KNM XIX
Universitas Brawijaya Malang, 24-26 Juli 2018

PENGEMBANGAN KRIPTOGRAFI: PENYANDIAN PESAN TEKS MELALUI SEBUAH PEMETAAN 2-DIMENSI YANG DAPAT DIBALIK, SIMETRI, DAN PERIODIK

L. Zakaria[1]

[1]Jurusan Matematika, Fakultas MIPA, Universitas Lampung, Indonesia
e-mail: lazakaria.1969@fmipa.unila.ac.id

Kata Kunci: Kriptografi, pemetaan periodik 2-dimensi, Mathematica

Abstrak. *Terdapat sejumlah cara/metode dan pendekatan untuk bekerja dengan sistem kriptografi. Dengan kriptografi diharapkan keamanan pesan yang meliputi aspek kerahasiaan, integritas data, serta otentikasi terjaga dengan baik. Algoritma enkripsi-dekripsi dengan menggunakan sebuah pemetaan (*mapping*) pernah dilakukan terhadap sebuah citra, misalnya pemetaan* Arnold Cat Map *(ACM). Dalam artikel ini akan diberikan sebuah algoritma enkripsi-dekripsi terhadap sebuah pesan teks melalui pendekatan yang dilakukan dengan melibatkan sebuah pemetaaan non linear 2-dimensi yang bersifat dapat dibalik, simetri, dan periodik. Algoritma enkripsi-dekripsi dan pemrograman dengan menggunakan* Mathematica *yang disampaikan dalam artikel ini merupakan sebuah studi kasus terhadap penggunaan pemetaan nonlinear 2-dimensi dapat dibalik-simetri-periodik yang diturunkan dari sebuah pemetaan nonlinear 2-dimensi $\Delta\Delta$-sine Gordon.*

1 PENDAHULUAN

Upaya memberi rasa aman pada penanganan file data digital (teks dan citra, misalnya) umumnya dengan menggunakan penyandian (kriptografi) atau dengan cara ”menyembunyikan” file data tersebut. Saat ini diketahui ada sejumlah cara/metode penyandian yang diklasifikasikan ke dalam dua jenis kunci, kunci simetris dan kunci asimetris [1].
Sebuah algoritma penyandian dikatakan efesien dan efektif dalam mengamankan data dari penanganan pihak-pihak yang tidak semestinya menggunakan data tersebut adalah ketika algoritma tersebut selain relatif sederhana diimplementasikan ke dalam sebuah pemrograman komputer dan menghasilkan tingkat kesulitan yang tinggi dalam menemukan kunci dekripsi baik kunci simetris maupun asimetris. Untuk kajian kunci asimetris (kunci publik) kriptografi yang didasari pada komputasi logaritma diskrit dengan tingkat kesulitan tinggi dapat dilihat pada artikel ElGamal (1985) dan artikel-artikel pada referensinya [2].
Diantara metode penyandian kriptografi yang populer, terdapat metode penyandian kriptografi yang melibatkan sebuah pemetaan (*map*). Untuk penyandian pada sebuah citra misalnya, Rinaldi (2012) telah memperkenalkan pemakaian pemetaan linear *Arnold Cat Map* (ACM) [3]. Sedangkan, Arinten dan Hidayat (2017) menggunakan pemetaan Logistik (*Logistic Map*). Demikian juga dengan Ronsen, Arwin, dan Indra (2014), mereka menggunakan ACM dan *Nonlinear Choatic Algorithm* (NCA) dalam melakukan penyandian untuk sebuah citra [4, 5]. Dengan demikian sebuah pemetaan dapat digunakan sebagai sarana membangun penyandian kriptografi untuk sebuah data digital (citra).
Terhadap data digital teks, algortima kriptografi yang cukup populer digunakan adalah algoritma kunci publik (*public key*) yang biasa disebut kunci asimetris, misalnya kunci publik ElGamal [6]. Sedangkan penggunaan sebuah pemetaan untuk algoritma kriptografi data teks belum banyak dipublikasikan.
Dalam artikel ini, akan dibahas tentang penggunaan pemetaan dalam algoritma kriptografi untuk data teks. Pilihan pemetaan yang digunakan adalah sebuah pemetaan nonlinear 2-dimensi yang memiliki sifat periodik, dapat dibalik (*reversible*), dan mengawetkan ukuran (*measure preserving*). Pemetaan sejenis ini, satu diantaranya adalah pemetaan yang diturunkan dari sebuah persamaan *traveling wave solution* $\Delta\Delta$-sine Gordon yang diperumum [7].
Artikel ini dibagi ke dalam 4 (empat) bagian. Pada bagian pertama diberikan sebuah ilustrasi algoritma deskriptif untuk penyandian kriptografi data teks dengan menggunakan sebuah pemetaan nonlinear periodik 2-dimensi. Pada bagian kedua, dalam bentuk studi kasus, dibahas tentang algoritma kriptografi data teks menggunakan pemetaan 2-dimensi yang diturunkan dari persamaan *traveling wave solution* $\Delta\Delta$-sine Gordon yang diperumum. Dalam bagian ketiga diberikan implementasi algoritma kriptografi data teks ke dalam bahasa pemrograman *Mathematica*. Pada bagian keempat, kesimpulan, dideskripsikan secara ringkas hasil-hasil yang diperoleh dalam bagian sebelumnya.

2 ALGORITMA DESKRIPTIF KRIPTOGRAFI TEKS MENGGUNAKAN PEMETAAN NONLINEAR PERIODIK 2-DIMENSI: SEBUAH ILUSTRASI

Pandang sebuah pemetaan nonlinear berikut:

$$\boldsymbol{\gamma}_{n+1} = \boldsymbol{f}_{\lambda}(\boldsymbol{\gamma}_n) \tag{1}$$

dimana

$$\begin{array}{rccc} \boldsymbol{f}_{\lambda}: & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & (x,y) & \longmapsto & \left(\dfrac{\lambda}{y}, x\right). \end{array}$$

Dapat diperiksa bahwa persamaan (1) merupakan sebuah pemetaan nonlinear 4-periodik dengan nilai parameter λ ditetapkan sebarang tetapi tidak nol.
Misalkan teks:
`Sebagai ungkapan rasa syukur kehadirat Allah, seharusnya kita banyak berbuat amal kebaikan.`
akan dilakukan penyandian dengan menggunakan pemetaan (1) yang kunci simetrisnya dipilih dari parameter λ. Secara deskriptif, algoritma kriptografi untuk contoh teks seperti ini dapat dilakukan dengan cara berikut.

Tahapan Enkripsi

1. Kelompokan Teks menjadi dua bagian, misalkan bagian $x(n)$ dan $y(n)$ dengan $n \in \mathbb{N}$ adalah nilai data numerik yang berasosiasi dengan data teks. Dan asumsikan panjang data teks l adalah sama yakni $l(x) = l(y) = m \in \mathbb{N}$.
2. Lakukan konversi data teks ke data numerik. Kode ASCII dapat digunakan atau menggunakan pengkodean yang dibuat sendiri.
3. Lakukan proses iterasi pemetaan sebanyak r kali dengan ketentuan $f^0 < f^r < f^p; r, p \in \mathbb{N}$ dengan $p = periode$.
4. Pilih nilai parameter $\lambda \neq 0$ dan jadikan sebagai nilai kunci.

Tahapan Dekripsi

1. Pergunakan kembali nilai parameter $\lambda \neq 0$ yang merupakan nilai kunci pada saat enkripsi.
2. Lakukan proses iterasi pemetaan yang diberikan hingga mencapai iterasi ke-p, yaitu $f^p; p \in \mathbb{N}$ dengan $p = periode$.
3. Lakukan konversi data numerik ke dalam data teks.
4. Selesai.

Implementasi algoritma deskriptif di atas dengan menggunakan *Matheamtica* diberikan dalam bagian berikutnya.

3 KRIPTOGRAFI TEKS MENGGUNAKAN PEMETAAN PERIODIK: STUDI KASUS PEMETAAN 2-DIMENSI YANG DITURUNKAN DARI PERSAMAAN $\Delta\Delta$-Sine GORDON YANG DIPERUMUM

3.1 Formulasi Pemetaan Periodik 2-Dimensi yang Diturunkan dari Persamaan $\Delta\Delta$-sine Gordon yang Diperumum

Pandang persamaan diskrit 3-parameter berikut ini.

$$\theta_1 \left(V_{n+z_2} V_{n+z_1} - V_{n+z_1+z_2} V_n\right) + \theta_2 V_{n+z_1+z_2} V_{n+z_2} V_{n+z_1} V_n = \theta_3 \tag{2}$$

Persamaan (2) disebut persamaan *Traveling Wave Solution* $\Delta\Delta$-Sine Gordon yang diperumum [7]. Pilih $z_1 = 1$, $z_2 = 2$, $\theta_1 = \mu\theta_2$, $\theta_3 = \kappa\theta_2$. Maka persamaan (2) menjadi sistem persamaan diskrit berikut:

$$\boldsymbol{\gamma}_{n+1} = \boldsymbol{g}_{\mu,\kappa}(\boldsymbol{\gamma}_n) \tag{3}$$

dimana

$$\begin{array}{rccc} \boldsymbol{g}_{\mu,\kappa}: & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & (x,y) & \longmapsto & \left(\dfrac{x\left(\kappa-\mu x\right)}{y\left(x-\mu\right)}, x\right). \end{array}$$

Pemetaan-pemetaan dalam (3) memiliki integral yakni

$$G_{(\mu,\kappa)}(x,y) = \mu\left(\frac{x}{y}+\frac{y}{x}\right) - (x+y) - \kappa\left(\frac{1}{x}+\frac{1}{y})\right). \tag{4}$$

Pemetaan-pemetaan (3) memiliki sifat-sifat:

- Terdapat sebuah *reversing symmetry* L sedemikian sehingga $L \circ \boldsymbol{g}_{(\mu,\kappa)} \circ L^{-1} = \boldsymbol{g}^{-1}_{(\mu,\kappa)}$. Dengan kata lain, sistem dinamik (3) adalah $reversible$ karena terdapat L sedemikian hingga $g_{(\mu,\kappa)} \circ L \circ g_{(\mu,\kappa)} = L$.
- Terdapat *manifold* $\mathfrak{M} = \{(\mu,\kappa)\,|\mu^2 - \kappa = 0\}$ sedemikian hingga pada setiap titik pada *manifold*, berlaku

$$g^6_{(\mu,\kappa)}\,(x,y) = (x,y) \tag{5}$$

Dari sifat yang terakhir ini, dapat diturunkan sebuah pemetaan 6-periodik berikut ini:

$$\begin{array}{rccc} \boldsymbol{g}_{\lambda}: & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & (x,y) & \longmapsto & \left(\lambda\dfrac{x}{y}, x\right). \end{array} \tag{6}$$

3.2 Implementasi Algoritma Kriptografi Teks Berdasarkan Pemetaan 2-Dimensi Menggunakan *Mathematica*

Untuk mengimplementasikan sebuah algoritma kriptografi ke dalam sebuah program komputer dapat digunakan sejumlah bahasa pemrograman, misalnya *Matlab* dan *Mathematica*. Dalam artikel ini akan digunakan pemrograman Mathematica yang aturan dan teknis penulisan programnya tersedia secara lengkap pada sebuah referensi yang ditulis Shifrin (2008) [8].
Pandang algoritma deskriptif yang dikemukan dalam bagian 2. Terhadap teks dan pemetaan 4-periodik yang diberikan dalam bagian tersebut, implementasi algoritma ke dalam pemrograman *Mathematica* adalah sebagai berikut.

str1 = “Sebagai ungkapan rasa syukur kehadirat Allah,”;
str2 = “seharusnya kita banyak berbuat amal kebaikan.”;
StringLength[str1]
StringLength[str2]
A = ToCharacterCode[str1] ;
B = ToCharacterCode[str2] ;
AccountingForm[Grid[Partition[A, 10]]]
AccountingForm[Grid[Partition[B, 10]]]
x = A;
y = B;
periode = 4;
$\lambda = 0.0001123$;

```
BAGIAN INI MERUPAKAN SUBRUTIN PROGRAM BERNAMA coding1 UNTUK
PROSES ITERASI f(A,B) HINGGA ITERASI KE (p-1)
```

xx = SetPrecision[coding1[[periode − 1, 1]], 10];
yy = SetPrecision[coding1[[periode − 1, 2]], 10];
AccountingForm[Grid[Partition[xx, 3]]]
AccountingForm[Grid[Partition[yy, 3]]]

```
BAGIAN INI MERUPAKAN SUBRUTIN PROGRAM BERNAMA recoding1 UNTUK
PROSES ITERASI f(AA,BB) HINGGA ITERASI KE (p-1)
```

StringJoin[Flatten[FromCharacterCode[Round[recoding1[[periode − 1]]]]]]

Dalam Gambar 1 diberikan hasil konversi data teks ke data numerik sebelum dan sesudah dilakukan proses iterasi pemetaan 1 yang digunakan.

Out[10]//AccountingForm=

83	101	98	97	103	97	105	32	117
110	103	107	97	112	97	110	32	114
97	115	97	32	115	121	117	107	117
114	32	107	101	104	97	100	105	114
97	116	32	65	108	108	97	104	44

Out[11]//AccountingForm=

115	101	104	97	114	117	115	110	121
97	32	107	105	116	97	32	98	97
110	121	97	107	32	98	101	114	98
117	97	116	32	97	109	97	108	32
107	101	98	97	105	107	97	110	46

Out[16]//AccountingForm=

0.000001353012048	0.000001111881188	0.000001145918367	0.000001157731959	0.000001090291262
0.000001157731959	0.000001069523810	0.000003509375000	0.0000009598290598	0.000001020909091
0.000001090291262	0.000001049532710	0.000001157731959	0.000001002678571	0.000001157731959
0.000001020909091	0.000003509375000	0.0000009850877193	0.000001157731959	0.0000009765217391
0.000001157731959	0.000003509375000	0.0000009765217391	0.0000009280991736	0.0000009598290598
0.000001049532710	0.0000009598290598	0.0000009850877193	0.000003509375000	0.000001049532710
0.000001111881188	0.000001079807692	0.000001157731959	0.000001123000000	0.000001069523810
0.0000009850877193	0.000001157731959	0.0000009681034483	0.000003509375000	0.000001727692308
0.000001039814815	0.000001039814815	0.000001157731959	0.000001079807692	0.000002552272727

Out[17]//AccountingForm=

0.0000009765217391	0.000001111881188	0.000001079807692	0.000001157731959	0.0000009850877193
0.0000009598290598	0.0000009765217391	0.000001020909091	0.0000009280991736	0.000001157731959
0.000003509375000	0.000001049532710	0.000001069523810	0.0000009681034483	0.000001157731959
0.000003509375000	0.000001145918367	0.000001157731959	0.000001020909091	0.0000009280991736
0.000001157731959	0.000001049532710	0.000003509375000	0.000001145918367	0.000001111881188
0.0000009850877193	0.000001145918367	0.0000009598290598	0.000001157731959	0.0000009681034483
0.000003509375000	0.000001157731959	0.000001030275229	0.000001157731959	0.000001039814815
0.000003509375000	0.000001049532710	0.000001111881188	0.000001145918367	0.000001157731959
0.000001069523810	0.000001049532710	0.000001157731959	0.000001020909091	0.000002441304348

Gambar 1: Hasil konversi data teks ke data numerik untuk λ=0.0001123. Sebelum proses iterasi pemetaan dilakukan (f^0) (Atas). Setelah proses iterasi pemetaan dilakukan (f^3) (Bawah).

Dengan algoritma dan implementasi algoritma serupa, untuk pemetaan (6) dengan pilihan nilai kunci λ=$\tan(0.123451123)$ sebagaimana diberikan dalam Gambar 2.

Out[269]//AccountingForm=

0.0001854984308	0.0001524393045	0.0001571058138	0.0001587254614	0.0001494793180
0.0001587254614	0.0001466320929	0.0004811365548	0.0001315929039	0.0001399669978
0.0001494793180	0.0001438913061	0.0001587254614	0.0001374675871	0.0001587254614
0.0001399669978	0.0004811365548	0.0001350558750	0.0001587254614	0.0001338814761
0.0001587254614	0.0004811365548	0.0001338814761	0.0001272427252	0.0001315929039
0.0001438913061	0.0001315929039	0.0001350558750	0.0004811365548	0.0001438913061
0.0001524393045	0.0001480420169	0.0001587254614	0.0001539636975	0.0001466320929
0.0001350558750	0.0001587254614	0.0001327273255	0.0004811365548	0.0002368672270
0.0001425589792	0.0001425589792	0.0001587254614	0.0001480420169	0.0003499174944

Out[270]//AccountingForm=

0.0001338814761	0.0001524393045	0.0001480420169	0.0001587254614	0.0001350558750
0.0001315929039	0.0001338814761	0.0001399669978	0.0001272427252	0.0001587254614
0.0004811365548	0.0001438913061	0.0001466320929	0.0001327273255	0.0001587254614
0.0004811365548	0.0001571058138	0.0001587254614	0.0001399669978	0.0001272427252
0.0001587254614	0.0001438913061	0.0004811365548	0.0001571058138	0.0001524393045
0.0001350558750	0.0001571058138	0.0001315929039	0.0001587254614	0.0001327273255
0.0004811365548	0.0001587254614	0.0001412510987	0.0001587254614	0.0001425589792
0.0004811365548	0.0001438913061	0.0001524393045	0.0001571058138	0.0001587254614
0.0001466320929	0.0001438913061	0.0001587254614	0.0001399669978	0.0003347036903

Gambar 2: Hasil konversi data teks ke data numerik untuk λ=$\tan(0.123451123)$, setelah proses iterasi pemetaan dilakukan (g^4).

4 KESIMPULAN

Dari hasil yang diperoleh dan dibahas pada bagian sebelumnya dapat disimpulkan bahwa pemetaan 2-dimensi nonlinear periodik dapat digunakan untuk mendisain sebuah kriptografi teks dengan relatif sederhana. Sebagaimana tujuan sebuah kriptografi adalah pengamanan data, maka pilihan jenis pemetaan dan kunci simetris yang berasosiasi dengan satu/lebih parameter dalam sebuah pemetaan menjadi penting dan perlu perhatian. Hasil penelitian ini, karena pemetaan yang dilibatkan adalah sebuah pemetaan nonlinear yang bersifat *reversing symmetry* dan *measure-preserving*, maka pemetaan dan prosedur algoritma kriptografi yang digunakan dapat dikembangkan untuk kriptografi sebuah citra.

PUSTAKA

[1] R. Sadikin, *Kriptografi Untuk Keamanan Jaringan*. Penerbit Andi, 2012.

[2] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions On Information Theory*, **IT-31 (4)**, 469-472,1985

[3] M. Rinaldi, Algoritma enkripsi selektif citra digital dalam ranah frekuensi berbasis permutasi chaos. *Jurnal Rekayasa Elektrika*, **10(2)**, 66-72, 2012.

[4] D. H. Arinten, A. Irawan, Sistem Kriptografi Citra Digital Pada Jaringan Intranet Menggunakan Metode Kombinasi Chaos Map Dan Teknik Selektif. *Ultimatics*, **9(1)**, 59-66, 2017.

[5] P. Ronsen, H. Arwin, S. Indra, Enkripsi citra digital menggunakan Arnolds cat map dan nonlinear chaotic algorithm. *Jurnal SIFO Mikroskil*, **15(2)**, 61-71, 2014.

[6] F. Al-Anshori, E. Ariwibowo, Implementasi algoritma kriptografi kunci publik ElGamal untuk proses enkripsi dan dekripsi guna pengamanan file data. *Jurnal Sarjana Teknik Informatika*, **2(2)**, 1-10, 2014.

[7] L. Zakaria, J.M. Tuwankotta, Dynamics and bifurcations in a two-dimensional maps derived from a generalized $\Delta\Delta$ sine-Gordon equation. *Far East Journal of Dynamical Systems*, **28(3)**, 165-194, 2016.

[8] L. Shifrin, *Mathematica programming: an advanced Introduction, Part I: the core language*. Wolfram Media, Inc., 2008.