ANALISA DAN IMPLEMENTASI ALGORITMA TRIANGLE CHAIN PADA PENYANDIAN RECORD DATABASE

Taronisokhi Zebua

Staf Pengajar Program Studi Manajemen Informatika STMIK Budi Darma Medan
Jl. Sisingamangaraja No. 338 Simpang Limun Medan
Email : taronizeb@gmail.com

Abstrak

Database merupakan data yang harus dijaga dan dipelihara oleh pemilik sistem informasi. Pemutakhiran informasi yang disajikan melalui sebuah sistem dapat dilakukan dengan adanya database. Sebuah database terdiri dari banyak record yang mengisi setiap field tabel yang telah tersedia di dalamnya. Record-record inilah yang nantinya akan menjadi informasi output yang disajikan kepada para pengguna sistem. Algoritma triangle chain merupakan salah satu algoritma penyandian yang beroperasi berdasarkan penyandian (kriptografi) klasik khususnya dalam teknik substitusi terhadap karakter. Setiap karakter akan disubstitusi berdasarkan kunci dan faktor pengali yang telah ditetapkan berdasarkan formula yang berlaku dalam algoritma ini. Algoritma ini melakukan penyandian pada record sebanyak dua kali dan selalu bergantung pada hasil proses sebelumnya. Hal inilah yang mendasari rumitnya pemecahan dari algoritma penyandian berantai ini. Penyandian record database merupakan salah satu hal yang sangat penting dilakukan dalam meningkatkan keamanan database dari berbagai tingkat kejahatan yang dilakukan oleh orang-orang yang tidak berhak dan tidak bertanggungjawab. Implementasi algoritma triangle chain pada penyandian record database dapat mempersulit siapa saja yang berhasil mengakses dan mendapatkan database untuk memahami dan mengerti, merusak, mendistribusikan, mencuri database atau tindakan lain yang dapat merugikan pihak-pihak pemilik database.

Kata kunci : *Record, Database, Kriptografi, Triangle Chain*

1. Pendahuluan

Database secara umum merupakan susunan *record* data operasional lengkap dari suatu organisasi atau perusahaan, yang diorganisir dan disimpan di dalam media penyimpanan secara terintegrasi yang dapat dijadikan sebagai salah satu sumber dari setiap sistem informasi yang sedang berjalan sehingga mampu memenuhi informasi yang optimal yang dibutuhkan oleh para pengguna. Dengan adanya *database*, maka proses pemutakhiran informasi dapat dilakukan. *Database* dapat dibuat dengan menggunakan *software* yang ada seperti Microsoft SQL Server, Oracle, MySQL, Microsoft Access, dBase III, Paradox, FoxPro, dan lain-lain. Selanjutnya *database* dimaksud dapat diintegrasikan dengan aplikasi yang dibuat untuk melakukan beberapa operasi DBMS (*Database Management System*).

Sering sekali *record* yang tersimpan di dalam *database* masih persis sama dengan teks-teks yang ditampilkan sebagai informasi akhir bagi pengguna. Hal ini dapat mempermudah seorang kriptanalis maupun orang lain yang tidak mempunyai hak akses untuk dapat mengetahui secara langsung isi dari *database* tersebut serta dapat memberi peluang kepada mereka untuk melakukan pembocoran, mendistribusikan maupun melakukan modifikasi lain terhadap *record database* tersebut.

Algoritma *triangle chain* atau umumnya dikenal dengan sebutan algoritma rantai segitiga merupakan

cipher yang ide awalnya dari algoritma kriptografi *One Time Pad*, yaitu kunci yang dibangkitkan secara *random* dan panjang kunci sepanjang *plaintext* yang akan dienkripsi. Pada algoritma kriptografi *triangle chain* ini pembangkitan kunci-kunci tersebut secara otomatis dilakukan dengan teknik berantai. 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.

2. Landasan Teori

2.1 Kriptografi

Penjagaan sebuah informasi sangatlah diperlukan agar tidak jatuh ke tangan orang-orang yang tidak berhak untuk mengaksesnya. Teknik kriptografi telah banyak digunakan sebagai salah satu cara untuk menciptakan sebuah informasi yang selalu terjaga keabsahannya[1].

2.1.1 Defenisi Kriptografi

Kriptografi pada awalnya merupakan ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kemudian seiring dengan berkembangnya kriptografi yaitu kriptografi tidak lagi

sebatas mengenkripsikan pesan, tetapi juga memberikan aspek keamanan yang lain seperti serangan dari kriptanalisis. Oleh karena itu pengertian kriptografi pun berubah menjadi ilmu sekaligus seni untuk menjaga keamanan pesan.

Cryptography (kriptografi) berasal dari bahasa Yunani yaitu dari kata *crypto* yang berarti penulisan *secret* (rahasia), sedangkan *graphein* artinya *writing* (tulisan). Jadi secara sederhana dapat diartikan *secret writing* (tulisan rahasia). Definisi lain dari kriptografi adalah sebuah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi[2].

Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain[1].

2.1.2 Algoritma Kriptografi

Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut. Algoritma kriptografi terdiri dari tiga fungsi dasar[1] :

1. Enkripsi
Merupakan hal yang sangat penting dalam kriptografi, merupakan pengamanan data yang dikirim agar terjaga kerahasiaannya. Pesan asli disebut *plaintext*, yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan sebagai *cipher* atau kode dengan menggunakan algoritma yang untuk mengkodekan data yang kita inginkan.
2. Dekripsi
Merupakan kebalikan dari proses enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (teks asli), disebut dengan dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma yang digunakan untuk enkripsi.
3. Kunci
Kunci adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, kunci rahasia (*private key*) dan kunci umum (*public key*).

Berdasarkan kunci yang dipakai dalam proses kriptografi, maka algoritma kriptografi dibagi menjadi[1]:

1. Algoritma Simetri
Algoritma ini sering disebut dengan algoritma klasik karena memakai kunci yang sama untuk kegiatan enkripsi dan dekripsi. Bila mengirim pesan dengan menggunakan algoritma ini, si penerima pesan harus diberitahu kunci dari pesan tersebut agar bisa mendekripsikan pesan yang dikirim. Keamanan dari pesan yang menggunakan algoritma ini tergantung pada kunci. Algoritma yang menggunakan kunci simetris misalnya DES,

Kode Rivest's, IDEA, AES, OTP, A5 dan lain-lain.

2. Algoritma Asimetri
Algoritma asimetri sering juga disebut dengan algoritma kunci publik, dengan arti kata kunci yang digunakan untuk melakukan enkripsi dan dekripsi berbeda. Pada algoritma asimetri kunci terbagi menjadi dua bagian yaitu kunci umum (*public key*) yang bisa diketahui oleh umum dan kunci rahasia (*private key*) yaitu kunci yang dirahasiakan dan hanya boleh diketahui oleh satu orang saja.
3. Fungsi Hash
Fungsi hash sering disebut dengan fungsi has satu arah (*one way function*), *message digest*, *fingerprint*, fungsi kompresi dan *Message Authentication Code* (MAC) yang merupakan suatu fungsi matematika yang mengambil masukan panjang variabel dan mengubahnya ke dalam urutan biner dengan panjang yang tetap. Algoritma kriptografi tersebut harus memiliki kekuatan untuk melakukannya[1]:
1. Konfusi/pembingungan (*confusion*), dari teks terang sehingga sulit untuk direkonstruksikan secara langsung tanpa menggunakan algoritma dekripsinya.
2. Difusi/peleburan (*diffusion*), dari teks terang sehingga karakteristik dari teks terang tersebut hilang sehingga dapat digunakan untuk mengamankan informasi.

2.1.3 Algoritma Kriptografi Klasik

Sebelum komputer ada, kriptografi dilakukan dengan menggunakan pensil dan kertas. Algoritma kriptografi (*cipher*) yang digunakan saat itu, dinamakan juga algoritma klasik, adalah berbasis karakter, yaitu enkripsi dan dekripsi dilakukan pada setiap karakter pesan. Semua algoritma klasik termasuk ke dalam sistem kriptografi simetris dan digunakan jauh sebelum kriptografi kunci publik ditemukan.

Kriptografi klasik memiliki beberapa ciri[1]:

1. Berbasis karakter
 2. Menggunakan pena dan kertas saja, belum ada komputer
 3. Termasuk ke dalam kriptografi kunci simetris.
- Tiga alasan mempelajari algoritma klasik :
1. Memahami konsep dasar kriptografi
 2. Dasar algoritma kriptografi modern
 3. Memahami kelemahan sistem kode.

Pada dasarnya, algoritma kriptografi klasik dapat dikelompokkan ke dalam dua macam *cipher*, yaitu[1]:

1. *Cipher substitusi* (*substitution cipher*)
Di dalam *cipher substitusi* setiap unit *plaintext* diganti dengan satu unit *ciphertext*. Satu "unit" di isini berarti satu huruf, pasangan huruf atau dikelompokkan lebih dari dua huruf. Algoritma substitusi tertua yang diketahui adalah *Caesar*

cipher yang digunakan oleh kaisar Romawi, Julius Caesar (sehingga dinamakan juga *caesar cipher*), untuk mengirimkan pesan yang dikirimkan kepada gubernurnya.

2. *Cipher* transposisi (*transposition cipher*)

Pada *cipher* transposisi, huruf-huruf di dalam plainteks tetap saja, hanya saja urutannya diubah. Dengan kata lain algoritma ini melakukan *transpose* terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah permutasi atau pengacakan (*scrambling*) karena *transpose* setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.

2.1.3.1 Algoritma *Triangle Chain* (Rantai Segitiga)

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 kriptografi 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 *fibonacci*, deret bilangan prima, serta deret bilangan yang dapat dibuat sendiri[3].

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 segitiga dapat digambarkan dengan matriks $N \times N$ dengan N merupakan panjang plainteks yang akan dienkripsi dan operasi pada alfabet ASCII.

Matriks dilambangkan dengan M_{ij} , dengan $1 \leq i \leq N$ dan $1 \leq j \leq N$, nilai integer kunci dengan K , faktor pengali merupakan tabel integer R . Plainteks dengan P dimana P merupakan tabel plainteks dengan panjang

N yaitu $P[N]$.

Berikut operasi matriks untuk proses enkripsi[3]:

1. Matriks enkripsi segitiga pertama

Untuk baris ke-1 :

$$M_{1j} = P[j] + (K * R[1]) \bmod 256$$

untuk baris ke-2 dan selanjutnya untuk nilai $j \geq i$:

$$M_{ij} = M_{(i-1)j} + (K * R[i]) \bmod 256$$

sehingga nilai *cipherteks* yang diperoleh adalah :

$$M_{ij} \text{ pada nilai } j = (N+i)-N.$$

2. Matriks enkripsi segitiga kedua

Nilai P diperoleh dari nilai M_{ij} pada $i = j$

Untuk baris ke-1 :

$$M_{1j} = P[j] + (K * R[1]) \bmod 256$$

untuk baris ke 2 dan selanjutnya untuk nilai $j \leq (N+1) - i$:

$$M_{ij} = M_{(i-1)j} + (K * R[i]) \bmod 256$$

sehingga nilai *cipherteks* yang diperoleh adalah :

$$M_{ij} \text{ pada nilai } j = (N+1)-i.$$

Keterangan :

P = Plainteks

N = Jumlah karakter plainteks

M = Matriks penampung hasil penyandian

K = Kunci

R = *Row* (baris perkalian faktor pengali dengan kunci)

i = Indeks faktor pengali

j = Indeks karakter plainteks

Sedangkan untuk proses dekripsi merupakan kebalikan dari proses enkripsi Berikut operasi matriks untuk proses dekripsi (Mohamad Firda Fauzan.Studi dan Implementasi Chiper Substitusi Rantai Segitiga. 12 Februari 2012. <http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2006-2007/Makalah1/Makalah1-088.pdf>) :

1. Matriks dekripsi segitiga pertama operasinya merupakan kebalikan dari matriks enkripsi, jadi operasi ini kebalikan operasi matriks enkripsi segitiga kedua. Nilai C merupakan tabel dari *cipherteks* dengan panjang N yaitu $C[N]$.

Untuk baris ke-1, berlaku formula :

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

$$M_{1j} = C[j] - (K * R[1]) \bmod 256$$

sedangkan untuk baris kedua dan selanjutnya

dimana nilai $j \geq i$, berlaku formula : $M_{ij} = (M_{(i-1)j} - K * (R[i])) \bmod 256$.

$$j - K * (R[i]) \bmod 256.$$

sehingga nilai *plainteks* yang diperoleh adalah :

$$M_{ij} \text{ pada nilai } j = (N+i)-i.$$

2. Matriks dekripsi segitiga kedua

Untuk baris pertama berlaku formula :

$$M_{1j} = C[j] - (K * R[1]) \bmod 256$$

sedangkan untuk baris kedua dan seterusnya

nilai $j \geq i$, berlaku formula :

$$M_{ij} = C_{[i-1]j} - (K * R[i]) \bmod 256.$$

nilai *plainteks* yang diperoleh adalah :

$$M_{ij} \text{ pada nilai } j = (N+1)-i.$$

sehingga nilai *plainteks* yang diperoleh adalah :
 M_{ij} pada nilai $j = (N+i)-N$.

Keterangan :

C = *Cipherteks*

N = Jumlah karakter *cipherteks*

M = Matriks penampung hasil *cipher* yang dijadikan sebagai *plaintext*

K = Kunci

R = *Row* (baris perkalian faktor pengali dengan kunci)

i = Indeks faktor pengali

j = Indeks karakter *cipherteks*

3. Analisa

3.1 Enkripsi Record Database

Record yang disandikan merupakan *record* yang terdapat di setiap *field* tabel *database* yang telah dipilih sebelumnya. Langkah-langkah yang dilakukan pada proses enkripsi *record* mengikuti aturan-aturan yang berlaku pada algoritma *triangle chain*. Sebelum proses enkripsi *record* dilakukan, terlebih dahulu setiap karakter dari *record* harus dikonversi ke dalam bilangan desimal sesuai dengan nilai-nilai pada tabel ASCII. Hal kedua yang dilakukan adalah pembacaan nilai kunci dan pembentukan tabel faktor pengali selanjutnya proses enkripsi *record* dilakukan. Nilai kunci yang digunakan merupakan bilangan integer positif (bukan nol), serta barisan bilangan pengali dapat menggunakan bilangan integer asli atau bilangan tertentu seperti deret bilangan ganjil, deret bilangan genap, deret bilangan prima, serta deret bilangan yang dapat dibuat sendiri. Proses enkripsi *record database* sesuai dengan algoritma *triangle chain* dapat digambarkan seperti pada gambar 1:

Gambar 1 :Gambaran Umum Proses Penyandian Record Database

Proses enkripsi dilakukan dengan dua tahap yaitu enkripsi segitiga pertama dan enkripsi segitiga ke dua, sehingga dihasilkan *chiper* akhir yang nantinya menjadi *record database*. Penyelesaian tahap enkripsi di atas dapat diuraikan melalui contoh kasus

penyandian sebuah *record* di bawah ini :

3. Matriks enkripsi segitiga pertama

Plainteks adalah TARONI

Kunci adalah 3 (bilangan integer asli)

Faktor pengali dengan kunci adalah deret bilangan asli (1, 2, 3, ..., n).

Langkah pertama yang dilakukan untuk proses enkripsi pertama ini adalah menentukan nilai desimal masing-masing karakter *plainteks* dalam ASCII :

T	A	R	O	N	I
84	65	82	79	78	73

Langkah ke dua adalah membentuk tabel faktor pengali :

Seperti pada kasus di atas, maka faktor pengali yang digunakan adalah deretan bilangan asli. Jumlah deret bilangan akan disesuaikan dengan jumlah banyaknya karakter dari *plainteks*.

Jadi, jumlah karakter *plainteks* (N) adalah 6. Deret bilangan asli (R) yang menjadi faktor pengali adalah 1, 2, 3, 4, 5, 6.

Langkah ke tiga adalah melakukan proses enkripsi segitiga pertama sesuai dengan formulanya.

Plainteks (P) = TARONI

N = 6

K = 3

R = 1,2,3,4,5,6

Untuk baris pertama ($i = 1$), maka :

$M_{11} = (P[1] + 3 * R[1]) \text{ mod } 256$
 $= (T + 3 * (1)) \text{ mod } 256$
 $= (84 + 3) \text{ Mod } 256$
 $= 87 \text{ (huruf "W" dalam karakter ASCII 256)}$

$M_{12} = (P[2] + 3 * R[1]) \text{ mod } 256$
 $= (A + 3 * (1)) \text{ Mod } 256$
 $= (65 + 3) \text{ Mod } 256$
 $= 68 \text{ (huruf "D" dalam karakter ASCII 256)}$

$M_{13} = (P[3] + 3 * R[1]) \text{ mod } 256$
 $= (R + 3 * (1)) \text{ Mod } 256$
 $= (82 + 3) \text{ Mod } 256$
 $= 85 \text{ (huruf "U" dalam karakter ASCII 256)}$

$M_{14} = (P[4] + 3 * R[1]) \text{ mod } 256$
 $= (O + 3 * (1)) \text{ mod } 256$
 $= (79 + 3) \text{ Mod } 256$
 $= 82 \text{ (huruf "R" dalam karakter ASCII 256)}$

$M_{15} = (P[5] + 3 * (1)) \text{ mod } 256$
 $= (N + 3 * (1)) \text{ mod } 256$
 $= (78 + 3) \text{ Mod } 256$
 $= 81 \text{ (huruf "Q" dalam karakter ASCII 256)}$

$M_{16} = (P[6] + 3 * (1)) \text{ mod } 256$

$= (I + 3 * (1)) \text{ mod } 256$
 $= (73 + 3) \text{ Mod } 256$
 $= 76 \text{ (huruf "L" dalam karakter ASCII 256)}$

ASCII 256)

hasil sandi pada tahap $i = 1$ (baris pertama) adalah WDURQL.

Sampai pada tahap ini hasil penyandian dapat ditunjukkan di bawah ini :

TARONI (nilai desimal dalam ASCII : 84 65 82 79 78 73) $\rightarrow i = 0$

WDURQL (nilai desimal dalam ASCII : 87 68 85 82 81 76) $\rightarrow i = 1$

Hasil penyandian baris pertama ($i = 1$) akan digunakan sebagai plainteks pada proses enkripsi baris ke dua ($i = 2$), dimana nilai $j \geq i$, sehingga :
 $i = 2, j = 2$

$$\begin{aligned} M_{22} &= (M_{(2-1)2} + 3 * (2)) \bmod 256 \\ &= (M_{(1)2} + 3 * (2)) \bmod 256 \\ &= (D + 6) \bmod 256 \\ &= (68 + 6) \bmod 256 \\ &= 74 \text{ (huruf "J" dalam karakter} \end{aligned}$$

ASCII 256)

$$\begin{aligned} M_{23} &= (M_{(2-1)3} + 3 * (2)) \bmod 256 \\ &= (M_{(1)3} + 3 * (2)) \bmod 256 \\ &= (85 + 6) \bmod 256 \\ &= 91 \text{ (huruf "[" dalam karakter} \end{aligned}$$

ASCII 256)

$$\begin{aligned} M_{24} &= (M_{(2-1)4} + 3 * (2)) \bmod 256 \\ &= (M_{(1)4} + 3 * (2)) \bmod 256 \\ &= (82 + 6) \bmod 256 \\ &= 88 \text{ (huruf "X" dalam karakter} \end{aligned}$$

ASCII 256)

$$\begin{aligned} M_{25} &= (M_{(2-1)5} + 3 * (2)) \bmod 256 \\ &= (M_{(1)5} + 3 * (2)) \bmod 256 \\ &= (81 + 6) \bmod 256 \\ &= 87 \text{ (huruf "W" dalam karakter} \end{aligned}$$

ASCII 256)

$$\begin{aligned} M_{26} &= (M_{(2-1)6} + 3 * (2)) \bmod 256 \\ &= (M_{(1)6} + 3 * (2)) \bmod 256 \\ &= (76 + 6) \bmod 256 \\ &= 82 \text{ (huruf "R" dalam karakter} \end{aligned}$$

ASCII 256)

hasil dari enkripsi baris ke dua ini adalah J[XWR. Hasil enkripsi sampai pada tahap ini ($i = 2$) dapat dilihat di bawah ini :

TARONI (dalam nilai ASCII 84 65 82 79 78 73) $\rightarrow i = 0$

WDURQL (dalam nilai ASCII 87 68 85 82 81 76) $\rightarrow i = 1$

J[XWR (dalam nilai ASCII 74 91 88 87 82) $\rightarrow i = 2$

Hasil enkripsi pada baris ke dua ($i=2$) akan digunakan sebagai plainteks pada proses enkripsi baris ke tiga ($i=3$), sehingga :

$i = 3, j = 3$

$$\begin{aligned} M_{33} &= (M_{(3-1)3} + 3 * (3)) \bmod 256 \\ &= (M_{(2)3} + 3 * (3)) \bmod 256 \\ &= (91 + 9) \bmod 256 \\ &= 100 \text{ (huruf "d" dalam karakter} \end{aligned}$$

ASCII 256)

$$\begin{aligned} M_{34} &= (M_{(3-1)4} + 3 * (3)) \bmod 256 \\ &= (M_{(2)4} + 3 * (3)) \bmod 256 \end{aligned}$$

$$= (88 + 9) \bmod 256$$

$$= 97 \text{ (huruf "a" dalam karakter}$$

ASCII 256)

$$M_{35} = (M_{(3-1)5} + 3 * (3)) \bmod 256$$

$$= (M_{(2)5} + 3 * (3)) \bmod 256$$

$$= (87 + 9) \bmod 256$$

$$= 96 \text{ (huruf "`" dalam karakter}$$

ASCII 256)

$$M_{36} = (M_{(3-1)6} + 3 * (3)) \bmod 256$$

$$= (M_{(2)6} + 3 * (3)) \bmod 256$$

$$= (82 + 9) \bmod 256$$

$$= 91 \text{ (huruf "[" dalam karakter}$$

ASCII 256)

hasil dari enkripsi baris ke tiga ($i=3$) ini adalah da`[.

Hasil enkripsi sampai pada tahap baris ke tiga ($i=3$) dapat dilihat di bawah ini:

TARONI (dalam nilai ASCII 84 65 82 79 78 73) $\rightarrow i = 0$

WDURQL (dalam nilai ASCII 87 68 85 82 81 76) $\rightarrow i = 1$

J[XWR (dalam nilai ASCII 74 91 88 87 82) $\rightarrow i = 2$

da`[(dalam nilai ASCII 100 97 96 91) $\rightarrow i = 3$

Hasil enkripsi pada baris ke tiga ($i=3$) akan digunakan sebagai plainteks pada proses enkripsi baris ke empat ($i=4$), sehingga :

$i = 4, j = 4$

$$M_{44} = (M_{(4-1)4} + 3 * (4)) \bmod 256$$

$$= (M_{(3)4} + 3 * (4)) \bmod 256$$

$$= (97 + 12) \bmod 256$$

$$= 109 \text{ (huruf "m" dalam karakter}$$

ASCII 256)

$$M_{45} = (M_{(4-1)5} + 3 * (4)) \bmod 256$$

$$= (M_{(3)5} + 3 * (4)) \bmod 256$$

$$= (96 + 12) \bmod 256$$

$$= 108 \text{ (huruf "l" dalam karakter}$$

ASCII 256)

$$M_{46} = (M_{(4-1)6} + 3 * (4)) \bmod 256$$

$$= (M_{(3)6} + 3 * (4)) \bmod 256$$

$$= (91 + 12) \bmod 256$$

$$= 103 \text{ (huruf "g" dalam karakter}$$

ASCII 256)

hasil dari enkripsi baris ke tiga ini adalah mlg.

Hasil enkripsi sampai pada tahap baris ke empat ($i = 4$) dapat dilihat di bawah ini:

TARONI (dalam nilai ASCII 84 65 82 79 78 73) $\rightarrow i = 0$

WDURQL (dalam nilai ASCII 87 68 85 82 81 76) $\rightarrow i = 1$

J[XWR (dalam nilai ASCII 74 91 88 87 82) $\rightarrow i = 2$

da`[(dalam nilai ASCII 100 97 96 91) $\rightarrow i = 3$

mlg (dalam nilai ASCII 109 108 103) $\rightarrow i = 4$

Hasil enkripsi pada baris ke empat ($i=4$) akan digunakan sebagai plainteks pada proses enkripsi

baris ke lima ($i=5$), sehingga :

$i = 5, j = 5$

$$\begin{aligned} M_{55} &= (M_{(5-1)5} + 3 * (5)) \text{ Mod } 256 \\ &= (M_{(4)5} + 3 * (5)) \text{ Mod } 256 \\ &= (108 + 15) \text{ mod } 256 \\ &= 123 \text{ (huruf “{” dalam karakter} \end{aligned}$$

ASCII 256)

$$\begin{aligned} M_{56} &= (M_{(5-1)6} + 3 * (5)) \text{ Mod } 256 \\ &= (M_{(4)6} + 3 * (5)) \text{ Mod } 256 \\ &= (103 + 15) \text{ mod } 256 \\ &= 118 \text{ (huruf “v” dalam karakter} \end{aligned}$$

ASCII 256)

hasil dari enkripsi baris ke lima ini adalah {v.

Hasil enkripsi sampai pada tahap baris ke lima ($i = 5$) dapat dilihat di bawah ini:

TARONI (dalam nilai ASCII 84 65 82 79 78 73) $\rightarrow i = 0$

WDURQL (dalam nilai ASCII 87 68 85 82 81 76) $\rightarrow i = 1$

J [XWR (dalam nilai ASCII 74 91 88 87 82) $\rightarrow i = 2$

d a ` [(dalam nilai ASCII 100 97 87 91) $\rightarrow i = 3$

mlg (dalam nilai ASCII 109 99 103) $\rightarrow i = 4$

{v (dalam nilai ASCII 123 118) $\rightarrow i = 5$

Hasil enkripsi pada baris ke lima ($i=5$) akan digunakan sebagai plainteks pada proses enkripsi baris ke enam ($i=6$), sehingga :

$i = 6, j = 6$

$$\begin{aligned} M_{66} &= (M_{(6-1)6} + 3 * (6)) \text{ Mod } 256 \\ &= (M_{(5)6} + 3 * (6)) \text{ Mod } 256 \\ &= (118 + 18) \text{ mod } 256 \\ &= 136 \text{ (huruf “^” dalam karakter} \end{aligned}$$

ASCII 256)

hasil dari enkripsi baris ke tiga ini adalah ^.

Hasil enkripsi sampai pada tahap baris ke enam ($i = 6$) dapat dilihat di bawah ini:

TARONI (dalam nilai ASCII 84 65 82 79 78 73) $\rightarrow i = 0$

WDURQL (dalam nilai ASCII 87 68 85 82 81 76) $\rightarrow i = 1$

J [XWR (dalam nilai ASCII 74 91 88 87 82) $\rightarrow i = 2$

d a ` [(dalam nilai ASCII 100 97 87 91) $\rightarrow i = 3$

mlg (dalam nilai ASCII 109 99 103) $\rightarrow i = 4$

{v (dalam nilai ASCII 123 118) $\rightarrow i = 5$

^ (dalam nilai ASCII 136) $\rightarrow i = 6$

huruf pertama dari masing-masing baris sebanyak satu karakter sesuai dengan formula M_{ij} pada nilai $j = (N+i)-N$ akan menjadi chiperteks pada proses enkripsi segitiga pertama, sehingga :

TARONI plainteks

WDURQL hasil sandi pada $i = 1$ dan $j = (6+1) - 6$

$= 1$

J [XWR hasil sandi pada $i = 2$ dan $j = (6+2) - 6$

$= 2$

d a ` [hasil sandi pada $i = 3$ dan $j = (6+3) - 6$

$= 3$

mlg hasil sandi pada $i = 4$ dan j

$= (6+4) - 6 = 4$

{v hasil sandi pada $i = 5$ dan j

$= (6+5) - 6 = 5$

^ hasil sandi pada $i = 6$ dan j

$= (6+6) - 6 = 6$

maka yang menjadi *cipher* pada proses enkripsi pertama adalah **WJdm{^** dimana dapat dilihat bahwa susunan dari baris dan kolomnya berbentuk segitiga yang mengerucut ke kiri.

4. Matriks enkripsi segitiga ke dua

Langkah-langkah yang dilakukan pada proses enkripsi segitiga kedua hampir sama dengan proses pada enkripsi segitiga pertama. Faktor pengali dan kunci yang digunakan tetap sama. Pada proses ini yang menjadi plainteks adalah *cipher* yang dihasilkan dari proses enkripsi segitiga pertama (**WJdm{^**) kemudian dienkrip lagi sesuai dengan formula yang berlaku pada proses enkripsi segitiga ke dua.

Plainteks = W J d m { ^ (cipher hasil enkripsi segitiga pertama)

87 74 100 109 123 136 (nilai

desimal dalam ASCII)

Untuk baris pertama ($i = 1$) :

$$M_{11} = (P[1] + (3 * 1)) \text{ mod } 256$$

$$= (W + (3 * 1)) \text{ mod } 256$$

$$= (87 + 3) \text{ mod } 256$$

$$= 90 \text{ (huruf “Z” dalam karakter}$$

ASCII 256)

$$M_{12} = (P[2] + (3 * 1)) \text{ mod } 256$$

$$= (J + (3 * 1)) \text{ mod } 256$$

$$= (74 + 3) \text{ mod } 256$$

$$= 77 \text{ (huruf “M” dalam karakter}$$

ASCII 256)

$$M_{13} = (P[3] + (3 * 1)) \text{ mod } 256$$

$$= (d + (3 * 1)) \text{ mod } 256$$

$$= (100 + 3) \text{ mod } 256$$

$$= 103 \text{ (huruf “g” dalam karakter}$$

ASCII 256)

$$M_{14} = (P[4] + (3 * 1)) \text{ mod } 256$$

$$= (m + (3 * 1)) \text{ mod } 256$$

$$= (109 + 3) \text{ mod } 256$$

$$= 112 \text{ (huruf “p” dalam karakter}$$

ASCII 256)

$$M_{15} = (P[5] + (3 * 1)) \text{ mod } 256$$

$$= ({^ + (3 * 1)) \text{ mod } 256$$

$$= (123 + 3) \text{ mod } 256$$

$$= 126 \text{ (huruf “~” dalam karakter}$$

ASCII 256)

$$M_{16} = (P[6] + (3 * 1)) \text{ mod } 256$$

$$= (^ + (3 * 1)) \text{ mod } 256$$

$$= (136 + 3) \text{ mod } 256$$

$$= 139 \text{ (huruf “<” dalam karakter}$$

ASCII 256)

hasil dari enkripsi baris pertama ($i = 1$) adalah ZMgp~<.

Hasil enkripsi sampai pada tahap baris pertama ($i = 1$) dapat dilihat di bawah ini:

W J d m { ^ (87 74 100 109 123 136
Z M g p ~ < (90 77 103 112 126 **139**

Hasil enkripsi baris pertama ($i = 1$) akan digunakan sebagai plainteks pada proses enkripsi baris ke dua dimana nilai $j \leq (N + 1) - i$, sehingga :

$i = 2; j \leq (6 + 1) - 2 \rightarrow j \leq 5$

$M_{21} = (M_{(2-1)1} + (K * R[i])) \bmod 256$
 $= (M_{(1)1} + (K * R[i])) \bmod 256$
 $= (Z + (3 * 2)) \bmod 256$
 $= (90 + 6) \bmod 256$
 $= 96$ (huruf “ ` ” dalam karakter

ASCII 256)

$M_{22} = (M_{(2-1)2} + (K * R[i])) \bmod 256$
 $= (M_{(1)2} + (K * R[i])) \bmod 256$
 $= (M + (3 * 2)) \bmod 256$
 $= (77 + 6) \bmod 256$
 $= 83$ (huruf “ S ” dalam karakter

ASCII 256)

$M_{23} = (M_{(2-1)3} + (K * R[i])) \bmod 256$
 $= (M_{(1)3} + (K * R[i])) \bmod 256$
 $= (g + (3 * 2)) \bmod 256$
 $= (103 + 6) \bmod 256$
 $= 109$ (huruf “ m ” dalam karakter

ASCII 256)

$M_{24} = (M_{(2-1)4} + (K * R[i])) \bmod 256$
 $= (M_{(1)4} + (K * R[i])) \bmod 256$
 $= (p + (3 * 2)) \bmod 256$
 $= (112 + 6) \bmod 256$
 $= 118$ (huruf “ v ” dalam karakter

ASCII 256)

$M_{25} = (M_{(2-1)5} + (K * R[i])) \bmod 256$
 $= (M_{(1)5} + (K * R[i])) \bmod 256$
 $= (~ + (3 * 2)) \bmod 256$
 $= (126 + 6) \bmod 256$
 $= 132$ (huruf “ , ” dalam karakter

ASCII 256)

hasil dari enkripsi baris ke dua ($i = 2$) adalah `SmV,,.

Hasil enkripsi sampai pada tahap baris ke dua ($i=2$) dapat dilihat di bawah ini:

W J d m { ^
Z M g p ~ < $\rightarrow 90 \quad 77 \quad 103$

112 126 **139** $\rightarrow i = 1$

` S m V ,, $\rightarrow 96 \quad 83 \quad 109 \quad 118 \quad 132$

Hasil enkripsi baris ke dua ($i=2$) akan digunakan sebagai plainteks pada proses enkripsi baris ke tiga, sehingga :

$i = 3; j \leq (6 + 1) - 3 \rightarrow j \leq 4$

$M_{31} = (M_{(3-1)1} + (K * R[i])) \bmod 256$
 $= (M_{(2)1} + (K * R[i])) \bmod 256$
 $= (~ + (3 * 3)) \bmod 256$
 $= (96 + 9) \bmod 256$

$= 105$ (huruf “ i ” dalam karakter

ASCII 256)

$M_{32} = (M_{(3-1)2} + (K * R[i])) \bmod 256$

$= (M_{(2)2} + (K * R[i])) \bmod 256$

$= (S + (3 * 3)) \bmod 256$

$\rightarrow i = 0 \quad (83 + 9) \bmod 256$

$\rightarrow i = 1 \quad 92$ (huruf “ \ ” dalam karakter

ASCII 256)

$M_{33} = (M_{(3-1)3} + (K * R[i])) \bmod 256$

$= (M_{(2)3} + (K * R[i])) \bmod 256$

$= (m + (3 * 3)) \bmod 256$

$= (109 + 9) \bmod 256$

$= 118$ (huruf “ v ” dalam karakter

ASCII 256)

$M_{34} = (M_{(3-1)4} + (K * R[i])) \bmod 256$

$= (M_{(2)4} + (K * R[i])) \bmod 256$

$= (V + (3 * 3)) \bmod 256$

$= (118 + 9) \bmod 256$

$= 127$ (huruf “ □ ” dalam karakter

ASCII 256 / delete)

hasil dari enkripsi baris ke tiga ($i = 3$) adalah i\v □ .

Hasil enkripsi sampai pada tahap baris ke tiga ($i = 3$) dapat dilihat di bawah ini:

W J d m { ^

Z M g p ~ < $\rightarrow 90 \quad 77 \quad 103$

112 126 139 $\rightarrow i = 1$

` S m V ,, $\rightarrow 96 \quad 83 \quad 109 \quad 118 \quad 132$

i \ v □ $\rightarrow 105 \quad 92 \quad 118$

127 $\rightarrow i = 3$

Hasil enkripsi baris ke tiga ($i=3$) akan digunakan sebagai plainteks pada proses enkripsi baris ke empat, sehingga :

$i = 4; j \leq (6 + 1) - 4 \rightarrow j \leq 3$

$M_{41} = (M_{(4-1)1} + (K * R[i])) \bmod 256$

$= (M_{(3)1} + (K * R[i])) \bmod 256$

$= (i + (3 * 4)) \bmod 256$

$= (105 + 12) \bmod 256$

$= 117$ (huruf “ u ” dalam karakter

ASCII 256)

$M_{42} = (M_{(4-1)2} + (K * R[i])) \bmod 256$

$= (M_{(3)2} + (K * R[i])) \bmod 256$

$= (\backslash + (3 * 4)) \bmod 256$

$= (92 + 12) \bmod 256$

$= 104$ (huruf “ h ” dalam karakter

ASCII 256)

$M_{43} = (M_{(4-1)3} + (K * R[i])) \bmod 256$

$\rightarrow i \notin (M_{(3)3} + (K * R[i])) \bmod 256$

$= (v + (3 * 4)) \bmod 256$

$= (118 + 12) \bmod 256$

$\rightarrow i \notin 30$ (huruf “ , ” dalam karakter

ASCII 256)

hasil dari enkripsi baris ke empat ($i = 4$) adalah uh, .

Hasil enkripsi sampai pada tahap baris ke empat ($i = 4$) dapat dilihat di bawah ini:

W J d m { ^

Z M g p ~ < $\rightarrow 90 \quad 77 \quad 103$

112 126 **139** $\rightarrow i = 1$

` S m V „ → 96 83 109 118 132
i \ v □ → 105 92 118
127 → i = 3
u h , → 117 104 130

Hasil enkripsi baris ke empat (i=4) akan digunakan sebagai plainteks pada proses enkripsi baris ke lima, sehingga :

$$i = 5; j \leq (6 + 1) - 5 \rightarrow j \leq 2$$

$$\begin{aligned} M_{51} &= (M_{(5-1)1} + (K * R[i])) \bmod 256 \\ &= (M_{(4)1} + (K * R[i])) \bmod 256 \\ &= (u + (3 * 5)) \bmod 256 \\ &= (117 + 15) \bmod 256 \\ &= 132 \text{ (huruf " „ " dalam karakter ASCII 256)} \end{aligned}$$

$$\begin{aligned} M_{52} &= (M_{(5-1)2} + (K * R[i])) \bmod 256 \\ &= (M_{(4)2} + (K * R[i])) \bmod 256 \\ &= (r + (3 * 5)) \bmod 256 \\ &= (104 + 15) \bmod 256 \\ &= 119 \text{ (huruf " w " dalam karakter ASCII 256)} \end{aligned}$$

ASCII 256)

hasil dari enkripsi baris ke lima (i = 5) adalah „w .

Hasil enkripsi sampai pada tahap baris ke lima (i = 5) dapat dilihat di bawah ini:

W J d m { ^
Z M g p ~ < → 90 77 103
112 126 139 → i = 1
` S m V „ → 96 83 109 118 132
i \ v □ → 105 92 118
127 → i = 3
u h , → 117 104 130
„ w → 132 119

hasil enkripsi baris ke lima (i = 5) akan digunakan sebagai plainteks pada proses enkripsi baris ke enam, sehingga :

$$i = 6; j \leq (6 + 1) - 6 \rightarrow j \leq 1$$

$$\begin{aligned} M_{61} &= (M_{(6-1)1} + (K * R[i])) \bmod 256 \\ &= (M_{(5)1} + (K * R[i])) \bmod 256 \\ &= („ + (3 * 6)) \bmod 256 \\ &= (132 + 18) \bmod 256 \\ &= 150 \text{ (huruf " - " dalam karakter ASCII 256)} \end{aligned}$$

ASCII 256)

hasil dari enkripsi baris ke enam (i = 6) adalah - .

Hasil enkripsi sampai pada tahap baris ke enam (i = 6) dapat dilihat di bawah ini:

W J d m { ^
Z M g p ~ < → 90 77 103
112 126 139 → i = 1
` S m V „ → 96 83 109 118 132
i \ v □ → 105 92 118
127 → i = 3
u h , → 117 104 130
„ w → 132 119
- → 150

karakter yang menjadi hasil enkrip segitiga kedua adalah huruf terakhir dari masing-masing baris dan diperoleh berdasarkan formula M_{ij} pada nilai $j = (N+1) - i$, sehingga :

$$Z M g p \rightarrow i = 2 \rightarrow i = 1 \text{ dan } j = (6 + 1) - 1 = 6 \rightarrow <$$

$$` S m V „ \rightarrow i = 2 \text{ dan } j = (6 + 1) - 2 = 5 \rightarrow „ \rightarrow i = 4$$

$$i \setminus v \square \rightarrow i = 3 \text{ dan } j = (6 + 1) - 3 = 4 \rightarrow \square$$

$$u r , \rightarrow i = 4 \text{ dan } j = (6 + 1) - 4 = 3 \rightarrow ,$$

$$„ w \rightarrow i = 5 \text{ dan } j = (6 + 1) - 5 = 2 \rightarrow w$$

$$- \rightarrow i = 6 \text{ dan } j = (6 + 1) - 6 = 1 \rightarrow -$$

Dapat dilihat bahwa hasil penyandian pada proses enkripsi segitiga kedua membentuk segitiga yang mengerucut ke kanan dan menghasilkan cipherteks akhir adalah -w,□,„< . Cipher terakhir inilah yang nantinya disimpan menjadi *record* di dalam *database*.

3.2 Dekripsi Record Database

Proses dekripsi merupakan kebalikan dari proses enkripsi *record database* yang telah dilakukan sebelumnya. Kunci dan faktor pengali yang digunakan tetap sama seperti pada proses enkripsi. Proses dekripsi *record database* diawali pemilihan nama *database* kemudian memilih tabel yang telah dienkripsi. Semua *record* tabel yang telah dipilih akan dikembalikan ke teks *record* semula (sebelum dienkripsi).

Proses dekripsi *record database* sesuai dengan algoritma *triangle chain* dapat digambarkan seperti pada gambar 2.

Gambar 2 : Gambaran Umum Proses Pengembalian Record Tersandi

Proses pengembalian *record* tersandi ke *record* asli dilakukan sebanyak dua kali, terdiri dari dekripsi segitiga pertama dan dekripsi segitiga kedua. Penyelesaian tahap dekripsi di atas dapat diuraikan

melalui contoh kasus di bawah ini dimana *record* sandi adalah hasil akhir dari penyandian contoh enkripsi :

1. Dekripsi segitiga pertama

chipertext adalah $-w, \square, ,, <$ pada $i = 0$

150 119 130 127 132

139 (nilai desimal dalam ASCII)

$i = 1 \quad j \leq (6 + 1) - 1$

$j \leq 6$

$M_{11} = C[1] - (3 * [1]) \bmod 256$
 $= (- - (3 * 1)) \bmod 256$
 $= (150 - 3) \bmod 256$
 $= 147$ (huruf “ $\square$ ” dalam karakter

ASCII 256)

$M_{12} = C[2] - (3 * [1]) \bmod 256$
 $= (w - (3 * 1)) \bmod 256$
 $= (119 - 3) \bmod 256$
 $= 116$ (huruf “ t ” dalam karakter

ASCII 256)

$M_{13} = C[3] - (3 * [1]) \bmod 256$
 $= (, - (3 * 1)) \bmod 256$
 $= (130 - 3) \bmod 256$
 $= 127$ (huruf “ $\square$ ” dalam karakter

ASCII 256)

$M_{14} = C[4] - (3 * [1]) \bmod 256$
 $= (\square - (3 * 1)) \bmod 256$
 $= (127 - 3) \bmod 256$
 $= 124$ (huruf “ $|$ ” dalam karakter

ASCII 256)

$M_{15} = C[5] - (3 * [1]) \bmod 256$
 $= (,, - (3 * 1)) \bmod 256$
 $= (132 - 3) \bmod 256$
 $= 129$ (huruf “ $\square$ ” dalam karakter

ASCII 256)

$M_{16} = C[6] - (3 * [1]) \bmod 256$
 $= (< - (3 * 1)) \bmod 256$
 $= (139 - 3) \bmod 256$
 $= 136$ (huruf “ $\wedge$ ” dalam karakter

ASCII 256)

hasil dari dekripsi baris pertama ($i = 1$) adalah “ $t \square | \square \wedge$ ”.

Hasil dekripsi sampai pada tahap baris pertama ($i = 1$) dapat dilihat di bawah ini :

$-w, \square, ,, < \quad (150 \ 119 \ 130 \ 127 \ 132 \ 139) \rightarrow$
 $i = 0$

“ $t \square | \square \wedge$ ” (147 116 127 124 129 136) $\rightarrow$
 $i = 1$

Hasil dekripsi baris pertama ($i=1$) akan digunakan sebagai *chipertext* pada proses dekripsi baris ke dua, sehingga :

$i = 2; \quad j \leq (6 + 1) - 2$
 $j \leq 5;$

$M_{21} = (M_{(2-1)1} - K * (R[2])) \bmod 256$
 $= (M_{(1)1} - 3 * (2)) \bmod 256$
 $= (\square - 6) \bmod 256$
 $= (147 - 6) \bmod 256$
 $= 141$ (huruf “ $\square$ ” dalam karakter

ASCII 256)

$M_{22} = (M_{(2-1)2} - K * (R[2])) \bmod 256$
 $= (M_{(1)2} - 3 * (2)) \bmod 256$
 $= (t - 6) \bmod 256$
 $= (116 - 6) \bmod 256$
 $= 110$ (huruf “ n ” dalam karakter

ASCII 256)

$M_{23} = (M_{(2-1)3} - K * (R[2])) \bmod 256$
 $= (M_{(1)3} - 3 * (2)) \bmod 256$
 $= (\square - 6) \bmod 256$
 $= (127 - 6) \bmod 256$
 $= 121$ (huruf “ y ” dalam karakter

ASCII 256)

$M_{24} = (M_{(2-1)4} - K * (R[2])) \bmod 256$
 $= (M_{(1)4} - 3 * (2)) \bmod 256$
 $= (| - 6) \bmod 256$
 $= (124 - 6) \bmod 256$
 $= 118$ (huruf “ v ” dalam karakter

ASCII 256)

$M_{25} = (M_{(2-1)5} - K * (R[2])) \bmod 256$
 $= (M_{(1)5} - 3 * (2)) \bmod 256$
 $= (\square - 6) \bmod 256$
 $= (129 - 6) \bmod 256$
 $= 123$ (huruf “ $\{$ ” dalam karakter

ASCII 256)

hasil dari dekripsi baris ke dua ($i = 2$) adalah $\square n y v \{$.

Hasil dekripsi sampai pada tahap baris ke dua ($i = 2$) dapat dilihat di bawah ini :

$-w, \square, ,, < \quad (150 \ 119 \ 130 \ 127$
 $132 \ 139) \rightarrow i = 0$

“ $t \square | \square \wedge$ ” (147 116 127 124
 $129 \ 136) \rightarrow i = 1$

$\square n y v \{$ (141 110 121 118
 $123) \rightarrow i = 2$

Hasil dekripsi baris ke dua ($i=2$) akan digunakan sebagai *chipertext* pada proses dekripsi baris ke tiga, sehingga :

$i = 3; \quad j \leq (6 + 1) - 3$
 $j \leq 4;$

$M_{31} = (M_{(3-1)1} - K * (R[3])) \bmod 256$
 $= (M_{(2)1} - 3 * (3)) \bmod 256$
 $= (\square - 9) \bmod 256$
 $= (141 - 9) \bmod 256$
 $= 132$ (huruf “ $,,$ ” dalam karakter

ASCII 256)

$M_{32} = (M_{(3-1)2} - K * (R[3])) \bmod 256$
 $= (M_{(2)2} - 3 * (3)) \bmod 256$
 $= (n - 9) \bmod 256$
 $= (110 - 9) \bmod 256$
 $= 101$ (huruf “ e ” dalam karakter

ASCII 256)

$M_{33} = (M_{(3-1)3} - K * (R[3])) \bmod 256$
 $= (M_{(2)3} - 3 * (3)) \bmod 256$
 $= (y - 9) \bmod 256$
 $= (121 - 9) \bmod 256$
 $= 112$ (huruf “ p ” dalam karakter

ASCII 256)

$M_{34} = (M_{(3-1)4} - K * (R[3])) \bmod 256$
 $= (M_{(2)4} - 3 * (3)) \bmod 256$

$= (v - 9) \bmod 256$
 $= (118 - 9) \bmod 256$
 $= 109$ (huruf " m " dalam karakter ASCII 256)

hasil dari dekripsi baris ke dua ($i = 2$) adalah „epm .

Hasil dekripsi sampai pada tahap baris ke tiga ($i = 3$) dapat dilihat di bawah ini :

- w , □ „ ‹ (150 119 130 127
 132 139) $\rightarrow i = 0$
 “ t □ | □ ^ (147 116 127 124
 129 136) $\rightarrow i = 1$

□ n y v { (141 110 121 118 123)
 „ e p m (132 101 112 109)
 $\rightarrow i = 3$

Hasil dekripsi baris ke tiga ($i = 3$) akan digunakan sebagai *chipertext* pada proses dekripsi baris ke empat, sehingga :

$i = 4;$ $j \leq (6 + 1) - 4$
 $j \leq 3;$
 $M_{41} = (M_{(4-1)1} - K * (R[4])) \bmod 256.$
 $= (M_{(3)1} - 3 * (4)) \bmod 256.$
 $= („ - 12) \bmod 256$
 $= (132 - 12) \bmod 256$
 $= 120$ (huruf " x " dalam karakter ASCII 256)

$M_{42} = (M_{(4-1)2} - K * (R[4])) \bmod 256.$
 $= (M_{(3)2} - 3 * (4)) \bmod 256.$
 $= (e - 12) \bmod 256$
 $= (101 - 12) \bmod 256$
 $= 89$ (huruf " Y " dalam karakter ASCII 256)

$M_{43} = (M_{(4-1)3} - K * (R[4])) \bmod 256.$
 $= (M_{(3)3} - 3 * (4)) \bmod 256.$
 $= (p - 12) \bmod 256$
 $= (112 - 12) \bmod 256$
 $= 100$ (huruf " d " dalam karakter ASCII 256)

hasil dari dekripsi baris ke empat ($i = 4$) adalah xYd .

Hasil dekripsi sampai pada tahap baris ke empat ($i = 4$) dapat dilihat di bawah ini :

- w , □ „ ‹ (150 119 130 127
 132 139) $\rightarrow i = 0$
 “ t □ | □ ^ (147 116 127 124
 129 136) $\rightarrow i = 1$

□ n y v { (141 110 121 118 123)
 „ e p m (132 101 112 109)
 $\rightarrow i = 3$

x Y d (120 89 100)

Hasil dekripsi baris ke empat ($i = 4$) akan digunakan sebagai *chipertext* pada proses dekripsi baris ke lima, sehingga :

$i = 5;$ $j \leq (6 + 1) - 5$
 $j \leq 2;$
 $M_{51} = (M_{(5-1)1} - K * (R[5])) \bmod 256.$
 $= (M_{(4)1} - 3 * (5)) \bmod 256.$
 $= (x - 15) \bmod 256$
 $= (120 - 15) \bmod 256$

$= 105$ (huruf " i " dalam karakter ASCII 256)

$M_{52} = (M_{(5-1)2} - K * (R[5])) \bmod 256.$
 $= (M_{(4)2} - 3 * (5)) \bmod 256.$
 $= (Y - 15) \bmod 256$
 $= (89 - 15) \bmod 256$
 $= 74$ (huruf " J " dalam karakter ASCII 256)

hasil dari dekripsi baris ke empat ($i = 5$) adalah iJ .

Hasil dekripsi sampai pada tahap baris ke lima ($i = 5$) dapat dilihat di bawah ini :

- w , □ „ ‹ $\rightarrow i = 2$ (150 119 130 127
 132 139) $\rightarrow i = 0$
 “ t □ | □ ^ (147 116 127 124
 129 136) $\rightarrow i = 1$

□ n y v { (141 110 121 118 123)
 „ e p m (132 101 112 109)
 $\rightarrow i = 3$

x Y d (120 89 100)
 i J (105 74)

Hasil dekripsi baris ke lima ($i = 5$) akan digunakan sebagai *chipertext* pada proses dekripsi baris ke enam, sehingga :

$i = 6;$ $j \leq (6 + 1) - 6$
 $j \leq 1;$
 $M_{61} = (M_{(6-1)1} - K * (R[6])) \bmod 256.$
 $= (M_{(5)1} - 3 * (6)) \bmod 256.$
 $= (i - 18) \bmod 256$
 $= (105 - 18) \bmod 256$
 $= 87$ (huruf " W " dalam karakter ASCII 256)

hasil dari dekripsi baris ke enam ($i = 6$) adalah W.

Hasil dekripsi sampai pada tahap baris ke enam ($i = 6$) dapat dilihat di bawah ini :

“ t □ | □ ^ (147 116 127 124
 129 136) $\rightarrow i = 1 ; j = 6$
 □ n y v { (141 110 121 118 123)
 „ e p m (132 101 112 109)

x Y d (120 89 100)
 i J (105 74) $\rightarrow i = 5 ; j = 2$
 W (87)

sehingga pada proses dekripsi segitiga pertama diperoleh plainteks sesuai dengan formula M_{ij} pada nilai $j = (N+i)-i$ adalah **WJdm** { ^ .

2. Dekripsi segitiga ke dua
 Proses dekripsi segitiga ke dua merupakan kebalikan dari hasil proses enkripsi segitiga pertama. Plainteks sumber adalah hasil akhir dari proses dekripsi segitiga pertama (**WJdm** { ^).

$Chipertext = W \quad J \quad d \quad m \quad \{ \quad ^$
 (hasil dekrip pertama)

87 74 100 109 123 136
 (nilai desimal dalam ASCII)

untuk baris pertama ($i = 1$) :

$M_{11} = C[1] - (3 * R[1]) \bmod 256$
 $= (W - (3 * 1)) \bmod 256$

$= (87 - 3) \bmod 256$
 $= 84$ (huruf " T " dalam karakter
 ASCII 256)
 $M_{12} = C[2] - (3 * R[1]) \bmod 256$
 $= (J - (3 * 1)) \bmod 256$
 $= (74 - 3) \bmod 256$
 $= 71$ (huruf " G " dalam karakter
 ASCII 256)
 $M_{13} = C[3] - (3 * R[1]) \bmod 256$
 $= (d - (3 * 1)) \bmod 256$
 $= (100 - 3) \bmod 256$
 $= 97$ (huruf " a " dalam karakter
 ASCII 256)
 $M_{14} = C[4] - (3 * R[1]) \bmod 256$
 $= (m - (3 * 1)) \bmod 256$
 $= (109 - 3) \bmod 256$
 $= 106$ (huruf " j " dalam karakter
 ASCII 256)
 $M_{15} = C[5] - (3 * R[1]) \bmod 256$
 $= (\{ - (3 * 1)) \bmod 256$
 $= (123 - 3) \bmod 256$
 $= 120$ (huruf " x " dalam karakter
 ASCII 256)
 $M_{16} = C[6] - (3 * R[1]) \bmod 256$
 $= (\wedge - (3 * 1)) \bmod 256$
 $= (136 - 3) \bmod 256$
 $= 133$ (huruf "... " dalam karakter
 ASCII 256)
 hasil dari dekripsi baris pertama ($i = 1$) adalah
 TGa jx
 Hasil dekripsi sampai pada tahap baris pertama ($i = 1$) dapat dilihat di bawah ini :
W J d m { ^ (dalam nilai ASCII 87
 74 100 109 123 136) $\rightarrow i = 0$
T G a j x ... (dalam nilai ASCII 84
 71 97 106 120 133)
 Hasil dekripsi baris pertama ($i = 1$) akan
 digunakan sebagai *chipertext* pada proses dekripsi
 baris ke dua, sehingga :
 $i = 2; j \geq 2;$
 $M_{22} = (C_{[2-1]2} - (3 * R[2])) \bmod 256$
 $= (C_{[1]2} - (3 * 2)) \bmod 256$
 $= (G - 6) \bmod 256$
 $= (71 - 6) \bmod 256$
 $= 65$ (huruf " A " dalam karakter
 ASCII 256)
 $M_{23} = (C_{[2-1]3} - (3 * R[2])) \bmod 256$
 $= (C_{[1]3} - (3 * 2)) \bmod 256$
 $= (a - 6) \bmod 256$
 $= (97 - 6) \bmod 256$
 $= 91$ (huruf " [" dalam karakter
 ASCII 256)
 $M_{24} = (C_{[2-1]4} - (3 * R[2])) \bmod 256$
 $= (C_{[1]4} - (3 * 2)) \bmod 256$
 $= (j - 6) \bmod 256$
 $= (106 - 6) \bmod 256$
 $= 100$ (huruf " d " dalam karakter
 ASCII 256)
 $M_{25} = (C_{[2-1]5} - (3 * R[2])) \bmod 256$

$= (C_{[1]5} - (3 * 2)) \bmod 256$
 $= (x - 6) \bmod 256$
 $= (120 - 6) \bmod 256$
 $= 114$ (huruf " r " dalam karakter
 ASCII 256)
 $M_{26} = (C_{[2-1]6} - (3 * R[2])) \bmod 256$
 $= (C_{[1]6} - (3 * 2)) \bmod 256$
 $= (... - 6) \bmod 256$
 $= (133 - 6) \bmod 256$
 $= 127$ (huruf " □ " dalam karakter
 ASCII 256)
 hasil dari dekripsi baris pertama ($i = 1$) adalah
 A [d r □
 Hasil dekripsi sampai pada tahap baris pertama ($i = 1$) dapat dilihat di bawah ini :
W J d m { ^ (dalam nilai ASCII 87
 74 100 109 123 136) $\rightarrow i = 0$
T G a j x ... (dalam nilai ASCII 84
 71 97 106 120 133)
A [d r □ (dalam nilai ASCII
 65 91 100 114 127)
 Hasil dekripsi baris ke dua ($i = 2$) akan digunakan
 sebagai *chipertext* pada proses dekripsi baris ke
 tiga, sehingga :
 $i = 3; j \geq 3;$
 $M_{33} = (C_{[3-1]3} - (3 * R[3])) \bmod 256$
 $= (C_{[2]3} - (3 * 3)) \bmod 256$
 $= ([- 9) \bmod 256$
 $= (91 - 9) \bmod 256$
 $= 82$ (huruf " R " dalam karakter
 ASCII 256)
 $M_{34} = (C_{[3-1]4} - (3 * R[3])) \bmod 256$
 $= (C_{[2]4} - (3 * 3)) \bmod 256$
 $= (d - 9) \bmod 256$
 $= (100 - 9) \bmod 256$
 $= 91$ (huruf " i " dalam karakter
 ASCII 256)
 $M_{35} = (C_{[3-1]5} - (3 * R[3])) \bmod 256$
 $= (C_{[2]5} - (3 * 3)) \bmod 256$
 $= (r - 9) \bmod 256$
 $= (114 - 9) \bmod 256$
 $= 105$ (huruf " i " dalam karakter
 ASCII 256)
 $M_{36} = (C_{[3-1]6} - (3 * R[3])) \bmod 256$
 $= (C_{[2]6} - (3 * 3)) \bmod 256$
 $= (\square - 9) \bmod 256$
 $= (127 - 9) \bmod 256$
 $= 118$ (huruf " v " dalam karakter
 ASCII 256)
 hasil dari dekripsi baris ke tiga ($i = 3$) adalah **R**
[i v
 Hasil dekripsi sampai pada tahap baris ke tiga ($i = 3$) dapat dilihat di bawah ini :
W J d m { ^ (dalam nilai ASCII 87
 74 100 109 123 136) $\rightarrow i = 0$
T G a j x ... (dalam nilai ASCII 84
 71 97 106 120 133)
A [d r □ (dalam nilai ASCII

65 91 100 114 127)
 $R[i \vee]$ (dalam nilai ASCII
 82 91 105 118) $\rightarrow i = 3$

Hasil dekripsi baris ke tiga ($i = 3$) akan digunakan sebagai *chipertext* pada proses dekripsi baris ke empat, sehingga :

$i = 4; j \geq 4;$

$M_{44} = (C_{[4-1]4} - (3 * R[4])) \bmod 256$
 $= (C_{[3]4} - (3 * 4)) \bmod 256$
 $= ([- 12] \bmod 256$
 $= (91 - 12) \bmod 256$
 $= 79$ (huruf " O " dalam karakter

ASCII 256)

$M_{45} = (C_{[4-1]5} - (3 * R[4])) \bmod 256$
 $= (C_{[3]5} - (3 * 4)) \bmod 256$
 $= (i - 12) \bmod 256$
 $= (105 - 12) \bmod 256$
 $= 93$ (huruf "] " dalam karakter

ASCII 256)

$M_{46} = (C_{[4-1]6} - (3 * R[4])) \bmod 256$
 $= (C_{[3]6} - (3 * 4)) \bmod 256$
 $= (v - 12) \bmod 256$
 $= (118 - 12) \bmod 256$
 $= 106$ (huruf " j " dalam karakter

ASCII 256)

hasil dari dekripsi baris ke empat ($i = 4$) adalah

O]j

Hasil dekripsi sampai pada tahap baris ke empat ($i = 4$) dapat dilihat di bawah ini :

W J d m { ^ (dalam nilai ASCII 87 74 100 109 123 136) $\rightarrow i = 0$

T G a j x ... (dalam nilai ASCII 84 71 97 106 120 133)

A [d r □ (dalam nilai ASCII

65 91 100 114 127)

R [i v (dalam nilai ASCII

82 91 105 118) $\rightarrow i = 3$

O] j (dalam nilai ASCII

79 93 106) $\rightarrow i = 4$

Hasil dekripsi baris ke empat ($i = 4$) akan

digunakan sebagai *chipertext* pada proses dekripsi

baris ke lima, sehingga :

$i = 5; j \geq 5;$

$M_{55} = (C_{[5-1]5} - (3 * R[5])) \bmod 256$
 $= (C_{[4]5} - (3 * 5)) \bmod 256$
 $= ([- 15] \bmod 256$
 $= (93 - 15) \bmod 256$
 $= 78$ (huruf " N " dalam karakter

ASCII 256)

$M_{56} = (C_{[5-1]6} - (3 * R[5])) \bmod 256$
 $= (C_{[4]6} - (3 * 5)) \bmod 256$
 $= (j - 15) \bmod 256$
 $= (106 - 15) \bmod 256$
 $= 91$ (huruf " [" dalam karakter

ASCII 256)

hasil dari dekripsi baris ke lima ($i = 5$) adalah **N[**

Hasil dekripsi sampai pada tahap baris ke lima ($i = 5$) dapat dilihat di bawah ini :

W J d m { ^ (dalam nilai ASCII 87

74 100 109 123 136) $\rightarrow i = 0$

T G a j x ... (dalam nilai ASCII 84 71 97 106 120 133)

A [d r □ (dalam nilai ASCII

65 91 100 114 127)

R [i v (dalam nilai ASCII

82 91 105 118) $\rightarrow i = 3$

O] j (dalam nilai ASCII

79 93 106) $\rightarrow i = 4$

N[(dalam nilai ASCII

78 91) $\rightarrow i = 5$

Hasil dekripsi baris ke lima ($i = 5$) akan

digunakan sebagai *chipertext* pada proses dekripsi

baris ke lima, sehingga :

$i = 6; j \geq 6;$

$M_{56} = (C_{[6-1]6} - (3 * R[6])) \bmod 256$
 $= (C_{[5]6} - (3 * 6)) \bmod 256$
 $= ([- 18] \bmod 256$
 $= (91 - 18) \bmod 256$
 $= 73$ (huruf " I " dalam karakter

ASCII 256)

hasil dari dekripsi baris ke enam ($i = 6$) adalah **I**

Hasil dekripsi sampai pada tahap baris ke enam ($i = 6$) dapat dilihat di bawah ini :

W J d m { ^ (dalam nilai ASCII 87 74 100 109 123 136) $\rightarrow i = 0$

T G a j x ... (dalam nilai ASCII 84 71 97 106 120 133) $\rightarrow i = 1$

A [d r □ (dalam nilai ASCII 65 91 100 114 127) $\rightarrow i = 2$

R [i v (dalam nilai ASCII 82 91 105 118) $\rightarrow i = 3$

O] j (dalam nilai ASCII 79 93 106) $\rightarrow i = 4$

N[(dalam nilai ASCII 78 91) $\rightarrow i = 5$

I (dalam nilai ASCII 73) $\rightarrow i = 6$

Penentuan karakter yang ditetapkan sebagai

plainteks (*record* asli) dilakukan berdasarkan formula

M_{ij} pada nilai $j = (N+i)-N$ pada masing-masing baris.

Sehingga didapatkan *plaintext* adalah **TARONI** (sama

seperti teks aslinya).

4 Kesimpulan

Setelah melakukan analisa terhadap penerapan

algoritma *triangle chain* pada penyandian *record*

database, maka penulis dapat menarik beberapa

kesimpulan sebagai berikut :

1. Algoritma *triangle chain* melakukan proses

penyandian pada setiap *record* dari tabel *database*

yang telah dipilih sebanyak dua kali (secara

ganda) dimana nilai substitusi setiap karakter

record tergantung pada nilai hasil perkalian kunci

dengan bilangan faktor pengali yang terbentuk.

Hasil akhir yang digunakan adalah hasil proses

penyandian segitiga kedua dimana hasilnya tidak

memiliki kemiripan dengan *record* asli.

Pembentukan bilangan faktor pengali dalam proses penyandian dapat menggunakan bilangan integer positif, prima positif, ataupun bilangan yang dapat ditentukan sendiri oleh penggun, sehingga mampu mempersulit pemecahan sandi yang dihasilkan.

2. Implementasi penyandian *record database* diawali dengan penentuan nama *database* dan pemilihan tabel yang memiliki *record* yang disandikan. Masing-masing *record* pada tabel yang telah dipilih disandikan berdasarkan algoritma *triangle chain* yang telah tersedia di dalam aplikasi yang telah dibuat.

Daftar Pustaka

- [1]. Doni Ariyus, 2008, Pengantar Ilmu Kriptografi, Yogyakarta, Andi.
- [2]. Rinaldi Munir, 2006, Kriptografi, Bandung, Informatika..
- [3]. <http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2006-2007/Makalah1/Makalah1-088.pdf>.
- [4]. <http://id.wikipedia.org/wiki/Analisis>
- [5]. Janner Simarmata, Iman Paryudi 2005, Basis Data, Yogyakarta, Andi.