EXPLORANDO A APLICAÇÃO DA GEOMETRIA FRACTAL NA CRIPTOGRAFIA: UMA ABORDAGEM PARA MELHORAR A RESILIÊNCIA EM ALGORITMOS CRIPTOGRÁFICOS

Felipe Jordão Silva[1]

[1]*Universidade Estadual de Maringá, Maringá, Brasil*
(ra140592@uem.br)

Resumo: Com o uso crescente das comunicações digitais e em paralelo o aumento das ameaças cibernéticas, a necessidade de algoritmos criptográficos seguros e resilientes a ataques se faz cada vez mais necessário. Os modelos atuais de algoritmos criptográficos utilizam fatoração e aritmética modular para garantir uma maior segurança, entretanto, esses algoritmos possuem certas limitações como vulnerabilidades a computadores quânticos. O presente artigo tem como objetivo a investigação da aplicação da geometria fractal como abordagem para aprimorar a resiliência em algoritmos de criptografia. Para avaliar a efetividade dessa abordagem, simulações computacionais são realizadas, os resultados demonstram que a utilização da geometria fractal na construção de algoritmos criptográficos pode ser um modelo alternativo promissor na busca pela modernização da segurança de sistemas criptográficos.

Palavras-chave: Criptografia baseada em fractais, Segurança da informação, Algoritmos, Computação quântica.

INTRODUÇÃO

A segurança da informação é um área em constante evolução, a criptografia desempenha um papel fundamental na proteção de informações sensíveis e confidenciais. A medida que os métodos tradicionais enfrentam desafios crescentes, a busca por novas abordagens para melhorar a segurança e aumentar a resiliência contra ataques mais sofisticados tem aumentado.

A geometria fractal vem com o objetivo de introduzir uma nova dimensão as abordagens criptográficas utilizadas, através dessa mescla entre a geometria fractal e a criptografia, é possível oferece oportunidades para o fortalecimento da segurança dos padrões criptográficos tradicionais, ao incorporar os princípios fractais, busca-se melhorar a complexidade e imprevisibilidade dos algoritmos criptográficos.

As propriedades singulares dos fractais, como autossimilaridade e escalabilidade, podem ser exploradas para criar sistemas criptográficos mais resistentes a ataques.

A integração de fractais em algoritmos de criptografia tem mostrado resultados promissores em termos de aumento da segurança e resiliência contra ataques cibernéticos (WANG et al., 2022)

FUNDAMENTAÇÃO TEÓRICA

GEOMETRIA FRACTAL

O termo fractal foi criado no ano de 1975 pelo matemático francês Benoit Mandelbrot, Fractais são formas complexas e irregulares que apresentam auto-similaridade em diferentes escalas, são gerados por funções interativas, possuem como característica a dimensionalidade não inteira, o que os tornam diferentes da geometria euclidiana tradicional.

Mandelbrot (1982), descreve fractais geométricos como "uma forma geométrica áspera ou fragmentada que pode ser dividida em partes, cada uma das quais é (pelo menos aproximadamente) uma cópia em tamanho reduzido do todo".

GERAÇÃO DE CHAVES CRIPTOGRÁFICAS

Os fractais com seus padrões imprevisíveis, apresentam um caminho interessante para melhorar a geração de chaves em sistemas criptográficos. Ao aproveitar a autossemelhança e a natureza caótica dos fractais, as chaves criptográficas podem ser geradas com entropia aprimorada, tornando-as mais resistentes a ataques de força bruta.

Estudos demonstram que técnicas de criptografia baseadas em fractais podem melhorar a robustez de algoritmos criptográficos (ASLAM et al., 2022).

A utilização de algoritmos de geração de chaves baseados em fractais introduz um elemento dinâmico e adaptativo aos sistemas criptográficos, aumentando sua robustez contra ameaças em evolução.

Além disso, os fractais tem sido utilizados para gerar keystreams one-time pad, que são essenciais para comunicação segura (MIKHAIl et.,2017)

MATERIAL E MÉTODOS

Para a ilustração da aplicação prática dos fractais, incorporamos uma metodologia de simulação através de um algoritmo feito na Linguagem R.

O algoritmo implementa um ambiente de simulação com parâmetros específicos para ilustrar a aplicação da geometria fractal na criptografia.

Utilizamos o conjunto de mandelbrot para gerar padrões fractais e incorporamos esses padrões na geração de chaves e cifragem de dados.

O ambiente também inclui a simulação de um ataque de força bruta sobre a chave gerada para avaliar a resistência para diferentes tamanhos de chaves.

GERAÇÃO DO PADRÃO FRACTAL

A função mandelbrot implementa um algoritmo para gerar um padrão fractal do conjunto de Mandelbrot. A função retorna uma matriz que representa o padrão fractal.

```
mandelbrot
<−
 function(width, height, max_iter) {     x_min
<− −2 x_max <− 2 y_min
<− −2 y_max <− 2 x
<− linspace(x_min, x_max, width) y
<− linspace(y_min, y_max, height) c
<− outer(x, y, FUN
= function(x, y) complex(real
= x, imaginary = y)) fractal
<− matrix(0L, nrow = height, ncol
= width) for (i in 1:max_iter) {  c
<− ifelse(abs(c)
< 1000, c^2 + outer(x, y, FUN
= function(x, y) complex(real
= x, imaginary
= y)), c) # Evita overflow mask
<− abs(c) < 1000 mask_matrix
<− matrix(mask, nrow
= height, ncol = width) l
<− fractal
+ mask_matrix } return(fractal)}}
```

GERAÇÃO DA CHAVE FRACTAL

A função gerar_chave_fractal utiliza um padrão fractal para gerar uma chave. Ela recebe o tamanho na chave desejada, número máximo de interações. A função retorna um vetor que representa a chave fractal.

```
gerar_chave_fractal
− function(tamanho_chave, max_iter, seed
NULL) { if (!is.null(seed)) { set.seed(seed) }
turn(as.integer(reshape2::melt(mandelbrot(tamanho_chave, 1, max_i
lue))}
```

CIFRAGEM DE DADOS

A cifragem é realizada por meio de uma conversão de string de entrada em uma representação binária e, em seguida, é executada uma operação XOR bit a bit com a chave fractal fornecida. A chave é repetida e ajustada para coincidir com o comprimento dos binários. A Função HMAC é utilizada para validar a integridade dos dados.

```
cifrar_e_plotar
<− function(dados, chave, title) { dados
<−
as.character(dados) # Converter dados em vetor de caracteres
<−
bitwXor(utf8ToInt(charToRaw(dados)), rep(chave, length.out
= (nchar(dados) + length(chave) − 1) %
/% length (chave))[1:nchar(dados)]) hmac
<− hmac(dados_cifrados, key
= chave) plotar_cifragem(dados_cifrados, title) cat("HMAC:",
\n")}
```

ATAQUE DE FORÇA BRUTA

A simulação de um ataque de força bruta é realizada tentando todas as combinações possíveis de uma chave fractal de um determinado tamanho e verificar se os dados decifrados correspondem aos dados originais.

Após a integração das etapas anteriores, os resultados são gerados através de gráficos com informações destacando métricas importantes para melhor visualização.

RESULTADOS E DISCUSSÃO

Os resultados preliminares indicam que a abordagem fractal na criptografia apresenta características promissoras de segurança.

A resistência ao ataque de força bruta é evidente, sendo mais eficaz em relação a chaves maiores, demonstrando a eficacia dessa abordagem.

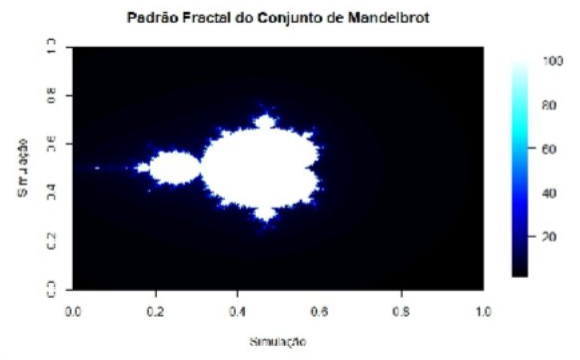

***Figura 1** - Padrão fractal de Mandelbro gerado. Fonte: https://rpubs.com/felpa/1155350*

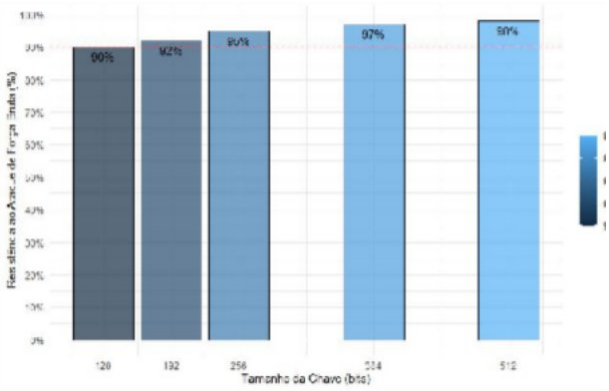

***Figura 2** - Resultado da simulação do ataque de força bruta demonstrando a resistência da chave com fractais. Fonte: https://rpubs.com/felpa/1153883*

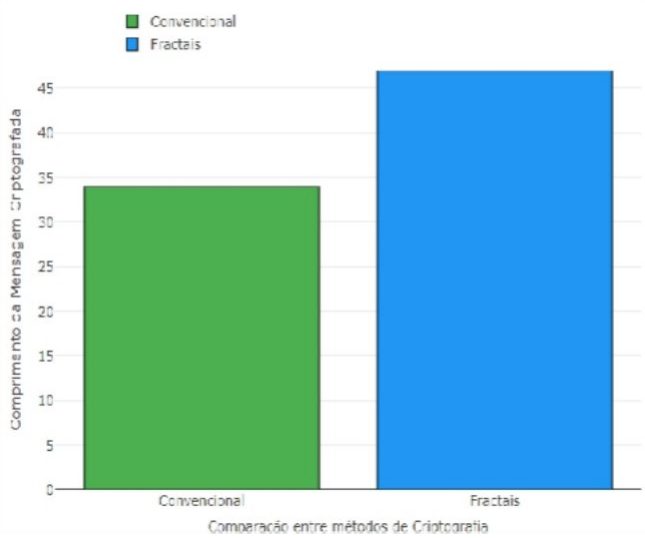

Figura 3 - Comparação entre métodos de cifragem criptográficos - Fonte: https://rpubs.com/felpa/1166479

CONCLUSÃO

Os resultados indicam que a utilização da geometria fractal em algoritmos de criptografia incorporam uma camada adicional de complexidade, embora essa integração ofereça inúmeros benefícios, também há desafios a serem abordados.

Como por exemplo garantir a escalabilidade e a eficiência das técnicas de criptografia baseadas em fractais, sobretudo em sistemas de grande escala.

Futuras pesquisas podem se concentrar na otimização de parâmetros fractais para criptografia, em especial em sistemas com uma grande proporção.

REFERÊNCIAS

Aslam, M. K., Beg, S., Anjum, A., Qadir, Z., Khan, S., Malik, S. U. R., … & Mahmud, M. P. 2022. A strong construction of s-box using mandelbrot set an image encryption scheme. PeerJ Computer Science, 8, e 892. https://doi.org/10.7717/peerj-cs.892 Acesso em 18.03.2024.

Mikhail, M., Abouelseoud, Y., & Elkobrosy, G. 2017. Two-phase image encryption scheme based on ffct and fractals. Security and Communication Networks, 2017, 1-13. https://doi.org/10.1155/2017/7367518 Acesso em 18.03.2024

Wang, J., Zhang, M., Tong, X., & Wang, Z. 2022. A chaos-based image compression and encryption

scheme using fractal coding and adaptive-thresholding sparsification. Physica Scripta, 97(10), https://doi.org/10.1088/1402-4896/ac8b41 Acesso em 18.03.2024.

J. W. Cannon (1984) *The Fractal Geometry of Nature*. By Benoit B. Mandelbrot, The American Mathematical Monthly, 91:9, 594-598, Disponivel em: https://www.tandfonline.com/doi/abs/10.1080/00029890.1984.11971507 Acesso em 07.01.2024.

Douglas R. Stinson and maura B Paterson . 1995. Cryptography: Theory and Practice Fourth Edition. CRC Press. Disponível em: https://www.ic.unicamp.br/~rdahab/cursos/mo421-mc889/Welcome_files/Stinson-Paterson_CryptographyTheoryAndPractice-CRC%20Press%20%282019%29.pdf Acesso em 08.01.2024.

1. Peitgen H-O Saupe D Barnsley MF. *The Science of Fractal Images*. Springer-Verlag; 1988. Disponivel em: https://search.worldcat.org/title/science-of-fractal-images/oclc/17919317 Acesso em 07/01/2024.

W. Diffie and M. Hellman, "New directions in cryptography," in IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, November 1976, doi: 10.1109/TIT.1976.1055638. Disponível em: https://ieeexplore.ieee.org/document/1055638 Acesso em 08.01.2024

Barnsley, M. F, Fractals Everywhere. Second Edition 1993. Disponível em: https://www.sciencedirect.com/book/9780120790616/fractals-everywhere Acesso em 09.01.2024

Falconer, K. J. Fractal geometry: mathematical foundations and applications. 1990. Disponível em: https://www.dm.uba.ar/materias/optativas/geometria_fractal/2006/1/Fractales/1.pdf Acesso em 10.01.2024