



# GAUSS ITERATED MAP

T U G A S   A K H I R   K R I P T O G R A F I  
T E K N I K   K O M P U T E R   U I   2 0 2 4



# OUR MEMBERS



Miranty Anjani Putri  
NPM 2006468270



Viony Elizabeth  
NPM 2006468371



M. Taqiy Nur Furqon  
NPM 2006468900



# ABOUT GAUSS CIRCLE MAP

Gauss map => fungsi iteratif yang didefinisikan oleh persamaan:

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

di mana a dan b adalah parameter

Learn More

02



# ABOUT GAUSS CIRCLE MAP

Untuk meningkatkan tingkat keamanan dapat dilakukan kombinasi Fungsi dengan Circle Combination. Yang setelah diturunkan, akan didapatkan persamaan sebagai berikut:

$$x_{n+1} = e^{-\alpha \left( \frac{5}{4} \left( (x_n + \Omega + \frac{K}{2\pi} \sin(2\pi x_n)) \bmod 1 \right) - \frac{1}{2} \right)^2} + \beta$$

di mana a dan b adalah parameter



# UI GAUSS ITERATED MAP





# HASIL UJI NIST

Type of Test	P-Value	Conclusion
Frequency Test (Monobit)	0.008879	Non-Random
<b>Frequency Test within a Block</b>	<b>0.350485</b>	<b>Random</b>
<b>Run Test</b>	<b>0.122325</b>	<b>Random</b>
<b>Longest Run of Ones in a Block</b>	<b>0.350485</b>	<b>Random</b>
<b>Binary Matrix Rank Test</b>	<b>0.534146</b>	<b>Random</b>
<b>Discrete Fourier Transform (Spectral) Test</b>	<b>0.911413</b>	<b>Random</b>
<b>Non-Overlapping Template Matching Test</b>	<b>0.911413</b>	<b>Random</b>
<b>Overlapping Template Matching Test</b>	<b>0.534146</b>	<b>Random</b>
Maurer's Universal Statistical Test	0	Non-Random

Type of Test	P-Value	Conclusion
<b>Linear Complexity Test</b>	<b>0.739918</b>	<b>Random</b>
<b>Serial Test</b>	<b>0.911413</b>	<b>Random</b>
<b>Serial Test</b>	<b>0.991468</b>	<b>Random</b>
Approximate Entropy Test	0	Non-Random
Cumulative Sums (Forward) Test	0.008879	Non-Random
Cumulative Sums (Reverse) Test	0.004301	Non-Random
Random Excursions Test	0	Non-Random
Random Excursions Variant Test	0	Non-Random

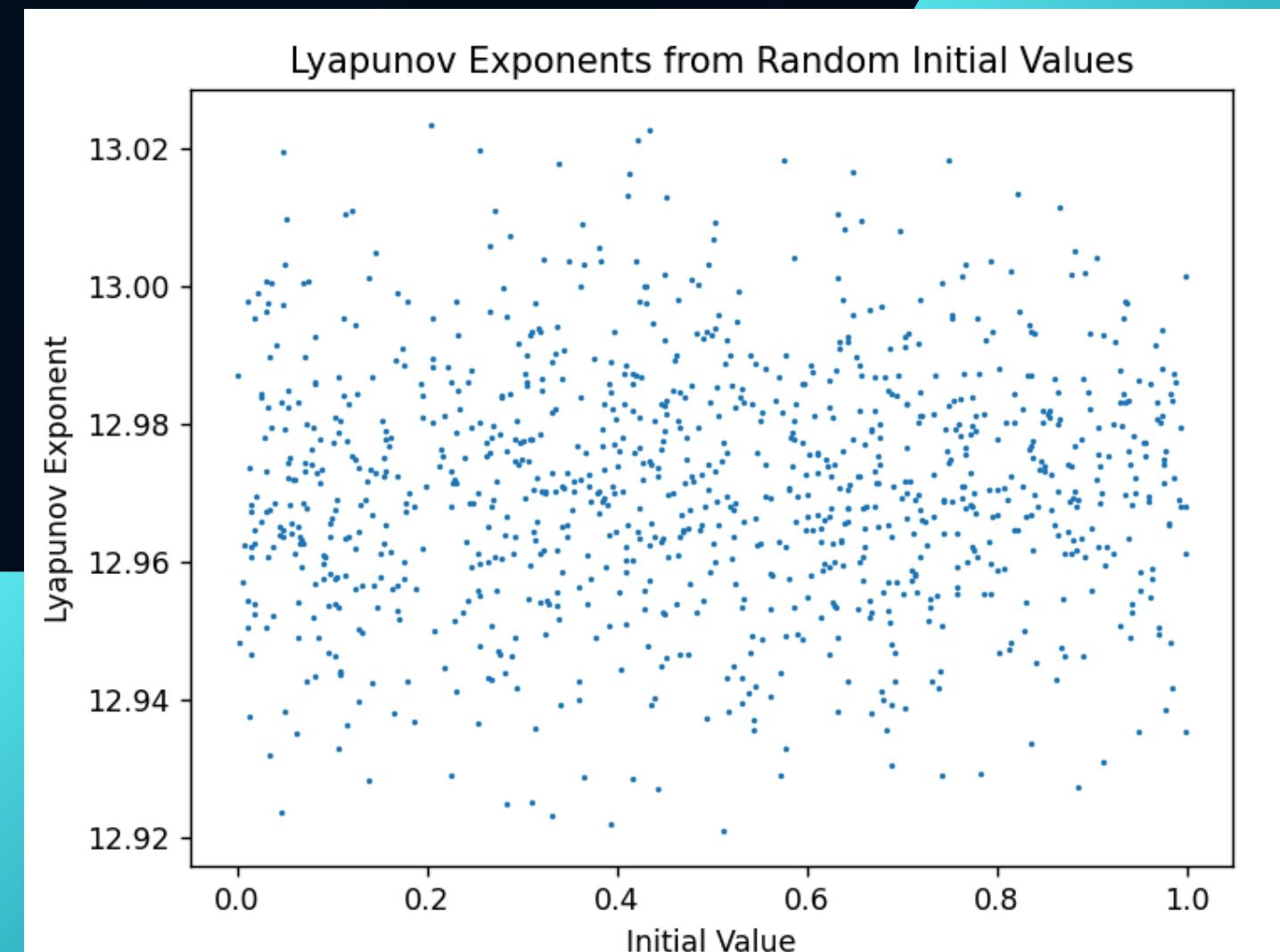


# UJI SENSIVITAS NILAI AWAL

Kami menggunakan Lyapunov Exponent (LE) untuk menguji sensitivitas nilai awal.

$$F^t(x_0 + \epsilon) - F^t(x_0) \approx \epsilon e^{\lambda t}$$

Lyapunov Exponen mengukur seberapa cepat dua keadaan dengan jarak yang dekat mengalami peningkatan jarak dari waktu ke waktu. Jika kedua titik itu tetap dekat maka sistem tidak chaos. Jika terjadi perubahan yang signifikan, maka sistem dapat dikatakan chaos.





# UJI ERGODISITY

Pengujian ini dilakukan untuk melihat apakah system yang dibangun akan menunjukkan semua kemungkinan yang dapat terjadi. Kami menggunakan Chi Square untuk menguji ergodisity dari system kami.

```
PS D:\Me\Tugas Kuliah\semester 8\Kripto\UAS\Gauss-Iterated-Cryptography\Code> python gauss_iterated_test.py
Chi-Square Statistic: 10.92, P-value: 0.28123243650941077
The distribution of states fits the expected uniform distribution.
```

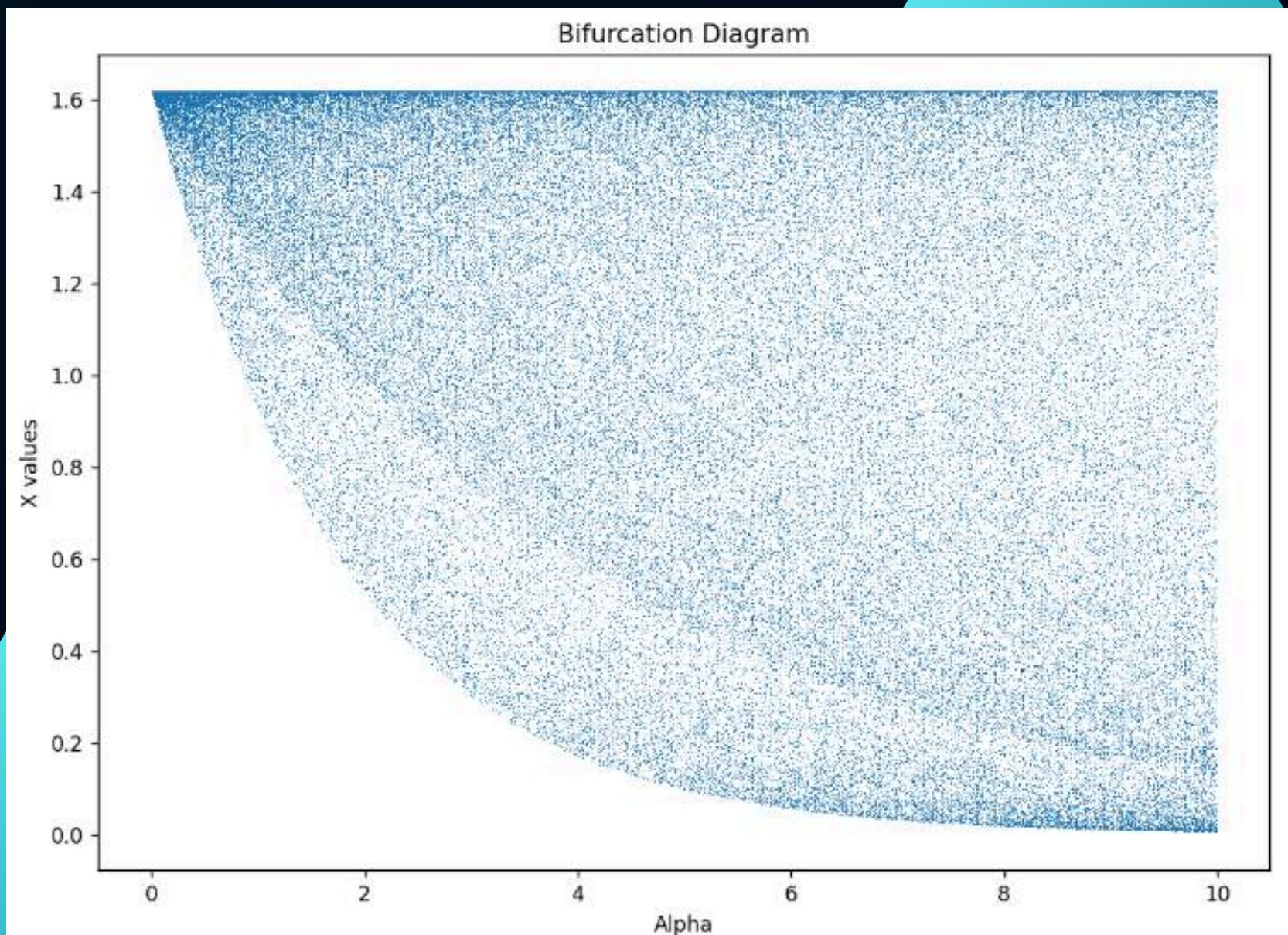
Perhitungan chi square kami menghitung perbedaan antara frekuensi terobservasi di setiap bin (pecahan data yang dikumpulkan) dan frekuensi yang diekspetasikan melalui perhitungan distribusi ini. Algoritma pengujian kami mendapatkan bahwa system kami ergodic atau dengan kata lain dapat menunjukkan semua kemungkinan outputnya.



# UJI KORELASI

Kami menggunakan Bifurcation Diagram untuk menguji ergodisity dari system kami.

Diagram ini menunjukkan nilai-nilai yang dikunjungi atau didekati secara asimtotik (titik tetap, orbit periodik, atau penarik kacau) dari suatu sistem sebagai fungsi dari parameter bifurkasi dalam sistem. Ini merangkum perubahan perilaku kualitatif suatu persamaan karena parameternya bervariasi.





# UJI UACI (UNIFIED AVERAGE CHANGING INTENSITY)

UACI digunakan untuk mengukur rerate perbedaan intensitas antara piksel yang sama dalam dua gambar, satu gambar asli dan gambar yang diubah sedikit setelah enkripsi

Semakin tinggi nilai UACI berarti sedikit perubahan yang ada dari citra asli yang menyebabkan perubahan signifikan pada citra yang terenkripsi

Dari hasil pengujian didapatkan nilai Uji UACI

**UACI: 45.654834046069055**



# UJI NPCR (NUMBER OF PIXELS CHANGING RATE)

UACI digunakan untuk mengukur persentase piksel yang berbeda antara dua gambar yang terenkripsi ketika ada sedikit perubahan pada gambar aslinya

Semakin tinggi nilai NPCR berarti sedikit perubahan yang ada dari citra asli yang menyebabkan perubahan signifikan pada citra yang terenkripsi

Dari hasil pengujian didapatkan nilai Uji NPCR

**NPCR: 99.53335048010975**



# UJI PSNR (PEAK SIGNAL-TO-NOISE-RATIO)

PSNR digunakan untuk mengevaluasi kualitas dari hasil pemrosesan citra dibandingkan dengan citra aslinya.

Rumus dari PSNR adalah

$$\text{PSNR} = 20 \cdot \log_{10} \left( \frac{\text{MAX}_I}{\text{RMSE}} \right)$$

MAX : nilai piksel maksimum dari citra

RMSE : root mean square error antara dua citra

Nilai yang lebih tinggi menunjukkan kualitas yang lebih baik. Ketika PSNR mencapai nilai yang tinggi, itu menunjukkan bahwa semakin sedikit perbedaan antara gambar asli dan gambar hasil pemrosesan.

PSNR: inf



# UJI WAKTU PROSES

Waktu pemrosesan dilakukan dengan melakukan pengukuran waktu dari sebelum fungsi enkripsi/dekripsi dijalankan dan setelah fungsi enkripsi/dekripsi selesai

```
Run 1: Encryption time: 15.154666423797607 seconds, Decryption time: 15.064035177230835
seconds
Run 2: Encryption time: 15.009799718856812 seconds, Decryption time: 14.73076844215393
seconds
Run 3: Encryption time: 14.0681471824646 seconds, Decryption time: 14.190502166748047
seconds
Run 4: Encryption time: 14.444775104522705 seconds, Decryption time: 13.969359636306763
seconds
Run 5: Encryption time: 14.869452476501465 seconds, Decryption time: 14.019267320632935
seconds
Run 6: Encryption time: 14.55416226387024 seconds, Decryption time: 15.934054136276245
seconds
Run 7: Encryption time: 15.422343015670776 seconds, Decryption time: 15.541199445724487
seconds
Run 8: Encryption time: 13.646287441253662 seconds, Decryption time: 14.883665800094604
seconds
Run 9: Encryption time: 14.874396085739136 seconds, Decryption time: 15.016717195510864
seconds
Run 10: Encryption time: 14.85313081741333 seconds, Decryption time: 14.11974287033081
seconds
Average encryption time over 10 runs: 14.689716053009032 seconds
Average decryption time over 10 runs: 14.746931219100953 seconds
```



# GITHUB

[https://github.com/MirantyAnjaniPutri/  
Gauss-Iterated-Cryptography](https://github.com/MirantyAnjaniPutri/Gauss-Iterated-Cryptography)





# THANK YOU

K E L O M P O K   0 1  
K E L A S   K R I P T O G R A F I  
T E K N I K   K O M P U T E R   U I   2 0 2 4