Penerapan Teori Chaos di Dalam Kriptografi

Oleh : Alvin Susanto (13506087)
Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : alvin_punya@yahoo.co.id

Abstraksi
Makalah ini secara khusus akan membahas tentang bagaimana teori chaos diterapkan di dalam dunia kriptografi, beserta perbandingan efek antara beberapa teori chaos tersebut terhadap tingkat keamanan cipherteks yang akan dihasilkannya. Dalam dunia kriptografi, teori chaos ini digunakan untuk membangkitkan bilangan secara acak. Bilangan acak ini kemudian akan dimanfaatkan sebagai kunci dalam melakukan proses enkripsi. Adapun beberapa teori chaos yang dibahas di dalam makalah ini antara lain : persamaan logistik, Henon map, duffing map, gingerbreadman map, dan Arnold's Cat Map. Selain itu, makalah ini juga akan membahas bagaimana lahirnya teori chaos beserta perkembangannya hingga saat ini, serta analisis termasuk kelebihan dan kekurangan dari masing-masing teori chaos yang akan dibahas.

Kata kunci : kriptografi, teori chaos, bilangan acak, enkripsi, persamaan logistik, Henon map, Arnold's Cat Map, keamanan

1. Pendahuluan

Dunia kriptografi modern saat ini telah menerapkan berbagai metode untuk penyandian pesan. Semakin rumit metode yang digunakan, maka tingkat keamanan yang dihasilkan pun akan semakin baik pula. Algoritma kriptografi modern telah menerapkan metode bit dalam penyandian pesan. Hal ini membuat pesan yang dihasilkan akan semakin sulit untuk dipecahkan oleh para kriptoanalis.

Walalupun demikian, tetap saja proses penyandian dengan metode bit ini masih dapat dipecahkan oleh kriptoanalis, terutama algoritma stream cipher. Salah satu caranya adalah dengan menggunakan brute force. Dalam rangka meningkatkan tingkat keamanan dalam algoritma kriptografi modern, digunakanlah teori chaos. Teori chaos ini merupakan cabang dari matematika yang mempelajari bagaimana membangkitkan bilangan secara acak. Teori chaos ini sangat sensitive pada nilai awal (initial condition). Hal ini sangat berguna dan dapat diterapkan di dalam dunia kriptografi sebagai pembangkit kunci acak yang nantinya akan diolah sebagai sarana dalam melakukan proses enkripsi. Semakin acak bilangan yang dihasilkan, semakin baik pula tingkat keamanan dari suatu cipherteks.

2. Sejarah Teori Chaos

Gagasan teori chaos atau teori acak telah dipikirkan sejak lama, akan tetapi yang tercatat sebagai penemu teori chaos ini adalah Henri Poincare yang pada tahun 1880 menemukan bahwa terdapat orbit yang bersifat nonperiodik, dalam arti tidak memiliki proses kemunculan secara tetap atau formulatif. Selain itu Jacques Hadamard juga mempublikasikan teori serupa pada tahun 1898. Selain kedua orang tersebut, masih banyak teori yang bermunculan pada zaman tersebut, yang hampir semuanya dikembangkan oleh matematikawan.

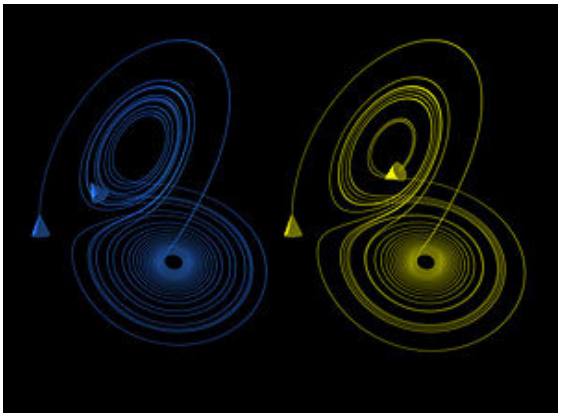
Teori chaos sendiri mulai diformulasikan sejak pertengahan abad ke-20, dengan perintisnya adalah Edward Lorenz yang menemukan permasalahan teori chaos saat melakukan peramalan cuaca pada tahun 1961. Lorenz melakukan suatu simulasi peramalan cuaca dengan menggunakan mesin yang telah ia buat. Lorenz menemukan bahwa prediksi yang ia buat dengan mesin ternyata jauh berbeda dengan kenyataan yang ada. Hal inilah yang menjadi dasar berkembangnya teori chaos. Setelah penemuan dari Lorentz ini, banyak ahli yang mempelajari teori chaos dan menerapkannya pada berbagai bidang, mulai dari dunia meteorologi, biologi, matematika, hingga dunia kriptografi yang juga akan dibahas pada makalah ini.

3. Teori Chaos

Bagian dari makalah ini akan membahas mengenai definisi dan penjelasan mendalam mengenai teori chaos secara lebih mendetail.

3.1 Definisi Teori Chaos

Dalam dunia matematika, teori chaos menggambarkan kebiasaan dari suatu sistem dinamis, yang keadaannya selalu berubah seiring dengan berubahnya waktu, dan sangat sensitif terhadap kondisi awal dirinya sendiri. Teori chaos ini juga sering disebut dengan sebutan butterfly effect. Gambar di bawah ini akan menggambarkan teori chaos sekaligus menjawab megapa teori chaos disebut memiliki butterfly effect.



Dikarenakan oleh sensitivitas yang dimiliki teori chaos terhadap keadaan awal dirinya, teori chaos memiliki sifat untuk muncul secara chaos (kacau). Bahkan perubahan keadaan awal sekecil (10^-100) saja akan membangkitkan bilangan yang benar-benar berbeda. Hal ini terjadi walaupun sistem yang digunakan bersifat deterministik, dalam arti perubahan kondisi dari kondisi yang ada sekarang bersifat statik atau tetap. Salah satu contoh nyata dari teori chaos ini dapat kita lihat pada kehidupan sehari-hari, terutama pada sistem alamiah seperti cuaca. Seperti yang telah disebutkan dalam bab sebelumnya, bahwa Lorentz telah meneliti perubahan cuaca, dan mencoba memodelkannya dengan mesin yang dia rancang sendiri. Akan tetapi, perubahan cuaca sebenarnya ternyata sangat berbeda dengan prediksi mesin yang dirancang oleh Lorentz.

Contoh lain dari chaos ini adalah pertumbuhan suatu populasi pada lingkungan hidup, gerakan pada neuron, pergerakan satelit dalam sistem tata surya, hingga pergerakan dari kerak bumi.

4. Metode Teori Chaos

Pada sesi ini, kita akan membahas berbagai contoh rumus atau ilmu yang dapat dikategorikan sebagai teori chaos, yaitu ilmu atau rumus yang digunakan untuk membangkitkan bilangan secara acak yang akan dimanfaatkan sebagai kunci pada berbagai algoritma kriptografi.

4.1 Logistic Map (Persamaan Logistik)

Persamaan logistik merupakan contoh pemetaan polinomial derajat dua, dan seringkali digunakan sebagai contoh bagaimana rumitnya sifat chaos (kacau) yang dapat muncul dari suatu persamaan yang sangat sederhana. Persamaan ini dipopulerkan oleh seorang ahli biologi yang bernama Robert May pada tahun 1976, melanjutkan persamaan logistik yang dikembangkan oleh Pierre Francois Verhulst.

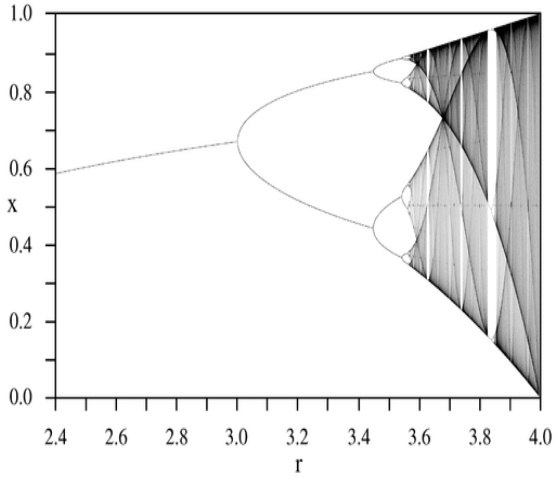
Secara matematis, persamaan logistik dapat dinyatakan dengan persamaan :

$$x_{i+1} = r\, x_i\, (1 - x_i)$$

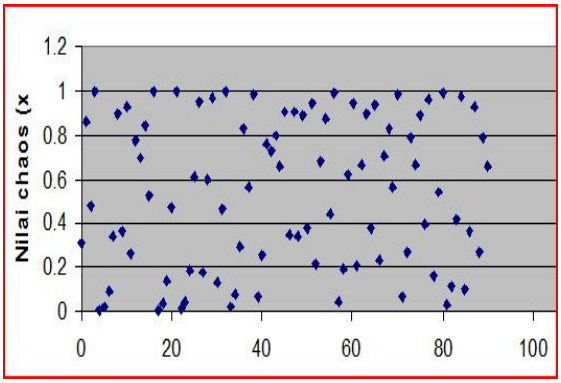
Dimana :

x : bilangan diantara nol dan satu, yang merepresentasikan populasi pada tahun ke i. Parameter x dapat disebut juga sebagai nilai chaos ($0 \le x \le 1$)

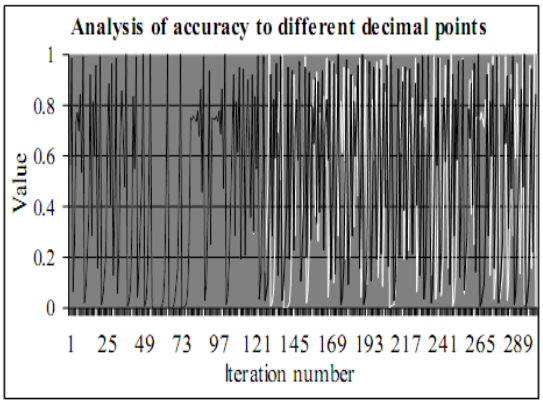
r : bilangan postif yang merepresentasikan kombinasi antara nilai reproduksi dan makanan. Parameter r dapat disebut juga dengan sebutan laju pertumbuhan ($0 \le r \le 4$)



Persamaan logistik ini dapat diterapkan dalam dunia kriptografi dengan membuat fungsi seperti yang telah dicantumkan diatas. Setelah membuat fungsi tersebut, kita lakukan proses perhitungan dengan melakukan iterasi secara berulang, sehingga kita akan selalu mendapatkan bilangan yang benar-benar acak. Kita dapat melihat contoh hasil bilangan acak yang kita dapatkan dengan melakukan puluhan dan ratusan kali proses iterasi pada gambar di bawah ini.



Dari gambar tersebut terlihat bahwa, dari sekitar 90 kali percobaan yang telah dilakukan, didapatkan nilai chaos yang selalu berbeda tanpa ada ritme kemunculan suatu bilangan secara jelas.

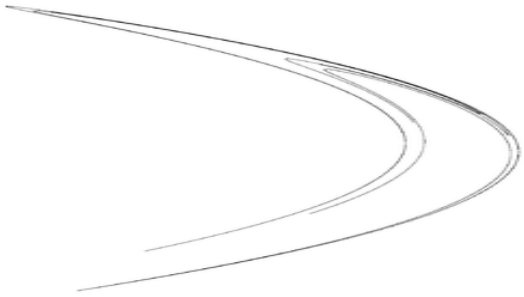


4.2 Henon Map (Persamaan Henon)

Persamaan Henon merupakan sistem dinamis yang menerapkan sistem diskrit. Persamaan Henon merupakan salah satu contoh yang paling banyak dipelajari dalam pembelajaran sistem dinamis yang bersifat chaos (kacau). Persamaan Henon menggunakan sebuah titik (x,y) pada suatu persamaan dan memetakannya menjadi sebuah titik baru dengan persamaan :

$$x_{n+1} = y_n + 1 - ax_n^2$$
$$y_{n+1} = bx_n.$$

Persamaan Henon sangat bergantung pada dua buah parameter, yang dapat kita anggap sebagai a dan b. Nilai dari a dan b ini dapat acak. Untuk persamaan henon yang kanonik, kita mengambil nilai a sebesar 1.4 dan nilai b sebesar 0.3. Gambar di bawah ini menggambarkan diagram persamaan Henon dengan nilai a = 1.4 dan b = 0.3



Persamaan Henon diperkenalkan oleh Michel Henon sebagai model sederhana dari Poincare section dari Lorenz model. Untuk persamaan yang bersifat kanonikal, titik awal yang digunakan akan mendekati kumpulan titik yang dikenal sebagai *strange attractor* Henon, dimana kumpulan titik-titik tersebut mengarah ke bilangan tidak terbatas.
Sebagai sistem yang bersifat dinamis, persamaan Henon sangat menarik dikarenakan orbitnya yang sederhana. Hal inilah yang membedakan persamaan Henon dengan persamaan logistik yang telah dibahas pada upabab sebelumnya.

4.3 Arnold's Cat Map

Arnold's cat map merupakan pemetaan chaos (kacau) yang dinamai berdasarkan penemunya, yaitu Vladimir Arnold, yang menggunakan efek algoritma yang diciptakannya pada tahun 1960 dengan menggunakan gambar seekor kucing.
Arnold's cat map menggunakan transformasi

$$\Gamma : \mathbb{T}^2 \rightarrow \mathbb{T}^2$$

Dengan formula berikut :

$$f(x,y) = \begin{cases} (2x, y/2), & 0 \le x \le 1/2, 0 \le y \le 1 \\ (2x-1, (y+1)/2), & 1/2 \le x \le 1, 0 \le y \le 1 \end{cases}$$

Berikut adalah contoh ilustrasi prinsip kacau pada arnold's cat map. Contoh ini merupakan contoh yang sangat sederhana, namun sangat elegan. Pada contoh ini, suatu gambar ditransformasikan dengan sebuah matriks yang mengacak pixel dari gambar tersebut. Akan tetapi, bila kita melakukan proses iterasi yang sama secara terus menerus, maka gambar yang asli akan muncul kembali.
Langkah pertama adalah kita anggap matriks :

$$X = \begin{bmatrix} x \\ y \end{bmatrix}$$

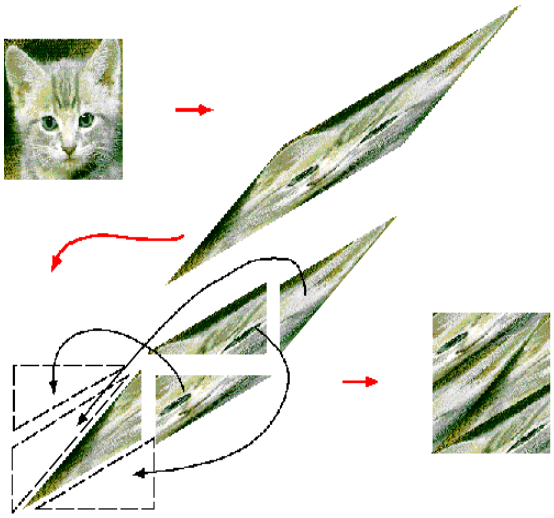
Menjadi N x N matriks yang membentuk gambar, lalu kita melakukan transformasi

$$1'\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ x+2y \end{bmatrix} \bmod n$$

Dimana mod merupakan modulo dari n dan matriks:

$$\begin{bmatrix} x+y \\ x+2y \end{bmatrix}$$

Gambar di bawah ini akan menggambarkan contoh perubahan gambar yang dilakukan dengan menggunakan metode ini :



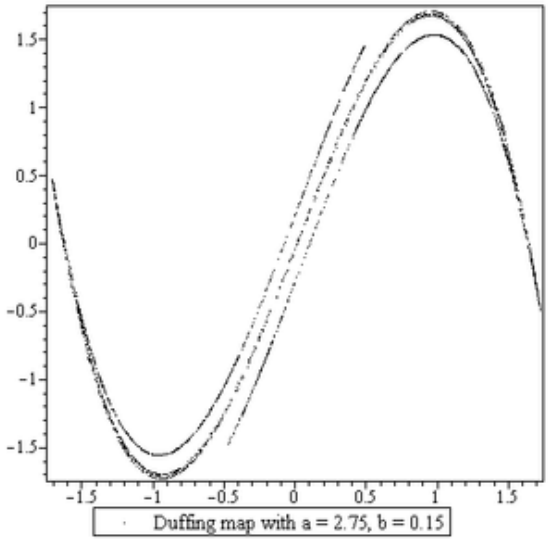
Proses pada gambar di atas merupakan contoh proses pembentukan gambar pada arnold's cat map. Bila proses ini kita ulangi sebanyak beberapa kali, maka secara ajaib gambar kucing akan muncul kembali.

4.4 Duffing Map

Duffing map merupakan salah satu sistem dinamis dengan menggunakan waktu diskrit yang menerapkan sifat chaos (kacau). Duffing map mengambil sebuah titik pada sebuah koordinat lalu memetakannya menjadi sebuah titik yang baru sesuai dengan persamaan :

$$x_{n+1} = y_n$$
$$y_{n+1} = -bx_n + ay_n - y_n^3.$$

Pemetaan sendiri diperngaruhi oleh dua buah nilai, yang pada persamaan diatas merupakan konstanta a dan b. Pada umumnya, nilai untuk konstanta a yang sering digunakan adalah 2.75 dan nilai yang sering digunakan untuk konstanta b adalah 0.2. Kedua nilai inilah yang seringkali digunakan untuk membangkitkan bilangan acak.



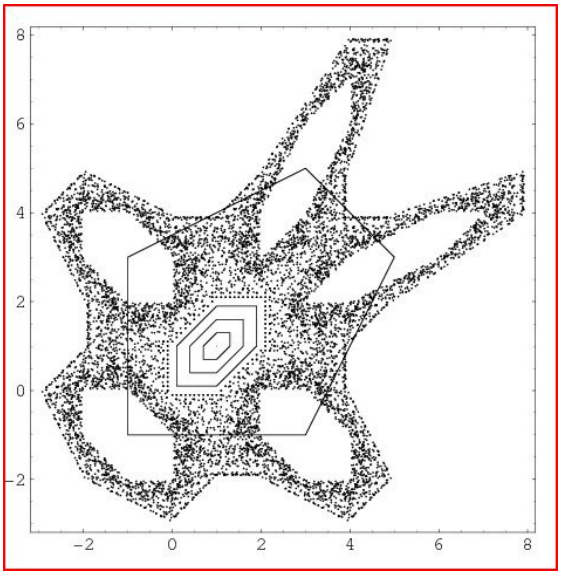
Gambar diatas merupakan diagram yang menggambarkan pembangkitan bilangan acak pada duffing map.

4.5 Gingerbreadman Map

Gingerbreadman map merupakan pemetaan yang bersifat dua dimensi yang didefinisikan oleh rumus sebagai berikut:

$$x_{n+1} = 1 - y_n + |x_n|$$
$$y_{n+1} = x_n -$$

Pemetaan yang dihasilkan akan bersifat acak pada enam wilayah heksagonal yang ada. Setiap titik di dalam heksagonal yang didefinisikan dengan (0, 0), (1, 0), (2, 1), (2, 2), (1, 2), dan (0, 1) memiliki orbit dengan periode sebesar enam, kecuali pada titik (1,1) yang memiliki periode sebesar satu.
Orbit pada lima heksagonal tersebut akan saling berputar dan mengisi satu sama lain. Akan tetapi, ada juga orbit unik dengan nilai periode lima, dengan orbit sisanya memiliki periode sebesar 30. Titik-titik yang memiliki orbit dengan periode sebesar lima adalah (-1, 3), (-1,-1), (3,-1), (5, 3), dan (3, 5). Titik-titik tersebut pada gambar akan digambarkan dengan garis berwarna hitam yang berbentuk gambar segilima di tengah.



5. Perbandingan dan Analisis Metode Teori Chaos

Bagian dari makalah ini akan membandingkan beberapa teori chaos yang telah dibahas pada bab sebelumnya. Di sini penulis tidak akan membandingkan akan metode mana yang lebih baik ataupun lebih buruk dari yang telah dibahas, akan tetapi penulis mencoba menganalisis kelebihan dan kekurangan dari tiap metode berdasarkan data yang didapat dan analsisi penerapannya di dalam dunia kriptografi.

5.1 Persamaan Logistik

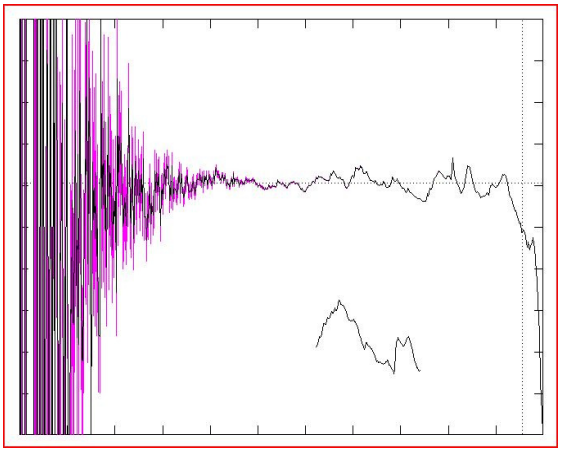
Secara umum algoritma persamaan logistik merupakan salah satu algoritma yang simpel tapi efektif dalam membangkitkan bilangan acak, dimana seperti telah bisa dilihat bahwa dengan sebuah rumus yang sangat sederhana saja, kita dapat membangkitkan bilangan yang benar-benar acak.

Keuntungan dari persamaan logistik adalah kita dapat membangkitkan bilangan yang acak secara terus menerus. Bilangan yang dibangkitkan ini tanpa pola yang akan berulang walaupun kita telah melakukan proses berkali-kali.

Meskipun demikian, persamaan logistik juga memiliki kelemahan besar yang sangat mendasar. Kelemahan yang dimaksud adalah bahwa dengan persamaan logistik, kita harus menyimpan kunci yang telah dibangkitkan dalam proses enkripsi. Proses penyimpanan kunci mutlak dilakukan agar kita dapat melakukan proses dekripsi. Hal ini akan sangat merugikan, sebab bila kita menyimpan kunci bersamaan dengan cipherteks yang dihasilkan, cipherteks akan dapat dipecahkan dengan mudah oleh pihak lawan yang berhasil mencuri cipherteks tersebut. Hal sebaliknya juga berlaku bila kita menyimpan kunci di tempat yang terpisah dengan cipherteks yang dihasilkan. Sang penerima pesan cipherteks tentunya tidak akan dapat melakukan proses dekripsi bila kunci yang digunakan tidak didapatkan atau tercuri pihak lain dikarenakan kunci yang tidak dapat diprediksi.

5.2 Henon Map

Henon map menggunakan polinomial derajat dua untuk membangkitkan bilangan acak, oleh karena itu, henon map sangat tergantung pada dua buah bilangan yang digunakan sebagai koefisien dari persamaan polinomial yang ada. Henon map ini memiliki bentuk orbit yang paling sederhana dibandingkan dengan setiap teori yang dibahas pada makalah ini. Walaupun demikian, secara keseluruhan, pembangkitan bilangan acak pada henon map ini dapat diandalkan. Hal tersebut dapat dilihat pada gambar di bawah ini, yang menggambarkan bagaimana hasil pengaplikasian henon map pada POWER BASIC :



Warna ungu pada bagan diatas adalah bagaimana hasil pembangkitan bilangan acak pada henon map.

5.3 Arnold Cat's Map

Arnold's cat map memanfaatkan matriks dalam membangkitkan bilangan acak yang diinginkan. Arnold's cat map ini cocok digunakan untuk melakukan enkripsi pada gambar, dikarenakan fungsi ini memanfaatkan matriks yang berarti minimal kita dapat melakukan enkripsi untuk suatu benda yang bersifat dua dimensi.

Keunggulan dari arnold's cat map ini adalah kita dapat membangkitkan suatu pengacakan dengan fungsi yang relatif sederhana. Selain proses enkripsi yang mudah, proses dekripsi pun dapat kita lakukan dengan mudah. Yang perlu kita lakukan dalam melakukan proses dekripsi adalah melakukan proses enkripsi secara berulang-ulang hingga gambar awal ditemukan kembali.

Kekurangan dari proses ini hampir sama dengan persamaan logistik, yakni proses penyimpanan kunci, dimana untuk hal ini dapat terjadi dua kemungkinan. Kemungkinan pertama adalah kita menyimpan kunci bersamaan dengan cipherteks,

dan juga kita menyimpan kunci di tempat yang berbeda dengan cipherteks. Kedua hal ini memiliki kekurangan tersendiri. Untuk penjelasan mengenai kekurangan dari kedua hal ini, dapat dilihat pada sesi 5.1 yang membahas persamaan logistik.

5.4 Duffing Map

Duffing map juga merupakan salah satu teori chaos dengan tingkat implementasi yang relatif mudah, walaupun duffing map ini memanfaatkan polinomial derajat tiga, yang menghasilkan grafik yang bersifat naik turun.

5.5 Gingerbreadman Map

Gingerbreadman map menggunakan sistem pemetaan yang sederhana. Pemetaan yang digunakan di dalam gingerbreadman map akan menghasilkan grafik yang indah, dengan lima buah heksagonal di dalam grafik tersebut.

Salah satu sifat dari gingerbreadman map ini adalah bahwa orbit dari tiap heksagonal yang terus berputar dan mengisi satu sama lain. Hal ini dapat mengakibatkan pengulangan bila dilakukan secara terus menerus, seperti juga halnya pada arnold's cat map.

6. Kesimpulan

Dalam rangka menigkatkan tingkat keamanan dari suatu algoritma kriptorafi modern, diperlukan juga suatu pembangkit bilangan acak yang menjamin bahwa para kriptoanalis akan menemui kesulitan untuk memecahkan cipherteks yang dihasilkan.

Penggunaan pembangkitan bilangan acak dengan menggunakan teori chaos ini memiliki banyak keuntungan dan kekurangan. Keuntungannya terletak pada hampir mustahilnya seorang kriptoanalis untuk menebak kunci yang dibangkitkan. Akan tetapi, pemanfaatan pembangkitan kunci secara chaos (kacau) ini juga dapat menjadi bumerang. Masalah penyimpanan kunci yang notabene tidak dapat diprediksi menjadi mutlak diperlukan. Hal ini menjadi dilema tersendiri mengingat untuk menyampaikan suatu cipherteks ke tujuan, kita harus menyertakan kunci agar tujuan pesan kita dapat melakukan proses dekripsi pesan yang telah kitaberikan sebelumnya.

Daftar Pustaka

1. Munir, Rinaldi, Diktat Kuliah IF5054 Kriptografi, Departemen Teknik Informatika Institut Teknologi Bandung, 2006
2. Slide kuliah IF5054 oleh Rinaldi Munir
3. http://networks.cs.ucdavis.edu/~amitabha/Adcom99.pdf
4. http://sprott.physics.wisc.edu/chaos/Henongp.htm
5. http://en.wikipedia.org
6. http://mathworld.wolfram.com