Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume (2) No.1 Maret 2018, pp. 1-11
ISSN:2548-9771/EISSN:2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Kombinasi Mode *Cipher Block Chaining* Dengan Algoritma *Triangle Chain Cipher* Pada Penyandian Login *Website*

Dafirius Lombu[1], Siska Dame Tarihoran[2], Irwan Gulo[3]
[1,2,3]Mahasiswa Prorgram Studi Teknik Informatika STMIK Budidarma Medan
[1,2,3]Jln. Sisingamangaraja No. 338 Sp. Limun Medan
[1]daffilomboe@gmail.com, [2]sisgalungtarihoran@gmail.com, [3]irwanjitsam@gmail.com

Abstract

Generally, the database access of a website lies in the user login. When the login data is not accompanied by security techniques, it is very easily accessible by other parties. One effort that can be done to solve the problem is to encode the login data of website users based on cryptographic technique algorithm. Triangle Chain Cipher (TCC) is one of the classic cryptographic algorithms that encode data doubly and generate keys randomly along the plain. The process of encryption and decryption are interdependent to be one of the advantages of this algorithm. This algorithm will be more effective when combined with the Cipher Block Chaining (CBC) operation mode that is widely used in modern cryptographic algorithms today. The feedback mechanism between the blocks in this mode of operation is the operating advantage. This study describes how to combine the mode of operation of block chaining cipher with triangle chain cipher algorithm so that cipher data login website generated more random and difficult to find its original meaning.

Keywords: *Login, Database, Website, Cryptography, CBC, TCC.*

Abstrak

Umumnya akses database sebuah website terletak pada login pengguna. Bila data login tidak disertai dengan teknik pengamanan, maka sangat mudah diakses oleh pihak lain. Salah satu upaya yang dapat dilakukan untuk menyelesaikan masalah tersebut adalah menyandikan data login pengguna website berdasarkan algoritma teknik kriptografi. Triangle Chain Cipher (TCC) merupakan salah satu algoritma kriptografi klasik yang menyandikan data secara ganda dan membangkitkan kunci secara acak sepanjang plain. Proses enkripsi dan dekripsi yang saling tergantung menjadi salah satu kelebihan algoritma ini. Algoritma ini akan lebih efektif bila dikombinasikan dengan mode operasi Cipher Block Chaining (CBC) yang banyak digunakan pada algoritma kriptografi modern saat ini. Mekanisme umpan balik (feedback) antar blok pada mode operasi ini menjadi keunggulan operasinya. Penelitian ini menguraikan bagaimana mengkombinasikan mode operasi cipher block chaining dengan algoritma triangle chain cipher agar cipher data login website yang dihasilkan lebih acak dan sulit untuk menemukan makna aslinya.

Kata Kunci*: Login, Database, Website, Kriptografi,* CBC*, TCC.*

1. PENDAHULUAN

Website merupakan kumpulan halaman *web* yang saling berhubungan berisikan kumpulan informasi yang disediakan untuk perorangan, kelompok, atau organisasi. Salah satu hal penting yang perlu diperhatikan dalam keamanan *website* adalah pengamanan data *login.* Proses *login* merupakan salah satu mekanisme yang digunakan untuk melakukan autentikasi pengguna pada sebuah

website. Keamanan *login* pada *website* merupakan salah satu masalah yang rentan untuk diretas[1]. Keberahasilan penyerang untuk mendapatkan *login website*, mengakibatkan *database website* dapat diakses secara bebas kemudian mengeksploitasinya. Umumnya *login* terdiri atas *user* dan *password*. *Login* juga terdapat sebuah *database* yang merupakan tempat semua data *user* dan *password* disimpan. Basis data merupakan aspek yang sangat penting dalam sistem informasi dimana basis data merupakan penyimpanan data yang akan diolah lebih lanjut [2][3]. Penelitian lain mengatakan bahwa sebuah *website* perlu dan penting untuk dikelola keamanannya secara seksama dan teknik kriptografi menjadi salah satu alternatif yang dapat digunakan untuk itu[4].

Kriptografi merupakan salah satu teknik yang dapat digunakan untuk mengamankan suatu informasi. Kriptografi memiliki dua tahap yang umum dilakukan adalah tahap enkripsi dan dekripsi. Enkripsi adalah suatu proses yang dilakukan untuk mengubah pesan asli menjadi *ciphertext*, sedangkan dekripsi adalah proses yang dilakukan untuk mengubah pesan tersandi menjadi pesan yang dapat dibaca dan dimengerti[5][6]. Saat ini algoritma kriptografi yang digunakan adalah optimasi algoritma-algoritma sebelumnya khususnya untuk mewujudkan prinsip-prinsip teknik kriptografi, yaitu *diffusion* (mengaburkan) dan *confusion* (membingungkan)[7].

Mode *cipher block chaining*, merupakan salah satu mode operasi yang digunakan oleh banyak algoritma kriptografi modern saat ini. Hasil enkripsi dari blok sebelumnya akan berpegaruh dan digunakan pada proses enkripsi selanjutnya. Setiap blok *ciphertext* bukan hanya bergantung pada blok *plaintext*nya, tetapi bergantung pula pada blok-blok *plaintext* sebelumnya sehingga *plaintext* yang sama belum tentu menghasilkan *ciphertext* yang sama pula[8]. Sedangkan metode *triangle chain cipher* kunci yang digunakan dalam proses enkripsi dan dekripsi dibangkitkan secara acak sapanjang *plaintext*. Penyandian yang dilakukan secara ganda (dua kali) untuk menghasilkan *cipher* yang benar-benar acak menjadi kelebihan dari algoritma ini [9].

Penelitian ini menguraikan pengkombinasian mode operasi *cipher block chaining* (CBC) dengan *triangle chain cipher* (TCC), dimana teks *login website* terlebih dahulu dienkripsi berdasarkan mode operasi *cipher block chaining* kemudian *cipher* tersebut dienkripsi kembali berdasarkan algoritma *triangle chain cipher*. *Cipher* akhir yang dihasilkan dari proses enkripsi berdasarkan algoritma *triangle chain cipher* inilah yang akan disimpan ke dalam tabel *database login wbsite*. Hal ini dilakukan untuk merubah karakter-karakter teks *login* menjadi simbol-simbol lain (sandi) yang lebih acak serta tidak memperlihatkan korelasi dengan teks aslinya, sehingga tidak mudah dipahami oleh pihak lain (penyerang).

2. METODOLOGI PENELITIAN

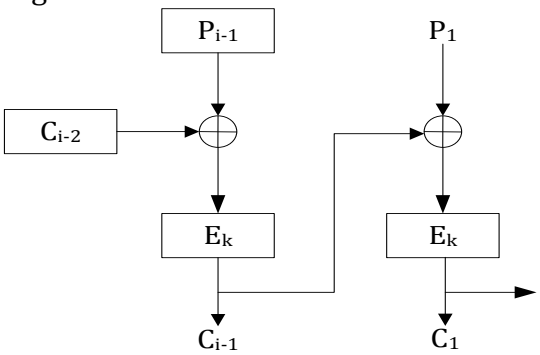
2.1 Kriptografi

Kriptografi merupakan salah satu teknik yang digunakan di dalam mengamankan data atau informasi yang bersifat penting dan rahasia. Teknik kriptografi sebagai salah satu teknik keamanan memiliki banyak algoritma untuk mengimplementasikan fungsinya. Algoritma tersebut seperti *hill cipher*, *triangle chain cipher*, *affine cipher*, DES, GOST, RSA, El-Gamal dan lainnya. Algoritma

kriptografi melakukan pengamanan data dengan cara merubah data asli menjadi karakter-karakter lain yang tidak lagi dimengerti maknanya oleh orang lain[5][9]. Proses ini disebut dengan istilah enkripsi, sedangkan proses untuk mengembalikan hasil hasil penyandian (*cipher*) menjadi teks asli (*plain*) dikenal dengan istilah dekripsi[12]. Adapun aspek atau tujuan yang harus dicapai dalam menerapkan teknik kriptografi adalah kerahasiaan, integritas, otentikasi dan ketiadaan penyangkalan[5][7]. Teknik kriptografi memiliki banyak algoritma dalam mencapai tujuandi atas, di antaranya algoritma *hill cipher*, *affine cipher*, DES, GOST, RC2, RC4 dan lainnya.

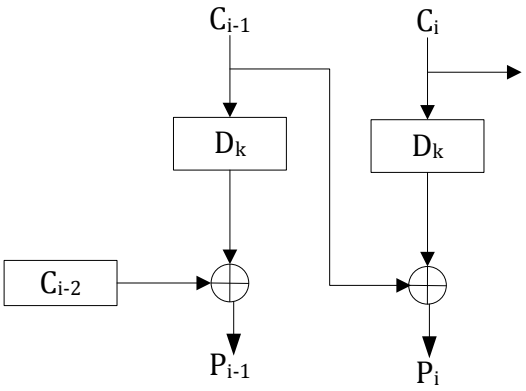
2.2 Mode Operasi Cipher Block Chaining

Mode operasi *Cipher Block Chaining* (CBC) melakukan proses enkripsi dan dekripsi berdasarkan operasi XOR antara blok *plain* dengan *cipher* sebelumnya. Salah satu ciri utama dari CBC adalah setiap blok *cipher* selalu bergantung pada blok-blok sebelumnya. Proses enkripsi yang pertama memerlukan *cipher* awal yang diwakili oleh sebuah blok biner yang ditentukan sendiri dan disebut dengan istilah *Initialization Vector* (IV) atau sering disebut *cipher* awal (C_0) dimana Jumlah bit C_0 harus sama dengan jumlah bit kunci [5]. Biner cipher yang dihasilkan dari setiap blok dipindahkan (*shift*) sebesar n-bit ke kanan atau kiri. Kesalahan satu bit pada sebuah blok *plaintext* akan merambat pada blok *ciphertext* yang ber-koresponden dan semua blok *ciphertext* berikutnya dan inilah yang menjadi kelemahan mode operasi ini. Mode operasi CBC juga memiliki kelebihan dimana blok-blok *plaintext* yang sama tidak menghasilkan blok-blok *ciphertext* yang sama, sehingga kriptanalisis menjadi lebih sulit [10]. Mode operasi *cipher block chaining* melakukan proses enkripsi pada setiap blok n-bit *plaintext yang* di-XOR-kan dengan blok n-bit *ciphertext* sebelumnya, kecuali blok *plaintext* pertama di-XOR-kan dengan *cipher* awal atau *Initialization Vector* (IV), sebesar n-bit. Skema *enkripsi* CBC dapat dilihat pada gambar 1 di bawah ini:



Gambar 1. Skema Enkripsi Berdasarkan Mode Operasi CBC

Proses dekripsi dilakukan dengan meng-XOR-kan blok *ciphertext* dengan blok *ciphertext* sebelumnya untuk menghasilkan blok *plaintext*. Proses dekripsi blok pertama dilakukan dengan meng-XOR-kannya dengan blok IV, sehingga dihasilkan *plaintext* blok pertama. Gambar skema dekripsi CBC dapat dilihat pada gambar 2 di bawah ini :



Gambar 2. Skema Dekripsi Berdasarkan Mode Operasi CBC

Secara matematis, enkripsi dan dekripsi berdasarkan mode operasi CBC adalah sebagai berikut :

$C_i = E_K(P_i \oplus (C_{i-1} \oplus K))$.....(1)

$P_i = D_K(C_i \oplus (C_{i-1} \oplus K))$ ..... (2)

Blok *plaintext* pertama menggunakan C_0 sebagai *cipher* awal dalam hal ini diwakili oleh blok *Initialization Vector* (IV).

2.3 Algoritma Triangle Chain Cipher

Triangle Chain Cipher (TCC) merupakan pengembangan dari algoritma kriptografi abjad tunggal khususnya algoritma substitusi abjad tunggal yang sangat mudah diserang dengan teknik analisis frekuensi. Kunci yang digunakan pada proses enkripsi dan dekripsi yaitu nilai integer yang menunjukkan pergeseran karakter-karakter sesuai dengan operasi pada *caesar cipher*. Hal inilah yang menjadi kekuatan utama dari algoritma ini. Barisan bilangan-bilangan yang berfungsi sebagai pengali dengan kunci yang berupa bilangan tertentu seperti deret bilangan ganjil, deret bilangan genap, deret fibonaci, deret bilangan prima, serta deret bilangan yang dapat dibuat sendiri menjadi kekuatan keduanya [9][11]. Algoritma ini melakukan proses enkripsi dan dekripsi secara ganda yang membentuk pola matriks segitiga pertama dan dan segitiga kedua.

Proses enkripsi dilakukan dua kali dalam pola matrix segitiga pertama dan segitiga kedua.

1. Matriks Enkripsi Segitiga Pertama
   Baris Ke-1:
   M [1j] = P[j] + (K * R[1]) Mod 256 .....(3)
   Baris ke-2 dan seterusnya untuk nilai j ≥ i :
   M [i j] = M [i-1], j + (K * R[i]) Mod 256 .....(4)
   Sehingga nilai *ciphertext* yang diperoleh dengan M [i j] pada nilai j = (N+i) – N
2. Matriks Enkripsi Segitiga Kedua
   untuk Baris Ke-1
   M[1j] = P[j] + (K * R[1]) Mod 256 .....(5)
   untuk baris ke-2 dan seterusnya untuk nilai j ≤ (N+1)- i :
   M [i j] = M [i-1], j + (K * R[i]) Mod 256 .....(6)
   Sehingga nilai *ciphertext* yang diperoleh dengan M [i j] = [(N+1) – i, j]

Proses dekirpsi dilakukan dengan pola segitiga terbalik dengan proses enkripsi.

1. Matriks dekripsi segitiga pertama
   untuk baris ke-1:
   M1j = C [j] – (K * (R[1])) Mod 256 .....(7)
   untuk baris ke-2:j ≤ (N+1) – i
   M[ij] = M[i-1], j – (K * (R[i])) Mod 256 .....(8)
   Sehingga nilai *plaintext* diperoleh dengan M [ij] = [(n+1)-i, i]
2. Matriks dekripsi segitiga kedua
   untuk baris ke-1:
   M1j = C [j] – (K* (R[1])) Mod 256 .....(9)
   untuk baris ke-2, nilai j ≥ i
   M[ij] = C[i-1], j – (K * (R[i])) Mod 256 .....(10)
   Sehingga nilai *plaintext* diperoleh dengan M[ij] pada nilai j = [i, (n+i)-N]

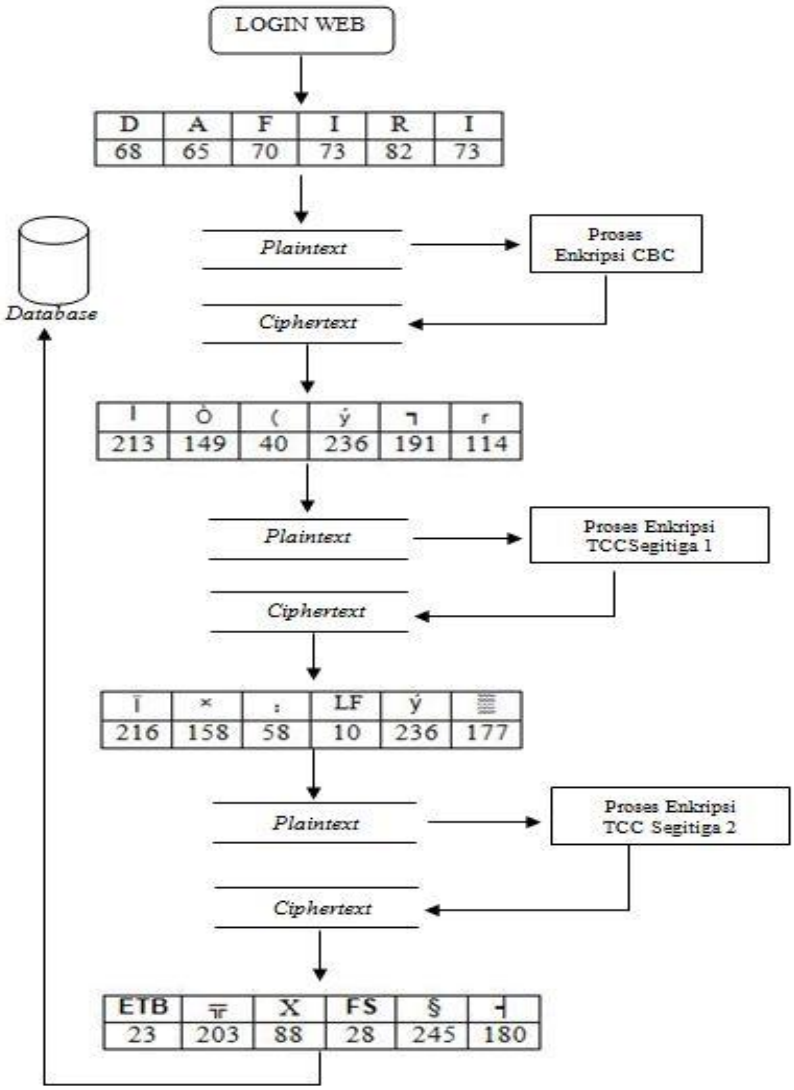
3. HASIL DAN PEMBAHASAN

3.1 Analisa Masalah

Keamanan data *login* sebuah *website* menjadi kunci utama dalam menjaga autentikasi pengguna website. Kelemahan pada sisi keamanan *login* akan menyebabkan pihak-pihak lain akan mudah mengakses isi *database website* yang dapat memungkina mereka untuk melakukan pencurian dan manipulasi bahkan penghancuran *website* itu sendiri. Selama ini, masih banyak pemiliki *website* yang menomor duakan atau mengabaikan keamanan data *login* pada *website* yang dimiliki, sehingga tidak mengherankan bila telah banyak *website* yang berhasil disadap dan disalahgunakan oleh pihak-pihak lain yang tidak bertanggungjawab.

Masalah ini dapat diminimalisir dengan menyandikan data *login* yang tersimpan di dalam *database website* berdasarkan algoritma kriptografi sehingga dapat mempersulit pihak-pihak lain yang berusaha mencuri dan menyalahgunakan data-data penting dari *website*. Pengkombinasian mode operasi *cipher block chaining* dengan algoritma *triangle chain cipher* menghasilkan *cipher login* pengguna yang cukup acak dan sulit ditemukan maknanya.

Langkah awal yang dilakukan adalah mengenkripsi teks asli dari *login* pengguna berdasarkan mode operasi *cipher block chaining* kemudian *cipher* yang dihasilkan dienkripsi kembali berdasarkan algoritma *triangle chain cipher*. Hasil enkripsi tersebut tersimpan dalam tabel *login*. Bila pengguna melakukan *login*, maka *record* tabel *login* yang ada di dalam *database* terlebih dahulu didekripsi secara otomatis oleh *website*. Hasil dekripsi tidak di-*update* menjadi isi *record* tabel *login*, tetapi akan disimpan pada *buffer* memori untuk sementara. Kemudian *website* akan melakukan pencarian *login* yang diinput oleh pengguna apakah ada pada *buffer* memori atau tidak. Bila ada, maka akses *database website* akan diizinkan, namun bila tidak ada maka akses ditolak. Skema penyandian *login* wbsite dapat diilustrasikan pada diagaram berikut ini.



Gambar 3. Skema Kombinasi CBC dengan TCC

Berdasarkan gambar 3 di atas, terlihat bahwa data login pengguna terlebih dhaulu dienkripsi berdasarkan mode operasi CBC. Hasil enkripsi CBC dienkripsi kembali berdasarkan algoitma TCC yang melakukan proses enkripsi secara ganda (dua kali). *Cipher* yang dihasilkan dari proses enkripsi segitiga kedua akan disimpan sebagai *cipher login* pada *database website*.

3.2 Implementasi

Berikut ini akan diimplementasikan penyandian data user website berdasarkan kombinasi mode operasi CBC dengan algoritma *triangle chain cipher*. Diasumsikan bahwa plainteks adalah kata **DAFIRI** (nama pengguna website).

a. Proses Enkripsi Berdasarkan Mode Operasi CBC
   Kunci = QR (2 byte atau 16 bit)
   IV/C0 = HJ (2 byte atau 16 bit)

Langkah pertama adalah mengkonversi *plaintext*, kunci dan C0 ke menjadi biner, sehingga dihasilkan :
DAFIRI = 010001000100000101000110010010010101001001001001
QR = 0101000101010010 (kunci)
HJ = 0100100001001010 (IV/C0)

Berikutnya adalah mengelompokkan biner *plaintext* sesuai dengan jumlah bit kunci (16 bit), sehingga :
P_1 = 0100010001000001
P_2 = 0100011001001001
P_3 = 0101001001001001

Proses enkripsi blok P1 :
P_1 = 0100010001000001
C_0 = 0100100001001010 XOR
$P_{1'}$ = 0000110000001011
Key = 0101000101010010 XOR
Hasil = 0101110101011001
Shift 4 bit hasil dari kiri ke kanan, menjadi :
C1 = 1101010110010101

Proses enkripsi blok P2 :
P_2 = 0100011001001001
C_1 = 1101010110010101 XOR
$P_{2'}$ = 1001001111011100
Key = 0101000101010010 XOR
Hasil = 1100001010001110
Shift 4 bit hasil dari kiri ke kanan, menjadi :
C2 = 0010100011101100

untuk mendapatkan *cipher* blok beriktunya dilakukan dengan cara yang sama seperti di atas, sehingga dihasilkan nilai desimal cipher dari seluruh blok *plaintext* adalah 213,149,40,236,191,114 atau dalam karakter **|ò(ý¬r** cipher yang dihasilkan pada proses CBC ini (**|ò(ý¬r)** akan dijadikan sebagai input (*plaintext*) pada proses enkripsi berdasarkan algoritma *triangle chain cipher*.

b. Proses Enkripsi Berdasarkan algoritma *Triangle Chain Cipher*
Plaintext adalah |ò(ý¬r (hasil enkripsi CBC), kunci yang digunakan dalam proses enkripsi maupun dekripsi adalah 3.
Proses Enkripsi Pola Segitiga Pertama :

Plaintext :	|	ò	(	ý	¬	r
	213	149	40	236	191	114

N = 6; Key = 3 dan R = 1,2,3,4,5,6

Untuk baris pertama i=1 dilakukan berdasarkan persamaan (3), maka :
M_{11} = (P[1] + (3*R[1])) mod 256
= (ı + (3*1)) mod 256
M_{14} = (P[4] + (3*R[1])) mod 256
= (ý + (3*1)) mod 256

= (213+3) mod 256
= 216 (ï)

M_{12} = (P[2] + (3*R[1])) mod 256
= (ò + (3*1)) mod 256
= (149+3) mod 256
= 152 (ÿ)

M_{13} = (P[3] + (3*R[1])) mod 256
= ((+ (3*1)) mod 256
= (40+3) mod 256
= 43 (+)

= (236+3) mod 256
= 239 (´)

M_{15} = (P[5] + (3*R[1])) mod 256
= (┐ + (3*1)) mod 256
= (191+3) mod 256
= 194 (┬)

M_{16} = (P[6] + (3*R[1])) mod 256
= (r + (3*1)) mod 256
= (114+3) mod 256
= 117 (u)

Untuk baris kedua (i=2) dan seterusnya, dimana j ≥ i, dilakukan berdasarkan persamaan (4), maka :

M_{22} = (M[2-1], 2 + (3*2)) mod 256
= (M12 + (3*2)) mod 256
= (ÿ+ 6) mod 256
= (152+6) mod 256
= 158 (×)

M_{23} = (M13 + (3*2)) mod 256
= (+ + 6) mod 256
= (43+6) mod 256
= 49 (1)

M_{24} = (M14 + (3*2)) mod 256
= (´+ 6) mod 256
= (239+6) mod 256
= 245 (§)

M_{25} = (M15 + (3*2)) mod 256
= (┬+ 6) mod 256
= (194+6) mod 256
= 200 (╚)

M_{26} = (M16 + (3*2)) mod 256
= (u + 6) mod 256
= (117+6) mod 256
= 123 ({)

Baris selanjutnya dapat dicari dengan cara yang sama seperti di atas, hingga didapatkan cipher seperti pada gambar 4.

ı ò (ý ┐ r ⟶ Sebagai *Plaintext*

Ciphertext						Hasil enkripsi pada i	Hasil enkripsi pada j = (n + i) - n	M_{ij}	Nilai Karakter	Nilai Desimal
Ï	ÿ	+	´	┬	u	1	(6+1) – 6 = 1	M_{11}	Ï	216
	×	1	§	╚	{	2	(6+2) – 6 = 2	M_{22}	×	158
		:	■	Ð	ä	3	(6+3) – 6 = 3	M_{33}	:	58
			LF	¦	Ė	4	(6+4) – 6 = 4	M_{44}	LF	10
				ý	ƒ	5	(6+5) – 6 = 5	M_{55}	ý	236
					▒	6	(6+6) – 6 = 6	M_{66}	▒	177

Ï × : LF ý ▒ ⟶ Hasil enkripsi (*ciphertext*) segitiga pertama

Gambar 4. Hasil Enkripsi Segitiga Pertama

Maka hasil dari tabel di atas proses enkripsi segitiga pertama adalah ï × : LF ý▒ dengan nilai desimal 216 158 58 10 236 177.

Proses Enkripsi Pola Segitiga Kedua :

Cipher yang dihasilkan pada proses segitiga pertama dijadikan sebagai *input* (*plain*) pada proses enkripsi segitiga kedua. Proses ini dilakukan dengan cara yang hampir sama dengan proses enkripsi segitiga pertama

yaitu berdasarkan persamaan (5) dan (6). Hasil keseluruhan dari proses enkripsi segitiga kedua, ditunjukkan pada gambar 5.

Ï × : LF ý ▒ ⟶ Sebagai *Plaintext*										
Ciphertext						Hasil enkripsi pada i	Hasil enkripsi pada j = (n + i) – i	M_{ij}	Nilai Karakter	Nilai Desimal
▉	í	=	CR	´	┤	1	(6+1) – 1 = 6	M_{16}	┤	23
ß	º	C	DC3	§		2	(6+1) – 2 = 5	M_{25}	§	203
Û	▒	L	FS			3	(6+1) – 3 = 4	M_{34}	FS	88
÷	╝	X				4	(6+1) – 4 = 3	M_{43}	X	28
ENQ	╦					5	(6+1) – 5 = 2	M_{52}	╦	245
ETB						6	(6+1) – 6 = 1	M_{61}	ETB	180
ETB ╦ X FS § ┤						⟶ Hasil enkripsi (*ciphertext*) segitiga kedua				

Gambar 5. Hasil Enkripsi Segitiga Kedua

Berdasarkan proses enkripsi segitiga kedua, maka didapatkan *cipher* akhir dari proses enkripsi berdasarkan algoritma *triangle chain cipher* adalah **ETB╦XFS§┤** dengan nilai desimal 23 203 88 28 245 180. *Cipher* inilah yang disimpan ke dalam tabel *database login*.

c. Proses Dekripsi

Berdasarkan analisa yang telah diuraikan sebelumnya bahwa dekripsi akan dilakukan secara otomatis oleh *website* pada saat pengguna melakukan *login* dimana hasil dekripsi *record* tabel *login* akan disimpan pada *buffer* memori untuk sementara. Data *login* yang diinput oleh pengguna akan dicek apakah ada atau tidak di dalam *buffer*.

Proses dekripsi dimulai dengan dekripsi *record* tabel *login* berdasarkan algoritma TCC, kemudian *plain* yang dihasilkan akan didekripsi kembali berdasarkan mode operasi CBC. Nilai kunci yang digunakan pada proses dekripsi berdasarkan algoritma TCC sama dengan kunci yang digunakan pada proses enkripsi. Hasil proses dekripsi berdasarkan algoritma TCC ditunjukkan pada gambar di bawah ini :

ETB ╦ X FS § ┤ ⟶ Sebagai *Ciphertext*										
Ciphertext						Hasil enkripsi pada i	Hasil enkripsi pada j = (n + i) – i	M_{ij}	Nilai Karakter	Nilai Desimal
DC4	╚	U	EM	_	▒	1	(6+1) – 1 = 6	M_{16}	Ï	216
SO	┬	O	DC3	ý		2	(6+1) – 2 = 5	M_{25}	×	158
ENQ	╣	F	LF			3	(6+1) – 3 = 4	M_{34}	:	58
¨	¡	:				4	(6+1) – 4 = 3	M_{43}	LF	10
Û	×					5	(6+1) – 5 = 2	M_{52}	ý	236
Ï						6	(6+1) – 6 = 1	M_{61}	▒	177
Ï × : LF ý▒						⟶ Hasil dekripsi (*ciphertext*) segitiga pertama				

Gambar 6. Hasil Dekripsi Segitiga Pertama Algoritma TCC

Berdasarkan gambar 6 di atas, maka *plaintext* proses dekripsi segitiga pertama adalah **ï × : LF ý▒** dengan nilai desimal 216 158 58 10 236 177. Plaintext ini akan dijadikan sebagai ciphertext pada proses dekripsi segitiga kedua.

ï × : LF ý ▒ ⟶ Sebagai *Ciphertext*										
Ciphertext						Hasil enkripsi pada		M_{ij}	Nilai Karakter	Nilai Desimal
						i	j = (n + i) - n			
ı	ø	7	BEL	Ù	«	1	(6+1) – 6 = 1	M_{11}		213
	ò	1	SOH	Ò	¿	2	(6+2) – 6 = 2	M_{22}		149
		(	°	┌	ƒ	3	(6+3) – 6 = 3	M_{33}		40
			ý	╬	ô	4	(6+4) – 6 = 4	M_{44}		236
				┐	ä	5	(6+5) – 6 = 5	M_{55}		191
					r	6	(6+6) – 6 = 6	M_{66}		114
ı	ò	(	ý	┐	r	⟶ Hasil dekripsi (*ciphertext*) segitiga kedua				

Gambar 7. Hasil Dekripsi Segitiga Kedua Algoritma TCC

Berdasarkan gambar 7 di atas, maka plainteks hasil proses dekripsi segitiga kedua adalah **ıò(ý┐ r** dengan nilai desimal 213 149 40236 191 114. *Plaintext* inilah yang kemudian dijadikan sebagai *ciphertext* yang didekripsi berdasarkan mode operasi *cipher block chaining*.

Sebelum proses dekripsi CBC dilakukan, maka terlebih dahulu dilakukan prososes pengelompokkan biner-biner *cipher* hasil dekripsi TCC, kemudian dilakukan proses pengembalian sejumlah n-bit pada posisi yang berlawanan dengan posisi *shift* pada proses enkripsi. Nilai kunci dan IV/C0 yang digunakan pada proses dekripsi berdasarkan CBC adalah sama dengan nilai kunci dan C0 yang digunakan pada proses enkripsi.

Ciphertext = ıò(ý┐ r (hasil dekripsi algoritma TCC)
Kunci algoritma TCC = 3
Kunci Mode Operasi CBC = QR dan IV/C0 adalah Hj
Berdasarkan proses dekripsi mode operasi CBC, maka diperoleh plaintext sebagai berikut :
P_1 = 0100010001000001 → DA (68 65)
P_2 = 0100011001001001 → FI (70 73)
P_3 = 0101001001001001 → RI (82 73)
Sehingga didapatkan *plaintext* adalah **DAFIRI** (sama seperti teks aslinya).

4. KESIMPULAN

Berdasarkan uraian analisa dan pembahasan, maka disimpulkan beberapa hal sebagai berikut :

a. Penyandian berdasarkan kombinasi mode operasi *cipher block chaining*(CBC) dan algoritma *Triangle Chain Cipher* (TCC) dapat diterapkan untuk menyandikan data *login user website* serta cukup memadai untuk menangkal penyerangan *record database* oleh pihak yang tidak berhak karena tingkat kesulitan dalam memecahkannya sangat rumit.
b. Sandi *login* yang dihasilkan cukup acak dan jauh berbeda dengan teks *login* asli sehingga pola-pola dan karakteristik teks *login* asli tidak lagi terlihat korelasinya dengan *cipher login* yang dihasilkan.
c. Selain hasil dari proses pengkombinasian CBC dan TCC yang cukup acak, maka waktu yang dibutuhkan dalam proses enkripsi maupun dekripsi menjadi lama.

DAFTAR PUSTAKA

[1] M. S. Dharmawan, Eka Adhitya , Erni Yudaningtyas, "Perlindungan Web pada Login Sistem Menggunakan Algoritma Rijndael," *Univ. Brawijaya*, vol. 7, no. 1, pp. 77–84, 2013.

[2] A. Nugroho, *Perancangan dan Implementasi Sistem Basis Data*, Yogyakarta: Andi, 2011.

[3] T. Zebua and Pritiwanto, "Pembangunan Web Mobile Absensi Mahasiswa Pada Platform Android Yang Terintegrasi Dengan Website Utama Sistem...," *J. Tek. Inform. Unika St. Thomas*, vol. 2, no. 1, pp. 100–107, 2017.

[4] Komarudin and A. R. Riswaya, "Sistem Keamanan Web Dengan Menggunakan Kriptografi Message Digest 5/MD5 Pada Koperasi Mitra Sejahtera Bandung," *J. Comput. Bisnis*, vol. 7, no. 1, pp. 30–41, 2013.

[5] E. Setyaningsih, *Kriptografi & Implementasinya Menggunakan Matlab*, Yogyakarta:Andi, 2015.

[6] R. Sadikin, 2012, *Kriptografi Untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java*, Yogyakarta, Andi.

[7] T. Zebua and E. Ndruru, "PENGAMANAN CITRA DIGITAL BERDASARKAN MODIFIKASI ALGORITMA RC4," *J. Teknol. Infomasi dan Ilmu Komput.*, vol. 4, no. 4, pp. 275–282, 2017.

[8] M. R. Faqih and E. Ariwibowo, "Visualisasi Algoritma Chiper Block Chaining Sebagai Media Pembelajaran Berbasis Mobile Android," *J. Sarj. Tek. Inform.*, vol. 2, no. 2, pp. 1381–1390, 2014.

[9] R.K. Hondro and G. W. Nurcahyo, "Analisis dan Perancangan Sistem Yang MenerapkanAlgoritma Triangle Chain Cipher (TCC) UntukEnkripsi Record Tabel Database." *Jurnal Teknologi Informasi dan Komputer*, vol.3, no.2. pp. 118-127, 2014.

[10] M. R. Faqih and E. Aribowo,"Visualisasi Algoritma Cipher Block Chaining Sebagai Media Pembelajaran Berbasis Mobile Android". *Jurnal Sarjana Teknik Informatika*, vol.2, no.2, pp. 1318-1390, 2014.

[11] T. Zebua, "ANALISA DAN IMPLEMENTASI ALGORITMA TRIANGLE CHAIN PADA PENYANDIAN RECORD DATABASE," *Pelita Inform. Budi Darma*, vol. 3, no. 2, pp. 37–49, 2013.

[12] E. Aribowo, "Aplikasi Pengamanan Dokumen Office Dengan Algoritma Kriptografi Kunci Asimetris Elgamal," *J. Inform.*, vol. 2, no. 2, pp. 209–219, 2008.