IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN METODE BLOWFISH DAN BASE 64 UNTUK MENGAMANKAN DATABASE INFORMASI AKADEMIK PADA KAMPUS AKADEMI TELEKOMUNIKASI BOGOR BERBASIS WEB-BASED

Annas Rifa'i[1*], Lilis Cucu Sumartini[2]
[1,2]Program Studi Teknik Listrik, Akademi Teknologi Bogor, Bogor, Indonesia
*Email: annasrifai23@gmail.com

Abstrak

Data merupakan suatu bukti yang sangat otentik sehingga perlu disimpan dengan baik karena data beresiko terhadap perubahan data oleh pihak yang ingin sekali menyalahgunakan data atau tidak berpengaruh terhadap data tersebut. Oleh karena itu agar tidak ada orang yang tidak berhak merubah data yang sudah ada, disimpan atau dapat mengambil data yang sangat penting, dibutuhkan suatu metode untuk dapat mengamankan dan merahasiakan data. Database merupakan tempat menyimpan data dan informasi. Seluruh sistem menyimpan datanya di dalam database, sehingga isi dari data yang tersimpan harus dijaga keamanan dan kerahasiannya. Untuk menjaga keamanan tersebut dibutuhkan sebuah pengaman yaitu kriptografi. Dengan memanfaatkannya database yang ada didalam dapat terhubung satu dengan lainnya, Database tidak hanya sekedar tempat untuk menyimpan data, database bisa juga digunakan untuk memfasilitasi penggunanya yang membutuhkan pemrosesan data dengan baik untuk analisa maupun evaluasi. Sistem keamanan komputer sangat dibutuhkan saat ini seiring dengan adanya peningkatannya penggunaan komputer di muka bumi ini. Sehingga keamanan data yang ada menjadi sangat terancam untuk diakses dari orang yang tidak bertanggung jawab. Keamanan komputer menjadi sangat penting saat ini karena itu terkait dengan privasi, integritas, otentikasi, dan kerahasiaan. Dengan demikian data perlu disimpan dengan mengunakan teknik penyimpanan yang benar, agar kerahasian dan keamanan data dapat terjaga. Teknik kriptografi dengan teknik enkripsi data pada database merupakan salah satu solusi yang dapat digunakan untuk memenuhi aspek kerahasiaan dan keaman data. Dengan adanya sebuah kriptografi yang meliputi proses enkripsi maka data pada database dapat dikodekan sehingga orang yang tidak berkepentingan tidak dapat membaca informasi tersebut, selain orang yang mengetahui kunci untuk mendeskripsikannya. Pengamanan data / informasi document dengan teknik kriptografi yang menggunakan metode algoritma Blowfish dipilih karena kriptografi modernmerupakan kunci simetris berbentuk cipher block. Algoritma Blowfish yang dibangun ini dapat mengenkripsi text dalam bentuk teks. Enkripsi dilakukan dengan menggunakan kunci tertentu, sehingga menghasilkan chipertext yang tidak dapat dimengerti dan dipahami. Chipertext tersebut dapat diubah kembali seperti awal jika di dekripsi menggunakan kunci yang sama di awal sewaktu mengekripsi database tersebut.

Kata kunci: *Database, Algoritma blowfish, Base 64, Enkripsi, Dekripsi*

Abstract

Data is a very authentic evidence that need to be saved because the data are at risk of data changes by the party who wanted to misuse the data or no effect on the data. Therefore, so that no unauthorized person to change the existing data, stored or can take the data that is very important, we need a method to be able to secure and keep data. The database is used to keep data and information. The whole system stores the data in the database, so that the contents of stored data security and confidentiality must be maintained. To maintain the security of a security that is required cryptography. With the use of databases that are in can be connected to each other, Database is not just a place to store data, Computer security system is needed at this time in line with the increase use of computers in the world. So existing data security has become seriously threatened to be accessed by people who are not responsible. Computer security becomes very important at this time because it is related to the privacy, integrity, authentication and confidentiality. Thus data need to be stored by using the correct storage techniques, so that the confidentiality and security of data is maintained. Cryptographic techniques with engineering data encryption on the database is one solution that can be used to meet the confidentiality and Data Security settings. With the existence of a cryptography that includes the encryption process, the data in the database can be encoded so that unauthorized persons can not read the information, in addition to those who know the key to describing it. Security of data / information document with a cryptographic technique that uses the Blowfish algorithm chosen method for cryptographic key modernmerupakan shaped symmetric block cipher. Blowfish algorithm which can encrypt text built in text form. Encryption

is done using a specific key, resulting ciphertext that can not be understood. The ciphertext can be changed back as the beginning if the decryption using the same key in the beginning when the database mengekripsi.

Keywords: *Database, Blowfish algorithm, Base 64, encryption, decryption*

1. PENDAHULUAN

Dengan kemajuan pesat teknologi saat ini mulai sangat banyak mempengaruhi gaya hidup seluruh masyarakat dimuka bumi. Sehingga keperluan terhadap teknologi saat ini menjadi sangat penting, kita dapat rasakan disegala bidang kehidupan baik di bidang politik, pendidikan, ekonomi, transportasi, perdagangan atau bisnis bahkan kehidupan rumah tangga. Hampir semua lapisan masyarakat saat ini tidak bisa terlepas dari kemajuan teknologi, sehingga banyak sekali data yang disimpan dan dikirim dengan memanfaatkan kemajuan teknologi saat ini. Banyak jenis data yang dapat disimpan dan dikirim. Dampak dari kemajuan teknologi komputer yang positif dapat digunakan oleh siapa aja. Namun selain adanya dampak positif yang ada dalam kemajuan teknologi saat ini, ada juga dampak negatif dari kemajuan teknologi bagi sebagian orang yang ingin mencari celah peluang untuk mengambil atau mengubah data untuk kepentingan sendiri. Dengan terjadi pengambilan dan pengubahan data secara diam-diam, maka dengan demikian sangat penting bagi pengguna teknologi menunjukan kualitas keamanan dalam menggunakan sebuah perangkat komputer.

Akademi Telekomunikasi Bogor mempunyai data yang sangat penting untuk disimpan kedalam sistem komputer. Jika data tersebut hanya disimpan kedalam sistem komputer tanpa adanya satupun pengamanan yang sangat baik, data tersebut akan rentan terhadap pengambilan ataupun perubahan data oleh orang yang ingin memalsukan atau tidak bertanggung jawab pada data tersebut. Oleh karena itu agar tidak ada orang yang tidak bertanggung jawab yang dapat merubah data yang sudah disimpan kedalam sistem komputer atau dapat mengambil data yang penting, dibutuhkan suatu metode untuk dapat mengamankan data. Pada saat ini sistem keamanan komputer sangat dibutuhkan dengan kemajuan teknologi sistem komputer di seluruh muka bumi. Maka dari itu semakin meningkatnya para *user* yang terhubung pada jaringan ke internet, tetapi tidak di selaraskan dengan SDM yang bisa mengelola keamanan data. Membuat keamanan data yang sudah ada sangat rentan dari orang yang tidak bertanggung jawab. Keamanan komputer akan sangat penting karena ini terkait dengan privasi, integritas, otentikasi, kerahasiaan dan ketersediaanya.

Berkaitan dengan hal tersebut penulis sangat tertarik untuk melakukan sebuah implementasi terhadap suatu pengamanan data / informasi *document* dengan teknik kriptografi yang menggunakan metode algoritma *Blowfish* dan *Base64*. Teknik algoritma ini dipilih karena kriptografi modern kunci simetris berbentuk cipher block. Algoritma *Blowfish* yang dibangun ini dapat mengenkripsi text dalam bentuk teks. Enkripsi dilakukan dengan menggunakan kunci tertentu, sehingga menghasilkan chipertext.

2. MATERI DAN METODE

2.1. Materi

a. Keamanan Data

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Sangat sayang sekali masalah keaman ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Seringkali masalah keamanan berada tidak ada diurutan pertama, atau bahkan diurutan kedua dalam daftar hal-hal yang dianggap penting. Apabila mengganggu performa dari sistem, seringkali kemanan tidak dipentingkan atau ditiadakan.

b. Kriptografi

Cryptography berasal dari bahasa Yunani Kuno yang sudah lama ada sejak dahulu: *"crypto"* artinya menyembunyikan atau merahasiakan (*hidden* atau *secret*) dan *"graphein"* artinya tulisan (*writing*). Jadi kriptografi adalah perpaduan antar ilmu dengan seni untuk menjaga kerahasiaan keamanan data dengan cara mengkodekan kedalam bentuk yang tidak akan bisa dipahami isi kandungan maknanya.

c. *Algoritma Kriptographi*

Konsep matematis yang didasari dari sebuah algoritma kriptografi yaitu relasi antara dua kompilasi yaitu kompilasi yang terdiri dari elemen-elemen plainteks dan kompilasi yang berisi chiperteks. Enkripsi dan dekripsi merupakan fungsi yang mematakan elemen-elemen antara kedua himpunan tersebut. Misalkan A menyatakan plainteks dan B menyatakan chiperteks, maka fungsi enkripsi C memetakan A ke B.

C(A) = B

Dan fungsi dekripsi memetakan kompilasi B ke kompilasi A,

D(B) = A

Jika proses enkripsi dengan dekripsi membalikan data ke data awal kemudian perbandingan berikut mesti benar,

D(C(A)) = A

Dengan memanfaatkan kunci K, hingga fungsi enkripsi dengan dekripsi menjadi,

EK(A) = B

DK(B) = A

dan kedua fungsi ini memenuhi :

DK(EK(A)) = A

d. Algoritma Kriptographi

Algoritma kriptografi adalah kumpulan metode bagi proses enkripsi dengan dekripsi. Dalam beberapa metode kriptografi terdapat beberapa variasi kegunaan enkripsi dengan dekripsi.

Konsep matematis yang didasari algoritma yaitu relasi antara kompilasi, yaitu relasi antara kompilasi yang diisi elemen-elemen *chipertext.* Enkripsi dengan dekripsi merupakan peranan yang menggambarkan elemen-elemen masa kedua kompilasi tesebut. Misalkan kompilasi elemen *plaintext* dinotasikan A dan himpunan elemen *chipertext* dinotasikan B, maka fungsi enkripsi C memetakan kompilasi A ke B.

1) Algoritma Asimetris

Kriptografi *public key* sering disebut dengan kriptografi asimetris. Kunci yang didukung antara metode enkripsi dengan dekripsi pada kriptografi kunci public ini bertentangan antara satu dengan yang lainnya. Didalam kriptografi kunci publik, yaitu kunci generator yang dapat memberikan dua kunci berbeda dengan satu kunci dipakai untuk menjalankan proses enkripsi dan kunci yang lain dijalankan ke proses dekripsi.

2) Algoritma Simetris

Kriptografi simetris atau *secret key* yaitu kriptografi yang dijalankan dengan satu kunci didalam proses enkripsi dengan dekripsi. Pada sistem kriptografi simetris, kunci yang akan diproses enkripsi sama dengan kunci yang akan diproses dekripsi. Keamanan sistem kriptografi simetris terletak pada kerahasiaan kunci. Istilah lain untuk kriptografi simetris adalah kriptografi kunci pribadi atau kriptografi konvensional.

e. Blowfish

1) Pengertian Blowfish

Blowfish disebut juga *OpenPGP.Cipher.4* adalah enkripsi yang ada didalam katagori *Symmetric Cryptosystem* , metode enkripsinya sama dengan DES (DES-like Cipher) yang dibuat oleh seorang *Cryptanalyst* yang bernama Bruce Schneier Presiden perusahaan Counterpane Internet Security, Inc dan diperkenalkan pada tahun 1994. Dan pada saat itu setelah dilakukan beraneka cara analisisa, dengan perlahan - lahan dapat pernyataan sebagai algoritma enkripsi paling kompeten. Dipergunakan pada komputer yang memiliki microposesor sebesar (32-bit keatas untuk *cache* data yang besar) saat ini tidak ada serangan yang bisa menghancurkan *Blowfish*. *Blowfish* dikembangkan guna mencukupi standar desain yang cepat dengan pelaksanaanya untuk kondisi yang ideal dapat mencapai 26 *clock cycle* per *byte*, bisa dijalankan pada memori kurang dari 5 KB, mudahnya pada algoritma dapat diketahui masalahnya, dan keamanan faktor dari panjang kunci bervariasi (minimnya 32 bit, maksimalnya 448 bit, multiple 8 bit, default 128 bit).

2) Kotak Permutasi/ Pemutihan

Algoritma *Blowfish*, menggunakan banyak *subkey*. Kunci-kunci ini wajib dihitung lebih dahulu sebelum dilakukan enkripsi maupun dekripsi. Maksud dari metode yaitu mengacak deretan bit-bit pada sebuah blok. Metode ini bertentangan dengan metode substitusi pada penyamaran bit.

f. Algoritma Base64

Perubahan dari *base64* adalah suatu algoritma untuk *encoding* dan *decoding* data untuk format *ASCII*, bisa berdasarkan bilangan dasar 64 ataupun dikatakan suatu metode yang digunakan untuk melakukan *encoding* (penyedian) untuk *binary*. Karakter yang dibuat untuk perubahan *base64* ini terdiri dari A..Z, a..z dan 0..9, menambahkan simbol ”+” dan ”/” sekaligus sebuah karakter sama dengan (=) diantara dua karakter terakhir guna pengisian, dengan kata lain penyesuaian maupun penggenapan data

binary. Karakter simbol bisa dihasilkan bergantung pada proses algoritma yang dijalankan (Wahyu, Rahangiar, and Fretes, 2012).

2.2. Metode

Metodologi penelitian yang digunakan dengan cara mempelajari study kepustakaan yang erat kaitannya dengan pembahasan referensi dibawah ini :

1) Penulis : Siswo Wardoyo, Rian Fahrizal, dan Zaidal Immamullah
   Judul : Aplikasi Teknik Enkripsi Dan Dekripsi File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android Bentuk SETRUM-Volume 3, No. 1 / ISSN Online : 2301-4652
   Terbitan Jurusan : Teknik Elektro, Universitas Sultan Agung Tirtayasa, Cilegon, Juni – 2014
   Dekripsi Hasil dari penelitiannya ini dapat disimpulkan sebagai berikut :
   Aplikasi enkripsi maupun dekripsi data akan berfungsi secara baik pada telepon genggam android untuk OS android 2.3, 4.0, dan 4.1. Aplikasi dibikin untuk diimplementasikan secara baik guna melakukan enkripsi maupun dekripsi data jika dienkripsi menjadi tidak akan bisa dimengerti isinya. Tahapan dari keamanan aplikasi yang dibikin sangat aman jika algoritma *blowfish* mempunyai panjang kunci yang sangat besar. Untuk memakai kunci yang berjumlah 72 bit dengan kata lain 9 karakter yang diperlukan waktu selama 1,49x108 tahun guna membobolnya untuk kecepatan komputasinya yaitu 106 key/sec.
2) Penulis : Ahmad Timbul Sholeh, Erwin Gunadhi, dan Asep Deddy Supriatna
   Judul : Mengamankan Skrip Pada Bahasa Pemograman PHP Dengan Menggunakan Kriptografi Base 64
   Bentuk : Jurnal / ISSN: 2302-7339
   Terbitan Sekolah Tinggi Teknologi Garut, September – 2012
   Dekripsi Kesimpulan yang dapat diperoleh dari hasil yang telah dikembangkan mengenai cara mengamankan skrip bahasa pemograman PHP, adalah sebagai berikut :
   Dengan adanya cara pengamanan ini, pengembang aplikasi yang menggunakan bahasa pemograman PHP dapat menyembunyikan skrip PHP supaya tidak mudah di salin, diubah sebagian / seluruhnya oleh orang yang tidak berhak.
   Integritas dari aplikasi yang telah di dekripsi akan lebih terjaga, karena skrip sudah dienkripsi tidak dapat diubah. Kelemahan-kelemahan dari alur program yang terdapat dalam aplikasi PHP dapat terjaga otomatis, karena skrip aplikasi PHP tidak bias dibaca kembali, kecuali menggunakan skrip yang belum dienkripsi.
3) Penulis : Aziz Pratama Nugraha, dan Erwin Gunadhi
   Judul : Implementasi Kriptografi *Base64* Untuk Mengamankan URL (*Uniform Resource Locator*) Web-based Untuk Penyerangan *SQL Injection*
   Bentuk Jurnal Algoritma, Vol. 13 No. 1 / ISSN : 2302-7339
   Terbitan Sekolah Tinggi Teknologi Garut, 2016
   Dekripsi Berdasarkan berbagai penjelasan dan hasil penelitian yang telah dilakukan, mengenai cara mengamankan URL website dari serangan *SQL Injection*. Dapat disimpulkan beberapa hal, diantaranya :
   Dengan diterapkannya cara pengamanan ini, URL website dapat disamarkan. Hal tersebut dapat mengatasi serangan yang mengancam keamanan data pada suatu website.
   Integritas dari URL yang telah dienkripsi akan lebih terjaga, karena metode *SQL Injection* tidak dapat diterapkan pada URL yang telah dienkripsi.
4) Penulis : Natsir Mohamad
   Judul : Pengembangan *Prototype* Sistem Kriptografi Enkripsi Dengan Dekripsi Pada Data *Office* Dengan Metode *Blowfish* Menggunakan Bahasa Pemograman Java
   Bentuk Jurnal Format, Volume 6, No. 1 / ISSN : 2089-5615
   Terbitan Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana, 2017
   Dekripsi Berdasarkan permasalahan, studi pustaka, tinjauan penelitian, tinjauan entitas penelitian, metodologi penelitian dan pembahasan produk dengan penelitian Prototipe Sistem Kriptografi kunci simetris menggunakan metode *Blowfish* guna enkripsi dengan dekripsi Data Office dengan Bahasa Pemograman Java, maka dapat disimpulkan sebagai berikut :
   Keamanan metode *Blowfish* yaitu salah satu algoritma yang tidak bisa dipatenkan, cukup kuat karena mempunyai kunci yang sangat besar dan panjangnya bisa beraneka ragam, membuat tidak bisa diserbu bagian kuncinya. Dalam sistem kriptografi yang baik mempunyai kerahasiaan kunci dan bukan pada kerahasiaan algoritmanya. *Blowfish* menggunakan strategi pelaksanaan yang

tepat guna lebih optimal, bisa dijalankan dengan memori kurang dari 5 KB dan kemudahan algoritmanya.
Aplikasi kriptografi algoritma *blowfish* dalam sistem keamanan data office menggunakan enkripsi atau dekripsi bisa memberikan otentikasi, integritas dan non repudiation guna syarat penting untuk hubungan antara penerima dengan pengirim data untuk jati diri dari pemilik data.
Adanya konsep kriptografi enkripsi dengan dekripsi menggunakan metode *Blowfish* adalah cara yang sangat ampuh guna menghilangkan segala kekhawatiran yang akan timbul perubahan data dan banyak dokumen yang bisa dilakukan oleh pihak-pihak yang tidak bertanggung jawab. Sehingga besar data / ukuran file untuk di enkripsi atau dekripsi akan semakin cepat waktu kecepatan guna proses enkripsi dan dekripsinya.

5) Penulis : Tetuko Pambudi Nusa, dan Anita Qoiriah
Judul : Rancangan Aplikasi Enkripsi Database Mysql Menggunakan Algoritma Blowfish
Bentuk : Jurnal Online
Terbitan Universitas Negeri Surabaya, Volume 02 Nomor 01 Tahun 2013, 39-44
Dekripsi Simpulan yang dapat diambil dari pembuatan aplikasi enkripsi *database MySQL* dengan algoritma *Blowfish* adalah : Salah satu cara yang dapat dilakukan untuk meningkatkan pengamanan data yaitu dengan menggunakan algoritma *Blowfish*. Algoritma *Blowfish* ini dapat digunakan untuk mengamankan data dalam *database* yang meliputi *database*, table dan *record*. Dalam penelitian ini *database* yang akan diamankan datanya adalah MySql. Algoritma *Blowfish* dipilih dalam penelitian ini karena algoritma tersebut mampu bekerja pada computer dengan spesifikasi minim, cepat, dan mudah dimengerti. Setelah dilakukan penelitian ini dapat diketahui bahwa enkripsi suatu *database* dapat dilakukan dengan menggunakan algoritma *Blowfish* dengan visual basic 6.0 sebagai bahasa pemogramannya.

6) Penulis : Rio Hamzah
Judul : Implementasi Algoritma RSA Dan Blowfish Untuk Enkripsi Dan
Deskripsi Data Menggunakan Delphi 7
Bentuk : Skripsi
Dekripsi dari teknologi informasi yang berkembang secara cepat, dengan perkembangan teknologi keamanan data. Data adalah hal yang sangat berguna bagi setiap orang ataupun perusahaan, karena adanya perihal yang bersifat rahasia guna orang maupun perusahaan. Karena itu sangat diperlukan suatu teknologi untuk menjaga keamanan dan kerahasiaan data, teknologi tersebut adalah kriptografi.

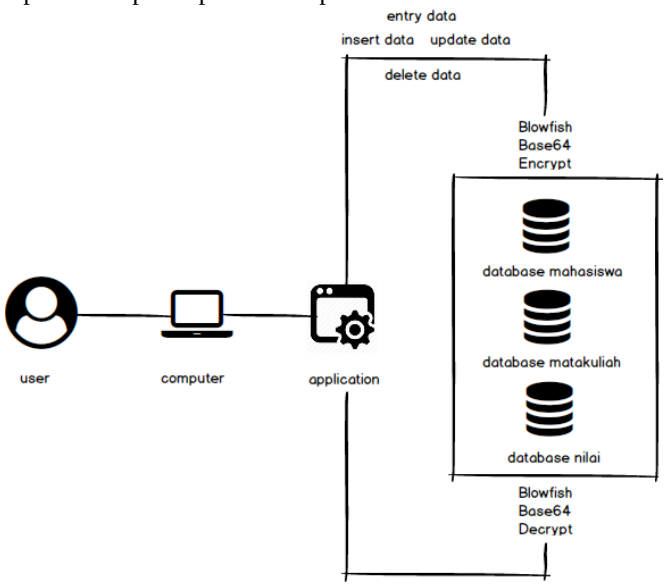
7) Penulis : Mohammad Gilang Kautzar
Judul : Implementasi Sistem Enkripsi Pengiriman Pesan Instan Java Dengan Algoritma Blowfish
Dekripsi Metode : komunikasi yang bersifat *real-time*. Pengiriman pesan pada protokol *YMSG* yang digunakan oleh *Yahoo Messenger* dengan menjalankan transaksi paket antara client dengan server. Pesan yang dienkapsulasikan ke dalam paket-paket tersebut tidak melewati enkripsi, membuat teks pesan bisa dibaca secara langsung. Guna meningkatkan keamanan pesan, maka diimplementasikan suatu sistem enkripsi pada client.

8) Penulis : Donzilo Antonio Meko
Judul : Perbandingan Algotima DES, AES, IDEA, dan Blowfish dalam Enkripsi dan Dekripsi data
Bentuk : Jurnal Teknologi Terpadu Vol. 4, No. 1, Juli 2018
Terbitan : STIMIK Kupang
Dekripsi Kemajuan teknologi informasi telah memberikan dampak yang sangat luas, salah satunya sebagai media penyampaian informasi dari satu tempat ke tempat lainnya, sehingga memudahkan orang dalam mengakses suatu informasi. Kemudahan pengaksesan media komunikasi oleh semua orang, tentunya akan memberikan dampak bagi kemanan informasi atau pesan yang menggunak media komnukasi tersebut. Informasi akan sangat rentan untuk diketahui, dikutip dan dimanipulasi oleh orang yang tidak bertanggung jawab. Oleh sebab itu dibutuhkan suatu metode atau cara untuk menjaga kerahasiaan informasi ini, yang salah satunya dikenal dengan sebutan kriptografi. Dalam kriptografi terdapat banyak algoritma , diantaranya algoritma DES, AES, IDEA, dan Blowfish. Penelitian ini bertujuan untuk membandingkan kinerja beberapa algoritma kriptografi dalam proses enkripsi dan dekripsi data berdasarkan segi kecepatan, atau lama waktu serta ukuran data hasil enkripsi. Hasil penelitian ini menunjukan adanya perbedaan waktu proses dan ukuran data dari hasil enkripsi dan dekripsi data dari masing" algoritma.

3. HASIL DAN PEMBAHASAN

3.1. Arsitektur Sistem Aplikasi

Arsitektur sistem aplikasi kriptografi pada database di Kampus Akademik Telekomunikasi Bogor ada beberapa tahap yaitu mulai dari isi data, data itu di enkripsi ke dalam database, proses dekripsi data di dekrip sebelum melalui proses output dapat di lihat pada Gambar 1.

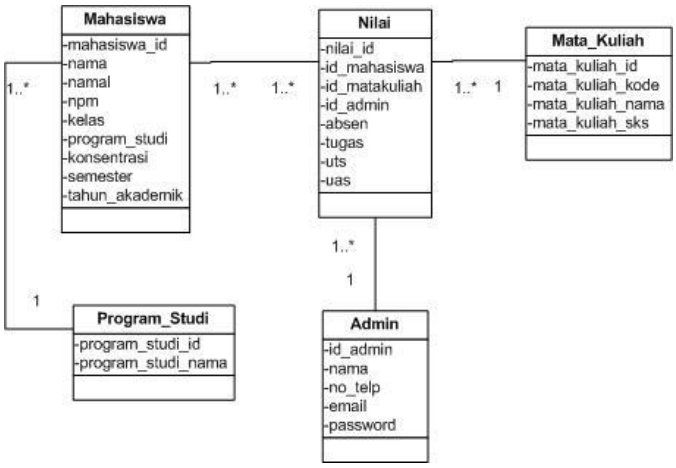


Gambar 1. Arsitektur Sistem Aplikasi

3.2. Rancangan Basis Data

a. *Class* Diagram

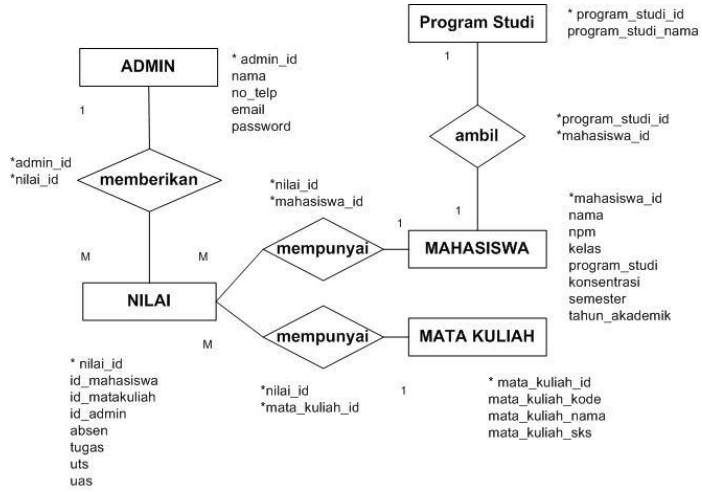
Class Diagram ini menerangkan hubungan antar kelas dengan penjelasannya detail tiap kelas yang berada dalam model *design* suatu sistem. Aturan dan tanggung jawab entitas yang menunjukan perilaku sistem, juga diperlihatkan pada *class diagram*, seperti yang di tunjukan pada Gambar 2.



Gambar 2. *Class* Diagram

b. *ERD (Entity Relationship Diagram)*

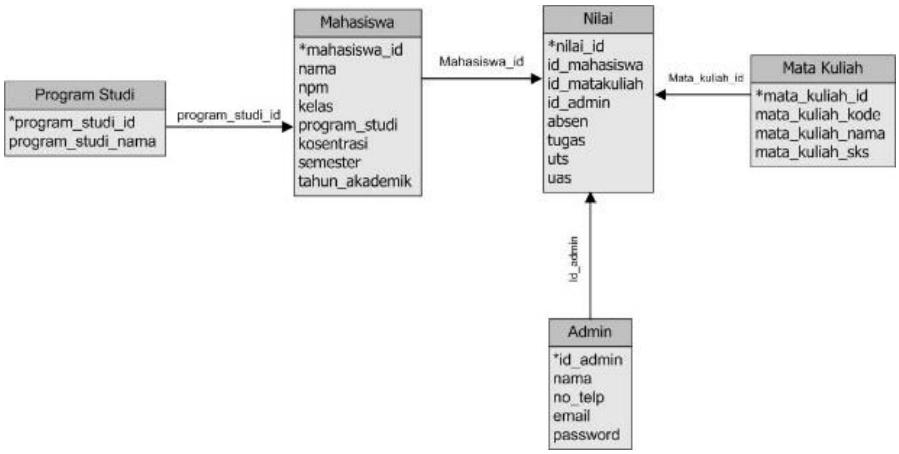
Menurut (Brady dan Loonam, h2010) Entity Relationship Diagram (ERD) dirancang guna menggambarkan maupun membikin model database guna diagram sederhana dapat memudahkan membuat sebuah database yang canggih maupun yang simpel. ERD ini membuat mudah pengguna dalam hal merancang database sehingga membuat perubahan didalam database jika sewaktu-waktu akan terjadi perubahan. Seperti yang di tunjukan pada Gambar 3.



Gambar 3. ERD (Entity Relationship Diagram)

c. *LRS (Logical Record Structure)*

Berdasarkan ERD pada gambar diatas maka didapatkan hasil transformasi ERD ke LRS (*Logical Record Structure)*. Seperti terlihat pada Gambar 4 berikut ini:



Gambar 4. LRS (*Logical Record Structure)*

d. Rancangan Menu

Berdasarkan aplikasi kriptografi sistem informasi akademik pada kampus akademik telekomunikasi bogor yang di buat ada beberapa menu yang ditentunkan.

e. *Flowchart* Ubah Data

Rancangan layar sangat penting dalam membuat suatu aplikasi atau program. Karena itu rancangan layar mesti mudah dimengerti, dan dipahami oleh *user*, supaya *user* merasa nyaman dalam memakainya. Sehingga, rancangan layar tidak membuat bingung seorang *user* dan tidak mengalami kesusahan dalam menjalankan atau mengoperasikan aplikasi ini. Dalam aplikasi ini, akan digambarkan rancangan layar dari masing-masing halaman tampil, tambah data dan hapus data, yaitu rancangan layar *form* login, menu dashboard, menu mahasiswa, menu mata kuliah, dan menu nilai.

3.3. Algoritma Aplikasi

a. Algoritma *Login*

Algoritma form login menjelaskan tentang awal mula user menggunakan aplikasi ini, sebelum menggunakan aplikasi ini user terlebih dahulu harus mengisi form login agar dapat masuk ke menu utama dan bisa menggunakan aplikasi ini. Untuk login user harus memasukan *email* dan *password*.

b. Algoritma *Dashboard*

Algoritma ini menjelaskan proses Menu Utama yang terdiri dari Dashboard, Mahasiswa, Mata Kuliah, Program Studi, Nilai, Bantuan dan Logout. Apabila user memilih menu Mahasiswa user akan ke halaman tampil data mahasiswa dan user dapat menambahkan, mengubah, menghapus data mahasiswa yang sudah terenkripsi oleh aplikasi sama dengan menu mata kuliah, program studi dan nilai dan jika memilih menu Bantuan makan akan tampil Bantuan, terkecuali dengan menu Logout, jika user memilih menu Logout maka akan logout dari aplikasi

c. Algoritma Tampil Mahasiswa

Algoritma ini menjelaskan proses dari tampilan Tampil Data Mahasiswa. Proses dimana *data* yang telah dienkrip ditampilkan kembali kembali menjadi *text* asli akan masuk ke tabel data Mahasiswa.

d. Algoritma Proses Sistem EncodingAlgoritma Base64

Algoritma proses enkripsi ini menjelaskan bagaimana proses algoritma Base64 melakukan proses enkripsi hingga berhasil mendapatkan *ciphertext*. Pada proses ini akan menjelaskan *plaintext* menjadi *chipertext* yang nantinya akan diproses dengan algoritma Base64

e. Algoritma Proses Sistem Deskripsi Blowfish

Algoritma proses dekripsi ini menjelaskan bagaimana proses dekripsi algoritma Blowfish melakukan proses dekripsi hingga berhasil mendapatkan *text* yang asli atau *plaintext*.

3.4. Implementasi Dan Uji Coba Solusi

a. Metode Testing

Metode black box yaitu pengecekan fungsionalitas input/output suatu program atau aplikasi. Pengecekan kondisi input kemudian melakukan sejumlah pengecekan terhadap program atau aplikasi guna menghasilkan suatu output yang nilainya dapat dipertimbangkan. Modul Testing dilakukan dengan pengecekan modul.

b. Data Masukan

Dalam pengecekan akan dibahas perbandingan antara proses enkripsi atau dekripsi data masukan yang dites yaitu data masukan sistem kriptografi *database* akademik. Pengecekannya menggunakan cara mengukur lamanya waktu proses enkripsi dan dekripsi dalam suatu program atau aplikasi.

c. Tabel Enkripsi

Dalam pengujian ini, akan dibahas proses enkripsi pada table data mahasiswa. Pengecekannya yaitu antara lain data asli sebelum di enkripsi, nama mahasiswa.

d. Tabel Deskripsi

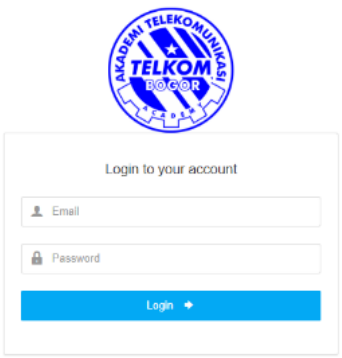
Pengecekan guna membahas suatu proses dekripsi. Pengecekannya dengan kata lain data sistem informasi akademik setelah dilakukan enkripsi yang akan dilakukan dekripsi seperti nama mahasiswa, *key*, menjadi data asli setelah dilakukan dekripsi.

3.5 Tampilan Layar

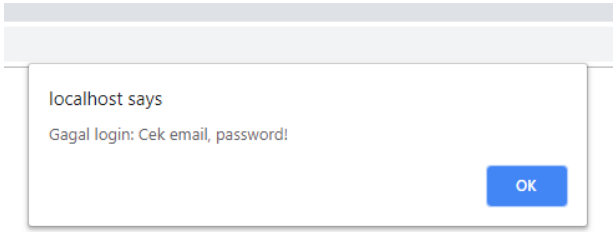
Tampilan layar aplikasi enkripsi dan dekripsi data informasi akademik mahasiswa mulai dari pertama kali aplikasi ini dijalankan sampai dengan selesai. Berikut ini akan diberikan penjelasan dan gambar mengenai tampilan yang ada pada aplikasi enkripsi dan dekripsi informasi akademik pada Kampus Akademi Telekomunikasi Bogor.

a. Tampilan Layar *Form* Login

Tampilan layar *form login*, dapat dilihat pada gambar dibawah ini, berguna untuk masuk menuju menu utama. Rancangan layar *form login*, disediakan menu *username* dan *password*. Tombol *Login* berfungsi untuk proses validasi ke *database*. Jika *username* dan *password* benar, akan tampil menu utama. Jika salah maka akan tampil pesan *error*. Seperti yang disajikan pada gambar 5. Dan 6.



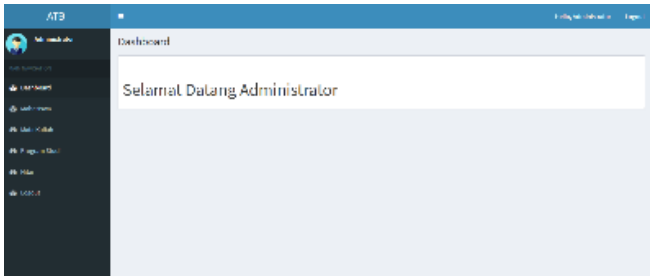
Gambar 5. Tampilan Layar *Form Login*



Gambar 6. Tampilan Layar *Form* Salah

b. Tampilan Layar Menu Dashboard

Tampilan layar dari menu utama bisa dilihat dari Gambar 4.3. *Form* ini akan pertama kali muncul pada saat penggunaan telah berhasil melakukan *login*. Tampilan layar menu *dashboar* disajikan pada gambar 7.



Gambar 7. Tampilan Layar Menu *Dashboar*

4. KESIMPULAN

4.1. Kesimpulan

Dari pengamatan analisa masalah dan penyelesaiannya, dapat disimpulkan bahwa aplikasi program pengamanan *database* berbasis Web-based menggunakan metode *blowfish* dan *base64* sangat diperlukan karena: Sebuah aplikasi yang mengimplementasikan algoritma kriptografi *Blowfish* dan *Base64* untuk enkripsi *database* telah berhasil diciptakan. Dengan adanya aplikasi ini maka *database* yang dianggap penting guna menjaga keamanan dari orang yang tidak berhak untuk mengetahui isi dari *database* tersebut. Diharapkan aplikasi ini dapat menjadi solusi dari kecemasan masyarakat terhadap pentingnya keamanan data yang terdapat dalam *database*. Aplikasi ini telah diatur oleh sistem sehingga isi *database* atau data yang terkandung di dalam *database* tersebut otomatis telah dienkripsi dengan baik.

4.2. Saran

Saran untuk pengembang supaya lebih lanjut lagi agar aplikasi ini dapat menjadi lebih baik, adapun saran yang diberikan antara lain:

a. Dikembangkan menggunakan algoritma Blowfish dan Base64 yang lebih baik lagi, supaya ukuran hasil proses dari data sangat diharapkan menjadi lebih kecil dari sebelumnya.
b. Adanya pengembangan aplikasi berbasis *mobile* dengan menggunakan algoritma yang sama.
c. Program ini dapat dikembangkan dengan menambahkan fitur dan desain yang lebih detail dan lebih baik lagi.

REFERENSI

1. Siswo, W., Rian, F., and Zaldi, I. (2015) 'Aplikasi Teknik Enkripsi Dan Dekripsi File Menggunakan Algoritma Blowfish Dengan Perangkat Ponsel Mobile Berbasis Android', SETRUM, Vol. 3, No. 1.
2. Ahmad, S., Erwin, G., and Asep, S. (2012) 'Mengamankan Skrip Pada Bahasa Pemograman PHP Dengan Menggunakan Kriptografi Base64'. Retrieved September, 2012, Garut: Sekolah Tinggi Teknologi Garut
3. Mohamad, N. (2017). 'Pengembangan *Prototype* Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data *Office* Dengan Menggunakan Metode Blowfish Dengan Bahasa Pemograman Java'. Jurnal Format. Vol. 6, No. 1.
4. Aziz, N., and Erwin, G. (2017) 'Penerapan Kriptografi Base64 Untuk Keamanan URL (*Uniform Resource Locator*) Website Dari Serangan *SQL Injection'*, Jurnal Algoritma, Vol. 13, No.1.
5. Tetuko, N., and Anita, Q. (2014) 'Rancang Bangun Aplikasi Enkripsi Database Mysql Dengan Algoritma Blowfish', Jurnal Online, Vol. 2, No. 1.
6. Rio, H. (2011) 'Implementasi Algoritma RSA Dan Blowfish Untuk Enkripsi Dan Deskripsi Data Menggunakan Delphi 7', Skripsi.
7. Mohammad, K. (2012) 'Implementasi Sistem Enkripsi Pengiriman Pesan Instan Java Dengan Algoritma Blowfish', Skripsi.
8. Donzilo, M. (2018) 'Perbandingan Algoritma DES,AES,IDEA, Dan Blowfish Dalam Enkripsi Dan Dekripsi Data', Jurnal Teknologi Terpadu, Vol. 4, No. 1.
9. Chandra, P., end Banni, A. (2016) 'Sistem Informasi Manajemen Pengarsipan Dengan Menggunakan Algoritma Blowfish', Jurnal Online, Teknik Elektro, Politeknik Negeri Malang, Vol. 2, No. 2.
10. Ady, W., Mujito., end Singgih, S. (2017) 'Implementasi Algoritma Kriptografi Blowfish, Standar.