B 3

ISBN :979-99529-0-5

Seminar Nasional 2005

PROSIDING

SURAKARTA, 7 Mei 2005

SEMINAR NASIONAL MATEMATIKA DAN INFORMATIKA

APLIKASI MATEMATIKA DAN TEKNOLOGI INFORMASI PADA PENGEMBANGAN INDUSTRI

terselenggara atas kerjasama

PUSKOM UNS

TELKOM INDONESIA

Program D3 Ilmu Komputer FMIPA

JURUSAN MATEMATIKA FAKULTAS MIPA
UNIVERSITAS SEBELAS MARET
SURAKARTA
2005

PEMANFAATAN KEUNIKAN DIGIT DESIMAL BILANGAN EULER PADA KRIPTOGRAFI

Kuswari Hernawati
Bambang Sumarno HM

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

ABSTRAK

Banyaknya transfer data di dalam jaringan menjadi alasan perlu adanya keamanan data di dalamnya. Salah satu cara yang ditempuh adalah melakukan transformasi data yang dikirimkan. Untuk melakukan transformasi data tersebut, di bidang ilmu Matematika telah berkembang kajian yang dikenal dengan kriptografi. Kriptografi merupakan sistem transformasi data yang mempunyai fungsi/fitur berkaitan dengan konfidensial (menjamin kerahasiaan data), integritas pesan (menjamin tidak terjadi perubahan pesan), nonrepudiasi, (menjamin kepemilikan dokumen) dan otentifikasi (menjamin keaslian pesan dan uji identitas pengguna sistem).

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 cara pengelompokan digitnya, sangat kecil kemungkinannya menghasilkan nilai rujukan

Kata kunci : Euler, transformasi data, kriptografi

1. Latar Belakang

Perkembangan teknologi jaringan komputer yang memungkinkan perbedaan platform sistem yang digunakan semakin tidak menjadi kendala. Hal ini disebabkan telah adanya kesepakatan penggunaan protokol (TCP/IP) yang dapat diimplementasikan pada setiap sistem yang ada.

Di sisi lain, perkembangan yang menggembirakan ini sedikit banyak berdampak pada penjaminan keamanan data. Hal ini disebabkan perlu adanya "biaya" yang harus dibayar terhadap penyesuaian di dalam implementasi protokol jaringan dari sistem-sistem yang berbeda.

Banyaknya transfer data di dalam jaringan menjadi alasan perlu adanya keamanan data di dalamnya. Salah satu cara yang ditempuh adalah melakukan transformasi data yang dikirimkan. Transformasi ini terutama untuk mengatasi masalah privasi (privacy) dan keotentikan (authentication). Adanya penanganan masalah privasi menjadikan data yang dikirim hanya dapat dimengerti informasinya oleh penerima yang berhak. Adapun keotentikan dapat mencegah pihak yang tidak berhak tidak dapat melakukan manipulasi terhadap data yang dikirimkan.

Untuk melakukan transformasi data seperti di atas, di bidang ilmu Matematika telah berkembang kajian yang dikenal dengan kriptografi. Kriptografi merupakan sistem transformasi data yang mempunyai fungsi/fitur berkaitan dengan konfidensial (menjamin kerahasiaan data), integritas pesan (menjamin tidak terjadi perubahan pesan), nonrepudasi, (menjamin kepemilikan dokumen) dan otentifikasi (menjamin keaslian pesan dan uji identitas pengguna sistem).

Pada makalah ini akan dibahas pemanfaatan keunikan digit desimal dari bilangan Euler (biasa disebut bilangan e) 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.

2. 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.

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

Pada tahun 1748 , Euler memberikan ide mengenai bilangan e yaitu

$e = 1 + 1/1! + 1/2! + 1/3! + 1/4! + \ldots$. dan bahwa $e = \lim_{n\to\infty}(1+\frac{1}{n})^n$. 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=2.7182818284590452353602874713526624977572470936999595749669676277240766303535475945713821785251664274274663919320030599218174135966290435729003342952605956307381323286279434907632338298807531952510190115738341879307021540891499348841675092447614606680822648001684774118537423454424371075390777449920695517027 61.....

3. Kriptografi

Kriptografi adalah ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirim pengirim dapat disampaikan kepada penerima dengan aman [Schneier,1996]. 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. Sedang-kan keotentikan data transaksi dapat dilakukan dengan tanda tangan digital. Tran-saksi 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)

4. Model-model enkripsi

4. 1. Enkripsi dengan kunci Pribadi

Enkripsi ini dapat dilakukan jika si pengirim dan si penerima telah sepakat meng-gunakan 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 dua metode yaitu *Caesar cipher* dan *poly alphabetical cipher*.

Metode Caesar cipher digunakan oleh Julius Caesar untuk berkomunikasi dengan tentaranya. Caesar memutuskan menggeser setiap huruf dalam pesan yang akan menjadi algorima standar, sehingga dapat menginformasikan semua keputusannya dan kemudian mengirim pesan ini dalam bentuk yang aman. Sebagai contoh, tabel karakter sandi merupakan kelipatan tiga dari tabel karakter aslinya :

Karakter asli : 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

Karakter sandi : 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

Berdasarkan tabel karakter di atas, huruf a akan diganti dengan huruf d, huruf b diganti dengan huruf e, dan seterusnya. (Kristanto, 2003)

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

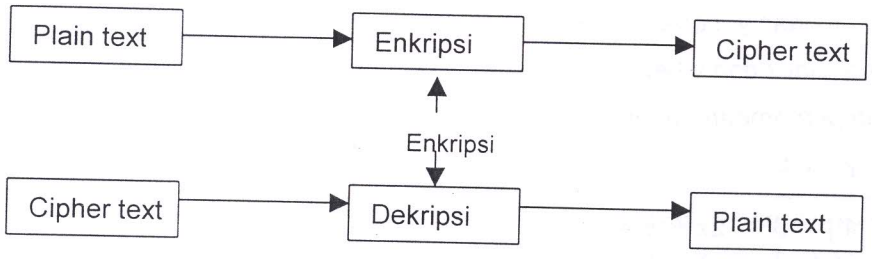
Misal akan dienkripsi pesan "JARINGAN", dengan kunci "KABEL", maka akan diperoleh:

Kunci : KABELKAB

Plaintext : JARINGAN

*Cipher*text : TAQMCWAM (Stallings, 1995)

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



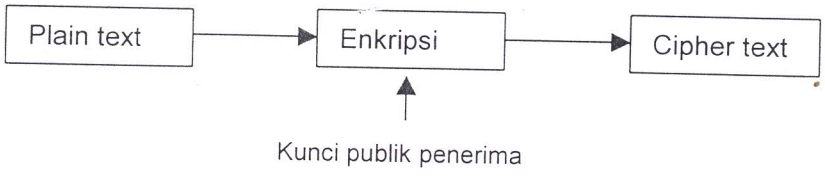
Gambar 1. Algoritma enkripsi dengan kunci pribadi

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)

4.2. Enkripsi dengan kunci Publik

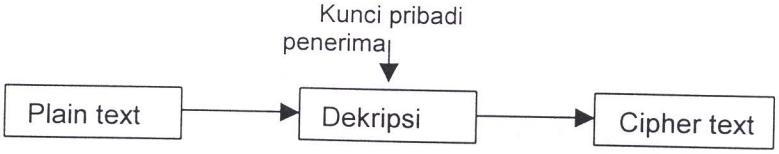
Enkripsi dengan cara ini menggunakan dua kunci yaitu satu kunci pribadi untuk enkripsi dan satu kunci publik untuk dekripsi. Algoritma dari enkripsi kunci publik adalah sebagai berikut :

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)

5. Cipher Hill

Misal diberikan masalah, sebagai berikut

$2x + y = a$ dan $x - y = b$ ... (1a)

Untuk memperoleh enkripsi dalam hill cipher sama artinya dengan mencari nilai a dan b dalam x dan y, sedangkan dekripsi adalah mencari nilai x dan y dalam a dan b; Dimana nilai x dan y berkisar dari 0 sampai dengan 25.

Dari persamaan 1a, dibawa ke bentuk matriks berikut:

```
 x y  a b
-------------
 2 1 | 1 0    2x + y = a
 1 -1 | 0 1     x - y = b
```

Proses pencari nilai x dan y dilakukan seperti pencarian invers.

x	y		a	b	
3	0	|	1	1	3x = a+ b
1	-1	|	0	1	x – y = b

3	0	|	1	1	3x = a+ b
-3	3	|	0	-3	-3x + 3y = -3b

3	0	|	1	1	3x = a+ b	
0	3	|	1	-2	3y = b	.....(1b)

Dari hasil tahap terakhir (persamaan 1b) nilai x dan y diperoleh dengan cara masing-masing baris dikalikan dengan 1/3. (Savard,1999)

6. Tranformasi Affine

Transformasi Affine adalah sebuah transformasi yang memetakan garis paralel ke garis paralel lainnya (paralelisme). Ada dua hal penting dalam tranformasi, yaitu :

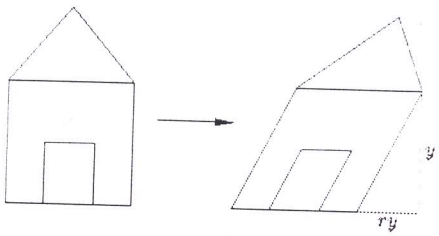
1. Transformasi skala yang tidak proporsional berpusat pada titik awal, dan mempunyai bentuk $(x,y) \rightarrow (ax,by)$, dengan $a,b \neq 0$ adalah faktor skala (bilangan real). Adapun hubungan matriks dalam koordinat homogennya adalah:

$$H_{a,b} = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

2. Garis horisontal yang memotong pada titik (x, y) berbentuk $(x,y) \rightarrow (x+ry,y)$, dengan r adalah faktor perpotongan (seperti diperlihatkan Gambar 3).

Hubungan matriks yang bersesuaian dalam koordinat homogennya adalah:

$$S_r = \begin{bmatrix} 1 & r & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$



Gambar 3: Suatu perpotongan dengan r=½.

Setiap transformasi Affine diperoleh dengan mengkomposisikan transformasi skala dengan isometri atau perpotongan dengan homotheti dan isometri. (Levy,1995)

7. Percobaan dan Pembahasan

Pada makalah ini akan dilakukan percobaan penggunaan digit nilai desimal bilangan e dalam kriptografi. Ada empat cara yang akan digunakan dalam enkripsi kunci pribadi.

7.1. Variasi dari Caesar *cipher.*

Misalkan akan dikirim sebuah pesan "KEAMANAN JARINGAN" pada tanggal 1 Maret. Penggunaan kode sederhana A↔1, B↔2, C↔3, D↔4, ... Z↔26, spasi ↔27 atau 0 (mod 27), maka pesan akan menjadi barisan dari 17 numerik yang merupakan *plaintext*, yaitu : 11 5 1 13 1 14 1 14 0 10 1 18 9 14 7 1 14.

Tanggal 1 maret dijadikan sebagai kunci, yang ditulis dalam bentuk 0103, yang artinya bahwa kunci dari enkripsi adalah 17 digit mulai dari digit ke 103 dari nilai desimal bilangan e, yaitu mulai dari 4 6 6 3 9 1 9 3 2 0 0 3 0 5 9 9 2 . Nilai ini selanjutnya tambahkan ke *plaintext* sebagai berikut:

11	5	1	13	1	14	1	14	0	10	1	18	9	14	7	1	14
4	6	6	3	9	1	9	3	2	0	0	3	0	5	9	9	2
15	11	7	16	10	15	10	17	2	10	1	21	9	19	16	10	16

Berdasarkan nilai numerik *ciphertext* di atas, selanjutnya dikonversikan ke string yang akan menghasilkan pesan "OKGPJOJQBJAUISPJP". Untuk mengembalikan pesan ke bentuk aslinya, maka dikonversi ke bentuk bilangan dan dikurangi dengan digit bilangan e mulai dari digit ke 103.

7.2. Variasi dari Transformasi Affine

Pada tranformasi affine diperlukan dua buah kunci, misal kunci 1 dan kunci 2. Andaikan a merupakan nilai dari digit ke (x+1) yang lokasinya ditunjuk oleh kunci 1 (yaitu: x), sedang b merupakan nilai dari digit ke (x+y+1) yang lokasinya dirujuk oleh kunci 2 (yaitu: y). Berdasarkan kedua nilai digit tersebut, maka *Cipher*text (C) dan *Plaintext* (P) dihubungkan berdasarkan persamaan: $C = aP + b \pmod{27}$.

Misal diberikan kunci 1 = 3 dan kunci 2 = 11, maka a = nilai dari digit ke (3+1)= 2 dan b = nilai dari digit ke (3+11+1) = 2. Sehingga diperoleh persamaan :

$$C = (2P + 2) \pmod{27} \quad \ldots (2)$$

Andaikan pesan yang akan dikirm adalah "KEAMANAN JARINGAN", maka *plaintext* dalam barisan integer dinyatakan dengan 11 5 1 13 1 14 1 14 0 10 1 18 9 14 7 1 14 yang selanjutnya akan dienkripsi berdasarkan persamaan 2 di atas sebagai berikut:

24 12 4 28 4 30 4 30 2 22 4 38 20 30 16 4 30 (nilai 2P+2), yang selanjutnya dimoduluskan dengan angka 27 sebagai berikut:

24 12 4 1 4 3 4 3 2 22 4 11 20 3 16 4 3 (mod 27)

Hasil enkripsi ini dalam bentuk string adalah "XLDADCDCBVDKTCPDC".

Untuk mendekripsikan hasil enkripsi di atas, string dikembalikan ke dalam bentuk numerik, dimana masing-masing digit dikurangi dengan 2 dan selanjutnya dibagi dengan 2.

7.3. Variasi dari metode Hills

Cara enkripsi-dekripsi di dalam metode Hills menggunakan matriks bujur sangkar, misal matriks 3x3. Contoh dipilih kunci = 4, maka elemen matriks diambil mulai dari digit ke 4 dari nilai desimal bilangan e, e=2.71828182845904523536028747135 2 ..., yaitu:

$$M = \begin{bmatrix} 2 & 8 & 1 \\ 8 & 2 & 8 \\ 4 & 5 & 9 \end{bmatrix}$$

Mengambil dari nilai *plaintext* di atas, digitnya dikelompokkan yang mana anggotanya terdiri dari 3 elemen, maka diperoleh kelompoknya adalah (11 5 1), (13 1 14), (1 14 0), (10 1 18), (9 14 7), dan (1 14 0). Adapun spasi ditambahkan sebagai anggota untuk kelompok terakhir yang anggotanya kurang dari 3 elemen, sehingga diperoleh *cipher*text untuk kelompok pertama (11 5 1) adalah:

$$\begin{bmatrix} 2 & 8 & 1 \\ 8 & 2 & 8 \\ 4 & 5 & 9 \end{bmatrix} \begin{bmatrix} 11 \\ 5 \\ 1 \end{bmatrix} = \begin{bmatrix} 63 \\ 106 \\ 78 \end{bmatrix}$$

Untuk kelompok kedua (13 1 14) dihasilkan chipertextnya:

$$\begin{bmatrix} 2 & 8 & 1 \\ 8 & 2 & 8 \\ 4 & 5 & 9 \end{bmatrix} \begin{bmatrix} 13 \\ 1 \\ 14 \end{bmatrix} = \begin{bmatrix} 259 \\ 104 \\ 88 \end{bmatrix}$$

Untuk kelompok tiga (1 14 0) sampai dengan kelompok enam (1 14 0) dihasilkan chipertextnya:

$$\begin{bmatrix} 155 \\ 78 \\ 23 \end{bmatrix}, \begin{bmatrix} 141 \\ 303 \\ 24 \end{bmatrix}, \begin{bmatrix} 201 \\ 212 \\ 252 \end{bmatrix} \text{dan} \begin{bmatrix} 141 \\ 28 \\ 252 \end{bmatrix}$$

Sehingga *cipher*text yang dihasilkan keseluruhan adalah

63 106 78 259 104 88 155 78 23 141 303 24 201 212 252 141 28 252

Dari hasil enkripsi di atas, untuk mendekripsikan kembali ke bentuk asli maka kelompok 3 elemen dikalikan dengan M^{-1} , yaitu sebagai berikut :

$$M^{-1} \cdot \begin{bmatrix} 63 \\ 106 \\ 78 \end{bmatrix} = \begin{bmatrix} 11 \\ 5 \\ 1 \end{bmatrix} \text{ dan seterusnya.}$$

7.4. Metode enkripsi dengan Tabel "Bujur Sangkar" Viginere

Dalam metode ini digunakan 26 alfabet untuk mengenkripsi data. Awalnya digit dibelakang koma dari bilangan e dikelompokkan dalam 2 digit, yang masing-masing kelompok direduksi dalam modulo 27.

e =2.71828182845904523536028747135266249775724709369995957496.....

2,	71	82	81	82	84	59	04	52	35	36	02	87	47	13	52	66	...
2,	71	01	0	01	03	05	04	25	08	09	02	06	20	13	15	12	...
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}	d_{16}	

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

Tabel 2. Tabel Matriks Kunci 3

0	1	2	3	4	5	6	7	8	9	10	11	12	13	....	25	26
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}	d_{16}		d_{29}	d_{30}
d_4	d_5	d_6	d_7	d_8	d_9	d_{10}	d_{11}	d_{12}	d_{13}	d_{14}	d_{15}	d_{16}	d_{17}	...	d_{30}	d_{31}
d_6	...															

...															

Dari pesan "KEAMANAN JARINGAN", huruf K mempunyai bentuk numerik 11 (urutan alfabetik). Berdasarkan Tabel 2 di atas. Dari kolom angka 11 di baris pertama berhubungan dengan nilai d_{14} di baris kedua. Untuk huruf E mempunyai bentuk numerik 5 (urutan alfabetik) berhubungan dengan d_9 di baris ketiga, dan seterusnya Dengan cara di atas, keseluruhan pesan tersebut dihasilkan tabel sebagai berikut :

Tabel 3.a. Tabel Enkripsi Matriks Kunci 3

K	E	A	M	A	N	A	N		J	A	R	I	N	G	A	N
d_{14}	d_9	d_6	d_{19}	d_8	d_{22}	d_{10}	d_{24}	d_{11}	D_{22}	d_{14}	d_{32}	d_{24}	d_{30}	d_{24}	d_{19}	d_{33}

Selanjutnya, nilai masing-masing digit yang dihasilkan (d_{14} d_9 d_6... d_{33}) dikonversikan ke digit nilai desimal bilangan e. Misal untuk nilai d_{14} merujuk pada nilai digit kelompok 2-digit ke 14 dari nilai desimal bilangan e. Secara lengkap hasilnya disajikan pada tabel di bawah ini.

Tabel 3.b. Tabel Enkripsi Kelompok 2-digit

d_{14}	d_9	d_6	d_{19}	d_8	d_{22}	d_{10}	d_{24}	d_{11}	d_{22}	d_{14}	d_{32}	d_{24}	d_{30}	d_{24}	d_{19}	d_{33}
13	8	3	21	25	9	9	18	2	9	13	8	18	15	18	21	23

Sehingga pesan yang terenkripsi menjadi "MHCUYIIRBIMHRORUW".

8. Kesimpulan dan Saran

Keunikan digit desimal dari bilangan Euler (biasa disebut bilangan e) dapat digunakan sebagai acuan penerapan 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 cara pengelompokan digitnya, sangat kecil kemungkinannya menghasilkan nilai rujukan.

Penggunaan nilai digit dari nilai desimal bilangan e, terdapat sedikit kelemahan. Implementasi dengan menggunakan metode Tabel "Bujur Sangkar" Viginere, yaitu ada kemungkinan dua kelompok d yang berbeda mempunyai nilai yang sama (seperti terlihat pada Tabel 3.b. untuk kelompok d_{22} dan d_{10} bernilai 9).

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. Schneier Bruce, *Applied Cryptography, 2nd ed.;* John Wiley & Sons, Inc., New York 1996.

8. 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