

APLIKASI KEAMANAN DATABASE MENGGUNAKAN ALGORITMA KRIPTOGRAFI *TRIANGLE CHAIN CIPHER* BERBASIS *DESKTOP*

Ajat Sudrajat¹⁾, Windarto²⁾

¹⁾Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur

^{1,2)}Jl. Raya Ciledug, Petukangan Utara, Jakarta Selatan 12260

Telp. (021) 5853753, Fax. (021) 5866369

E-mail : ajatsudrajat0903@gmail.com¹⁾, windarto@budiluhur.ac.id²⁾

ABSTRAK

Kampus Budi Luhur Salemba adalah cabang dari Universitas Budi Luhur. Dalam melakukan penyimpanan data mahasiswa kampus budi luhur salemba menggunakan fasilitas database agar lebih mudah untuk dikelola. Informasi yang ada di database Oracle diambil oleh aplikasi dan diubah kebentuk file JSON kemudian dikirim dengan cara diunggah ke web kampus pusat untuk dilaporkan. Informasi yang dikirim ke kampus pusat masih sama persis dengan data yang ditampilkan sebagai informasi akhir sehingga masih bisa dilihat oleh pihak yang tidak berwenang. Untuk menjaga data dari pihak yang tidak berwenang maka diperlukan suatu metode pengamanan data agar informasi yang dikirim tidak mudah dilihat atau diakses oleh pihak yang tidak berwenang. Metode yang dimaksud adalah metode enkripsi dengan Algoritma Triangle Chain Cipher. Untuk mengenkripsi data mahasiswa, sebelum data dikirim ke kampus pusat terlebih dahulu data dari Oracle diambil oleh aplikasi untuk dienkrip dan dirubah menjadi database access. Setelah melewati proses enkripsi, kemudian data dikirim melalui web atau email setelah data diterima oleh kampus pusat, data harus didekripsi terlebih dahulu sebelum diolah. Cara kerja dari algoritma ini proses enkripsi pada record dilakukan dua kali jadi tiap-tiap karakter disubstitusi dengan kunci dan faktor yang digunakan sebagai pengali seperti pada formula algoritma, kunci yang digunakan adalah simetrik yaitu kunci untuk enkripsi dan dekripsi sama dan harus bernilai integer. Database yang telah dienkripsi akan berubah menjadi kode ASCII, kode tersebut yang kemudian menjadi ciphertext. aplikasi pengamanan database ini menggunakan VB.Net berbasis desktop. Dengan diterapkannya aplikasi ini, data mahasiswa yang akan dikirim ke kampus pusat diharapkan akan lebih terjaga dari pihak-pihak yang tidak berwenang.

Kata Kunci : *triangle chain cipher*, kriptografi, keamanan

1. Pendahuluan

Seiring dengan perkembangan teknologi informasi yang begitu pesat saat ini dan dengan diiringi kebutuhan masyarakat terhadap informasi yang semakin hari semakin bertambah, berdampak pada perubahan pola pikir masyarakat, lembaga ataupun perusahaan dalam mendapatkan informasi. Sebagai contoh, informasi yang dahulu mudah didapat dari media cetak, sekarang sudah menggunakan media internet. Begitu pentingnya nilai suatu informasi yang akurat dan terpercaya, mengharuskan para pakar komputer untuk memikirkan bagaimana cara untuk mengamankan sebuah informasi yang sifatnya rahasia dan tidak boleh diketahui oleh siapapun. Hal tersebut dilakukan agar sebuah informasi tetap terjaga dengan aman, sehingga membuat rasa nyaman kepada penggunaanya.

Kampus Budi Luhur Salemba adalah cabang dari Universitas Budi Luhur. Untuk memudahkan pengelolaan data mahasiswa, kampus Budi Luhur Salemba menggunakan sistem informasi, informasi tersebut disimpan ke database Oracle. Informasi yang ada di database secara berkala akan diambil dan diubah ke file JSON untuk dikirimkan ke kampus pusat, informasi yang dikirim ke kampus pusat

masih sama persis dengan data yang ditampilkan sebagai informasi akhir sehingga masih bisa dilihat oleh pihak yang tidak berwenang. Tentunya data tersebut sangat rentan mengalami manipulasi, perubahan ataupun penambahan data yang dilakukan oleh pihak yang tidak punya kewenangan akan data tersebut sehingga data yang ada disalahgunakan.

Untuk meminimalisir segala bentuk penyalahgunaan informasi, Kampus Budi Luhur Salemba tersebut perlu mengamankan data mahasiswa sebelum dikirim ke kampus pusat. Maka dibutuhkan suatu teknik pengamanan. Salah satu teknik pengamanan data ialah kriptografi. Dengan menggunakan metode kriptografi, data akan diubah dalam bentuk sandi sehingga tidak mudah dibaca bahkan jika data berhasil dicuri pun tidak mudah untuk membukannya karena tidak berbentuk data asli. Metode kriptografi yang dapat digunakan untuk pengamanan data, salah satunya adalah Algoritma *Triangle Chain Cipher*. Algoritma ini melakukan penyandian pada karakter sebanyak dua kali dan bergabung pada hasil proses sebelumnya, tiap-tiap karakter disubstitusi dengan kunci dan faktor yang digunakan sebagai pengalinya yang menghasilkan penyandian berdasarkan kode ASCII 256.

Diharapkan dengan mengenkripsi data mahasiswa yang dikirim ke kampus pusat, data tersebut akan lebih terjaga dari penyalahgunaan oleh pihak-pihak yang tidak berwenang.

Setelah melihat dari latar belakang diatas, maka bisa dirumuskan atau diambil permasalahannya yaitu data mahasiswa yang dikirim dari kampus cabang ke kampus pusat masih dalam keadaan seperti data aslinya sehingga berpotensi atau rentan untuk disalahgunakan jika terjadi pencurian data.

Setelah menganalisa permasalahan yang ada maka pertanyaan riset yang dapat diajukan adalah bagaimana cara mengamankan data mahasiswa agar data yang dikirim dari kampus cabang ke kampus pusat tidak mudah terbaca oleh pihak yang tidak berwenang ?.

Agar penelitian ini terarah dan tidak keluar dari pembahasan, maka penulis memberikan batasan-batasan dalam penelitian ini diantaranya:

- Algoritma yang digunakan untuk enkripsi dan dekripsi *database* ini adalah algoritma *triangle chain chiper*.
- Data yang dienkripsi adalah data mahasiswa pada *table* MMAHASISWACABANG.
- Data yang dienkripsi akan disimpan dalam format *Ms. Access*.
- Hasil enkripsi yang ditampilkan berdasarkan kode *ASCII 256*.
- Kunci (*key*) yang digunakan hanya dibatasi angka 1 sampai dengan 20.

2. LANDASAN TEORI

2.1 DATABASE

Database atau basis data adalah sekumpulan data atau informasi digital yang dibuat secara sistematis dan dapat dimodifikasi oleh pembuatnya dan dapat diakses setiap saat, *database* sendiri terdiri dari baris dan kolom (tabel) dan dapat saling terhubung dengan tabel yang lainnya, dengan diterapkannya *database* akan lebih efisien dalam pengelolaan data dan informasi[5].

2.2 KRIPTOGRAFI

Menurut Ningtyas [3]. Kriptografi sendiri diabil dari bahasa Yunani, ada dua suku kata dari kriptografi yaitu *crypto* dan *graphia* yang artinya 'penulisan rahasia'. Sedangkan kriptografi adalah suatu ilmu ataupun seni yang mempelajari bagaimana pesan yang dikirim sampai dengan aman kepada yang menerimanya. Kriptografi sendiri hadir untuk meminimalisir segala bentuk kejahatan pencurian, manipulasi data oleh pihak-pihak tertentu yang tidak sah.

Algoritma kriptografi terdiri dari tiga fungsi [1] yaitu:

- Enkripsi : merupakan pengamanan data atau informasi yang dijaga kerahasiaannya. Enkripsi juga bisa dirtikan sebagai proses memanipulasi suatu data atau informasi sehingga sulit dan bahkan tidak lagi mudah untuk dimengerti.
- Dekripsi: merupakan pengembalian data atau informasi yang telah diamankan sebelumnya ke bentuk semula tanpa mengalami kerusakan sedikitpun.
- Kunci: Kunci (*Key*) yang digunakan untuk proses enkripsi dan dekripsi terdiri dari dua kunci yaitu kunci rahasia dan kunci umum.



Gambar 2:1 Mekanisme Kriptografi

Proses kriptografi pada dasarnya sangat sederhana. *Plaintext* akan dilewatkan pada proses enkripsi sehingga menghasilkan *ciphertext*. Kemudian, untuk memperoleh kembali *plaintext*, *ciphertext* melalui proses dekripsi akan menghasilkan kembali *plaintext*. Secara matematis prosesnya dapat dinyatakan sebagai berikut:

- Proses enkripsi

$$C = E(M)$$

Keterangan:

M = pesan asli / *plaintext*

E = *enkripsi*

C = pesan yang tersandikan

- Proses dekripsi

$$M = D(C)$$

Keterangan:

M = pesan asli

D = proses dekripsi

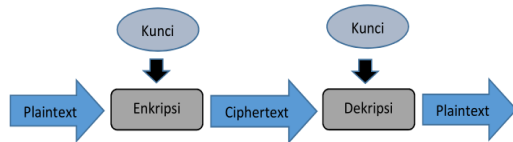
C = pesan yang tersandikan

Kriptografi yang digunakan dalam penyandian ini adalah algoritma yang disebut *cipher*. Kerahasiaannya sangat bergantung pada algoritma yang digunakan. Oleh karena itu, algoritmanya harus dirahasiakan. Kriptografi yang digunakan pada kelompok yang besar dengan anggota yang senantiasa berubah akan menimbulkan masalah. Permasalahan timbul jika ada anggota yang meninggalkan kelompok. Jika itu yang terjadi, algoritma harus diganti karena anggota tersebut bisa saja membocorkan algoritma. Selain memanfaatkan algoritma, kriptografi modern juga menggunakan kunci (*key*) untuk memecahkan masalah keluarnya anggota kelompok. Proses enkripsi dan dekripsi dilakukan dengan kunci. Masing-masing anggota

mempunyai kunci sendiri, sehingga dilakukan perubahan pada gambar 2.1 menjadi seperti gambar 2.2 berikut:

Gambar 2.2: Kriptografi Berbasis Kunci

Mekanisme kriptografi pada gambar 2.2 dinamakan kriptografi berbasis kunci. *Cryptosystem* akan terdiri atas algoritma dan kunci beserta segala *plaintext* dan *ciphertext* -



nya. Persamaan matematisnya menjadi seperti berikut:

- a. Proses enkripsi

$$C = E_e(M)$$

Keterangan:

M = pesan asli / plaintext

E = proses enkripsi

C = pesan yang tersandikan

e = kunci enkripsi

- b. Proses dekripsi

$$M = D_d(C)$$

Keterangan:

M = pesan asli

D = proses dekripsi

C = pesan yang tersandikan

d = kunci dekripsi

Dalam perkembangannya ada dua jenis algoritma kriptosistem, yaitu algoritma enkripsi kunci simetrik dan algoritma enkripsi kunci asimetrik.

- d. Kriptografi Kunci Simetrik

Kriptografi kunci simetrik (*symmetric cryptosystem*) menggunakan kunci yang pada prinsipnya identik untuk proses enkripsi dan dekripsi, tetapi satu buah kunci dapat pula diturunkan dari kunci lainnya. Kriptografi kunci simetrik kadang disebut kriptografi kunci rahasia (*secret-key cryptography*) yang merupakan bentuk kriptografi yang lebih tradisional, dimana sebuah kunci tunggal dapat digunakan untuk mengenkripsi dan mendekripsi pesan.

Kriptografi kunci simetrik mengarah pada metode enkripsi dimana baik pengirim maupun penerima memiliki kunci yang sama. Secara matematis kriptografi kunci simetrik dapat dinyatakan dengan persamaan berikut:

$$E_k(m) = c$$

$$D_k(c) = m$$

Keterangan:

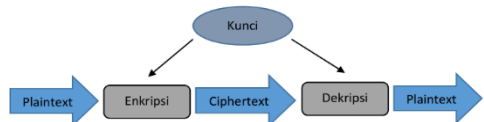
E=proses enkripsi

m = Plaintext

D = proses dekripsi

C = Ciphertext

K = kunci yang digunakan baik untuk proses enkripsi maupun proses dekripsi

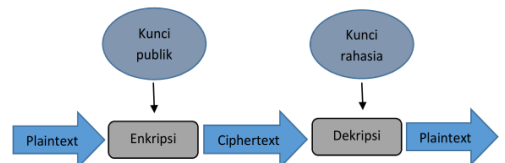


Gambar 2.3: Kriptografi Berbasis Kunci Simetris

Dengan menggunakan metode kriptografi kunci simetris maka pengirim dan penerima informasi harus menyetujui kunci yang digunakan dimana kedua belah pihak tidak takut pesan dicuri. Meskipun memiliki kelemahan, kriptografi kunci simetrik juga memiliki keuntungan seperti kecepatan operasi yang jauh lebih tinggi dibandingkan dengan kriptografi asimetrik

- e. Kriptografi Kunci Asimetris

Kriptografi kunci asimetrik (*asymmetric cryptosystem*) menggunakan dua buah kunci. Satu kunci dapat dipublikasikan (kunci publik) sedangkan kunci yang lain harus dirahasiakan (kunci rahasia), seperti diilustrasikan pada gambar 2.4 berikut:



Gambar 2.4: Kriptografi Yang Berbasis Kunci Asimetrik

- (1) Kunci umum (*public key*): adalah kunci yang siapa saja boleh tahu.
- (2) Kunci rahasia (*private key*): kunci yang sangat hasiakan (tidak boleh dipublikasikan).

Dengan kunci public pengguna hanya dapat mengenkripsi data atau pesan akan tetapi tidak dapat untuk mendekripsinya dan hanya penggunanya saja yang mempunyai kunci rahasia untuk mendekripsinya kembali. Algoritma asimetri dapat mengirim data lebih aman dari pada algoritma simetris.

2.3 EMPAT TUJUAN KRIPTOGRAFI

Dalam ilmu kriptografi Ada empat tujuan yang mendasar dan merupakan aspek keamanan didalam kriptografi diantaranya [1].

- Confidentiality* (Kerahasiaan) adalah layanan yang menjaga kerahasiaan suatu pesan atau data agar tidak bisa dibaca oleh sembarang orang atau pihak yang tidak berhak.
- Data *Integrity* (Integritas) adalah layanan yang memastikan bahwa pesan atau data yang diterima asli dan belum mengalami manipulasi.
- Authentication* (Otentikasi) adalah layanan yang memastikan bahwa pengirim maupun penerima pesan saling mengidentifikasi kebenaran antara dua belah pihak yang sedang berkomunikasi.
- Non-repudiation* (ketiadaan penyangkalan) adalah layanan yang menjamin bahwa tidak ada penyangkalan suatu transaksi yang dilakukan.

2.4 ALGORITMA TRIANGLE CHAIN CIPHER (TCC)

Menurut Hondro dan Nurcahyo [2]. Algoritma kriptografi *triangle chain cipher* adalah perkembangan dari algoritma *One Time Pad* dimana kunci yang digunakan secara otomatis dan banyaknya kunci sebanyak *plaintext*, Algoritma ini mempunyai aturan seperti *Caesar Cipher* dimana setiap karakter akan digeser menggunakan kunci, kunci yang digunakan harus bernilai integer guna untuk menggeser karakter, karakter yang dienkripsi selama dua kali dan akan bergantung pada hasil enkripsi sebelumnya sehingga disebut algoritma segitiga berantai, algoritma ini juga memperbaiki enkripsi substitusi abjad tunggal yang rentan mengalami analisis frekuensi.

a. Algoritma Enkripsi TCC

Berikut ini adalah rumus enkripsi dari algoritma *triangle chain cipher*:

- Rumus Matriks Enkripsi Segitiga Pertama

Rumus baris pertama:

$$M[1j] = P[j] + (K * R[1j]) \text{ Mod } 26$$

Rumus baris kedua dan seterusnya untuk nilai $j \geq i$:

$$M[ij] = M[i-1j] + (K * R[ij]) \text{ Mod } 26$$

Sehingga didapat nilai *ciphertext*-nya sebagai berikut:

$$M[ij] \text{ pada nilai } j = (N+1) - N$$

- Rumus Matrik Enkripsi Segitiga kedua

Nilai P didapat dari nilai M i j pada i = j

Rumus baris pertama:

$$M[1j] = P[j] + (K * R[1j]) \text{ Mod } 26$$

Rumus baris kedua dan seterusnya untuk nilai $j \leq (N+1) - i$:

$$M[ij] = M[i-1j] + (K * R[ij]) \text{ Mod } 26$$

Sehingga didapat nilai *ciphertext*-nya sebagai berikut:

$$M[ij] \text{ pada nilai } j = (N+1) - i$$

Keterangan:

P = Plaintext atau karkter

N = Jumlah karakter atau plaintext

M = Matriks yang penampung hasil enkripsi

K = Kunci enkripsi

R = Row (adalah faktor pengali yang di kalikan dengan kunci)

i = adalah indeks faktor sebagai pengali

j = index karakter atau *plaintext* pada baris

b. Algoritam Dekripsi TCC

Berikut ini adalah rumus enkripsi dari algoritma *triangle chain cipher*:

- Rumus Matriks Dekripsi segitiga pertama.

Rumus baris pertama :

$$M[1j] = C[j] - (K * (R[1j])) \text{ Mod } 26$$

Rumus untuk baris kedua:

$$j \leq (N+1) - i$$

$$M[ij] = M[i-1j] - (K * (R[ij])) \text{ Mod } 26$$

Setelah hasil nilai plaintext didapat dari hasil proses segitiga pertama kemudian diambil setiap barisnya dengan ketentuan sebagai berikut:

$$M[ij] \text{ dengan nilai } i=n \text{ dan } j \leq (N+1) - i$$

- Rumus Matriks Dekripsi segitiga kedua. Rumus untuk baris pertama:

$$M[1j] = C[j] - (K * (R[1j])) \text{ Mod } 26$$

Rumus untuk baris kedua:

$$j \geq i$$

$$M[ij] = C[i-1j] - (K * (R[ij])) \text{ Mod } 26$$

sehingga nilai plaintext yang didapat untuk ciphertext yang asli adalah sebagai berikut: $M[ij] \text{ pada nilai } j = (N+1) - N$

Keterangan:

P = Plaintext atau karkter

N = Jumlah karakter atau plaintext

M = Matriks yang penampung hasil enkripsi

K = Kunci enkripsi

R = Row (adalah faktor pengali yang di kalikan dengan kunci)

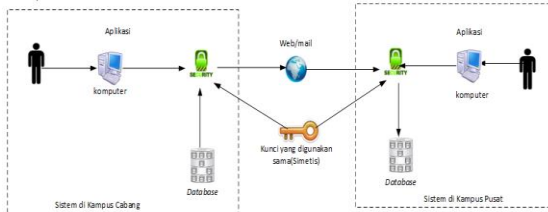
i = adalah indeks faktor sebagai pengali

j = index karakter atau *plaintext* pada baris

3. SISTEM DAN APLIKASI

3.1 Arsitektur Sistem

Untuk memahami memahami konsep aplikasi yang akan dibangun dapat melihat gambar arsitektur sistem pada gambar 3.1 pada gambar arsitektur sistem menggambarkan rancangan sitem secara garis besar dari proses keseluruhan sistem yang dibangun.



Gambar 3.1: Arsitektur sistem

3.2 Rancangan Layar

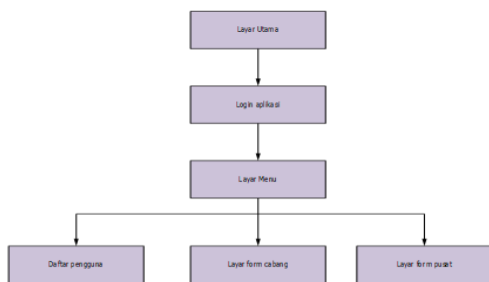
Perancangan merupakan proses yang dilakukan oleh penulis untuk melakukan perancangan aplikasi yang akan dibangun. Perancangan aplikasi yang dibuat secara umum adalah enkripsi dan dekripsi menggunakan kriptografi simetrik dengan algoritma *Triangle Chain Cipher* berbasis desktop, adapun beberapa tahap dalam perancangan aplikasi adalah sebagai berikut:

a. Proses

Perancangan proses yang dimaksud adalah bagaimana sistem akan bekerja, proses-proses yang digunakan mulai dari user melakukan login lalu melakukan pemilihan data yang kemudian diproses oleh aplikasi sehingga dapat mengeluarkan output berupa hasil enkripsi data tersebut. Begitu pula dengan proses untuk dekripsi data.

b. Antarmuka (Interfaces)

Perancangan antarmuka mengandung penjelasan tentang desain dan implementasi sistem yang digunakan dalam aplikasi seperti pada gambar berikut.



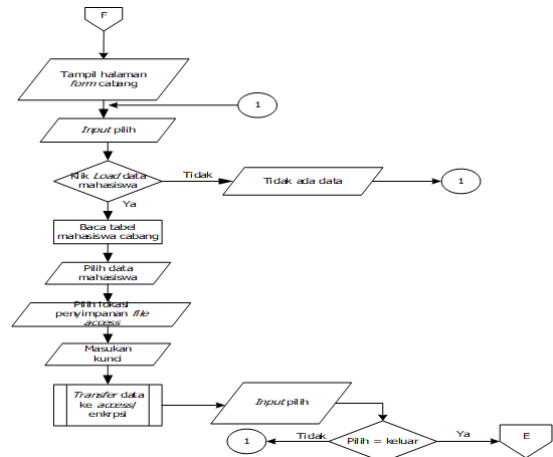
Gambar 3.2: Rancangan Sistem

3.3 FLOWCHART PROGRAM

a. Flowchart Halaman Form Cabang

Flowchart halaman form cabang menggambarkan alur proses dari halaman

form cabang. Flowchart disajikan dalam gambar berikut:



Gambar 3.3: Flowchart Form Cabang

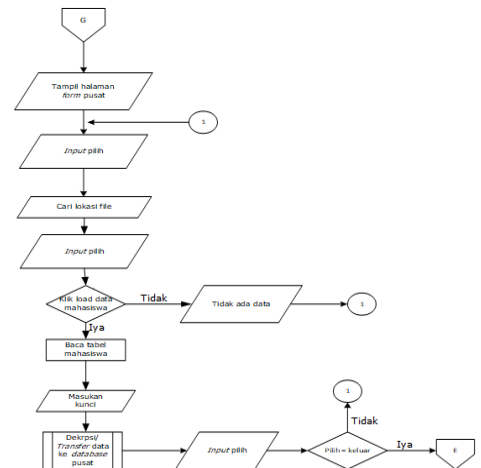
Keterangan:

E = halaman menu

F = halaman form cabang

b. Flowchart Halaman Form Pusat

Flowchart halaman form Pusat menggambarkan alur proses dari halaman form Pusat. Flowchart disajikan dalam gambar berikut:



Gambar 3.4: Flowchart Form Pusat

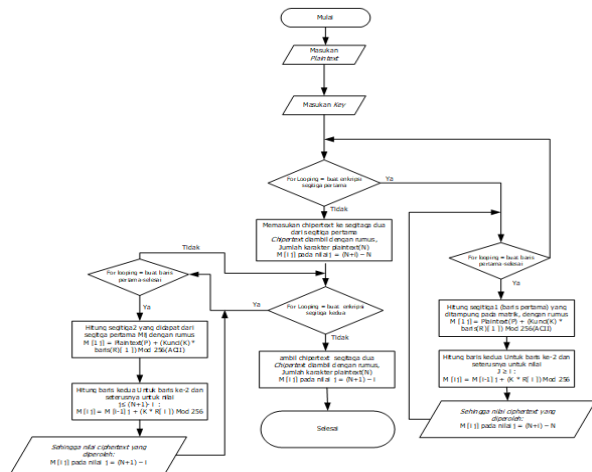
Keterangan:

E = halaman menu

G = halaman form pusat

c. Flowchart proses enkripsi Triangle Chain Cipher.

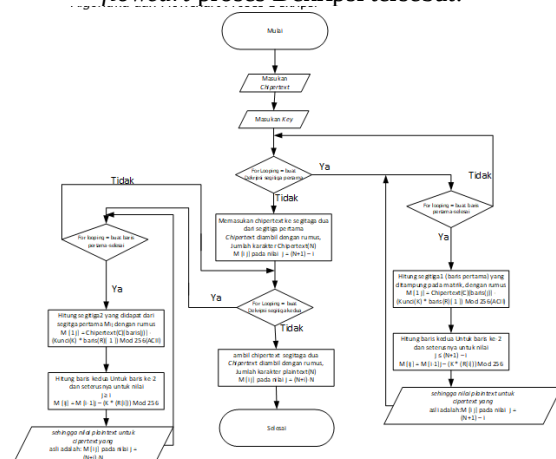
Flowchart ini menjelaskan apa saja yang terjadi pada proses pengembalian plaintext ke ciphertext (enkripsi) pada *Triangle Chain Cipher*. Flowchart disajikan dalam gambar berikut:



Gambar 3.5: *Flowcart* Proses Enkripsi

d. *Flowcart* proses dekripsi *Triangle Chain CIPHER*.

Dan berikut adalah Algoritma untuk *flowchart* proses Dekripsi tersebut:



Gambar 3.6: *Flowcart* Proses Dekripsi

4. Tampilan Layar dan Pengujian Program

4.1 Proses pengujian enkripsi

Pengujian proses enkripsi dengan cara menjalankan proses penarikan data mahasiswa dari *database* kampus cabang yang kemudian setelah data melewati proses enkripsi akan di simpan ke *Ms. Access*. Data yang diuji adalah tabel MMAHASISWACABANG. Berikut ini adalah Pengujian dengan mengenkripsi lima belas *record* seperti pada gambar berikut.

Form Cabang									
Load Data Mahasiswa							Kuliah		
NO	CRM	CNRM	KDOKLO	CNAMA	CALAMAT	CNORMH	CRT	CRW	
☒	1211530070		3	Sipnadi Alifan	Jl. Daulat Turin LRI, F	10	006	014	
☒	1211530082		3	ARIEF ARDIYANTO	Jl Cemara 2 Blok A5, Jati Asih		001	002	
☒	1211530090		3	Ti Shiro Wilaya	Jl. Benteang IV, Surter Jaya		006	009	
☒	1211530108		3	Alpa Syahfira Prodia	Jl. Nenas Gg. Pesmeran, Uluu Kay	36C	003	020	
☒	1212530024		3	Sopanto	Jl. Kayu Menei 1 Lema, Palimem Jak...		001	08	
☒	1212530032		3	Bayu Mahdha	Jl. Sendaing Batai Jaya	27	011	005	
☒	1212530040		3	Nusadi Purno	Cempaka Blauh Uti, Cempaka Putih	31A			
☒	1212530057		3	Hen Sarinya Purni	Jl. Pengayonan 1	35	012	009	
☒	1212530088		3	Eka Ita Nurazzi	Jl. Kramat, Sentrong	1105			
☒	1212530096		3	Murati Hanif	Taman Pulo Gelang Blok C6/4		006	013	
☒	1212530020		3	Dimes Anggie Permana	Jl. Kemuning Pulo, Bering Delang	45	001	01	
☒	1212530046		3	Muhammad Al Anas	Jl. Sengodai Denda 11, Senayan	14A	001	002	
☒	1212530053		3	Pevay Dedy Restanti	Gg Kembarang Nunung Timor	28	05	01	
☒	1211531517		3	Ast Sutisna	Rt. Gunung Pual	28	05	01	
☒	1215500311		3	Alvendi Mustafa Al-Jufri	Jl Methandi 1 Blok M 40 Dondor Riang	14	05	01	
< Jumlah Record : 15 >									
☒ Plih Sensus Data ☐ Plih Lokasi Penyempurnan File Access ☐ T:\Tugas Akhir\ppl\data/cabang.accds Masukkan Key Urutak, Enkrip Data 									
Transfer Data Ke Access									

Gambar 4.1 Proses Sebelum Di Enkripsi

Setelah proses enkripsi lima belas *record* berhasil maka data akan disimpan ke *Ms. Access*

[illegible]

Gambar 4.2: Hasil Sesudah Di Enkripsi

4.2 Proses Pengujian Dekripsi

Pengujian proses dekripsi dengan cara mengembalikan *file Ms. Access* yang sudah di enkripsi ke bentuk semula, Berikut adalah proses dekripsi data dengan lima belas *record* seperti pada gambar berikut.

Form Pustak											
Cat Logok File D:\Tugas Akhir\Apt\dataabcabc.doc											
Load Data Mahasiswa											Keluar
NO	CNIM	CNIRM	CKDLOK	CNAMA	CALAMAT	CNORMH	CRT	CRW	CNOTELP		
☐	1	1211530074	(	IQ4YE5="Tc,4a2	S'4ed,4c AY1B6	i	IEO	IED	u04944000 AUS		
☐	2	1211530082		W'444444444444	444444444444		IEI	IEI	u04944000 AUS		
☐	3	1211530090		444444444444	444444444444		IEI	IEI	u04944000 AUS		
☐	4	1211530108		444444444444	444444444444		IEI	IEI	u04944000 AUS		
☐	5	1211530024		444444444444	444444444444		IEI	IEI	u04944000 AUS		
☐	6	1211530032		444444444444	444444444444		IEI	IEI	u04944000 AUS		
☐	7	1211530040		444444444444	444444444444		IEI	IEI	u04944000 AUS		
☐	8	1211530057		444444444444	444444444444		IEI	IEI	u04944000 AUS		
☐	9	1211530088		444444444444	444444444444		IEI	IEI	u04944000 AUS		
☐	10	1211530096		444444444444	444444444444		IEI	IEI	u04944000 AUS		
☐	11	1211530020		444444444444	444444444444		IEI	IEI	u04944000 AUS		
☐	12	1211530046		444444444444	444444444444		IEI	IEI	u04944000 AUS		
☐	13	1211530053		444444444444	444444444444		IEI	IEI	u04944000 AUS		
☐	14	1311511537		444444444444	444444444444		IEI	IEI	u04944000 AUS		
☐	15	153150181		444444444444	444444444444		IEI	IEI	u04944000 AUS		

Gambar 4.3: Proses Sebelum Di Dekripsi

Setelah data berhasil dibalikan ke bentuk semula maka data tesebut di *transfer* ke *database*

[illegible]

Gambar 4.4: Hasil Sesudah Di Dekripsi

4.3 Tabel Hasil Pengujian Enkripsi Dan Dekripsi

Dalam tabel pengujian akan dibahas perbandingan antara proses enkripsi dan dekripsi *record* tabel MMAHASISWACABANG. Dari data hasil pengujian-pengujian telah dilakukan, maka dapat dijelaskan pada tabel 4.1 dan 4.2.

Tabel 4.2: Hasil Pengujian Proses Enkripsi

Pengujian	Jumlah Record	Ukuran (size) sebelum	Ukuran (size) sesudah	Waktu proses
Pengujian 1	Satu record	283 bytes	283 bytes	07.20 detik
Pengujian 2	Dua record	560 bytes	560 bytes	11.40 detik
Pengujian 3	Lima belas record	4.502 bytes	4.502 bytes	01:19.31 detik

Tabel 4.2: Hasil Pengujian Proses Dekripsi

Pengujian	Jumlah Record	Ukuran (size) sebelum	Ukuran (size) sesudah	Waktu proses
Pengujian 1	Satu record	283 bytes	283 bytes	05.34 detik
Pengujian 2	Dua record	560 bytes	560 bytes	09.62 detik
Pengujian 3	Lima belas record	4.502 bytes	4.502 bytes	01:15.54 detik

4.4 Analisa Hasil uji Program

Berdasarkan hasil analisa terhadap hasil pengujian program, ditemukan beberapa kelebihan dan juga kekurangan dari program ini, yaitu sebagai berikut:

- 1) Kelebihan Program
 - (1) Waktu proses dekripsi lebih cepat dari proses enkripsi.
 - (2) Aplikasi ini dilengkapi dengan halaman bantuan sehingga memudahkan pengguna.
 - (3) data hasil dekripsi tidak mengalami kerusakan dan dapat kembali dibaca oleh pengguna.
- 2) Kekurangan Program
 - (1) Program ini hanya dapat mengenkripsi *text*.
 - (2) Perhitungan waktu proses enkripsi maupun dekripsi masih manual.

5. KESIMPULAN

1.1 KESIMPULAN

Berdasarkan dari hasil pengujian dan analisis yang telah dilakukan dengan berbagai variasi data uji, maka dapat diambil kesimpulan bahwa:

- a. Algoritma pengamanan database dengan triangle chain cipher berjalan dengan baik pada aplikasi berbasis *Desktop*.
- b. Dengan adanya aplikasi kriptografi menggunakan metode *Triangle Chain Cipher* ini dapat mengamankan data atau informasi mahasiswa universitas budi luhur cabang salemba sebelum dikirim ke

kampus pusat, agar lebih aman dari pihak-pihak yang tidak berwenang.

- c. Aplikasi dapat melakukan proses enkripsi dan dekripsi pada *record* tabel *mmahasiswacabang*.
- d. Aplikasi ini juga dapat mengembalikannya data yang sudah disandikan atau diamankan menggunakan metode *Triangle Chain Cipher* menjadi data semula tanpa mengalami perubahan.

1.2 SARAN

Tentunya dalam pembuatan aplikasi ini masih belum sempurna, oleh karena itu diperlukannya pengembangan untuk meningkatkan kemampuan aplikasi tersebut, berikut beberapa masukan serta saran sebagai perbaikan dan pengembangan, yaitu:

- a. Aplikasi ini diharapkan dapat mengenkripsi selain *text*.
- b. Aplikasi ini diharapkan dapat menggunakan metode kompresi sehingga menghemat penyimpanan.

DAFTAR PUSTAKA

- [1] Donny, A. 2008. *Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi*. Yogyakarta: C.V Andi Offset.
- [2] Hondro, R.K., dan Gunadi, W.N., 2014. Analisis dan Perancangan Sistem yang Menerapkan Algoritma Triangle Chain Cipher (TCC) Untuk Enkripsi Record Tabel Database. *Jurnal Informasi & Pengembangan Iptek*, 3(2), hal. 118-127.
- [3] Ningtyas, A.L., 2015. Pengertian Data dan Informasi. <http://ayulestariningtyas.blog.widyatama.ac.id/2016/02/29/pengertian-data-dan-informasi/> [Diakses Oktober 10, 2017].
- [4] Singh, S., 2016. Implementasi Pengamanan File Text dengan Metode Triangle Chain Cipher dan RC4. <http://Repository.Potensi-Utama.Ac.Id/Jspui/Handle/123456789/1290> [Diakses November 12, 2017].
- [5] Situmorang, H., 2016. Keamanan Basis Data Dengan Teknik Enkripsi. *Jurnal Mahajana Informasi*, 1(1), hal. 22-27.
- [6] Sommerville, I., 2003. *Rekayasa Perangkat Lunak*. Terj. Yuhilza Mahnum. Jakarta: Erlangga.