IMPLEMENTASI KEAMANAN DATA MENGGUNAKAN ALGORITMA *BLOWFISH* PADA SISTEM INFORMASI KOPERASI RIAS

Susanto
Program Studi Teknik Informatika
STMIK MUSIRAWAS
Email: susanto@muralinggau.ac.id

ABSTRAK

Database merupakan tempat penyimpanan data dan informasi yang harus dijaga keamanan dan kerahasiaannya. Untuk menjaga keamanan dan kerahasiaannya data yang di simpan di dalam database menggunakan kriptografi. Sistem informasi koperasi RIAS merupakan sistem yang memproses data anggota, simpanan dan peminjaman sehingga data yang tersimpan harus terjamin kerahasiaannya. Guna menjaga keamanan data pada sistem informasi koperasi RIAS, menggunakan algoritma kriptografi simetris *blowfish*. Algoritma kriptografi simetris *blowfish* merupakan algoritma modern kunci simetris berbentuk cipher blok. Kunci simetris yang digunakan untuk enkripsi dan dekripsi harus sama,sehinggauntuk mempermudah proses enkripsi dan dekripsi pada *database* yang jumlah datanya sangat banyak maka kunci *public* yang digunakan pada sistem informasi koperasi RIAS dimasukkan kedalam *source code*. Sistem informasi koperasi rias dibangun menggunakan bahasa pemrograman php dan *database* menggunakan MySQL.Berdasarkan hasil, data yang di inputkan pada sistem informasi koperasi RIAS pada *database* berhasil di enkripsi sehingga tidak dapat dibaca dan dimengerti artinya, selanjutnya data yang sebenarnya dapat ditampilkan pada menu tampil data ataupun laporan.

Kata kunci: *database*, algoritma *blowfish*, sistem informasi.

ABSTRACT

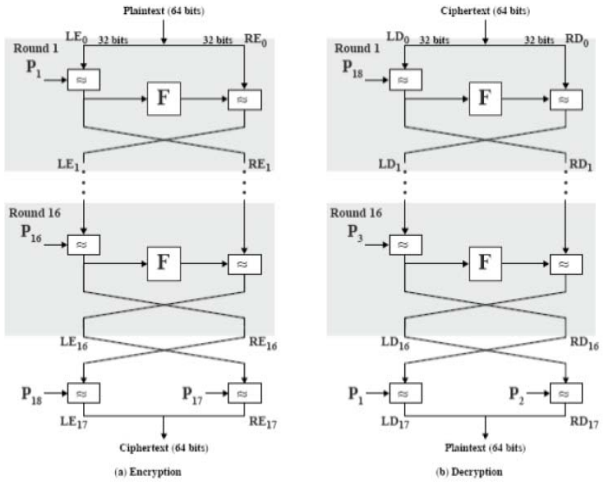
Database is a place to save data and information that have to be guarded security and secrecy. To keep security and secrecy data which is saved in database should be using cryptography. RIAS cooperative of information systems is a system which processes the data members, saving and loan so the data that stored to be guaranteed of secrecy. To keep a security data, it used symmentric cryptographic algorithms blowfish. Symmentric cryptographic algorithms blowfish is algorithms modern symmentric key shaped block chipher. The symmentrickey was used for encryption and description should be the same so that it could give easy processing for encryption and description on the database that the data was so full, thus the public key which's used at RIAS cooperative of information systemswas input at source code. RIAS cooperative of information systemswas constructed by PHP programming language and it's database by MYSQL.Based on the result, the data that's input in RIAS cooperative of information systems in database has succeed for encryption so the meaning can't be read and understood. Finally, the next real data can be showed in desktop or report.

Keywords: *database, algorithm blowfish, information systems.*

1. PENDAHULUAN

Database [10] merupakan tempat penyimpanan data dan informasi. Seluruh sistem menyimpan datanya di dalam *database*, sehingga isi data yang tersimpan harus dijaga keamanan dan kerahasiaannya. Untuk menjaga keamanan [5] *database* tersebut diperlukan sebuah metode, metode tersebut adalah kriptografi.

Kriptografi [2] merupakan teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentifikasi. Algoritma kriptografi terbagi menjadi dua yaitu algoritma simetris dan algoritma asimetris [2]. Salah satu contoh algoritma simetris adalah *blowfish*. Algoritma kriptografi simetris *blowfish* [1] merupakan algoritma modern kunci simetris berbentuk *cipher block*. Kunci simetris yang digunakan untuk proses enkripsi dan dekripsi sama seperti yang terlihat pada gambar 1.



Gambar 1. Proses Enkripsi dan Dekripsi *Blowfish*

Sistem informasi [6] koperasi RIAS merupakan sistem yang memproses data anggota, simpanan, peminjaman dan angsuran yang datanya di simpan ke dalam *database*, sehingga data yang tersimpan di dalam *database* perlu dijamin keamanan dan kerahasiaannya. untuk mempermudah proses enkripsi dan dekripsi [3] pada sistem informasi koperasi [4] RIAS yang jumlah datanya sangat banyak dan kunci yang digunakan harus sama, maka kunci publik dimasukkan kedalam *source code*. Sistem informasi koperasi RIAS dibangun menggunakan bahasa pemrograman php dan *database* menggunakan MySql.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan model *Prototyping* [9]. Peneliti menggunakan metode ini dikarenakan didalam model ini peneliti dalam merancang sistem dan membuat sistem dilakukan secara bertahap. Sehingga dapat mengurangi tingkat kesalahan. Adapun tahapan yang dilakukan dalam penelitian ini menggunakan *prototyping* [8] adalah sebagai berikut:

1) Peneliti menganalisis sistem dan keamanan sistem yang sedang berjalan. Analisa dilakukan dengan cara wawancara dengan pimpinan dan meninjau langsung sistem informasi koperasi yang sudah ada.
2) Peneliti mulai membangun sistem dan keamanannya. Sistem informasi dibangun menggunakan bahasa pemrograman PHP dan basis datanya menggunakan MySQL, serta menggunakan algoritma *blowfish* membangun keamanan datanya.
3) Peneliti dan pihak Koperasi RIAS menguji sistem yang sudah dibuat dan memberikan masukan terhadap sistem baru tersebut. Pengujian sistem ini menggunakan metode *blackbox testing.*
4) Jika sistem dan kemananannya sudah tepat maka siap di implementasikan.

3. HASIL DAN PEMBAHASAN

Implementasi keamanan data menggunakan algoritma *blowfish* pada sistem informasi koperasi RIAS yang merupakan hasil penelitian ini meliputi:

3.1 Analisis Sistem

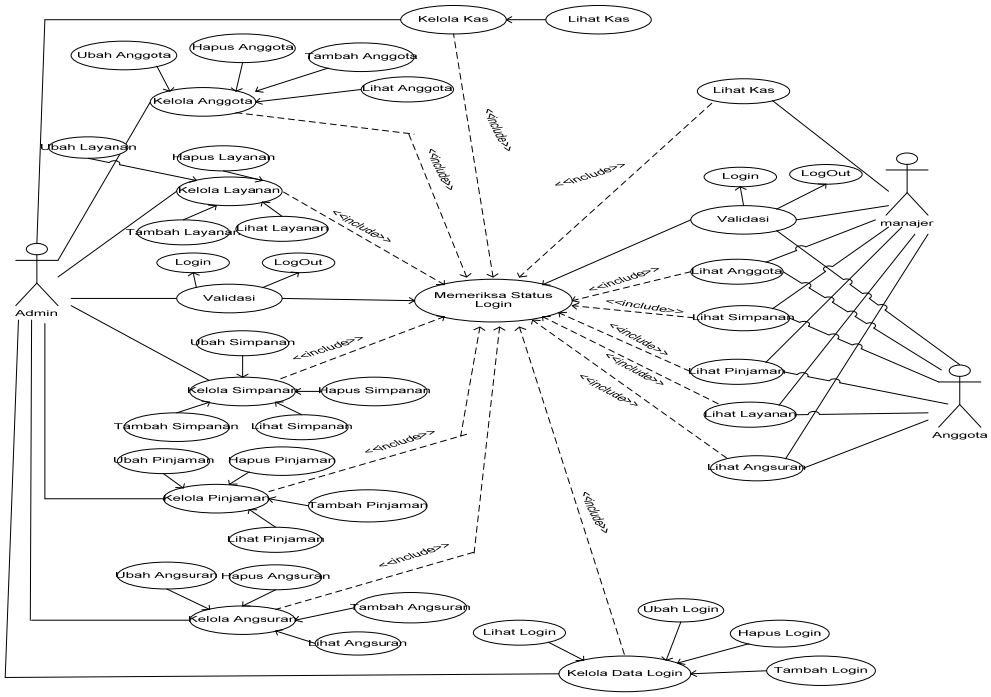
Proses analisis sistem dimulai dengan menganalisa sistem informasi yang sudah ada. Proses analisis ini dilakukan dengan wawancara secara langsung dengan karyawan dan pimpinan Koperasi RIAS, setelah itu dilanjutkan dengan pengecekan langsung sistem yang lama dengan melihat isi data di dalam *database.*

3.2 Membangun Sistem dan Keamanannya

Proses membangun sistem dimulai dengan merancang sistem yang dibantu dengan diagram bantu menggunakan *use casediagram* dan *class diagram*, dilanjutkan dengan merancang *database* menggunakan MySQL yang digunakan untuk menyimpan data. Setelah selesai merancang sistem, dilanjutkan dengan merancang antar muka sistem informasi dan membuat algoritma *blowfish*.

1) Use case diagram

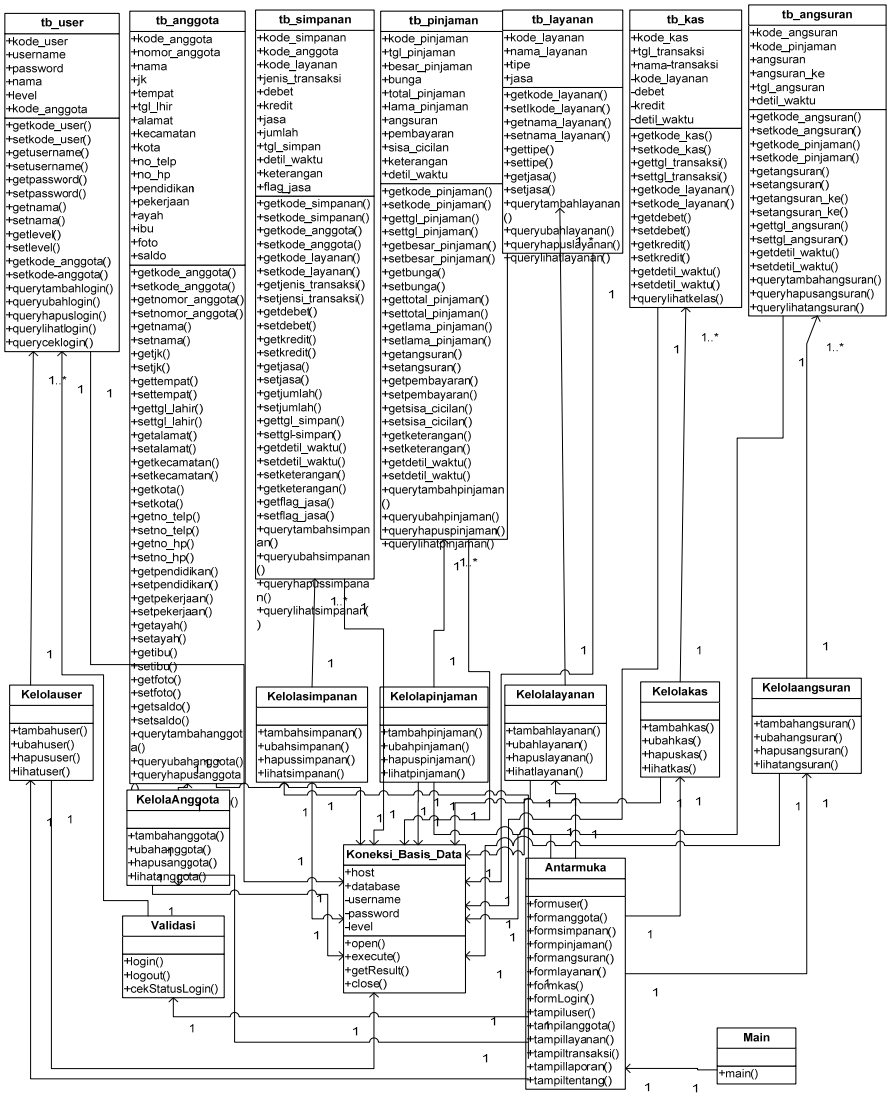
Use case diagram berfungsiuntuk menggambarkan dan memodelkan serta mengorganisasi pada sistem sistem informasi koperasi RIAS, dimana pembuatan diagram ini terdiri dari 3 aktor yaitu admin, anggota dan manajer. Sehingga apa yang diperbuat oleh aktor tersebut pada sistem infomasi koperasi terlihat dengan jelas yang disajikan pada gambar 2.



Gambar 2. ***Use Case Diagram***

2) Class diagram

Class diagram berfungsi untuk menjelaskan hubungan antar *class* pada sistem informasi koperasi RIAS. *Class diagram*tersebut disajikan pada gambar 3.



Gambar 3. Class Diagram

3) Database

Rancangan *database* yang dibuat antara lain

a. Tabel *user*
b. Tabel anggota
c. Tabel simpanan
d. Tabel pinjaman
e. Tabel angsuran
f. Tabel kas
g. Tabel layanan
h. Tabel pengaturan profil

4) Antar muka

Antarmuka pada sistem informasi koperasi terdiri dari level admin, level anggota dan level pimpinan. Rancangan antar muka yang akan dibuat antara lain :

a. Halaman *login.*
b. Halaman data anggota yang terdiri dari tampil data anggota, tambah data anggota, detail data anggota, ubah data anggota, hapus data anggota, cetak data anggota dan pencarian data anggota.
c. Halaman produk layanan yang terdiri dari tampil data produk layanan, tambah data produk layanan dan ubah data produk layanan.

d. Halaman transaksi yang terdiri dari sub menu simpanan yaitu tampil data simpanan, detail simpanan, tambah data simpanan, pencarian data simpanan; sub menu pinjaman yaitu tambah data pinjamanan, detail data pinjaman, angsuran dan pencarian data pinjaman; sub menu kas yaitu tampil data kas.
e. Halaman data *user* yang terdiri dari tampil data *user*, tambah data *user*, ubah data *user* dan hapus data *user*.
f. Halaman pengaturan profil.

5) Algoritma *Blowfish*

Pada dasarnya, algoritma enkripsi *blowfish* membutuhkan 32 bit mikroprosesor pada tingkat satu *byte* untuk setiap 26 siklus *clock*. *Blowfish* berisi 16 putaran. Setiap putaran terdiri dari XOR operasi dan fungsi. Setiap putaran terdiri dari ekspansi kunci dan enkripsi data. Kunci ekspansi umumnya digunakan untuk menghasilkan isi dari satu *array* dan enkripsi data menggunakan 16 putaran *feiestel* metode jaringan. Gambar 1 menunjukkan algoritma bagaimana *blowfish* bekerja. teks dan kunci biasa adalah masukan dari algoritma. 64 bit *plaintext* diambil dibagi menjadi dua masing-masing 32 bit data dan di setiap putaran kunci yang diberikan diperluas dan disimpan dalam 18 *array* dan memberikan kunci 32 bit sebagai *input* dan XOR dengan data sebelumnya.

Kemudian, untuk i = 1 sampai 14:

xL = xL XOR Pi

xR = F (xL) XOR xR

Swap xL dan xR

Setelah putaran keenam belas, pertukaran xL dan xR lagi untuk mengembalikan kembali ke*swap* terakhir. Kemudian, xR = xR XOR P15 dan xL = xL XOR P16. Akhirnya, bergabung kembali XL dan xR untuk mendapatkan *ciphertext*.

Sehingga jika algoritma *blowfish* dituangkan kedalam *source code* PHP menjadi sebagai berikut :

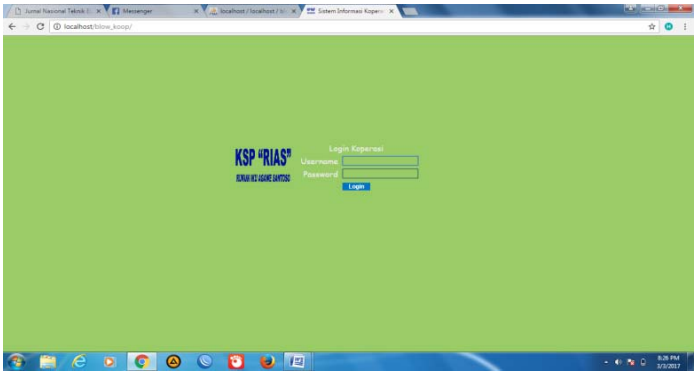
```
<?php
class Cipher {
     private $algo;
     private $mode;
     private $source;
     private $iv = null;
     private $key = null;
     public   function   __construct($algo   =   MCRYPT_BLOWFISH,   $mode   =
MCRYPT_MODE_CBC, $source = MCRYPT_RAND) {
        $this->algo = $algo;
        $this->mode = $mode;
        $this->source = $source;
        if (is_null($this->algo) || (strlen($this->algo) == 0)) {
            $this->algo = MCRYPT_BLOWFISH;
        }
        if (is_null($this->mode) || (strlen($this->mode) == 0)) {
            $this->mode = MCRYPT_MODE_CBC;
        }
    }
     public function encrypt($data, $key = null, $iv = null) {
        $key = (strlen($key) == 0) ? $key = null : $key;
        $this->setKey($key);
        $this->setIV($iv);
        $out = mcrypt_encrypt($this->algo, $this->key, $data, $this->mode,
$this->iv);
        return base64_encode($out);
    }
     public function decrypt($data, $key = null, $iv = null) {
        $key = (strlen($key) == 0) ? $key = null : $key;
        $this->setKey($key);
        $this->setIV($iv);

        $data = base64_decode($data);
        $out = mcrypt_decrypt($this->algo, $this->key, $data, $this->mode,
$this->iv);
        return trim($out);
    }
     public function getIV() {
        return base64_encode($this->iv);
    }
     private function setIV($iv) {
```

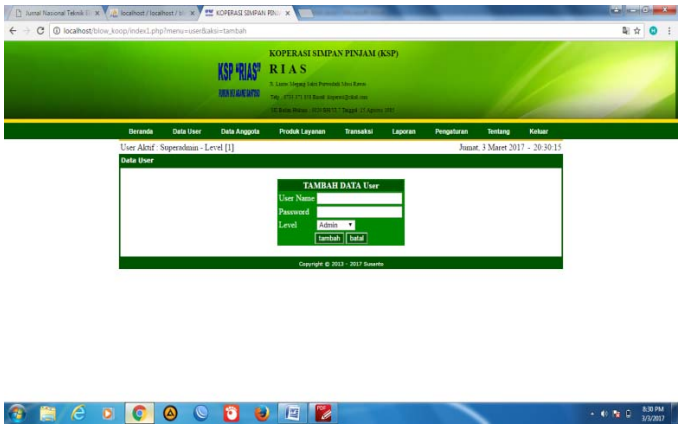
```
            if (!is_null($iv)) {
                $this->iv = base64_decode($iv);
            }
            if (is_null($this->iv)) {
                $iv_size = mcrypt_get_iv_size($this->algo, $this->mode);
                $this->iv = mcrypt_create_iv($iv_size, $this->source);
            }
        }
         private function setKey($key) {
            if (!is_null($key)) {
                $key_size = mcrypt_get_key_size($this->algo, $this->mode);
                $this->key = hash("sha256", $key, true);
                $this->key = substr($this->key, 0, $key_size);
            }
            if (is_null($this->key)) {
                trigger_error("You must specify a key at least once in either
    Cipher::encrpyt() or Cipher::decrypt().", E_USER_ERROR);
            }
        }
    }
    ?>
```

3.3 Implementasi dan Pengujian Keamanan Data pada Sistem

Implementasi bertujuan untuk mengkonfirmasi hasil perancangan sistem informasi yang telah dilakukan, sehingga pengguna dapat memberi masukanpada pengembangan sistem informasi. implementasisistem informasi koperasi RIAS dilakukan dengan bahasa pemrograman PHP dan MySQL sebagai *Database Management System*.Pengujian keamanan data pada sistem informasi koperasi RIAS dapat terlihat pada gambar 4 sampai dengan gambar 22, data yang tersimpan didalam *database* yang terenkripsi dan terdekripsi ke bentuk semula terlihat pada form tampilan data.

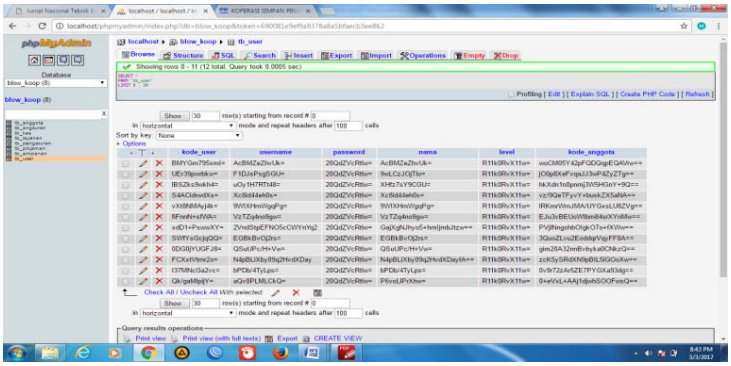


Gambar 4. Form Login



Gambar 5. Form Tambah Data User

Halaman tambah data *user*ini digunakan untuk memasukkan data *user* yang akan menggunakan sistem informasi koperasi RIAS.



Gambar 6. Database Data User

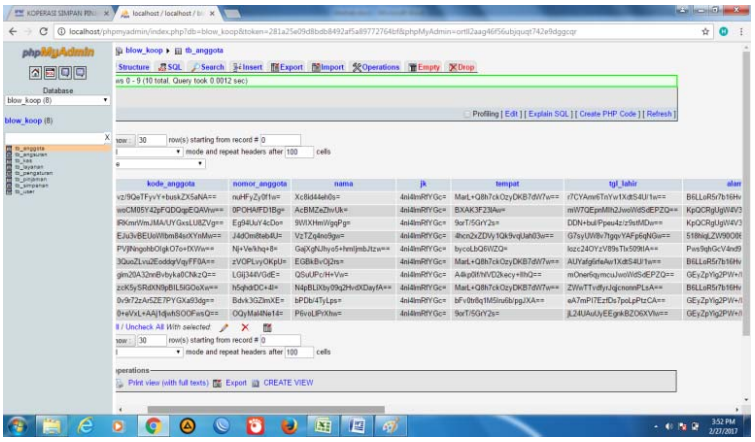
Data yang telah di masukan pada form tambah data anggota akan tersimpan pada *database* data *user*. Data yang tersimpan tersebut terenkripsi.

Gambar 7. Tampilan Data User

Pada halaman tampilan data *user*ini menampilkan seluruh informasi data *user*, informasi data *user* yang di tampilkan telah terdekripsi ke bentuk aslinya sehinnga dapat dimengerti isinya.

Gambar 8 Form Tambah Data Anggota

Halaman tambah data anggota ini digunakan untuk memasukkan data diri setiap anggota koperasi RIAS.



Gambar 9. Database Data Anggota

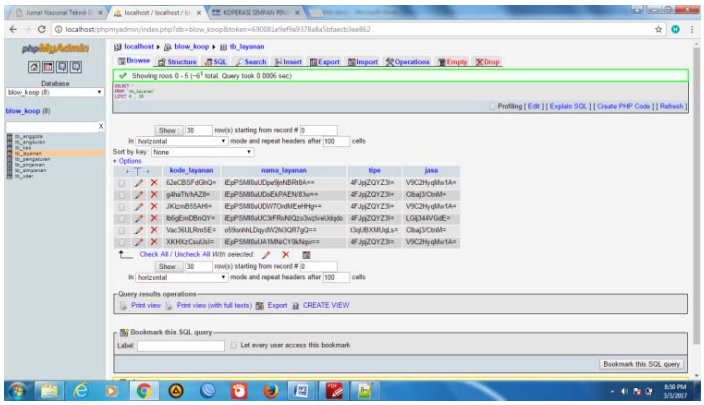
Data yang telah di masukkan pada *form*tambah data anggota akan tersimpan pada *database* data anggota. Data yang tersimpan tersebut terenkripsi.

Gambar 10. Tampilan Data Anggota

Pada halaman tampilan data anggota ini menampilkan seluruh informasi data anggota, informasi data anggota yang di tampilkan telah terdekripsi ke bentuk aslinya sehinnga dapat dimengerti isinya.

Gambar 11. Form Tambah Data Layanan

Halaman tambah data layanan ini digunakan untuk memasukkan data layanan yang terdapat pada sistem informasi koperasi RIAS.

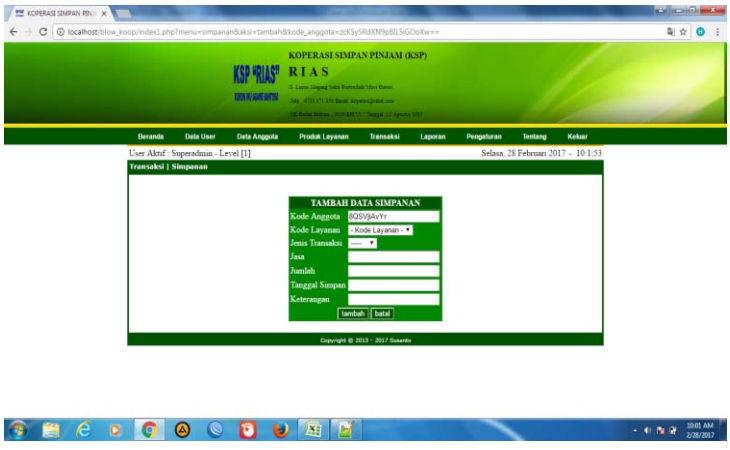


Gambar 12. Database Data Anggota

Data yang telah di masukkan pada *form*tambah data layanan akan tersimpan pada *database* data layanan. Data yang tersimpan tersebut terenkripsi.

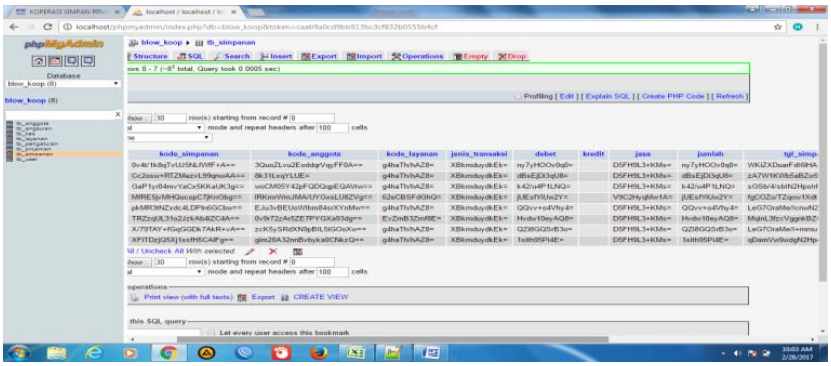
Gambar 13. Tampilan Data Layanan

Pada halaman tampilan data layanan ini menampilkan seluruh informasi data layanan, informasi data layanan yang di tampilkan telah terdekripsi ke bentuk aslinya sehinnga dapat dimengerti isinya.



Gambar 14. Form Tambah Data Anggota

Halaman tambah data simpanan anggota ini digunakan untuk memasukkan data simpanan anggota koperasi RIAS.



Gambar 15. Database Data Simpanan

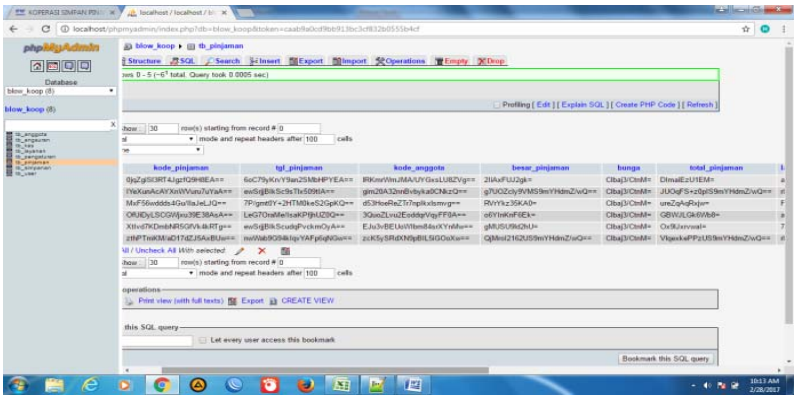
Data yang telah di masukkan pada form tambah data simpanan akan tersimpan pada *database* simpanan anggota. Data yang tersimpan tersebut terenkripsi.

Gambar 16. Tampilan Data Simpanan Anggota

Pada halaman tampilan data simpanan anggota ini menampilkan seluruh informasi data simpanan anggota, informasi data simpanan anggota yang di tampilkan telah terdekripsi ke bentuk aslinya sehinnga dapat dimengerti isinya.

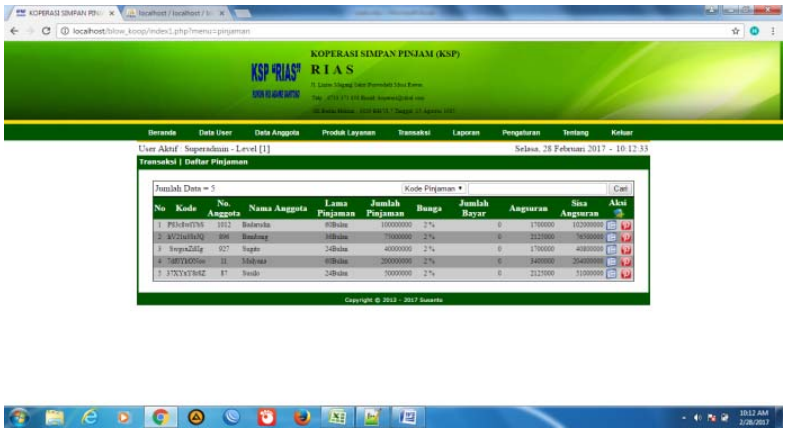
Gambar 17. Form Tambah Data Pinjaman Anggota

Halaman tambah data pinjaman anggota ini digunakan untuk memasukkan data pinjaman anggota koperasi RIAS.



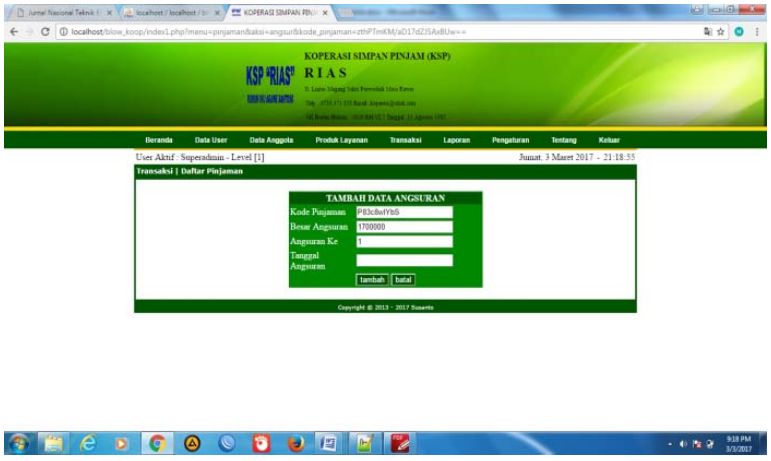
Gambar 18. Database Data Pinjaman Anggota

Data yang telah di dimasukkan pada *form*tambah data pinjaman anggota akan tersimpan pada *database* data pinjaman anggota. Data yang tersimpan tersebut terenkripsi.



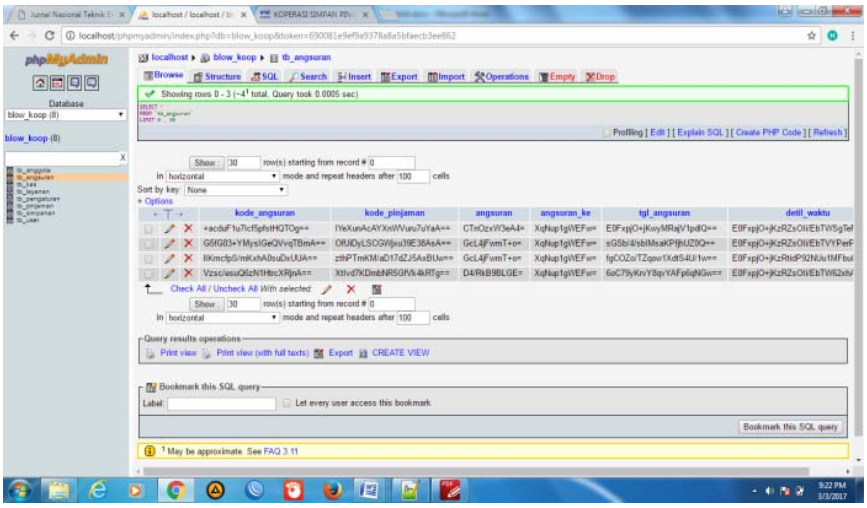
Gambar 19. Tampilan Data Pinjaman Anggota

Pada halaman tampilan data pinjaman anggota ini menampilkan seluruh informasi data pinjaman anggota, informasi data pinjaman anggota yang di tampilkan telah terdekripsi ke bentuk aslinya sehinnga dapat dimengerti isinya.



Gambar 20. Form Tambah Data Angsuran Pinjaman

Halaman tambah data angsuran pinjaman anggota ini digunakan untuk memasukkan data angsuran pinjaman anggota koperasi RIAS.



Gambar 21. Database Data Angsuran Pinjaman

Data yang telah di dimasukkan pada *form*tambah data angsuran pinjaman anggota akan tersimpan pada *database* data angsuran pinjaman anggota. Data yang tersimpan tersebut terenkripsi.

Gambar 22. Tampilan Data Angsuran Pinjaman Anggota

Pada halaman tampilan data angsuranpinjaman anggota ini menampilkan seluruh informasi data angsuranpinjaman anggota, informasi data angsuranpinjaman anggota yang di tampilkan telah terdekripsi ke bentuk aslinya sehinnga dapat dimengerti isinya.

Pengujian keamanan data pada sistem informasi koperasi RIAS dilakukan dengan metode *Black Box Testing*[11] yang merupakan proses pengujian yang fokus pada proses masukan dan keluaran pada saat sistem informasi dijalankan. Penggunaan metode *Black Box Testing* pada tahap ini karena bertujuan untuk mengetahui sejauh mana keamanan data program dapat memenuhi kebutuhan (*requirement*) yang disebutkan dalam analisis pengguna. Pada pengujian keamanan data pada sistem informasi koperasi RIAS ini dilakukan proses pengujian sebagai berikut:

1) Halaman data *user,* dilakukan proses pengujian antara lain dengan memasukkan data pada *form* tambah data *user* kemudian melihat isi data yang terenkripsi pada *database* serta melihat data yang terdekripsi pada tampil data *user*

2) Halaman data anggota, dilakukan proses pengujian antara lain dengan memasukkan data pada *form* tambah data anggota kemudian melihat isi data yang terenkripsi pada *database* serta melihat data yang terdekripsi pada tampil data anggota
3) Halaman data simpanan, dilakukan proses pengujian antara lain dengan memasukkan data pada *form* tambah data simpanan kemudian melihat isi data yang terenkripsi pada *database* serta melihat data yang terdekripsi pada tampil data simpanan
4) Halaman data pinjaman, dilakukan proses pengujian antara lain dengan memasukkan data pada *form* tambah data pinjaman kemudian melihat isi data yang terenkripsi pada *database* serta melihat data yang terdekripsi pada tampil data pinjaman
5) Halaman data layanan, dilakukan proses pengujian antara lain dengan memasukkan data pada *form* tambah data layanan kemudian melihat isi data yang terenkripsi pada *database* serta melihat data yang terdekripsi pada tampil data layanan.
6) Halaman data angsuran, dilakukan proses pengujian antara lain dengan memasukkan data pada *form* tambah data angsuran kemudian melihat isi data yang terenkripsi pada *database* serta melihat data yang terdekripsi pada tampil data angsuran.

Sistem informasi koperasi yang diusulkan pada makalah ini memiliki beberapa perbedaan dengan sistem informasi koperasi yang lain yang sudah pernah dibuat, di antaranya adalah sistem informasi simpan pinjam karyawan [12], sistem informasi koperasi simpan pinjam bahtera [13]. Sedangkan pada sistem informasi yang diusulkan, data yang disimpan didalam *database*adalah terenkripsi. Pada sistem informasi simpan pinjam karyawan dan sistem informasi koperasi simpan pinjam bahtera, semua data yang tersimpan di dalam *database* tidak terenkripsi atau dalam bentuk yang aslinya [12] [13].

4. KESIMPULAN

Berdasarkan keseluruhan pengujian yang telah dilaksanakan, data yang di inputkan pada sistem informasi [7] koperasi RIAS dan di simpan di dalam *database* berhasil di enkripsi sehingga tidak dapat dibaca dan dimengerti artinya. Sistem informasi koperasi RIAS juga telah berhasil mengembalikan data yang sebenarnya pada menu tampil data ataupun laporan.

Sistem-sistem yang dibangun sebelumnya hanya menyimpan data pada *database* dengan bentuk sesuai dengan apa yang di*input*, sehingga orang yang melihat isi *database* tersebut dapat membaca dan mengerti artinya.

DAFTAR PUSTAKA

[1] Manku, Saikumar and Vasanth,K. 2015. "Blowfish Encryption Algorithm For Information Security." *ARPN Journal of Engineering and Applied Sciences*, vol. 10. no. 10, 4717 – 4719.
[2] Basri.2016. "Kriptografi Simetris Dan Asimetris Dalam Perspektif Keamanan Data Dan Kompleksitas Komputasi." *Jurnal Ilmiah Ilmu Komputer*, vol. 2. no. 2, 17 – 23.
[3] Primartha, Rifkie. 2011. "Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES)." *Jurnal Sistem Informasi (JSI)*, vol. 3. no. 2, 371 – 387.
[4] Andriani, Anik. 2015. "Perancangan Sistem Informasi Deteksi Kegagalan Koperasi Di Tingkat Provinsi Berbasis Algoritma C4.5." *J. Nas. Tek. Elektro Dan Teknol. Inf. JNTETI*, vol. 4. no. 1, 25 – 31.
[5] Manuaba, Ida Bagus Verry Hendrawan, et al. 2012. " Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus : Kantor Pusat Fakultas Teknik Universitas Gadjah Mada)." *J. Nas. Tek. Elektro Dan Teknol. Inf. JNTETI*, vol. 1, no. 1, 13 – 17.
[6] Kodarisman, Raden and Nugroho, Eko. 2013. "Evaluasi Penerapan Sistem Informasi Manajemen Kepegawaian (SIMPEG) di Pemerintah Kota Bogor." *J. Nas. Tek. Elektro Dan Teknol. Inf. JNTETI*, vol. 2. no. 2, 24 – 32.
[7] Iskandar, Dadang and Insap Santosa, P.2013. "Sistem Informasi Gardu Induk dan Gardu Distribusi berbasis Web." *J. Nas. Tek. Elektro Dan Teknol. Inf. JNTETI*, vol. 2. no. 2, 33 - 37
[8] Novaliendry, Dony. 2011. "Multimedia Pembelajaran Bahasa Mandarin Dan Website Promosi," Jurnal Teknologi Informasi & Pendidikan, vol. 3. no. 1, 122 - 139
[9] Rosmala, Dewi, et al. 2012. "Implementasi Aplikasi Website E-Commerce Batik Sunda Dengan Menggunakan Protokol Secure Socket Layer (Ssl)." *Jurnal Informatika*, vol. 3. no. 3, 58 – 67.
[10] Ali, Achmad Holil Noor and Hutagalung, Alexander Farady. 2013. " Rancang Bangun Sistem Informasi Manajemen Dealer, Studi Kasus PT Telkomsel," *SISFO-Jurnal Sistem Informasi*, vol. 2. no. 1, 23 – 28.
[11] A.S, Rosa, Salahuddin. (2014). *Rekayasa Perangkat Lunak*. Bandung Indonesia: Informatika.

[12] Puspitasari, Diah.2015. ”Rancang Bangun Sistem Informasi Koperasi Simpan Pinjam Karyawan Berbasis Web.” *Jurnal Pilar Nus Mandiri*, vol. xi. no. 2, 186 - 196.
[13] Wijaya, Kristanto. 2015. ”Rancang Bangun Sistem Informasi Simpan Pinjam Pada Credit Union Koperasi Simpan Pinjam Bahtera Dengan Fitur Nilai Rekomendasi Pemberian Pinjaman Berbasis Fuzzy.” *Jurnal Sistem dan Teknologi Informasi. JustIN*, vol. 2. no. 1, 1-6.