ANALISA KRIPTOGRAFI BLOCK CIPHER PADA PENGAMANAN TEKS MENGGUNAKAN METODE TRIPLE TRANSPOSITION VIGENERE CIPHER

Sinawati[1*], Indrianti[2] , M. Hafid[3]
[123]Program Studi Sistem Infromasi, Sistem Informasi, STMIK PPKIA Tarakanita Rahmawati
Jl. Yos Sudarso No. 6 Tarakan Tengah 77111
*Email: indri@ppkia.ac.id

Abstrak

Sistem pada keamanan data dan kerahasiaan data merupakan salah satu aspek penting dalam perkembangan kemajuan teknologi informasi, namun yang cukup disayangkan adalah ketidakseimbangan antara setiap perkembangan suatu teknologi yang tidak diiringi dengan perkembangan pada sistem keamanannya itu sendiri, dengan demikian cukup banyak sistem yang masih lemah dan harus ditingkatkan keamanannya. Oleh karena itu pengamanan data yang sifatnya rahasia harus benar-benar diperhatikan. Penelitian ini bertujuan untuk melakukan proteksi terhadap pengamanan teks dengan cara melakukan proses acak teks atau enkripsi, serta melakukan proses pengembalian teks ke bentuk semula atau dekripsi dengan menerapkan algoritma kriptografi block cipher menggunakan metode Triple Transposition Vigenere Cipher. Block Cipher adalah algoritma enkripsi yang akan membagi-bagi plaintext yang akan dikirimkan dengan ukuran tertentu (disebut blok). Algoritma enkripsi menghasilkan blok cipherteks yang berukuran sama dengan blok plainteks. Metode Triple Transposition Vigenere Cipher adalah salah satu metode block cipher dengan menerapkan dua metode penyandian yaitu teknik transposisi dan subtitusi.

***Kata kunci**: Kriptografi Block Cipher; Triple Transposition Vigenere Cipher*

1. PENDAHULUAN

Pada saat ini komputer sudah memasuki hampir setiap aspek kehidupan manusia. Teknologi komputer telah mendapat perhatian dari banyak orang di dunia ini. Banyak hal yang dulu dilakukan manusia secara manual dan manusia itu sendiri tidak lepas dari kebutuhan akan informasi, seiring berjalannya waktu yang terus berputar, dari hari kehari dari bulan kebulan dan dari tahun ketahun maka secara otomatis segala sesuatu yang ada disekeliling pun turut berubah-ubah layaknya sebuah metamorfosis sempurna. Teknologi komputer telah berevolusi secara cepat disegala bidang. Dalam sekejap mata saja, informasi yang ada dibelahan dunia ada digenggaman kita. Teknologi komputerisasi itu yang dikenal dengan Internet.

Internet merupakan jaringan komputer yang dibentuk oleh Departemen Pertahanan Amerika Serikat pada tahun 1969, melalui proyek ARPA yang disebut ARPANEThttp://id.wikipedia.org/wiki/ARPANET (*Advanced Research Project Agency Network*). ARPA berganti menjadi DARPA atau (*Defence Advanced Research Project Agency*). DARPA bekerjasama dengan berbagai lembaga pendidikan dan institusi riset, memulai program riset untuk menginvestigasi teknologi yang mampu menyatukan paket-paket jaringan dalam beragam bentuk. Sasaran utamanya adalah mengembangakan protocol komunikasi yang memungkinkan komputer-komputer dapat berkomunikasi secara transparan melintasi multi paket jaringan yang terhubung, ini dikenal dengan "*The Interneting Project"* dan "*The System of Networks"*, yang kemudian melahirkan Internet. Internet juga merupakan media yang sangat strategis dalam membangun informasi. Dengan berkembangnya internet, kebutuhan untuk menuangkan informasi yang lebih interaktif menjadi kebutuhan yang mutlak dalam penyajian informasi melalui situs di internet atau website.

Sejak pertama kali munculnya kriptografi, metode enkripsi selalu mengalami perubahan. Metode ini berkembang dari waktu ke waktu mulai dari algoritma kriptografi klasik hingga kriptografi modern, dari yang menggunakan kunci *simetris* hinggan kunci *assimetris.* Semua perkembangan ini menjadi satu tujuan, yaitu membuat kriptanalisis yang sesulit mungkin meningkatkan keamanan. Untuk membuat sebuah algoritma enkripsi yang

tidak dapat dipecahkan, ada beberapa syarat yang harus dipenuhi. Syarat tersebut yaitu kunci yang benar-benar acak dan panjang kunci harus sama dengan panjang plainteks sehingga plainteks yang sama tidak selalu menghasilkan ciphertext yang sama.

Dalam penelitian ini, muncul sebuah gagasan untuk menerapkan metode Triple Transposition Vigenere Cipher dalam proses penyandian huruf. Huruf yang digunakan sebanyak sembilan puluh lima karakter (95) terdiri dari huruf besar (a-z), huruf kecil (a-z), angka (0-9) dan tanda baca yang terdapat pada *keyboard.* Huruf-huruf tersebut yang biasanya digunakan dalam pembentukan teks atau pesan.

2. METODOLOGI PENELITIAN

Data dalam dunia informatika sangat penting perannya, karena dalam suatu operasi logika sangat diperlukan untuk proses input. Basis dari masing-masing data dapat berupa teks, sinyal listrik, gerakan suatu objek dan lain sebagainya. Pentingnya sebuah data bagi proses, maka untuk itu diperlukan suatu metode pengamanan data yang tujuan utamanya untuk melindungi data dalam hal ini berupa pesan atau teks yang terdiri dari karakter inputan seperti huruf abjad kapital A – Z, a – z , angka 0 – 9 dan tanda baca yang ada pada *keyboard*. Pada kriptografi klasik ada dua macam cara enkripsi yang dilakukan. Teknik enripsi itu adalah subtitusi dan transposisi.

2.1. Teknik Subtitusi

Algoritma kriptografi teknik substitusi adalah teknik kriptografi yang mula-mula digunakan oleh kaisar Romawi “Julius Caesar” untuk berkirim pesan dengan para gubernurnya. Teknik ini menyandikan pesan yang dikirim dengan mengganti setiap karakter dengan karakter lain dalam susunan abjad (alfabet). Ada empat jenis teknik subtitusi yaitu :

a) *Cipher abjad-tunggal***,** merupakan proses enkripsi yang dilakukan dengan mengganti satu huruf pada plainteks dengan satu huruf yang bersesuaian.
b) *Cipher subtitusi homofonik*, setiap huruf plainteks dipetakan kedalam salah satu huruf ciphertext yang mungkin. Tujuan pemetaan ini adalah untuk menyembunyikan hubungan statistik antara plainteks dengan cipherteks.
c) *Cipher abjad-majemuk*, menggunakan kunci yang berbeda-beda untuk setiap huruf plainteks.
d) *Cipher subtitusi poligram*, proses enkripsi dilakukan dengan pengelompokkan huruf-huruf dalam plainteks menjadi n huruf tiap bloknya dengan membuang spasi.

2.2. Teknik Transposisi

Metode Penyandian transposisi adalah metode penyandian dengan cara merubah letak dari teks pesan yang akan disandikan. Untuk membaca pesan aslinya kembali cukup dengan mengembalikan letak dari pesan tersebut berdasarkan kunci dan algoritma pergeseran huruf yang telah disepakati. Nama lain untuk metode ini adalah permutasi, karena transpose setiap huruf didalam teks sama dengan mempermutasikan karakter-karakter tersebut. Contoh paling sederhana adalah dengan membalik kata-kata pada plainteks :

Plainteks : MANFAAT ILMU KRIPTOGRAFI INI
Ciphertekx : TAAFNAM UMLI IFARGOTPIRK INI

Contoh transposisi lainnya adalah menyusun plainteks menjadi n baris dengan bentuk *Rail Fence.* Berikut contoh menggunakan algoritma 5 baris :

M								L								O								I
	A						I		M						T		G						N	
		N				T				U				P				R				I		
			F		A						K		I						A		I			
				A								R								F				

Ciphertekx : MLOIAIMTGNNTUPRIFAKIAIARF

3. HASIL PENELITIAN DAN PEMBAHASAN

Dalam proses pengiriman pesan, kerahasiaan itu menjadi kunci utama dalam proses pengiriman. Banyak cara user mengamankan pesan menggunakan beberapa metode pengamanan. Pada penelitian ini, penggunaan karakter pesan terdiri dari sembilan puluh lima (95) karakter meliputi :

a) Abjad huruf kecil (a-z), sebanyak 26 huruf
b) Abjad huruf besar (A-Z), sebanyak 26 huruf
c) Angka (0-9), sebanyak 10 angka
d) Tanda baca, sebanyak 16 karakter, meliputi: blank, (.), koma (,), !, ;, :, -, ?, (,), {, }, ‘, “, /,`
e) Simbol sebanyak 17 karakter, meliputi: @, #, $, %, ^, &, ~, _, =, +, *, |, [,], \, <, >

3.1. Vigenere Cipher

Kode Vigenere termasuk kode abjad majemuk (*polyalphabetic subsitution cipher*). Dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaisce de Vigenere pada abad 16, tahun 1586 yaitu Giovan Batista Belaso dalam bukunya yang berjudul La Cifra Del Sig. Algoritma ini baru dikenal luas 200 tahun kemudian dan dinamakan kode Vigenere. Kemudian pada tahun 1508, Johannes Trithemius dalam Poligraphia karyanya menemukan *Recta Tabula* yang merupakan komponen terpenting dari Vigenere Cipher.Penelitian ini menggunakan jumlah karakter inputan sebagai Recta Tabula yang menjadi komponen subtitusi. Beberapa ketentuan dalam metode Vigenere Cipher antara lain:

a) Kata kunci digunakan secara berulang
b) Kata kunci digunakan untuk menentukan enkrispsi setiap alphabet dalam plainteks
c) Huruf ke-i dalam plainteks di spesifikasikan oleh alphabet yang digunakan dalam kunci
d) Penggunaan alphabet bisa berulang

Pada Vigenere cipher tiap baris tabel cocok dengan Caesar cipher. Baris pertama merupakan shift 0, baris kedua merupakan shift 1 dan baris terakhir merupakan shift 94. Vigenere cipher menggunakan kode tersebut bersama dengan sebuah karakter sebanyak 95 karakter untuk melakukan *encipher* pesan. Teknik Vigenere Cipher bisa dilakukan dengan dua cara, yaitu:

(1) Pergeseran Huruf

P / K	(blank)	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/	0
Kode Pergeseran	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
P / K	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?	@	A
Kode Pergeseran	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
P / K	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
Kode Pergeseran	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
P / K	S	T	U	V	W	X	Y	Z	[	\	]	^	_	`	a	b	c
Kode Pergeseran	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67
P / K	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
Kode Pergeseran	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84
P / K	u	v	w	x	y	z	{	|	}	~							
Kode Pergeseran	85	86	87	88	89	90	91	92	93	94							

Gambar 1. Kode Pergeseran Huruf

Teknik pergeseran menggunakan angka dilakukan dengan menukarkan kode pergeseran dari karakter (kunci) tersebut. Pemberian angka yang dimulai dengan kode pergeseran 0 menjadi karakter ‘*Blank*’ atau merupakan karakter ‘Spasi’ dan diakhiri kode pergeseran

94 menjadi karakter '~'. Pada proses enkripsi, karakter cipherteks didapat dengan rumus :

$$C(P) = (P + k) \bmod 95$$

Proses dekripsi pada Vigenere Cipher dapat dilakukan dengan cara sebaliknya, karakter plainteks didapat dengan rumus :

$$P = (C - k) \bmod 95$$

Tabel 1. Enkripsi menggunakan Pergeseran Huruf

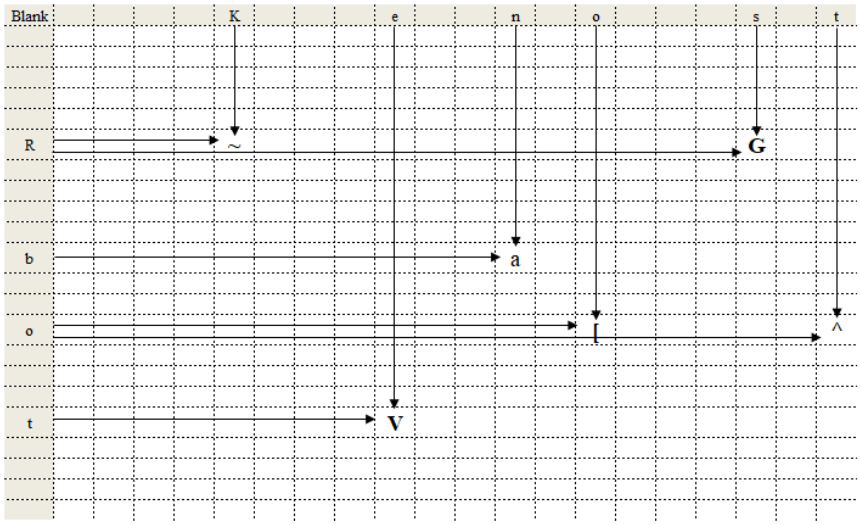
Plainteks	**K**	**o**	**n**	**t**	**e**	**s**
Kode Pergeseran	43	79	78	84	69	83
K	R	o	b	o	t	R
Kode Pergeseran	51	75	82	73	80	51
C (P)	94 (~)	59 ([ )	65 (a)	62 (^)	54 (V)	39 (G)

Terlihat dari contoh diatas bahwa huruf yang sama tidak selalu dienkripsi menjadi huruf yang sama pula. Hal ini merupakan karakteristik dari cipher abjad majemuk yaitu setiap huruf cipherteks dapat memiliki kemungkinan banyak huruf plainteks. Hasil dekripsi dari kasus tersebut disajikan pada tabel 2.

Tabel 2. Dekripsi menggunakan Pergeseran Huruf

Plainteks	**~**	**[**	**a**	**^**	**V**	**G**
Kode Pergeseran	94	59	65	62	54	39
K	R	o	b	o	t	R
Kode Pergeseran	51	75	82	73	80	51
C (P)	43 (K)	79 (o)	78 (n)	84 (t)	69 (e)	83 (s)

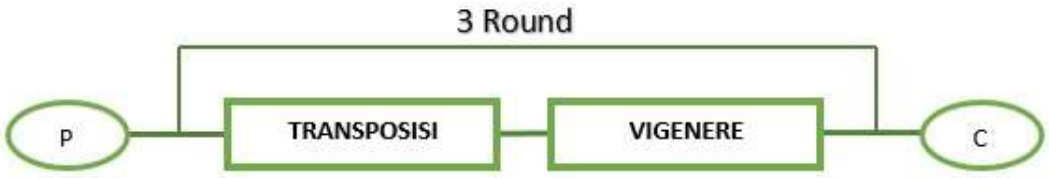
(2) Teknik Subtitusi (*Sumbu x , y*)
Teknik subtitusi dengan cara menghubungkan plaintext dengan key dapat diamati pada gambar 2 berikut :



Gambar 2. Subtitusi

3.2. Triple Transposition Vigenere Cipher

TTVC adalah metode pengamanan dengan cara mengulang teknik Vigenere Cipher yang setiap plainteksnya dilakukan transposisi terlebih dahulu sebanyak tiga kali dengan menggunakan kunci yang tiap kuncinya harus berbeda dengan satu dengan yang lainnya. Proses yang terjadi pada TTVC terbagi menjadi dua bagian. Proses tersebut dapat dilihat pada gambar 3 berikut :



Gambar 3. Metode TTVC

Metode transposisi dapat disimbolkan dengan T dan metode Vigenere disimbolkan dengan E serta kunci untuk melakukan subtitusi *k*. Secara matematis metode enkripsi TTVC ini dapat dituliskan sebagai :

$$\mathbf{C} = S_3 (T_3 (S_2 (T_2 (S_1 (T_1 (\mathbf{P})))))) \quad (1)$$

Bila dijabarkan, cipherteks diperoleh dengan mentransposisikan plainteks, kemudian hasilnya disubtitusikan menggunakan kunci pertama lalu dilakukan proses yang sama menggunakan kunci kedua hingga kunci ketiga. Proses dekripsi dapat dilakukan dengan arah sebaliknya, bila dirumuskan makan akan terlihat secara sistematis sebagai berikut :

$$\mathbf{P} = T_1' (S_1' (T_2' (S_2 ' (T_3' (S_3' (\mathbf{C})))))) \quad (2)$$

Maksud T' disini adalah transposisi kebalikannya dan S' adalah subtitusi kebalikannya. Pada penelitian ini penerapan metode transposisi karakter *spasi* akan diganti dengan karakter 'Q'. Ilustrasi dari proses enkripsi hingga dekripsi dapat lihat contoh sebagai berikut :

Plainteks (P) :
Kontes Robotika STMIK

Transposisi pertama (T_1) , Kunci : 3

K	o	n
t	e	s
Q	R	o
b	o	t
i	k	a
Q	S	T
M	I	K

Hasil **T_1 : KtQbiQMoeRokSInsotaTK**

Subtitusi pertama **(S_1)** menggunakan metode Vigenere Cipher dengan rumus enkripsi yang telah dijelaskan pada point sebelumnya. Proses enkripsi dari hasil transposisi **(T_1)** dapat dilihat pada gambar 4 dengan *k* (S_1) = 'Sepuluh'.

T1	K	t	Q	b	i	Q	M	o	e	R	o	k	S	I	n	s	o	t	a	T	K
Kode Pergeseran	43	84	0	66	73	0	45	79	69	50	79	75	51	41	78	83	79	84	65	52	43
k (S1)	S	e	p	u	l	u	h	S	e	p	u	l	u	h	S	e	p	u	l	u	h
Kode Pergeseran	51	69	80	85	76	85	72	51	69	80	85	76	85	72	51	69	80	85	76	85	72
C (P)	94	58	80	56	54	85	22	35	43	35	69	56	41	18	34	57	64	74	46	42	20

Gambar 4. Enkripsi pertama (E_1)

Melihat kode pergeseran yang disajikan dalam gambar 1, maka karakter dari nilai C(P) tersebut adalah " **~ZpXVu6CKCeXI2BY`jNJ4** ". Setelah itu dilanjutkan dengan melakukan proses transpos yang kedua (**T_2**). Proses transpos yang kedua sama dengan proses transpose yang pertama, hanya saja proses transpose yang kedua menggunakan kunci : 2. Proses ini dapat dilihat pada penjelasan berikut :

Cipherteks (P) :
~ZpXVu6CKCeXI2BY`jNJ4

Transposisi kedua (T_2) , Kunci : 2

~	Z
p	X
V	u
6	C
K	C
e	X
I	2
B	Y
`	j
N	J
4	

Hasil **T_2 : ~pV6KeIB`N4ZXuCCX2YjJ**

Proses enkripsi subtitusi dari hasil transposisi **(T_2)** dapat dilihat pada gambar 5 dengan *k* (S_2) = 'Sembilan'.

T2	~	p	V	6	K	e	I	B	`	N	4	Z	X	u	C	C	X	2	Y	j	J
Kode Pergeseran	94	80	54	22	43	69	41	34	64	46	20	58	56	85	35	35	56	18	57	74	42
k (S2)	S	e	m	b	i	l	a	n	S	e	m	b	i	l	a	n	S	e	m	b	i
Kode Pergeseran	51	69	77	66	73	76	65	78	51	69	77	66	73	76	65	78	51	69	77	66	73
C (P)	50	54	36	88	21	50	11	17	20	20	2	29	34	66	5	18	12	87	39	45	20

Gambar 5. Enkripsi kedua (E_2)

Karakter dari nilai C(P) tersebut adalah " **RVDx5R+144!=Bb%2,wGM4** ". Setelah itu dilanjutkan dengan melakukan proses transpos yang ketiga (**T_3**) menggunakan kunci : 7.

Cipherteks (P) :
RVDx5R+144!=Bb%2,wGM4

Transposisi ketiga (T_3) , Kunci : 7

R	V	D	x	5	R	+
1	4	4	!	=	B	b
%	2	,	w	G	M	4

Hasil **T_3 : R1%V42D4,x!w5=GRBM+b4**

Proses enkripsi subtitusi dari hasil transposisi **(T_3)** dapat dilihat pada gambar 6 dengan *k* (S_3) = 'LiFe'.

T3	R	1	%	V	4	2	D	4	,	x	!	w	5	=	G	R	B	M	+	b	4
Kode Pergeseran	50	17	5	54	20	18	36	20	12	88	1	87	21	29	39	50	34	45	11	66	20
k (S3)	L	i	F	e	L	i	F	e	L	i	F	e	L	i	F	e	L	i	F	e	L
Kode Pergeseran	44	73	38	69	44	73	38	69	44	73	38	69	44	73	38	69	44	73	38	69	44
C (P)	94	90	43	28	64	91	74	89	56	66	39	61	65	7	77	24	78	23	49	40	64

Gambar 6. Enkripsi ketiga (E_3)

Jadi dari proses enkripsi menggunakan metode TTVC, cipherteks dari plainteks "**Kontes Robotika STMIK**" adalah "**~zK<`{jyXbG]a'm8n7QH`**". Selanjutnya dilakukan proses dekripsi menggunakan rumus yang telah dibahas pada pembahasan sebelumnya. Berdasarkan rumus tersebut, proses dekripsi dapat dilihat pada gambar 7 dengan kunci yang sama :

C (P)	~	z	K	<	`	{	j	y	X	b	G	]	a	'	m	8	n	7	Q	H	`
Kode Pergeseran	94	90	43	28	64	91	74	89	56	66	39	61	65	7	77	24	78	23	49	40	64
k (S3)	L	i	F	e	L	i	F	e	L	i	F	e	L	i	F	e	L	i	F	e	L
Kode Pergeseran	44	73	38	69	44	73	38	69	44	73	38	69	44	73	38	69	44	73	38	69	44
T2	50	17	5	54	20	18	36	20	12	88	1	87	21	29	39	50	34	45	11	66	20

Gambar 7. Dekripsi pertama (D_1)

Karakter dari nilai dekripsi dengan melihat kode pergeseran tersebut sama dengan karakter hasil transpose T_3 yaitu "**R1%V42D4,x!w5=GRBM+b4".** Dalam hal ini selanjutnya akan dilakukan transpose pertama T_1 menggunakan kunci = 7.

Transposisi pertama (T_1) , Kunci : 7

R	V	D	x	5	R	+
1	4	4	!	=	B	b
%	2	,	w	G	M	4

Hasil **T_3 : RVDx5R+144!=Bb%2,wGM4**

Selanjutnya akan dilakukan proses yang sama mulai dari subtitusi menggunakan kunci "Sembilan" dan transpose menggunakan kunci = 2 hingga subtitusi menggunakan kunci "Sepuluh" dan transpose menggunakan kunci = 3.

4. KESIMPULAN

Metode TTVC ini terlihat bahwa ketergantungan hasil cipherteks terhadap kunci sangat tinggi. Setiap kunci harus didefinisikan dengan baik. Dengan begitu dapat dikatakan bahwa TTVC berpotensi untuk mengimbangi kekuatan *One Time Pad*. Bila ditinjau lebih jauh lagi,

kunci dapat ditransposisikan terlebih dahulu baru disubtitusikan secara virtual. Ada beberapa hal yang perlu diperhatikan saat menetapkan kunci, antara lain :

a) Kunci subtitusi sebaiknya memiliki panjang yang berbeda satu dengan yang lainnya.
b) Kunci transposisi harus merupakan yang berbeda satu dengan yang lain agar hasil transposisinya berbeda-beda.

Kelemahan dari metode ini adalah untuk ukuran plainteks yang sangat besar sulit mendapatkan tiga buah kunci yang cukup pendek dengan tetap memenuhi syarat kedua bahwa kunci yang digunakan merupakan bilangan atau angka acak. Dalam hal ini diperlukan saluran komunikasi untuk mengirim kuncinya. Seperti yang telah dibahas bahwa saluran komunikasi tidak aman dan tidak dapat dipercaya.

DAFTAR PUSTAKA

Ariyus, Dony. 2008. Pengantar Ilmu Kriptografi. Yogyakarta : CV Andi Offset.

Febi Trafena T. 2016. *MANFAAT INTERNET SEBAGAI MEDIA KOMUNIKASI BAGI REMAJA DI DESA AIR MANGGA KECAMATAN LAIWUI KABUPATEN HALMAHERA SELATAN*. e-journal "Acta Diurna" Volume V. No.1. Tahun 2016.

Maureen Linda C. 2011. Metode Enkripsi Baru : Triple Transposition Vigenere Cipher. Makalah IF3058 Kriptografi – Sem. II Tahun 2010/2011.

Munir, Rinaldi. Kriptografi. Bandung : Informatika Bandung. Yurika Permanasari. 2017. *KRIPTOGRAFI KLASIK MONOALPHABETIC* . Jurnal Matematika Vol. 16, No. 1, Mei 2017.