Implementasi Cipher Viginere pada kode ASCII dengan Memanfaatkan Digit Desimal Bilangan Euler

Kuswari Hernawati

Jurusan Pendidikan Matematika
FMIPA Universitas Negeri Yogyakarta
Alamat: Jl. Colombo Karangmalang Yogyakarta 55281

Abstrak

Perkembangan teknologi telekomunikasi dan penyimpanan data dengan menggunakan komputer memungkinkan pengiriman data jarak jauh yang relatif cepat dan murah. Di sisi lain pengiriman data jarak jauh memungkinkan pihak lain dapat menyadap dan mengubah data yang dikirimkan, sehingga perlu adanya keamanan data di dalamnya. Cara yang ditempuh adalah dengan kriptografi yang menggunakan transformasi data sehingga data yang dikirimkan tidak mudah dimengerti oleh pihak ketiga, salah satu cara transformasi data adalah dengan cipher viginere.

Keunikan digit desimal dari bilangan Euler (biasa disebut bilangan e) dapat digunakan sebagai acuan penerapkan algoritma yang ada di kajian kriptografi. Hal ini dengan pertimbangan bahwa pembangkitan bilangan/kode acuan dapat diperoleh dari formulasi perhitungan digit desimal bilangan Euler yang sudah mapan dan diakui dunia.

Selain itu, deretan digit dari nilai desimal bilangan e untuk implementasi enkripsi-dekripsi dengan cipher viginere yaitu dengan cara pengelompokan digitnya, sangat kecil kemungkinannya menghasilkan nilai rujukan yang sama.

Kata kunci : Euler, transformasi data, kriptografi, viginere

Latar Belakang

Perkembangan teknologi telekomunikasi dan penyimpanan data dengan menggunakan komputer memungkinkan pengiriman data jarak jauh yang relatif cepat dan murah. Di sisi lain pengiriman data jarak jauh memungkinkan pihak lain dapat menyadap dan mengubah data yang dikirimkan, sehingga perlu adanya keamanan data di dalamnya. Cara yang ditempuh adalah dengan kriptografi yang menggunakan transformasi data sehingga data yang dikirimkan tidak mudah dimengerti oleh pihak ketiga, salah satu cara transformasi data adalah dengan cipher viginere.

Pada makalah ini akan dibahas bagaimana digit desimal dari bilangan Euler (biasa disebut bilangan e) digunakan sebagai acuan penerapan algoritma cipher viginere pada kode ASCII. Hal ini dengan pertimbangan bahwa pembangkitan bilangan/kode acuan dapat diperoleh dari formulasi perhitungan digit desimal bilangan Euler yang sudah mapan dan diakui dunia.

Bilangan Euler

Bilangan e yang kemudian disebut sebagai bilangan euler merupakan bilangan yang diperoleh dari pendekatan nilai $(1+1/n)^n$ untuk n menuju tak hingga, yang ditemukan pada tahun 1683 oleh Jacob Bernoulli.

$$e = \lim_{n\to\infty}(1+\tfrac{1}{n})^n$$

Pada tahun 1748 , Euler memberikan ide mengenai bilangan e yaitu

$e = 1+ 1/1! + 1/2! + 1/3! + 1/4! + ...$ dan bahwa $e = \lim_{n\to\infty}(1+\tfrac{1}{n})^n$. Dari formulasi tersebut, Euler memberikan pendekatan untuk bilangan e 18 digit dibelakang koma, yaitu: e= 2,718281828459045235

Pada tahun 1884 Boorman menghitung e sampai dengan 346 digit dibelakang koma dan telah dihitung sampai dengan 869.894.101 digit dibelakang koma oleh Sebastian Wedeniwski. (O'Connor, 2001)

e =

2.71828182845904523536028747135266249775724709369995957496696762772407
66303535475945713821785251664274274663919320030599218174135966290435720
90033429526059563073813232862794349076323382988075319525101901157383341
87930702154089149934884167509244761460668082264800168477411853742345441
24371075390777449920695517027618386062613313845830007520449338265602970
60673711320070932870912744374704723069697720931014169285368190255151086
57463772111252389784425056953696770785449969967946864454905987931636880
92300987931277361782154249992295763514822082698951936680331825288693980
49646510582093923982948879332036250944311730123819706841614039701983760
79320683282376464804295311802328782509819455815301756717361332069811250
09961818815930416903515988885193458072738667385894228792284998920868050
82574927961048419844436346324496848756023362482704197862320900216099020
35304369941849146314093431738143640546253152096183690888707016768396420
43781405927145635490613031072085103837505101157477041718986106873969650
52126715468895703503540212340784981933432106817012100562788023519303320
24745015853904730419957777093503660416997329725088687696640355570716220
68447162560798826517871341951246652010305921236677194325278675398558940
48969709640975459185695638023637016211204774272283648961342251644507810
82442352948636372141740238893441247963574370263755294448337998016125490
22785092577825620926226483262779333865664816277251640191050049164499800
28931505660472580277863186415519565324425869829469593080191529872117250
56347546396447910145904090586298496791287406870504895858674174798546677
57573205681288459205413340539220001137863009455606881667400169842055800
40336379537645203040243225661352783695117788386387443966253224985065490
95886234281899707733276171783928034946501434558897071942586398772754710
09629537415211151368350627526023264847287039207643100595841166120545290
70302364725492966693811513732275364509888903136020572481765851180630360
44281231496550704751025446501172721155519486685080036853228183152196000
37356252794495158284188294787610852639813955990067376482922443752871840
62457803619298197139914756448826260390338144182326251509748279877799640
37308997038886778227138360577297882412561190717663946507063304527954660
18550966661856647097113444740160704626215680717481877844371436988218550
96709591025968620023537185887485696522000503117343920732113908032936340
47972735.....

Kode ASCII

Kode ASCII (Standard Code for Information Interchange) merupakan representasi numerik dari suatu karakter seperti ‘a’ atau ‘@’ atau karakter yang tidak tercetak, misalnya ‘Σ’. Tabel dibawah ini menunjukkan karakter ASCII termasuk 32 karakter yang tidak tercetak.

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

32 Karakter tidak tercetak

128	Ç	144	É	161	í	177	▒	193	┴	209	╤	225	ß	241	±
129	ü	145	æ	162	ó	178	▓	194	┬	210	╥	226	Γ	242	≥
130	é	146	Æ	163	ú	179	│	195	├	211	╙	227	π	243	≤
131	â	147	ô	164	ñ	180	┤	196	─	212	╘	228	Σ	244	⌠
132	ä	148	ö	165	Ñ	181	╡	197	┼	213	╒	229	σ	245	⌡
133	à	149	ò	166	ª	182	╢	198	╞	214	╓	230	µ	246	÷
134	å	150	û	167	º	183	╖	199	╟	215	╫	231	τ	247	≈
135	ç	151	ù	168	¿	184	╕	200	╚	216	╪	232	Φ	248	°
136	ê	152	ÿ	169	⌐	185	╣	201	╔	217	┘	233	Θ	249	∙
137	ë	153	Ö	170	¬	186	║	202	╩	218	┌	234	Ω	250	·
138	è	154	Ü	171	½	187	╗	203	╦	219	█	235	δ	251	√
139	ï	156	£	172	¼	188	╝	204	╠	220	▄	236	∞	252	⁻
140	î	157	¥	173	¡	189	╜	205	═	221	▌	237	φ	253	²
141	ì	158	₧	174	«	190	╛	206	╬	222	▐	238	ε	254	■
142	Ä	159	ƒ	175	»	191	┐	207	╧	223	▀	239	∩	255	
143	Å	160	á	176	░	192	└	208	╨	224	α	240	≡		

Kriptografi

Kriptografi adalah ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirim pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi dapat memenuhi kebutuhan umum suatu transaksi. Kebutuhan untuk kerahasiaan (*confidentiality*) dengan cara melakukan enkripsi (penyandian). Keutuhan (*integrity*) atas data-data pembayaran dilakukan dengan fungsi hash satu arah.

Jaminan atas identitas dan keabsahan (*authenticity*) pihak-pihak yang melakukan transaksi dilakukan dengan menggunakan password atau sertifikat digital. Sedangkan keotentikan data transaksi dapat dilakukan dengan tanda tangan digital. Transaksi dapat dijadikan barang bukti yang tidak bisa disangkal (*non-repudiation*) dengan memanfaatkan tanda tangan digital dan sertifikat digital.

Pembakuan penulisan pada kriptografi dapat ditulis dalam bahasa matematika. Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan dekripsi. Enkripsi adalah proses mengubah suatu pesan asli (*plaintext*) menjadi suatu pesan dalam bahasa sandi (*ciphertext*).

C = E (M)

dimana

M = pesan asli

E = proses enkripsi

C = pesan dalam bahasa sandi (untuk ringkasnya disebut sandi)

Sedangkan dekripsi adalah proses mengubah pesan dalam suatu bahasa sandi menjadi pesan asli kembali.

M = D (C)

D = proses dekripsi

Umumnya, selain menggunakan fungsi tertentu dalam melakukan enkripsi dan dekripsi, seringkali fungsi itu diberi parameter tambahan yang disebut dengan istilah kunci. Terdapat tiga kategori enkripsi, yaitu: (1) kunci enkripsi rahasia, dalam hal ini terdapat sebuah kunci yang digunakan untuk mengenkripsi dan juga sekaligus mendekripsi informasi, (2) kunci enkripsi publik, menggunakan dua kunci satu untuk proses enkripsi dan satu untuk proses dekripsi, dan (3) fungsi one-way, atau fungsi satu arah adalah suatu fungsi di mana informasi dienkripsi untuk menciptakan "signature" dari informasi asli yang bisa digunakan untuk keperluan autentifikasi.
(Wibowo, 1997)

Model-model enkripsi

1. Enkripsi dengan kunci Pribadi

Enkripsi ini dapat dilakukan jika si pengirim dan si penerima telah sepakat menggunakan kunci dan metode enkripsi tertentu. Metode enkripsi atau kunci yang digunakan harus dijaga agar tidak ada pihak luar yang mengetahuinya. Kesepakatan cara enkripsi atau kunci enkripsi ini bisa dicapai lewat jalur komunikasi lain yang lebih aman, misalnya dengan pertemuan langsung. Cara enkripsi dengan kesepakatan atau kunci enkripsi ini dikenal dengan istilah enkripsi dengan kunci pribadi, karena kunci hanya boleh diketahui oleh dua pribadi yang berkomunikasi tersebut.

Cara enkripsi dengan kunci pribadi umumnya digunakan untuk kalangan bisnis maupun pemerintahan. Beberapa metode yang termasuk dalam enkripsi dengan kunci pribadi antara lain: *subtitution cipher*, *Caesar cipher* (mono alphabetical cipher), *transposition cipher*, *Data Encryption Standard* (DES), *Triplel DES*, *Rivest Code 2 (RC2)* dan *Rivest Code 4 (RC4)*, *IDEA*, *Skipjack*, *Gost Block Cipher*, dan *Poly alphabetical cipher*.

Dari beberapa metode di atas, di dalam pembahasan makalah ini hanya digunakan *poly alphabetical cipher.*

Metode *Poly alphabetical cipher* pada prinsipnya merupakan: (a) satu himpunan yang berhubungan dengan teknik subtitusi *monoalphabetical,* dan (b) sebuah kunci yang ditentukan dengan aturan tertentu dan dipilih untuk transformasi data.

Skema yang digunakan dalam *Poly alphabetical cipher* ini adalah sebuah matriks bujur sangkar yang biasanya disebut Tabel **Viginere**, yaitu :

Tabel 1. Tabel Viginere

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

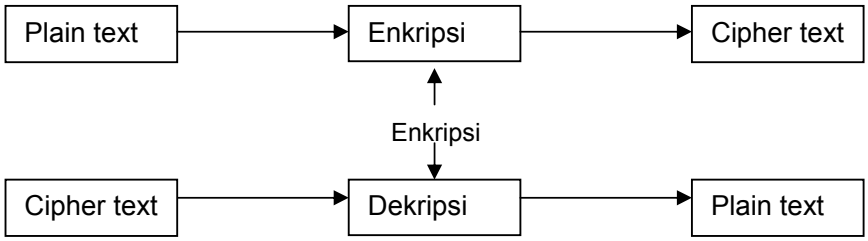
Misal akan dienkripsi pesan “JARINGAN”, dengan kunci “KABEL”, maka akan diperoleh:

Kunci : KABE LKABELK

Plaintext : DATA RAHASIA

*Cipher*text : NAUE CKHBWTK (Stallings, 1995)

Proses enkripsi-dekripsi dengan menggunakan algoritma dari enkripsi kunci pribadi dapat digambarkan sebagai berikut:



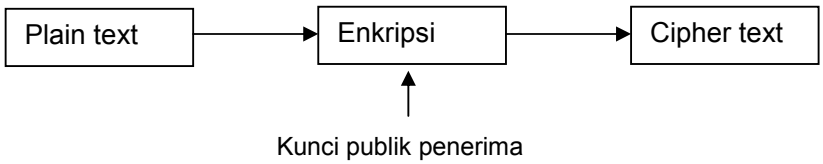
Gambar 1. Algoritma enkripsi dengan kunci pribadi

Dalam algoritma kunci pribadi, kunci digunakan untuk enkripsi data dan tidak diberikan kuasa kepada publik tetapi hanya pada orang tertentu yang tahu dan dapat membaca data yang dienkripsi. Karakteristik dari algoritma kriptografi kunci pribadi adalah bahwa kunci enkripsi sama dengan kunci dekripsi. (Kristanto, 2003)

2. Enkripsi dengan kunci Publik

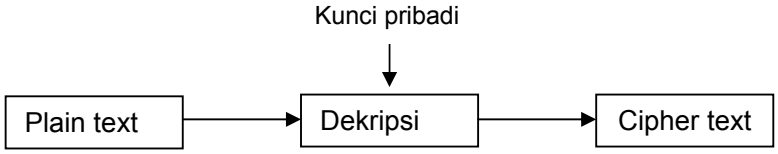
Enkripsi dengan cara ini menggunakan dua kunci yaitu satu kunci pribadi untuk enkripsi dan satu kunci publik untuk dekripsi. Algoritma dari enkripsi kunci publik adalah sebagai berikut :

a. Algoritma enkripsi pengiriman digambarkan dalam skema berikut:



Gambar 2.a. Algoritma Enkripsi Pengiriman

b. Adapun algoritma dekripsi penerimaan seperti skema di bawah ini:



Gambar 2.b. Algoritma Dekripsi Penerimaan

Dalam algorima kunci publik, kunci enkripsi dibuka sehingga tak seorangpun dapat menggunakannya, tetapi untuk dekripsi hanya satu orang yang punya kunci dan dapat menggunakannya. (Kristanto, 2003)

Percobaan dan Pembahasan

Pada artikel ini akan dilakukan percobaan penggunaan digit nilai desimal bilangan e dalam chipher viginere yang diimplementasikan pada kode ASCII.

Dalam metode ini digunakan 256 karakter untuk mengenkripsi data. Awalnya digit decimal dari bilangan e dikelompokkan dalam 3 digit, yang masing-masing kelompok direduksi dalam modulo 256.

e =2.7182818284590452353602874713526624977572470936999595749 6…..

2,	718	281	828	459	045	235	360	287	471	352	662	497	757	247	709	…
2,	206	25	60	173	045	235	104	31	215	96	150	241	245	247	197	…
2.	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8	d_9	d_{10}	d_{11}	d_{12}	d_{13}	d_{14}	d_{15}	…

Misal nilai kunci=3, hal ini menunjukkan kelompok mana yang pertama ditulis dalam baris pertama, yaitu :

Tabel 2. Tabel Matriks Kunci 3

Baris

1	**0**	**1**	**2**		**107**	**108**	**109**	**110**	**111**	**112**	**113**	**114**	**….**	**255**	**256**
2	d_3	d_4	d_5	…	d_{110}	d_{111}	d_{112}	d_{113}	d_{114}	d_{115}	d_{116}	d_{117}		d_{258}	d_{259}
3	d_4	d_5	d_6	…	d_{111}	d_{112}	d_{113}	d_{114}	d_{115}	d_{116}	d_{117}	d_{118}	…	d_{259}	d_{260}
4	d_5	d_6	d_7	…	d_{112}	d_{113}	d_{114}	d_{115}	d_{116}	d_{117}	d_{118}	d_{119}	…	d_{260}	d_{261}
5	d_6	d_7	d_8	…	d_{113}	d_{114}	d_{115}	d_{116}	d_{117}	d_{118}	d_{119}	d_{120}	…	d_{261}	d_{262}
6	d_7	d_8	d_9	…	d_{114}	d_{115}	d_{116}	d_{117}	d_{118}	d_{119}	d_{120}	d_{121}	…	d_{262}	d_{263}
254	d_{255}	d_{z56}	d_{257}	…	d_{259}	d_{260}	d_{261}	d_{259}	d_{260}	d_{261}	d_{262}	d_{263}		d_{510}	d_{511}
	…														

Misalnya akan dikirim pesan **kuswari@uny.ac.id**, karakter k mempunyai nilai numerik 107(kode ASCII). Berdasarkan Tabel 2 di atas. Dari kolom angka 107 di baris pertama berhubungan dengan nilai d_{110} di baris kedua. Untuk karakter u mempunyai nilai numerik 117 (kode ASCII) berhubungan dengan d_{121} di baris ketiga, karakter s mempunyai nilai numerik 115 (kode ASCII) berhubungan dengan d_{120} di baris keempat, karakter w mempunyai nilai numerik 119 (kode ASCII) berhubungan dengan d_{126} di baris kelima dan seterusnya Dengan cara di atas, keseluruhan pesan tersebut dihasilkan tabel sebagai berikut :

Tabel 3.a. Tabel Enkripsi Matriks Kunci 3

k	u	s	w	a	r	i	@	u	n	y	.	a	c	.	i	d
107	117	115	119	97	114	105	64	117	110	121	46	97	99	46	105	100
d_{110}	d_{121}	d_{120}	d_{125}	d_{114}	d_{122}	d_{114}	d_{74}	d_{128}	d_{122}	d_{134}	d_{60}	d_{122}	d_{115}	d_{63}	d_{123}	d_{119}

Baris pertama dari tabel 2 di atas menunjukkan pesan yang akan dienkripsi, baris kedua menunjukkan nilai numerik dalam kode ASCII dari karakter dalam pesan yang akan dienkripsi.

Selanjutnya, nilai masing-masing digit yang dihasilkan (d_{110} d_{120} d_{118}… d_{103}) dikonversikan ke digit nilai desimal bilangan e. Misal untuk nilai d_{110} merujuk pada nilai digit kelompok 3-digit ke 110 dari nilai desimal bilangan e, nilai d_{121} merujuk pada nilai digit kelompok 3-digit ke 121 dari nilai desimal bilangan e dan seterusnya. Secara lengkap hasilnya disajikan pada tabel di bawah ini.

Tabel 3.b. Tabel Enkripsi Kelompok 3-digit

d_{110}	d_{121}	d_{120}	d_{125}	d_{114}	d_{122}	d_{114}	d_{74}	d_{128}	d_{122}	d_{134}	d_{60}	d_{122}	d_{115}	d_{63}	d_{123}	d_{119}
0	709	200	443	826	387	826	89	230	387	692	233	387	560	753	709	113
0	197	200	187	58	131	58	89	230	131	180	233	131	48	241	197	113

Baris ketiga dari tabel 3.b diatas merupakan hasil dari baris kedua yang telah dimodulo 256. Dari baris ketiga tersebut dikonversikan kembali kedalam karakter ASCII sehingga pesan yang terenkripsi menjadi **NULâ╚╗:â:Yµ â┤Θâ0±┼q**

Implementasi cipher viginere pada kode ASCII ini akan menghasilkan suatu deretan karakter yang tidak mudah untuk ditebak. Jika pada cipher viginere yang diterapkan hanya untuk deretan 26 alfabet, salah satu contohnya adalah 'spasi' tidak dikodekan menjadi suatu bilangan atau karakter, sehingga cenderung lebih mudah untuk ditebak, tetapi pada kode ASCII ini semua simbol, spasi, operator dan sebagainya dapat dikodekan menjadi suatu bilangan, maka kemungkinan untuk menebak(mendekripsi) oleh orang yang tidak berhak akan menjadi lebih sulit.

Kesimpulan

Implementasi cipher viginere pada kode ASCII memberikan kemungkinan yang luas pada lebih banyak karakter yang tercakup, tidak hanya terbatas pada 26 alfabet, tetapi juga mencakup karakter-karakter seperti . ,", ',= dan sebagainya.

Keunikan digit desimal dari bilangan Euler (biasa disebut bilangan e) dapat digunakan sebagai acuan penerapan algoritma yang ada di kajian kriptografi, yang salah satunya adalah cipher viginere. Hal ini dengan pertimbangan bahwa pembangkitan bilangan/kode acuan dapat diperoleh dari formulasi perhitungan digit desimal bilangan Euler yang sudah mapan dan diakui dunia.

Deretan digit dari nilai desimal bilangan e untuk implementasi enkripsi-dekripsi dengan cara pengelompokan digitnya, sangat kecil kemungkinannya menghasilkan nilai rujukan yang sama

Daftar Pustaka

1. Stallings, William, *Network and Internetwork Security*, Pentice Hall, New Jersey, 1995
2. Kristanto, Andri, *Keamanan data pada Jaringan Komputer*, Gava Media, 2003
3. Dence, Thomas P and Heath, Steven, *Using Pi in Cryptology*, Math Computing Education 39 no 1 winter 2005, Wilson Company, 2005
4. O'Connor JJ and Robertson, E F, *History topic : The Number of e*, 2001, http://www-groups.dcs.st-and.ac.uk/history/printHT/e.html
5. Levy, Silvio*,AffineTransformation,*1995, *http://www.geom.uiuc.edu/docs/reference/CRC-formulas/figshear*,
6. Savard, John J.G, *The Hill Cipher*,1999. http://home.ecn.ab.ca/%7Ejsavard/crypto/ro020103.htm
7. Wibowo, Arrianto Mukti, *Studi Perbandingan Sistem-sistem Perdagangan di Internet dan Desain Protokol Cek Bilyet Digital* ,Universitas Indonesia,1997 http://www.geocities.com/amwibowo/resource.html
9. Martyn Parker, *Gifted and Talented Enhancement Course:Codes and Ciphers* Mathematics Institute University of Warwick, 2005
10. Sami Dahlman, *Key management schemes in multicast environments* University of Tampere Department of Computer Science Pro gradu Thesis, 2001