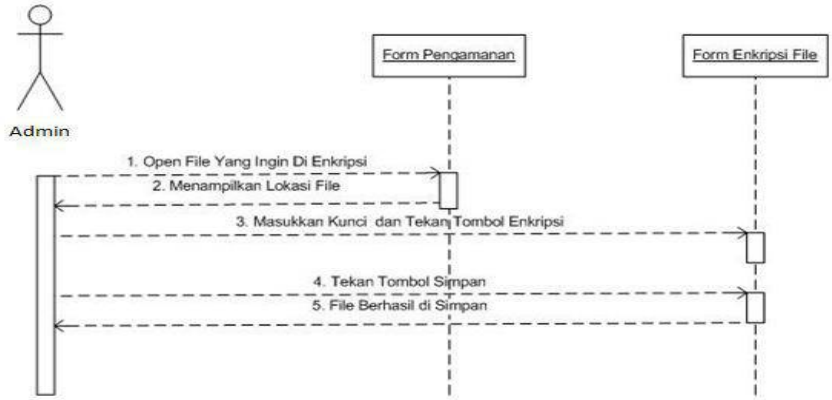
Gambar 3.8. adalah *sequence* diagram soal pada aplikasi ujian cat metode aes.



Gambar 3.8. *Sequence Diagram* Soal

3.4.10. *Sequence Diagram* Enkripsi

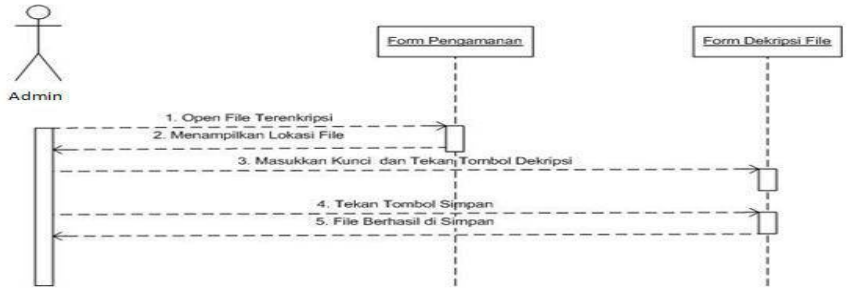
Gambar 3.9. adalah *sequence* diagram Proses Enkripsi dari Perancangan Aplikasi Keamanan Data Nilai Dan Soal Ujian Semester Dengan Implementasi Algoritma AES.



Gambar 3.9. *SequenceDiagram* Proses Enkripsi

3.4.11. *Sequence Diagram* Dekripsi

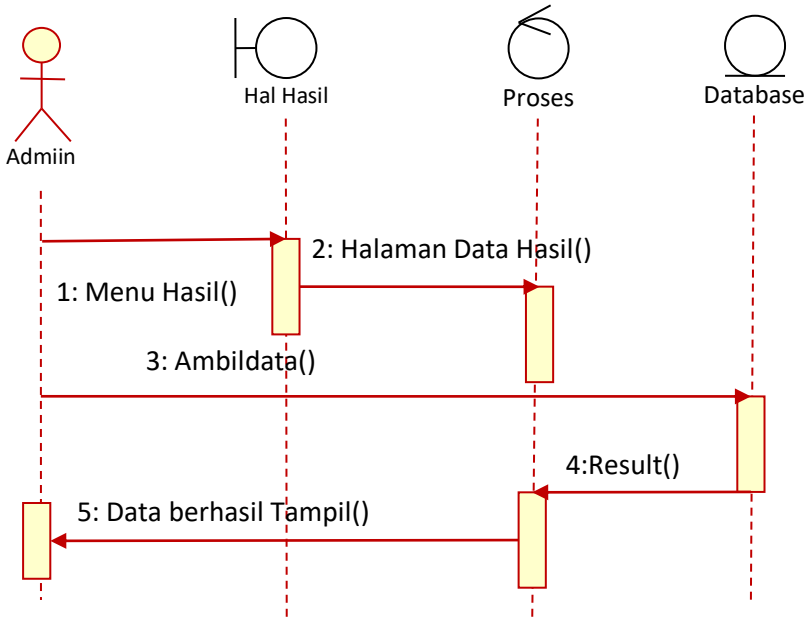
Gambar 3.10. adalah *sequence* diagram Dekripsi dari Perancangan Aplikasi Keamanan Data Nilai Dan Soal Ujian Semester Dengan Implementasi Algoritma AES.



Gambar 3.10. *Sequence Diagram* Dekripsi

3.4.12. *Sequence Diagram* Hasil

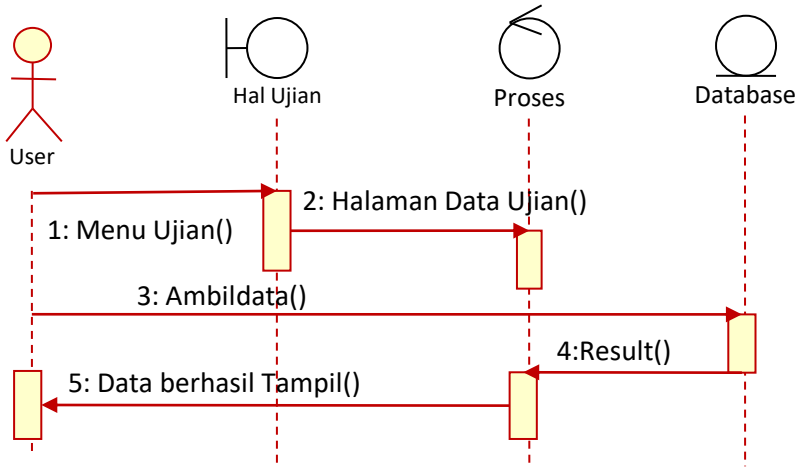
Gambar 3.11. adalah *sequence* diagram hasil pada aplikasi ujian cat metode aes.



Gambar 3.11. *SequenceDiagram* Hasil

3.4.13. *Sequence Diagram* User Ujian

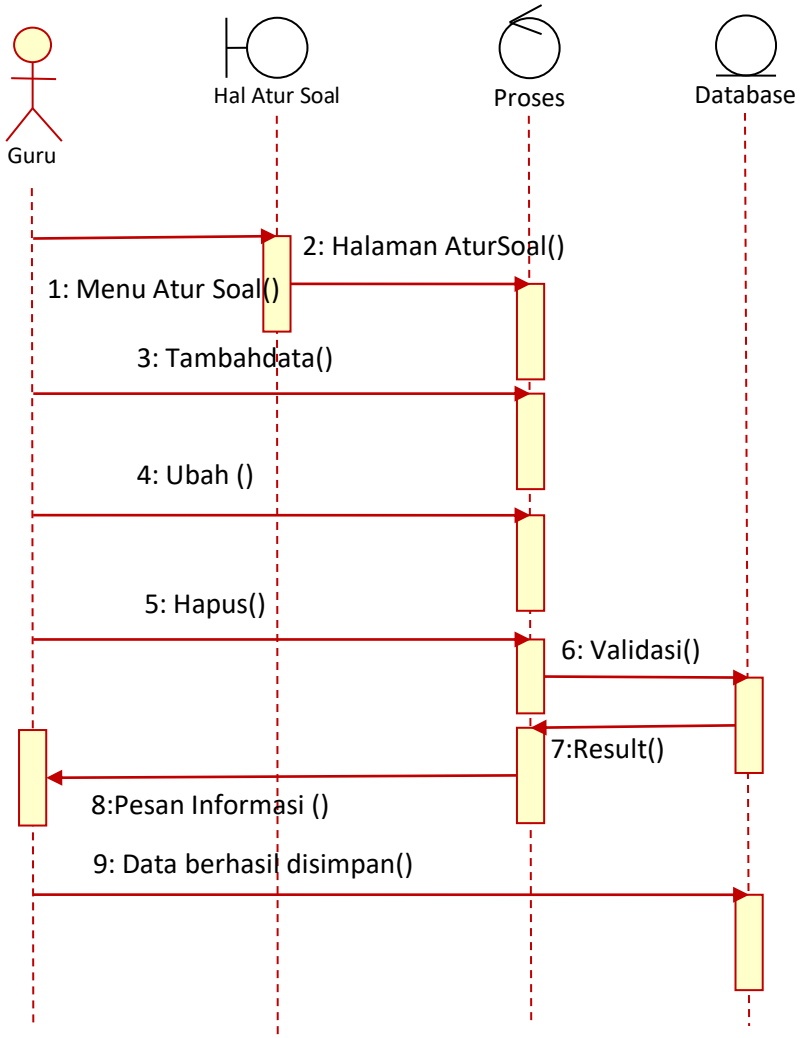
Gambar 3.12. adalah *sequence* diagram user ujian pada aplikasi ujian cat metode aes.



Gambar 3.12. *Sequence Diagram* User Ujian

3.4.14. *Sequence Diagram* Atur Soal

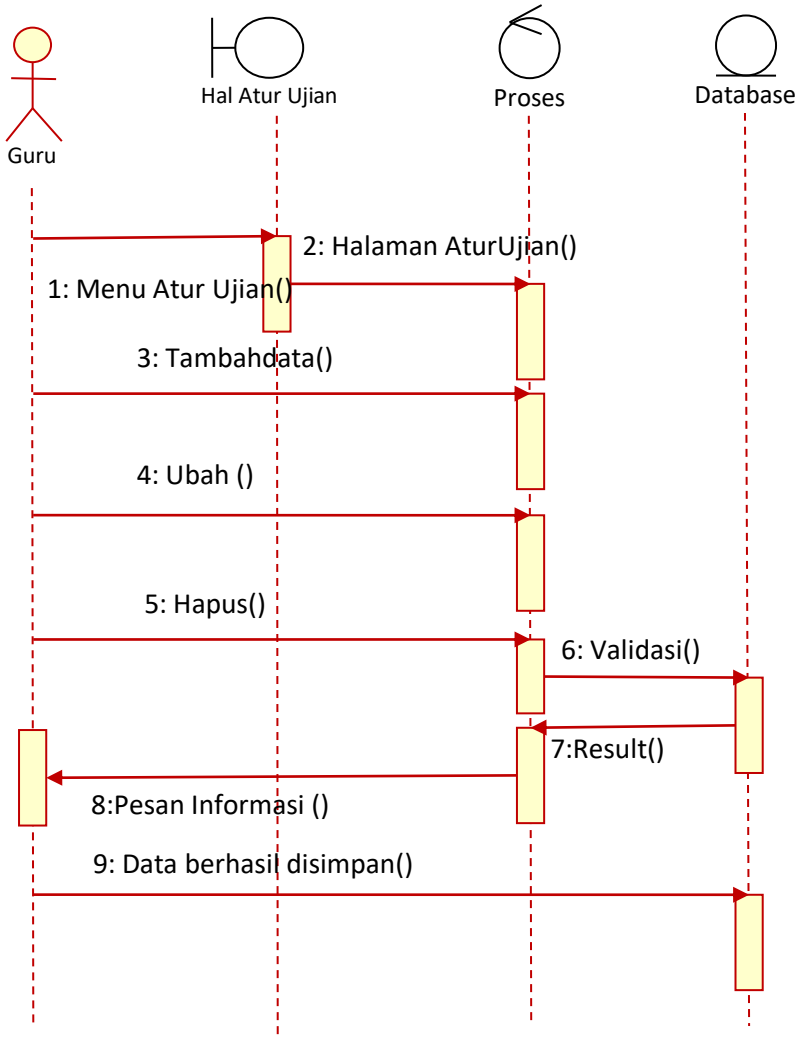
Gambar 3.13. adalah *sequence* diagram guru atur soal pada aplikasi ujian cat metode aes.



Gambar 3.13. *Sequence Diagram* Atur Ujian

3.4.15. *Sequence Diagram* Atur Ujian

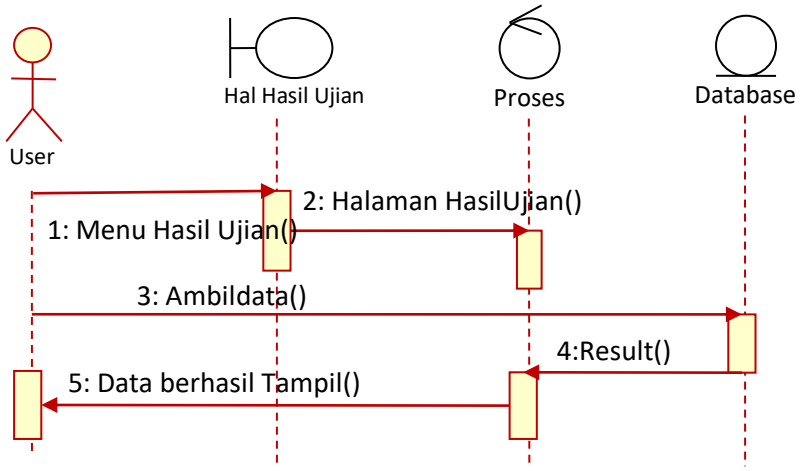
Gambar 3.14. adalah *sequence* diagram guru atur ujian pada aplikasi ujian cat metode aes.



Gambar 3.14. *SequenceDiagram* Atur Ujian

3.4.16. *Sequence Diagram* Hasil Ujian

Gambar 3.15. adalah *sequence* diagram guru hasil ujian pada aplikasi ujian cat metode aes.



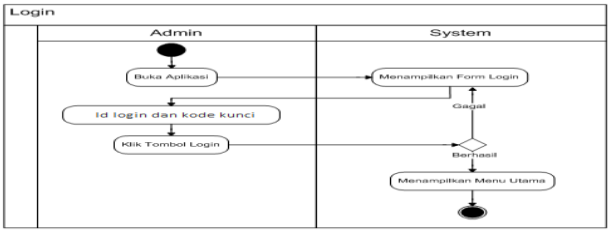
Gambar 3.15. *Sequence Diagram* Hasil Ujian

3.4.17. *Activity Diagram*

Proses yang digambarkan dalam *use case diagram* diatas dijabarkan dengan *activity diagram* :

3.4.18. *Activity Diagram Login*

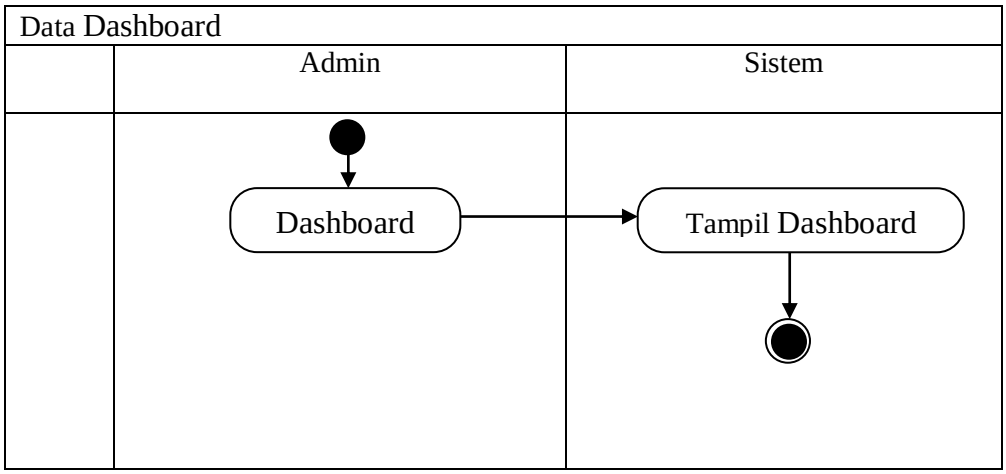
Aktivitas *login* yang dilakukan oleh admin dapat diterangkan dengan langkah-langkah *state* yang ditunjukkan pada gambar 3.16 sebagai berikut :



Gambar 3.16. *Activity Diagram Login*

3.4.19. *Activity Diagram* Dashboard

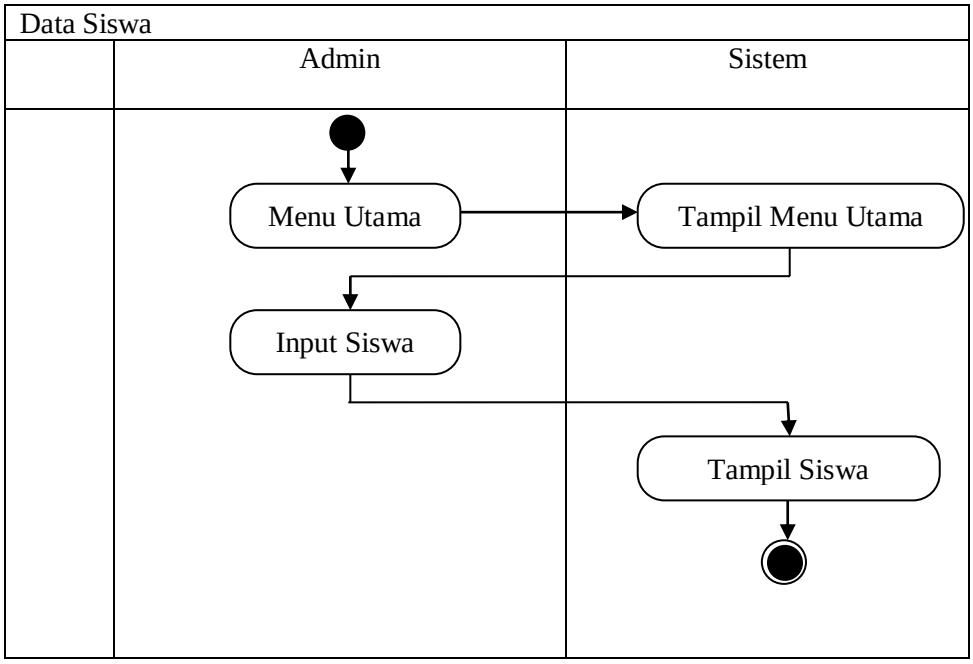
Aktivitas dashboard dapat dilihat pada gambar 3.17 sebagai berikut :



Gambar 3.17. *Activity Diagram* Dashboard

3.4.20. *Activity Diagram* Siswa

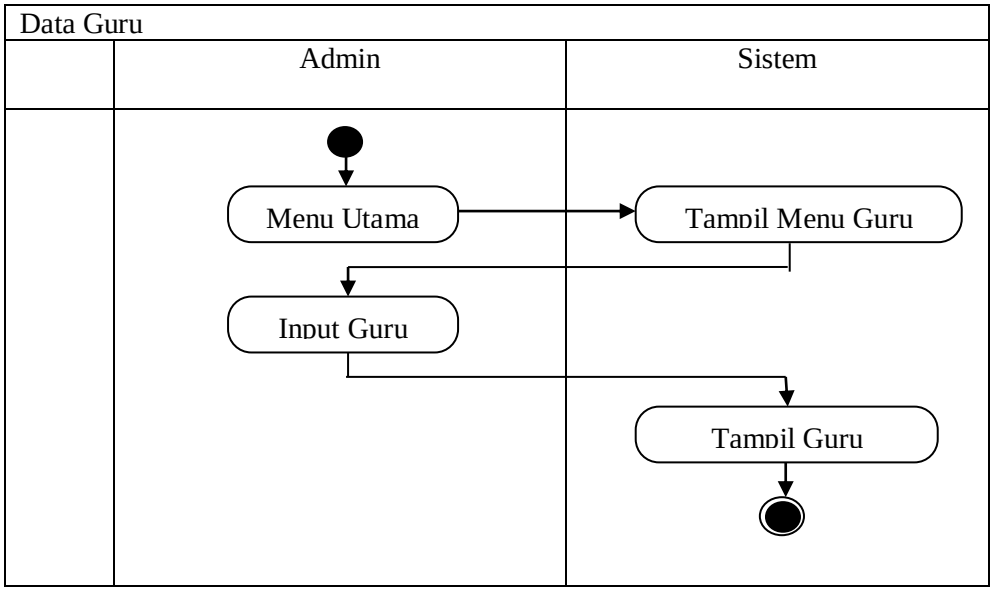
Aktivitas siswa yang dilakukan oleh admin dapat diterangkan dengan langkah-langkah *state* yang ditunjukkan pada gambar 3.18 sebagai berikut :



Gambar 3.18. *Activity Diagram* Data Siswa

3.4.21. *Activity Diagram* Guru

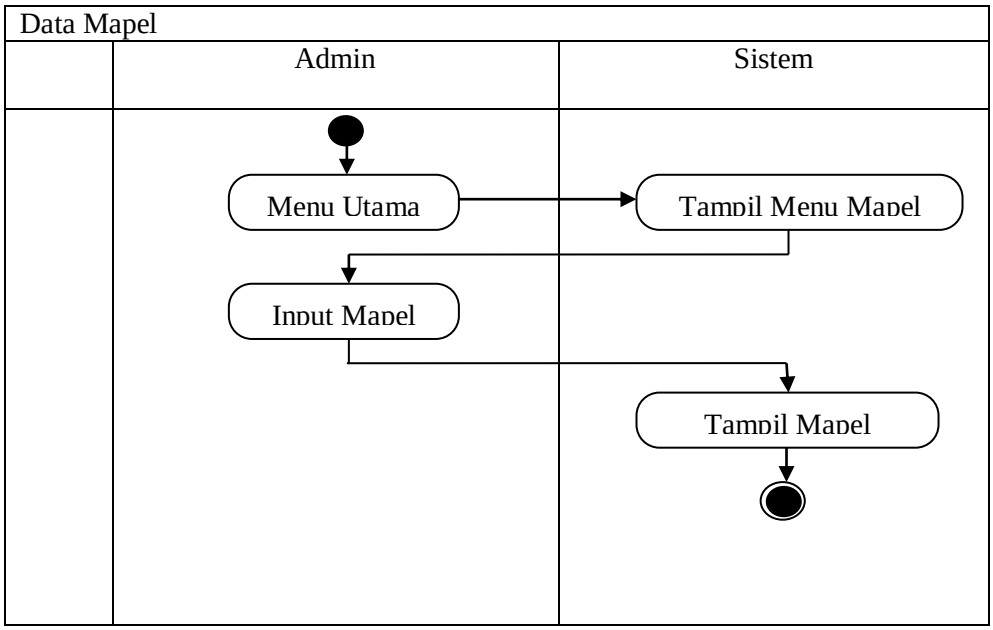
Aktivitas guru yang dilakukan oleh admin dapat diterangkan dengan langkah-langkah *state* yang ditunjukkan pada gambar 3.19 sebagai berikut :



Gambar 3.19. *Activity Diagram* Data Guru

3.4.22. *Activity Diagram* Mapel

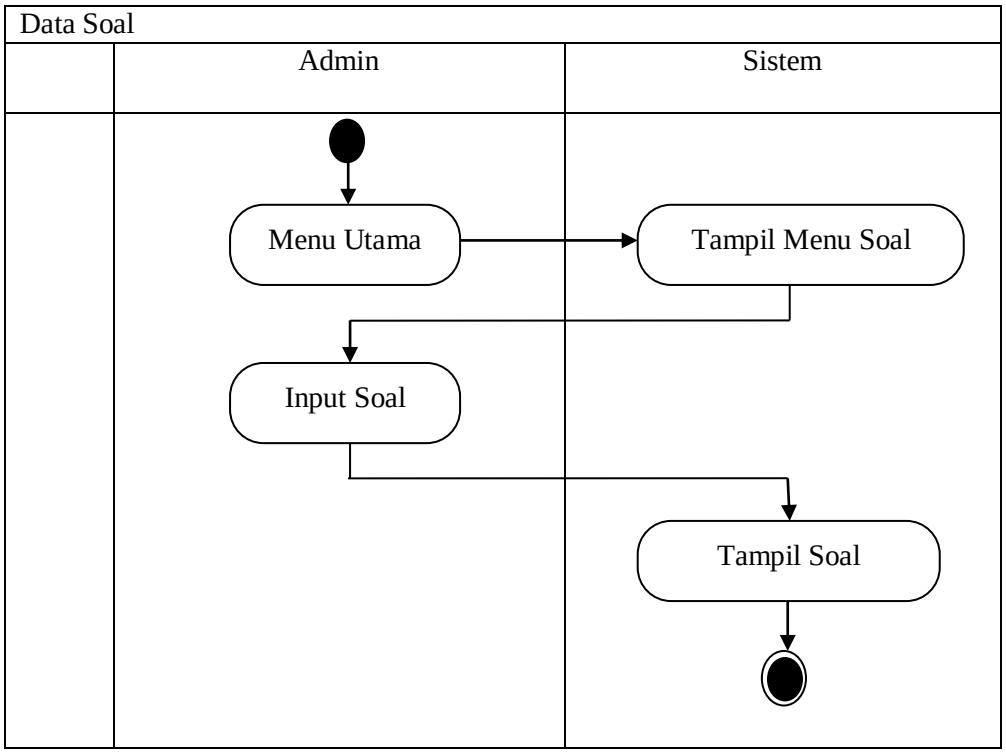
Aktivitas data mapel dapat dilihat pada gambar 3.20 sebagai berikut :



Gambar 3.20. *Activity Diagram* Data Mapel

3.4.23. *Activity Diagram* Soal

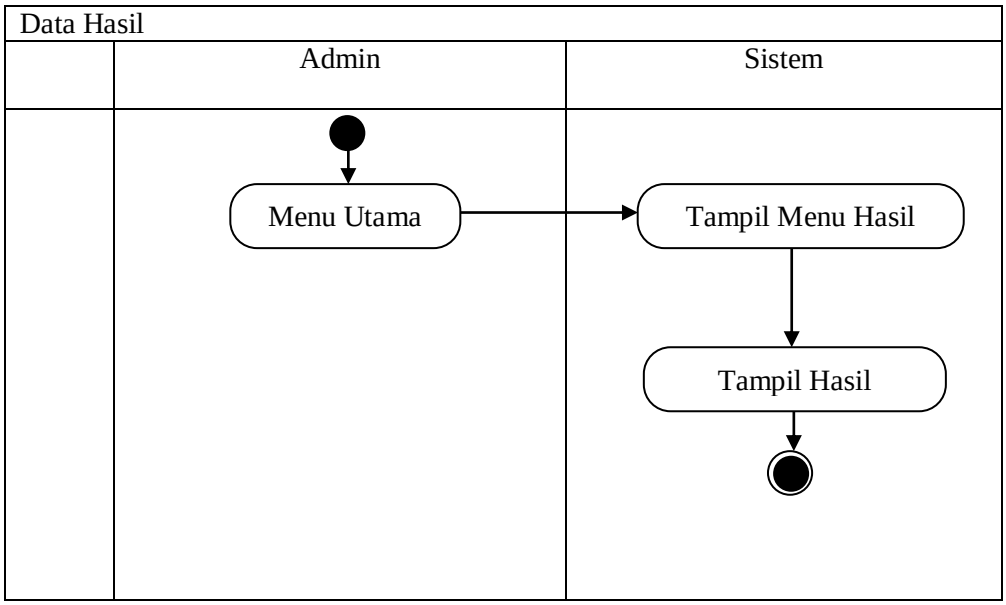
Aktivitas data soal dapat dilihat pada gambar 3.21 sebagai berikut :



Gambar 3.21. *Activity Diagram* Data Soal

3.4.24. *Activity Diagram* Hasil

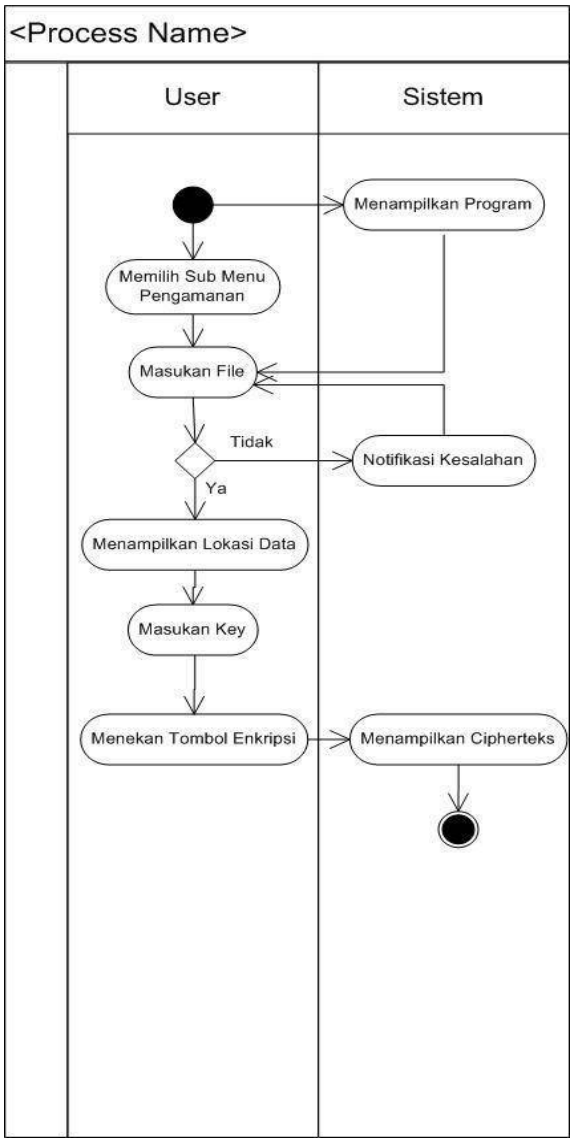
Aktivitas data hasil dapat dilihat pada gambar 3.22 sebagai berikut :



Gambar 3.22. *Activity Diagram*Hasil

3.4.25. *Activity Diagram Enkripsi*

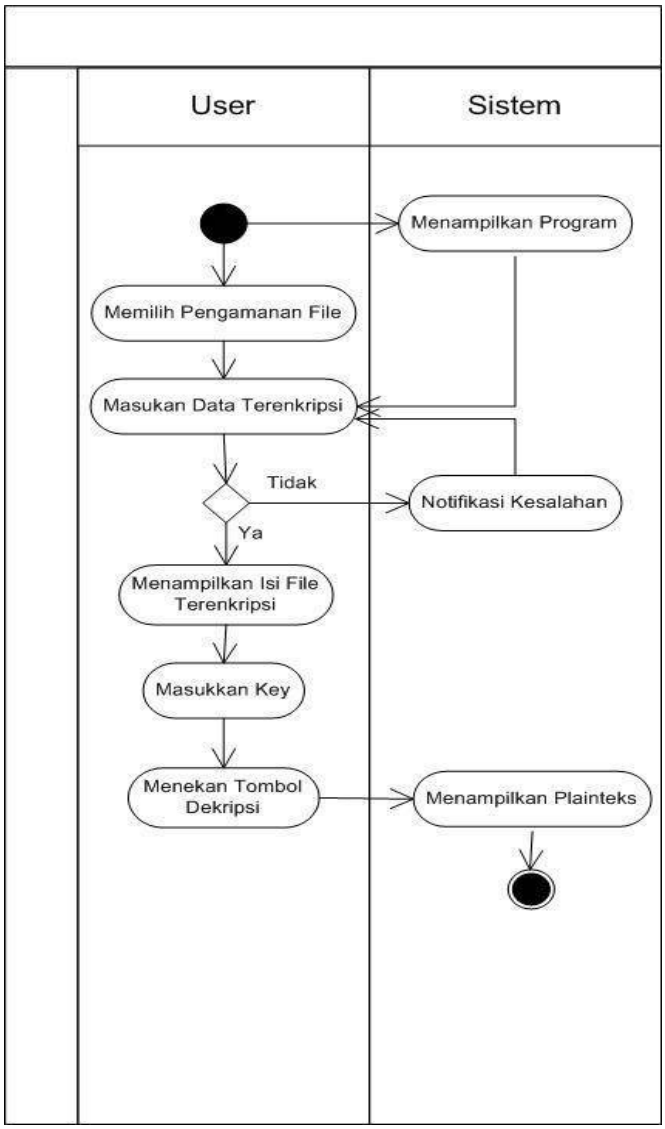
Gambar 3.23. adalah *activity diagramenkripsi* dari Perancangan Aplikasi Keamanan Data Nilai Dan Soal Ujian Semester Dengan Implementasi Algoritma AES.



Gambar 3.23. *Activity Diagram Enkripsi*

3.4.26. *Activity Diagram Dekripsi*

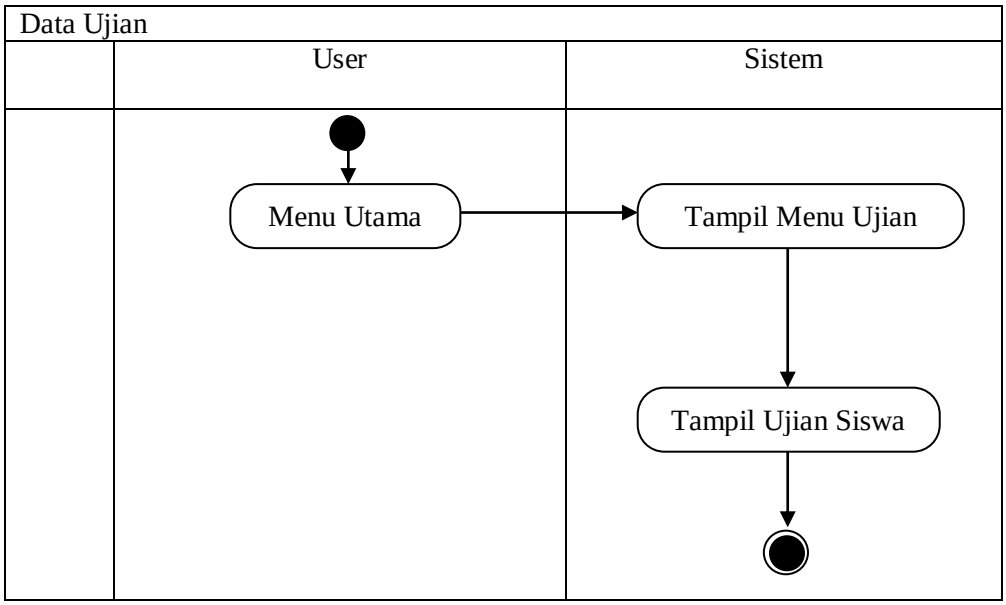
Gambar 3.24. adalah *activity diagram dekripsi* dari Perancangan Aplikasi Keamanan Data Nilai Dan Soal Ujian Semester Dengan Implementasi Algoritma AES.



Gambar 3.24. *Activity Diagram Dekripsi*

3.4.27. *Activity Diagram* User Ujian

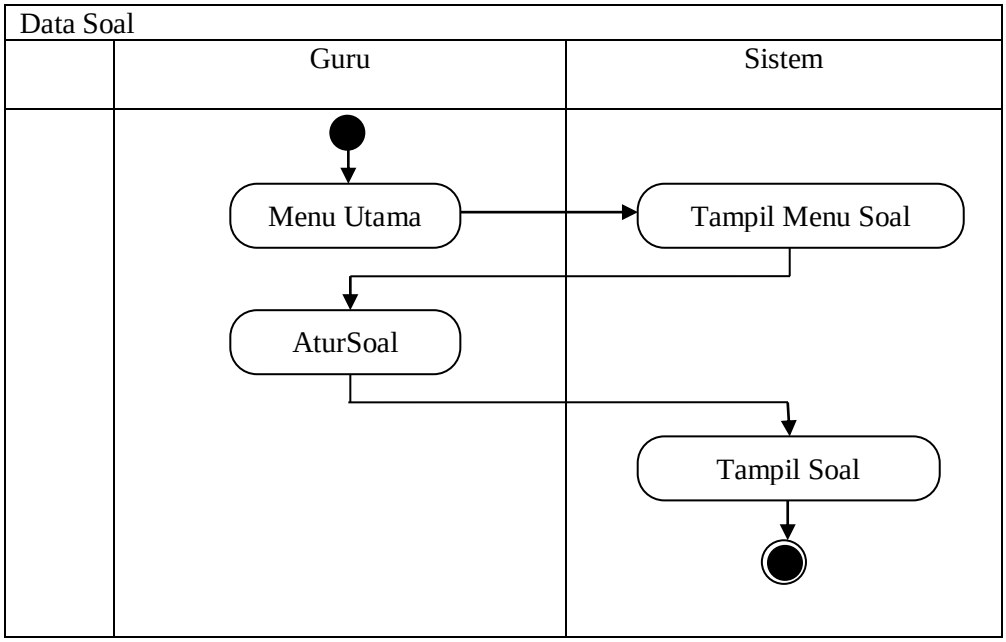
Aktivitas data user ujian dapat dilihat pada gambar 3.25 sebagai berikut :



Gambar 3.25. *Activity Diagram* User Ujian

3.4.28. *Activity Diagram* Guru Atur Soal

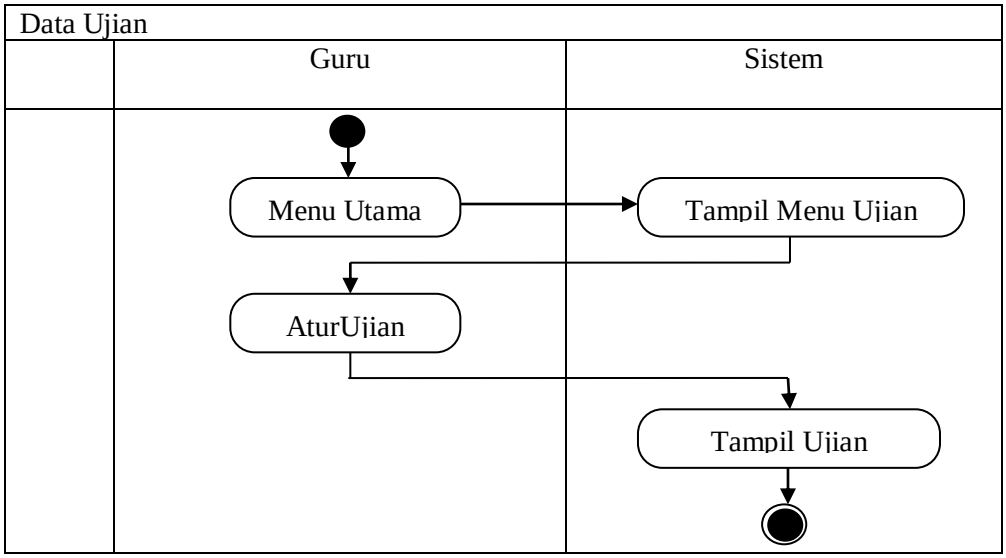
Aktivitas data guru atur soal dapat dilihat pada gambar 3.26 sebagai berikut :



Gambar 3.26. *Activity Diagram* Guru Atur Soal

3.4.29. *Activity Diagram* Guru Atur Ujian

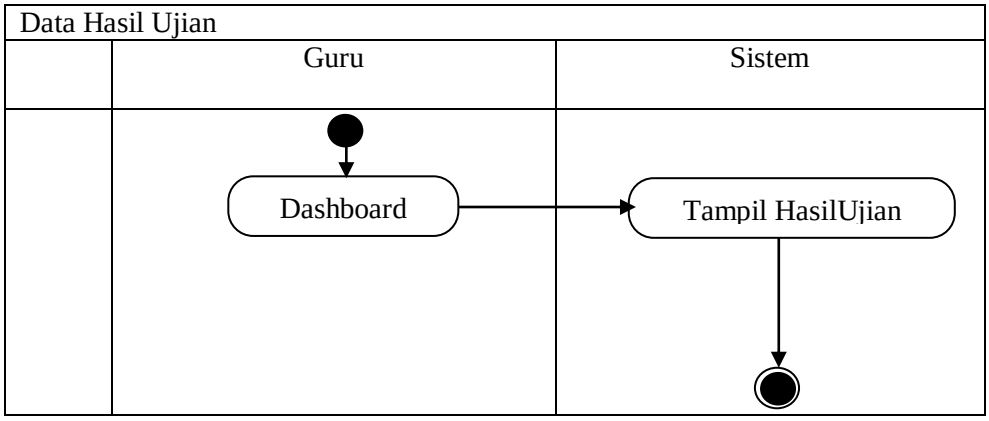
Aktivitas data guru atur ujian dapat dilihat pada gambar 3.27 sebagai berikut :



Gambar 3.27. *Activity Diagram* Guru Atur Ujian

3.4.30. *Activity Diagram* Guru Hasil Ujian

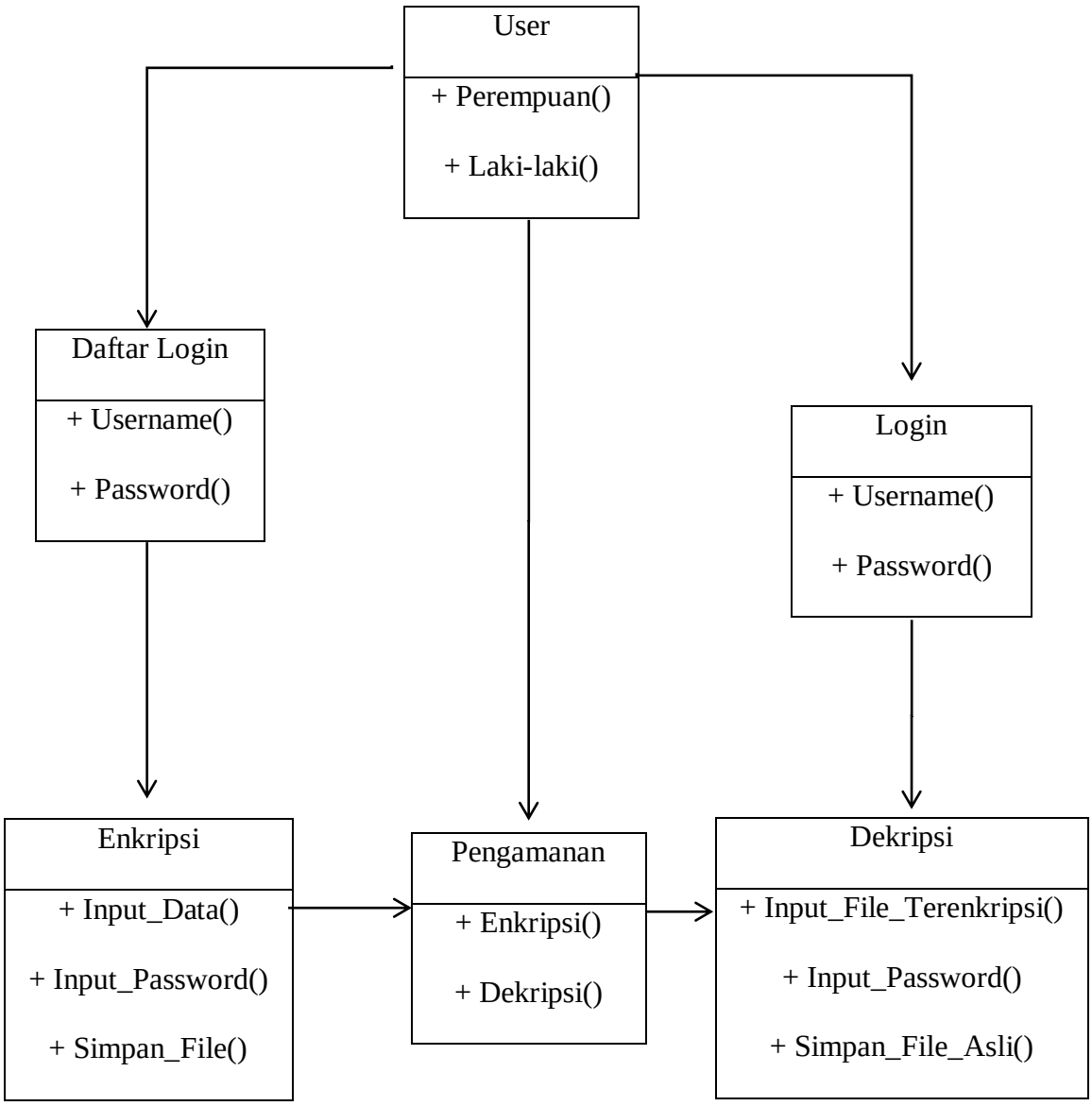
Aktivitas data guru hasil ujian dapat dilihat pada gambar 3.28 sebagai berikut:



Gambar 3.28. *Activity Diagram* Guru Hasil Ujian

3.4.31. *Class Diagram*

Perancangan dari *Class Diagram* di mulai dari *User*,dapat di lihat pada gambar 3.29. sebagai berikut.



Gambar 3.29. *Class Diagram*

3.5.1. Desain Tabel

Merancang struktur tabel pada *database* yang akan dibuat, berikut ini merupakan rancangan strukrut tabel tersebut :

1. Struktur Tabel *Login*

Tabel *login* digunakan untuk menyimpan data *username dan password* selengkapnya mengenai struktur tabel ini dapat dilihat pada tabel 3.1berikut ini :

Tabel 3.1. Rancangan Tabel *Login*

Nama Database		Dbcatdua	
Nama Tabel		Login	
Nama Field	**Tipe Data**	**Ukuran**	**Keterangan**
*username	Varchar	10	*Primary Key*
Password	int	11	-

2. Struktur Tabel Siswa

Tabel ini digunakan untuk menyimpan data siswa dapat dilihat pada tabel 3.2 berikut ini :

Tabel 3.2. Rancangan Tabel Siswa

Nama Database	dbcatdua		
Nama Tabel	M_siswa		
Nama Field	**Tipe Data**	**Ukuran**	**Keterangan**
*id	Varchar	10	*Primary Key*
Nama	Varchar	30	-
Nis	Varchar	10	-
Kelas	Varchar	15	

3. Struktur Tabel Guru

Tabel ini digunakan untuk menyimpan data guru dapat dilihat pada tabel 3.3 berikut ini :

Tabel 3.3. Rancangan Tabel Guru

Nama Database	dbcatdua		
Nama Tabel	M_guru		
Nama Field	**Tipe Data**	**Ukuran**	**Keterangan**
*id	Varchar	10	*Primary Key*
Nip	Varchar	30	-
Nama	Varchar	50	-

4. Struktur Tabel Mapel

Tabel ini digunakan untuk menyimpan data mapel dapat dilihat pada tabel 3.4 berikut ini :

Tabel 3.4. Rancangan Tabel Mapel

Nama Database	dbcatdua		
Nama Tabel	M_mapel		
Nama Field	**Tipe Data**	**Ukuran**	**Keterangan**
*id	Int	5	*Primary Key*
Nama	Varchar	30	-

5. Struktur Tabel Soal

Tabel ini digunakan untuk menyimpan data soal dapat dilihat pada tabel 3.5 berikut ini :

Tabel 3.5. Rancangan Tabel Soal

Nama Database	dbcatdua		
Nama Tabel	M_soal		
Nama Field	**Tipe Data**	**Ukuran**	**Keterangan**
*id	Int	6	*Primary Key*
Id_guru	Int	6	-
Id_mapel	Int	6	
Bobot	Int	2	
File	Varchar	150	
Tipe_file	Varchar	50	
Soal	longtext		
Opsi_a	longtext		
Opsi_b	longtext		
Opsi_c	longtext		
Opsi_d	longtext		
Opsi_e	longtext		
Jawaban	Varchar	5	
Tgl_input	datetime		
Jml_benar	int	6	
Jml_salah	int	6	

6. Struktur Tabel Ujian

Tabel ini digunakan untuk menyimpan data ikut ujian dapat dilihat pada tabel 3.6 berikut ini :

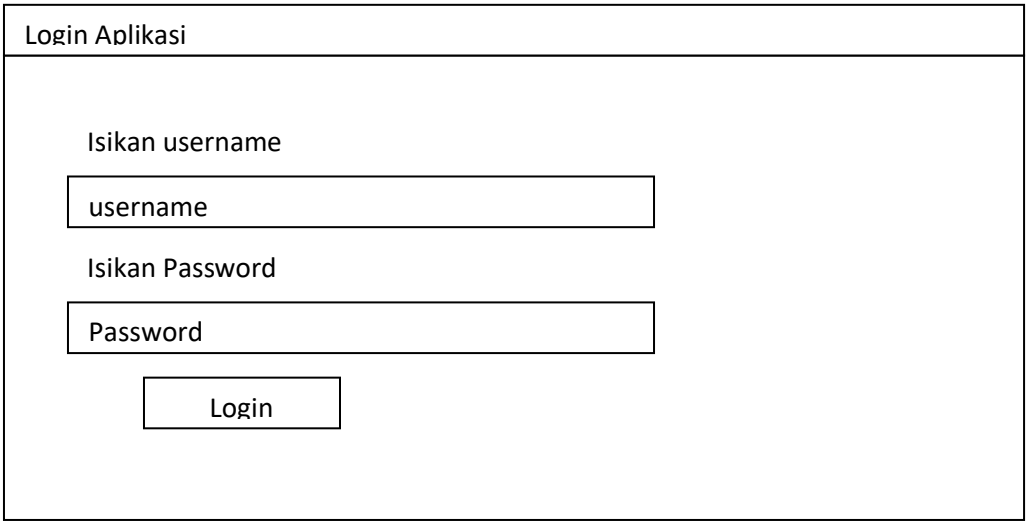
Tabel 3.6. Rancangan Tabel Ikut Ujian

Nama Database	dbcatdua		
Nama Tabel	M_ikut_ujian		
Nama Field	**Tipe Data**	**Ukuran**	**Keterangan**
*id	Int	6	*Primary Key*
Id_tes	Int	6	-
Id_user	Int	6	
List_soal	longtext		
List_jawaban	longtext		
Jlh_benar	int	6	
Nilai	decimal	10,2	
Nilai_bobot	decimal	10,2	
Tgl_mulai	datetime		
Tgl_selesai	datetime		
Status	enum		

3.6.1. Perancangan Desain

Perancangan tampilan awal berfungi untuk mengetahui beberapa sub menu masing-masing dari tombol pada tampilan menu awal dapat dilihat pada gambar 3.29. sebagai berikut:

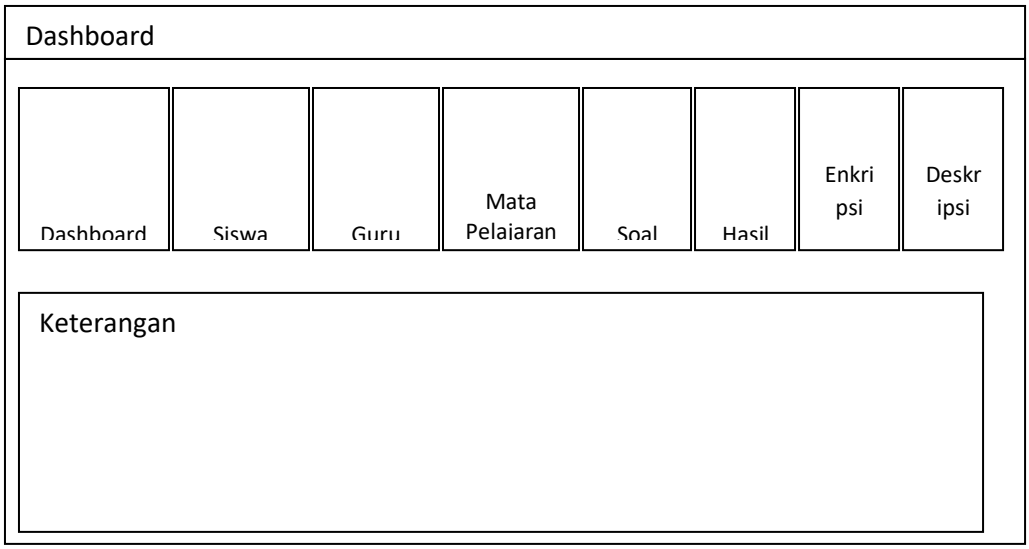
1. Tampilan Login



Gambar 3.30. Tampilan Login

2. Menu Tampilan Dashboard

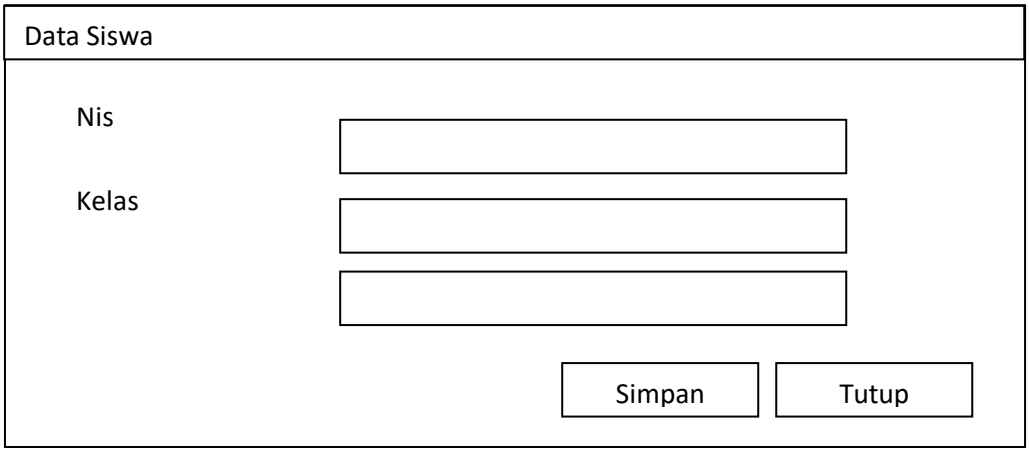
Perancangan *desain* tampilan awal yang disebut dengan dashboard dapat dilihat pada gambar 3.31. sebagai berikut :



Gambar 3.31. Tampilan Dashboard

3. Menu Tampilan Siswa

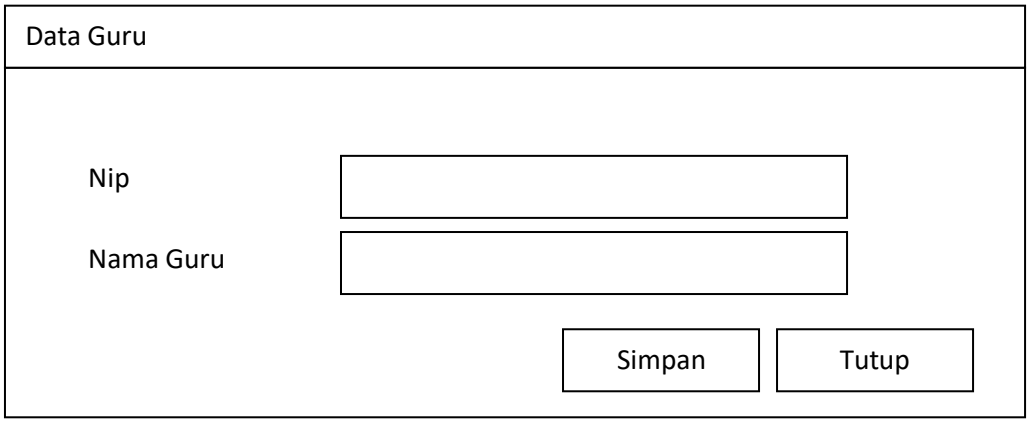
Perancangan *desain* data siswa dapat dilihat pada gambar 3.32. sebagai berikut



Gambar 3.32. Tampilan Data Siswa

4. Menu Tampilan Guru

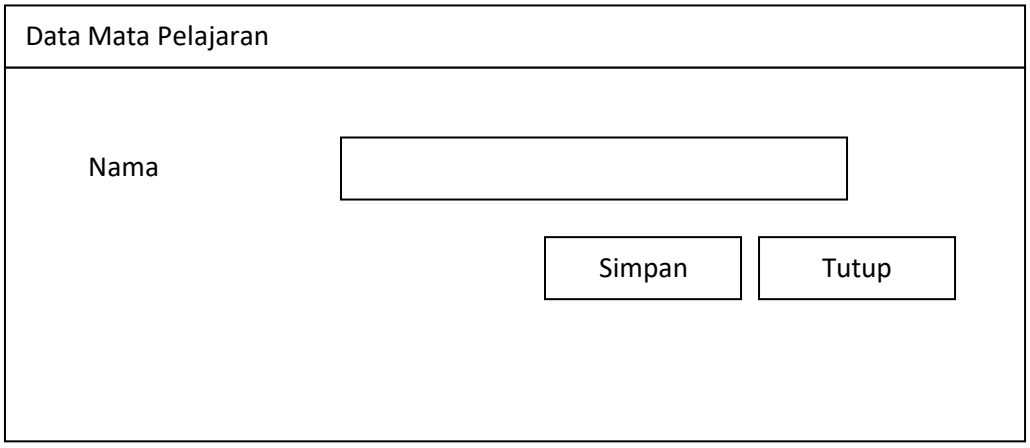
Perancangan *desain*data guru dapat dilihat pada gambar 3.33. sebagai berikut:



Gambar 3.33. Tampilan Data Guru

5. Menu Tampilan Mapel

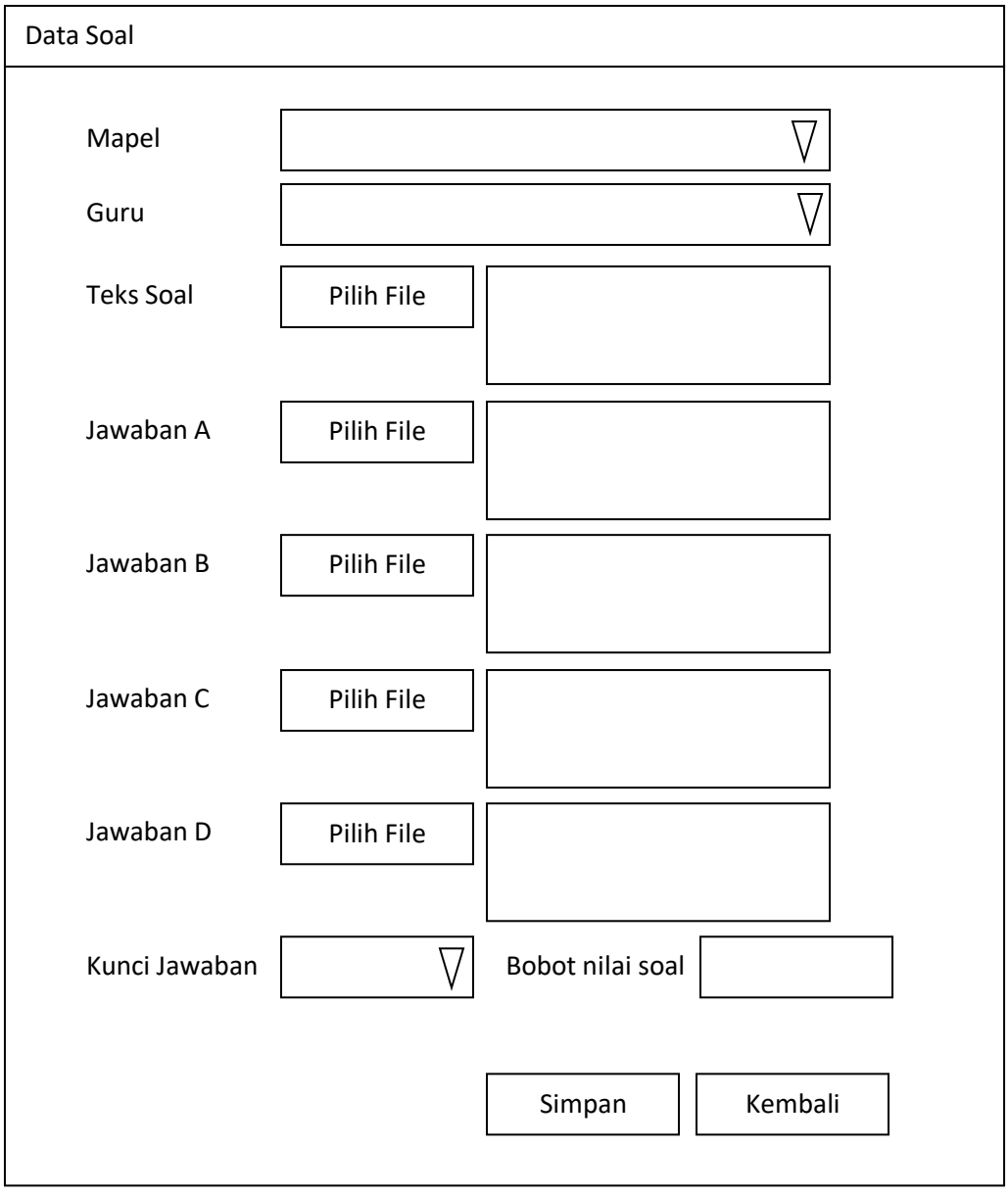
Perancangan *desain*data mapel dapat dilihat pada gambar 3.34. sebagai berikut :



Gambar 3.34. Tampilan Data Mapel

6. Menu Tampilan Soal

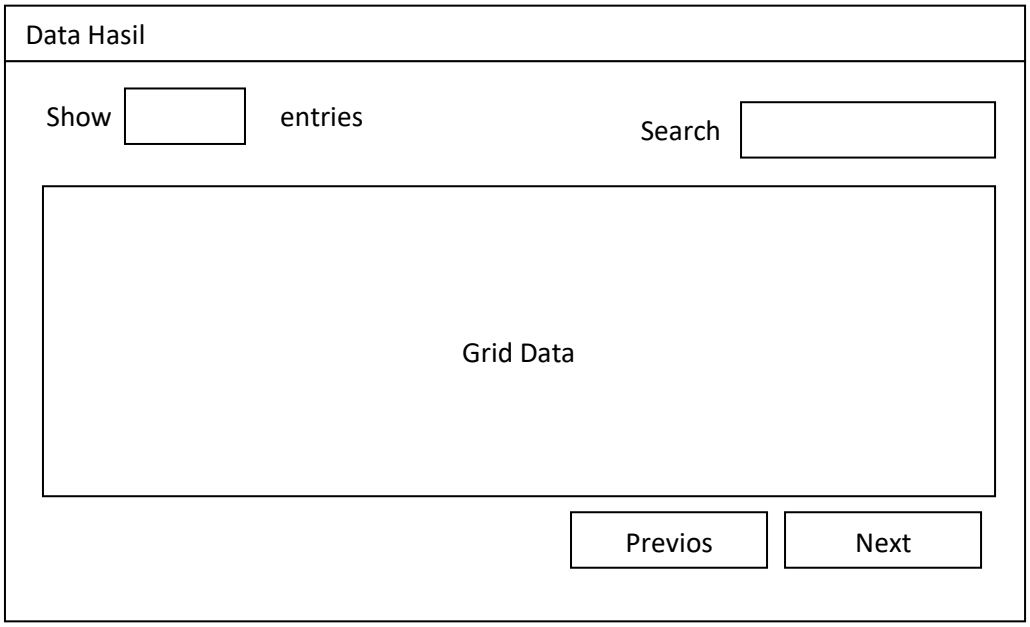
Perancangan *desain* data soal dapat dilihat pada gambar 3.35. sebagai berikut :



Gambar 3.35. Tampilan Data Soal

7. Menu Tampilan Hasil

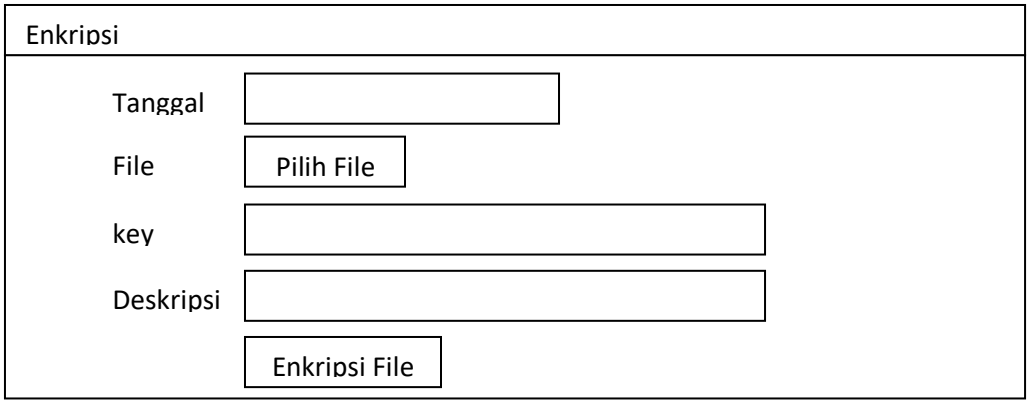
Perancangan *desain* hasil dapat dilihat pada gambar 3.36. sebagai berikut



Gambar 3.36. Tampilan Hasil

8. Menu Tampilan Enkripsi

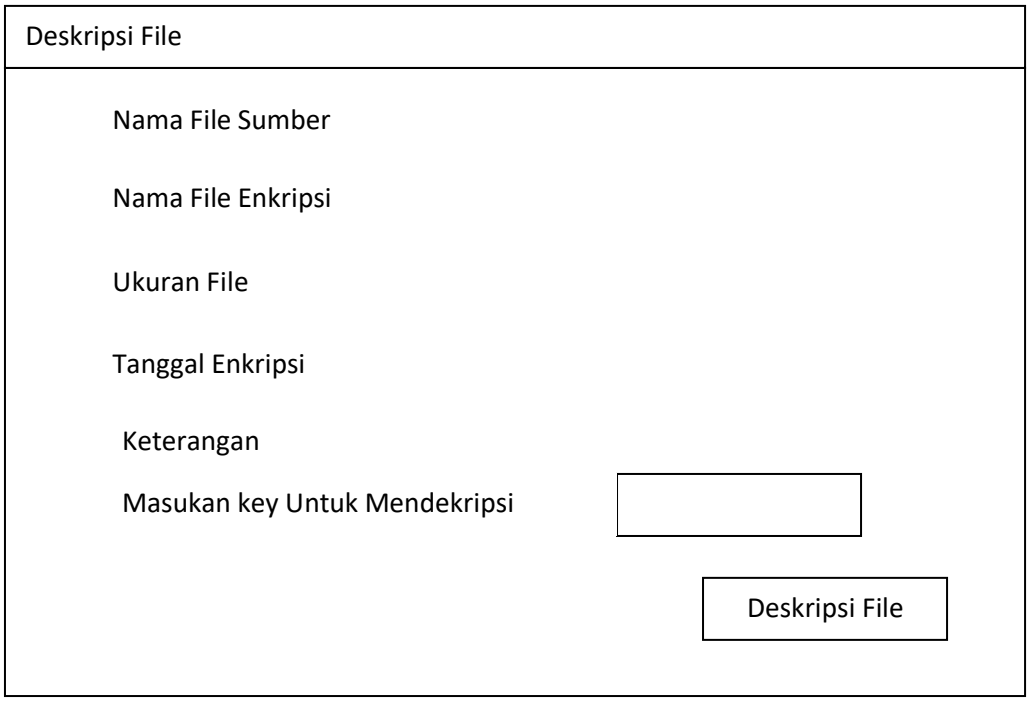
Perancangan *desain* enkripsi dapat dilihat pada gambar 3.37. sebagai berikut



Gambar 3.37. Tampilan Enkripsi

9. Menu Tampilan Deskripsi

Perancangan *desain* deskripsi dapat dilihat pada gambar 3.38. sebagai berikut



Gambar 3.38. Tampilan Deskripsi File

BAB IV

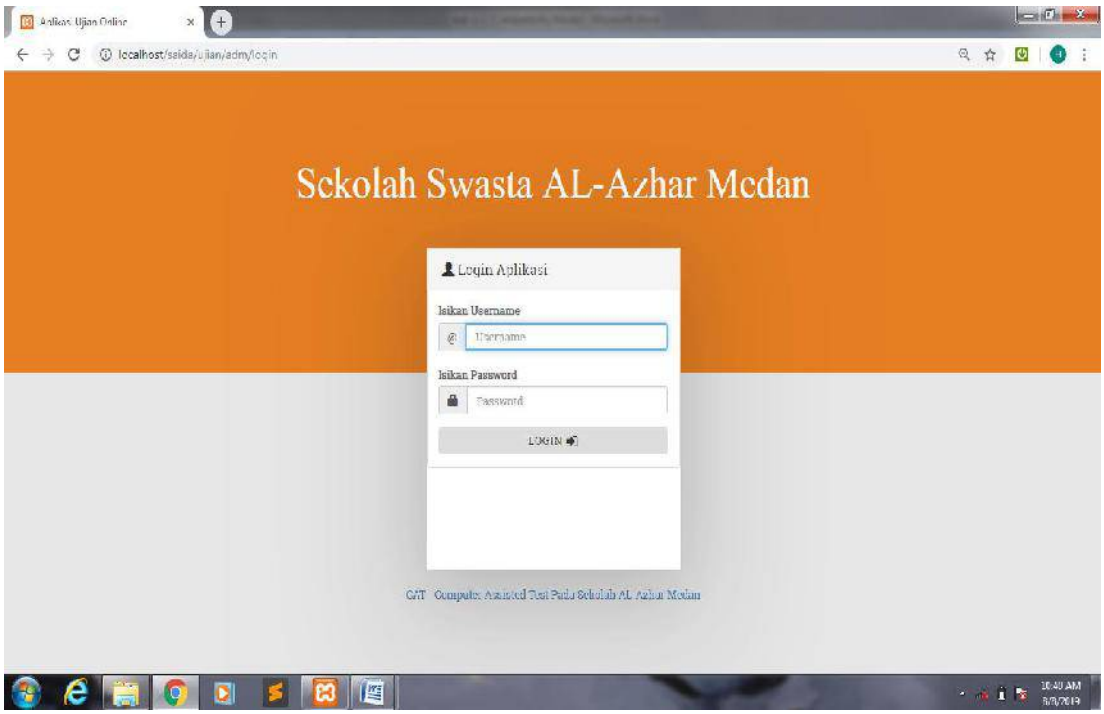
HASIL DAN UJI COBA

4.1. Tampilan Hasil

Berikut adalah tampilan hasil dan pembahasan dari Aplikasi Keamanan Data Tentang Ujian Berbasis CAT Di Sekolah AL-AZHAR Menggunakan Metode AES Berbasis WEB.

4.1.1. Tampilan Login

Tampilan login terdiri dari beberapa tombol, untuk lebih jelasnya dapat dilihat pada Gambar 4.1.



Gambar 4.1. Tampilan Login

4.1.2. Tampilan Dashboard

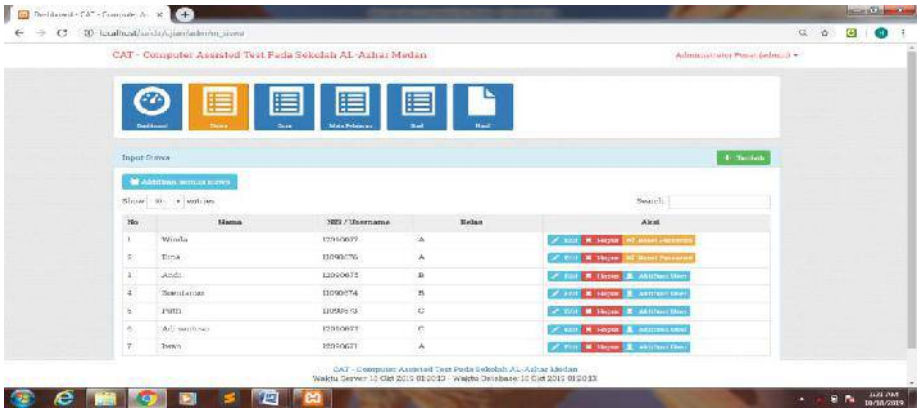
Tampilan dashboard terdiri dari beberapa tombol dan menu, untuk lebih jelasnya dapat dilihat pada Gambar 4.2.

Gambar 4.2. Tampilan Dashboard

Pada Gambar 4.2 menampilkan Dashboard yang berfungsi sebagai pusat seluruh program yang ada.

4.1.3. Tampilan Data Siswa

Tampilan ini menampilkan seluruh siswa yang telah ada, untuk lebih jelasnya dapat dilihat pada Gambar 4.3.

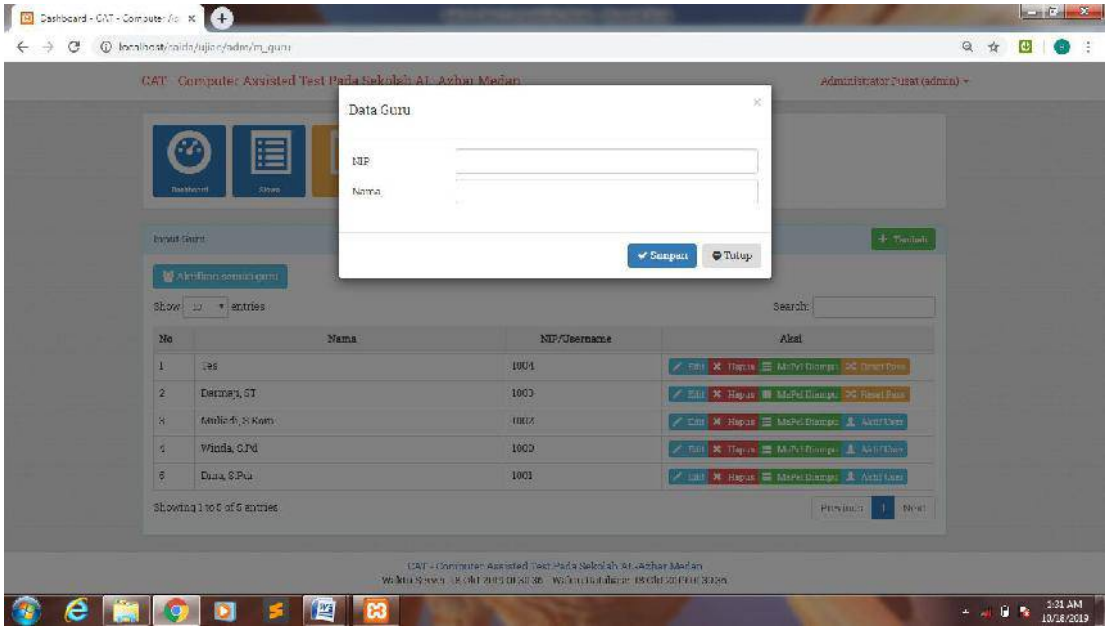


Gambar 4.3. Tampilan Data Siswa

Halaman pada gambar 4.3 menjelaskan bahwa admin dapat melakukan tambah data, perbaiki data, hapus data dan dilengkapi dengan tombol batal dan keluar dari aplikasi tersebut dan user dapat melihat data yang telah masuk kedalam database dengan mempergunakan *grid coloum*.

4.1.4. Tampilan Data Guru

Tampilan data ini adalah data guru, untuk lebih jelasnya dapat dilihat pada Gambar 4.4.

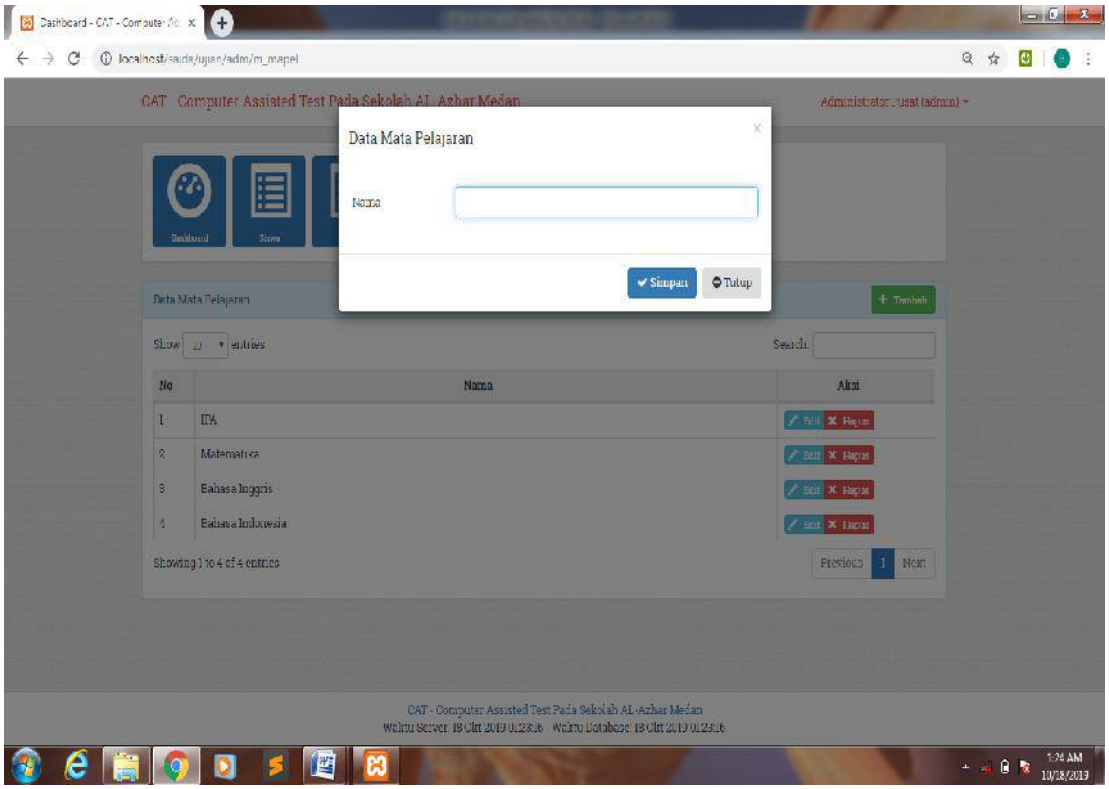


Gambar 4.4. Tampilan Data Guru

Halaman pada gambar 4.4 menjelaskan bahwa admin dapat melakukan tambah data, perbaiki data, hapus data dan dilengkapi dengan tombol batal dan keluar dari aplikasi tersebut dan user dapat melihat data yang telah masuk kedalam *database* dengan mempergunakan *grid coloum*.

4.1.5. Tampilan Form Mapel

Tampilan halaman form ini memberitahukan informasi tentang data mata pelajaran, untuk lebih jelasnya dapat dilihat pada Gambar 4.5.

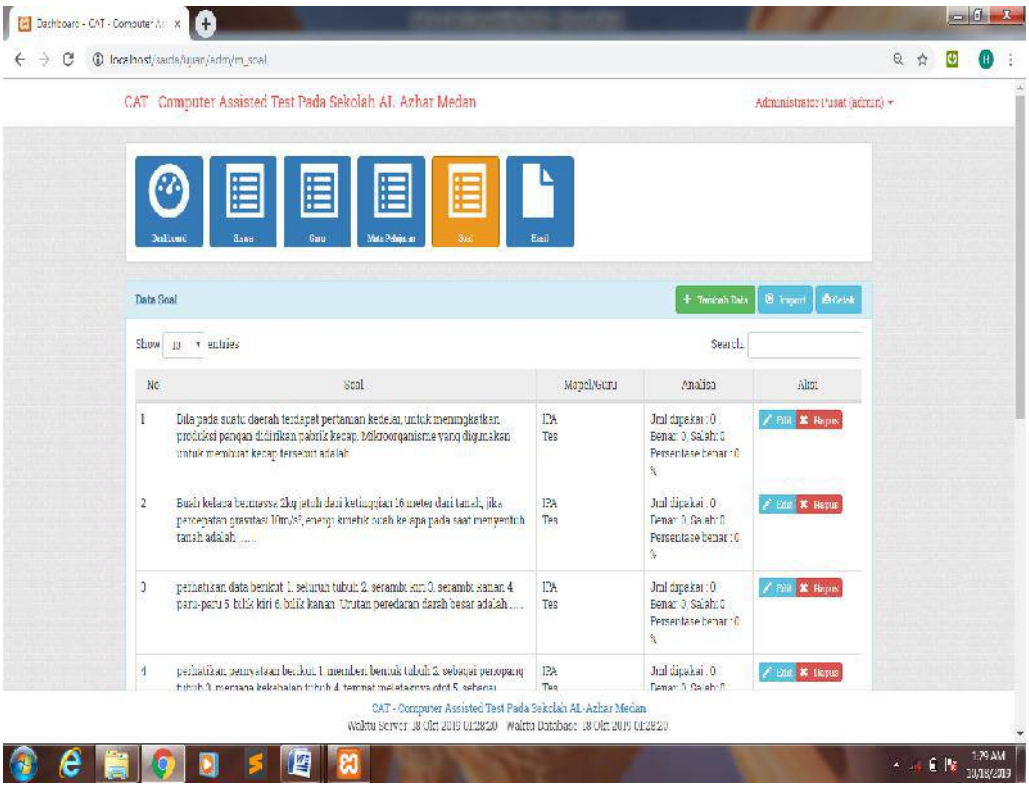


Gambar 4.5. Tampilan Form Mata Pelajaran

Halaman pada gambar 4.5 menjelaskan bahwa admin dapat melakukan tambah data, perbaiki data, hapus data dan dilengkapi dengan tombol batal dan keluar dari aplikasi tersebut dan user dapat melihat data yang telah masuk kedalam *database* dengan mempergunakan *grid coloum*.

4.1.6. Tampilan Form Soal

Tampilan halaman *form* ini memasukan soal, untuk lebih jelasnya dapat dilihat pada Gambar 4.6.

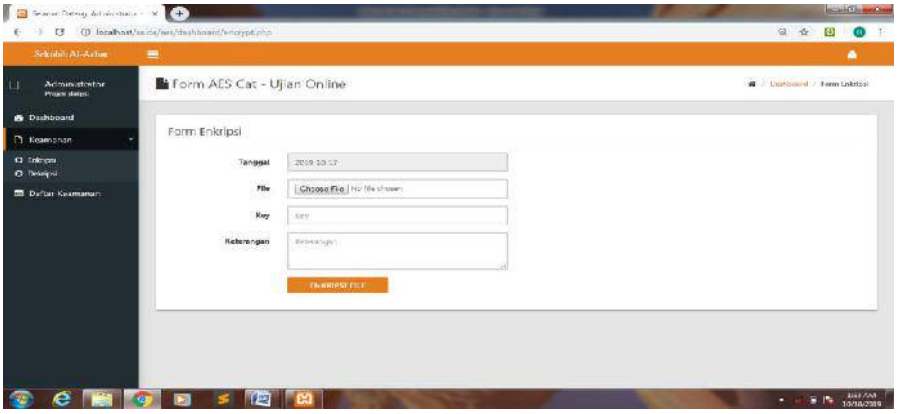


Gambar 4.6. Tampilan Form Soal

Halaman pada gambar 4.6 menjelaskan bahwa admin dapat melakukan memasukan soal baik berupa file atau langsung soal diketikan.

4.1.7. Tampilan Form Enkripsi

Tampilan halaman *form* ini memasukan file yang dienkripsikan, untuk lebih jelasnya dapat dilihat pada Gambar 4.7.



Gambar 4.7. Tampilan Form Enkripsi

Halaman pada gambar 4.7 menjelaskan bahwa admin dapat melakukan enkripsi berupa file.

Contoh perhitungan Enkripsi AES

Pesan : PANCABUDI

Key : ABCDEFGHI

Langkah – langkahnya sebagai berikut :

Tabel 4.1 Tabel Alfabert

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

· Plainteks : 15(P) 0(A) 13(N) 2(C) 0(A) 1(B) 20(U) 3(D) 8(I)

· Kunci 0(A) 1(B) 2(C) 3(D) 4(E) 5(F) 6(G) 7(H) 8(I)

· ---------- +

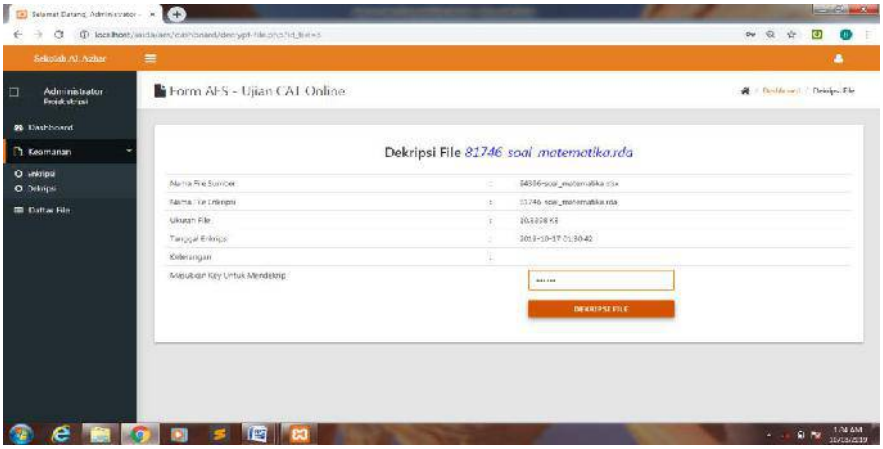
· Hasil mod 26 : 15 1 15 5 4 6 26 10 16

· Chiperteks : PBPFEGAKQ

Jadi, chiperteks yang dihasilkan dari PANCABUDI dan key ABCDEFGHI adalah PBPFEGAKQ

4.1.8. Tampilan Form Deskripsi

Tampilan halaman *form* ini mengembalikan data terenkripsi, untuk lebih jelasnya dapat dilihat pada Gambar 4.8



Gambar 4.8. Tampilan Form Deskripsi

Halaman pada gambar 4.8 menjelaskan bahwa admin dapat melakukan keamanan data berupa data terdapat di database.

Contoh Perhitungan Deskripsi AES

Chiperteks : 15(P) 1(B) 15(P) 5(F) 4(E) 6(G) 26(A) 10(K) 16(Q)

Key : 0(A) 1(B) 2(C) 3(D) 4(E) 5(F) 6(G) 7(H) 8(I)

---------- -

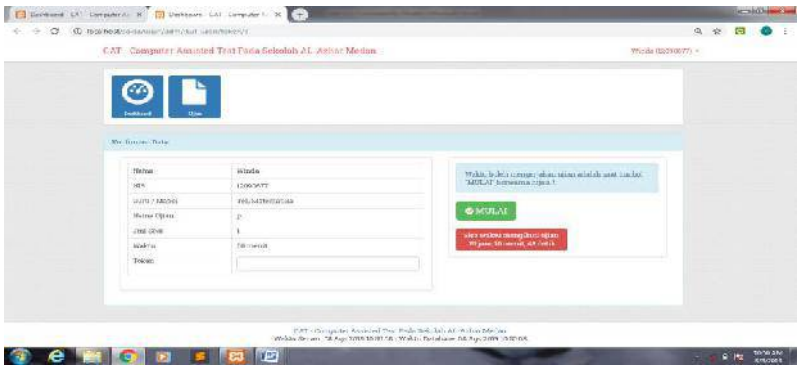
Mod 26 : 15 0 13 2 0 1 20 3 8

Plainteks : P A N C A B U D I

Jadi, Plainteks yang dihasilkan dari PBPFEGAKQ adalah PANCABUDI.

4.1.9. Tampilan Halaman Waktu Ujian

Tampilan halaman ini memberitahukan informasi tentang waktu ujian, untuk lebih jelasnya dapat dilihat pada Gambar 4.9



Gambar 4.9. Tampilan Halaman Waktu Ujian

Halaman pada gambar 4.9 menjelaskan bahwa user melakukan ujian langsung.

4.2. Pengujian

Dalam pengujian ini penulis melakukan pengujian dengan hasil aplikasi keamanan data kriptografi dengan metode AES, kemudian dari hasil tersebut dilakukan uji coba dengan berupa file pdf, dengan memunculkan data berupa *file* yang ingin di lakukan keamanan data tersebut.

4.2.1. Rencana Pengujian

Pada tahap implementasi dan pengujian terhadap keamanan data yang dirancang secara sederhana, agar *user* dapat dengan mudah melakukan keamanan data dengan cepat dan akurat.

Tabel 4.2 Skenario Pengujian Sistem

Komponen yang di uji	Pengujian	Tingkat pengujian	Jenis pengujian
Pengujian pengisian data berupa file	pengisian data user (pengguna)	Sistem	Blackbox
Pengujian Enkripsi	Pengecekan algoritma aes	Sistem	Blackbox

Tabel 4.3 Pengujian Sistem data Keamanan Data

Kasus hasil uji (Data normal)				
No	**Data masukkan**	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
1.	Data berupa file	Data berupa file yang akan dimasukan	Data berupa file yang di enkripsikan dengan metode des	[✓] diterima [] ditolak
2.	Enkripsi file	Data file yang akan di enkripsi	Data file berubah menjadi data terenkripsi	[✓] diterima [] ditolak
Kasus hasil uji (Data salah)				
No	**Data masukkan**	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
3.	Masukkan data tidak lengkap	Ada pesan bahwa pengisian data tidak lengkap	Muncul pesan bahwa pengisian data tidak lengkap	[✓] diterima [] ditolak

4.2.2. Pengujian Kasus dan Hasil

Dalam pengujian keamanan data dengan metode aes yang penulis lakukan dengan menggunakan aplikasi dokumen yang terdapat pada sistem operasi windows7. Untuk lebih jelasnya dapat dilihat pada tabel 4.3.

Tabel 4.4. Pengujian Keamanan File Metode AES

No	File Asli	File Enkripsi	Tanggal Enkripsi	Ukuran
1.	95097-6195-22295-1-pb.pdf	96272-6195-22295-1-pb.rda	2019-04-13 11:28:57	1136.71 KB
2.	40143-85-167-1-sm.pdf	54092-85-167-1-sm.rda	2019-04-01 10:39:10	626.385 KB
3.	38493-test1.txt	1129-test1.rda	2019-04-01 10:49:44	0.00976562 KB

Pada tabel 4.3. dalam pengujian keamanan data metode aes menggunakan *pdf* dengan kapasitas 1136.71 KB. Adapun hasil dari aplikasi tersebut berbeda hasil karena tergantung biner dan isi dari *file* asli tersebut.

4.3. Pembahasan

Hasil aplikasi sistem keamanan data untuk memberikan kemudahan mengenai pengamanan data dan *file*. Agar sistem keamanan data ini dapat berjalan dengan sempurna, pertama sekali harus ada *file* yang ingin di enkripsikan selanjutnya jalankan aplikasi yang penulis rancang.

4.4. Kelebihan Dan Kekurangan Sistem Yang Dirancang

Sistem yang dirancang mempunyai beberapa kelebihan dan kekurangan ketika diterapkan diantaranya :

1. Kelebihan dari sistem yang dirancang :
    a. Aplikasi sistem yang dirancang mempercepat proses keamanan data yang terdiri dari aplikasi yang berextension pdf dan teks.
    b. Mempermudah *user* dalam pengolahan data.
    c. *File* yang sudah di *enkripsi* sangat susah untuk diketahui oleh pihak-pihak yang tidak bertanggung jawab.

2. Kekurangan dari sistem yang dirancang :
    a. Tidak dapat memproteksi *file* seperti *setup.exe*.
    b. Hanya satu *file* saja yang bisa di enkripsikan.
    c. Tidak dapat mengenkripsi *file* berupa gambar

BAB V

PENUTUP

5.1. Kesimpulan

1. Dengan adanya perancangan aplikasi keamanan data tentang ujian berbasis cat disekolah yang dibuat penulis dapat meningkatan keamanan data ujian sehingga soal – soal ujian lebih sulit bocor ke siswa – siswi.
2. Dengan adanya aplikasi ini, maka siswa – siswi akan lebih serius dan giat lagi dalam belajar dan menerima pelajaran.
3. Dengan adanya aplikasi ini, maka guru – guru akan lebih mudah untuk mengawasi siswa – siswi saat ujian berlangsung.
4. Aplikasi ini mengurangi siswa – siswi mencontek saat ujian sedang berlangsung.

5.2. Saran

Untuk menyempurnakan sistem yang telah dibuat ini penulis memberikan saran:

1. Perlu adanya pengembangan dari aplikasi ini supaya tidak hanya data ujian berbasis cat yang dilakukan pengamanan data.
2. Perlu adanya pengembangan agar aplikasi dapat melakukan enkripsi terhadap dua metode yang berlainan
3. Perlu dibuat aplikasi backup data di dalam keamanan data

DAFTAR PUSTAKA

Ana Kurniawati. 2015. *Implementasi AES untuk enkripsi dan deskripsi pada dokumen teks*. Jakarta Selatan.

Arisantoso. 2017. *Penerapan aplikasi pengamanan data dengan metode enkripsi dan deskripsi algoritma 3DES dalam jaringan local area.* Jakarta Selatan.

Aulia. 2016. *Aplikasi enkripsi dan deskripsi menggunakan visual basic 2012 dengan algoritma AES.* Bandung.

Erwin Gunadhi. 2015. *Mengamankan basis data keuangan koperasi dengan menggunakan kriptografi advanced encryption standard.* Bandung.

Fachri, barany, agus perdana windarto, and ikhsan parinduri. "penerapan backpropagation dan analisis sensitivitas pada prediksi indikator terpenting perusahaan listrik." jepin (jurnal edukasi dan penelitian informatika) 5.2 (2019): 202-208.

Fachri, b., windarto, a. P., & parinduri, i. (2019). Penerapan backpropagation dan analisis sensitivitas pada prediksi indikator terpenting perusahaan listrik. Jepin (jurnal edukasi dan penelitian informatika), 5(2), 202-208.

Fachri, barany; windarto, agus perdana; parinduri, ikhsan. Penerapan backpropagation dan analisis sensitivitas pada prediksi indikator terpenting perusahaan listrik. Jepin (jurnal edukasi dan penelitian informatika), 2019, 5.2: 202-208.

Fricles Ariwisanto. 2015. *Perancangan aplikasi pengaman data dengan kriptografi aes*.

Hamdi, nurul. "model penyiraman otomatis pada tanaman cabe rawit berbasis programmable logic control." jurnal ilmiah core it: community research information technology 7.2 (2019).

Indra Saefudin. 2017. *Metode Algoritma Advanced Encryption Standar (AES)*.

Indra Suryanto. 2017. *Pengembangan aplikasi chat messenger dengan metode advanced encryption standard (aes) pada smartphone.* Garut.

Joko Susanto. 2016. *Aplikasi enkripsi dan dekripsi untuk keamanan dokumen menggunakan triple des dengan memanfaatkan usb flash drive*. Pontianak.

Khusnul Khotimah. 2016. *Pengembangan Prototipe Computer Assisted Test(CAT) menggunakan arsitektur model view controller pada Badan Kepegawaian Negara*. Jakarta.

Permana, aminuddin indra. "kombinasi algoritma kriptografi one time pad dengan generate random keys dan vigenere cipher dengan kunci em2b." (2019).

Putra, randi rian. "sistem informasi web pariwisata hutan mangrove di kelurahan belawan sicanang kecamatan medan belawan sebagai media promosi." jurnal ilmiah core it: community research information technology 7.2 (2019).

Putra, randi rian, et al. "decision support system in selecting additional employees using multi-factor evaluation process method." (2019).

Putra, randi rian. "implementasi metode backpropagation jaringan saraf tiruan dalam memprediksi pola pengunjung terhadap transaksi." jurti (jurnal teknologi informasi) 3.1 (2019): 16-20.

Rahmat Tullah. 2016. *Perancangan aplikasi kriptografi file dengan metode algoritma advanced encryption standard (AES)*.

Saputra, muhammad juanda, and nurul hamdi. "rancang bangun aplikasi sejarah kebudayaan aceh berbasis android studi kasus dinas kebudayaan dan pariwisata aceh." journal of informatics and computer science 5.2 (2019): 147-157

Sidik, a. P., efendi, s., & suherman, s. (2019, june). Improving one-time pad algorithm on shamir's three-pass protocol scheme by using rsa and elgamal algorithms. In journal of physics: conference series (vol. 1235, no. 1, p. 012007). Iop publishing.

Sitepu, n. B., zarlis, m., efendi, s., & dhany, h. W. (2019, august). Analysis of decision tree and smooth support vector machine methods on data mining. In journal of physics: conference series (vol. 1255, no. 1, p. 012067). Iop publishing.

Sholeh. 2016. *Mengamankan skrip pada bahasa pemprograman PHP dengan kriptografi BASE64.*

Tasril, v., wijaya, r. F., & widya, r. (2019). Aplikasi pintar belajar bimbingan dan konseling untuk siswa sma berbasis macromedia flash. Jurnal informasi komputer logika, 1(3).

Voni Yuniati. 2015. *Enkripsi dan Deskripsi dengan algoritma aes 256 untuk semua jenis file*.