Implementasi Algoritma Triangle Chain Cipher Dalam Mengamankan Pesan Teks

Eriana Manik
STMIK Budi Darma Medan, Jl. SM.Raja No.338 Sp.Limun Medan, Sumut, Indonesia.
Email : Eriana.Manik@facebook.com

ABSTRACT
Chatting is a form of communication directly between two parties using typed text. If text messages on chat are very important and must be kept confidential, it is necessary to secure text messages on chat media that will be sent using cryptographic algorithms to prevent irresponsible parties. To fulfill this, the encryption (decryption and decryption) process of the text message will be sent. Encryption is done when sending by converting the original text message into a secret text message while decryption is done at the time of reception by converting the secret text message to the original text message. So the text message sent when chatting is a secret text message, so that the original text message cannot be known by unauthorized parties.

Kata kunci: Chatting, Kriptografi,Rahasia, Enkripsi, Dekripsi

PENDAHULUAN

Adanya perkembangan teknologi yang sangat pesat pada masa sekarang membuat manusia dapat dengan mudah bertukar informasi pada suatu individu ataupun organisasi sesuai dengan kebutuhan, menggunakan media *internet*. Media *internet* memungkinkan pengguna untuk berkomunikasi secara *real time* dengan menggunakan antarmuka *web,* seperti *chatting, email* dan lain sebagainya yang mudah diakses bagi pengguna untuk berkomunikasi dengan pesan teks. Pesan teks merupakan pemberitahuan, kata, atau komunikasi tertulis yang dikirimkan dari satu orang ke orang lain [9]. *Chatting* adalah suatu bentuk komunikasi secara langsung antara dua pihak menggunakan teks yang diketik. Jika pesan teks pada *chatting* sangat penting dan harus dijaga kerahasiaannya maka diperlukan pengamanan pesan teks pada media *chatting* yang akan dikirim dengan menggunakan algoritma kriptografi untuk mencegah dari pihak yang tidak bertanggung jawab.

Dalam masalah keamanan, ilmu kriptografi sangat penting untuk dikembangkan dan diterapkan. Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan informasi seperti kerahasiaan, integritas serta otentikasi. Sejarah ilmu kriptografi dibagi menjadi dua yaitu algoritma kriptografi klasik dan algoritma kriptografi modern.

Kriptografi klasik merupakan suatu algoritma yang menggunakan suatu kunci untuk mengamankan. Dua teknik dasar yang biasa digunakan pada algoritma jenis ini adalah teknik subtitusi dan teknik transposisi. Algoritma klasik melakukan penyandian karakter per karakter. Algoritma *Triangle Chain Cipher* merupakan salah satu dari algoritma klasik.

Algoritma *Triangle Chain Cipher* atau umumnya dikenal dengan sebutan algoritma rantai segitiga yaitu kunci yang dibangkitkan secara *random* dan panjang kunci sepanjang *plaintext* yang akan dienkripsi [7]. Pada algoritma kriptogarfi *triagle chain cipher* 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[6].

Dari pembahasan ini ada pun beberapa yang menjadi manfaat baik bagi penulis maupun bagi pembaca antara lain : Memungkinkan pesan teks yang dikirim tidak dapat dibaca oleh pihak yang tidak berkepentingan, Memberikan keamanan pesan teks pada media *chatting,* Bagi *user* yang membutuhkan keamanan dan kerahasian pesan teks, aplikasi keamanan pesan teks kombinasi algoritma *Triangle Chain Cipher* dapat dijadikan sebagai alternatif.

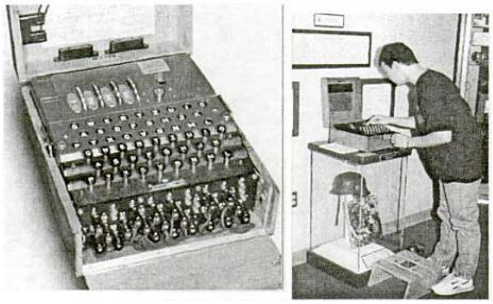
LANDASAN TEORI

Kriptografi berasal dari Bahasa Yunani, *crypto* dan *graphia. Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim kesuatu tempat ke tempat lain[4].

Kriptografi sudah digunakan 400 tahun yang lalu, diperkenalkan oleh orang-orang mesir lewat *hieroglyph[7]*. Pada zaman Romawi kuno Julius Caesar ingin mengirimkan pesan memalui seorang kurir, karena pesan tersebut mengandung rahasia Julius Caesar tidak inginpesan rahasia tersebut sampai terbuka dijalan. Julius Caesar kemudian memikirkan bagaimana mengatasinya, ia kemudian mengacak pesan tersebut hingga menjadi suatu pesan yang tidak dapat dipahamai oleh siapapun kecuali jendralnya saja. Julius Caesar kemudian mengganti semua susunan alfabet dari a, b, c yaitu a menjadi d, b menjadi e, c menjadi f dan seterusnya. Alat pembuat pesan rahasia pada zaman Romawi disebut *scytale* yang digunakan oleh tentara Sparta. *Scytale* merupakan suatu alat yang memiliki pita panjang dari daun papirus dan ditambah dengan sebatang silinder, setelah itu pita-dilepaskan dan dikirim [3].

Gambar 1 Scytale
sumber: Dony Ariyus, 2008 : 15.

Pada perang dunia kedua, Jerman menggunakan *Enigma* atau juga disebut mesin rotor yang digunakan Hitler untuk mengirimkan pesan ke tentaranya. *Enigma* yang digunakan jerman bisa mengenkripsikan satu pesan bisa mempunyai 15 miliyar-miliyar untuk dapat mendekripsikan satu pesan [3]



Gambar 2 Enigma
sumber: Dony Ariyus, 2008 : 22.

Selama bertahun-tahun kriptografi menjadi bidang khusus yang hanya dipelajari oleh kalangan militer, seperti agen keamanan nasional Amerika (*National Security Agency*), Uni Soviet, Inggris, Francis, Israel dan negara-negara lain. Dengan adanya persaingan ini maka kriptografi berkembang sesuai perkembangan zaman[4].

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

1. Enkripsi
   merupakan hal yang sangat penting dalam kriptografi yang merupakan pengamanan data yang dikirimkan terjaga sahasianya. Pesan teks asli disebut *plain*teks yang dirubah menjadi kode-kode yang tidak dimengerti enkripsi bisa diartikan *cipher.*
2. Dekripsi
   Dekripsi merupakan kebalikan dari enkripsi, pesan yang telah dikirim dikembalikan kebentuk asalnya (*Plain*teks) disebut dengan dekripsi pesan.
3. Kunci
   Kunci yang dimaksud disini adalah kunci yang dipakai unuk melakukan enkripsi dan dekripsi, kunci terbagi dua bagian, kunci pribadi (*Private key*) dan kunci umum atau *Private key* [3].

Algoritma kriptografi dibagi menjadi tiga bagian berdasarkan kunci yang dipakainya :

a. Algoritma simetri (menggunakan satu kunci untuk enkripsi dan dekripsinya).
b. Algoritma asimetri (menggunakan kunci berbeda untuk enkripsi dan dekripsi).
c. *Hash Function* [7]

2.4 Algoritma Kriptografi Klasik

Kriptografi klasik merupakan suatu algoritma yang menggunkan satu kunci untuk mengamankan data. Dua teknik dasar yang biasa digunakan pada algoritma-jenis ini, diantaranya adalah :

1. Teknik Subtitusi
   Penggantian setiap karakter *plain*teks dengan karakter lain. Ada 4 istilah dari-subtitusi *cipher* diantaranya adalah *monoalohabet, polyalphabet, monograf, polygraph.*
2. Teknik transposisi (Permutasi)
   Teknik ini menggunakan permutasi karakter [8]

2.5Algoritma *Triangle Chain Cipher*

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.

PEMBAHASAN

Berikut ini merupakan penerapan penyandian pesan teks menggunakan algoritma *Triangle Chain Cipher* dan bagaimana algoritma *Triangle Chain Cipher* bekerja pada aplikasi kriptografi yang akan dirancang, berdasarkan sistem aplikasi yang akan dibangun menggunakan algoritma *Triangle Chain Cipher*.

Enkripsi :

Enkripsi algoritma *Triangle Chain Cipher*

M_{11} = [M_{01} + (K * R_1)] mod 256
= [E + (3 * 1)] mod 256
= (69 + 3) mod 256
= 72 mod 256
= 72
= H

M_{13} = [M_{03} + (K * R_1)] mod 256
= [I + (3 * 1)] mod 256
= (73 + 3) mod 256
= 76 mod 256
= 76
= L

M_{15} = [M_{05} + (K * R_1)] mod 256
= [N + (3 * 1)] mod 256
= (78 + 3) mod 256
= 81 mod 256
= 81
= Q

M_{17} = [M_{07} + (K * R_1)] mod 256
= [B + (3 * 1)] mod 256
= (66 + 3) mod 256
= mod 256
= 69

Keterangan :
P = Plainteks
N = Jumlah karakter *plain*teks
M = Matriks penampung hasil penyandian
K = Kunci
R = *Row* (baris perkalian faktor pengali dengan kunci)
i = Indeks faktor pengali
j = Indek karakter p*lain*teks

Berikut ini merupakan penerapan penyandian pesan teks menggunakan algoritma *Triangle Chain Cipher* dan bagaimana algoritma *Triangle Chain Cipher* bekerja pada aplikasi kriptografi yang akan dirancang, berdasarkan sistem aplikasi yang akan dibangun menggunakan algoritma *Triangle Chain Cipher*.

Enkripsi :

Enkripsi algoritma *Triangle Chain Cipher*

Keterangan :
P = Plainteks
N = Jumlah karakter *plain*teks
M = Matriks penampung hasil penyandian
K = Kunci
R = *Row* (baris perkalian faktor pengali dengan kunci)
i = Indeks faktor pengali
j = Indek karakter p*lain*teks

Plain teks :

E	R	I	A	N	A	B	R	M	A	N	I	K
69	82	73	65	78	65	66	114	77	65	78	73	75

Nb : kunci = 3 ; R = N, i = R ; J = N
- Baris satu (i = 1)
j >= i : { 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 }

M_{12} = [M_{02} + (K * R_1)] mod 256
= [R + (3 * 1)] mod 256
= (82 + 3) mod 256
= 85 mod 256
= 85
= U

M_{14} = [M_{04} + (K * R_1)] mod 256
= [A + (3 * 1)] mod 256
= (65 + 3) mod 256
= 68 mod 256
= 68
= D

M_{16} = [M_{06} + (K * R_1)] mod 256
= [A + (3 * 1)] mod 256
= (65 + 3) mod 256
= 68 mod 256
= 68
= D

M_{18} = [M_{08} + (K * R_1)] mod 256
= [r + (3 * 1)] mod 256
= (114 + 3) mod 256
= 117 mod 256
= 117

= E

M_{19} = [M_{09} + (K * R_1)] mod 256
= [M + (3 * 1)] mod 256
= (77 + 3) mod 256
= 80 mod 256
= 80
= P

M_{111} = [M_{011} + (K * R_1)] mod 256
= [N + (3 * 1)] mod 256
= (78 + 3) mod 256
= 81 mod 256
= 81
= Q

M_{113} =[M_{013} + (K * R_1)] mod 256
= [K + (3 * 1)] mod 256
= (75 + 3) mod 256
= 78 mod 256
= 78
= N

= u

M_{110} = [M_{010} + (K * R_1)] mod 256
= [A + (3 * 1)] mod 256
= (65 + 3) mod 256
= 68 mod 256
= 68
= D

M_{112} = [M_{012} + (K * R_1)] mod 256
= [I + (3 * 1)] mod 256
= (73 + 3) mod 256
= 76 mod 256
= 76
= L

- Baris dua (i = 2)

j >= i : { 2,3,4,5,6,7,8,9,10,11,12,13}

M_{22} = [M_{12} + (K * R_2)] mod 256
= [U + (3 * 2)] mod 256
= (85 + 6) mod 256
= 91 mod 256
= 91
= [

M_{23} = [M_{13} + (K * R_2)] mod 256
= [L + (3 * 2)] mod 256
= (76 + 6) mod 256
= 82 mod 256
= 82
= R

M_{24} = [M_{14} + (K * R_2)] mod 256
= [D + (3 * 2)] mod 256
= (68 + 6) mod 256
= 74 mod 256
= 74
= J

M_{25} = [M_{15} + (K * R_2)] mod 256
= [Q + (3 * 2)] mod 256
= (81 + 6) mod 256
= 87 mod 256
= 87
= W

M_{26} = [M_{16} + (K * R_2)] mod 256
= [D + (3 * 2)] mod 256
= (68 + 6) mod 256
= 74 mod 256
= 74
= J

M_{27} = [M_{17} + (K * R_2)] mod 256
= [E + (3 * 2)] mod 256
= (69 + 6) mod 256
= 75 mod 256
= 75
= K

M_{28} = [M_{18} + (K * R_2)] mod 256
= [u + (3 * 2)] mod 256
= (117 + 6) mod 256
= 123 mod 256
= 123
= {

M_{29} = [M_{19} + (K * R_2)] mod 256
= [P + (3 * 2)] mod 256
= (80 + 6) mod 256
= 86 mod 256
= 86
= V

M_{210} =[M_{110} + (K * R2)] mod 256
= [D + (3 * 2)] mod 256
= (68 + 6) mod 256
= 74 mod 256
= 74
= J

M_{211} =[M_{111} + (K * R_2)] mod 256
= [Q + (3 * 2)] mod 256
= (81 + 6) mod 256
= 87 mod 256
= 87
= W

M_{212} =[M_{112} + (K * R_2)] mod 256
= [L + (3 * 2)] mod 256
= (76 + 6) mod 256
= 82 mod 256
= 82
= R

M_{213} =[M_{113} + (K * R_2)] mod 256
= [N + (3 * 2)] mod 256
= (78 + 6) mod 256
= 84 mod 256
= 84
= T

- Baris satu (i = 3)
j >= i : { 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 }
- Baris satu (i = 4)
j >= i : { 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 }
- Baris Lima (i = 5)
j >= i : { 5,6,7,8,9,10,11,12,13}
- Baris Enam (i = 6)
j >= i : { 6,7,8,9,10,11,12,13}
- Baris Tujuh (i = 7)
j >= i : { 7,8,9,10,11,12,13}
- Baris Delapan (i = 8)
j >= i : { 8,9,10,11,12,13}
- Baris Sembilan (i = 9)
j >= i : { 9,10,11,12,13}
- Baris Sepuluh (i = 10)
j >= i : { 10,11,12,13}
- Baris Sebelas (i = 11)
j >= i : { 11,12,13}
- Baris duabelas (i = 12)
j >= i : {12,13}
- Baris tigabelas (i = 13)
j >= i : {13}

Tabel 1 Enkripsi Segitiga Pertama.

	J1	J2	J3	J4	J5	J6	J7	J8	J9	J10	J11	J12	J13
I0	E	R	I	A	N	A	B	r	M	A	N	I	K
I1	H	U	L	D	Q	D	E	u	P	D	Q	L	N
I2		[	R	J	W	J	K	{	V	J	W	R	T
I3			[	S	`	S	T	„	_	S	`	[	]
I4				_	L	_	`	□	k	_	l	g	¡
I5					{	N	O	Ÿ	z	N	{	v	x
I6						€	□	±	Œ	€	□	^	Š
I7							–	Æ	¡	•	¢	□	Ÿ
I8								Þ	¹		º	µ	·
I9									Ô	È	Õ	Đ	Ò
I10										Æ	ó	¡	ð
I11													
I12												3	5
I13													\

Segitiga Enkripsi Kedua
-Baris satu (i = 1)
j >= i : { 1,2,3,4,5,6,7,8,9,10,11,12,13}
- Baris dua (i = 2)
j <=(n+1)- i = (13+1)-2 = 14-2= 12 : { 1,2,3,4,5,6,7,8,9,10,11,12}

- Baris Tiga (i = 3)
j <=(n+1)- i = (13+1)-3 = 14-3= 11 : { 1,2,3,4,5,6,7,8,9,10,11}
- Baris Empat (i = 4)
j <=(n+1)- i = (13+1)-4 = 14-4= 10 : { 1,2,3,4,5,6,7,8,9,10}
- Baris Lima (i = 5)
j <=(n+1)- i = (13+1)-5 = 14-5= 9 : { 1,2,3,4,5,6,7,8,9}
- Baris Enam (i = 6)
j <=(n+1)- i = (13+1)-6 = 14-6= 8 : { 1,2,3,4,5,6,7,8}
- Baris Tujuh (i = 7)
j <=(n+1)- i = (13+1)-7 = 14-7= 7 : { 1,2,3,4,5,6,7}
- Baris Delapan (i = 8)
j <=(n+1)- i = (13+1)-8 = 14-8= 6 : { 1,2,3,4,5,6}
- Baris Sembilan (i = 9)
j <=(n+1)- i = (13+1)-9 = 14-9= 6 : { 1,2,3,4,5}
- Baris Sepuluh (i = 10)
j <=(n+1)- i = (13+1)-10 = 14-10= 4 : { 1,2,3,4}
- Baris Sebelas (i = 11)
j <=(n+1)- i = (13+1)-11 = 14-11= 3 : { 1,2,3}
- Baris Duabelas (i = 12)
j <=(n+1)- i = (13+1)-12 = 14-12= 2 : { 1,2}
- Baris Tigabelas (i = 13)
j <=(n+1)- i = (13+1)-13 = 14-13= 1 : { 1}
M131 = [M121 + (K * R13)] mod 256
= [2 + (3 * 39)] mod 256
= (50 + 39) mod 256
= 89 mod 256
= 89
= Y

Tabel 2 Enkripsi Segitiga Kedua

	J1	J2	J3	J4	J5	J6	J7	J8	J9	J10	J11	J12	J13
I0	H	[	[	_	{	€	–	Þ	Ô	Æ		3	\
I1	K	^	^	b	~	ƒ	™	á	×	É		6	_
I2	Q	d	D	h	„	‰	Ÿ	ç	Ý	0		<	
I3	Z	m	M	q	□	'	¨	ä	æ	Ø	&		
I4	f	y	Y	}	™	Ž	´	ü	ò				
I5	u	^	^	Œ	¨		Å						
I6	‡	š	Š	ž	º	¿	Õ						
I7	œ	¯	¯	³	Ï	Ô	Ê						
I8	´	Ç	Ç	¶	Ò	×							
I9	Ï	â	Â	Ñ	Í								
I10	í			Ï									
I11		!	!										
I12	2	E											
I13	Y												

Cipher teks algoritma *Triangle Chain Cipher* = Y E ! ï í × ê & < _

Dekripsi :
Proses dekripsi algoritma *Triangle Chain Cipher*
Segitiga Dekripsi Pertama
- Baris satu (i = 1)
j >= i : { 1,2,3,4,5,6,7,8,9,10,11,12,13}
- Baris dua (i = 2)
j >= i : { 2,3,4,5,6,7,8,9,10,11,12,13}
- Baris Tiga (i = 3)
j >= i : { 3,4,5,6,7,8,9,10,11,12,13}
- Baris Empat (i = 4)
j >= i : { 4,5,6,7,8,9,10,11,12,13}
- Baris Lima (i = 5)
j >= i : { 5,6,7,8,9,10,11,12,13}
- Baris Enam (i = 6)
j >= i : { 6,7,8,9,10,11,12,13}
- Baris Tujuh (i = 7)
j >= i : { 7,8,9,10,11,12,13}
- Baris Delapan (i = 8)

j >= i : { 8,9,10,11,12,13}
- Baris Sembilan (i = 9)
j >= i : { 9,10,11,12,13}
- Baris Sepuluh (i = 10**)**
j >= i : { 10,11,12,13}
- Baris Sebelas (i = 11)
j >= i : { 11,12,13}
- Baris Duabelas (i = 12)
j >= i : { 12,13}
- Baris Tigabelas (i = 13)
j >= i : { 13}

Tabel 3 Dekripsi Segitiga Pertama

	J1	J2	J3	J4	J5	J6	J7	J8	J9	J10	J11	J12	J13
I0	Y	E	!	¡	í	×	Ê				&	<	_
I1	V	B	-	ì	ê	Ô	Ç		þ		#	9	\
I2		<		æ	ä	Î	Á		248	û		3	V
I3				Ý	Û	Å	ø		ï	ò		*	M
I4				Ñ	Ï	¹	Ì	ÿ	ã	æ		-	A
I5					À	ª	½	ä	Ô	×	ù		2
I6						˜	«	Þ	Â	Å	ç	ý	
I7							–	É		º	Ò	è	
I8								±	•	˜	º	Ð	ó
I9									z	}	Ÿ	µ	Ø
I10										_	□	—	º
I11											`	v	™
I12												R	u
I13													N

Segitiga Dekripsi Kedua
- Baris satu (i = 1)
j >= i : { 1,2,3,4,5,6,7,8,9,10,11,12,13}
- Baris dua (i = 2)
j <=(n+1)- i = (13+1)-2 = 14-2= 12 : { 1,2,3,4,5,6,7,8,9,10,11,12}

- Baris Tiga (i = 3)
j <=(n+1)- i = (13+1)-3 = 14-3= 11 : { 1,2,3,4,5,6,7,8,9,10,11}
- Baris Empat (i = 4)
j <=(n+1)- i = (13+1)-4 = 14-4= 10 : { 1,2,3,4,5,6,7,8,9,10}

- Baris Lima (i = 5)
j <=(n+1)- i = (13+1)-5 = 14-5= 9 : { 1,2,3,4,5,6,7,8,9}
- Baris Enam (i = 6)
j <=(n+1)- i = (13+1)-6 = 14-6= 8 : { 1,2,3,4,5,6,7,8}
- Baris Tujuh (i = 7)
j <=(n+1)- i = (13+1)-7 = 14-7= 7 : { 1,2,3,4,5,6,7}
- Baris Delapan (i = 8)
j <=(n+1)- i = (13+1)-8 = 14-8= 6 : { 1,2,3,4,5,6}
- Baris Sembilan (i = 9)
j <=(n+1)- i = (13+1)-9 = 14-9= 6 : { 1,2,3,4,5}
- Baris Sepuluh (i = 10)
j <=(n+1)- i = (13+1)-10 = 14-10= 4 : { 1,2,3,4}
- Baris Sebelas (i = 11)
j <=(n+1)- i = (13+1)-11 = 14-11= 3 : { 1,2,3}
- Baris Duabelas (i = 12)
j <=(n+1)- i = (13+1)-12 = 14-12= 2 : { 1,2}
- Baris Tigabelas (i = 13)
j <=(n+1)- i = (13+1)-13 = 14-13= 1 : { 1}

Tabel 4 Dekripsi Segitiga Kedua

	J1	J2	J3	J4	J5	J6	J7	J8	J9	J10	J11	J12	J13
I0	V	<		Ñ	À	˜	–	±	z	_	`	R	N
I1	S	9		Î	½	•	“	®	w	\	]	O	K
I2	M	3		È	·	□	□	¨	q	V	W	I	
I3	D	*	ý	¿	®	†	„	Ÿ	h	M	N		
I4	8	-	ñ	³	¢	Z	x	“	\	A			
I5	)		â	¤	“	K	¡	„	M				
I6		Ý	Ð	’	□	Y	W	R					
I7		È	»	}	L	D	B						
I8	ê	Ð	£	Z	I	A							
I9	Ï	µ	^	_	N								
I10	±	—	j	A									
I11	□	v	I										
I12	I	R											
I13	E												

KESIMPULAN

Berdasarkan penelitian yang telah dilakukan penulis pada aplikasi *chatting* menggunakan teknik kriptografi yang dibangun maka dapat disimpulkan :

1. Konsep pengamanan pesan teks dapat menggunakan proses penyandian (enkripsi dan dekripsi) terhadap pesan teks yang akan dikirimkan sehingga pihak yang tidak berkepentingan tidak mengetahui keseluruhan isi obrolan.
2. penerapan algoritma *Triangle Chain Cipher* pada aplikasi *chatting* ini dapat pengamankan isi obrolan via tulisan, Dengan ini penggunaan algoritma *Triangle Chain Cipher* dapat mengamankan pesan teks, serta dapat menyajikan enkripsi dan dekripsi dengan tepat.
3. Aplikasi *chatting* dengan menerapkan teknik kriptografi algoritma *Triangle Chain Cipher* telah selesai dirancang dan dapat dijadikan salah satu alternatif aplikasi *chatting* dengan teknik kriptografi.

DAFTAR PUSTAKA

[1]. Abdul Kadir. (2013). “Pengertian Algoritma, Pendekatan Secara Visual dan Interaktif Menggunakan Raptor”. Yogyakarta : ANDI.
[2]. Adi nugroho. (2010). “Rekayasa Perangkat Lunak Berorientasi Objek Dengan Metode USDP (unified Software Development Process)”. Yogyakarta : ANDI.
[3]. Dony Ariyus. (2006). “Keamanan Data dan Komunikasi”. Yogyakarta : Graha Ilmu.
[4]. Dony Ariyus. (2008). “pengantar ilmu kriptografi: teori analisis dan implementasi”. Yogyakarta : ANDI.

[5]. Edy Irwansyah dan Jurike V. Moniaga. (2014). "Pengantar Teknologi Informasi". Yogyakarta : Deepublish.
[6]. Rifki Sadikin. (2012). "Kriptografi untuk Keamanan Jaringan". Yogyakarta : ANDI.
[7]. Rinaldi Munir. (2007). "Algoritma dan Pemograman Dalam Bahasa Pascal dan C". Bandung : INFORMATIKA.
[8]. Taronisoki Zebua (2013). "Analisa Dan Implementasi Algoritma Triangle Chain Pada Penyandian Record Database".
[9]. Windu Gara, Grace Gata. (2013). "Sukses Membangun Aplikasi Penjualan Dengan Java". Jakarta : PT. Alex Media Komputindo.
[10]. Zainal Arifin & Smitdev Community (2008). "36 Menit Belajar Komputer: Php Dan Mysql". Jakarta : PT. Alex Media Komputindo.