MODIFIKASI METODE HILL CHIPER MENGGUNAKAN FUNGSI HIMPUNAN FUZZY DAN KODE ASCII

Noviyanti. P, Dony Ariyus

Magister Teknik Informatika, Universitas AMIKOM Yogyakarta
Jl. Ring Road Utara, Ngringin, Condongcatur, Kec. Depok, Kab. Sleman Yogakarta 55281
noviyanti.p@students.amikom.ac.id, dony.a@amikom.ac.id

Abstract - Maintaining the confidentiality of a message is important to do so that it can keep the message reaching a person or organization safely without being noticed by an irresponsible person. There are several methods used to maintain the security or confidentiality of a message commonly referred to as cryptography, one of which is the Hill Chiper method. The Hill Chiper method is a type of symmetric method or algorithm. The research carried out aims to make modifications to the method with symmetric algorithms, namely Hill Chiper. By doing the modification it is hoped that the cryptanalysis will not easily open a ciphertext and this modification also aims to provide better message security and have a more varied plaintext. Modifications made are by combining the matrix with the fuzzy set function and the ASCII code. The encryption process produces a matrix and symbols according to the number of plaintexts entered. While the decryption process is done by entering the ciphertext matrix, initial key and ciphertext symbols obtained from the encryption process so that the plaintext is returned. In this study using MatLab. Plaintext can be in the form of uppercase, lowercase letters, numbers, and some of the symbols contained in the ASCII code.
Keywords - Hill Chiper Modification, Fuzzy Set Function, Cryptography, and ASCII Code.

Abstrak - Menjaga kerahasiaan sebuah pesan penting untuk dilakukan agar dapat menjaga pesan sampai pada seseorang atau organisasi dengan aman tanpa diketahui oleh orang yang tidak bertanggung jawab. Terdapat beberapa metode yang digunakan untuk menjaga keamanan atau kerahasiaan sebuah pesan yang biasa disebut juga dengan kriptografi, salah satunya adalah metode Hill Chiper. Metode Hill Chiper merupakan salah satu jenis metode atau algoritma simetris. Penelitian yang dilakukan bertujuan untuk melakukan modifikasi terhadap metode dengan algoritma simetris, yaitu Hill Chiper. Dengan dilakukannya modifikasi diharapkan agar para kriptanalisis tidak mudah membuka sebuah chiperteks dan modifikasi ini juga bertujuan untuk memberikan keamanan pesan agar lebih baik dan memiliki plainteks yang lebih bervariasi pula. Modifikasi yang dilakukan adalah dengan melakukan kombinasi antara matriks dengan fungsi himpunan fuzzy dan kode ASCII. Proses enkripsi menghasilkan matriks dan simbol sesuai dengan jumlah plainteks yang dimasukkan. Sedangkan proses dekripsi dilakukan dengan memasukkan matriks chiperteks, kunci awal dan simbol chiperteks yang diperoleh dari proses enkripsi sehingga dihasilkan plainteks kembali. Pada penelitian ini menggunakan MatLab. Plainteks dapat berupa huruf besar, huruf kecil, angka, dan beberapa simbol yang terdapat pada kode ASCII.
Kata Kunci - Modifikasi Hill Chiper, Fungsi Himpunan Fuzzy, Kriptografi, dan Kode ASCII.

I. PENDAHULUAN

Perkembangan teknologi saat ini memberikan pro dan kontra. Pro, bahwa dengan adanya teknologi pekerjaan mejadi lebih mudah, informasi juga lebih mudah untuk diakses dan didapatkan, sedangkan kontra, teknologi kurang terjamin keamanannya.

Keamanan yang dimaksud dapat berupa keamanan data. Dalam mengamankan sebuah data pada dasarnya dapat memanfaatkan salah satu ilmu menyembunyikan pesan, yaitu kriptografi. Kriptografi dapat digunakan untuk menyandikan sebuah pesan dan hanya orang yang bersangkuan yang dapat membuka pesan tersebut, sehingga hanya orang tersebut pula yang dapat membuka data yang mungkin dirahasiakan dan dapat dibuka dengan menggunakan pesan rahasia tersebut.

Pada penelitian yang dilakukan ini bertujuan untuk memberikan keamanan dalam merahasiakan sebuah pesan. Dengan melakukan modifikasi terhadap metode Hill Chiper menggunakan Fungsi Himpunan Fuzzy dan Kode ASCII agar kriptanalisis tidak mudah membuka sebuah chiperteks dan dan modifikasi ini juga bertujuan untuk memberikan keamanan pesan agar lebih baik dan memiliki plainteks yang lebih bervariasi pula. Hasil enkripsi yang diperoleh pada penelitian ini berupa matriks dan simbol chiperteks dan untuk proses dekripsi, matriks chiperteks, kunci awal, dan simbol chiperteks yang diperoleh pada proses enkripsi digunakan untuk proses dekripsi agar dapat menghasilkan plainteks kembali.

A. Kriptografi

Kriptografi merupakan suatu ilmu atau sebuah kecerdasan untuk menjaga kerahasiaansebuah pesan yang ditampilkan dalam bentuk kode-kode yang tidak dapat dimengerti oleh orang lain. Kriptografi berasal dari 2 kata dalam Bahasa Yunani, yaitu *crypto* dan

graphia. *Crypto* memiliki arti rahasia dan *graphia* memiliki arti tulisan sehingga kriptografi secara umum merupakan tulisan yang dirahasiakan [1]. Adapun konsep dasar dari kriptografi adalah memiliki proses enkripsi dan dekripsi. Enkripsi dilakukan untuk menghasilkan chipertets dan dekripsi digunakan untuk memperoleh plainteks kembali.

Kriptografi pada dasarnya telah digunakan sejak dari abad sebelum masehi. Orang-orang jaman dulu menyampaikan pesan rahasia dengan menggunakan beberapa cara, seperti menggunakan simbol, gambar yang dituliskan pada batu. Seiiring berjalannya waktu para ilmuan menemukan kertas sehingga kertas sebagai media untuk membuat tulisan dan akhirnya menemukan komputer yang hingga sekarang menjadi salah satu alat untuk dapat digunakan sebagai bagian dari proses melakukan kriptografi dengan menggunakan berbagai macam algoritma.

B. Metode Hill Chiper

Seiiring dengan perkembangan zaman, telah banyak modifikasi yang dilakukan terhadap algoritma untuk menjaga kerahasiaan sebuah pesan. Modifikasi sebuah metode dilakukan bertujuan agar terdapat algoritma yang dapat menjaga kerahasiaan pesan dengan lebih aman dan lebih bervariasi. Salah satu metode yang dapat dimodifikasi adalah metode Hill Chiper. Hill cipher merupakan algoritma simetris yang termasuk pada algoritma klasik dan hill cipher merupakan salah satu metode dari cipher subsitusi dengan perkalian matriks [2].

Terdapat beberapa penelitian yang dijadikan acuan dilakukannya penelitian ini. Penelitian yang dilakukan oleh [2], pada penelitian tersebut melakukan modifikasi algoritma Hill Chiper dan *twofish* menggunakan kode wilayah telepon. Penelitian yang dilakukan bertujuan untuk memodifikasi metode Hill Chiper agar dapat membuat sebuah chiperteks yang sulit untuk dipecahkan oleh kriptanalisis. Peneliti melakukan modifikasi dengan mengkombinasikan algoritma Hill Chiper dengan kode wilayah kemudian melakukan enkripsi dengan menggunakan metode *Twofish*. Hasil enkripsi yang diperoleh pada penelitian ini berupa *file* yang dapat diakses menggunakan *notepad*. Skenario pengujian dilakukan dengan menggunakan beberapa jenis *file* yang memiliki ukuran data yang berbeda kemudian membandingkan tiap *file* tersebut dari segi kecepatan dalam melakukan proses enkripsi dan dekripsi. *File* dengan ukuran yang lebih besar akan memiliki proses enkripsi dan dekripsi yang lebih lama.

Penelitian yang dilakukan oleh [3], pada penelitian tersebut melakukan modifikasi metode Hill Chiper dengan kunci matriks persegi panjang menggunakan fungsi Xor dan fungsi Xnor. Pada penelitian tersebut dilakukan modifikasi terhadap algoritma Hill Cipher dengan menggunakan *pseudoinvers* dan operasi biner Xor dan Xnor. Langkah pertama yang dilakukan pada penelitian ini adalah inisialisasi Hill Cipher dengan *pseudoinvers*, karena apabila matriks kunci tidak memiliki *pseudoinvers* maka matriks kunci tidak dapat digunakan untuk proses dekripsi. Modifikasi terhadap algoritma hill cipher dengan menggunakan *pseudoinvers* pada penelitian tersebut dilakukan pada proses enkripsi dan dekripsi dan selanjutnya dilakukan penambahan berupa operasi biner Xor dan Xnor.

Penelitian yang dilakukan oleh [4], pada penelitian tersebut melakukan modifikasi metode Hill Chiper dengan matriks sirkulan. Matriks sirkulan pada metode ini digunakan untuk membangkitkan kunci publik dan memperoleh kunci privat, sehingga menghasilkan kunci asimetris dari sebelumnya kunci simetris. Kunci yang diperoleh digunakan untuk proses enkripsi dan menghasilkan chiperteks dan selanjuntya digunakan untuk proses dekripsi dan menghasilkan plainteks kembali.

Penelitian yang dilakukan oleh [5], pada penelitian tersebut dilakukan modifikasi matriks kunci Hill Chiper menggunakan algoritma genetika. Pada penelitian tersebut kunci yang akan digunakan pada proses enkripsi dan dekripsi dihasilkan menggunakan bantuan algoritma genetika. Matriks yang digunakan pada penelitian tersebut adalah matriks 3x3. Pada penelitian tersebut, untuk memperoleh kunci matriks Hill Chiper menggunakan algoritma genetika yang bertujuan untuk mempersingkat waktu dan memudahkan untuk memperoleh kunci yang dapat diaplikasi pada enkripsi dan dekripsi berdasarkan pada nilai *fitness* yang diperoleh pada algoritma genetika.

Penelitian yang dilakukan oleh [6], pada penelitian tersebut menjelaskan bahwa aplikasi kriptografi memainkan peran penting dalam kehidupan sehari-hari, seperti mengirim email, bertukar informasi transaksi rekening bank, komunikasi seluler dan transaksi kartu ATM. Untuk mengamankan informasi dari pengguna yang tidak sah, Hill Cipher adalah salah satu *cryptosystem* simetris yang paling terkenal. Modifikasi Hill Chiper pada penelitian ini dilakukan dengan proses enkripsi dan dekripsi yang didasarkan pada transposisi, substitusi, dan pergeseran kiri-kanan. Modifikasi yang dilakukan dapat memberikan hasil yang optimal dan hasilnya memberikan *throughput* yang lebih baik untuk ukuran *file* jenis apa pun jika dibandingkan dengan algoritma yang sebenarnya.

Penelitian yang dilakukan oleh [7], pada penelitian tersebut dilakukan modifikasi dengan menggunakan *convert between base*. Menurut penelitian [7], menggunakan matriks pada umumnya yang terdapat pada metode Hill Chiper dapat dipecahkan oleh kriptanalisis, sehingga dengan adanya modifikasi dapat membantu memberikan keamanan data yang lebih baik.

C. Himpunan Fuzzy

Himpunan fuzzy merupakan teori yang didasarkan oleh fungsi keanggotaan dan dinyatakan dalam bentuk derajat keanggotaan [8]. Pada penelitian ini fungsi

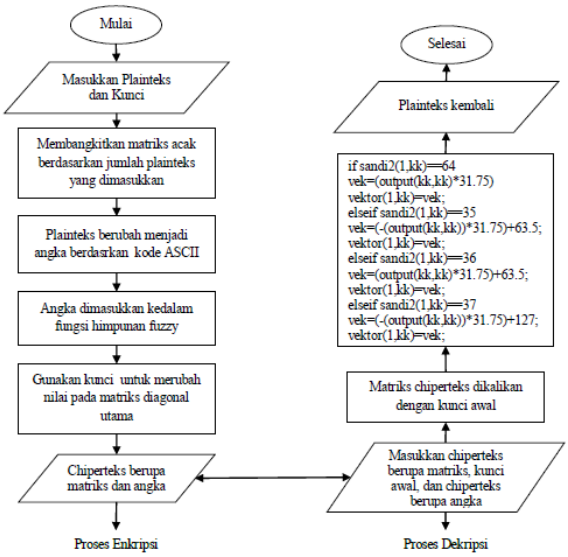
himpunan fuzzy menghasilkan derajat keanggotaan yang diperoleh berdasarkan plainteks yang dimasukkan dengan mengacu pada kode ASCII.

D. MatLab

Pada penelitian ini menggunakan *software MatLab* dalam proses melakukan enkripsi dan dekripsi. Menurut [9], *MatLab* atau singkatan dari *Matrix Laboratory* merupakan perangkat lunak yang bergerak dibidang sains dan rekayasa yang dilengkapi dengan berbagai macam fitur yang dapat digunakan baik berupa *tools* maupun menciptakan algoritma sendiri. Terdapat pula penelitian tentang kriptografi dengan menggunakan *software MatLab*, yaitu penelitian yang dilakukan oleh [10]. Pada penelitian tersebut melakukan modifikasi terhadap algoritma caesar chiper dan *rail fence* untuk peningkatan keamanan teks alfanumerik dan karakter khusus. Pada penelitian ini menggunakan *sofware MatLab* yang bertujuan untuk melakukan simulasi dalam proses enkripsi dan dekripsi.

II. METODE PENELITIAN

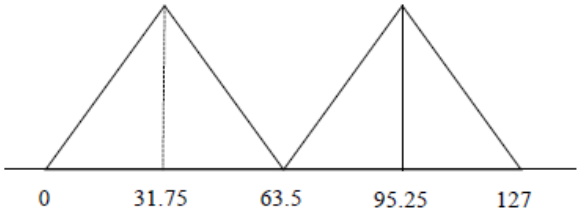
Penelitian ini melakukan modifikasi terhadap metode Hill Chiper dengan Fungsi Himpunan Fuzzy dan Kode ASCII. Alur penelitian secara umum terdiri dari proses enkripsi dan dekripsi dan dapat dilihat pada Gambar 1.



Gambar 1. Alur Penelitian Secara Umum

1. Proses Enkripsi

   Berdasarkan pada Gambar 1, proses enkripsi dilakukan dengan memasukkan plainteks atau pesan sebenarnya dan memasukkan kunci yang ingin digunakan dapat berupa angka, huruf maupun simbol yang terdapat pada kode ASCII, kemudian akan dimunculkan sebuah matriks acak yang ukurannya sesuai dengan jumlah plainteks yang dimasukkan. Selanjutnya plainteks diubah menjadi angka dan angka tersebut akan digunakan pada fungsi himpunan fuzzy untuk memperoleh derajat keanggotaan dan nilai derajat keanggotaan tersebut akan dimasukkan pada diagonal utama matriks yang dibangkitkan secara acak sebelumnya. Kemudian matriks tersebut dikalikan dengan kunci awal, maka diperolehlah chiperteks berupa matriks dan simbol. Adapun bentuk kurva yang digunakan untuk fungsi himpunan fuzzy adalah kurva segitiga dan kode ASCII, dapat dilihat pada Gambar 2 dan Gambar 3.



Gambar 2. Kurva Segitiga Fungsi Himpunan Fuzzy

Dengan persamaan fungsi himpunan fuzzy berdasarkan Gambar 1 adalah sebagai berikut :

$$a = \begin{cases} 0, untuk\ x \le 0\ dan\ x \ge 63.5 \\ \dfrac{x-0}{31.75}, untuk\ 0 \le x < 31.75\ ('@') \\ \dfrac{63.5-x}{31.75}, untuk\ 31.75 \le x < 63.5\ ('\#') \end{cases}$$

$$b = \begin{cases} 0, untuk\ x \le 63.5\ dan\ x \ge 127 \\ \dfrac{x-63.5}{31.75}, untuk\ 63.5 \le x < 95.25\ ('\$') \\ \dfrac{127-x}{31.75}, untuk\ 95.25 \le x \le 127\ ('\%') \end{cases}$$

Dec	Hex	Name	Char	Ctrl-char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	0	Null	NUL	CTRL-@	32	20	Space	64	40	@	96	60	`
1	1	Start of heading	SOH	CTRL-A	33	21	!	65	41	A	97	61	a
2	2	Start of text	STX	CTRL-B	34	22	"	66	42	B	98	62	b
3	3	End of text	ETX	CTRL-C	35	23	#	67	43	C	99	63	c
4	4	End of xmit	EOT	CTRL-D	36	24	$	68	44	D	100	64	d
5	5	Enquiry	ENQ	CTRL-E	37	25	%	69	45	E	101	65	e
6	6	Acknowledge	ACK	CTRL-F	38	26	&	70	46	F	102	66	f
7	7	Bell	BEL	CTRL-G	39	27	'	71	47	G	103	67	g
8	8	Backspace	BS	CTRL-H	40	28	(	72	48	H	104	68	h
9	9	Horizontal tab	HT	CTRL-I	41	29	)	73	49	I	105	69	i
10	0A	Line feed	LF	CTRL-J	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	VT	CTRL-K	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	FF	CTRL-L	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage feed	CR	CTRL-M	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	SO	CTRL-N	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	SI	CTRL-O	47	2F	/	79	4F	O	111	6F	o
16	10	Data line escape	DLE	CTRL-P	48	30	0	80	50	P	112	70	p
17	11	Device control 1	DC1	CTRL-Q	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	DC2	CTRL-R	50	32	2	82	52	R	114	72	r
19	13	Device control 3	DC3	CTRL-S	51	33	3	83	53	S	115	73	s
20	14	Device control 4	DC4	CTRL-T	52	34	4	84	54	T	116	74	t
21	15	Neg acknowledge	NAK	CTRL-U	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	SYN	CTRL-V	54	36	6	86	56	V	118	76	v
23	17	End of xmit block	ETB	CTRL-W	55	37	7	87	57	W	119	77	w
24	18	Cancel	CAN	CTRL-X	56	38	8	88	58	X	120	78	x
25	19	End of medium	EM	CTRL-Y	57	39	9	89	59	Y	121	79	y
26	1A	Substitute	SUB	CTRL-Z	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	ESC	CTRL-[	59	3B	;	91	5B	[	123	7B	{
28	1C	File separator	FS	CTRL-\	60	3C	<	92	5C	\	124	7C	|
29	1D	Group separator	GS	CTRL-]	61	3D	=	93	5D	]	125	7D	}
30	1E	Record separator	RS	CTRL-^	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	US	CTRL-_	63	3F	?	95	5F	_	127	7F	DEL

Gambar 3. Kode ASCII

2. Proses dekripsi dilakukan dengan cara memasukkan chiperteks matriks, kunci awal, dan chiperteks simbol. Kalikan chiperteks matriks dengan kunci awal, kemudian lihat chiperteks simbol lalu gunakan kondisi apabila chiperteks simbol berupa simbol @ maka kondisi yang digunakan pada proses dekripsi adalah angka 64, simbol # maka angka 35, simbol $ maka angka 36, atau simbol % maka angka 37 untuk

melakukan perhitungan berdasarkan proses dekripsi pada Gambar 1. Akan diperoleh hasil berupa angka kemudian dicocokkan dengan angka pada kode ASCII dan akhirnya akan diperoleh plainteks kembali.

III. HASIL DAN PEMBAHASAN

1. Analisa Manual

Pada penelitian dilakukan analisa manual dengan melakukan sebuah percobaan untuk melakukan enkripsi dan dekripsi. Terdapat plainteks dengan kata 'NOVI' dan kunci yang digunakan adalah '1945'. Langkah pertama yang dilakukan untuk melakukan enkripsi adalah membangkitkan matriks acak sesuai dengan jumlah plainteks, yaitu 4x4.

0.9670	0.2290	0.4427	0.9133
0.0782	0.8900	0.1230	0.5383
0.5197	0.0838	0.6520	0.5505
0.1524	0.3524	0.7650	0.7630

Setelah diperoleh sebuah matriks selanjutnya mengkode kata NOVI dengan melihat huruf N O V I pada kode ASCII dan diperoleh angka berikut :

N	O	V	I
78	79	86	73

Kemudian ubah matriks acak berdasarkan rentang pada fungsi himpunan fuzzy dengan melihat pada plainteks NOVI, kemudian letakkan pada diagonal utama matriks. Huruf N dengan nilai 78, dimana 78 merupakan nilai x maka berdasarkan persamaan fungsi himpunan fuzzy dengan melihat kurva segitiga pada Gambar 2, diperoleh:

$$\frac{78-63.5}{31.75} = 0.4567$$

Kemudian huruf O nilai 79, menggunakan perhitungan yang sama :

$$\frac{79-63.5}{31.75} = 0.4882$$

Selanjutnya huruf V nilai 86, menggunakan perhitungan yang sama :

$$\frac{86-63.5}{31.75} = 0.7087$$

Dan terakhir huruf I nilai 83, menggunakan perhitungan yang sama :

$$\frac{73-63.5}{31.75} = 0.2992$$

Sehingga matriks acak diatas berubah menjadi seperti berikut :

0.4567	0.1290	0.5427	0.8133
0.8820	0.4882	0.9230	0.2383
0.4197	0.0438	0.7087	0.5805
0.3524	0.3824	0.6650	0.2992

Selanjutnya ubah lagi nilai matriks dengan mengalikannya dengan kunci awal, kunci awal yang digunakan adalah 1945. Kunci awal tersebut kemudian dicocokkan dengan kode ASCII. Jadi angka 1 pada kode ASCII bernilai apa, angka 9, angka 4, dan angka 5. Perhitungan yang digunakan adalah :

$$\frac{1}{kunci\ awal\ ke-x} * matriks\ diagonal\ utama$$

Dimulai dengan kunci awal ke-1, yaitu 1, maka :

$$\frac{1}{49} * 0.4567 = 0.00932$$

$$\frac{1}{49} * 0.4882 = 0.00996$$

$$\frac{1}{49} * 0.70867 = 0.01446$$

$$\frac{1}{49} * 0.2992 = 0.00611$$

Kemudian kunci awal ke-2, yaitu angka 9 dengan nilai pada kode ASCII adalah 57 dan untuk nilai matriks yang digunakan adalah nilai matriks yang telah dikali dengan kunci awal ke-1, maka :

$$\frac{1}{57} * 0.00932 = 0.00016$$

$$\frac{1}{57} * 0.00996 = 0.00017$$

$$\frac{1}{57} * 0.01446 = 0.00025$$

$$\frac{1}{57} * 0.00611 = 0.00011$$

Kemudian kunci awal ke-3, yaitu 4 dengan nilai pada kode ASCII adalah 52 dan untuk nilai matriks yang digunakan adalah nilai matriks yang telah dikali dengan kunci awal ke-2, maka :

$$\frac{1}{52} * 0.00016 = 0.000003144$$

$$\frac{1}{52} * 0.00017 = 0.000003361$$

$$\frac{1}{52} * 0.00025 = 0.000004879$$

$$\frac{1}{52} * 0.00011 = 0.000002060$$

Kemudian kunci awal ke-4, yaitu 5 dengan nilai pada kode ASCII adalah 53 dan untuk nilai matriks yang digunakan adalah nilai matriks yang telah dikali dengan kunci awal ke-3, maka :

$$\frac{1}{53} * 0.000003144 = 0.0000000593$$

$$\frac{1}{53} * 0.000003361 = 0.0000000634$$

$$\frac{1}{53} * 0.000004879 = 0.0000000921$$

$$\frac{1}{53} * 0.000002060 = 0.0000000389$$

Sehingga diperoleh matriks yang disederhanakan dengan perkalian $1E*006$, maka matriksnya menjadi ssebagai berikut :

0.0593	0.0377	0.1277	0.0140
0.0500	0.0634	0.0949	0.1177
0.0757	0.0345	0.0921	0.1143
0.0327	0.1071	0.0759	0.0389

Untuk hasil pada matriks diatas, nilai selain diagonal utama matriks diperoleh secara acak dan sifatnya diabaikan.

Berdasarkan fungsi himpunan fuzzy maka kata NOVI disandikan dalam bentuk simbol menjadi :

$	$	$	$

Hasil sandi tersebut diperoleh karena nilai pada kata N O V I terletak pada segitiga b dengan rentang nilai antara 63.5 sampai 95.25 dengan simbol $ angka 36.

Selanjutnya proses dekripsi dilakukan dengan memasukkan matriks chiperteks, kunci awal, dan simbol chiperteks. Langkah awal yang dilakukan untuk melakukan dekripsi adalah mengalikan matriks chiperteks dengan kunci awal menggunakan rumus berikut :

0.0593	0.0377	0.1277	0.0140
0.0500	0.0634	0.0949	0.1177
0.0757	0.0345	0.0921	0.1143
0.0327	0.1071	0.0759	0.0389

$$kunci\ awal\ ke-x * matriks\ diagonal\ utama$$

Dimulai dengan kunci awal ke-1, yaitu nilai 1 dimana nilainya pada kode ASCII adalah 49, sehingga diperoleh :

$$49 * 0.0000000593 = 0.00000291$$

$$49 * 0.0000000634 = 0.00000311$$

$$49 * 0.0000000921 = 0.00000451$$

$$49 * 0.0000000389 = 0.00000190$$

Kemudian kunci awal ke-2, yaitu 9 dimana nilainya pada kode ASCII adalah 57 dan untuk nilai matriks yang digunakan adalah nilai matriks yang telah dikali dengan kunci awal ke-1, maka :

$$57 * 0.00000291 = 0.00017$$

$$57 * 0.00000311 = 0.00018$$

$$57 * 0.00000451 = 0.00026$$

$$57 * 0.00000190 = 0.00011$$

Kemudian kunci awal ke-3, yaitu 4 dimana nilainya pada kode ASCII adalah 52 dan untuk nilai matriks yang digunakan adalah nilai matriks yang telah dikali dengan kunci awal ke-2, maka :

$$52 * 0.00017 = 0.00862$$

$$52 * 0.00018 = 0.00921$$

$$52 * 0.00026 = 0.01337$$

$$52 * 0.00011 = 0.00565$$

Kemudian kunci awal ke-4, yaitu 5 dimana nilainya pada kode ASCII adalah 53 dan untuk nilai matriks yang digunakan adalah nilai matriks yang telah dikali dengan kunci awal ke-3, maka :

$$53 * 0.00862 = 0.4567$$

$$53 * 0.00921 = 0.4882$$

$$53 * 0.01337 = 0.7087$$

$$53 * 0.00565 = 0.2992$$

Sehingga diperoleh matriks dengan diagonal utama matriks sama dengan nilai matriks diagonal utama diawal proses enkripsi.

0.4567	0.8687	0.8001	0.2638
0.0046	0.4882	0.4314	0.1455
0.7749	0.3998	0.7087	0.1361
0.8173	0.2599	0.1818	0.2992

Langkah selanjutnya simbol chiperteks digunakan untuk menentukan kondisi untuk melakukan proses perhitungan akhir dalam memperoleh plainteks kembali, yaitu :

$	$	$	$

Untuk simbol $ merupakan angka 36 kondisi yang diberikan adalah perhitungan sebagai berikut :

$$(matriks\ diagonal\ utama\ nxm * 31.75) + 63.5$$

$$(0.4567 * 31.75) + 63.5 = 78$$

$$(0.4882 * 31.75) + 63.5 = 79$$

$$(0.7087 * 31.75) + 63.5 = 86$$

$$(0.2992 * 31.75) + 63.5 = 73$$

Kemudian cek pada kode ASCII angka tersebut merupakan huruf, angka, atau simbol apa dan diperoleh hasil :

78	79	86	73
N	O	V	I

2. Hasil Sistem

Pengujian sistem pada penelitian ini menggunakan *MatLab*. Kriptografi yang dilakukan memiliki konsep enkripsi dan dekripsi. Langkah awal melakukan enkripsi adalah dengan memasukkan plainteks dan kunci awal, dapat dilihat pada Gambar 4.

Gambar 4. Plainteks dan Kunci Awal

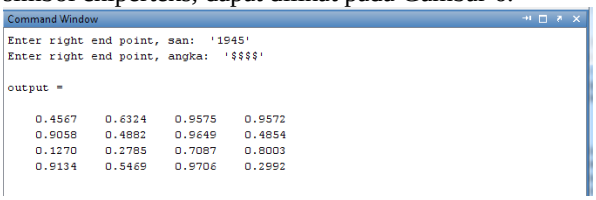
Gambar 4 merupakan plainteks dan kunci awal dengan plainteks nya 'NOVI' dan kunci awal '1945'. Pada pengujian ini menggunakan plainteks dengan huruf besar dan kunci berupa angka. Setelah dimasukkan plainteks dan kunci awal diperoleh matriks seperti pada Gambar 5.

```
output =

  1.0e-006 *

    0.0593    0.0377    0.1277    0.0140
    0.0500    0.0634    0.0949    0.1177
    0.0757    0.0345    0.0921    0.1143
    0.0327    0.1071    0.0759    0.0389


kata_sandi2 =

$$$$
```

Gambar 5. Chiperteks Berupa Matriks dan Simbol

Gambar 5 merupakan hasil enkripsi yang diperoleh dari plainteks 'NOVI' dan kunci awal '1945'. Hasil berupa matriks yang telah memiliki nilai derajat keanggotaan pada diagonal utama matriks dan merupakan *output* atau disebut matriks chiperteks. Selain matriks diperoleh pula simbol chiperteks, sehingga untuk menghasilkan plainteks kembali harus memiliki matriks chiperteks, kunci awal, dan simbol chiperteks.

Selanjutnya proses dekripsi dilakukan dengan memasukkan matriks chiperteks, kunci awal, dan simbol chiperteks, dapat dilihat pada Gambar 6.



Gambar 6. Matriks Chiperteks, Kunci Awal, dan simbol Chiperteks

Gambar 6 merupakan inputan yang diperlukan untuk dapat memperoleh plainteks kembali. Hasil akhirnya menghasilkan matriks yang memiliki derajat keanggotaan yang sama dengan nilai sebelum melakukan enkripsi pada diagonal utama matriks dan untuk nilai lain sifatnya acak dan diabaikan. Hasil plaineks kembali dapat dilihat pada Gambar 7.

```
vektor =

    78    79    86    73


ans =

NOVI
```

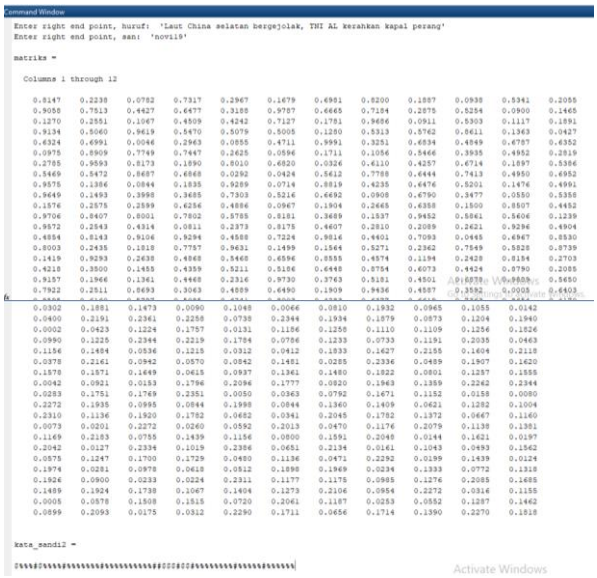
Gambar 7. Hasil Plainteks Kembali

Gambar 7 merupakan hasil dekripsi untuk memperoleh plainteks kembali dan dapat dilihat bahwa plainteks yang dihasilkan sama, yaitu NOVI.

Pengujian lain dapat dilakukan dengan menggunakan plainteks berupa huruf besar, spasi, dan huruf kecil. Seperti pada Gambar 8.

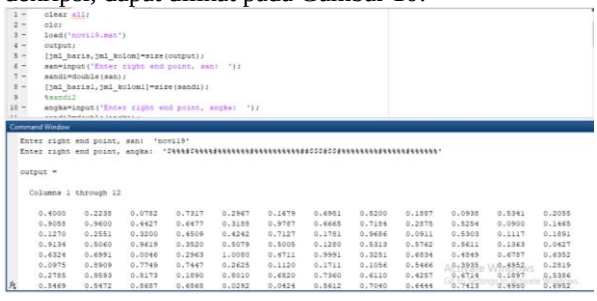
Gambar 8. Plainteks dan Kunci Awal

Gambar 8 merupakan plainteks berupa huruf besar, spasi, dan huruf kecil dan kunci awal menggunakan huruf kecil dan angka. Hasil matriks chiperteks dan simbol chiperteks dapat dilihat pada Gambar 9.



Gambar 9. Matriks Chiperteks dan Simbol Chiperteks

Gambar 9 merupakan matriks chiperteks dan simbol chiperteks yang diperoleh pada proses enkripsi, yaitu'$%%%#$%%%%#%%%%%%%#%%%%%%%%%%%##$$$#$$#%%%%%%%%#%%%%%#%%%%%%' dan kunci awal 'novi19'. Hasil enkripsi tersebut akan digunakan untuk melakukan proses dekripsi, dapat dilihat pada Gambar 10.



Gambar 10. Matriks Chiperteks, Kunci Awal, dan simbol Chiperteks

Gambar 10 merupakan matriks chiperteks, kunci awal, dan simbol chiperteks yang digunakan untuk memperoleh plainteks kembali. Hasil plainteks dapat dilihat pada Gambar 11.

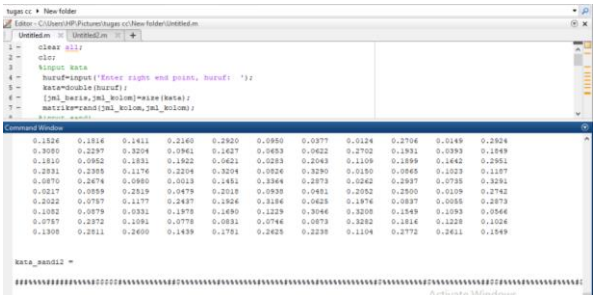
Gambar 11. Hasil Plainteks Kembali

Gambar 11 merupakan hasil plainteks yang diperoleh dan hasilnya sama dengan plainteks awal, yaitu 'Laut China selatan bergejolak, TNI AL kerahkan kapal perang'.

Pada penelitian ini dapat pula mengenkripsi plainteks berupa angka, spasi, huruf besar, dan huruf kecil berdasarkan yang terdapat pada kode ASCII, pengujian dapat dilihat pada Gambar 12.

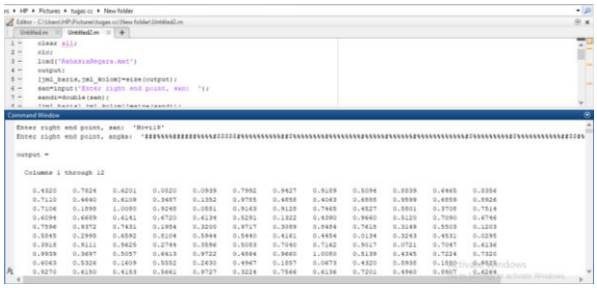
Gambar 12. Plainteks dan Kunci Awal

Gambar 12 merupakan plainteks berupa angka, spasi, huruf besar, dan huruf kecil dan kunci awal menggunakan huruf kecil dan angka. Hasil matriks chiperteks dan simbol chiperteks dapat dilihat pada Gambar 13.



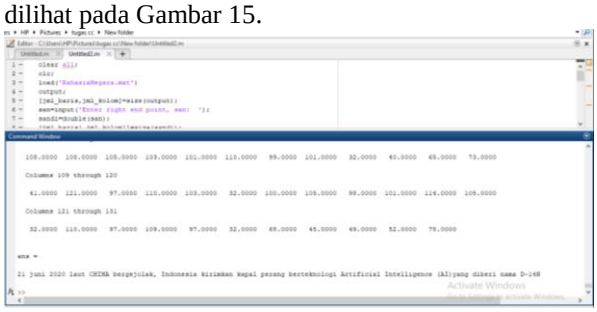
Gambar 13. Matriks Chiperteks dan Simbol Chiperteks

Gambar 13 merupakan matriks chiperteks dan simbol chiperteks yang diperoleh pada proses enkripsi, yaitu‘###%%%######%%%%#$$$$$#%%%%%%%%%##$%%%%%%%%%#%%%%%%%%%#%%%%%%#%%%%%%%#%%%%%%%%%%%%%%#$%%%%%%%%%%#$%%%%%%%%%%%%##$$#%%%%%#%%%%%%%#%%%%%#$###$’ dan kunci awal ‘Novi19’. Hasil tersebut akan digunakan untuk melakukan proses dekripsi, dapat dilihat pada Gambar 14.



Gambar 14. Matriks Chiperteks, Kunci Awal, dan Simbol Chiperteks

Gambar 14 merupakan matriks chiperteks, kunci awal, dan simbol chiperteks yang digunakan untuk memperoleh plainteks kembali. Hasil plainteks dapat dilihat pada Gambar 15.



Gambar 15. Hasil Plainteks Kembali

Gambar 15 merupakan hasil plainteks yang diperoleh dan hasilnya sama dengan plainteks awal, yaitu '21 juni 2020 laut CHINA bergejolak, Indonesia kirimkan kapal perang berteknologi Artificial Intelligence (AI)yang diberi nama D-14N'.

IV. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan maka dapat disimpulkan bahwa:

1. Modifikasi Hill Chiper dengan melakukan kombinasi fungsi himpunan fuzzy dan kode ASCII dapat diterapkan untuk melakukan penyandian atau kriptografi dan dapat membantu memberikan keamanan data yang lebih baik, karena modifikasi tidak menggunakan perhitungan metode Hill Chiper pada umumnya.
2. Penggunaan fungsi himpunan fuzzy menghasilkan nilai derajat keanggotaan dan nilai tersebut terdapat pada diagonal utama matriks.
3. Plainteks dan kunci awal yang digunakan bervariasi, seperti angka, spasi, huruf kecil, huruf besar, dan simbol berdasarkan pada kode ASCII.

DAFTAR PUSTAKA

[1] D. Ariyus, *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi*. Yogyakarta: Andi Offset, 2008.

[2] S. Yunita, P. Hasan, and D. Ariyus, “Modifikasi Algoritma Hill Cipher dan Twofish Menggunakan Kode Wilayah Telepon,” *Sisfotenika*, vol. 9, no. 2, pp. 213–

224, 2019.

[3] T. Alawiyah, "Modifikasi Kriptografi Hill Cipher Kunci Matriks Persegi Panjang Menggunakan Fungsi Xor Dan Fungsi Xnor," *IJCIT (Indonesian J. Comput. Inf. Technol.*, vol. 1, no. 1, pp. 68–82, 2016.

[4] M. H. Adiwibawa, R. Marwati, and R. Sispiyati, "Pemgimplementasian Modifikasi Kripografi Hill Cipher dengan Matriks Sirkulan," *J. EurekaMatika*, vol. 6, no. 2, pp. 1–11, 2019.

[5] A. Putera, A. P. U. Siahaan, and R. Rahim, "Dynamic key matrix of hill cipher using genetic algorithm," *Int. J. Secur. its Appl.*, vol. 10, no. 8, pp. 173–180, 2016, doi: 10.14257/ijsia.2016.10.8.15.

[6] F. Qazi, F. H. Khan, D. Agha, S. A. Khan, and S. ur Rehman, "Modification in Hill Cipher for Cryptographic Application," *3C Tecnol. innovación Apl. a la pyme*, no. May, pp. 240–257, 2019, doi: 10.17993/3ctecno.2019.specialissue2.240-257.

[7] A. Danny Wowor, "Modifikasi Kriptografi Hill Cipher Menggunakan Convert Between Base," *Semin. Nas. Sist. Inf. Indones.*, pp. 2–4, 2013.

[8] S. Kusumadewi and H. Purnomo, *Aplikasi Logika Fuzzy untuk Pendukung Keputusan*. Yogyakarta: Graha Ilmu, 2013.

[9] R. Sianipar, *Dasar Pemrograman Citra Digital dengan MatLab*. Yogyakarta: Andi Offset, 2018.

[10] A. W. Primaningtyas Nur Arifah, "Implementasi Kriptografi Caesar Chiper Menggunakan Matlab R2013a," pp. 1–8, 2017.