ISSN 2337-6805

RANCANG BANGUN APLIKASI ENKRIPSI DAN DEKRIPSI PADA DATABASE SQL PERMIKOMAS MENGGUNAKAN ALGORITMA BLOWFISH

DESIGN AND DEVELOPMENT OF AN ENCRYPTION AND DECRYPTION APPLICATION FOR THE SQL PERMIKOMAS DATABASE USING THE BLOWFISH ALGORITHM

Ardi Juliardi[1] Siti Madinah Ladjamuddin[2]
[1,2] Program Studi Teknik Informatika, Fakultas Sains dan Teknologi Informasi
Institut Sains dan Teknologi Nasional
ardijuliardi24@gmail.com[1] , citymadinah07@istn.ac.id[2]

ABSTRAKS
Untuk menjaga keamanan data ataupun informasi yang tersimpan dalam database SQL adalah dengan menggunakan enkripsi. Ada banyak algoritma enkripsi yang ada dan salah satunya adalah algoritma Blowfish. Algoritma Blowfish merupakan algoritma modern kunci simetris berbentuk chiperblock. Enkripsi dilakukan dengan menggunakan kunci tertentu, sehingga menghasilkan chipertext yang tidak bisa dibaca. Chipertext tersebut dapat dikembalikan seperti semula jika didekripsi menggunakan kunci yang sama. Algoritma Blowfish memiliki 16 putaran dan masukan berupa data 448 bit. Bagi data 448 bit tersebut menjadi 2 bagian XL dan XR yang masing-masing 224 bit, selanjutnya lakukan operasi XL = XL xor Pi dan XR = F(XL) xor XR, kemudian tukar XL dan XR, lakukan proses sebanyak 16 kali. Pada proses ke-17 lakukan operasi untuk XR = XR xor P17 dan XL = XL xor P18, kemudia satukan kembali XL dan XR sehingga menjadi 448 bit kembali sehingga menghasilkan chipertext. Dari penggunaan algoritma Blowfish ini membuat data dari database SQL yang meliputi database, table, field, dan record tidak dapat terbaca karena telah terenkripsi, sehingga hanya user tertentu yang dapat membaca isi dari database dengan cara mendekripsinya.
Kata Kunci : Algoritma Blowfish, enkripsi, dekripsi, kunci simetris.

ABSTRACT
To maintain the security of data or information stored in the SQL database is to use encryption. There are many existing encryption algorithms and one of them is the Blowfish algorithm. Blowfish algorithm is a modern algorithm of symmetrical keys in the form of chiperblock. Encryption is done by using a certain key, resulting in an unreadable chipertext. The chipertext can be returned as if it were decrypted using the same key. Blowfish algorithm has 16 rounds and input is 448 bit data. Divide the 448 bit data into 2 parts XL and XR each 224 bit, then do XL = XL Xor Pi and XR = F (XL) xor XR, then exchange XL and XR, do the process 16 times. In the 17th process do the operation for XR = XR xor P17 and XL = XL xor P18, then reconnect XL and XR so that it becomes 448 bits back to produce a chipertext. The use of Blowfish algorithm makes data from SQL databases that include databases, tables, fields, and records can not be read because they are encrypted, so that only certain users can read the contents of the database by decrypting them.
Keywords : *Blowfish algorithm, encryption, decryption, symmetric keys..*

1. PENDAHULUAN

Database 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 database tersebut diperlukan sebuah metode, metode tersebut adalah kriptografi.

Tetuko Pambudi Nusa, Anita Qoiriah, pada penelitiannya yang berjudul Rancang Bangun Aplikasi Enkripsi Database MySQL Dengan Algoritma Blowfish menjelaskan bahwa aplikasi tersebut dibuat dengan tujuan untuk mengenkripsi data yang ada dalam database MySQL sehingga tidak semua orang dapat mengaksesnya. Serta manfaat pembuatan aplikasi ini adalah keamanan informasi dalam sebuah database akan lebih terjamin. Dari penelitian tersebut dapat disimpulkan salah satu cara yang dapat dilakukan untuk meningkatkan pengamanan data yaitu dengan menggunakan algoritma Blowfish. Setelah dilakukan penelitian ini dapat diketahui bahwa enkripsi suatu database dapat dilakukan dengan menggunakan algoritma Blowfish dengan visual basic 6.0 sebagai bahasa pemrogramannya. [1]

Siswo Wardoyo, Rian Fahrizal , Zaldi Imanullah, pada penelitiannya yang berjudul Aplikasi Teknik Enkripsi Dan Depenelitian File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android menjelaskan bahwa aplikasi tersebut dibuat

ISSN 2337-6805

dengan tujuan untuk pengamanan data berupa dokumen, gambar, dan video dengan menggunakan metode algoritma Blowfish untuk mengenkripsi data yang berjalan pada sistem operasi Android sehingga pemilik merasa aman untuk menyimpan datanya. Dari penelitian tersebut dapat disimpulkan Tingkat keamanan dari aplikasi yang dibuat cukup aman karena algoritma Blowfish memiliki panjang kunci yang besar. Dengan menggunakan kunci berjumlah 72 bit atau 9 karakter dibutuhkan waktu 1,49x108 tahun untuk membongkarnya dengan kecepatan komputasinya adalah 106 key/sec. Aplikasi ini dapat berfungsi dengan baik pada handphone Android dengan OS Android 2.3, 4.0, dan 4.1[2].

Ada 2 syarat keamanan suatu sistem enkripsi, yaitu true random bits dan key space yang sangat besar untuk algoritma enkripsi tersebut. Jika kedua syarat dipenuhi, maka tidak ada masalah seberapa kompleks algoritma enkripsinya. Bahakan semakin sederhana semakin baik, karena semakin sederhana, maka makin sedikit proses komputasinya, dan semakin sedikit waktu yang dibutuhkan untuk mengeksekusinya. Algoritma Blowfish adalah sebuah algoritma enkripsi simetris yang berarti bahwa algoritma ini menggunakan kunci yang sama baik untuk melakukan enkripsi dan dekripsi. Dengan menggunakan algoritma blowfish maka keamananpun akan lebih meningkat.

PERMIKOMNAS (Perhimpunan Mahasiswa Komputer Nasional) merupakan sebuah organisasi di bidang ilmu komputer dan manajemen, banyak data dan informasi penting yang dibutuhkan organisasi tersebut yang harus dijaga kerahasiaan data informasinya, salah satunya data-data mahasiswa atau anggota. Maka dari itu melalui ilmu kriptografi yang di terapkan dalam implementasi sebuah aplikasi pengaman data, nantinya diharapkan dapat membantu dalam proses pengamanan data pada bagian badan koordinasi wilayah (BAKORWIL) di Permikomnas wilayah VI Jakarta.

Berdasarkan latar belakang diatas, rumusan masalah yang akan dibahas yaitu ,bagaimana merancang aplikasi kriptografi untuk mengamankan database SQL dengan menggunakan algoritma Blowfish. Di karenakan apabila database SQL dibuat sebuah interface maka akan berkurang keamanannya. Dengan mudahnya akses untuk melihat isi dari sebuah database, maka dari itu diperlukan suatu enkripsi untuk menjaga keamanan data tersebut.

2. METODOLOGI PENELITIAN

Metode Penelitian

Metodologi penelitian yang akan di guanakan yaitu menggunakan metodologi analisis deskriptif, yaitu metode yang menggambarkan fakta-fakta dan informasi dalam situasi atau kejadian secara sistematis, faktual dan akurat, melalui metode pengumpulan data.

Metode Pengumpulan Data

Metode pengumpulan data ini bertujuan untuk memperoleh data-data apa saja yang di butuhkan dalam membangun aplikasi enkripsi database MySQL ini. Dibawah ini adalah metode yang dilakukan dalam tahap pengumpulan data:

Wawancara (Interview)

Wawancara telah dilaksanakan dengan melakukan tanya jawab secara langsung dengan badan koordinasi wilayah (BAKORWIL) di Permikomnas wilayah VI Jakarta. Kesimpulan dari wawancara tersebut yaitu, Permikomnas membutuhkan pengamanan database. Karena keamanan database di Permikonas saat ini belum ada, hal itu menyebabkan siapa saja dengan mudahnya mengakses untuk melihat isi dari sebuah database, maka dari itu diperlukan suatu keamanan untuk data tersebut.

Pengamatan (Observation)

Pengamatan telah di lakukan yaitu dengan cara melakukan pengamatan dan pengecekan mengenai kekurangn-kekurangan apa saja yang di butuhkan pada keamanan database di Permikomnas. Setelah melakukan pengamatan terhadap keamanan database yang sudah ada, masih terdapat banyak kekurangan.

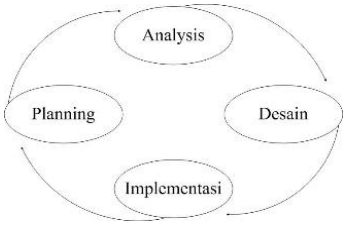
Kepustakaan (Library Study)

Metode pengumpulan data yang telah di lakukan yaitu, melalui buku, laporan laporan, E-journal, E-book, hasil penelitian ilmiah, internet dan sumber penulisan terpercaya lainnya yang berhubungan dengan keamanan database sebagai bahan acuan dalam hal perancangan aplikasi keamanan database di permikomnas. Pengumpulan data yang di lakukan yaitu mengenai apa saja yang harus digunakan untuk merancang aplikasi keamanan database pada Permikomnas.

Metode Rancang Bangun

Pengembangan sistem merupakan sebuah alternatif dalam berapresiasi dalam mendalami suatu kajian ilmu. Namun tetap harus mempunyai landasan dalam pengembangan sistem yang akan dilakukan. Metode pengembangan yang digunakan adalah SDLC (Systems Development Life Cycle). Berikut gambar tahapan pada SDLC :

ISSN 2337-6805



Gambar Peroses SDLC

Planning

Dalam tahap ini hal yang pertama dilakukan adalah memberikan form ke user yang digunakan untuk mengetahui permintaan user. Tahap ini dilakukan dengan wawancara langsung kepada bagian badan koordinasi wilayah dan ketua koordinator Permikomnas wilayah VI Jakarta.

Analisis

Dalam tahap ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa teknologi, dan analisa informasi yang sudah ada saat ini.

Perancangan

Dari data-data yang didapatkan sebelumnya, tahap Design ini akan membuat gambar design application yang akan dibangun, diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada.

Implementasi

Dalam tahap ini implementasi menerapkan semua yang telah di rencanakan dan dirancang sebelumnya. Tahap implementasi merupakan tahapan yang sangat menentukan dari berhasil atau tidaknya project yang dibangun.

Analisis

Untuk mendapatkan gambaran awal yang jelas mengenai sistem yang terdapat pada Permikomnas, maka di lakukan analisis sebagai berikut ini :

Analisis Sistem Berjalan

Pada sistem bank data permikomnas untuk saat ini berikut struktur bang data permikomnas yang sudah terancang.

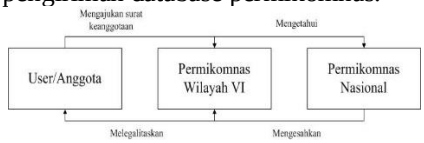
Gambar Data Center Permikomnas

Identifikasi Masalah

Setelah melihat dan melakukan analisis pada sistem bang data yang ada pada birokrasi keanggotaan permikonas, dapat dilihat jika dalam sistem tersebut masih belum adanya sistem komputerisasi dan belum adanya media keamanan untuk database yang dapat mengamankan hak ases.

Solusi Penyelesaian Masalah

Berdasarkan hasil permasalahan yang ada, maka di usulkan pemecahan masalah dengan cara membangun sebuah aplikasi enkripsi dan dekripsi sebagai media keamanan saat melakukan pengiriman database ke pusat atau keanggota. Berikut contoh peroses pengiriman database permikomnas.



Gambar Peroses Pengiriman Database

Proses Enkripsi Dan Dekripsi Algoritma Blowfish

Blowfish merupakan blok cipher 64-bit dengan panjang
kunci variabel. Algoritma ini terdiri dari dua bagian: key expansion atau perluasan kunci dan enkripsi data. Yang berfungsi merubah kunci (Minimum 32-bit, Maksimum 448-bit) menjadi beberapa array subkunci (subkey) dengan total 4168 byte. (18x32-bit untuk P-array dan 4x256x32 bit untuk S-box sehingga totalnya 33344 bit atau 4168 byte). Kunci disimpan dalam K array: K1, K2, ... Kj $1 \leq j \leq 14$
Kunci-kunci ini yang dibangkitkan (generate) dengan menggunakan subkunci yang harus dihitung terlebih dahulu sebelum enkripsi atau dekripsi data. Sub-sub kunci yang digunakan terdiri dari :
P-array yang terdiri dari 18 buah 32-bit subkunci,
P1, P2, ..., P18
S-box yang terdiri dari 4 buah 32-bit, masing-masing memiliki 256 entri :
S1,0, S1,1, ..., S1,255
S2,0, S2,1, ..., S2,255
S3,0, S3,1, ..., S3,255
S4,0, S4,1, ..., S4,255

Langkah-langkah perhitungan atau pembangkitan subkunci tersebut adalah sebagai berikut:

1) Inisialisasi P-array yang pertama dan juga empat S-box, berututan, dengan string yang telah pasti. String tersebut terdiri dari digit-digit heksadesimal dari phi, tidak termasuk angka tiga di awal. Contoh :
   P1= 0x243f6a88

ISSN 2337-6805

P2= 0x85a308d3
P3= 0x13198a2e
P4= 0x03707344
dan seterusnya sampai S-box yang terakhir (daftar heksadesimal digit dari phi untuk P-array dan Sbox bisa lihat Lampiran).

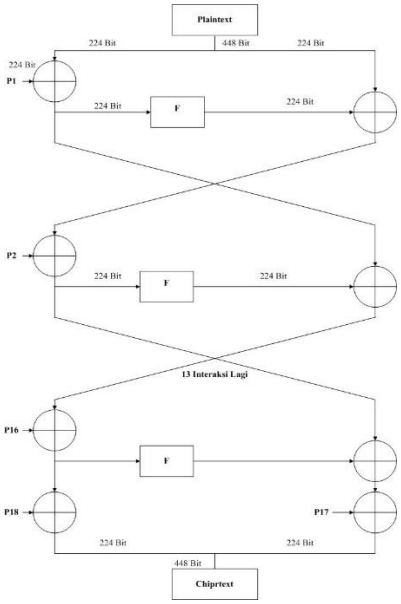
2) XOR-kan P1 dengan 32-bit awal kunci, XOR-kan P2 dengan 32-bit berikutnya dari kunci, dan seterusnya untuk semua bit kunci. Ulangi siklus seluruh bit kunci secara berurutan sampai seluruh P-array ter-XOR-kan dengan bit-bit kunci. Atau jika disimbolkan : P1 = P1 ⊕ K1, P2 = P2 ⊕ K2, P3 = P3 ⊕ K3, . . . P14 = P14 ⊕ K14, P15 = P15 ⊕ K1, . . . P18 = P18 ⊕ K4. Keterangan : ⊕ adalah simbol untuk XOR.
3) Enkripsikan string yang seluruhnya nol (all-zero string) dengan algoritma Blowfish, menggunakan subkunci yang telah didepenelitian kan pada langkah 1 dan 2.
4) Gantikan P1 dan P2 dengan keluaran dari langkah 3.
5) Enkripsikan keluaran langkah 3 menggunakan algoritma Blowfish dengan subkunci yang telah dimodifikasi.
6) Gantikan P3 dan P4 dengan keluaran dari langkah 5.
7) Lanjutkan langkah-langkah di atas, gantikan seluruh elemen P-array dan kemudian keempat S-box secara berurutan, dengan hasil keluaran algoritma Blowfish yang terus-menerus berubah.

Total keseluruhan, terdapat 521 iterasi untuk menghasilkan subkunci subkunci dan membutuhkan memori sebesar 4KB.

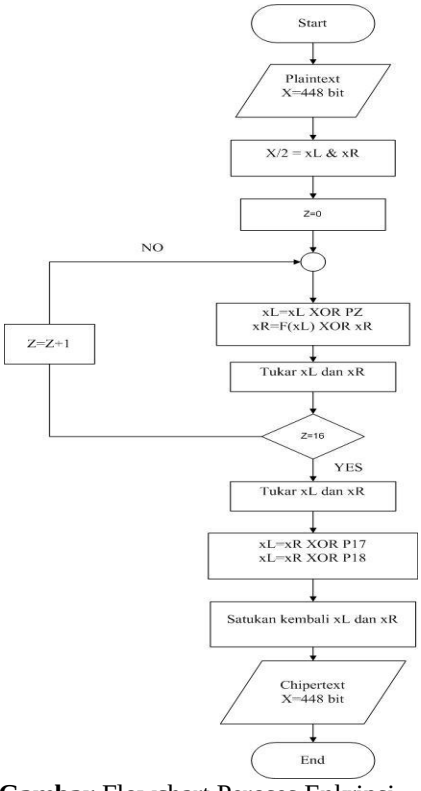
Peroses Enkripsi

Terdiri dari iterasi fungsi sederhana (Feistel Network) sebanyak 16 kali putaran, masukannya adalah 448-bit elemen data X. Setiap putaran terdiri dari permutasi kunci-dependent dan substitusi kunci- dan data-dependent. Semua operasi adalah penambahan (addition) dan XOR pada variabel 32-bit. Operasi tambahan lainnya hanyalah empat penelusuran tabel (table lookup) array berindeks untuk setiap putaran. Untuk alur algoritma enkripsi dengan metoda Blowfish dijelaskan sebagai berikut :

1. Memulai proses enkripsi (plaintext) dengan x=448 bit
2. X dibagi menjadi 2, XL (x left =224 bit) dan XR (x right =224 bit)
3. z = 0 merupakan inisial perputaran yang dimulai dari 0
4. Melanjutkan proses selanjutnya, yaitu operasi XL = XL xor Pi dan XR = F(XL) xor XR
5. Menukar hasil dari XL dan XR (XL= XR dan XR=XL)
6. Melakukan perulangan sebanyak 16 kali perulangan, dan melakukan kembali penukaran XL dan XR (z = z + 1)
7. Pada proses ke-17 lakukan operasi untuk XR = XR xor P17 dan XL = XL xor P18.
8. Menggabungkan kembali XL dan XR (sehingga menjadi x=448 bit)
9. Menghasilkan chipertext dengan x=448 bit

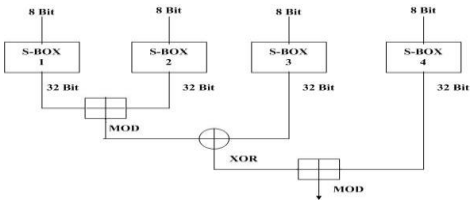


Gambar Blok Diagram Algoritma Enkripsi



Gambar Flowchart Peroses Enkripsi

ISSN 2337-6805

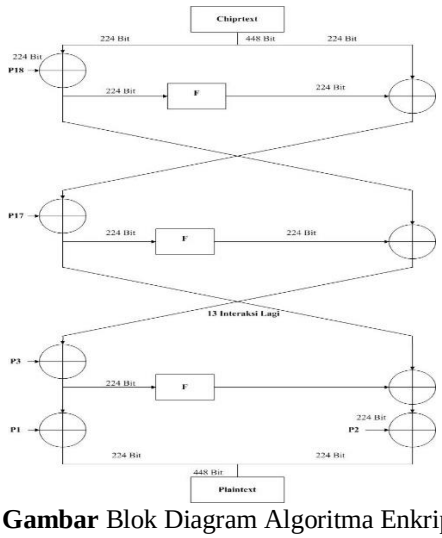


Gambar Fungsi F Dalam Blowfish

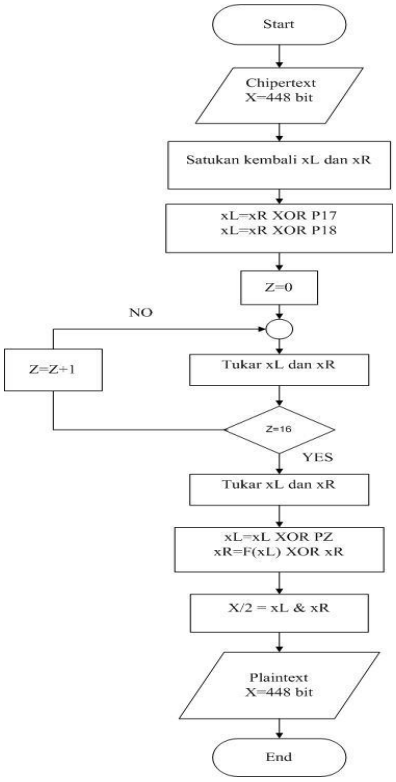
Peroses Dekripsi

Algoritma Blowfish memiliki keunikan dalam hal proses dekripsi, yaitu proses dekripsi dilakukan dengan urutan yang sama persis dengan proses enkripsi, hanya saja pada proses dekripsi P1, P2, …, P18 digunakan dalam urutan yang terbalik. Dalam algoritma Blowfish juga terdapat fungsi f. Berikut ini gambar mengenai fungsi f tersebut. Gambar 3. Fungsi f dalam algoritma Blowfish Sebelumnya dijelaskan bahwa Array P terdiri dari delapan belas subkunci. Subkunci dihitung menggunakan algoritma Blowfish, metodenya adalah sebagai berikut :

1. Memulai proses dekripsi (chipertext) x= 448 bit (xL= 224 bit dan xR=224 bit)
2. Menggabungkan XL dan XR (sehingga menjadi x=448 bit)
3. Pada proses ke-17 lakukan operasi untuk XR = XR xor P17 dan XL = XL xor P18.
4. Menukar hasil nilai XL dan XR (XL= XR dan XR=XL)
5. i = 0 merupakan inisial perputaran yang dimulai dari 0
6. Melakukan perulangan sebanyak 16 kali perulangan, dan melakukan kembali penukaran XL dan XR (i= i + 1)
7. Melanjutkan proses selanjutnya, yaitu operasi XL = XL xor Pi dan XR = F(XL) xor XR
8. Menggabungkan kembali XL dan XR (sehingga menjadi x=448 bit)
9. Menghasilkan Plaintext dengan x=448 bit



Gambar Blok Diagram Algoritma Enkripsi



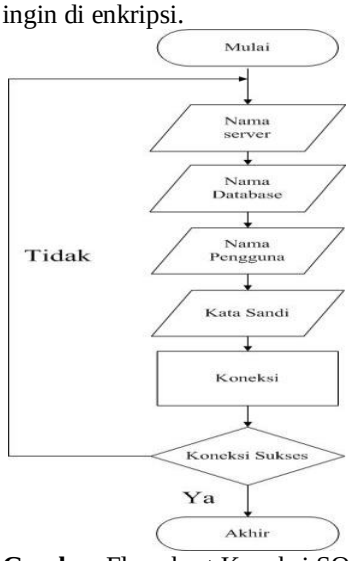
Gambar Flowchart Peroses Dekripsi

Proses Enkripsi Dan Dekripsi Database Pada Aplikasi

Pada tahap ini merancang program untuk mengekripsi dan dekripsi database ,berikut proses pengekripsian dan dekripsian:

Flowchart Koneksi SQL

Sebelum melakukan enkripsi dan dekripsi harus melakukan conect database terlebih dahulu agar dapat mengambil database yang ingin di enkripsi.



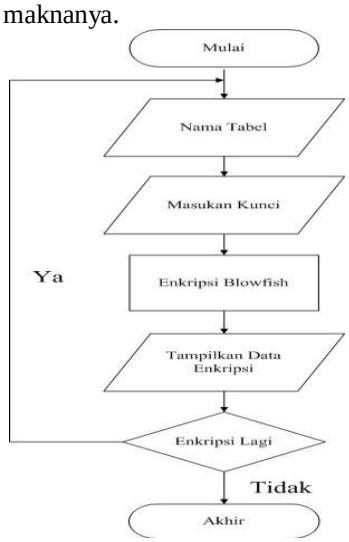
Gambar Flowchart Koneksi SQL

Flowchart Enkripsi

Pada flowchart enkripsi untuk melakukan proses enkrips ,hal pertama yang dilakukan

ISSN 2337-6805

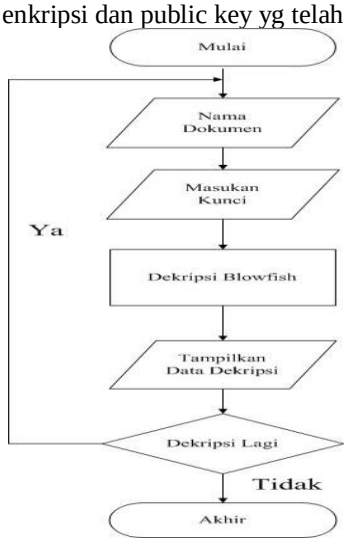
adalah mengambil database yang ingin di enkripsi. Kemudian mengambil private key yg telah di buat , setelah proses enkripsi file berhasil maka hasil outputnya berupa cipherteks yang sudah tidak dapat dimengerti maknanya.



Gambar Flowchart Enkripsi

Flowchart Dekripsi

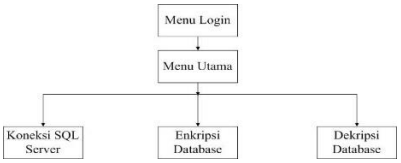
Pada flowchart dekripsi untuk melakukan proses dekrips ,hal pertama yang dilakukan adalah mengambil database yang ingin di enkripsi dan public key yg telah di buat.



Gambar Flowchart Dekripsi

Perancangan Antarmuka

Perancangan ini dibagi kedalam beberapa halaman yang bertujuan untuk mempermudah pemahaman dan pengoperasian Aplikasi Enkripsi Dan Depenelitian Database SQL Pada Bank Data Permikomnas Menggunakan Algoritma Blowfish Menu-menu yang digunakan dapat dilihat pada struktur menu di bawah ini :



Gambar Hipotesi

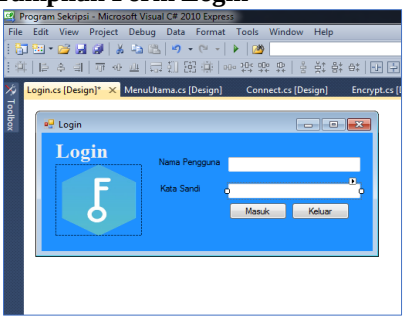
3. HASIL DAN PEMBAHASAN

Implementasi Sistem

Implementasi sistem dilakukan setelah tahap perancangan dengan fungsi-fungsi yang diinginkan selesai. Tahap dimana aplikasi atau program siap dioperasikan pada keadaan yang sebenarnya sehingga dari sini kita akan mengetahui apakah aplikasi atau program enkripasi dan dekripsi databse sql benar-benar dapat menghasilkan keluaran yang sesuai dengan tujuan yang diinginkan.

Pengujian sistem dilakukan sebagai pembuktian bahwa sistem keamanan yang dibuat berfungsi dengan baik dan sesuai dengan yang sudah dirancang melalui beberapa skenario pengajuan.

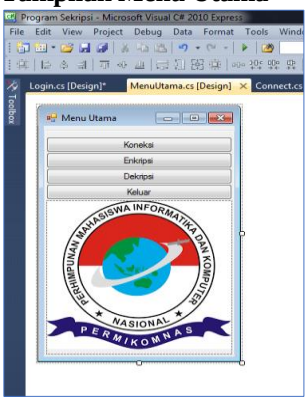
Tampilan Form Login



Gambar Tampilan Form Login

Form Login merupakan halaman utama yang pertama kali muncul. Sebelum menggunakan aplikasi ini, Pengguna diharuskan untuk login terlebih dahulu dengan cara menginputkan Nama Pengguna dan Kata Sandi.

Tampilan Menu Utama

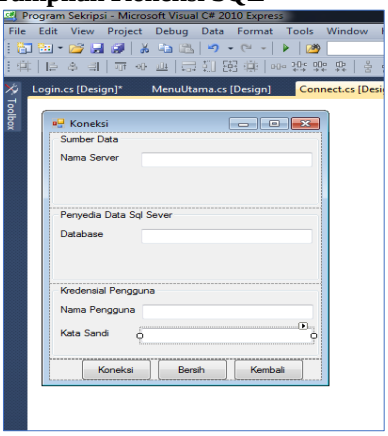


Gambar Tampilan Form Menu Utama

ISSN 2337-6805

Setelah login sukses, maka akan muncul Form Menu Utama yang merupakan induk dari semua form yang ada. Pada Menu Utama terdapat beberapa pilihan-pilihan menu yaitu sebagai berikut :
-Koneksi:Digunakan untuk menuju from koneksi
-Enkripsi:Digunakan untuk menuju from enkripsi
-Dekripsi:Digunakan untuk menuju from dekripsi
-Keluar : Digunakan untuk keluar aplikasi

Tampilan Koneksi SQL



Gambar Tampilan Form Koneksi SQL

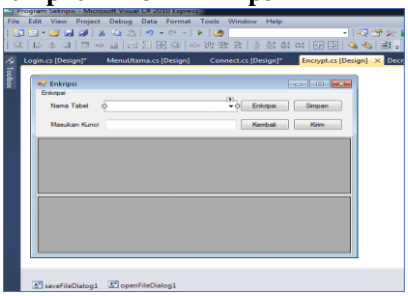
Pada gambar Tampilan Form Koneksi SQL merupakan Form Koneksi dimana form ini di gunakan untuk melakukan koneksi atau login pada databse sql sever, Berikut merupakan keterangan nya :

1. Nama Server : Berisi nama server database
2. Database : Berisi nama database yang ingin digunakan
3. Nama Pengguna : Berisi user name login sever
4. Kata Sandi : Berisi password login server

Berikut tombol perintah pada from koneksi :

5. Koneksi : Berfungsi untuk memproses koneksi atau login
6. Bersih : Berfungsi untuk menghapus semua textbox
7. Kembali : Berfungsu untuk kembali ke menu utama

Tampilan From Enkripsi



Gambar Tampilan Form Enkripsi

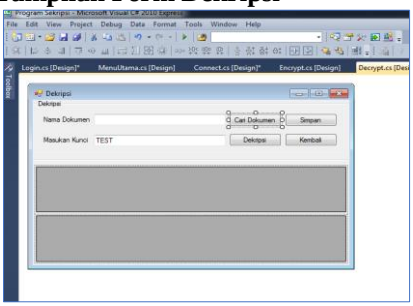
Pada from ini terdapat menu enkripsi untuk database sql, Berikut merupakan keterangan dari from encrypt :

- Nama Tabel : Berisi nama-nama tabel yang berada di database
- Masukan Kunci : Berisi kunci enkripsi

Berikut tombol perintah pada form encrypt:

- Enkripsi : Berfungsi untuk memulai proses enkripsi
- Kembali : Berfungsi untuk kembali ke menu utama
- Simpan : Berfungsi untuk menyimpan hasil enkripsi
- Kirim : Berfungsi untuk menuju halaman gmail

Tampilan Form Dekripsi



Gambar Tampilan Form Dekripsi

Pada Gambar Tampilan Form Dekripsi merupakan Form Decrypt dimana form ini digunakan untuk mendekripsi file yang telah di enkripsi, Berikut merupakan keterangan nya :

- Name Dokumen : Berisi file yang ingin di dekripsi
- Masukan Kunci : Berisi kunci dekripsi

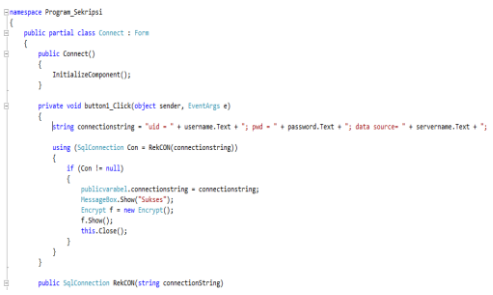
Berikut tombol perintah pada form encrypt:

- Cari Dokumen : Berfungsi untuk mencari file yang ingin di dekripsi
- Dekripsi : Berfungsi untuk memulai proses dekripsi
- Simpan : Berfungsi untuk menyimpan hasil dekripsi
- Kembal : Berfungsi untuk kembali ke menu utama

Proses System

Pada tahap ini membahas tentang bagaimana penerapan algoritma blowfish pada Aplikasi Ekripsi Dan Dekripsi Database SQL Menggunakan Algoritma Belowfish.

Proses Koneksi SQL



```
namespace Program_Sekripsi
{
    public partial class Connect : Form
    {
        public Connect()
        {
            InitializeComponent();
        }

        private void button1_Click(object sender, EventArgs e)
        {
            string connectionstring = "uid = " + username.Text + "; pwd = " + password.Text + "; data source= " + servername.Text + ";

            using (SqlConnection Con = RekCON(connectionstring))
            {
                if (Con != null)
                {
                    publicvarabel.connectionstring = connectionstring;
                    MessageBox.Show("Sukses");
                    Encrypt f = new Encrypt();
                    f.Show();
                    this.Close();
                }
            }
        }

        public SqlConnection RekCON(string connectionString)
```

ISSN 2337-6805

```
{
    SqlConnection Con;
    try
    {
        Con = new SqlConnection(connectionString);

        if (Con.State == ConnectionState.Closed)
        {
            Con.Open();
        }

        return Con;
    }
    catch (Exception ex)
    {
        MessageBox.Show(ex.Message);
        return null;
    }
}
```

Gambar Proses Koneksi SQL

Pada gambar Proses Koneksi SQL adalah fungsi beberapa coding koneksi sql yang diimplementasikan dalam sistem Aplikasi Ekripsi Dan Dekripsi Database SQL Menggunakan Algoritma Belowfish.

Proses Enkripsi Dan Dekripsi

```
private void button3_Click(object sender, EventArgs e)
{
    try
    {
        Blowfish blowfish1 = new Blowfish(Encoding.Unicode.GetBytes(textBox1.Text));

        DataTable dtsource = GetData();

        for (int i = 0; i < dtsource.Rows.Count; i++)
        {
            for (int l = 0; l < dtsource.Columns.Count; l++)
            {
                string input = dtsource.Rows[i][l].ToString();

                int div = 4 - (input.Length % 4);

                if (div == 4)
                {
                    div = 0;
                }

                for (int x = 0; x < div; x++)
                {
                    input = input + " ";
                }

                dtsource.Rows[i][l] = blowfish1.Encipher(input);
            }
private void button2_Click(object sender, EventArgs e)
{
    DataTable dtDecript = new DataTable();
    foreach (DataGridViewC
    {
        dtDecript.Columns.Add(dgvColumn.HeaderText, typeof(String));
    }

    Blowfish blowfish1 = new Blowfish(Encoding.Unicode.GetBytes(textBox2.Text));

    //string value = blowfish1.Decipher("<encrypted>");

    foreach (DataGridViewRow dgvRow in dataGridView1.Rows)
    {
        if (!dgvRow.IsNewRow)
        {
            dtDecript.Rows.Add();

            for (int c = 0; c < dgvRow.Cells.Count; c++)
            {
                dtDecript.Rows[dtDecript.Rows.Count - 1][c] = blowfish1.Decipher(dgvRow.Cells[c].Value.ToString()).Trim();
            }
        }
    }

    dataGridView2.DataSource = dtDecript;
}
```

DataTable.DataTable() (+ 2 overload(s))
(The documentation cache is still being constructed. Please try again in a few seconds.)

Gambar Proses Enkripsi Dan Dekripsi

Pada gambar Proses Enkripsi Dan Dekripsi adalah fungsi berupa coding enkripsi dan dekripsi yang diimplementasikan dalam sistem Aplikasi Ekripsi Dan Dekripsi Database SQL Menggunakan Algoritma Belowfish. Berikut contoh hasil dari enkripsi dan dekripsi:

	nim	nama	alamat
▶	+BcezYOovZuyH...	HNPFCWSLmZU=	v3r4ZeSuCciMmi...
	+BcezYOovZvY6...	9Tt8pY2aDqM=	vmQNw/PGp/jb2...
	+BcezYOovZvbB...	IXrBx1heV5w=	IVEwswQsjndnV...
	+BcezYOovZuac...	/qAKSrWQ7uY=	9I3KzT6DyyF36r...
	LW3hFDeKoiP6y...	Z9f/t/MBHVxkU...	vp/v24CXoS9us...
	LW3hFDeKoiOy...	xA2BCvfUtdOn0...	LTTaO34CUAh8i...

	nim	nama	alamat
▶	13360001	adam	cimanggis
	13360011	doni	cilodong
	13360010	ardi	bogor
	13360022	augi	margonda
	14360009	sadid	kebagusan
	14360001	aulia	cibinong

Gambar Hasil Enkripsi Dan Dekripsi

Uji Coba

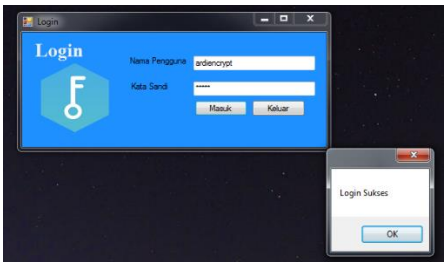
Pengujian di lakukan untuk mengetahui apakah Algoritma Blowfish yang telah di gunakan pada sistem aplikasi enkripsi dan dekripsi database dapat mencapai tujuan yang diinginkan dan menemukan kesalahan-kesalahan yang terjadi pada saat implementasi.

Pengujian Blackbox

Aplikasi enkripsi dan dekripsi database sql menggunakan metode algoritma Blowfish selanjutnya akan diuji dengan menggunakan metode blackbox. Tahap pengujian dilakukan dengan tujuan untuk menjamin sistem yang dibuat sesuai dengan hasil analisis dan perancangan.

Selanjutnya pengujian sistem di lakukan setelah algoritma Blowfish berhsil diintegrasikan pada Aplikasi enkripsi dan dekripsi database. Di depenelitian kan dengan beberapa langkah, yaitu:

Login



Gambar Login

Pada gambar 4.9 adalah halaman login ,di sini user diwajibkan untuk login terlebih dahulu dengan menginput nama pengguna dan kata sandi. Apabila Nama Pengguna dan Kata Sandi yang diinputkan sesuai dengan yang sudah di tentukan maka akan muncul Menu Utama, namun apabila Nama Pengguna dan Kata Sandi tidak sesuai dengan yang ada maka tidak akan muncul Menu Utama.

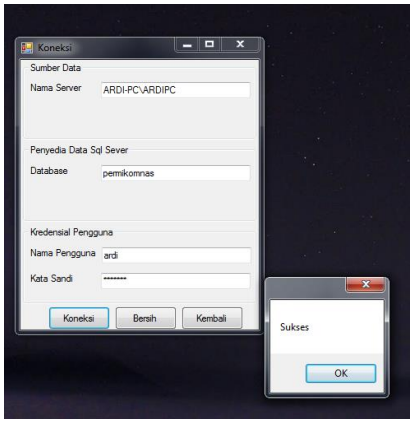
Menu utama

Gambar Menu Utama

ISSN 2337-6805

Pada gambar Menu Utama adalah halaman menu utama ,di sini ada beberapa pilihan untuk menuju halaman koneksi, enkripsi, dekripsi, dan keluar. User dapat memilih menu yang ingin digunakan.

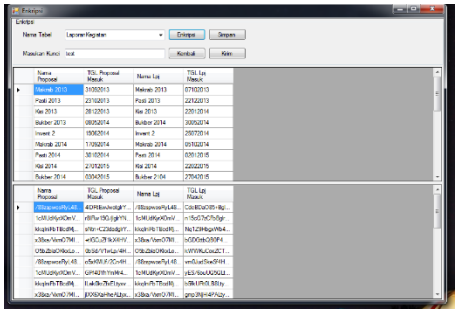
Koneksi



Gambar Koneksi

Pada gambar Koneksi adalah halaman koneksi ,disini user di wajibkan melakukan koneksi terlebih dahulu sebelum melakukan enkripsi database. Yang harus diinput oleh user adalah nama server, nama database, nama pengguna dan kata sandi sql server.

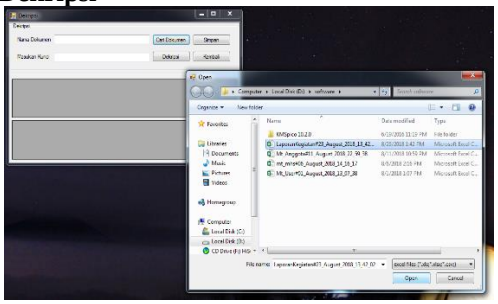
Enkripsi



Gambar Enkripsi

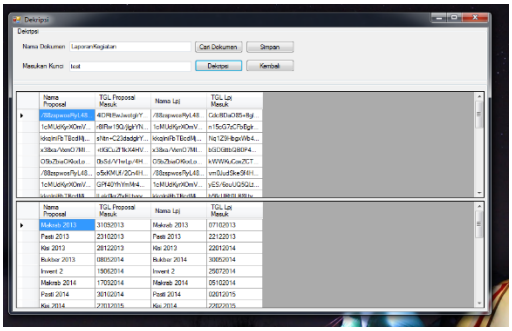
Pada gambar Enkripsi adalah halaman enkripsi ,setelah melakukan koneksi ke database sql user dapat melakukan enkripsi database.

Dekripsi



Gambar Pilih Dokumen

Pada gambar Pilih Dokumen adalah halaman dekripsi, sebelum melakukan dekripsi user harus memilih dokumen yang ingin di dekripsi telebih dahulu.



Gambar Dekripsi

Setelah memilih dokumen kita masukan kunci yang sama pada saat enkripsi lalu dokumen akan kembali seperti sebelum di enkripsi seperti pada gambar Dekripsi

4. SIMPULAN

Berdasarkan pengujian dan analisis yang telah dilakukan dalam penelitian ini dapat diambil kesimpulan sebagai berikut:

1. Amplikasi enkripsi dan dekripsi databse sql dapat berfungsi dengan baik dan sesuai tujuan yaitu mengamankan database sehingga tidak dapat di baca atau di mengerti.
2. Aplikasi ini juga telah berhasil mengembalikian database yang telah diacak tersebut seperti semula dengan menggunakan kunci yang sama sewaktu enkripsi.
3. Aplikasi ini menggunakan software Visual studio 2010 dan C# atau C Sharp sebagai bahasa pemogramannya.

Saran

Berdasarkan penelitian yang di peroleh, ada beberapa saran-saran untuk pengembangkan sistem lebih lanjut. Saran-saran tersebut yaitu:

1. aplikasi enkripsi dan dekripsi database SQL dengan algoritma blowfish ini dapat di kembangkan agar tidak hanya mengenkripsi dan depenelitian pertabel.
2. aplikasi enkripsi dan dekripsi database SQL dengan algoritma blowfish ini dapat di kembangkan untuk mengenkripsi dan dekripsi database lain seperti Access, MySQL, Oracle, Dan lain-lain.
3. Aplikasi ini bisa di kembangkan dengan mengkombinasikan algoritma lain atau algoritma asimetri agar dapat menggunakan dua kunci yang berbeda saat mengenkripsi dan dekripsi.

ISSN 2337-6805

5. DAFTAR PUSTAKA

Tetuko Pambudi Nusa, Anita Qoiriah, "Rancang Bangun Aplikasi Enkripsi Database MySQL Dengan Algoritma Blowfish", Jurnal Manajemen Informatika : https://ejournal.unesa.ac.id/index.php/jurnal-manajemen-informatika/article/view/4718

Siswo Wardoyo, Rian Fahrizal , Zaldi Imanullah, "Enkripsi dan Dekripsi File dengan Algoritma Blowfish pada Perangkat Mobile Berbasis Android", Jurnal Nasional Teknik Elektro 5(1):36, DOI: 10.25077/jnte.v5n1.199.2016

Dony Ariyus. 2008. Pengantar Kriptografi Teori Konsep Dasar Enkripsi Dan Dekripsi, Analisis dan Implementasi. Yogyakarta: Penerbit Andi

Kromodimoeljo, Sentot. 2010. Teori dan Aplikasi Kriptografi. Penerbit: SPK IT Consulting.

Bambang Hariyanto, (2007), Sistem Manajemen Basis Data, Informatika, Bandung.

Widhi Arianto Putra. 2011. Pengamanan Data. Universitas PGRI Yogyakarta

Raharjo Budi. (2011). Belajar Otodidak Membuat Database menggunakan MySQL. Informatika. Bandung.

Susanto, E. 2009. Perancangan aplikasi enkripsi dan dekripsi data. Jakarta : Teknik Informatika.

Kurniawan, Erick. (2010). Cepat Mahir Visual Studio 2010. Bandung : Penerbit, Andi.

Agitya, Lingga. 2013. Eksplorasi Metodologi SDLC. Sistem Informasi UNIKOM.

Aswan M.Si. 2012. Kumpulan Program Kreatif Dengan VB. Bandung: Penerbit, Informatika