Implementasi Sistem Keamanan Database Menggunakan Metode Triangle Chain

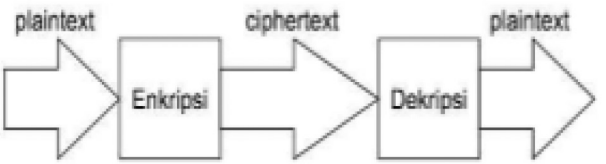
Yeni Yanti*, Munawir, Zulfan, Erdiwansyah
Teknik Informatika, Fakultas Teknik, Universitas Serambi Mekkah
Jl. Tgk. Imum Lueng Bata Desa Bathoh, Kota Banda Aceh, Propinsi Aceh, Indonesia
***Koresponden email**: yeniyanti@serambimekkah.ac.id

Abstrak. Masalah keamanan dan kerahasiaan data merupakan hal yang penting dalam suatu organisasi. Data yang bersifat rahasia tersebut perlu dibuatkan sistem penyimpanan dan pengirimannya agar tidak terbaca atau diubah oleh orang- orang yang tidak bertanggung jawab, baik saat data tersebut tersimpan sebagai file di dalam komputer maupun saat data tersebut dikirim melalui email.Sering kali masalah keamanan kurang mendapat perhatian dari pemilik berkas, perancang dan pengelola sistem informasi tersebut. Salah satu cara mengantisipasinya adalah dengan metode kriptografi yang merupakan ilmu dan seni untuk menjaga keamanan pesan. Penelitian ini bertujuan mengimplementasi sistem keamanan database dengan membangun prototipe sistem keamanan menggunakan metode Triangel Chain. Algoritma Kriptografi *Triangel Chain* merupakan algoritma yang difungsikan untuk melakukan pengenkripsi *database*, sebuah data input data ASCII dapat dijaga kerahasian dari sebuah *database*. Adapun pengujian yang dilakukan dalam penelitian ini menggunakan databaseadalah jenis file yang berisi data teks normal tanpa tanpa format lain didalamnya. Dengan masing-masing file pengenkripsian untuk melakukan pemilihan algoritma yang digunakan dan teks sebagai kinerja dari metode algoritma enkripsi database. Hasil yang didapat aplikasi sistem keamanan berbasis visual basic dapat digunakan untuk mengamankan sistem informasi database.
Kata kunci : *Sistem Keamanan, File Teks, Metode Triangle Chain, Enkripsi, ASCII*

Abstract. Data security and confidentiality issues are important in an organization. The confidential data needs to be set up for storage and delivery systems to be unreadable or modified by irresponsible people, either when the data is stored as a file on the computer or when the data is sent via email. Often the security issue gets less attention From the file owner, designer and manager of the information system. One way to anticipate it is by cryptographic method which is the science and art to keep message security. This study aims to implement text file security system by building prototype of security system using Triangle Chain method. Triangle Chain Cryptography algorithm is an algorithm that is enabled to encrypt the file, an ASCII data input data can be kept confidential from a text file. The testing done in this study using a text file is a file type that contains normal text data without any other formatting therein. With each encryption file to perform the selection of the algorithm used and the text as the performance of the text file encryption algorithm method. The results obtained by visual-based security-based application system can be used to secure the text file information system.
Keywords*: Security System, Text File, Triangle Chain Method, Encryption, ASCII*

1. Pendahuluan

Dengan berkembangnya teknologi informasi diharapkan dapat menjadi media yang paling efektif untuk mencari dan menyebarkan. Salah satunya adalah komputer yang saat ini sudah bukan barang baru dan kini tidak hanya digunakan untuk kepentingan perkantoran tetapi juga dapat digunakan untuk kepentingan bisnis. Oleh sebab itu komputer telah menjadi kebutuhan manusia dan memberikan manfaat yang luar biasa,bukan saja digunakan oleh ribuan pakar untuk mengakases komputer berbagi file, dan mengirim e-mail(surat elektronik), tetapi lebih dari itu komputer telah menciptakan suatu sistem informasi global yang



Gambar 1. *Mekanisme Enkripsi dan Deskripsi*

menjadikan dunia ini semakin kecil [1].

Masalah keamanan dan kerahasiaan data merupakan hal yang penting dalam suatu organisasi. Data yang bersifat rahasia tersebut perlu dibuatkan sistem penyimpanan dan pengirimannya agar tidak terbaca atau diubah oleh orang- orang yang tidak bertanggung jawab, baik saat data tersebut tersimpan sebagai file di dalam komputer maupun saat data tersebut dikirim melalui email. Untuk menyimpan data tersebut agar benar-benar aman, tentunya dilakukan sistem pengamanan yang baik, yang bebas dari jangkauan orang-orang yang tidak berhak, baik bebas dari jangkauan secara fisik maupun secara sistem[2].

Algoritma Kriptografi *Triangle Chain* merupakan algoritma yang difungsikan untuk melakukan pengenkripsi *file*, sebuah data input data ASCII dapat dijaga kerahasian dari sebuah *file* teks. Dari keamanan data tersebut menimbulkan tuntutan akan tersedianya suatu sistem pengamanan data yang lebih baik agar dapat mengamankan data dari berbagai ancaman yang mungkin timbul[5].

Berdasarkan latar belakang inilah maka peneliti berkeinginan mengangkat permasalah tersebut sebagai bahan penelitian. Adapun judul penelitian adalah " Implementasi Sistem Keamanan Database Enkripsi dan Dekrippsi menggunakan Metode Triangle Chain".

2. Studi Literatur

2.1. Kriptografi

Kriptografi (*cryptographi*) berasal dari BahasaYunani: "*cryptos*" artinya "*secret*" (rahasia), sedangkan "*graphein*" artinya "*writing*" (tulisan). Sehingga kriptografi berarti "*secret writing*" (tulisan rahasia). Jadi kriptografi didefinisikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya kebentuk yang tidak dapat dimengerti lagi maknanya. Secara umum kriptografi merupakan teknik pengamanan informasi yang dilakukan dengan cara mengolah informasi awal (plainteks) dengan suatu kunci tertentu menggunakan suatu metode enkripsi tertentu sehingga menghasilkan informasi baru (chipertext) yang tidak dapat dibaca secara langsung. Chipertext tersebut dapat dikembalikan menjadi informasi awal (plainteks) melalui proses deskripsi [4].

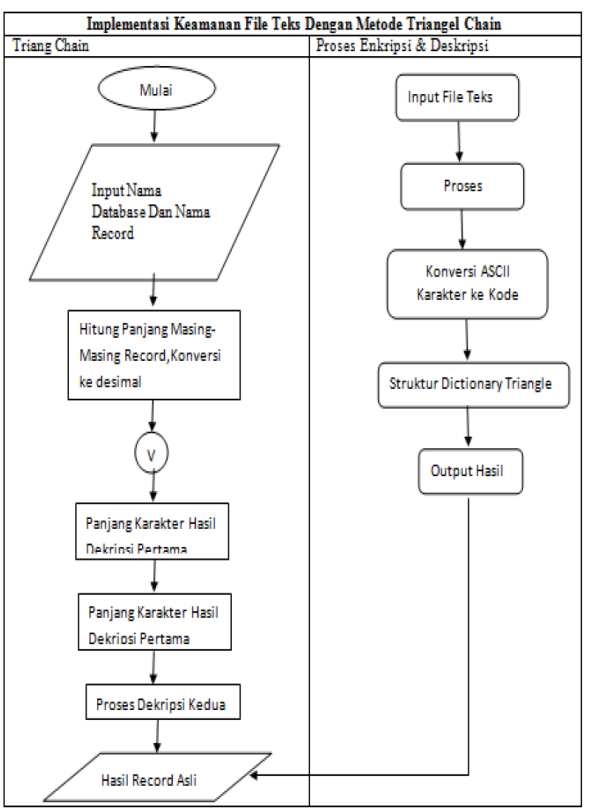
Urutan proses kriptografi secara umum dapat dilihat pada Gambar 1. Terdapat dua jenis algoritma kriptografi berdasar jenis kuncinya :

1. Algoritma Simetri (konvensional)
2. Algoritma Asimetri (kunci public)

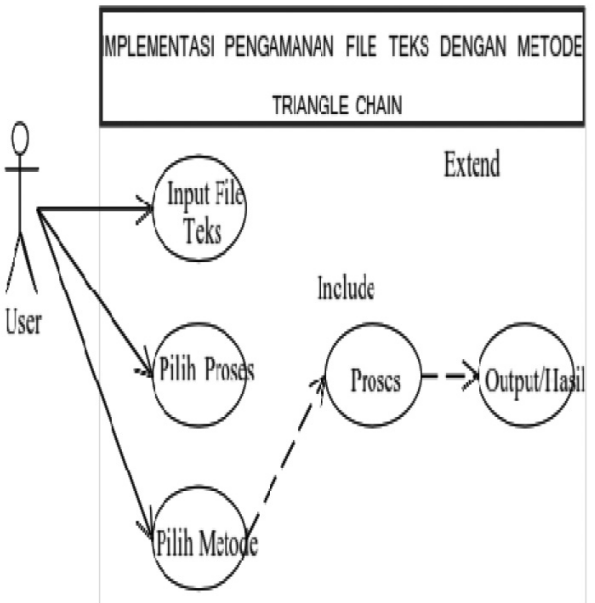
2.2 Tujuan Kriptografi

4 aspek yang terdapat pada kriptografi:

1. *Confidentiality* (kerahasiaan) Layanan yang ditujukan untuk menjaga pesan agar tidak dapat dibaca oleh pihakpihak yang tidak berhak.
2. *Authentication* (otentikasi) Penerima pesan dapat memastikan keaslian pengirimnya. Penyerang tidak dapat berpura-pura sebagai pengirim atau penerima pesan.



Gambar 2. *Diagram Enkripsi & Dekripsi*



Gambar 3. *Use Case Diagram Pengguna Aplikasi*

3. *Integrity* (integritas) Penerima harus dapat memeriksa apakah pesan telah dimodifikasi ditengah jalan atau tidak. Seorang penyusup seharusnya tidak dapat memasukkan tambahan ke dalam pesan, mengurangi atau mengubah pesan selama data berada di perjalanan.
4. *Nonrepudiation* (nirpenyangkalan) Pengirim tidak dapat mengelak bahwa dia telah mengirim pesan, penerima juga tidak dapat mengelak bahwa dia telah menerima pesan tersebut[4].

2.3 Algoritma Triangle Chain

Algoritma kriptografi triangle chain atau umumnya dikenal dengan sebutan rantai segitiga merupakan cipher yang ide awalnya dari algoritma kriptografi One Time Pad, yaitu kunci yang dibangkitkan secara random dan panjang kunci sepanjang *plainteks* yang akan dienkripsi. Tetapi pada algoritma kriptogarfi rantai segitiga pembangkitan kunci-kunci tersebut secara otomatis dengan teknik berantai.

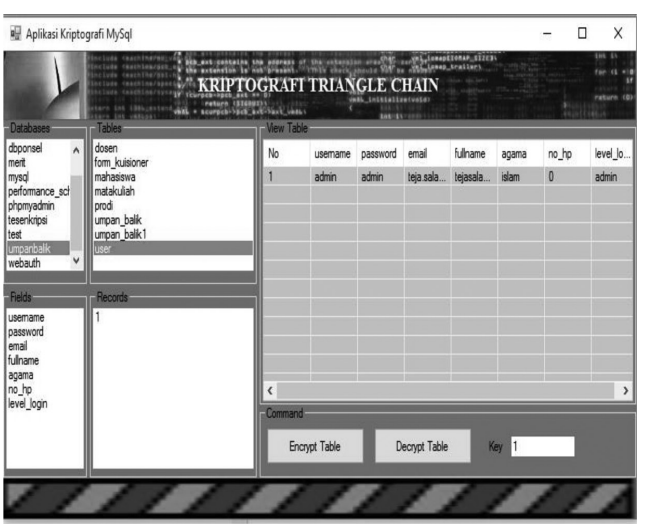
Algoritma rantai segitiga ini memiliki aturan substitusi berdasar pada *caesar cipher* yaitu dengan pergeseran huruf-huruf. Kekuatan cipher ini terletak pada kunci yaitu nilai integer yang menunjukkan pergeseran karakter-karakter sesuai dengan operasi pada caesar cipher. Kekuatan kedua terletak pada barisan bilangan-bilangan yang berfungsi sebagai pengali dengan kunci. Barisan bilangan tersebut dapat berupa bilangan tertentu seperti deret bilangan ganjil, deret bilangan genap, deret fibonancci, deret bilangan prima, serta deret bilangan yang dapat dibuat sendiri. Pada kenyataannya cipher substitusi segitiga tidak dibuat secara sederhana, tetapi dengan mengenkripsi ganda (mengenkripsi dua kali), jadi plainteks dienkripsi dengan cipher segitiga I, kemudian hasil enkripsi pertama dienkripsi kembali dengan cipher segitiga II yang arah segitiga II merupakan kebalikan arah segitiga I.

Untuk itu maka standar untuk cipher segitiga ini adalah cipher segitiga ganda yaitu cipher rantai segitiga yang melakukan enkripsi ganda, yaitu dengan membuat pola enkripsi pertama dengan mengerucut ke arah kanan dan enkripsi kedua mengerucut ke arah kiri. Secara matematis pola enkripsi rantai segitigadapat digambarkan dengan matriks N x N dengan N merupakan panjang plainteks yang akan dienkripsi dan operasi pada alfabet ASCII [5].

3. Perancangan Sistem

3.1 Sistem Perancangan

Sistem pengiriman informasi yang dienkripsi dan di deskripsikan dapat dilihat pada gambar 3.1. Kegiatan atau pengguna aplikasi enkripsi file teks, pengguna dapat memahami hasil penelitian ini dan dapat dimanfaatkan khususnya dibidang



Gambar 4. *Enkripsi Database*

implemeantasi pengamanan *database* dan melakukan enkripsi terhadap suatu *database* yang sifatnya rahasia, dari hasil algoritma *tringel chain* [3].

Untuk U*se case* diagram digunakan untuk menggambarkan aplikasi dan perilaku pengguna, dapat dilihat pada gambar 3.2. Adapun kegiatan aktor atau pengguna pada aplikasi enkripsi *database*, pengguna dapat memilih melakukan proses enkripsi *database* atau dekripsi *database* serta memilih metode yang akan digunakan. Dari proses akan menampilkan media ataupun hasil *output* dari hasil kerja algoritma *triangle chain* [3].

4. Hasil Dan Pembahasan

Dalam melakukan proses penginputan database yaitu dengan cara menentukan lokasi tempat penyimpanan database dan memilih database yang akan di enkripsi. Setelah memilih database, maka akan muncul table, fields dan jumlah record. Untuk lebih jelas dapat dilihat pada Gambar 4.

Berdasarkan Gambar 4 dapat dijelaskan bahwa untuk enkripsi database, hal yang dilakukan adalah memilih database yang akan dienkripsi, selanjutnya muncul nama tabel dan fields. Setelah muncul nama table, maka pilih tombol enkripsi dan masukkan key.

Setelah melakukan proses enkripsi, maka akan muncul hasilnya yaitu berupa chipertext. Untuk lebih jelasnya dapat dilihat pada Gambar 5.

5. Daftar Pustaka

Novianto A, Sahfitri V, Tujni B. 2014. Penerapan Metode Pengamanan Data Enkrispsi Dan Dekripsi Menggunakan Metode Twofish Pada PT.Gaya Makmur Tractor. Januari 2014

Rahajoeningroem T, Aria M. 2013. Studi Dan Implementasi Algoritma Rsa Untuk Pengamanan Data Transkrip Akademik Mahasiswa. Majalah Ilmiah Unikom Vol.8, No. 1. Page 77-90

Singh, Sanwinder .2016. Implementasi Pengamanan Database Dengan Metode Triangle Chain Atau Rc4. Http://Repository.Potensi-Utama.Ac.Id/Jspui/Handle/123456789/1290. Desember 2016

Wahana Komputer. "Memahami Model Enkripsi & Security Data". Penerbit Andi. Yogyakarta. 2003.

Zebua, *Taronisoki*. 2013 . Analisa Dan Implementasi Algoritma Triangle Chain Pada Penyandian Record Databese. Articles. Vol 3, No 2 . April 2013