IMPLEMANTASI ALGORITMA BLOWFISH PADA DATABASE AKADEMIK SISTEM PENILAIAN SISWA BERBASIS WEB DI SMKN 1 MIRI, SRAGEN

Egi Budi Wijayanto[1)], Ferdiansyah[2)]

Program Studi Teknik Informasi, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Jakarta Selatan 12260
E-mail :egibudiubl@gmail.com[1)], ferdiansyah@budiluhur.ac.id [2)]

ABSTRAK

Perkembangan teknologi informasi semakin maju hampir membuat segala sesuatu dapat dilakukan menggunakan internet kapanpun dan dimanapun. Termasuk dalam dunia pendidikan sekarang ini bisa dilakukan secara online. Pada dasarnya dunia internet bersifat umum dan siapa saja dapat menggunakan dan pada dasarnya tidak aman. Untuk itu diperlukan suatu keamanan sistem informasi berbasis internet yang memang harus dilakukan pada sistem yang menggunakan jaringan internet. Web sistem penilaian siswa pada SMKN 1 Miri memiliki keuntungan dari segi akses yang bisa diakses kapan saja dan dimana saja oleh siswa menggunakan smartphone pribadi. Untuk itu diperlukan keamanan mengenai data data yag diakses oleh web siswa tersebut, data data yang diakses tersebut berada dalam database yang disimpan pada server dan telah diamankan dengan kriptografi yang menggunakan algoritma blowfish. Setiap guru dan admin yang input data mengenai siswa maupun guru dilakukan tidak menggunakan web berbasis desktop yang berbeda dengan siswa, hal tersebut dilakukan untuk keamanan data yang ada dalam database, data yang diinput oleh guru dan admin tersebutlah yang akan di enkripsi didalam database. Hanya guru yang mempunyai hak akses untuk input, mengubah, dan menghapus data nilai siswa, admin mempunyai hak untuk mengubah data guru dan siswa tidak termasuk nilai siswa, siswa hanya dapat mengakses data akademiknya. Agar user dapat akses web, user harus melakukan login terlebih dahulu untuk masuk ke halaman utama web, masing masing user memiliki username dan password sendiri untuk mengakses web ini. Setiap data yang ditampilkan pada web yaitu data yang telah terdekripsi pada saat ditampilkan yang sebelumnya terenkripsi didalam database, menggunakan proses enkripsi dan dekripsi ini maka data yang diakses oleh web sudah aman.

Kata kunci : Blowfish, Database, Enkripsi, Dekripsi

1. PENDAHULUAN

1.1 Latar Belakang

Perkembangan Ilmu Teknologi Informasi saat ini semakin berkembang, dengan seiring berkembangnya teknologi saat ini proses bertukar informasi semakin mudah, dan akurat. Metode metode baru dibidang komunikasi terhadap transmisi data maupun *content* atau isi data terus dikembangkan agar bisa menyesuakan dengan berkembangnya teknologi informasi saat ini, dalam akses komunikasi via *web mobile* lebih efisien untuk mengakses transmisi data maupun *content* atau isi data.

SMK N 1 MIRI adalah sekolah yang berada daerah Kabupaten Sragen, Jawa Tengah. SMK N 1 MIRI adalah sekolah menengah kejuruan yang mempunyai banyak jurusan, Dan mempunyai jumlah siswa lebih dari 1000 siswa. SMK N 1 MIRI memiliki banyak data akademik yang bersifat rahasia yang tidak boleh diketahui oleh pihak lain yang tidak berkepentingan.

Dalam akses informasi data akademik sekolah dibutuhkan keamanan akan data data yang diakses agar data tidak dapat diakses atau diketahui oleh pihak lain yang tidak berkepentingan dan tidak mempunya hak ases data tersebut. Maka dibutuhkan keamanan yaitu dengan cara mengenkripsi *database* yang digunakan untuk penyimpanan data, kemudian dilakukan dekripsi saat data akan di tampilkan**.** *Web* sistem penilaian siswa dapat mempermudah pihak sekolah untuk memberikan informasi data akademik siswa yang bersangkutan dengan informasi tersebut. Informasi dapat diakses menggunakan *smartphone* sehingga dapat diakses dimana saja dan kapan saja. Dengan mengimplementasikan algoritma *blowfish* pada pengamanan database akademik siswa, maka data akademik siswa aman dan tidak diketahui oleh pihak yang tidak berkepentingan**.** Atas dasar uraian diatas, maka pada penulisan Tugas Akhir ini akan membahas mengenai implementasi algoritma blowfish pada database akademik sistem penilaian siswa berbasis *web* di SMKN 1 miri, sragen.

1.2 Permasalahan

Berikut ini adalah permasalahan yang ditemukan, antara lain;

a. Untuk memperoleh informasi data nilai siswa masih menggunakan sistem *offline*.
b. Bagaimana agar data akademik siswa yang dikelola oleh guru dapat disampaikan kepada siswa dengan aman dan tidak diketahui oleh pihak lain?
c. Bagaimna membuat *web* penilaian siswa dengan mengimplementasikan adalah bagaimana dalam akses data akademik siswa dan nformasi sekolah dapat diakses oleh algoritma blowfish sehingga dapaat digunakan untuk mengamankan data akaedemik siswa?

1.3 Tujuan Penulisan

Adapun tujuan penulisan tugas akhir ini adalah sebagai berikut:

a. Membuat sistem penilaian siswa berbasis *web* menggunakan keamanan pada database untuk memenuhi kebutuhan sistem akademik SMK N 1 MIRI.
b. Menyajikan layanan akses data siswa, guru dan informasi sekolah dengan *web* yang dapat digunakan perangkat *mobile* untuk siswa dan *desktop* untuk guru dan admin.
c. Membantu pihak sekolah untuk menyampaikan informasi mengenai nilai akademik siswa.

2. LANDASAN TEORI

2.1. Sistem Akademik Sekolah

Pengertian dari sistem informasi akademik sekolah adalah sebuah sistem yang digunakan untuk keperluan mengolah data Akademik sekolah dengan menerapkan teknologi *computer* baik '*hardware'* maupun *'software'*. Yang dimaksud *'hardware'* (perangkat keras) adalah peralatan seperti Komputer *(PC Computer), Printer, CD* ROM*, HardDisk,* dan sebagainya, sedangkan *'software'* (perangkat lunak) adalah program komputer yang mempergunakan *'hardware'* tersebut yang dibuat untuk memenuhi kebutuhan pengolahan data akademik sekolah. (Andi 2010). (M.Zaldi, 2015

2.2 Kriptografi

Kriptografi (*Cryptography*) berasal dari bahasa yunani, *Cyptos* artinya *secret* atau rahasia, sedangkan *graphein* berarti: *writing* atau tulisan. Sehingga kriptografi yang berarti *secret writing* atau dapat diartikan sebagai tulisan rahasia, menurut Menezes (1996): Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data. Dapat diartikan Kriptografi sebagai suatu ilmu untuk menjaga kerahasiaan suatu informasi atau data dengan metode dan teknik matematika yang mencangkup aspek *confidentiality, integrity, authentication* dan *non-repudiation.*

2.3 Algoritma Blowfish

a. Pengertian Algoritma Blowfish

Blowfish adalah algoritma kriptografi simetris *block cipher* yang dibuat oleh *Bruce Schneier, Blowfish* menyandi teks terang dalam blok-blok berukuran 64-bit menjadi blok-blok teks sandi dengan ukuran sama yaitu 64-bit. Algoritma *Blowfish* terdiri dari dua bagian yaitu pembangkitan sub-kunci (*key-expansion)* dan enkripsi data. Enkripsi data terdiri dari iterasi fungsi sederhana (*feistel Network)* sebanyak 16 kali putaran. Semua operasi adalah penambahan (*addition*) dan XOR pada variable 32-bit. *Key-expansion* mengubah kunci dapat mencapai 448 bit menjadi beberapa *array* subkunci (subkey) dengan total 4168 byte.

Algoritma *Blowfish* dikembangkan untuk memenuhi kriteria yaitu. Cepat, Kompak , Sederhana, *blowfish* hanya menggunakan operasi yang simpel yaitu penambahan (*addition*), XOR, dan penelusuran tabel (*table lookup)* pada operand 32 bit.

Keamanan yang variable, panjang kunci *blowfish* dapat bervariasi dan dapat mencapai 448 bit (56 byte). (Mohamad Natsir, 2017)

b. Bagian – Bagian Algoritma Blowfish

Blowfish termasuk dalam enkripsi *block Chiper* 64-*bit* dengan panjang kunci minimal 32-*bit* sampai 448-*bit*. Algoritma *Blowfish* terdiri atas dua bagian yaitu:(Schneier, 1996):

1) *Key-Expansion*

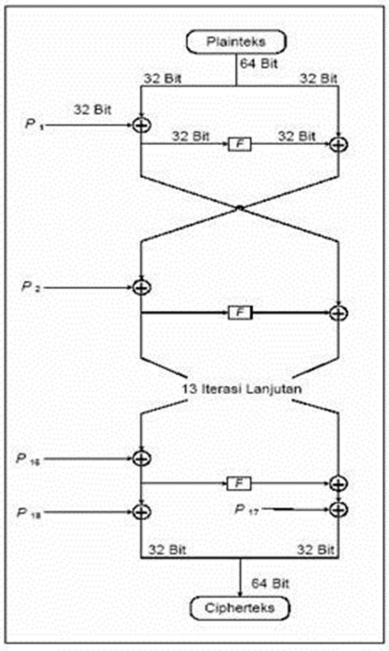
Key-Expansion mempunyai fungsi merubah kunci menjadi beberapa array subkunci r(subkey) (Sutanto, 2009).

2) *Enkripsi Data*

Enkripsi data Terdiri dari iterasi fungsi sederhana (*Feistel Network*) sebanyak 16 kali putaran. Setiap putaran terdiri atas, permutasi kunci-dependent dan subtitansi kunci dan datapendent. Semua operasi merupakan penambahan dari (*addition*) dan XOR..

c. Perhitungan Subkunci Algoritma Blowfish

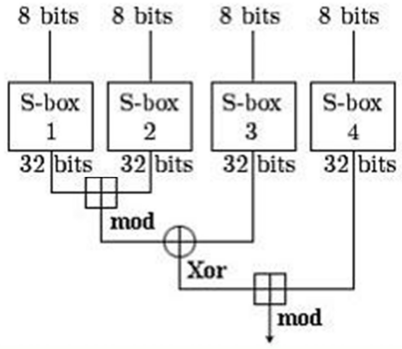
a. Awalnya inisialisasi *P-array* dan kemudian 4 *S-box* secara berurutan dengan *string* yang tetap. *String* ini terdiri dari bilangan hexadesimal dari Pi. Bilangan hexadesimal bilangan pi adalah deret bilangan, pi dalam bentuk heksadesimal (*n* = 3,243Sa8885a308d3 I3 198a2e0370344 A4093822...) yang dapat di banglatkan oleh formula Bailey-Borwien-Plouffe (Finch,1995).
b. XOR P1 dengan 32-bit pertama kunci, XOR P2 dengan 32-bit kedua dari *key,* dan seterusnya untuk setiap bitnya dari *key* (sampai P18). Ulangi terhadap bit *key* sampai seluruh P-*array* di XOR dengan bit *key*.
c. Enkripsi semua *string* nol dengan algoritma *Blowfish* dengan menggunakan *key* seperti pada langkah (a) dan (b).



Gambar 2. 1 :
Gambar Diagram Proses *Blowfish* (Sutanto, 2009)

d. Proses selanjutnya Ganti P1 dan P2 *output* dari langkah (c).
e. Selanjutnya enkrip *output* dari langkah (c) dengan algoritma *Blowfish* dengan *key* yang sudah dimodifikasi dengan *Blowfish.*.
f. Selanjutnya ganti P3 dan P4 dengan *output* dari langkah (e).
g. Proses berikutnya ganti keempat S-box berurutan. (guritman, 2003).

Berikut Gambar 2 adalah fungsi F dalam Blowfish :



Gambar 2. 2 :

Gambar Fungsi F(Feistel) (Tetuko, 2013)

Secara keseluruhan ada 521 iterasi atau putaran yang digunakan untuk membangkitkan seluruh *subKey* yang digunakan. Aplikasi dapat menyimpan subkunci yang telah dihasilkan. Proses pembangkitan *key* ini tidak harus dilakukan setiap saat.

Untuk proses dekripsi sama dengan proses enkripsi, (Sitinjak, 2010). (Tetuko Pambudi Nusa, 2013)

3. ANALISA DAN RANCANGAN PROGRAM

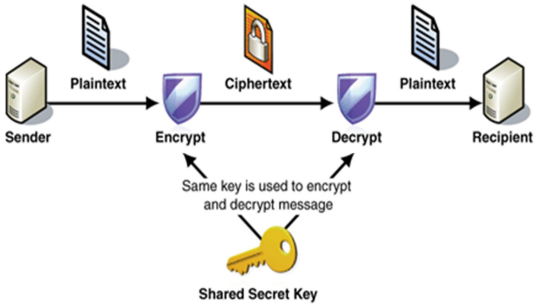
3.1 Analisa Masalah

Siswa sering kali mengeluh akan hal dalam informasi akademik mengenai dirinya, meliputi nilai, jadwal dan lain-lain. Untuk saat ini proses untuk memperoleh informasi masih dibilang sulit, siswa harus menanyakan kepada pihak sekolah untuk memperoleh informasi akademik.

SMK Negeri 1 Miri membutuhkan layanan untuk mempermudah akses data akademik mengenai siswa dan informasi sekolah yang dapat mengamankan database akademik.

3.2 Penyelesaian Masalah

Tujuan dari penelitian ini adalah membangun *web* untuk akses data akademik siswa yang menggunakan keamanan pada *database*. Enkripsi dan deskripsi *database* menggunakan algoritma *blowfish* untuk pengamanan *database*. Pada gambar 3.1 berikut adalah gambaran dari proses enkripsi dan dekripsi saat berjalan:



Gambar 3. 1 :
***Rich Picture* Proses Enkripsi dan Dekripsi**

Tahap awal dari penelitian ini mempelajari landasan teori tentang *database,* dan agoritma *Blowfish* pada studi literatur dan referensi. Teori dan referensi berupa jurnal dan dokumen lain yang berkaitan dengan peneletian ini.

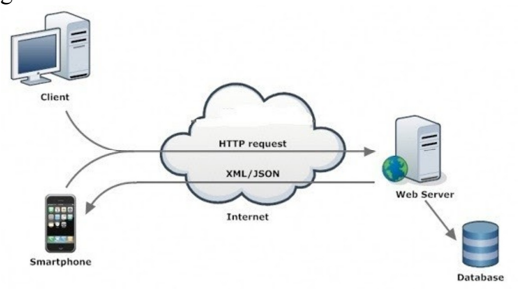
pada penelitian ini akan dibangun *web* untuk mengakses data akademik siswa yang dapat diakses siswa yang ingin mengetahui tentang perkembangan belajar akan dirinya di sekolah dengan cara mengakses *web yang* dibangun ini menggunakan *handphone* atau *semartphone* yang digunakan oleh masing masing. Data akademik siswa ini bersifat akurat karene dikelola oleh pihak sekolah, dan *database* yang di pakai di enkripsi sehingga tidak diketahui oleh pihak lain yang tidak berkepentingan.

Bagi siswa yang akan mengakses data akademik siswa pada layanan ini harus login yaitu memasukan *username* dan *password* untuk masuk pada layanan ini. dan untuk para guru dan admin

juga login yaitu memasukan *username* dan *password* agar dapat mengakses dan mengelola data yang terdapat dalam layanan ini. bagi siswa untuk login menggunakan Email sebagai *username* dan tanggal lahir sebagai *password.* bagi guru dan admin untuk login menggunakan *email* sebagai *username* dan tanggal lahir sebagai *password.* data akademik siswa yang dapat di akses atau dilihat dalam layanan ini adalah meliputi nilai, absensi, dan informasi lainya.

3.3 Arsitektur Sistem

Arsitektur Sistem untuk dapat memahami proses sistem yang dibangun, pada gambar 3.2 dibawah menjelaskan tentang proses sistem secara garis besar.



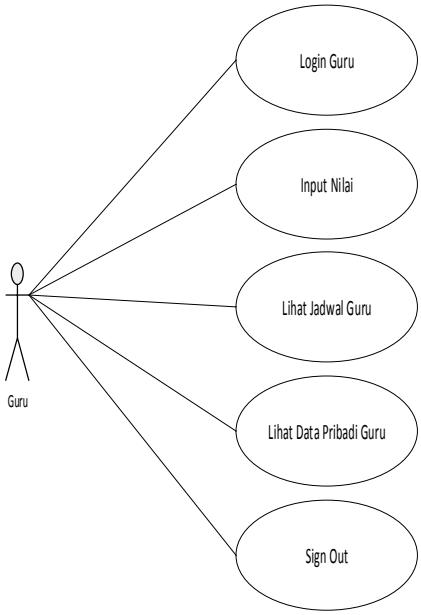
Gambar 3. 2 :
Arsitektur Sistem *Web* Akademik Sekolah

Pada *web* akademik sekolah SMK N 1 MIRI dapat diakses oleh siswa dan guru yang dikelola sekolah via *web mobile* diakses menggunakan *smartphone,* informasi yang ditampilkan adalah informasi yang telah di dekripsi yang sebelumnya telah terenkrisi di dalam *database*.

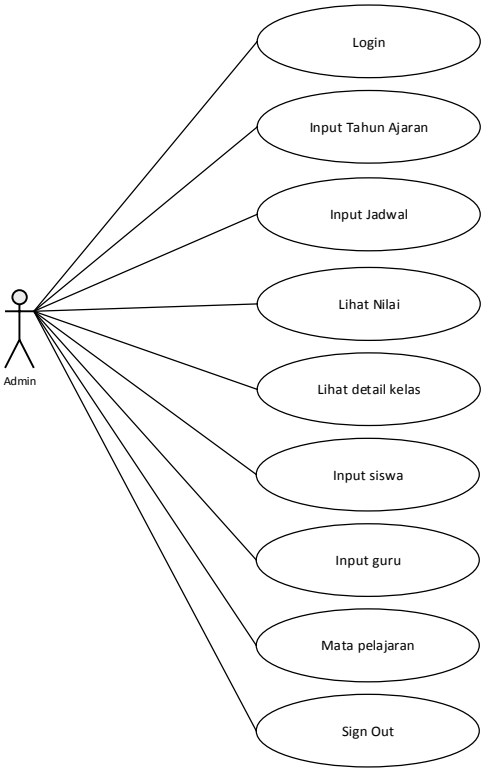
3.4 *Use Case Diagram*

Use case diagram merupakan kontruksi untuk mendeskripsikan hubungan-hubungan yang terjadi antar aktor dengan aktivitas yang terdapat pada sistem. Sasaran pemodelan *use case* diantaranya adalah mendefinisikan kebutuhan fungsional dan operasional sistem dengan mendefinisikan sekenario penggunaan sistem yang akan dibangun. Dari hasil analisa aplikasi yang ada maka *use case diagram* untuk aplikasi yang dibangun dapat dilihat pada gambar 3.3, 3.4, dan 3,5 sebagai berikut:

Gambar 3. 3 :
***Use case diagram* Siswa**



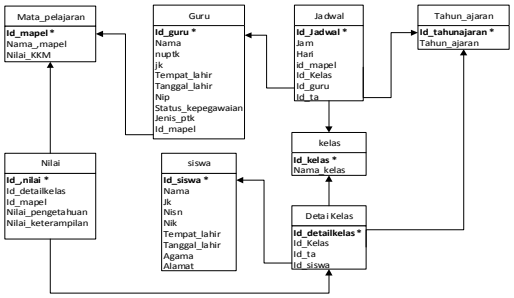
Gambar 3. 4 :
***Use case diagram* Guru**



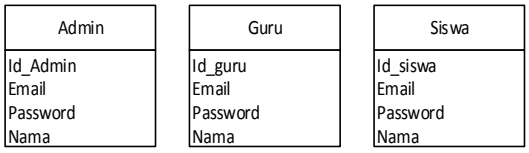
Gambar 3. 5 :
***Use case diagram* admin**

LRS (*Logical Record Structure*) Database

Berikut adalah bentuk rancangan LRS (*Logical Record Structure)* untuk *web yang* dibangun dapat dilihat pada gambar 3.6 dan 3.7 sebagai berikut:



Gambar 3. 6 :
Rancangan LRS *(Logical Record Structure)*
***Database* Utama**

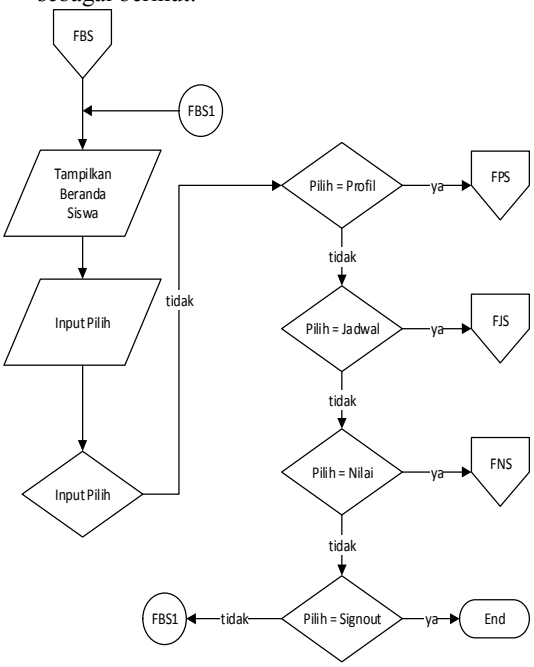


Gambar 3. 7 :
Rancangan Struktur *Database User*

3.5 *Flowchart*

a. *Flowchart* Utama Siswa

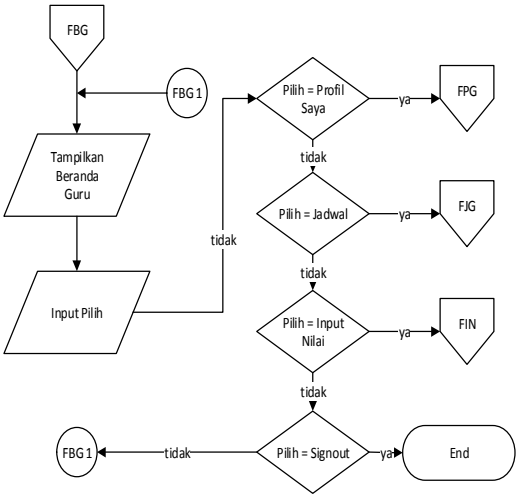
Pada *flowchart* halaman beranda siswa merupakan gambaran dari proses pada halaman beranda guru. Dapat dilihat pada gambar 3.6 sebagai berikut:



Gambar 3. 6:
***Flowchart* Halaman Beranda Siswa**

b. *Flowchart* Utama Guru

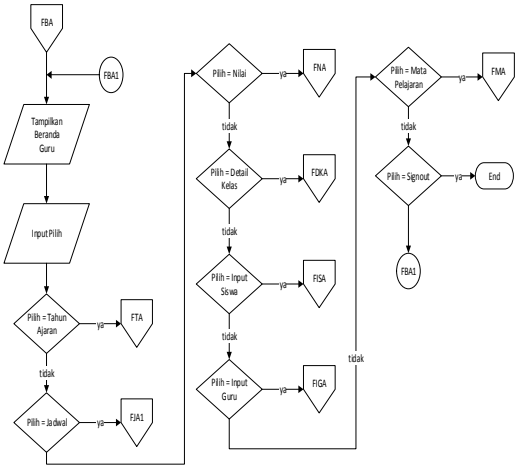
Flowchart halaman beranda guru menggambarkan alur proses pada halaman beranda dimana guru memilih proses yang selanjutnya akan di pilih. Halaman beranda merupakan halaman utama. Dapat dilihat pada gambar 3.7 sebagai berikut:



Gambar 3. 7 :
***Flowchart* Halaman Beranda Guru**

c. *Flowchart* Utama Admin

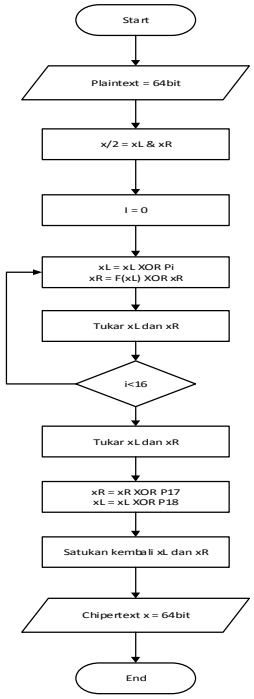
Flowchart halaman beranda admin menggambarkan alur proses pada halaman beranda dimana admin memilih proses yang selanjutnya akan di pilih. Halaman beranda merupakan halaman utama. Dapat dilihat pada gambar 3.8 sebagai berikut:



Gambar 3. 8:
***Flowchart* Halaman Beranda Admin**

d. *Flowchart* algortima blowfish

Pada *Flowchart* enkripsi algoritma *blowfish* menjelaskan alur proses enkripsi dari algoritma *blowfish* dapat dilihat pada gambar 3.9 sebagai berikut:



Gambar 3. 9:
***Flowchart* Algoritma Blowfish**

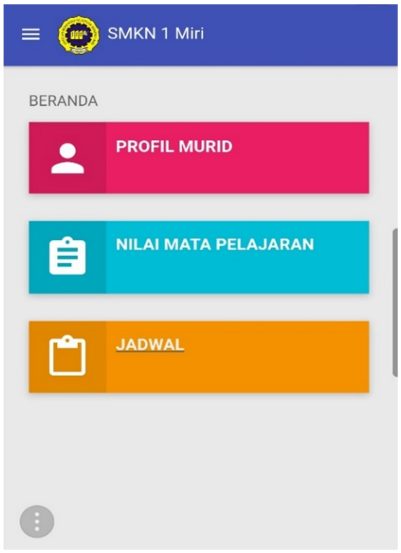
4. HASIL DAN PEMBAHASAN

4.1 Tampilan Layar

Pada tampilan layar akan dijelasakan langkah langkah dalam penggunakan aplikasi *web* dari awal hingga akhir program. Berikut adalah tampilan layar dan lagkah langkah penggunaan aplikasi *web.*

a. Tampilan Layar Halaman Beranda Siswa

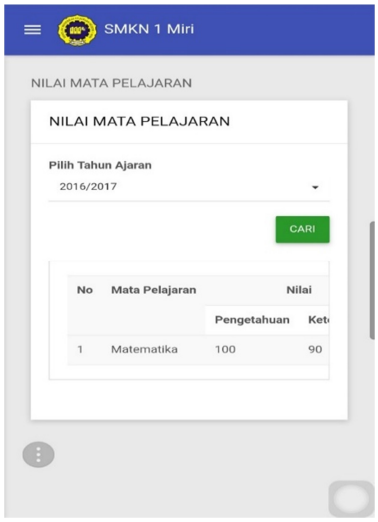
Tampilan layar beranda guru mucul setelah dilakukanya login pada halaman login siswa. Pada halaman ini terdapat menu menu yang dapat dipilih seperti profil,jadwal, nilai dan, *sign out* untuk keluar dari *username* yaitu kembai ke halaman login siswa. Dapat dilihat pada gambar 4.1 sebagai berikut:



Gambar 4. 1 :
Tampilan Layar Beranda Siswa

b. Tampilan Layar Nilai Siswa

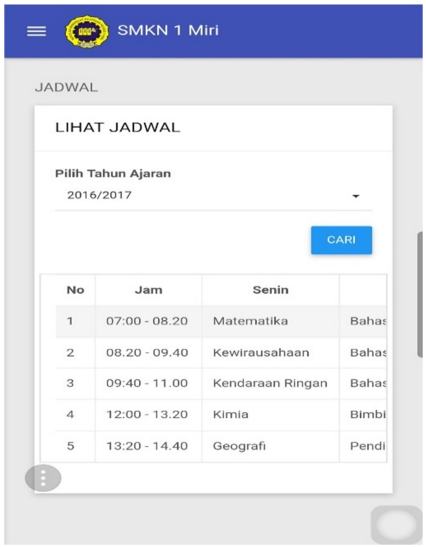
Pada tampilan layar nilai siswa adalah halaman dimana siswa bisa melihat nilai, dihalaman ini siswa memilih tahun ajaran yang akan ditampilkan nilainya. Dapat dilihat pada gambar 4.2 dibawah ini:



Gambar 4. 2 :
Tampilan Layar Halaman Nilai Siswa

c. Tampilan Layar Jadwal Siswa

Tampilan layar jadwal siswa adalah halama dimana siswa dapat melihat jadwal pelajaran, jadwal akan ditampilan setelah memilih tahun ajaran, jadwal ditampilkan sesuai tahun ajaran yang telah dipilih, dapat dilihat pada gambar 4.3 sebagai berikut:



Gambar 4. 3 :
Tampilan Layar Halaman Jadwa Siswa

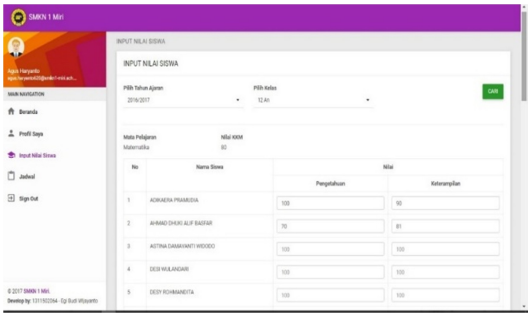
d. Tampilan Layar Beranda Guru

Apabila *user* telah memasukan *username* dan *password* secara bernar maka akan dilanjutkan ke halaman beranda. Pada tampilan layar beranda guru akan ditampilkan halaman beranda guru dimana *user* akan memilih tombol botton untuk membuka halaman selanjutnya yaitu halaman profil, jadwal, input nilai dan *Sign out*. *Sign out* adalah untuk keluar ke halaman login. Gambar 4.4 Berikut adalah tampilan layar pada halaman beranda guru:

Gambar 4. 4 :
Tampilan Layar Beranda Guru

e. Tampilan Layar Input Nilai

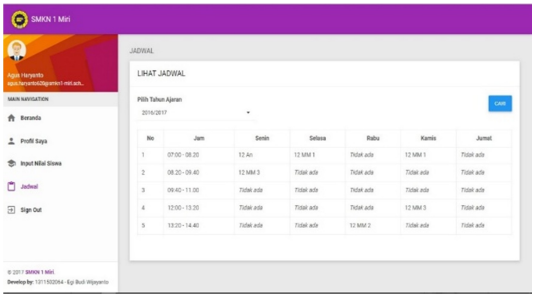
Pada tampilan layar input nilai adalah halaman dimana guru input nilai, guru harus memilih tahun ajaran, mata pelajaran, dan kelas yang akan di input nilai. Dapat dilihat pada gambar 4.5 sebagai berikut:



Gambar 4. 5 :
Tampilan Layar Input Nilai

f. Tampilan Layar Jadwal Guru

Tampilan layar jadwal guru adalah halaman dimana guru dapat melihat jadwal pelajaran, jadwal akan ditampilan setelah memilih tahun ajaran, jadwal ditampilkan sesuai tahun ajaran yang telah dipilih, dapat dilihat pada gambar 4.6 sebagai berikut:



Gambar 4. 6:
Tampilan Layar Halaman Jadwal Guru

4.2 Analisa Aplikasi

Web akademik SMKN 1 MIRI ini telah melakukan uji coba pada akun *user*, setiap yang ingin melakukan akses *web* ini maka harus melakukan login terlebih dahulu untuk bisa masuk ke halaman utama yaitu menggunakan *username* dan *password*, *password* itu sendiri telah di enkripsi sehingga menjadi cipher teks yang tidak dapat dibaca dengan mata biasa, dan juga data data yang ada didalam *database* telah di enkripsi menjadi cipher text**.**

Dari hasi pengujian yang dipaparkan, maka dapat dibuktikan *web* ini dapat mengamankan data data akademik yang dimiliki sekolah dengan enkripsi menggunakan algoritma *blowfish* pada *database* yang digunakan pada *web*. Seehingga data tidak dapat diketahui oleh pihak lain yang tidak berkepentingan.

a. Kelebihan Program

1) Setiap *user* yang ingin mengakses harus melakukan login agar dapat membuka halaman utama dari *web*.
2) Setiap *password* disimpan didalam *database* dan telah di enkripsi.
3) Semua data yang diakses aman didalam *database*.
4) *Web* untuk siswa sudah compatibe diakses menggunakan *smartphone*.

b. Kekurangan Program

1) Hanya menggunakan algoritma blowfish.
2) *Web* ini hanya baru bisa mengakses mata pelajaran, nilai, jadwal, tahun ajaran dan profil.
3) Belum ada untuk menambah kelas dan memasukan siswa ke kelas.
4) Belum dilengkapi dengan sistem ganti *password* dan lupa *password*.

5. PENUTUP

5.1 Kesimpulan

Berdasarkan proses perancangan, pembuatan, dan pengujian yang telah dilakukan mengenai implementasi algoritma *blowfish* pada *database* akademik dengan *web* di SMKN 1 Miri Sragen, maka dapat ditarik kesimpulan:

a. Sistem sekolah lebih baik dan aman dengan adanya aplikasi *web* yang dilengkapi keamanan pada *database* yang digunakan.
b. Kunci *privat* dan *public* dikirimkan ke *web.*
c. Data di enkripsi pada saat data disimpan ke dalam *database*.
d. Dekripsi dilakukan pada saat data sedang diakses.

DAFTAR PUSTAKA

[1] P. A. Q. Tetuko, "Rancang Bangun Aplikasi Enkripsi Database MYSQL Dengan Algoritma BLOWFISH," *Jurnal Manejemen Informatika,* vol. 02, no. 01, pp. 39-44, 2013.

[2] M. Natsir, "Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office Menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java," vol. 6, pp. 87-105, 2017.

[3] S. Alfian Tanggela, "Perancangan Sistem Informasi Akademik Berbasis Web pada SMA Negeri 1 Wewewa Tengah," pp. 1-7, 2013.