Penerapan Matriks dan Determinan sebagai Algoritma H-1U dalam Kriptografi

Ahmad Farhan Ghifari (13515602)
Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13515602@std.stei.itb.ac.id

***Abstrak*—Kriptogarafi merupakan ilmu dan seni untuk menyandikan suatu pesan agar tidak dapat dimengerti oleh orang lain. Kriptografi telah banyak digunakan untuk mengamankan pesan yang membutuhkan tingkat pengamanan yang sangat tinggi karena pesan tersebut merupakan pesan rahasia. Dengan menggunakan matriks dan determinan kita dapat membuat sebuah algoritma baru yang digunakan untuk mengamankan pesan. Algoritma ini cukup mudah untuk di implementasikan di dalam komputer namun cukup sulit bagi orang lain untuk memecahkan algoritma ini. Algoritma ini diberi nama H-1U.**

***Keywords*—Matriks, Determinan, Algortima, Kriptografi.**

I. PENDAHULUAN

Pada zaman sekarang ini perkembangan teknologi semakin pesat. Arus informasi mengalir begitu derasnya. Kebutuhan akan suatu alat yang dapat mendukung komunikasi semakin meningkat. Teknologi setiap hari selalu mengalami perkembangan. Para ilmuan berlomba – lomba untuk menciptakan suatu alat yang lebih efisien dan fleksibel untuk membantu manusia dalam berkomunikasi.

Semakin canggihnya perkembangan teknologi maka akan semakin marak pula kejahatan yang dapat dilakukan dengan teknologi. Salah satu nya adalah membaca pesan rahasia yang tersimpan pada sebuah perangkat. Pesan penting yang disimpan dalam sebuah perangkat dapat dibaca dengan mudah oleh orang lain apabila pesan tersebut tidak dilindungi.

Salah satu cara untuk melindungi pesan adalah dengan teknik kriptografi. Kriptografi merupakan seni mengubah pesan asli menjadi pesan lain yang artinya menjadi berubah dari pesan semula. Kriptografi juga memiliki arti ilmu yang ditujukan untuk mempelajari dan melakukan eksplorasi seputar keamanan pengiriman sebuah pesan (*message*)[1]. Atau dalam arti lain kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan dengan cara menyandikannya menjadi bentuk lain yang tidak bermakna[2].

Dengan menggunakan kriptografi kita dapat mengubah bentuk asli pesan menjadi bentuk lain. Dengan kata lain keamanan pada suatu pesan akan semakin terjaga. Dalam perkembanganya telah ditemukan berbagai macam algoritma yang dibuat untuk menyandikan suatu pesan. Diantaranya adalah algoritma RSA, Caesar Chipper, Monoalphabetic Chipper, Polyalphabethic Chipper, dan masih banyak lagi.

Namun yang menjadi pertanyaan adalah apakah algoritma tersebut sudah teruji keamanannya atau belum. Atau bahkan apakah algoritma tersebut tepat digunakan pada sebuah sistem atau tidak. Seperti contohnya adalah pada algoritma RSA. Algoritma ini dipercaya cukup aman untuk digunakan pada sebuah pesan karena akan cukup sulit bagi orang lain untuk mencoba memecahkan pesan yang telah terenkrip dengan algoritma ini. Algoritma ini akan menghasilkan pesan terenkrip yang cukup panjang dari pesan aslinya.

Dari paparan diatas penulis ingin membuat sebuah algoritma kriptografi yang cara pengimplementasianya cukup sederhana namun tidak mudah untuk dipecahkan oleh orang lain. Pada makalah ini akan dibahas mengenai algoritma kriptografi dengan menggunakan matriks dan determinan sebagai salah satu implementasi algoritma nya. Penulis memberikan nama untuk algoritma ini yaitu H-1U.

II. DASAR TEORI

A. Kriptografi

Secara etimologi kata kriptografi (Cryptography) berasal dari bahasa Yunani, yaitu kryptos yang artinya yang tersembunyi dan graphein yang artinya tulisan[3]. Pada awalnya kriptografi ini dipahami sebagai ilmu tentang menyembunyikan pesan, tetapi seiring dengan perkembangan zaman hingga saat ini pengertian kriptografi berkembang menadi ilmu tentang teknik matematis yang digunakan untuk menyelesaikan persoalan keamanan berupa privasi dan otentikasi[3].

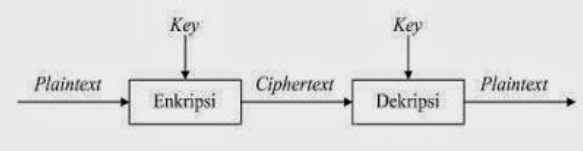
Sejarah penulisan rahasia tertua dapat ditemukan pada peradaban Mesir kuno, yaitu pada tahun 3000 SM. Bangsa Mesir menggunakan ukiran rahasia yang disebut dengan *hieroglyphics* untuk menyampaikan pesan kepada

orang – orang yang memiliki hak. Pada awalnya di tahun 400 SM bangsa Spartan di Yunani memanfaatkan kriptografi di bidang militer dengan menggunakan alat yang disebut *scytale*, yaitu pita panjang berbahan daun papyrus yang dibaca dengan cara digulungkan ke sebatang silinder. Sedangkan pada peradaban Cina dan Jepang menemukan kriptografi pada abad 15 SM.

Kita dapat menjumpai beberapa istilah penting dalam kriptografi antara lain plaintext, chippertext, enkripsi, dekripsi, cryptanalaysis, dan cryptology. Plaintext adalah data yang dapat dibaca, sedangkan teknik untuk menjadikan data tidak dapat dibaca disebut enkripsi[3]. Data yang telah dienkripsi disebut chippertext, dan teknik untuk mengembalikan chippertext menjadi plaintext disebut dekripsi[3].

Chipper merupakan salah satu algoritma kriptografi, yaitu fungsi matematika yang memiliki peran dalam mengenkripsi dan mendektripsi data. Pelaku yang ahli dalam bidang kriptografi disebut cryptographer[3].

Cryptanalisis adalah ilmu untuk memecahan cihpertext menjadi plaintext dengan tidak melalui cara yang semestinya, sedangkan orang yang menguasai ilmu ini disebut Cryptanalyst. Cabang matematika yang meliputi kriptografi dan cryptanalysis disebut Cryptology, sedangkan orang yang menguasai ilmu ini disebut cryptologist[3].



Gambar 1. Proses enkripsi – dekripsi.
Sumber :
http://www.kajianpustaka.com/2014/01/pengertian-sejarah-dan-jenis-kriptografi.html

Dalam perkembangannya kriptografi memiliki beberapa jenis. Algoritma kriptografi dapat diklasifikasikan menjadi dua jenis berdasarkan perkembanganya, yaitu kriptografi klasik dan kriptografi modern[3].

1. Kriptografi klasik

Algoritma ini digunakan sejak sebelum era komputerisasi dan kebanyakan menggunakan teknik kunci simetris. Metode yang menyembunyikan pesannya adalah dengan teknik substitusi atau transposisi atau keduanya[3]. Teknik substitusi adalah menggantikan karakter dalam plaintext menjadi karakter lain ayng hasilnya adlaah chippertext. Sedangkan transposisi adalah teknik mengubah plaintext menjadi chipertext dengan cara permutasi karakter. Kombinasi keduanya kompleks adalah yang melatarbelakangi terbentuknya berbagai macam algoritma kriptografi modern[3].

2. Kriptografi modern

Algoritma ini digunakan setelah era komputer. Sehingga kebanyakan algoritma ini memiliki tingkat kesulitan yang kompleks. Jenis kriptografi dapat dibedakan berdasarkan kuncinya, yaitu algoritma simetris dan algorimta asimetris.

a. Algoritma simetris
   Algortima ini disebut simetris karena memiliki key atau kunci yang sama dalam proses enkripsi dan dekripsi sehingga algotima ini juga sering disebut algortima kunci tunggal atau algoritma satu kunci. Key dalam algoritma ini bersifat rahasia atau *private key* sehingga algoritma ini juga disebut dengan algortima kunci rahasia[3].
b. Algoritma asimetris
   Algoritma ini disebut asimetris karena kunci yang digunakan untuk enkripsi berbeda dengan unci yang digunakan untuk dekripsi. Kunci yang digunakan untuk enkripsi adalah kunci publik atau publik key sehingga algoritma ini juga disebut dengan algoritma kunci publik. Sedangkan kunci untuk dekripsi menggunakan kunci rahasia atau *private key*[3].

B. Matriks

Matriks dalam matematika merupakan kumpulan bilangan, simbol atau ekspresi berbentuk persegi panjang yang disusun menurut baris dan kolom[4]. Bilangan – bilangan yang terdapat pada suatu matriks disebut dengan elemen atau disebut juga anggota dari suatu matriks[4].

Matriks memiliki dimensi. Dimensi ini dapat bersifat bujur sangkar (jumlah kolom dan baris sama banyak) maupun bentuk persegi panjang (jumlah kolom tidak sama dengan jumlah baris).

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

Gambar 2. Contoh matriks 3x3
Sumber : http://rumus-matematika.com/materi-matriks-lengkap-dan-contohnya/

Matriks juga memiliki beberapa operasi dasar aritmatika yaitu penjumlahan, pengurangan dan perkalian. Operasi lain yang terdapat dalam matriks salah satu nya adalah transpose dan determinan.

a. Penjumlahan dan Pengurangan

Penjumlahan dalam matriks hanya dapat dilakukan apbila kedua matriks tersebut mempunyai ukuran atau tipe ayng sama. Elemen – elemen dalam suatu matriks yang dijumlahkan atau dikurangkan yaitu elemen yang memiliki posisi/letak yang sama.

$A_{ij} \pm B_{ij} = C_{ij}$

Representasi penjumlahan atau pengurangan adalah sebagi berikut.

$$\begin{bmatrix}(a_{11} \pm b_{11}) & (a_{12} \pm b_{12}) & (a_{13} \pm b_{13})\\ (a_{21} \pm b_{21}) & (a_{22} \pm b_{22}) & (a_{23} \pm b_{23})\end{bmatrix} = \begin{bmatrix}c_{11} & c_{12} & c_{13}\\ c_{21} & c_{22} & c_{23}\end{bmatrix}$$

Gambar 3. Penjumlahan dan pengurangan di matriks.

Sumber : http://rumus-matematika.com/materi-matriks-lengkap-dan-contohnya/

b. Perkalian

Perkalian dua buah matriks A dan B dapat dikalikan apabila banyak kolom matriks A sama dengan banyak baris pada matriks V. Misalnya matriks ordo 2 x 3 dapat dikalikan dengan matriks ordo 3 x 3 tetapi tidak bisa dikalikan dengan matriks berordo 5 x 7. Hal ini karena jumlah kolom di matriks 2 x 3 tidak sama dengan jumlah baris di matriks 5 x 7.

Konsep perkalian matriks dengan matriks adalah sebagai berikut

$$A_{m \times n} . B_{n \times k} = C_{m \times k}$$

Gambar 4. Perkalian Matriks

Contoh dari perkalian matriks adalah sebagai berikut.

$$A.B = \begin{bmatrix}2 & 4 & -2\\ 3 & 2 & 1\\ -2 & 2 & 2\\ 1 & 3 & 4\end{bmatrix} . \begin{bmatrix}3 & 2\\ 2 & 3\\ 3 & 2\end{bmatrix}$$

$$A.B = \begin{bmatrix}2.3+4.2+(-2).3 & 2.2+4.3+(-2).2\\ 3.3+2.2+1.3 & 3.2+2.3+1.2\\ (-2).3+2.2+2.3 & (-2).2+2.3+2.2\\ 1.3+3.2+4.3 & 1.2+3.3+4.2\end{bmatrix}$$

$$A.B = \begin{bmatrix}8 & 12\\ 16 & 14\\ 4 & 6\\ 21 & 19\end{bmatrix}$$

Gambar 5. Contoh perkalian matriks.

Sumber : http://bahanbelajarsekolah.blogspot.co.id/2014/11/kumpulan-soal-dan-pembahasan-perkalian.html

c. Transpose

Matriks transpose merupakan matriks yang mengalami pertukaran elemen dari kolom menjadi baris atau sebaliknya. Contohnya adalah sebagai berikut :

$$A = \begin{pmatrix}1 & 3 & 1\\ 2 & 4 & 5\\ 0 & 7 & 6\end{pmatrix} \qquad A^T = \begin{pmatrix}1 & 2 & 0\\ 3 & 4 & 7\\ 1 & 5 & 6\end{pmatrix}$$

Gambar 6. Transpose matriks.

Sumber : http://www.rumusmatematikadasar.com/2015/01/pengertian-transpose-matriks-sifat-sifatnya-serta-contoh-soal-dan-pembahasan.html

d. Determinan

Determinan adalah suatu fungsi tertentu yang menghubungkan suatu bilangan real dengan suatu matriks bujursangkar[5]. Misal ada suatu matriks dengan nama A, maka determinan dari A dapat ditulis dengan | A |. Untuk menentukan determinan matriks dapat digunakan beberapa cara, namun pada makalah ini penulis hanya akan menggunakan dua cara yaitu determinan untuk matriks dengan ordo 2 x 2 dan matriks dengan ordo 3 x 3 dengan menggunakan metode ekspansi baris dan kolom.

1. Matriks ordo 2 x 2

   $A = \begin{bmatrix}3 & 2\\ 5 & 6\end{bmatrix}$

   | A | = 3 x 6 – 2 x 5

   = 20

2. Matriks ordo 3 x 3 dengan menggunakan metode ekspansi baris dan kolom

   $M = \begin{bmatrix}-2 & 0 & 1\\ 3 & 2 & -1\\ 1 & -3 & 5\end{bmatrix}$

   $$| M | = -2 \begin{vmatrix}2 & -1\\ -3 & 5\end{vmatrix} - 0 \begin{vmatrix}3 & -1\\ 1 & 5\end{vmatrix} + 1 \begin{vmatrix}3 & 2\\ 1 & -3\end{vmatrix}$$

   = -2 (10 - 3) – 0 + 1 (-9 – 2)

   = -25

e. Tabel ASCII

ASCII merupakan singkatan dari *American Standard Code for Information Interchange.* ASCII adalah standar untuk karakter enkoding yang digunakan oleh komputer dan peralatan komunikasi untuk merepresentasikan teks, dan digunakan pada kebanyakan komputer (atau beberapa ekstensi yang kompatibel dengan itu)[6].

ASCII menggunakan *byte* tunggal untuk merepresentasikan setiap karakter. *Byte* merupakan unit pengalamatan data komputer terkecil yang terdiri dari delapan bit. Pada ASCII terdapat 128 standar karakter. Bila menggunakan notasi biner maka kode ASCII berada pada biner 0000 0000 hingga 0111 1111. Berikut adalah tabel ASCII.

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

www.bibase.com

Gambar 7. Tabel ASCII

Sumber : www.bibase.com

III. PERANCANGAN ALGORITMA

Seperti yang telah dibahas pada bab sebelumnya,

kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan dengan cara mengubahnya menjadi bentuk lain yang tidak bermakna. Kita dapat membuat algoritma kriptografi dengan memanfaatkan konsep matriks dan determinan. Determinan akan digunakan sebagai kunci untuk penyandian serta pendekripan suatu pesan.

A. Enkripsi

Langkah – langkah enkripsi pada algoritma ini adalah sebagai berikut.

1. Ubah pesan ke dalam bentuk ASCII.

Pesan yang akan disandikan diubah terlebih dahulu menjadi bentuk ASCII. Hal ini dilakukan agar penyandian lebih mudah untuk dilakukan dengan menggunakan konsep matriks.

2. Susun pesan dalam ASCII menjadi bentuk matriks.

Pesan yang telah diubah menjadi bentuk ASCII selanjutnya disusun kedalam bentuk matriks. Pesan disusun terurut dengan karakter pertama sebagai A_{11} (matriks baris satu kolom satu), karakter kedua diletakkan pada A_{12} (matriks bari satu kolom 2) hingga jumlah mencapai maksimal yang penulis tentukan yaitu 2, 3, atau 4 (sesuai dengan kondisi jumlah karakter yang akan dijelaskan setelah ini).

Terdapat beberapa kondisi untuk penyusunan matriks tergantung dari banyaknya jumlah karakter (x). Kondisi tersebut adalah sebagai berikut :

a. Jumlah karakter kurang dari atau sama dengan 4 ($x \leq 4$).

   Bila karakter kurang dari 4 maka ditambahkan karakter spasi yang memiliki kode ASCII desimal yaitu 32 sehingga jumlah karakter nya menjadi 4. Bila jumlah karakter sama dengan 4 maka tinggal disusun menjadi matriks 2 x 2. Sehingga pesan akan menjadi matriks dengan ordo 2 x 2.

b. Jumlah karakter lebih dari 4 dan kurang dari atau sama dengan 9 ($4 > x \leq 9$).

   Bila karakter lebih dari 4 dan kurang dari 9 maka ditambahkan karakter spasi yang memiliki kode ASCII desimal yaitu 32 sehingga jumlah karakter nya menjadi 9. Bila jumlah karakter sama dengan 9 maka tinggal disusun menjadi matriks 3 x 3.

c. Jumlah karakter lebih dari 9 ($x > 9$).

   Bila jumlah karakter lebih dari 9 maka susun menjadi matriks dengan jumlah kolom sama dengan 4. Jumlah baris tidak terbatas. Jumlah karakter seluruhnya harus habis dibagi 4 atau bila di modulo 4 maka hasilnya adalah 0 (x modulo 4 = 0). Bila di modulo hasilnya bukan 0 maka jumlah karakter harus ditambah karakter spasi yang memiliki kode ASCII desimal 32 hingga jumlah karakter sama dengan kelipatan 4 yang terdekat. Contoh apabila jumlah karakter adalah 17, maka harus ditambah 3 karakter spasi sehingga jumlahnya adalah 20.

3. Transpose matriks tersebut.

Setelah matriks tersusun lakukan transpose pada matriks tersebut.

4. Cari determinan dari matriks tersebut.

Determinan ini akan digunakan sebagai kunci untuk melakukan penyandian maupun untuk melakukan pendekripan. Dalam menentukan determinan dari matriks tersebut terdapat dua kondisi yang harus diperhatikan. Kondisi tersebut adalah sebagai berikut.

a. Ordo matriks 2 x 2

   Apabila ordo matriks 2 x 2 maka cari determinan sesuai dengan aturan mencari determinan matriks 2 x 2.

b. Ordo matriks 3 x 3 atau Y x 4

   Apabila ordo matriks 3 x 3 atau Y x 4 maka gunakan elemen matriks $A_{11} – A_{ii}$ dengan i adalah 3 sebagai elemen yang digunakan untuk mencari determinan. Pencarian determinan dapat dilakukan dengan menggunakan metode ekspansi baris dan kolom.

Setelah determinan ditemukan, simpan angka tersebut untuk melakukan dekripsi pada pesan yang telah disandikan. Hasil determinan ini merupakan kunci dekripsi.

5. Lakukan operasi penjumlahan matriks dengan hasil determinan.
6. Modulo kan setiap elemen pada hasil langkah lima dengan 128.

Matriks yang setiap elemenya telah dijumlahkan dengan hasil determinan (langkah 5) selanjutnya di modulo dengan 128 (jumlah ASCII adalah 128). Sehingga kini kita memiliki matriks dengan setiap elemen telah di modulo dengan 128.

7. Letakkan angka 0 di awal setiap elemen apabila jumlah digit elemen tersebut kurang dari 3
8. Ambil setiap elemen untuk disusun menjadi sebuah pesan.

Pengambilan elemen dilakukan dengan cara dimulai dari baris ke 1 kolom ke 1 hingga kolom maks. Lalu dilanjutkan baris ke 2 kolom ke 1 hingga kolom maksimal dan berakhir pada baris maks dan kolom maks.

Sekarang pesan telah terenkripsi dengan menggunakan algoritma H-1U.

B. Dekripsi

Langkah – langkah dekripsi pada algoritma ini adalah sebagai berikut.

1. Susun lah chippertext menjadi sebuah elemen yang memiliki 3 digit angka.

Jumlah karakter pada chippertext pasti memiliki kelipatan 3. Susunlah chippertext menjadi beberapa elemen dengan 3 digit angka. Semisal kita memiliki chippertext 023123432 maka susunlah menjadi 023 123 432.

2. Susun chippertext menjadi bentuk matriks.

Penyusunan chippertext menjadi bentuk matriks sama dengan aturan penyusunan saat penyandian. Jumlah elemen dalam chippertext pasti berjumlah 4, 9 atau kelipatan 4. Apabila jumlah elemen nya adalah 4 maka

susun menjadi matriks dengan ordo 2 x 2. Apabila jumlah elemen nya adalah 9 maka susun menjadi matriks dengan ordo 3 x 3. Apabila jumlah elemen nya adalah kelipatan 4 maka susun matriks menjadi matriks yang memiliki jumlah kolom 4 dan jumlah baris menyesuaikan jumlah karakter.

3. Buang angka 0 yang terdapat di awal elemen.
4. Lakukan operasi pengurangan matriks dengan kunci determinan.
5. Lakukan operasi modulo.

Setiap elemen pada matriks tersebut di modulo dengan 128.

6. Transpose matriks tersebut.
7. Ubah matriks tersebut menjadi karakter sesuai dengan kode ASCII.
8. Ambil setiap elemen untuk disusun menjadi sebuah pesan dan buang karakter spasi yang terdapat di akhir kalimat.

Pengambilan elemen dilakukan dengan cara dimulai dari baris ke 1 kolom ke 1 hingga kolom maks. Lalu dilanjutkan baris ke 2 kolom ke 1 hingga kolom maksimal dan berakhir pada baris maks dan kolom maks.

Kini kita telah mendapatkan kembali pesan asli atau disebut dengan *plaintext*.

IV. IMPLEMENTASI

Semisal kita memiliki *plaintext* yaitu "ITB". Maka kita dapat menyandikan pesan tersebut dengan menggunakan algoritma H-1U dengan langkah – langkah sebagai berikut.

1. Ubah pesan menjadi bentuk ASCII

Kode ASCII untuk pesan tersebut adalah 73 84 66.

2. Susun pesan dalam ASCII menjadi bentuk matriks.

Jumlah karakter pada pesan tersebut adalah 3. Oleh karena itu kita dapat menyusun pesan ini menjadi matriks dengan ordo 2 x 2. Hasilnya adalah sebagai berikut

$$A = \begin{bmatrix} 73 & 84 \\ 66 & 32 \end{bmatrix}$$

Angka 32 ditambahkan agar elemen matriks berjumlah 4.

3. Transpose matriks tersebut.

Hasil nya adalah sebagai berikut.

$B = A^T$

$$B = \begin{bmatrix} 73 & 66 \\ 84 & 32 \end{bmatrix}$$

4. Cari determinan matriks tersebut.

Determinan dari matriks tersebut adalah sebagi berikut.

$|B| = 73 \times 32 - 84 \times 66$

$= -3208$

5. Lakukan operasi penjumlahan dengan hasil determinan

$$B = \begin{bmatrix} 73 & 66 \\ 84 & 32 \end{bmatrix} + (-3208)$$

$$= \begin{bmatrix} -3135 & -3142 \\ -3124 & -3176 \end{bmatrix}$$

6. Modulo kan setiap elemen pada hasil langkah lima dengan 128.

$$B = \begin{bmatrix} -3135 & -3142 \\ -3124 & -3176 \end{bmatrix} \bmod 128$$

$$= \begin{bmatrix} 65 & 58 \\ 76 & 24 \end{bmatrix}$$

7. Letakkan angka 0 di awal setiap elemen apabila jumlah digit elemen tersebut kurang dari 3.

$$B = \begin{bmatrix} 065 & 058 \\ 076 & 024 \end{bmatrix}$$

8. Ambil setiap elemen untuk disusun menjadi sebuah pesan.

Setelah melalui langkah ini maka kita telah mendapatkan chipper text dari pesan tersebut yaitu "065058076024"

Dari chipper text itu kita dapat melakukan dekripsi dengan langkah – langkah sebagi berikut.

1. Susun lah chippertext menjadi sebuah elemen yang memiliki 3 digit angka.

Hasilnya penyusunan tersebut adalah 065 058 076 024.

2. Susun chipper text menjadi bentuk matriks.

$$A = \begin{bmatrix} 065 & 058 \\ 076 & 024 \end{bmatrix}$$

3. Buang angka 0 yang terdapat di awal elemen.

$$A = \begin{bmatrix} 65 & 58 \\ 76 & 24 \end{bmatrix}$$

4. Lakukan operasi pengurangan matriks dengan kunci determinan

$$A = \begin{bmatrix} 65 & 58 \\ 76 & 24 \end{bmatrix} - (-3208)$$

$$= \begin{bmatrix} 3273 & 3266 \\ 3284 & 3232 \end{bmatrix}$$

5. Lakukan operasi modulo

$$A = \begin{bmatrix} 3273 & 3266 \\ 3284 & 3232 \end{bmatrix} \bmod 128$$

$$= \begin{bmatrix} 73 & 66 \\ 84 & 32 \end{bmatrix}$$

6. Transpose matriks tersebut

$B = A^T$

$$B = \begin{bmatrix} 73 & 84 \\ 66 & 32 \end{bmatrix}$$

7. Ubah matriks tersebut menjadi karakter sesuai dengan kode ASCII.

$$A = \begin{bmatrix} I & T \\ B & \end{bmatrix}$$

8. Ambil setiap elemen untuk disusun menjadi sebuah pesan dan buang karakter spasi yang terdapat di akhir kalimat.

Pesan yang di dapat dari hasil dekripsi tersebut adalah "ITB".

V. KESIMPULAN

Kriptografi memiliki manfaat yang sangat besar karena dapat digunakan untuk melindungi suatu pesan yang harus terjaga kerahasiaannya. Dengan memanfaatkan kode ASCII, matriks dan determinan kita dapat membuat sebuah algoritma kriptografi baru. Dalam makalah ini penulis memberikan nama untuk algoritma ini yaitu H-1U.

Determinan digunakan sebagai kunci dalam pengenkripsian suatu pesan dan pendekripan suatu chipper text. Dengan algoritma ini akan cukup mudah di implementasikan dalam program komputer namun cukup sulit untuk dipecahkan oleh orang lain.

VI. UCAPAN TERIMAKASIH

Alhamdulillah, penulis menngucapkan rasa syukur kepada Allah SWT yang telah memberikan kesempatan untuk selalu berkarya dan bermanfaat bagi masyarakat. Limpahan serta curahan rahmat Nya begitu besar sehingga penulis masih bisa terus belajar, memperbaiki kesalahan dan terus mengembangkan diri lagi menjadi pribadi yang lebih bermanfaat untuk masyarakat. Penulis juga mengucapkan terimakasih kepada orang tua khususnya untuk Ibu yang tidak pernah berhenti berdoa dan memberikan support untuk penulis. Tidak lupa penulis juga mengucapkan terimakasih kepada dosen pembimbing yaitu Bapak Rinaldi Munir dan Bapak Judhi Santoso yang telah memberikan bimbingan dan membagikan ilmunya kepada penulis. Ucapan terimakasih juga penulis sampaikan kepada pihak lain yang tidak bisa penulis sebutkan satu – persatu. Semoga apa yang telah kita lakukan hari ini dapat memberikan manfaat untuk Indonesia.

REFERENSI

[1] Shidik, Guruh Fajar, *Introduction Kriptografi*, 2013.
[2] Munir, Rinaldi. 2003. Matematika Diskrit Edisi Kedua. Bandung: Penerbit Informatika.
[3] http://www.kajianpustaka.com/2014/01/pengertian-sejarah-dan-jenis-kriptografi.html. Diakses pada 14 Desember 2015, pukul 23.00 WIB.
[4] http://rumus-matematika.com/materi-matriks-lengkap-dan-contohnya/. Dikases pada 15 Desember 2015, pukul 09.00 WIB.
[5] https://elnicovengeance.wordpress.com/2011/08/04/determinan-matriks/. Diakses pada 15 Desember 2015, pukul 11.15 WIB.
[6] http://www.linfo.org/ascii.html. Diakses pada 15 Desember 2015, pukul 15.00 WIB.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 16 Desember 2015

Ahmad Farhan Ghifari
13515602