MODIFIKASI CAESAR CIPHER DENGAN PERMUTASI, TRANSPOSISI, BINARY, GERBANG LOGIKA, ASCII DAN HEXA

Akhmad Syarif

Magister Teknik Informatika Universitas AMIKOM Yogyakarta
Jl. Ring Road Utara. Condong Catur, Sleman, Yogyakarta
akhmad.syarif@students.amikom.ac.id

Abstract - Cryptography is the art of securing and keeping text or message from other people except those who receive it. Caesar Cipher algorithm is a classic algorithm that is vulnerable to hacker attacks by the brute force method. Caesar Cipher with 7 methods, the first is a transposition, the second is a permutation, the third is binary converting, the fourth is logistic gate calculation, the sixth is converting ASCII and the seventh is converting Hexa. With seven combinations of these methods, it can improve Caesar's algorithm Cipher from hacker attacks and add variations to the modification of Caesar Cipher in classical encryption. Making ciphertext very complex and to overcome so many possibilities that must be tried.
Keywords - Caesar Cipher, Modification, Convert, Transposition.

Abstrak - Kriptografi adalah seni dalam mengamankan dan merahasiakan suatu teks atau pesan dari orang lain kecuali yang menerima. Algoritma Caesar Cipher adalah algoritma klasik yang rentan akan serangan hacker dengan metode brute force. Pada penelitian ini dilakukan memodifikasi algoritma Caesar Cipher dengan 7 metode yaitu pertama adalah tranposisi, ke-dua permutasi, ke-tiga convert biner, ke-empat perhitungan gerbang logika, ke-enam convert ASCII dan ke-tujuh convert hexa. Dengan tujuh kombinasi metode ini harapan bisa memperkuat algoritma Caesar Cipher dari serangan hacker dan menambah variasi modifikasi dari Caesar Cipher dalam enkripsi klasik. Menjadikan ciphertext sangat komplek dan untuk mengatasinya begitu banyak kemungkinan yang harus dicoba.
Kata Kunci - Caesar Cipher, Modifikasi, Mengubah, Transposisi.

I. PENDAHULUAN

Saat ini pertukaran data dalam bentuk pesan atau teks secara digital melalui jaringan internet secara publik telah banyak dilakukan. Sehingga salah satu permasalahan yang terjadi dari hal tersebut adalah keamanan teks yang dikirimkan ataupun yang diterima[1].

Kriptografi adalah ilmu merancang metode yang memungkinkan informasi dikirim dalam bentuk yang aman sedemikian rupa cara satu-satunya orang yang dapat mengambil informasi ini penerima yang dimaksud [2]. Awalnya kriptografi dulu dilakukan dengan teknik manual. Kerangka dasar melakukan kriptografi tetaplah sama pada dulu hingga banyak dilakukan sampai sekarang ke kriptografi modern. Ada 2 cara dalam menyembunyikan informasi yaitu kriptografi dan steganografi. Kriptografi terdiri dari 2 bagian, yaitu enkripsi dan dekripsi [3]. Enkripsi adalah proses mengubah teks biasa (plaintext) menjadi teks yang acak (chipertext) [3]. Dekripsi adalah mengubah teks acak (ciphertext) menjadi teks biasa (plaintext) [3]. Algoritma kriptografi dibagi menjadi 2 bagian yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik adalah algoritma yang pada umumnya digunakan pada jaman dulu dengan hanya menggunakan metode subtitusi dan permutasi [4]. Sedangkan kriptografi modern adalah algoritma yang digunakan pada jaman sekarang. Hasil dari pengembangan kriptografi klasik dimana didalam prosesnya ditambahkan penggunaan biner, hexa dll.

Caesar Cipher adalah algoritma klasik substitusi terlama bahkan tertua yang terkenal sampai sekarang. Caesar cipher tidak memiliki kunci dalam algoritma enkripsinya dimana keamanan dari algoritma tersebut terletak pada kerahasiaan algoritmanya itu sendiri. Seiring dengan waktu algoritma ini semakin ditinggal oleh zaman sekarang dikarenakan dianggap kurang aman. Oleh karena itu diperlukan untuk memodifikasi dengan beberapa metode dari algoritma klasik lainnya seperti tranposisi dan lainya untuk meningkatkan dan memberikan kekuatan lebih pada hasil enkripsi agar kesulitian dalam teknik brute force [5]. Pada umum nya enkripsi dan dekripsi pada Caesar Cipher adalah [1] :

Enkripsi :

$$E(x) = x + K \bmod 26 \qquad (1)$$

Dekirpsi :

$$D(x) = x - K \bmod 26 \qquad (2)$$

Dimana K adalah nilai kunci yang digunakan untuk menggeser setiap karakter x.

Misal dengan mengkodekan setiap huruf alfabet dengan sebuah angka integer: A = 0, B = 1, C = 2, D = 3, E = 4, F = 5, G = 6, H = 7, I = 8, J = 9, K = 10, L = 11, M = 12, N = 13, O = 14, P = 15, Q = 16, R = 17, S = 18, T = 19, U = 20, V = 21, W = 22, X = 23, Y = 24, Z = 25. Pergesaran 2 huruf alfabet di dalam Caesar Cipher dengan melakukan penjumlahan plainteks

(p) dengan 2 dalam modulus 26 atau dalam bentuk kesamaan [6]:

$$E(p) = p + 2 \, mod \, 26 \quad (3)$$

Untuk melakukan dekripsi dengan operasi kebalikan dari enkripsi, dengan pengurangan cipherteks (c) dengan 3 dalam modulus 26 :

$$E(c) = c - 2 \, mod \, 26 \quad (4)$$

Dimana :

p = plaintext

c = chipertext

Algoritma Caesar Cipher adalah algoritma yang melakukan pergantian posisi huruf awal dengan alphabet atau disebut dengan ROT3. Algoritma transposisi adalah dengan cara mengubah letak dari teks pesan yang disandikangn dengan menggunakan pola tertentu [7].

Algoritma SPICA-XB adalah algoritma yang menggabungkan sifat algoritma kriptografi Caesar Cipher dengan beberapa sifat dari algoritma kriptografi modern [8].

Priya Verma dan teman-teman dengan judul Modified Caesar Cipher using Rectangular Method For Enhanced Security. Mereka melakukan modifikasi kriptografi Caesar Cipher dengan metode rectangular. Mereka memberikan nama kepada teknik yang mereka rancang dengan nama MCC. Teknik MCC menggunakan subtitusi dan tranposisi pada teks biasa dan menggunakan 2 kunci berbeda untuk enkripsi sehingga membuat lebih kuat dan aman.

Galih Fathul Rohmi dan teman-teman dengan judul Implementasi Algoritma Cipher Ceasar untuk Enkripsi dan Dekripsi pada Tabel ASCII menggunakan Bahasa Java. Mereka melakukan modifikasi pada kriptografi dengan menambahkan tabel ASCII untuk memperkuat hasil enkripsi dengan menggunakan bahasa JAVA.

Fahrul Ikhsan Lubis dan teman-teman dengan judul Combination of Caesar Cipher Modification with Transposition Cipher. Mereka melakukan modifikasi pada kriptografi Caesar Cipher dengan penambahan transposisi sehingga terdapat 3x proses enkripsi yang mengharuskan cryptanalis harus menemukan algoritma yang digunakan, karakter yang ditambahkan, bagian yang tidak terenkripsi dan mencari kunci yang digunakan.

Penelitian ini betujuan untuk memperkuat kriptografi pada Ceasar Cipher dengan beberapa tambahan metode dari algoritma klasik lainnya sehingga kriptografi Caesar Cipher menjadi lebih kuat dan lebih sulit untuk dipecah dari pada kriptografi Caesar Cipher klasik. Yang membedakan dari penelitian terdahulu diatas adalah metode yang digunakan peneliti menggunakan 7 metode algoritma dengan permutasi, tranposisi, binary, perhitungan gerbang logika dan juga vonversi ke ASCII dan hexa. Salah satu metode yang sering digunakan yaitu perubahan ASCII ke dalam biner untuk enkripsi dan sebaliknya untuk dekripsi [9]. Sehingga mempersulit bagi cryptanalis dalam memecahkan kriptografi ini.

II. METODE PENELITIAN

Dalam perkembangan ilmu kriptografi semakin luas dan banyak sekali dimanfaatkan terutama dalam mengamankan informasi.

Pada kasus ini untuk algoritma klasik Cipher Caesar sendiri diterapkan pada aspek transposisi huruf dengan huruf yang diacak. Dilanjutkan dengan conversi ke biner lalu subtitusi gerbang logika yang dilakukan 4 kali dan dilanjutkan substitusi tabel ASCII dan Hexa pada huruf tertentu.

Langkah enkripsi pada implementasi di program ini adalah memasukan plaintext dan kunci sesuai keinginan dengan banyak kunci 2. Misal kunci HALO dan kunci GUNUNG MERAPI. Pertama hapus huruf yang terlihat *double* sehingga terlihat hanya ada 1 huruf saja dalam deretan tersebut. Dalam kunci HALO akan tetap menjadi HALO karena dari deretan tersebut tidak terdapat huruf double atau perulangan huruf sehingga tidak ada perubahaan. Jika pada kunci GUNUNG MERAPI terdapat beberapa huruf double yaitu U, N, G sehingga menjadi GUNMERAPI, disini juga akan dihapus spasi yang ada sehingga menjadi 1 kata saja.

Lalu dilakukan tranposisi huruf pada kunci dengan table 1 dibawah ini, dengan memasukan huruf pada kunci diawal box, dan dilanjutkan huruf alpabet dari Z sampai A dimana huruf tidak boleh ada yang double.

Tabel 1. Tabel Transposisi 1 kunci HALO

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
H	A	L	O	Z	Y	X	W	V	U	T	S	R	Q	P	N	M	K	J	I	G	F	E	D	C	B

Pada kunci ke 2 juga sama seperti transposisi kunci ke 1. Bisa dilihat pada table 2 dibawah ini :

Tabel 2. Tabel Transposisi 1 kunci GUNUNG MERAPI

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
G	U	N	M	E	R	A	P	I	Z	Y	X	W	V	T	S	Q	O	L	K	J	H	F	D	C	Z

Dilanjutkan dengan mengubah kalimat plaintext menjadi satu kata yaitu mengganti space dengan tanda simbol underscore (_). Dengan plaintext adalah SAYA MAU MAKAN KETEMPAT YANG JAUH DARI KOTA. Menjadi SAYA_MAU_MAKAN_KETEMPAT_YANG_JAU H_DARI_KOTA.

Lalu dilanjutkan tranposisi plaintext dengan table tranposisi kunci yang telah dibuat sebelumnya. Dengan urutan huruf 1 dari plaintext ditransposisi dengan hasil transposisi kunci 1, urutan huruf 2 dari plaintext ditransposisi dengan hasil transposisi kunci 2, urutan huruf 3 dari plaintext ditransposisi dengan hasil transposisi 1 dan diulang terus urutannya dari kunci 1, kunci 2 dan balik lagi ke kunci 1 sampai huruf terakhir plaintext. Trnaposisi pada plaintext bisa dilihat pada tabel 3 dibawah ini :

Tabel 3. Tabel Transposisi plaintext

K1	K2	K1	K2	K1	K2	K1	K2	K1	K2	K1	K2	K1	K2	K1	K2	K1
K	E	T	I	K	A	C	O	R	O	N	A	D	A	T	A	N
T	E	G	I	T	G	L	T	J	T	Q	G	O	G	G	G	Q

Tabel 4. Tabel LanjutanTransposisi plaintext

K2	K1	K2	K1	K2	K1	K2	K1	K2	K1	K2	K1	K2	K1	K2	K1	K2
G	E	N	G	K	A	U	D	I	P	A	K	S	A	M	E	N
A	Z	V	X	Y	H	J	O	I	M	G	T	L	H	W	Z	V

Tabel 5. Tabel Lanjutan Transposisi plaintext

K1	K2	K1	K2	K1	K2	K1	K2	K1
C	A	R	I	T	U	H	A	N
L	G	J	I	G	J	W	G	Q

Maka akan menjadi IGBG_RGF_WHYHV_TEGERSHK_BGQA_UGFP_OGJI_TTGG.

Selanjutnya hasil dari transposisi plaintext tadi didapatkan hasil ciphertext pertama yang akan dilanjutkan dengan permutasi, yang mana huruf urutan genap pada hasil ciphertext pertama akan di mutasi ke angka sesuai tabel 4 dibawah ini.

Tabel 6. Tabel Mutasi Hasil Ciphertext 1

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Maka hasilnya adalah I7B7_18G6_23H25H22_20E7E18S8K_B7Q1_21G6P_O7J9_20T7G.

Lalu dilanjutkan dengan conversi kunci 1, kunci 2 dan hasil mutasi ciphertext 1 kedalam bentuk biner. Untuk conversi ASCII ke Biner bisa dilihat pada gambar 1 dibawah ini.

Oct	Dec	Hex	Char	Oct	Dec	Hex	Char	Oct	Dec	Hex	Char	Oct	Dec	Hex	Char
000	0	00	NUL	040	32	20	SPACE	100	64	40	@	140	96	60	`
001	1	01	SOH	041	33	21	!	101	65	41	A	141	97	61	a
002	2	02	STX	042	34	22	"	102	66	42	B	142	98	62	b
003	3	03	ETX	043	35	23	#	103	67	43	C	143	99	63	c
004	4	04	EOT	044	36	24	$	104	68	44	D	144	100	64	d
005	5	05	ENQ	045	37	25	%	105	69	45	E	145	101	65	e
006	6	06	ACK	046	38	26	&	106	70	46	F	146	102	66	f
007	7	07	BEL	047	39	27	'	107	71	47	G	147	103	67	g
010	8	08	BS	050	40	28	(	110	72	48	H	150	104	68	h
011	9	09	HT	051	41	29	)	111	73	49	I	151	105	69	i
012	10	0A	LF	052	42	2A	*	112	74	4A	J	152	106	6A	j
013	11	0B	VT	053	43	2B	+	113	75	4B	K	153	107	6B	k
014	12	0C	FF	054	44	2C	,	114	76	4C	L	154	108	6C	l
015	13	0D	CR	055	45	2D	-	115	77	4D	M	155	109	6D	m
016	14	0E	SO	056	46	2E	.	116	78	4E	N	156	110	6E	n
017	15	0F	SI	057	47	2F	/	117	79	4F	O	157	111	6F	o
020	16	10	DLE	060	48	30	0	120	80	50	P	160	112	70	p
021	17	11	DC1	061	49	31	1	121	81	51	Q	161	113	71	q
022	18	12	DC2	062	50	32	2	122	82	52	R	162	114	72	r
023	19	13	DC3	063	51	33	3	123	83	53	S	163	115	73	s
024	20	14	DC4	064	52	34	4	124	84	54	T	164	116	74	t
025	21	15	NAK	065	53	35	5	125	85	55	U	165	117	75	u
026	22	16	SYN	066	54	36	6	126	86	56	V	166	118	76	v
027	23	17	ETB	067	55	37	7	127	87	57	W	167	119	77	w
030	24	18	CAN	070	56	38	8	130	88	58	X	170	120	78	x
031	25	19	EM	071	57	39	9	131	89	59	Y	171	121	79	y
032	26	1A	SUB	072	58	3A	:	132	90	5A	Z	172	122	7A	z
033	27	1B	ESC	073	59	3B	;	133	91	5B	[	173	123	7B	{
034	28	1C	FS	074	60	3C	<	134	92	5C	\	174	124	7C	|
035	29	1D	GS	075	61	3D	=	135	93	5D	]	175	125	7D	}
036	30	1E	RS	076	62	3E	>	136	94	5E	^	176	126	7E	~
037	31	1F	US	077	63	3F	?	137	95	5F	_	177	127	7F	DEL

Gambar 1. Tabel Decimal-Binary-Octal-Hex-ASCII

Maka untuk conversi kunci 1 adalah :

H = 01001100
A = 01000001
L = 01001100
O = 01001111

Untuk conversi binary kunci 2 adalah :

G = 01000111
U = 01010101
N = 01001110
M = 01001101
E = 01000101
R = 01010010
A = 01000001
P = 01010000
I = 01001001

Dan untuk conversi binary dari plaintext yang telah menjadi chipertext 1 tadi adalah :

I = 01001001
7 = 00000111
B = 01000010

7 = 00000111
_ = 01011111
18 = 00010010
G = 01000111
6 = 00000110
_ = 01011111
23 = 00010111
H = 01001000
25 = 00011001
H = 01001000
22 = 00010110
_ = 01011111
20 = 00010100
E = 01000101
7 = 00000111
E = 01000101
18 = 00010010
S = 01010011
8 = 00001000
K = 01001011
_ = 00000000
B = 01000010
7 = 00000111
Q = 01010001
1 = 00000001
_ = 01011111
21 = 00010101
G = 01000111
6 = 00000110
P = 01010000
_ = 00000000
O = 01001111
7 = 00000111
J = 01001010
9 = 00001001
_ = 01011111
20 = 00010100
T = 01010100
7 = 00000111
G = 01000111

Setelah dilakukan konversi ke biner. Pada kunci 1 dan 2 setiap kuruf dilakukan perhitungan gerbang logika XOR. Pada kunci 1 untuk perhitungan XOR sebagai berikut :

H = 01001100
A = 01000001
L = 01001100
O = 01001111

Akan menghasilkan XOR = 00001010. Pada kunci 2 untuk perhitungan XOR sebagai berikut :

G = 01000111
U = 01010101
N = 01001110
M = 01001101
E = 01000101
R = 01010010
A = 01000001
P = 01010000
I = 01001001

Akan menghasilkan XOR = 01011110.

Setelah didapat 1 deretan biner 8 bit disetiap kunci maka kunci 1 dan kunci 2 hasil dari perhitungan XOR pada setiap kunci dilakukan perhitungan gerbang logika OR.

Kunci 1 = 00001010
Kunci 2 = 00001010

Akan mengahasilkan OR = 01011110.

Selanjutnya hasil konversi dari ciphertext 1 dilakukan perhitungan XNOR terhadap hasil dari OR diatas. Didapatkan hasil nya adalah

11101000 10100110 11100011 10100110 11111110 10110011 11100110 10100111 11111110 10110110 11101001 10111000 11101001 10110111 11111110 10110101 11100100 10100110 11100100 10110011 11110010 10101001 11101010 10100001 11100011 10100110 11110000 10100000 11111110 10110100 11100110 10100111 11110001 10100001 11101110 10100110 11101011 10101000 11111110 10110101 11110101 10100110 11100110

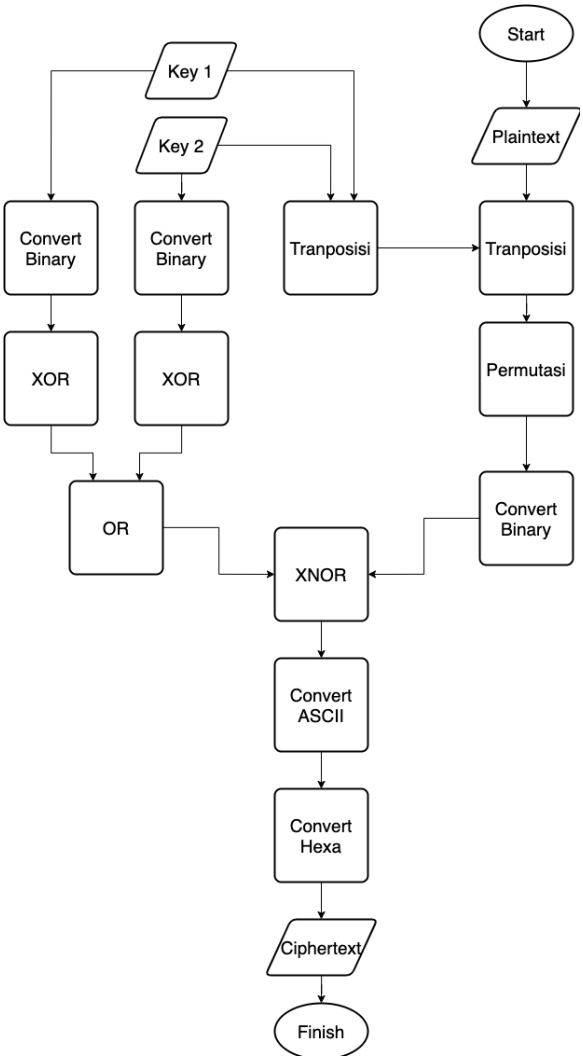
Setelah didapat hasil XNOR dilakukan perubahan pada huruf pertama biner disetiap huruf ciphertext 1 menjadi angka 0 seperti dibawah ini.

01101000 00100110 01100011 00100110 01111110 00110011 01100110 00100111 01111110 00110110 01101001 00111000 01101001 00110111 01111110 00110101 01100100 00100110 01100100 00110011 01110010 00101001 01101010 00100001 01100011 00100110 01110000 00100000 01111110 00110100 01100110 00100111 01110001 00100001 01101110 00100110 01101011 00101000 01111110 00110101 01110101 00100110 01100110

Selanjutnya dari perhitungan gerbang logika XNOR dilakukan konversi ke ASCII, maka akan menjadi seperti ini : h&c&~3f'~6i8i7~5d&d3r)j!c&p ~4f'q!n&k(~5u&f

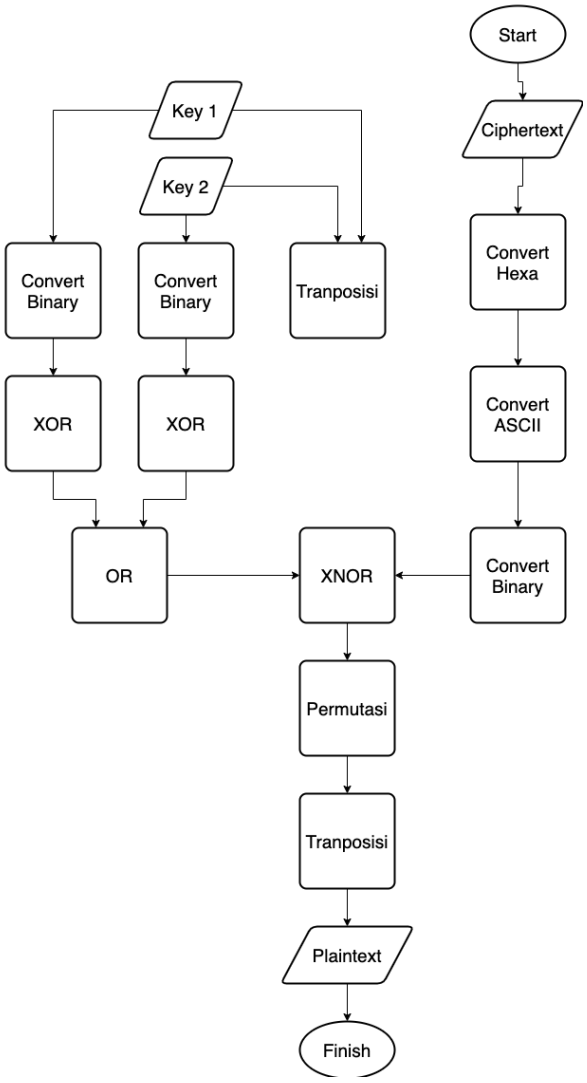
Dilanjutkan dengan conversi ke HEXA yang mana konversi ke HEXA adalah pada urutan ganjil saja pada hasil ASCII tadi. Maka akan seperti ini : 68&63&7e366'7e66986977e564&64372)6a!63&70 7e466'71!6e&6b(7e575&66. Itulah hasil akhir dari ciphertext pada kriptografi ini.

Alur enkripsi dari metode ini ada pada gambar dibawah ini :



Gambar 2. Tabel Alur Enkripsi

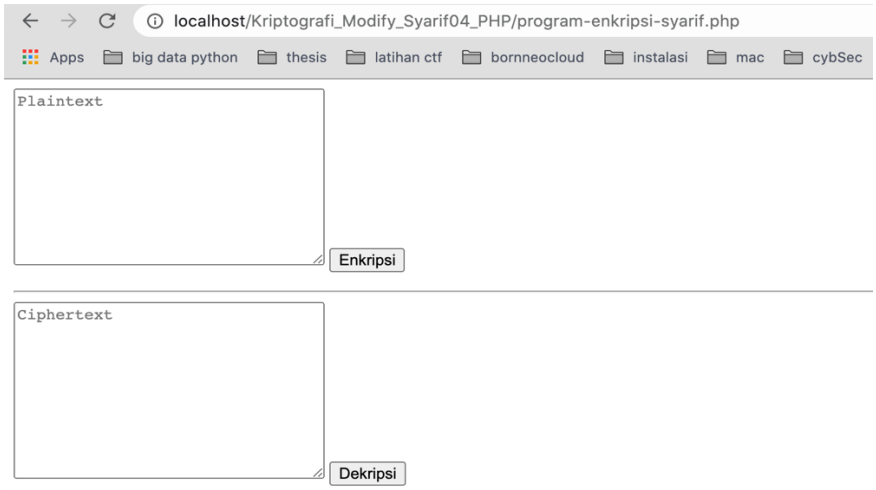
Pada dekripsi dilakukan hal sama seperti enkripsi akan tetapi dengan alur terbalik dari enkripsi diatas tadi. Berikut gambar dari alur proses dekripsi kriptografi ini pada gambar 3 dibawah ini :



Gambar 3. Tabel Alur Dekripsi

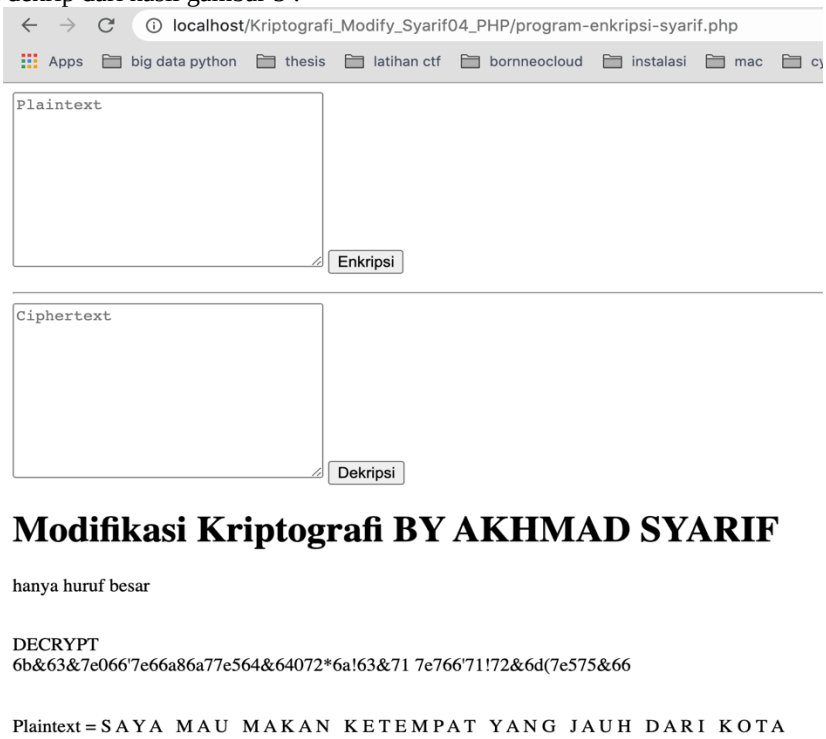
III.HASIL DAN PEMBAHASAN

Penulis menggunakan bahasa program PHP dalam pembuatan program algoritma modifikasi Caesar Cipher. Pada program ini terdapat beberapa fungsi 3 button dan 3 input yaitu button enkripsi, button dekripsi, button proses dan pada input yaitu input plaintext untuk enkripsi dan input ciphertext untuk decript. Berikut hasil data pengujian dari implementasi pada program PHP dengan percobaan enkripsi pada plaintext SAYA MAU MAKAN KETEMPAT YANG JAUH DARI KOTA pada gambar 4 :



Gambar 4. Gambar hasil aplikasi enkripsi pada kriptografi ini

Dan berikut ini juga hasil dari implementasi modifikasi algoritma Caesar Cipher pada program PHP dengan percobaan dekrip dari hasil gambar 5 :



Gambar 5. Gambar hasil aplikasi dekripsi pada kriptografi ini

Kekurangan dari algoritma ini adalah tidak bisa enkripsi dari huruf kecil dan juga pada kunci yang masih static dari koding menggunakan 2 kunci.

Dari hasil program diatas dapat disimpulkan bahwa algoritma Caesar Cipher yang telah dimodifikasi menggunakan metode yang telah dibahas pada metode penelitian dengan beberapa campuran metode algoritma yang ada pada algoritma kriptografi medern dapat dilakukan dan juga dapat memperkuat kriptografi Caesar Cipher itu sendiri.

IV. KESIMPULAN

Dalam pengimplementasian algoritma klasik Caesar Cipher yang telah dimodifikasi dengan beberapa tambahan menggunakan tranposisi, permutasi, conversi Biner, ASCII dan Hexa dan juga perhitungan gerbang logika sebagai acuan untuk memungkinkan lebih banyak karakter dan memperkuat ekripsi ini sendiri. Dengan ini setidaknya akan menambah daftar algoritma modifikasi pada Caesar Cipher yang digunakan untuk menghindari kerahasiaan informasi diketahui selain penerima. Penggunaan 2 kunci dilakukan pada enkripsi ini. Adanya penggabungan beberapa metode mutasi, tranposisi, conversi (biner, ASCII, Hexa) yang mana membuat algoritma Chiper Caesar akan lebih kuat dan aman sehingga tidak mudah bagi hacker untuk mencoba untuk menyerang atau menemukan plaintext tersebut.

DAFTAR PUSTAKA

[1] R. Latifah, S. N. Ambo, and S. I. Kurnia, "Modifikasi Algoritma Caesar Chiper dan Rail Fence untuk Peningkatan Keamanan Teks Alfanumerik dan Karakter Khusus," *Semin. Nas. Sains dan Teknol.*, no. 1-2 November, pp. 1–7, 2017.

[2] B. Purnama and A. H. H. Rohayani, "A New Modified Caesar Cipher Cryptography Method with LegibleCiphertext from a Message to Be Encrypted," *Procedia Comput. Sci.*, vol. 59, pp. 195–204, 2015.

[3] G. F. Rohmi, "IMPLEMENTASI ALGORITMA CHIPER CAESAR UNTUK ENKRIPSI DAN DEKRIPSI PADA TABEL ASCII MENGGUNKAN BAHASA JAVA," *ResearchGate*, 2016.

[4] F. I. Lubis, H. F. S. Simbolon, T. P. Batubara, and R. W. Sembiring, "Combination of caesar cipher modification with transposition cipher," *Adv. Sci. Technol. Eng. Syst.*, vol. 2, no. 5, pp. 22–25, 2017.

[5] P. Verma, G. Singh Gaba, and H. Monga, "Modified Caesar Cipher Using Rectangular Method for Enhanced Security," *J. Commun. Technol. Electron. Comput. Sci.*, vol. 8, 2016.

[6] R. Munir, *Kriptografi Edisi Kedua*. Bandung: Informatika, 2019.

[7] I. Gunawan, "Kombinasi Algoritma Caesar Cipher dan Algoritma RSA untuk pengamanan File Dokumen dan Pesan Teks," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 2, no. 2, pp. 124–129, 2018.

[8] R. P. Islami, "Modifikasi Algoritma Caesar Cipher Menjadi SPICA-XB (Spinning Caesar dengan XOR Binary)," *J. Mantik*, vol. 3.

[9] N. S. B. Sembiring, "Perancangan Aplikasi Kriptografi dengan Metode Modifikasi Caesar Cipher yang Diperkuat dengan Vernam Cipher untuk Keamanan Teks," *e-jurnal JUSITI*, vol. 5, 2016.