Regenerasi Fungsi $x^2 - 9x - 99$ Dalam Pembangkit Bilangan Acak Berbasis CSRPNG Chaos

David Lihananto¹, Alz Danny Wowor²

^{1,2}Fakultas Teknologi Informasi Universitas Kristen Satya Wacana

Jl. Dr. O. Notohamidjojo 1-10, Salatiga 50711, Indonesia

Email : ¹672015059@student.uksw.edu, ²alzdanny.wowor@staff.uksw.edu

Abstract

This study examines whether the function $f(x) = x^2 - 9x - 99$ can be used as a key generator in cryptography. The quadratic function is regenerated using the fixed point iteration method into an iteration function. The distribution of digits to the output of iterative function to generate a number of chaos. Randomization testing uses run test and monobit testing. Followed by cryptographic testing to get the correlation between ciphertext and key which will be used as a decision whether the resulting key is random or not. Based on research that has been done iteration function $x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$ can generate CSRPNG Chaos random numbers with the correlation level closest to the value of 0.

Keywords: Cryptography, Quadratic Function, Iteration Method, Random Number, Key Generator

Abstrak

Penelitian ini menguji apakah fungsi $f(x) = x^2 - 9x - 99$ dapat digunakan sebagai pembangkit kunci dalam kriptografi. Fungsi kuadrat diregenerasi menggunakan metode iterasi titik tetap menjadi fungsi iterasi. Dilakukan pembagian digit angka untuk hasil keluaran fungsi iterasi untuk menghasilkan bilangan chaos. Pengujian pengacakan menggunakan pengujian run test dan monobit. Dilanjutkan dengan pengujian kriptografi untuk dapatkan hasil korelasi antara chiperteks dan kunci yang akan dijadikan sebagai keputusan apakah kunci yang dihasilkan sudah acak atau tidak. Berdasarkan penelitian yang telah dilakukan fungsi iterasi $x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$ dapat menghasilkan bilangan acak CSRPNG Chaos dengan tingkat korelasi yang paling mendekati nilai 0.

Kata kunci: Kriptografi, Fungsi Kuadrat, Metode Iterasi, Bilangan Acak, Pembangkit Kunci

1. Pendahuluan

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 logistik dapat diterapkan dalam dunia kriptografi dengan membuat suatu fungsi. Setelah mendapatkan suatu fungsi

kita perlu melakukan proses iterasi agar sehingga kita bisa mendapatkan bilangan-bilangan yang benar-benar acak[1].

Secara matematis, persamaan logistik dapat dinyatakan dengan persamaan $x_i = r x_i(1 - x_i)$ dimana x adalah bilangan diantara nol dan satu, Parameter x dapat disebut juga sebagai nilai *chaos* ($0 \leq x \leq 1$). Sedangkan r adalah bilangan positif yang merepresentasikan kombinasi antara nilai reproduksi dan makanan. Parameter r dapat disebut juga dengan sebutan laju pertumbuhan ($0 \leq r \leq 4$)[1].

Penelitian ini bertujuan untuk menggunakan fungsi $x^2 - 9x - 99$ sebagai pembangkit bilangan acak dalam kriptografi dengan alasan belum pernah digunakan sebelumnya sebagai pembangkit kunci dan dengan menggunakan metode iterasi tetap akan menghasilkan fungsi-fungsi iterasi. Dimana fungsi tersebut diharapkan menghasilkan kunci yang acak. Kunci yang acak akan lebih sulit dipecahkan dari pada fungsi yang menghasilkan pola tertentu secara beraturan.

2. Tinjauan Pustaka

Pada penelitian berjudul Regenerasi Fungsi Kuadrat lain sebagai Pembangkit Kunci Berbasis Metode Iterasi Titik Tetap (Fixed Point) pada Kriptografi, membahas tentang penggunaan fungsi kuadrat yang dapat digunakan sebagai pembangkit kunci dalam kriptografi untuk memperluas ruang penebakan pemecahan kunci. Berdasarkan pencarian nilai determinan diketahui bahwa fungsi kuadrat yang berpeluang besar menjadi fungsi generator adalah fungsi yang memiliki dua akar bilangan real yang berbeda[2].

Pada penelitian yang berjudul Regenerasi Fungsi Polinomial Dalam Rancangan Algoritma Berbasis CSPRNG Chaos Sebagai Pembangkit Kunci Pada Kriptografi Block Cipher, membahas tentang menggunakan fungsi polynomial derajat-1, derajat-2, dan derajat-3 sebagai fungsi pembangkit[3].

Pada penelitian Regenerasi Fungsi $(x) = x^2 - 7x + 5$ sebagai Pembangkit Bilangan Acak Menggunakan Metode Iterasi Titik Tetap (*Fixed Point Iteration*), membahas tentang menggunakan fungsi $f(x) = x^2 - 7x + 5$ sebagai pembangkit kunci. Hasil dari penelitian menunjukan bahwa fungsi belum menunjukan pola yang acak sehingga diperlukan manipulasi pada koefisien dan konstanta sehingga didapat fungsi iterasi yang dapat menghasilkan baris bilangan acak berbasis CSPNRG Chaos [4].

Penelitian ini mengembangkan penelitian sebelumnya yang berjudul Regenerasi Fungsi Kuadrat sebagai Pembangkit Kunci Berbasis Metode Iterasi Titik Tetap (Fixed Point) pada Kriptografi. Dimana peneliti tersebut menggunakan fungsi yang belum pernah digunakan sebagai pembangkit kunci yang memiliki kendala pada pemilihan koefisien dan konstantanya sehingga harus dimanipulasi. Dan pengembangan pada penelitian berjudul Regenerasi Fungsi Polinomial Dalam

Rancangan Algoritma Berbasis CSPRNG Chaos Sebagai Pembangkit Kunci Pada Kriptografi Block Cipher. Penelitian ini mengembangkan penelitian-penelitian sebelumnya dengan menggunakan fungsi polynomial derajat-2 yang akan diproses menggunakan metode iterasi tetap untuk menghasilkan fungsi-fungsi pembangkit bilangan acak.

Sebuah polynomial n dalam matematika dapat didefinisikan sebagai sebuah fungsi dari deret dengan variabelnya berpangkat maksimal n . ini dapat ditulis sebagai berikut :

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0 \quad (1)$$

dengan nilai x sebagai variabel fungsi polynomial, a sebagai koefisien pada variabel x yang bersangkutan[5].

Metode Iterasi Titik Tetap atau Metode iterasi satu titik adalah suatu metode pencarian akar suatu fungsi $f(x)$ secara sederhana dengan menggunakan satu titik awal. Perlu diketahui bahwa fungsi $f(x)$ yang ingin dicari hampiran akarnya harus konvergen (nilai yang semakin kecil). Misal x adalah *Fixed Point* (Titik Tetap) fungsi $f(x)$ bila $g(x)=x$ dan $f(x) = 0$ [6].

Teori chaos adalah teori yang menggambarkan perilaku sistem dinamis nirlanjar yang menunjukkan fenomena yang kacau. Salah satu teori sistem chaos adalah sangat peka terhadap nilai awal. Hal ini menunjukkan hasil yang sangat kacau jika nilai awal berbeda sedikit saja. Map dari suatu nilai tertentu yang polanya sangat sensitif terhadap perubahan disebut *Chaotic Map*. Ada banyak *chaotic map* yang telah ditemukan, salah satunya adalah *Logistic Map*[7].

Logistic Map juga merupakan satu dimensi yang telah digunakan secara luas, yang didefinisikan sebagai berikut [7]:

$$x_i + 1 = r x_i (1 - x_i) \quad (1)$$

$$x_{i+1} = r x_i (1 - x_i) \quad (2)$$

Dengan parameter-parameter :

r = laju pertumbuhan ($0 \leq r \leq 4$)

x = nilai chaos ($0 \leq x \leq 1$)

Korelasi merupakan salah satu nilai statistik yang digunakan untuk melihat hubungan antara variabel bebas (x) dan tak bebas (y) yang bersifat kuantitatif. Persamaan korelasi diformulasikan sebagai berikut [8]:

dengan ditentukan $-1 \leq r \leq 1$ dan interpretasi nilai korelasi ini didapat dan dirangkum pada Tabel 1.

Tabel 1 Tingkat Hubungan Korelasi

Nilai Korelasi	Hubungan Korelasi
0,00 - 0,19	Sangat Rendah
0,20 - 0,39	Rendah
0,40 - 0,59	Cukup
0,60 - 0,79	Kuat
0,80 - 1,00	Sangat Kuat

3. Metode Penelitian

Metode penelitian dilakukan dalam beberapa tahap. Masing-masing tahap harus dilakukan secara berurutan dari study hingga penulisan laporan.

Tahap-tahap dari penelitian, dijelaskan sebagai berikut. study: pada tahap ini mempelajari materi yang berkaitan dengan topik penelitian dan mencari beberapa sumber dan referensi untuk membantu penelitian. Perancangan : menentukan fungsi polinomial kuadrat dua yang akan digunakan sebagai pembangkit kunci. dengan menggunakan metode iterasi titik tetap akan menghasilkan pembangkit kunci yang baru. Pengujian dan analisis : dalam tahap ini setelah mendapatkan beberapa fungsi baru maka akan dilakukan pengujian menggunakan pengujian *run test*, *mobo bit*, dan *block bit*. Setelah mendapatkan hasil pengujian maka akan dianalisa apakah fungsi tersebut dapat digunakan sebagai pembangkit kunci yang baru atau tidak. Penulisan laporan : pada tahap ini dilakukan penulisan hasil pengujian dan analisis dari penelitian dalam bentuk laporan penelitian.

4. Hasil dan Pembahasan

Regenerasi fungsi $x^2 - 9x - 99$ dilakukan dengan memanipulasi fungsi menggunakan metode iterasi tetap yang menghasilkan beberapa fungsi iterasi. Fungsi iterasi yang dihasilkan kemudian akan diuji keacakannya menggunakan pengujian *run test* dan *monobit*, yang kemudian akan diperoleh mana fungsi yang acak dan tidak acak.

Hasil dari fungsi yang telah diuji kemudian akan disimulasikan kedalam pengujian kriptografi untuk menguji apakah kunci yang digunakan sudah bersifat acak. pengujian korelasi untuk mengetahui hubungan antara cipherteks dengan kunci yang akan melihat pembangkit kunci yang paling efektif.

Fungsi yang digunakan $f(x) = x^2 - 9x - 99$ yang menghasilkan fungsi literasi seperti pada Tabel 2 dengan nilai $x_0 = 12,43$ pada setiap fungsi iterasi.

Tabel 2 Fungsi iterasi dari $f(x) = x^2 - 9x - 99$

Fungsi	Hasil Iterasi Titik tetap	Fungsi Iterasi
Fungsi 1	$x = (x^2 - 9)/9$	$xi = (x_{i-1}^2 - 9)/9$
Fungsi 2	$x = \sqrt{9x + 99}$	$x_i = \sqrt{9x_{i-1} + 99}$
Fungsi 3	$x = 99/x - 9$	$x_i = 99/x_{i-1} - 9$
Fungsi 4	$x = (x^2 - 9x - 99)/9$	$x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$

Hasil keluaran dari fungsi iterasi dibagi menjadi lima bagian data untuk pengambilan angka. Setiap data berisikan 3 digit angka yang di dapatkan dari nilai x_i . Hasil dari 10 iterasi pertama pada fungsi $x_i = (x_{i-1}^2 - 9)/9$ seperti pada Tabel 3.

Tabel 3 Hasil Bilangan Acak $x_i = (x_{i-1}^2 - 9x - 99)/9$

Urutan iterasi	Xi	Data1	Data2	Data3	Data4	Data5
1	-6,262788888888890	0,26	278	888	888	889
2	-0,379152814801095	0,37	915	281	480	109
3	-10,604874201091000	0,6	48	742	10	91
4	12,100802736753700	0,1	80	273	675	37
5	-6,830866417439780	0,83	86	641	743	978
6	1,015392641096050	15	392	641	96	5
7	-11,900834617141400	1,9	8	346	171	414
8	16,637486237647000	0,63	748	623	764	7
9	3,118730241007890	118	730	241	7	89
10	-13,038010428099300	3	380	104	280	993

Hasil penelitian terhadap keempat fungsi iterasi menunjukkan bahwa fungsi iterasi pertama $x_i = (x_{i-1}^2 - 9)/9$, menghasilkan pola mengerucut, tetapi perbandingan setiap datanya semakin acak antara satu data kedata yang lainnya. Fungsi iterasi kedua $x_i = \sqrt{9x_{i-1} + 99}$ tidak bisa dijadikan sebagai pembangkit kunci karena pola yang dihasilkan membentuk garis lurus. Fungsi iterasi ketiga $x_i = 99/x_{i-1} - 9$ tidak bisa dijadikan sebagai pembangkit kunci karena pola yang dihasilkan membentuk garis lurus. Untuk 200 iterasi pertama pada fungsi iterasi keempat $x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$ menghasilkan pola yang acak seperti terlihat dalam gambar 1, dimana hasil dari iterasi yang cukup acak tetapi pada data pertama masih ada pola garis.

Gambar 1 Grafik Fungsi Iterasi $x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$

Uji *run test* dilakukan untuk mengetahui keacakan dari suatu data. Nilai X_o yang digunakan dalam pengujian ini $X_o = 12.43$

Tabel 4 Hasil Pengujian *Run Test*

Fungsi iterasi	Pengambila n data	Hasil Uji	Keterangan
$xi = (x_{i-1}^2 - 9)/9$	Data1	1	acak
$xi = (x_{i-1}^2 - 9)/9$	Data2	0,993651565	acak
$xi = (x_{i-1}^2 - 9)/9$	Data3	0,983545805	acak
$xi = (x_{i-1}^2 - 9)/9$	Data4	0,722654883	acak
$xi = (x_{i-1}^2 - 9)/9$	Data5	1	acak
$x_i = \sqrt{9x_{i-1} + 99}$	Data1	1,22E-34	tidak acak
$x_i = \sqrt{9x_{i-1} + 99}$	Data2	2,83E-42	tidak acak
$x_i = \sqrt{9x_{i-1} + 99}$	Data3	2,35E-28	tidak acak
$x_i = \sqrt{9x_{i-1} + 99}$	Data4	4,08E-25	tidak acak
$x_i = \sqrt{9x_{i-1} + 99}$	Data5	1,37E-35	tidak acak
$x_i = 99/x_{i-1} - 9$	Data1	0,540028	acak
$x_i = 99/x_{i-1} - 9$	Data2	7,37E-37	tidak acak
$x_i = 99/x_{i-1} - 9$	Data3	9,23E-05	tidak acak
$x_i = 99/x_{i-1} - 9$	Data4	1,22E-08	tidak acak
$x_i = 99/x_{i-1} - 9$	Data5	1,48E-20	tidak acak
$x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$	Data1	0,99665952	acak
$x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$	Data2	0,809147572	acak
$x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$	Data3	0,706988391	acak
$x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$	Data4	0,081155246	acak
$x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$	Data5	0,919206208	acak

Tabel 4 menunjukkan hasil dari pengujian Run test terhadap fungsi-fungsi iterasi. Untuk $xi = x_{i-1}^2 - 9/9$ memperoleh hasil acak pada setiap datanya. Pada fungsi $x_i = \sqrt{9x_{i-1} + 99}$ data pertama memperoleh hasil yang acak dan sisanya data kedua, ketiga, keempat, dan kelima memperoleh hasil yang tidak acak. Pada fungsi $x_i = 99/x_{i-1} - 9$ memperoleh hasil tidak acak pada setiap data. Pada $x_i = x_{i-1}^2 - 9x_{i-1} - 99/9$ memperoleh hasil yang acak pada setiap datanya. Dari pengujian *Run test* tersebut dapat menunjukkan data dari fungsi $xi = x_{i-1}^2 - 9/9$ dan fungsi $x_i = x_{i-1}^2 - 9x_{i-1} - 99/9$ dapat dijadikan sebagai kandidat kunci yang efisien dalam mengamankan informasi.

Uji monobit dilakukan untuk mengetahui keacakan dari suatu data. Nilai x_0 yang digunakan dalam pengujian ini $x_0 = 12,43$

Tabel 5 Hasil pengujian *Monobit*

Fungsi iterasi	Pengambilan data	Hasil Uji	Keterangan
$xi = (x_{i-1}^2 - 9)/9$	Data1	0,317310508	Acak
$xi = (x_{i-1}^2 - 9)/9$	Data2	6,66409E-08	tidak acak
$xi = (x_{i-1}^2 - 9)/9$	Data3	0,689156517	acak
$xi = (x_{i-1}^2 - 9)/9$	Data4	0,423710797	acak
$xi = (x_{i-1}^2 - 9)/9$	Data5	1,97318E-09	tidak acak
$x_i = \sqrt{9x_{i-1} + 99}$	Data1	7,55E-79	tidak acak
$x_i = \sqrt{9x_{i-1} + 99}$	Data2	3,21E-77	tidak acak
$x_i = \sqrt{9x_{i-1} + 99}$	Data3	7,07E-71	tidak acak
$x_i = \sqrt{9x_{i-1} + 99}$	Data4	7,07E-71	tidak acak
$x_i = \sqrt{9x_{i-1} + 99}$	Data5	3,11E-56	tidak acak
$x_i = 99/x_{i-1} - 9$	Data1	2,98E-87	tidak acak
$x_i = 99/x_{i-1} - 9$	Data2	8,25E-68	tidak acak
$x_i = 99/x_{i-1} - 9$	Data3	8,25E-68	tidak acak
$x_i = 99/x_{i-1} - 9$	Data4	2,44E-63	tidak acak
$x_i = 99/x_{i-1} - 9$	Data5	1,46E-49	tidak acak
$x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$	Data1	0,317310508	acak
$x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$	Data2	6,66409E-08	tidak acak
$x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$	Data3	0,689156517	acak
$x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$	Data4	0,423710797	acak
$x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$	Data5	1,97318E-09	tidak acak

Tabel 5 menunjukan hasil dari pengujian monobit terhadap fungsi-fungsi iterasi. Pada fungsi $xi = (x_{i-1}^2 - 9)/9$ memperoleh hasil yang tidak acak pada data kedua dan data kelima sedangkan pada data kesatu, data kedua, dan data keempat memperoleh hasil yang acak. Pada fungsi $x_i = \sqrt{9x_{i-1} + 99}$ setiap datanya memperoleh hasil yang tidak acak. Sedangkan pada fungsi $x_i = 99/x_{i-1} - 9$ setiap datanya juga memperoleh hasil yang tidak acak. Pada fungsi $x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$ hasil yang diperoleh pada data kedua dan kelima memperoleh hasil yang tidak acak dan pada data pertama, kedua, dan keempat memperoleh hasil yang acak. Dari hasil pengujian monobit tersebut data yang menunjukkan hasil yang acak akan digunakan sebagai kandidat kunci.

Dari pengujian *run test* dan *monobit* akan diambil data yang memperoleh hasil acak pada setiap pengujian. Pada pengujian *run test* dan *monobit* menunjukkan data yang memperoleh hasil acak pada kedua pengujian, pada fungsi $x_i = (x_{i-1}^2 - 9)/9$ data kedua, data ketiga, dan data keempat bisa digunakan sebagai kunci. Pada fungsi $x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$ data pertama, data ketiga dan data keempat dapat digunakan sebagai kunci.

Pegujian dilakukan dengan cara melakukan proses enkripsi $E_k : P + K = C \text{ mod } (256)$, dimana P, C, dan K secara berturut-turut adalah plainteks, cipberteks dan kunci. Plainteks yang akan digunakan “FTI UKSW SALATIGA”, yang akan diuji menggunakan fungsi iterasi $x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$, khususnya pada data ke empat yang digunakan sebagai kunci. Proses pengujian dilakukan dengan mengubah plaintesks mendadi ASCII, kemudian dilanjutkan memnggunakan proses enkripsi dengan nilai $X_0=0,413124123$.

Menguji CSPRPNG CHAOS dengan *butterfly effect* untuk mengetahui seberapa kuat fungsinya, gambar 2 menampilkan perbandingan nilai $X_0 = 0,413124123$ dengan nilai $X_0 = 0,41312410001$. Hasil yang didapat dari pengujian menunjukan perbedaan dari grafik chipberteks hanya dengan menggunakan nilai X_0 yang berbeda. Dari pengujian ini *butterfly effect* berlaku pada fungsi ini.

Gambar 2 Enkripsi dengan nilai X_0 yang berbeda pada $x_i = x_{i-1}^2 - 9x_{i-1} - 99$

Pengujian korelasi dilakukan untuk melihat seberapa kuat kunci yang digunakan pada proses enkripsi. Dalam hal ini semakin rendah tingkat hubungan maka kunci tersebut semakin efisien untuk digunakan dalam mengamankan informasi.

Tabel 6 Hasil Uji Korelasi

Fungsi Iterasi	Pengambilan Data	Hasil Korelasi	Tingkat Hubungan
$x_i = (x_{i-1}^2 - 9)/9$	Data 2	-0,11968	Sangat Rendah
$x_i = (x_{i-1}^2 - 9)/9$	Data 3	-0,52828	Cukup
$x_i = (x_{i-1}^2 - 9)/9$	Data 4	-0,0719	Sangat Rendah
$x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$	Data 1	0,265354	Rendah
$x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$	Data 2	-0,23014	Rendah
$x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$	Data 4	-0,05372	Sangat Rendah

Tabel 6 menunjukkan hasil dari pengujian korelasi fungsi -fungsi iterasi dengan nilai $X_0=0,41312412343$. Berdasarkan hasil pengujian pada tabel 6 (dengan mengabaikan tanda negative), ditunjukkan pada fungsi iterasi $x_i = x_{i-1}^2 - 9/9$ memperoleh nilai korelasi sangat rendah pada data kedua dan keempat. Sedangkan pada data ketiga memperoleh nilai korelasi cukup. Pada fungsi $x_i = x_{i-1}^2 - 9x_{i-1} - 99/9$ nilai korelasi pada data pertama dan data kedua memperoleh nilai korelasi yang cukup. Sedangkan pada data keempat memperoleh nilai korelasi sangat rendah.

Hasil pengujian korelasi menunjukkan bahwa fungsi iterasi $x_i = x_{i-1}^2 - 9/9$ data kedua dan data keempat lalu fungsi $x_i = x_{i-1}^2 - 9x_{i-1} - 99/9$ data keempat memiliki nilai korelasi yang sangat rendah. Sehingga ketiga data tersebut dapat digunakan sebagai kunci yang memiliki sifat acak untuk mempersulit dalam pemecahan kunci. Sedangkan data yang lainnya masih bias digunakan sebagai kunci tetapi karna nilai korelasinya lebih tinggi maka akan lebih mudah untuk dipecahkan.

5. Simpulan

Berdasarkan penelitian regenerasi fungsi $x^2 - 9x - 99$ dalam pengangkitan bilangan acak berbasis CSPRNG CHAOS dapat disimpulkan bahwa dengan menggunakan metode iterasi tetap menghasilkan beberapa fungsi iterasi yang bisa digunakan sebagai kunci yang efisien. Fungsi $x^2 - 9x - 99$ masih bisa menghasilkan fungsi iterasi yang lebih beragam. Berdasarkan simulasi pengujian kriptografi, ciperteks yang dihasilkan memiliki sifat *butterfly effect* dimana bila merubah nilai dari X_0 walaupun hanya beberapa karakter tetapi merubah pola tersebut. Dari hasil pengujian korelasi didapatkan fungsi $x_i = (x_{i-1}^2 - 9)/9$ data kedua dan data keempat lalu fungsi $x_i = (x_{i-1}^2 - 9x_{i-1} - 99)/9$ data keempat memiliki nilai korelasi yang sangat rendah yang cocok digunakan sebagai pembangkit kunci karena sifatnya tidak saling terhubung.

Daftar Pustaka

- [1] Susanto, Alvin, 2009, Penerapan Teori Chaos di Dalam Kriptografi, <http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2008-2009/Makalah2/MakalahIF3058-2009-b031.pdf>
- [2] Suling, Pricillia M., dan Wowor, Alz D., 2017, Regenerasi Fungsi Kuadrat sebagai Pembangkit Kunci Berbasis Metode Iterasi Titik Tetap (Fixed Point) pada Kriptografi, <http://repository.uksw.edu/handle/123456789/16397>.
- [3] Wowor, Alz D., 2017, Regenerasi Fungsi Polinomial Dalam Rancangan Algoritma Berbasis CSPRNG Chaos Sebagai Pembangkit Kunci pada Kriptografi Block Cipher. Limits, 14 : 4, A.

-
- [4] Irawan, Abednego, dan dan Wowor, Alz D., 2019, Regenerasi Fungsi $f(x)=x^2-7x+5$ sebagai Pembangkit Bilangan Acak Menggunakan Metode Iterasi Titik Tetap (Fixed Point Iteration), <http://repository.uksw.edu/handle/123456789/18992>
- [5] Supriyanto, Edy, 2004, Polynomial Dalam Mathlab, <https://www.unisbank.ac.id/ojs/index.php/fti1/article/download/633/403>
- [6] Siswipraptini, Puji C., dan Martono, Wisnu H., 2015, Penentuan Tingkat Daya Dukung Implementasi Aplikasi Simulasi Akar Persamaan Iterasi Satu Titik Mata Kuliah Metode Numerik di STT PLN, <http://journal.uinjkt.ac.id/index.php/ti/article/download/1933/1503>
- [7] Kurniawan, Ervyn Yoga Indra, 2014, Penerapan Teori *Chaos* pada Kriptografi Menggunakan Algoritma *Stream cipherI* dan *Electronic Code Book (ECB)* untuk Keamanan Pesan Teks, <http://mahasiswa.dinus.ac.id/docs/skripsi/jurnal/13608.pdf>
- [8] Steward, J., 2012, Calculus; Early Transcendentals, Belmont: Brooks/Cole