Implementasi Pembangkit Bilangan Acak Semu dengan *Henon-Sine Hyperchaotic Map*

Putri Nurhaliza - 13520066
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 13520066@std.stei.itb.ac.id

***Abstrak*— Kriptografi sebagai bidang ilmu yang berkembang untuk menjaga kerahasiaan, integritas, serta autentikasi memanfaatkan bilangan acak untuk keamanan yang lebih tinggi. Salah satu teori yang digunakan pada pembangkit bilangan acak semu adalah teori *chaos*. Fokus utama makalah ini adalah dua fungsi pembangkit bilangan acak semu, yaitu *Henon map* dan *Sine map*. Berlandaskan pada sistem dinamika nonlinier pada kedua *map* tersebut, dibuat suatu fungsi baru untuk membangkitkan bilangan acak semu yang lebih kuat (*hyperchaotic)*. Pada makalah ini dipaparkan implementasi fungsi-fungsi tersebut beserta analisis menggunakan beberapa metrik.**

Kata Kunci*— *Kriptografi; Bilangan Acak; Teori Chaos; Henon Map; Sine map

I. PENDAHULUAN

Dalam konteks kriptografi, kebutuhan akan bilangan acak semu berkaitan erat dengan keamanan sistem komputer dan kegiatan enkripsi data. Penggunaan bilangan acak semu dalam komputasi modern berasal dari upaya untuk menyimulasikan fenomena acak dalam lingkungan yang deterministik seperti komputer. Pada awalnya, penghasilan bilangan acak semu dilakukan melalui algoritma yang menghasilkan pola yang terlihat acak tetapi sebenarnya dapat diprediksi. Namun, kebutuhan akan bilangan acak semu yang lebih kuat, yaitu yang benar-benar acak dan tidak dapat diprediksi, semakin meningkat seiring berkembangnya aplikasi kriptografi.

Kriptografi merupakan ilmu yang berhubungan dengan keamanan informasi dan komunikasi. Beberapa pengaplikasian bilangan acak semu dalam kriptografi adalah sebagai berikut.

- Kunci enkripsi.

  Pada kriptografi modern, algoritma enkripsi simetris dan asimetris menggunakan kunci yang dibangkitkan secara acak. Bilangan acak semu digunakan untuk menghasilkan kunci yang sulit ditebak, sehingga menjaga keamanan data untuk mencegah serangan kriptanalis.

- Inisialisasi Vektor Awal (IV).

  Dalam mode operasi beberapa algoritma enkripsi blok, seperti *Cipher Block Chaining* (CBC) dan *Galois Counter Mod*e (GCM), IV digunakan untuk memulai proses enkripsi.

- Penambahan *Salt*

  Dalam fungsi hash kriptografis, seperti SHA-256, penambahan *salt* dilakukan untuk meningkatkan keamanan hash, misalkan pada kata sandi.

- Protokol Kriptografi

  Protokol kriptografi, seperti SSL/TLS yang digunakan dalam komunikasi aman di web, memanfaatkan bilangan acak semu untuk generasi kunci sesi yang aman dan menghindari replay attack (serangan ulang).

Pentingnya kekuatan dan keunikan bilangan acak semu dalam kriptografi telah memicu pengembangan berbagai metode dan algoritma untuk menghasilkan bilangan acak semu yang kuat. PRNG (*Pseudorandom Number Generator*) sebagai algoritma yang menghasilkan deret bilangan yang tampak acak ttidak cukup aman karena dapat diprediksi jika *seed* awalnya diketahui. Oleh karena itu, digunakanlah CSPRNG (*Cryptographically Secure Pseudorandom Number Generator*), yang didesain khusus untuk keperluan kriptografi. Salah satu metode untuk CSPRNG adalah pemanfaatan teori *chaos*.

Teori *chaos* adalah cabang matematika yang mempelajari perilaku sistem dinamika nonlinier yang sangat sensitif terhadap kondisi awal. Sistem yang mengikuti teori chaos memiliki sifat *non-deterministik*, kompleks, ergodisitas, dan acak dalam jangka panjang. Fenomena ini ditemukan pada awal abad ke-20 oleh sejumlah matematikawan seperti Poincaré, Birkhoff, dan Lorenz. Teori *chaos* membantu meningkatkan kekuatan kriptografi dengan menghasilkan deret bilangan acak yang sulit diprediksi dan menjaga kerahasiaan informasi. Fungsi *chaos* seperti *Henon map* maupun *Sine map* memiliki aplikasi dalam pembangkitan bilangan acak, kriptografi, dan analisis sistem dinamika nonlinier.

II. TEORI DASAR

A. Bilangan Acak Semu

Bilangan acak semu (*pseudorandom*) adalah serangkaian angka yang dihasilkan secara tidak terduga dan tampak acak. Meskipun sebenarnya tidak sepenuhnya acak, bilangan acak semu digunakan untuk mensimulasikan keacakan dalam berbagai aplikasi dan algoritma. Bilangan acak semu umumnya dihasilkan oleh algoritma yang menghasilkan deret angka berdasarkan suatu rumus matematika atau pola tertentu.

Algoritma ini memanfaatkan kondisi awal yang disebut "*seed*" dan menggunakan operasi matematika dalam algoritma. Dari sudut pandang kriptografi, sebuah pembangkit bilangan acak semu harus memiliki parameter penting berikut:

- Periode dalam bilangan acak yang dihasilkan harus cukup besar sehingga tidak mudah diprediksi
- Menghasilkan bilangan acak dengan cara yang praktis dan mudah dilakukan.
- Secara statistik lolos uji keacakan (*randomness test*)
- Tahan terhadap serangan attack yang serius. Serangan ini bertujuan untuk memprediksi bilangan acak yang dihasilkan dari nilai nilai sebelumnya.

B. Teori Chaos

Teori *Chaos* adalah sebuah cabang dalam matematika yang mempelajari perilaku sistem dinamis yang sangat sensitif terhadap kondisi awal. Dalam sistem yang memiliki sifat *chaos*, perubahan kecil dalam kondisi awal dapat menghasilkan perubahan yang sangat besar dan tidak dapat diprediksi dalam jangka waktu yang lama. Istilah "*chaos*" di sini merujuk pada kompleksitas yang tinggi dan ketidakdugaan yang terjadi dalam sistem tersebut.

Dalam konteks kriptografi, teori chaos memiliki penerapan penting. Prinsip-prinsip teori chaos digunakan dalam menghasilkan bilangan acak semu yang kuat untuk kunci enkripsi dan pengacakan data. Sifat ketidakdugaan, sensitivitas terhadap kondisi awal, dan efek gelembung informasi dalam sistem keos memberikan dasar yang kuat untuk menghasilkan urutan angka yang tidak dapat diprediksi dan mengamankan proses kriptografi. Perilaku yang tidak dapat diprediksi dari *chaos map* ini digunakan dalam pembangkitan bilangan acak. Salah satu generator bilangan acak berbasis *chaos* yang paling awal mencoba adalah *logistic map*.

C. Henon Map

Henon Map merupakan salah satu fungsi *chaos* pada ruang fase dua dimensi. *Henon Map* didefinisikan oleh dua persamaan rekursif sebagai berikut.

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

$$y_{n+1} = bx_n$$

Dalam persamaan di atas, x_n dan y_n adalah koordinat titik pada ruang fase, sedangkan a dan b adalah parameter yang mengontrol perilaku map. *Henon map* menghasilkan serangkaian pasangan koordinat $(x_n,\ y_n)$ yang mewakili pergerakan dalam ruang fase.

Perilaku *Henon Map* sangat bergantung pada nilai-nilai parameter *a* dan *b*. Ketika nilai parameter dipilih dengan baik, peta ini dapat menunjukkan sifat *chaos* seperti sensitivitas terhadap kondisi awal, orde tinggi dalam dinamika, dan perubahan yang tidak dapat diprediksi dalam jangka waktu yang lama. Parameter *Henon map* yang paling dasar digunakan adalah $a = 1.4$ dan $b = 0.3$. Dalam kriptografi, *map* ini dapat digunakan sebagai pembangkit bilangan acak semu

D. Sine Map

Sine Map merupakan fungsi *chaos* pada ruang fase satu dimensi yang mendasarkan perubahannya pada fungsi sinus, didefinisikan dengan fungsi berikut.

$$x_{n+1} = \mu \sin(\pi x_n)$$

Dalam persamaan di atas, x_n adalah nilai titik pada ruang fase pada iterasi ke-*n*, dan μ adalah parameter yang mengendalikan perilaku peta. Rentang nilai μ biasanya adalah antara 0 hingga 1, namun optimal ketika $\mu \in [0.87,1]$. *Sine Map* menggambarkan perubahan nonlinier pada ruang fase. Ketika nilai parameter μ dinaikkan, sistem mengalami bifurkasi secara periodik, di mana nilai-nilai x_n membentuk pola yang berulang dengan periode yang semakin kompleks. Fenomena ini mencerminkan sifat *chaos* dari *map* ini.

III. IMPLEMENTASI

Pembangkit bilangan acak semu yang baru dibuat dengan mengkombinasikan *Henon* dan *Sine Map* sebagai berikut

$$x_{n+1} = (1 - \mathrm{a}sin^2(x_n) + y_n) * 100\ mod\ 1$$

$$y_{n+1} = bx_n * 100\ mod\ 1$$

dengan parameter *a* dan *b* keduanya diperluas ke $(-\infty, +\infty)$.

Formula matematika di atas diimplementasikan dengan program python untuk membangkitkan bilangan acak. Berikut merupakan potongan program yang memanfaatkan ketiga fungsi di atas.

```
def henon_map(xn1,yn1):
        xn = 1 - a * math.pow(xn1, 2) + yn1
        yn = b * xn1
        return xn, yn
def sine_map(xn1):
        xn = r * math.sin(math.pi * x)
        return xn
def henon_sine_map(xn1,yn1):
        xn = (1 - a * math.pow(math.sin(x), 2) + y)*100 % 1
       yn = (b * x)*100 % 1
       return xn, yn
def generate():
        xns = []
        yns = []
        for _ in range(iteration):
           if (method == "HENON"):
              xn, yn = henon_map(xn1,yn1)
              xn1 = xn
              yn1 = yn
```

```
            xns.append(xn)
            yns.append(yn)
        elif (self.method == "SINE"):
            xn = sine_map(xn1)
            xn1 = xn
            xns.append(xn)
        elif (self.method == "HENON_SINE"):
            xn, yn = henon_sine_map(xn1,yn1)
            xn1 = xn
            yn1 = yn
            xns.append(xn)
            yns.append(yn)
        else:
            raise("Method is invalid")
    return xns, yns
```

Untuk visualisasi *Bifurcation* diagram dan *Lyapunov Exponent*, berikut rancangan program yang dibuat. Visualisasi pada bagian ini memanfaatkan *library matplotlib*.

1. Inisialisasi variabel
   - *iteration*, jumlah iterasi yang akan dilakukan pada pembangkitan bilangan acak.
   - *n*
   - *x*, array dengan nilai awal *0.1* sebanyak *n* elemen.
   - *y*, array dengan nilai awal *0.1* sebanyak *n* elemen.
   - *a*, pada *henon* dan *henon-sine map a* merupakan array pada suatu rentang nilai sebanyak *n* elemen.
   - μ, berupa nilai tetap μ pada *Henon-Sine* map, sedangkan pada *Sine map* berupa array pada suatu rentang nilai sebanyak *n* elemen.
   - λ, array dengan nilai awal *0* sebanyak *n* elemen.
2. *for loop* digunakan untuk melakukan iterasi sebanyak *iterations*.
3. Pada setiap iterasi, dilakukan pemanggilan fungsi *henon_map*, *sine_map*, dan *henon_sine_map* untuk memperbaharui nilai *x* dan *y*.
4. Selanjutnya, nilai Lyapunov exponent (λ) diupdate dengan fungsi lyapunov exponent yang melibatkan tiga fungsi turunan berikut.

$$\frac{dhenon}{dx} = -2 * a * x$$
$$\frac{dsine}{dx} = \pi\mu\cos(\pi x)$$
$$\frac{dhenon\_sine}{dx} = -200 * a * \sin(x) * \cos(x)$$

5. Plot *bifurcation* diagram dengan menggunakan *a* atau μ pada sumbu-*x* sebagai parameter yang divariasikan, serta *x* pada sumbu-*y* sebagai bilangan acak yang dibangkitkan pada setiap iterasi.
6. Setelah *for loop* selesai, dilakukan plot *Lyapunov exponen*t diagram dengan menggunakan *a* atau μ pada sumbu-*x* sebagi parameter yang divariasikan, serta λ pada sumbu-*y* yang mereperesentasikan nilai *Lyapunov exponent*.

IV. Analisis

Henon-Sine map yang diusulkan memiliki *behavior chaos* yang lebih baik dibandingkan dengan dua *map* awal.Berikut merupakan hasil analisis *chaotic map* yang telah dibuat.

A. *Phase Diagram*

Pada pembangkitan bilangan acak, *phase* diagram digunakan untuk memvisualisasikan trajektori hubungan antara nilai x_n dengan nilai x_{n+1}.

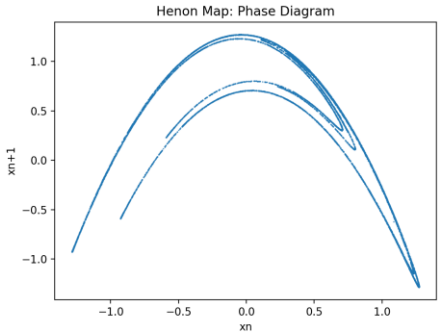

Fig. 1. *Phase* diagram *Henon Map*

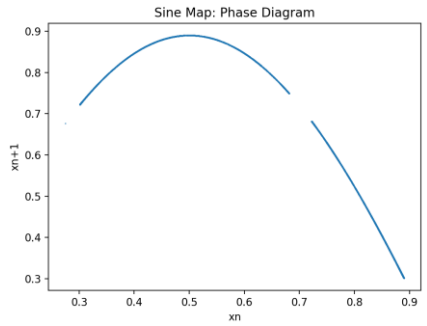

Fig. 2. *Phase* diagram *Sine Map*

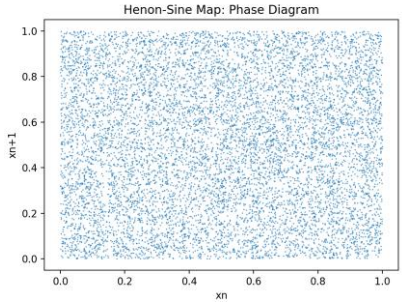

Fig. 3. *Phase* diagram *Henon-Sine Map*

Dengan menggunakan nilai awal dan parameter yang sama pada ketiga fungsi di atas, dapat ditunjukkan bahwa *Henon-Sine Map* terdistribusi di seluruh rentang dari bidang dan lebih terdistribusi dibandingkan dengan diagram fase dari *Henon Map* dan *Sine Map*. Gambar 1-2 ini menunjukkan bahwa trajektori kedua map tersebut tidak terlalu kompleks dan mengarah pada sifat deterministik, sehingga kedua *map* tersebut dapat diprediksi dengan mudah dan tidak cukup aman. Oleh karena itu, *Henon-Sine* memiliki ergodisitas yang lebih baik dan keluaran yang lebih acak, dibandingkan dengan *Henon* dan *Sine Map*.

Analisis lebih lanjut dilakukan dengan memvisualisasikan *phase* diagram dari pembangkit bilangan acak dari *library python* yaitu *random()*. Fungsi tersebut membangkitkan bilangan *float* secara uniform pada rentang 0 hingga 1, serta telah diuji secara ekstensif.

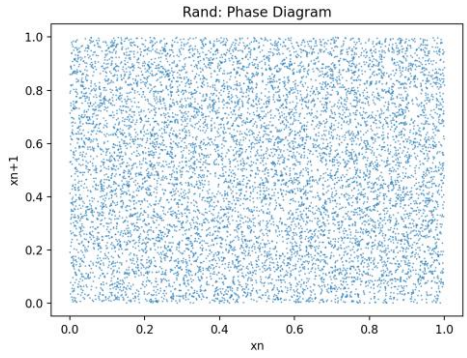

Fig. 4. *Phase* diagram *library random*

Pada gambar di atas, dapat dibandingkan bahwa distribusi bilangan acak hasil *Henon-Sine map* mendekati distribusi fungsi *random*.

B. Bifurcation Diagram

Bifurcation diagram merupakan visualisasi grafis yang menggambarkan perubahan perilaku fungsi nonlinier seiring dengan perubahan suatu parameter yang dapat dikendalikan. Pada *bifurcation* diagram, sumbu horizontal mewakili nilai parameter yang diubah. Pada pengujian ini, parameter yang diubah pada *Sine Map* adalah μ, sementara parameter yang diubah pada *Henon Map* dan *Henon-Sine Map* adalah a. Sumbu vertikal mewakili nilai yang diamati, dalam hal ini adalah nilai bilangan acak yang dibangkitkan (x). Pada setiap nilai parameter, titik pada *bifurcation* diagram mewakili nilai-nilai yang dicapai oleh fungsi setelah beberapa iterasi.

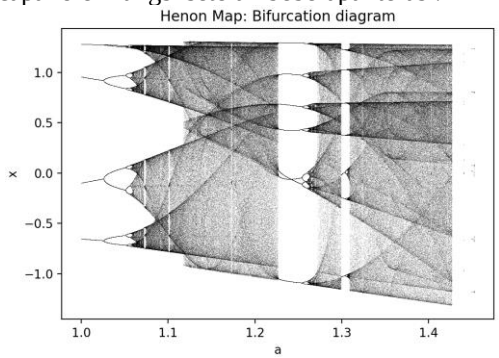

Fig. 5. Bifurcation diagram *Henon Map*

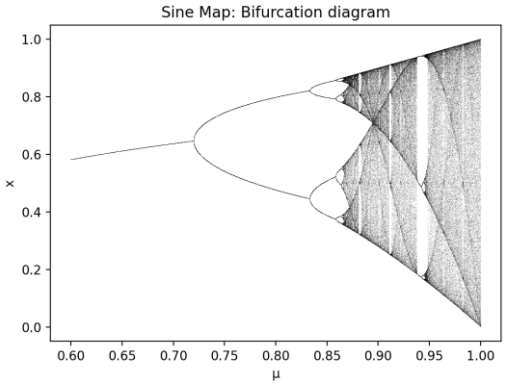

Fig. 6. Bifurcation diagram *Sine Map*

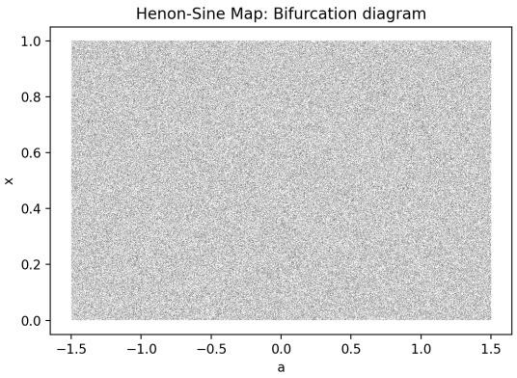

Fig. 7. Bifurcation diagram *Henon-Sine Map*

Gambar 7 menunjukkan bahwa *Henon-Sine map* tidak memiliki keadaan periodik apa pun, melainkan sangat kacau. Di sisi lain, Gambar 5 dan 6 menunjukkan bahwa *Henon map* dan *Sine map* yang memiliki perulangan yang semakin kompleks ketika parameter semaki besar, namun terdapat rentang nilai arameter tertentu yang menyebabkan nilai *x* yang dihasilkan tidak cukup acak. Oleh karena itu, keadaan *chaos* pada *Henon-Sine map* memiliki rentang parameter yang luas, menunjukkan bahwa dapat meningkatkan ruang kunci untuk aplikasi kriptografi.

C. *Lyapunov Exponent*

Lyapunov exponent adalah sebuah konsep dalam teori sistem dinamika yang digunakan untuk mengukur tingkat kepekaan sistem terhadap perubahan kecil pada kondisi awal. Lyapunov exponent menggambarkan laju pertumbuhan atau penurunan eksponensial dari perbedaan antara dua nilai yang berdekatan dalam ruang fase sistem. Misalkan, untuk perubahan setiap *value* dari parameter r, didefinisikan fungsi *Lyapunov exponent* sebagai berikut.

$$\lambda(\mathrm{r}) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} log \left| \frac{df_r}{dx}(x_i) \right|$$

Lyapunov exponent dapat memberikan informasi tentang stabilitas, kekacauan, dan prediktabilitas sistem dinamika nonlinier. Nilai *Lyapunov exponent* yang positif ($\lambda > 0$) menunjukkan bahwa sistem sensitif terhadap kondisi awal, sehingga seuatu sistem dinamis bersifat *chaotic*. Sebaliknya, *Lyapunov exponent* dengan nilai negatif menunjukkan bahwa sistem konvergen ke suatu titik atau siklus stabil. Berikut adalah hasil analisis *Lyapunov exponent* pada ketiga fungsi *chaos* di atas.

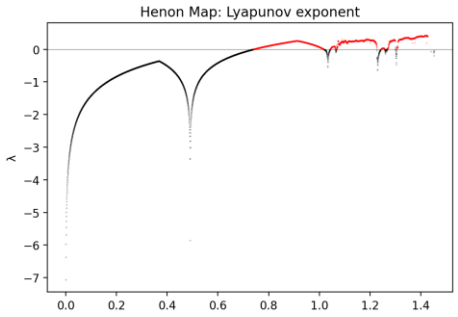

Fig. 8. *Lyapunov exponent Henon Map*

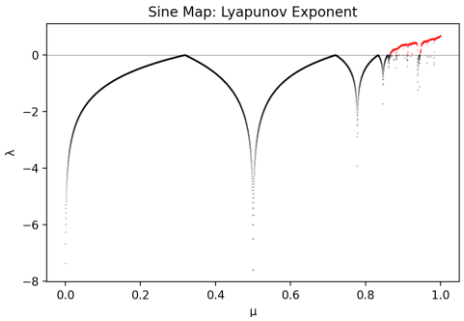

Fig. 9. *Lyapunov exponent Sine Map*

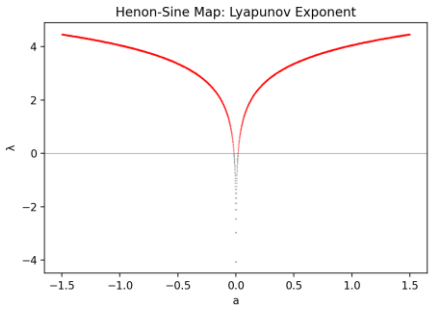

Fig. 10. *Lyapunov exponent Henon-Sine Map*

Gambar 8-10 menunjukkan bahwa *Henon-Sine* Map memiliki rentang *chaos* yang lebih besar serta *nilai lyapunov exponent* yang lebih tinggi dibandingkan Henon Map dan Sine Map. Artinya , *Henon-Sine* map lebih sensitif terhadap nilai awal dibandingkan dengan *Henon map* maupun *Sine map* karena bilangan acak yang dihasilkan semakin tidak terprediksi. Dengan fungsi di atas, dapat diketahui bahwa *Henon-Sine Map* memiliki *chaotic behavior* ketika nilai $a \in (-\infty, -0.031] \cup [0.031, \infty), b = 0.3$.

D. *Sensitivitas Nilai Awal*

Untuk analisis lebih lanjut, dilakukan variasi nilai awal x dan y dengan total 50 iterasi pada *Henon-Sine map* yang menghasilkan bilangan acak sebagai berikut.

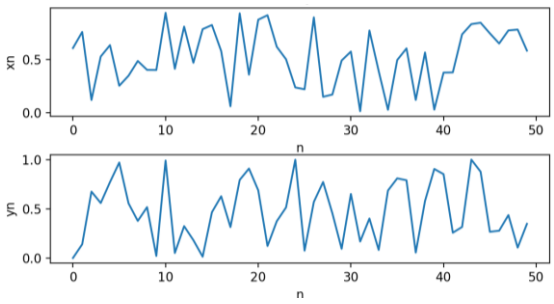

Fig. 11. Variasi $x_0 = 0.1$ dan $y_0 = 0.1$

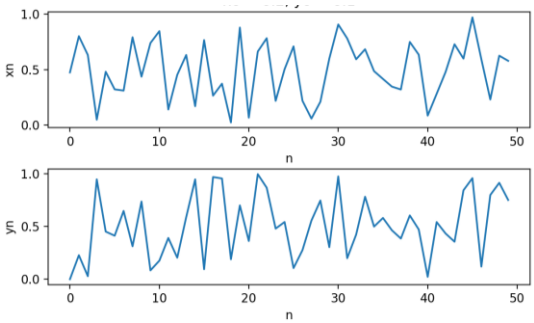

Fig. 12. Variasi $x_0 = 0.2$ dan $y_0 = 0.1$

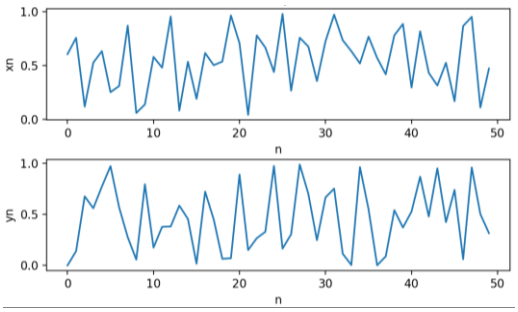

Fig. 13. Variasi $x_0 = 0.1$ dan $y_0 = 0.2$

Grafik di atas menunjukkan bahwa sistem Henon-Sine Map sangat sensitif terhadap kondisi awal, yaitu nilai awal x_0 dan y_0. Meskipun perubahan kecil dalam nilai x_0 atau y_0, perubahan yang dihasilkan signifikan pada pembangkitan bilangan acak di setiap iterasi. Sifat sensitivitas terhadap kondisi awal ini sering kali terkait dengan sifat kekacauan dalam sistem dinamika nonlinier. Selain itu, periode hasil bilangan acak yang dibangkitkan juga sangat besar. Dalam konteks *Henon-Sine Map*, *behavior chaos* ini dapat menghasilkan output yang terlihat acak dan tidak dapat diprediksi.

V. KESIMPULAN

Dalam makalah ini, telah berhasil dikembangkan sebuah fungsi chaos yang menggabungkan *Henon Map* dan *Sine Map* untuk pembangkit bilangan acak semu. Fungsi ini menunjukkan peningkatan performa dengan menghasilkan deret angka acak yang memiliki tingkat keacakan yang lebih baik dan lebih sulit diprediksi. Hasil dari fungsi tersebut dievaluasi melalui analisis menggunakan beberapa pengujian statistik, termasuk *phase* diagram untuk memvisualisasikan trajektori, *bifurcation* diagram untuk memahami perubahan perilaku sistem dengan variasi parameter, *Lyapunov Exponent* untuk mengukur tingkat kekacauan sistem, dan analisis sensitivitas terhadap variasi nilai awal. Analisis yang dilakukan memberikan wawasan penting tentang sifat dan performa dari fungsi *chaos* yang dikembangkan ini, serta memberikan pemahaman lebih dalam tentang karakteristik kekacauan dan penggunaan bilangan acak semu dalam aplikasi kriptografi.

UCAPAN TERIMAKASIH

Pertama-tama, penulis memanjatkan puji dan syukur atas kehadirat Tuhan Yang Maha Esa yang telah memberikan berkat dan rahmat yang tak terhingga, sehingga akhirnya penulis dapat menyelesaikan makalah ini dengan baik. Penulis mengucapkan terima kasih kepada semua pihak yang telah mendukung penulis dalam proses penulisan makalah ini. Khususnya kepada dosen pengampu Kriptografi IF40120, yaitu Bapak Rinaldi Munir yang telah mengajarkan dan membagi ilmunya yang diperlukan dalam penulisan makalah ini, beserta asisten yang telah membantu proses perkuliahan.

DAFTAR PUSTAKA

[1] Munir, Rinaldi. Pembangkit Bilangan Acak (Bahan Kuliah IF4020 Kriptografi). 2023.
Diakses pada 18 Mei 2023
(https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/37-Pembangkit-bilangan-acak-2023.pdf)

[2] Kocarev, L. Chaos-based cryptography: a brief overview. IEEE Circuits Syst. Mag. 1, 6–21. 2001.

[3] Lambić, D., Nikolić, M.: Pseudo-random number generator based on discrete-space chaotic map. Nonlinear Dyn. 90, 223–232. 2017.

[4] Wolf, A.: Quantifying Chaos with Lyapunov Exponents. Princeton University Press. 13, 273–289 (1986)

[5] Short K M. Steps toward unmasking secure communications[J]. International Journal of Bifurcation and Chaos. 4(04): 959-977. 1994.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 22 Mei 2023

Putri Nurhaliza