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

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 Phi 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 Phi yang sudah mapan dan diakui dunia.

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

Kata kunci : Phi, 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 Phi 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 Phi yang sudah mapan dan diakui dunia.

Bilangan Phi

Cara untuk menemukan bilangan phi adalah dengan menentukan penyelesaian dari persamaan $x^2 - x - 1 = 0$, dimana akar-akarnya diperoleh

$$x = \frac{1+\sqrt{5}}{2} \sim 1.618... \text{ or } x = \frac{1-\sqrt{5}}{2} \sim -.618...$$

Akar yang pertama itulah bilangan Phi, dalam bahasa latin disimbulkan dengan Φ (huruf latin kapital) dan akar yang kedua disebut bilangan ~phi, yang disimbulkan ϕ (huruf latin kecil).

Bilangan Phi mempunyai nilai desimal yang tak terhingga banyaknya. Berikut ini adalah nilai Phi yang mempunyai nilai desimal sampai dengan digit ke 1000

```
1·61803 39887 49894 84820 45868 34365 63811 77203 09179 80576   50
  28621 35448 62270 52604 62818 90244 97072 07204 18939 11374  100
  84754 08807 53868 91752 12663 38622 23536 93179 31800 60766
  72635 44333 89086 59593 95829 05638 32266 13199 28290 26788  200
  06752 08766 89250 17116 96207 03222 10432 16269 54862 62963
  13614 43814 97587 01220 34080 58879 54454 74924 61856 95364  300
  86444 92410 44320 77134 49470 49565 84678 85098 74339 44221
  25448 77066 47809 15884 60749 98871 24007 65217 05751 79788  400
  34166 25624 94075 89069 70400 02812 10427 62177 11177 78053
  15317 14101 17046 66599 14669 79873 17613 56006 70874 80710  500

  13179 52368 94275 21948 43530 56783 00228 78569 97829 77834
  78458 78228 91109 76250 03026 96156 17002 50464 33824 37764
  86102 83831 26833 03724 29267 52631 16533 92473 16711 12115
  88186 38513 31620 38400 52221 65791 28667 52946 54906 81131
  71599 34323 59734 94985 09040 94762 13222 98101 72610 70596
  11645 62990 98162 90555 20852 47903 52406 02017 27997 47175
  34277 75927 78625 61943 20827 50513 12181 56285 51222 48093
  94712 34145 17022 37358 05772 78616 00868 83829 52304 59264
  78780 17889 92199 02707 76903 89532 19681 98615 14378 03149
  97411 06926 08867 42962 26757 56052 31727 77520 35361 39362 1000
```

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
0	NUL
1	SOH
2	STX
3	ETX
4	EOT
5	ENQ
6	ACK

Desimal	Karakter
32	Space
33	!
34	“
35	#
36	$
37	%
38	&

Desimal	Karakter
64	@
65	A
66	B
67	C
68	D
69	E
70	F

Desimal	Karakter
96	`
97	a
98	b
99	c
100	d
101	e
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	_	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

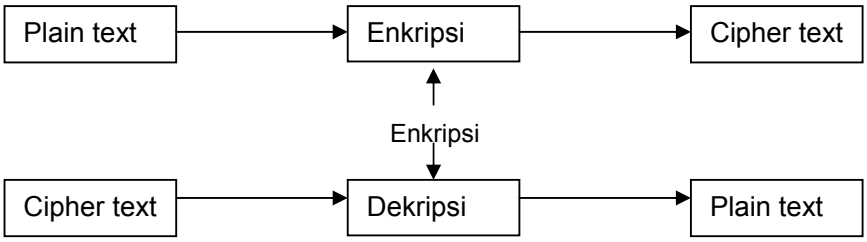
Misal akan dienkripsi pesan “JARINGAN”, dengan kunci “KABEL”, maka akan diperoleh:

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:



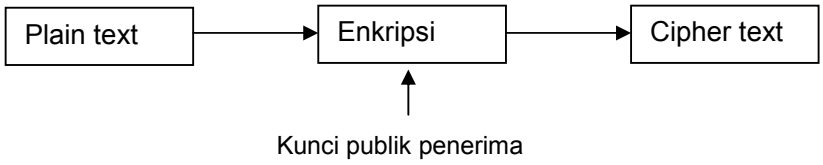
Gambar 1. Algoritma enkripsi dengan kunci pribadi

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

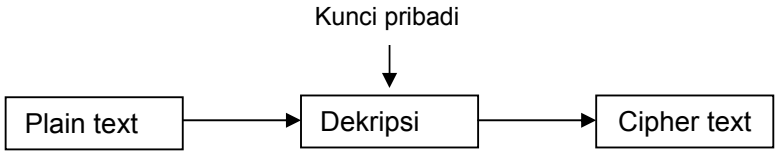
Enkripsi dengan cara ini menggunakan dua kunci yaitu satu kunci pribadi untuk enkripsi dan satu kunci publik untuk dekripsi. Algoritma dari enkripsi kunci publik adalah sebagai berikut :

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 Phi dalam chipher viginere yang diimplementasikan pada kode ASCII.

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

e =1·61803 39887 49894 84820 45868 34365 63811 77203 09179 80576…..

1,	618	033	988	749	894	848	204	586	834	365	638	117	720	309	179	…
1,	106	33	220	237	126	80	204	74	66	109	127	117	208	53	179	…
1.	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_{256}	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 Phi. Misal untuk nilai d_{110} merujuk pada nilai digit kelompok 3-digit ke 110 dari nilai desimal bilangan Phi, nilai d_{121} merujuk pada nilai digit kelompok 3-digit ke 121 dari nilai desimal bilangan Phi 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}
565	478	066	749	874	091	874	696	400	091	834	638	091	339	319	588	877
53	222	66	237	106	91	106	184	144	91	66	126	91	83	63	76	109

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 **5 ▌Bϕj[j ╕ Ė[B~[S?Lm**

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