Título em Português:	Criptografia baseada em caos utilizando mapas de recorrência e autômatos celulares
Título em Inglês:	Chaos based cryptography using recurrence maps and cellular automata
Autor:	Nicolas Caldas Borsari
Instituição:	Universidade de São Paulo
Unidade:	Instituto de Física de São Carlos
Orientador:	Odemir Martinez Bruno
Área de Pesquisa / SubÁrea:	Matemática da Computação
Agência Financiadora:	CNPq - PIBIC

CRIPTOGRAFIA BASEADA EM CAOS UTIIZANDO MAPAS DE RECORRÊNCIA E AUTÔMATOS CELULARES

Nícolas Caldas Borsari

Prof. Dr. Odemir Martinez Bruno

Instituto de Física de São Carlos - IFSC/USP

nicborsari@usp.br

Objetivos

Este estudo tem como objetivo explorar e desenvolver técnicas de criptografia baseadas na aplicação de sistemas caóticos, especificamente mapas de recorrência e autômatos celulares, sugerindo uma nova forma de otimizar a segurança dos dados em um ambiente digital.

A capacidade intrínseca desses modelos gerarem comportamentos caóticos a partir de regras simples, capazes de produzir um Gerador de Números Pseudo-Aleatórios (PRNG) ideal para a construção de um robusto e seguro algoritimo criptográfico, se torna a motivação do projeto.

Pretende-se aqui estudar e contribuir ao campo da criptografia baseada em caos sob a luz de três sistemas: o Autômato Celular Elementar de Regra 30, o Atrator de Lorenz e o Mapa Logístico, além da implementação da técnica de ampliação de caos conhecida como *deep zoom* (MACHICAO; BRUNO, 2017).

Com novas perspectivas e abordagens, constrói-se então uma revisão e análise de conceitos caóticos e criptográficos já conhecidos, visando entender a viabilidade da integração entre eles. Espera-se também que os resultados aqui apresentados possam ser adotados em aplicações práticas de segurança da informação, fortalecendo a integridade e confidencialidade dos dados em um mundo digitalmente conectado.

Métodos e Procedimentos

Com o objetivo de integrar sistemas caóticos à técnicas de criptografia, optou-se pelo uso dos sistemas Autômato Celular Elementar de Regra 30, o Atrator de Lorenz e o Mapa Logístico como os fundamentos deste estudo. Caracterizados por comportamentos complexos gerados por regras simples, estes sistemas possuem propriedades únicas ideais para a construção de um algoritimo robusto. Vale ressaltar que, além de conceitos populares, tais modelos também já foram objeto de estudo pelo Scientific Computing Group (SCG), grupo que viabiliza este projeto.

Ao inicializar o algoritimo de criptografia, converte-se o texto alvo em seus valores UTF-8. Para o tratamento destes valores, o algoritimo proposto adota o Modo de Operação Caótico, apresentado por Marco et al. (2010). Este método de criptografia se fundamenta na operação lógica *xor*. Nele, o próximo valor da cifra é produzido por duas operações *xor* consecutivas. A primeira delas é entre o valor UTF-8 em questão *e* o byte aleatório gerado pelo PRNG, A segunda, então, executa *xor* entre este resultado e o valor anterior da cifra, conferindo um nível adicional de complexidade ao sistema. Portanto, é necessário gerar um byte extra C_0 antes de começar a cifrar o texto alvo. Vale notar que, devido à comutatividade e associatividade inerentes à operação *xor*, a

ordem em que são realizadas não alteram o resultado final, podendo ser facilmente revertida no momento de descriptografar.

O Autômato Celular Elementar de regra 30, sistema dinâmico discreto de comportamento caótico baseado em 8 condições simples, foi empregado para gerar as condições iniciais. Para isso, transforma-se a senha do usuário em um número binário, que configura a primeira geração do Autômato. Definidos os critérios de parada, as representações binárias das gerações correspondentes são convertidas para valores decimais pertencentes ao intervalo [0,1], à serem utilizados como origem para o PRNG. Além disso, também é gerado desta forma o byte inicial C_0 comentado anteriormente.

O Mapa Logístico e o Atrator de Lorenz são mapas de recorrência conhecidos por seus comportamentos caóticos para certos parâmetros, que serão aqui utilizados na geração do PRNG. O primeiro consiste em uma simples equação de segundo grau, enquanto o segundo é um sistema tridimencional onde o comportamento de suas variáveis é definido por um conjunto de 3 equações diferenciais. No entanto, ao analisar as propriedades do Mapa Logístico e do Atrator de Lorenz, percebeu-se que ambos possuem padrões de comportamento e não exploram uniformemente seus respectivos espaços de fase, fatores indesejáveis para um PRNG.

Para resolver este problema, adaptou-se estes dois sistemas a partir da operação de *k-deep zoom*, onde a variável *k* define a ordem da operação. Esta abordagem calcula, para um dado valor, o produto deste por 10^k, e então extrai o fracionário do resultado através da operação `floor`. Tal implementação confere resultados surpreendentes, aumentando o aproveitamento das regiões de alta complexidade dos valores produzidos sem alterar a eficiência computacional do algoritimo.

Com este tratamento, os dois sistemas foram utilizados para a construção de 2 PRNG, respectivamente. Para isto, itera-se o sistema, seja o Mapa Logístico ou o Atrator de Lorenz, a partir das condições iniciais, aplicando o *deep* zoom aos valores produzidos. No entanto, vale notar que há diferença entre as duas implementações. No caso do Atrator de Lorenz, os resultados das operações de *deep zoom* são reintegradas ao sistema, substituindo os valores precedentes. Já no Mapa Logístico, os resultados do *deep zoom* só são utilizados para a geração de números pseudo-aleatórios, sem interferir no cálculo da próxima geração.

Para ambos os métodos, define-se um número mínimo de iterações, evitando assim o período transiente. Após alcançar este valor temporal, os próximos valores gerados são transformados em bytes. Como os resultados estão uniformemente distribuídos entre 0 e 1, basta tomar o produto deste com o tamanho de um byte (256) e aplicar a função `floor`, obtendo assim um valor inteiro no intervalo [0,255], equivalente aos valores possíveis de um byte, construindo assim o PRNG desejado. Utilizando o Modo de Operação Caótico, a cifra é então produzida e, posteriormente, decifrada.

Após a implementação do processo descrito é imperativo, no entanto, avaliar seus resultados. Para isto, foram utilizados métodos estatísticos, gerando histogramas e incluindo dois testes de aleatoriedade reconhecidos internacionalmente, o NIST e o DIEHARDER Test Suite. Adicionalmente, a função SHA256 e a mensuração do tempo computacional necessário para a execução foram implementadas, fornecendo informações valiosas para uma análise aprofundada.

Resultados

A análise de um algoritimo criptográfico não é formalmente definida, com novas abordagens criptoanaliticas emergindo todos os anos. Neste contexto, nossa analise se atém na integridade da informação, na segurança proporcionada pelo método e em sua eficiência computacional.

Para avaliar a integridade da informação após implementação descrita, foi utilizada a função SHA256. Quando aplicada tanto ao texto original quanto ao decifrado, os valores *hash*

obtidos foram congruentes, garantindo a integridade dos dados recuperados após a criptografia.

Para a qualidade e robustez do algoritimo criptográfico proposto, foi realizado um tratamento estatístico abrangente dos resultados. Primeiramente, foi necessário o impacto da técnica de *deep zoom* sobre os dados obtidos, para em um segundo momento analisar o funcionamento do algorítmo como um todo. As figuras abaixo mostram o espaço de fase dos dois sistemas caóticos utilizados no PRNG, antes e depois do uso desta técnica.

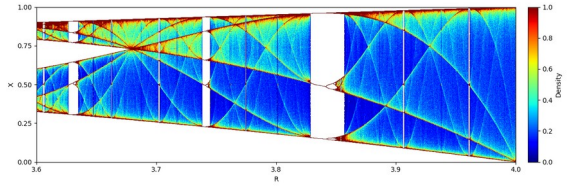


Figura 1: Diagrama de Bifurcação do Mapa Logístico para o *r* variando entre 3.6 e 4, sem *deep zoom*, com as cores representando a densidade local relativa ao conjunto.

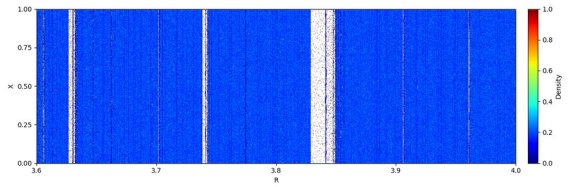
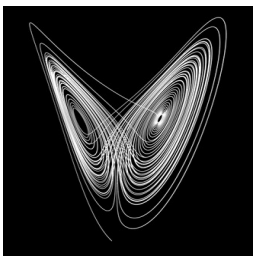
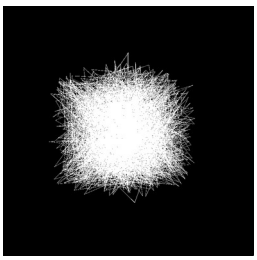


Figura 2: O mesmo diagrama, mas agora aplicando *deep zoom* com *k = 4.*





Figuras 3 e 4: Espaços de fase do Atrator de Lorenz para as mesmas condições iniciais. Na esquerda, sem *deep zoom*, e na direita com *deep zoom* de ordem *k = 5.*

Nas figuras apresentadas, fica evidente a transformação qualitativa que a técnica de *deep zoom* confere ao sistema. Sua ergodicidade, a capacidade de um sistema explorar todas as suas configurações possíveis, foi notavelmente ampliada. Também é perceptível que todos os padrões presentes nas configurações originais foram quebrados com o uso do *deep zoom.* Assim, a imprevisibilidade do sistema foi significantemente reforçada, tornando inviável a previsão de seu comportamento através de um ataque diferencial, por exemplo.

Para analisar a distribuição dos bytes gerados pelos PRNG, foram construídos histogramas para ambos os métodos, que podem ser vistos abaixo.

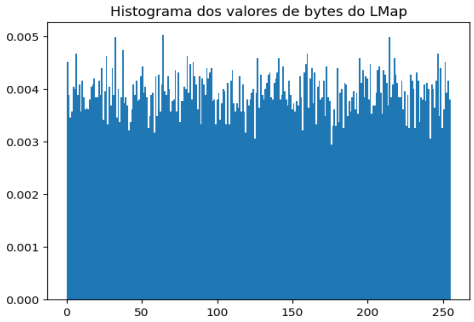


Figura 5: Histograma dos bytes gerados pelo PRNG baseado no k-Mapa Logístico de ordem *k = 4.*

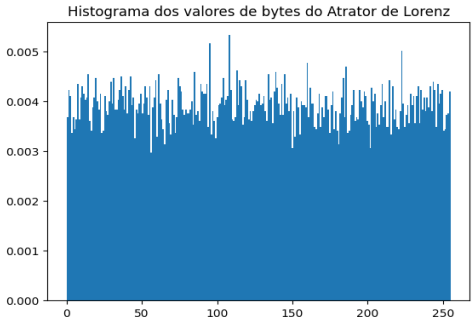


Figura 6: Histograma dos bytes gerados pelo PRNG baseado no k-Atrator de Lorenz de ordem *k = 5.*

Assim, uma distribuição uniforme e característica de comportamentos aleatórios foi evidenciada, sendo aparentemente ideal para um PRNG. Como ambos os sistemas foram

aceitos neste primeiro momento, avançou-se para a aplicação dos renomados NIST e DIEHARDER, que, no entanto, apontaram diferenças significativas em seus resultados.
Para ambos os testes, o mapa logístico apresentou saídas menos consistentes, indicando que, embora possa gerar números pseudoaleatórios, sua confiabilidade e robustez é questiionável. Em contraste, o atrator de Lorenz superou as expectativas, alinhando-se de maneira notável aos resultados esperados. Isto não só sugere que o Atrator de Lorenz é mais adequado que o mapa logístico para a confecção do algoritimo proposto, mas também garante que sua implementação culminará em um método criptográfico ideal para a era digital.
Finamente, a eficiência de seu funcionamento se mostrou de qualidade, apresentando tempos de execução dentro do aceitável. Porém, este estudo não foi aprofundado no mesmo nível feito para a segurança e integridade dos dados, que passaram por testes rigorosos. Este ponto pode ser um foco para otimizações futuras.
Vale ressaltar que a implementação de certas técnicas, como o Modo de Operação Caótico e a geração de condições a partir do Autômato Celular de regra 30, reforçam a segurança do sistema ao conferir mais camadas de complexidade para a quebra do algoritimo.

Conclusões

A aplicação de sistemas caóticos na criptografia reforça a relevância da teoria do caos no cenário da segurança cibernética. Neste contexto, esta pesquisa contribui com nuances e abordagens relevantes para a área. Os resultados vistos no uso de sistemas como o Autômato Celular de Regra 30, o Atrator de Lorenz e o Mapa Logístico não apenas introduzem um nível adicional de complexidade e imprevisibilidade, mas também oferecem um grande potencial para serem empregados em técnicas e métodos em criptografia.
Embora o Modo de Operação Caótico e o Autômato Celular de Regra 30 tenham incrementado a complexidade e a segurança do algoritmo, os resultados dos testes estatísticos utilizados evidenciam que a escolha do sistema caótico adequado é um fator determinante para a qualidade do algorítmo. Neste sentido, o k-Atrator de Lorenz recebe destaque especial, sendo então o sistema que de fato cumpre o que foi proposto, garantindo que sua implementação para tais objetivos é coerente com o mundo digital atual.
Assim sendo, a integração deste sistema caótico não só atingiu os objetivos propostos, de estudo e construção de um robusto e confiável sistema criptográfico, como também apresenta resultados instigantes para a continuação do desenvolvimento científico nesta área. O algorítmo proposto é uma possibilidade para fortalecer ainda mais a integridade e confidencialidade dos dados presentes nos dia de hoje.
No entanto, o contínuo avanço da tecnologia e as novas ameaças emergentes requerem que toda metodologia criptográfica seja constantemente revisada e adaptada, reassegurando sua aplicabilidade prática. Enquanto os resultados preliminares aqui descritos são promissores, principalmente nos quesitos de segurança e imprevisibilidade, há espaço para que pesquisas adicionais avaliem plenamente a viabilidade desta implementação em cenários práticos.

Agradecimentos

Agradeço ao Professor Dr. Odemir M. Bruno por toda a experiência acadêmica proporcionada, abordando diversos temas em conversas e estudos aprofundados que agregaram muito aos meus conhecimentos. Agradeço também ao Scientific Computing Group e à toda infraestrutura garantida ao grupo pela USP, sem os quais seria impossível a realização deste trabalho. Por último, mas não menos importante, agradeço ao meu companheiro de pesquisa Kauê H. Bazilli, com sua sagacidade e disposição sempre presentes nos momentos cruciais do desenvolvimento do projeto.

Referências

1. BAPTISTA, M. S. Cryptography with chaos. **Physics Letters A**, v. 240, n. 1-2, p. 50-54, mar. 1998. Disponível em: https://doi.org/10.1016/s0375-9601(98)00086-3.

2. WOLFRAM, Stephen. **New Kind of Science**. [S. l.]: Wolfram Media, 2002. ISBN 1579550088. Disponível em: https://www.wolframscience.com.

3. MARCO, Anderson Gonçalves; MARTINEZ, Alexandre Souto; BRUNO, Odemir Martinez. Fast, parallel, and secure cryptography algorithm using lorenz's attractor. **International Journal of Modern Physics C**, v. 21, n. 03, p. 365-382, mar. 2010. Disponível em: https://doi.org/10.1142/s0129183110015166.

4. JUSTO, M. J. M. **Autômatos celulares caóticos aplicados na Criptografia e Criptoanálise**. 2013. Dissertação (Mestrado) – Universidade de São Paulo, São Carlos, 2013. Disponível em: http://www.teses.usp.br/teses/disponiveis/76/76132/tde-20092013-153518/.

5. MACHICAO, Jeaneth; BRUNO, Odemir M. Improving the pseudo-randomness properties of chaotic maps using deep-zoom. **Chaos: An Interdisciplinary Journal of Nonlinear Science**, v. 27, n. 5, p. 053116, maio 2017. Disponível em: https://doi.org/10.1063/1.4983836.

6. MACHICAO, Jeaneth et al. Exploiting ergodicity of the logistic map using deep-zoom to improve security of chaos-based cryptosystems. **International Journal of Modern Physics C**, v. 30, n. 05, p. 1950033, maio 2019. Disponível em: https://doi.org/10.1142/s0129183119500335.

7. MACHICAO, Jeaneth; BRUNO, Odemir M.; BAPTISTA, Murilo S. Zooming into chaos as a pathway for the creation of a fast, light and reliable cryptosystem. **Nonlinear Dynamics**, v. 104, n. 1, p. 753-764, 22 fev. 2021. Disponível em: https://doi.org/10.1007/s11071-021-06280-y.

CHAOS-BASED CRYPTOGRAPHY USING RECURRENCE MAPS AND CELLULAR AUTOMATA

Nícolas Caldas Borsari

Prof. Dr. Odemir Martinez Bruno

São Carlos Institute of Physics - IFSC/USP

nicborsari@usp.br

Objectives

The primary goal of this study is to explore and develop cryptographic techniques grounded on the application of chaotic systems, specifically recurrence maps and cellular automata. It presents a new way to optimize data security in a digital environment.

The intrinsic capability of these models to produce chaotic behaviors from simple rules, capable of yielding an ideal Pseudo-Random Number Generator (PRNG) for creating a strong and secure cryptographic algorithm, serves as the motivation for this project.

It is intended to study and contribute to the field of chaos-based cryptography examining three systems, namely the Elementary Cellular Automaton with Rule 30, the Lorenz Attractor, and the Logistic Map, in addition to the implementation of a chaos amplification technique known as *deep zoom* (MACHICAO; BRUNO, 2017).

By introducing new perspectives and approaches, it is made a comprehensive review and analysis of established chaotic and cryptographic concepts, aiming to assess the feasibility of their integration. It is also expected that the results presented here can be adopted in practical information security applications, strengthening data integrity and confidentiality in a digitally connected world

Materials and Methods

To integrate chaotic systems into cryptographic techniques, the Elementary Cellular Automaton Rule 30, the Lorenz Attractor, and the Logistic Map were chosen as the foundations of this study. Characterized by complex behaviors driven by simple rules, these systems have unique properties optimal for crafting a robust algorithm. It's noteworthy that, besides being popular concepts, these models have also been previously studied by the Scientific Computing Group (SCG), the group making this project possible.

In the algorythm beggining, the target text is converted to its UTF-8 values. For processing these values, the proposed algorithm adopts the Chaotic Operation Mode, introduced by Marco et al. (2010). This encryption technique relies on the logical *xor* operation. It says that the next cipher value emerges from two consecutive xor operations. The initial operation is between the correspondent UTF-8 value and the random byte produced by the PRNG. The subsequent operation executes *xor* between this result and the prior cipher value, adding another layer of complexity to the system. Hence, it is necessary to generate an extra byte C_0 before start ciphering the target text. Notably, due to the inherent commutativity and associativity of the xor function, the sequence

of operations doesn't alter the end result, being easily reversible, thus facilitating decryption.

The Elementary Cellular Automaton with Rule 30, a discrete dynamic system with chaotic behavior based on 8 simple conditions, was used for generating the initial conditions. The user's password is transformed into a binary number, configuring the Automaton's first generation. After setting the stopping criteria, the corresponding generations binary representations are converted into float values within the [0,1] range, to be used as the PRNG origin. The initial C_0 byte is also derived from one of the generations.

The Logistic Map and the Lorenz Attractor are recurrence maps renowned for their chaotic behaviors under certain parameters. The former is a basic quadratic equation, whereas the latter is a three-dimensional system with its behavior defined by a set of three differential equations. However, upon examining the Logistic Map and Lorenz Attractor properties, both were observed to have behavior patterns and do not uniformly exploit their respective phase spaces, undesirable features for a PRNG.

To address this problem, both systems were adapted using the *k-deep zoom* operation, where the *k* variable defines the operation's magnitude. This method calculates, for a given value, its product by 10^k, then extracts its result's fractional component through the `floor` operation. Such implementation yields surprising results, maximizing the usage of the high-complexity regions of the generated without altering the algorithm's computational efficiency.

With this treatment, these two systems were employed to build 2 PRNGs, respectively. To achieve this, the system is iterated from its initial conditions, applying deep zoom to the resultant values, being it based on the Logistic Map or on the Lorenz Attractor. However, there's a notable difference between the two implementations. In the Lorenz Attractor's case, the deep zoom operation results are reintegrated into the system, replacing its prior values. Iin the Logistic Map, however, *deep zoom* results are solely used for generating pseudo-random numbers, without influencing the calculation of the subsequent generation.

For both methods, a minimum iteration number is set, sidestepping the transient period. Upon reaching this time threshold, the subsequent generated values are converted into bytes. As the outcomes are uniformly distributed between 0 and 1, simply multiplying them by the byte size (256) and applying the floor function will produce an integer in the [0,255] range, which is equivalent of all possible byte values, thus creating the desired PRNG. Utilizing the Chaotic Operation Mode, the cipher is then produced and later decrypted.

After implementing the described process, however, it's imperative to assess its outcomes. Statistical methods were employed for this purpose, creating histograms and applying two internationally recognized randomness tests, the NIST and the DIEHARDER Test Suite. Additionally, the SHA256 function and the measurement of execution computational time were integrated, providing valuable information for a thorough analysis.

Results

The analysis of a cryptographic algorithm is not formally defined, with new cryptoanalytic approaches emerging every year. In this context, our assess focuses on data integrity, the security provided by the method, and its computational efficiency.

To evaluate the data integrity after the described implementation the SHA256 function was used. When applied to both the original and decrypted text, the obtained hash values were identical, ensuring the integrity of the data recovered after encryption.

For the quality and robustness of the proposed cryptographic algorithm, a comprehensive statistical treatment of the results was conducted. Firstly, the impact of the deep zoom technique on the obtained data was examined and, subsequently, the overall functioning of the algorithm. The figures below depict the phase

space of the two chaotic systems used in the PRNG, both before and after the application of this technique.

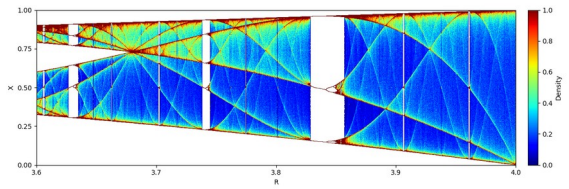


Figure 1: Bifurcation Diagram of the Logistic Map for *r* ranging from 3.6 to 4, whitout *deep zoom*, with colors representing the relative local density within the set.

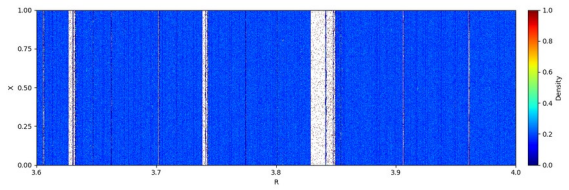
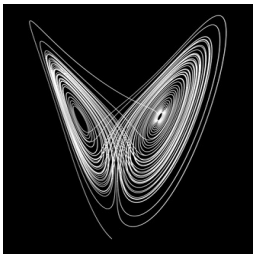
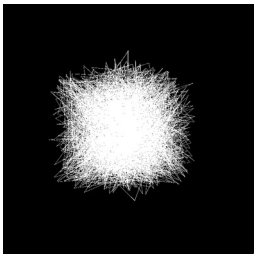


Figure 2: The same diagram, but now using *deep zoom* method with *k = 4.*





Figures 3 and 4: Phase spaces of the Lorenz Attractor for the same initial conditions. On the left, without *deep zoom,* and on the right, with a *deep zoom* of order *k = 5.*

In the presented figures, the system's qualitative transformation imparted by the deep zoom technique becomes evident. Its ergodicity, a system's capability to explore all of its possible configurations, was notably enhanced. It is also perceptible that all patterns present in the original configurations were disrupted with the use of deep zoom. Thus, the unpredictability of the system was significantly reinforced, making it impossible to predict its behavior by, for an example, a differential attack

To analyze the PRNG generated bytes distribuiton, histograms were constructed for both methods, as depicted below.

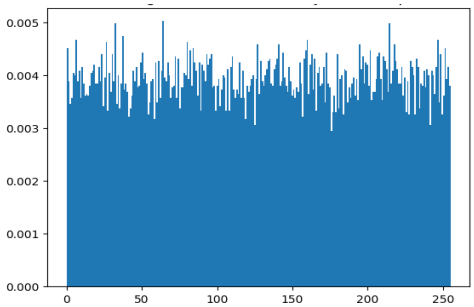


Figura 5: k-Logistic Map based PRNG generated bytes histogram, for *k = 4.*

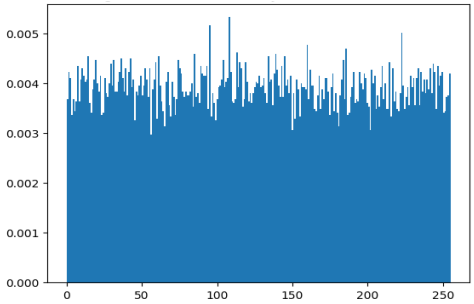


Figura 6: k-Lorenz Attractor based PRNG generated bytes histogram, for *k = 5.*

Now, a random behavior's charateristic uniform distribution were evidenced, apparently ideal for a PRNG. As both systems were accepted in this initial stage, further progress was made by applying the renowned NIST and DIEHARDER tests, which, however, revealed significant differences in their results.

For both tests, the logistic map exhibited less consistent outputs indicating that, although it can generate pseudo-random numbers, its reliability and robustness are questionable. In contrast, the Lorenz attractor exceeded expectations, aligning notably with the expected results. This not only suggests that the Lorenz Attractor is more suitable than the logistic map

for the proposed algorithm, but also ensures that its implementation will result in an ideal cryptographic method for the digital era.
Finally, the efficiency of its operation proved to be of high quality, with execution times falling within acceptable limits. However, it should be noted that this study did not delve as deeply into efficiency as it did into data security and integrity, which underwent rigorous testing. This point may serve as a focus for future optimizations.
It is worth emphasizing that the implementation of certain techniques, such as the Chaotic Operation Mode and the generation of initial conditions using Rule 30 Cellular Automaton, enhances system security by adding layers of complexity to the algorithm's breaking.

Conclusions

The application of chaotic systems in cryptography reinforces the relevance of chaos theory in the cybersecurity landscape. In this context, this research contributes nuanced and relevant approaches to the field. The results seen by the utilization of systems such as Rule 30 Cellular Automaton, the Lorenz Attractor, and the Logistic Map not only introduces an additional level of complexity and unpredictability but also offers significant potential for deployment in cryptographic techniques and methods.
While the Chaotic Operation Mode and Rule 30 Cellular Automaton have augmented the complexity and security of the algorithm, the results of the statistical tests employed underscore that the selection of the appropriate chaotic system is a decisive factor for the algorithm's quality. In this regard, the k-Lorenz Attractor stands out, serving as the system that truly fulfills the proposed objectives, ensuring that its implementation for such purposes aligns with the current digital world.
Therefore, the integration of this chaotic system has not only achieved the stated objectives of studying and constructing a robust and reliable cryptographic system, but also presents intriguing results for the furtherance of scientific development in this field. The proposed algorithm represents a possibility to further enhance data integrity and confidentiality in today's word.

However, the continuous evolution of technology and the emergence of new threats necessitate that all cryptographic methodologies be constanly reviewed and adapted to ensure their practical applicability. While the preliminary results described here are promising, particularly in terms of security and unpredictability, there is room for additional research to fully assess the feasibility of this implementation in practical scenarios.

Acknowledgements

I would like to express my gratitude to Professor Dr. Odemir M. Bruno for the invaluable academic experience provided, encompassing diverse topics in conversations and in-depth studies that greatly enriched my knowledge. I would also like to extend my thanks to the Scientific Computing Group and its entire infrastructure provided by USP, without which the completion of this work would have been impossible. Last but not least, I want to express my appreciation to my research partner, Kauê H. Bazilli, whose wit and unwavering commitment were always present during the critical phases of this project's development.

References

1. BAPTISTA, M. S. Cryptography with chaos. **Physics Letters A**, v. 240, n. 1-2, p. 50-54, mar. 1998. Available at: https://doi.org/10.1016/s0375-9601(98)00086-3.
2. WOLFRAM, Stephen. **New Kind of Science**. [S. l.]: Wolfram Media, 2002. ISBN 1579550088. Available at: https://www.wolframscience.com.

3. MARCO, Anderson Gonçalves; MARTINEZ, Alexandre Souto; BRUNO, Odemir Martinez. Fast, parallel, and secure cryptography algorithm using lorenz's attractor. **International Journal of Modern Physics C**, v. 21, n. 03, p. 365-382, mar. 2010. Available at: https://doi.org/10.1142/s0129183110015166.
4. JUSTO, M. J. M. **Autômatos celulares caóticos aplicados na Criptografia e Criptoanálise**. 2013. Dissertation (Master's) – University of São Paulo, São Carlos, 2013. Available at: http://www.teses.usp.br/teses/disponiveis/76/76132/tde-20092013-153518/.
5. MACHICAO, Jeaneth; BRUNO, Odemir M. Improving the pseudo-randomness properties of chaotic maps using deep-zoom. **Chaos: An Interdisciplinary Journal of Nonlinear Science**, v. 27, n. 5, p. 053116, maio 2017. Available at: https://doi.org/10.1063/1.4983836.
6. MACHICAO, Jeaneth et al. Exploiting ergodicity of the logistic map using deep-zoom to improve security of chaos-based cryptosystems. **International Journal of Modern Physics C**, v. 30, n. 05, p. 1950033, maio 2019. Available at: https://doi.org/10.1142/s0129183119500335.
7. MACHICAO, Jeaneth; BRUNO, Odemir M.; BAPTISTA, Murilo S. Zooming into chaos as a pathway for the creation of a fast, light and reliable cryptosystem. **Nonlinear Dynamics**, v. 104, n. 1, p. 753-764, 22 fev. 2021. Available at: https://doi.org/10.1007/s11071-021-06280-y.