Criptografia Baseada em Fractais: Uma Abordagem Interdisciplinar entre Matemática, Computação e Educação Tecnológica

João Ricardo Siqueira de Oliveira[1], Sandra Mara Alves Jorge[3], Filipe Lorenzato Cardoso Rodrigues[3], Marcos Vinícius Nunes Reis[4], Mateus Fasciani Viggiani Rios de Castro[5], Lucas Vinicius Pedroso Pereira[6]

[1]PUC Minas, Belo Horizonte, Brasil (joaoricardopuc@gmail.com)
[2]CEFET-MG, Belo Horizonte, Brasil (sandramaracefet@gmail.com)
[3]PUC Minas, Belo Horizonte, Brasil (4º período do curso de Ciência da Computação)
[4]PUC Minas, Belo Horizonte, Brasil (4º período do curso de Ciência da Computação)
[5]PUC Minas, Belo Horizonte, Brasil (5º período do curso de Ciência da Computação)
[6]PUC Minas, Belo Horizonte, Brasil (4º período do curso de Jogos Digitais)

Resumo: Este trabalho investiga a aplicação de fractais e sistemas dinâmicos na criptografia visual e textual, articulando Matemática, Computação e Educação Tecnológica. Utilizando Python como ambiente experimental, o projeto desenvolve modelos baseados em caos e auto-similaridade para segurança digital. A proposta também enfatiza metodologias ativas e formação científica interdisciplinar por meio da iniciação científica e do desenvolvimento colaborativo de algoritmos.

Palavras-chave: Criptografia Caótica; Geometria Fractal; Sistemas Dinâmicos; Educação Tecnológica.

INTRODUÇÃO

A crescente complexidade dos sistemas digitais e o avanço das tecnologias de processamento de dados têm ampliado os desafios relacionados à segurança da informação. Nesse contexto, pesquisas envolvendo sistemas dinâmicos e geometria fractal vêm sendo investigadas como alternativas para modelagem de algoritmos criptográficos não lineares.

Este trabalho apresenta uma proposta interdisciplinar desenvolvida no âmbito de um projeto de iniciação científica entre os Departamentos de Matemática e Ciência da Computação. A pesquisa busca integrar conceitos de geometria fractal, sistemas caóticos e programação computacional para explorar aplicações em criptografia visual e textual.

A proposta também possui caráter educacional, uma vez que utiliza metodologias ativas e aprendizagem baseada em projetos para aproximar estudantes de graduação de problemas reais envolvendo modelagem matemática, segurança digital e desenvolvimento computacional.

Nesta etapa inicial da pesquisa, os estudantes realizaram a implementação computacional do Conjunto de Cantor e do Triângulo de Sierpinski utilizando Python. Os códigos produzidos encontram-se disponíveis em repositório público no GitHub, permitindo reprodutibilidade e colaboração acadêmica.

O estudo não pretende apresentar um sistema criptográfico definitivo ou substituir algoritmos consolidados, mas investigar o potencial de sistemas dinâmicos e estruturas fractais na geração de padrões complexos aplicáveis à segurança digital.

FUNDAMENTAÇÃO TEÓRICA

Criptografia Moderna

A criptografia constitui uma das áreas centrais da segurança computacional contemporânea. Sua principal função consiste em proteger informações contra acessos não autorizados por meio de técnicas de codificação capazes de transformar dados legíveis em representações cifradas.

Historicamente, os primeiros métodos criptográficos surgiram ainda na Antiguidade, destacando-se a Cifra de César como um dos exemplos clássicos de substituição monoalfabética. Ao longo do tempo, a evolução tecnológica exigiu o desenvolvimento de mecanismos cada vez mais sofisticados.

Durante a Segunda Guerra Mundial, a máquina Enigma tornou-se um marco histórico da criptografia mecânica, demonstrando a importância estratégica da proteção de informações em contextos militares.

Em 1949, Claude Shannon estabeleceu fundamentos matemáticos importantes para a criptografia moderna ao introduzir os princípios de confusão e difusão em seu trabalho “Communication Theory of Secrecy Systems”. Segundo Shannon, um sistema criptográfico eficiente deve:

- dificultar a relação direta entre chave e mensagem;

- dispersar estatisticamente os padrões da informação original;
- reduzir previsibilidade computacional.

Atualmente, algoritmos como RSA, AES e ECC são amplamente utilizados em sistemas de comunicação digital, autenticação em redes e proteção de dados sensíveis.
Entretanto, o avanço da computação quântica vem motivando pesquisas relacionadas à chamada criptografia pós-quântica, área que busca desenvolver modelos resistentes ao aumento da capacidade computacional futura.
Nesse cenário, sistemas dinâmicos não lineares passaram a ser investigados como possíveis ferramentas auxiliares na geração de sequências pseudoaleatórias e estruturas criptográficas experimentais.

Sistemas Dinâmicos e Caos Determinístico
Os sistemas dinâmicos constituem modelos matemáticos utilizados para descrever a evolução temporal de fenômenos físicos, computacionais e naturais.
Em muitos casos, pequenas alterações nas condições iniciais podem produzir comportamentos significativamente distintos ao longo do tempo. Essa característica é conhecida como sensibilidade às condições iniciais e representa um dos elementos centrais da teoria do caos.
O matemático e meteorologista Edward Lorenz demonstrou esse comportamento ao investigar modelos computacionais relacionados à previsão climática, formulando o chamado "efeito borboleta", conceito que descreve como pequenas variações podem provocar grandes alterações em sistemas complexos.
Os sistemas caóticos apresentam comportamento determinístico, ou seja, seguem regras matemáticas definidas, mas produzem trajetórias difíceis de prever devido à elevada sensibilidade dos parâmetros envolvidos.
Uma das representações matemáticas mais conhecidas desse comportamento é o mapa logístico:

$$x_{n+1} = r x_n (1 - x_n)$$

Nesse modelo:

- x_n representa o estado atual do sistema;
- r corresponde ao parâmetro de controle;
- x_{n+1} representa o próximo estado.

Dependendo do valor de r, o sistema pode apresentar:

- convergência estável;
- comportamento periódico;
- bifurcações;
- caos determinístico.

Em regiões caóticas, pequenas alterações nos valores iniciais produzem trajetórias completamente distintas após algumas iterações.
Essa propriedade desperta interesse em pesquisas sobre criptografia caótica, pois possibilita a geração de sequências complexas e pseudoaleatórias.
Além disso, sistemas dinâmicos possuem aplicações em diversas áreas científicas, incluindo:

- meteorologia;
- biologia;
- física;
- engenharia;
- computação.

Geometria Fractal
A geometria fractal foi formalizada pelo matemático Benoit Mandelbrot durante a década de 1970, propondo uma nova forma de representação matemática para estruturas irregulares presentes na natureza.
Diferentemente da geometria euclidiana clássica, os fractais descrevem objetos caracterizados por:

- auto-similaridade;
- recursividade;
- complexidade geométrica;
- irregularidade em múltiplas escalas.

A auto-similaridade consiste na repetição parcial da estrutura em diferentes níveis de ampliação.
Entre os exemplos matemáticos mais conhecidos destacam-se:

- Conjunto de Cantor;
- Triângulo de Sierpinski;
- Curva de Koch;
- Conjunto de Mandelbrot.

O Conjunto de Cantor é construído a partir de um processo recursivo de remoção sucessiva do terço central de segmentos lineares.
Sua representação pode ser descrita como:

$$C = \bigcap_{n=1}^{\infty} C_n$$

Essa estrutura apresenta propriedades relevantes para estudos computacionais relacionados à descontinuidade, fragmentação e geração de padrões complexos.
Outro elemento importante da geometria fractal é a dimensão fractal, conceito utilizado para descrever objetos cuja dimensionalidade não pode ser representada adequadamente pelos modelos inteiros da geometria clássica.
A dimensão de Hausdorff, frequentemente associada aos fractais, permite quantificar matematicamente níveis de irregularidade e complexidade geométrica.
Atualmente, estruturas fractais possuem aplicações em:

- computação gráfica;
- processamento de imagens;
- modelagem de antenas;
- compressão de dados;

- análise de sinais;
- sistemas biológicos.

A elevada complexidade geométrica dessas estruturas torna os fractais relevantes para pesquisas relacionadas à geração de padrões computacionais complexos e máscaras criptográficas experimentais.

Essas propriedades motivam investigações sobre a integração entre geometria fractal e sistemas criptográficos baseados em caos determinístico.

Criptografia Caótica

A criptografia caótica corresponde a uma área de pesquisa que investiga aplicações de sistemas dinâmicos não lineares na proteção de informações digitais.

Diferentemente dos métodos criptográficos tradicionais, os modelos caóticos utilizam propriedades matemáticas associadas à imprevisibilidade e à sensibilidade às condições iniciais.

Entre as principais características investigadas em criptografia caótica destacam-se:

- elevada variabilidade das sequências geradas;
- comportamento não linear;
- dependência crítica das sementes iniciais;
- geração pseudoaleatória;
- dispersão estatística.

Pesquisas recentes têm explorado aplicações desses sistemas em:

- criptografia de imagens;
- mascaramento visual;
- transmissão segura de sinais;
- geração de chaves dinâmicas;
- codificação híbrida.

Uma das propriedades mais relevantes para aplicações criptográficas é a dificuldade de reconstrução das trajetórias caóticas sem conhecimento preciso dos parâmetros iniciais do sistema.

Entretanto, estudos sobre criptografia caótica ainda enfrentam desafios importantes relacionados a:

- sincronização entre emissor e receptor;
- precisão computacional;
- estabilidade numérica;
- validação estatística;
- resistência criptoanalítica.

Por esse motivo, muitos trabalhos da área ainda possuem caráter experimental e exploratório. Nesse contexto, estruturas fractais passaram a ser investigadas como mecanismos auxiliares para geração de padrões complexos, difusão espacial e mascaramento criptográfico.

Integração entre Fractais e Criptografia

A integração entre geometria fractal e criptografia emerge como uma abordagem promissora para construção de modelos computacionais capazes de combinar complexidade geométrica, geração de padrões difíceis de prever e elevada sensibilidade a pequenas alterações nos parâmetros iniciais.

A relação entre geometria fractal e criptografia ocorre principalmente pela capacidade dos fractais de gerar estruturas altamente complexas, recursivas e sensíveis a pequenas alterações paramétricas. Essas propriedades tornam os fractais candidatos interessantes para aplicações em segurança digital, especialmente na geração de máscaras criptográficas, sequências pseudoaleatórias e codificação visual.

Enquanto sistemas caóticos fornecem comportamentos difíceis de prever ao longo das iterações, os fractais acrescentam complexidade geométrica e repetição estrutural em diferentes escalas. Em conjunto, essas propriedades podem aumentar a dispersão estatística das informações codificadas.

Em aplicações criptográficas experimentais, estruturas fractais podem atuar como:

- geradores de padrões pseudoaleatórios;
- matrizes de permutação;
- máscaras de embaralhamento;
- mecanismos de difusão espacial;
- codificação visual de imagens.

Uma possibilidade consiste na utilização de mapas caóticos para geração de parâmetros iniciais responsáveis pela construção de fractais computacionais. Pequenas alterações nesses parâmetros produzem estruturas significativamente diferentes, dificultando processos de reconstrução sem conhecimento da chave correta.

No presente projeto, investigou-se a utilização de sequências derivadas do mapa logístico associadas a padrões geométricos fractais para realização de operações XOR sobre mensagens digitais.

O processo experimental pode ser descrito nas seguintes etapas:

1. Preparação da Mensagem (Conversão)

O processo inicia-se com a conversão da mensagem em formato numérico. Cada caractere do texto original é mapeado para o seu valor correspondente na tabela ASCII.

- Exemplo*:* O caractere 'c' torna-se 99.

2. Geração da Chave (Base Fractal)

Em vez de usar uma chave estática comum, utiliza-se um parâmetro complexo para definir a estrutura de um Conjunto de Julia, por exemplo,

$$P(k) = -0.1458 + 0.1968i$$

Este parâmetro funciona como a "semente" ou chave privada. Sem este valor exato, a estrutura fractal (e consequentemente a sequência numérica) não pode ser reproduzida.

A chave P(k) atua como uma "regra de comportamento" para o sistema dinâmico. O sistema segue essa regra para "caminhar" pelo plano fractal; Para o caractere “c” geramos o número 152 que é, essencialmente, uma medida (ou coordenada) colhida desse caminho caótico em um momento específico da iteração.

3. Geração da Sequência Computacional

A partir da chave definida, um sistema dinâmico (neste caso, baseado na geometria fractal) gera uma sequência numérica pseudoaleatória. O tamanho desta sequência deve corresponder exatamente ao número de caracteres da mensagem original. Cada valor gerado servirá como um componente para mascarar um caractere específico da mensagem.

4. Aplicação da Cifra (Operação XOR)

Esta é a fase de cifragem propriamente dita, onde ocorre o embaralhamento:

- A operação XOR é aplicada entre cada valor ASCII da mensagem original e o valor correspondente da sequência gerada pela chave fractal.

Exemplo:

A representação binária da operação:
ASCII do caractere ('c'): 99
Valor da sequência gerada: 152
Convertendo os números decimais para a base binária (8 bits):
$99 = (01100011)_2$
$152 = (10011000)_2$
Agora, aplicamos a operação XOR bit a bit:

Bit	Valor (99)	Chave (152)	Resultado (XOR)
b7	0	1	**1**
b6	1	0	**1**
b5	1	0	**1**
b4	0	1	**1**
b3	0	1	**1**
b2	0	0	**0**
b1	1	0	**1**
b0	1	0	**1**

O resultado binário é $(11111011)_2 = 251$ na base decimal, ou seja,

$$99 \oplus 152 = 251.$$

- O resultado é uma nova sequência numérica que não possui relação visual ou lógica imediata com o texto original.

5. Recuperação da Mensagem (Decifragem)

O processo de descriptografia é a operação inversa, que exige a posse da mesma "chave" (parâmetro fractal):

- Reconstrução: O receptor insere o mesmo parâmetro P(k) no algoritmo, que gera a mesma sequência numérica utilizada na cifragem.
- Decodificação: Aplica-se novamente a operação XOR entre os valores cifrados e a sequência gerada pela chave.

O XOR é fundamental em criptografia devido a uma propriedade matemática essencial: ele é sua própria inversa. Portanto, o valor 251, ao ser submetido ao XOR novamente com o valor 152 da sequência gerada, retorna obrigatoriamente ao valor original 99. Essa simplicidade computacional, aliada à imprevisibilidade da sequência gerada pelo fractal, cria uma barreira de segurança eficiente contra ataques estatísticos.

6. Modelo Experimental de Cifragem

Para demonstrar experimentalmente a aplicação de estruturas fractais em criptografia textual, foi desenvolvido um processo computacional baseado em:

- conversão ASCII;
- geração de parâmetros fractais;
- produção de sequências pseudoaleatórias;
- aplicação da operação XOR.

O modelo utiliza parâmetros associados ao Conjunto de Julia para geração de sequências numéricas utilizadas na cifragem e recuperação das mensagens. O processo completo encontra-se ilustrado na Figura 5.

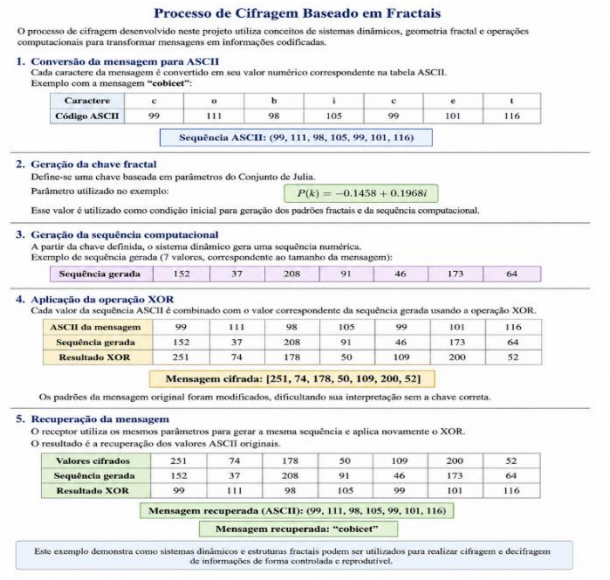

Figura 1 – Processo experimental de cifragem baseado em fractais.

Pesquisas Recentes e Aplicações
Nos últimos anos, diversos estudos têm investigado a utilização de fractais e sistemas dinâmicos em aplicações relacionadas à segurança digital.
Negi et al. (2025), por exemplo, propuseram um modelo de transmissão segura de dados baseado em estruturas fractais e processos iterativos.
Outras pesquisas recentes exploram:

- mapas caóticos híbridos;
- criptografia de imagens digitais;
- geração pseudoaleatória de alta entropia;
- sistemas de mascaramento fractal;
- integração entre caos e inteligência artificial.

Além das aplicações técnicas, projetos interdisciplinares envolvendo criptografia e programação também têm sido utilizados em contextos educacionais para estimular:

- pensamento computacional;
- resolução de problemas;
- modelagem matemática;
- aprendizagem baseada em projetos.

Nesse sentido, a integração entre Matemática, Computação e Educação Tecnológica possibilita a construção de ambientes de aprendizagem mais investigativos e conectados a desafios contemporâneos.

IMPLEMENTAÇÃO E METODOLOGIA

A pesquisa caracteriza-se como qualitativa, exploratória e interdisciplinar, articulando conceitos de Matemática, Computação e Educação Tecnológica.
A implementação computacional foi desenvolvida utilizando a linguagem Python devido à sua flexibilidade para modelagem matemática e visualização gráfica.
A metodologia do projeto foi estruturada em quatro etapas principais:

1. Modelagem Matemática
Inicialmente, os estudantes investigaram propriedades matemáticas relacionadas à geometria fractal e aos sistemas dinâmicos.
Foram analisados:

- auto-similaridade;
- recursividade;
- sensibilidade às condições iniciais;
- comportamento caótico.

2. Implementação Computacional
Os estudantes implementaram algoritmos para geração do:

- Conjunto de Cantor;
- Triângulo de Sierpinski;
- sequências baseadas em mapas caóticos.

As implementações foram desenvolvidas em ambiente Python utilizando bibliotecas matemáticas e gráficas.

3. Simulação de Codificação
A pesquisa realizou testes preliminares utilizando operações XOR associadas a sequências geradas por sistemas dinâmicos.
Nessa etapa, foram analisados:

- sincronismo entre emissor e receptor;
- sensibilidade das sementes iniciais;
- comportamento computacional das máscaras geradas.

4. Formação Científica Interdisciplinar
Além do desenvolvimento técnico, o projeto também buscou estimular:

- pensamento computacional;
- investigação científica;
- resolução de problemas;
- aprendizagem colaborativa.

Os estudantes participaram de:

- seminários;
- implementação de algoritmos;
- estudos matemáticos;
- documentação computacional.

Todo o material produzido foi disponibilizado em repositório público no GitHub.

ANÁLISE COMPUTACIONAL E DESAFIOS

Sensibilidade às Condições Iniciais
Os sistemas caóticos apresentam forte dependência dos valores iniciais utilizados na geração das sequências.
Durante os testes computacionais, pequenas alterações nas sementes produziram padrões significativamente distintos, dificultando previsibilidade linear das sequências geradas.
Essa propriedade é frequentemente investigada em estudos sobre criptografia caótica.

Sincronismo entre Emissor e Receptor
Nos testes realizados, observou-se que o sincronismo entre os estados do sistema dinâmico é fundamental para recuperação correta da informação.
A perda de alinhamento entre emissor e receptor impossibilita a reconstrução adequada da mensagem codificada.

Limitações Computacionais
O estudo também identificou desafios importantes:

- erros de arredondamento;
- precisão de ponto flutuante;
- divergência entre arquiteturas computacionais;
- propagação de erros em sistemas iterativos.

Esses fatores demonstram que modelos baseados em caos exigem elevada precisão computacional.

Potenciais Propriedades de Segurança
Os experimentos preliminares indicam algumas propriedades relevantes:

1. elevada variabilidade das sequências geradas;
2. comportamento não linear;
3. sensibilidade às sementes iniciais;
4. dispersão estatística dos padrões produzidos.

Entretanto, este trabalho não pretende afirmar segurança criptográfica definitiva, uma vez que ainda são necessários:

- testes estatísticos avançados;
- análise de entropia;
- comparação com algoritmos consolidados;
- validação computacional em larga escala.

APLICAÇÕES EDUCACIONAIS

O projeto também possui importante dimensão pedagógica ao integrar pesquisa científica, programação e modelagem matemática.
A utilização de metodologias ativas permitiu que os estudantes participassem diretamente da construção dos algoritmos e da investigação dos modelos matemáticos.

Tabela 1: Matriz de Competências

Eixo	**Desenvolvimento**
Matemática	Modelagem fractal e sistemas dinâmicos
Computação	Implementação de algoritmos em Python
Segurança Digital	Estudos introdutórios sobre criptografia
Formação Científica	Pesquisa, documentação e análise crítica
Trabalho Colaborativo	Desenvolvimento interdisciplinar

A abordagem também favoreceu:

- protagonismo estudantil;
- aprendizagem investigativa;
- integração entre teoria e prática;
- desenvolvimento de pensamento computacional.

DESENVOLVIMENTO PRÁTICO

A etapa prática foi conduzida pelos estudantes do Curso de Ciências da Computação e Jogos Digitais da Pontifícia Universidade Católica de Minas Gerais (PUC Minas): Filipe Lorenzato Cardoso Rodrigues, Marcos Vinícius Nunes Reis, Mateus Fasciani Viggiani Rios de Castro e Lucas Vinicius Pedroso Pereira.

Conjunto de Cantor
Os estudantes implementaram o processo recursivo de geração do Conjunto de Cantor, removendo sucessivamente o terço central dos segmentos.

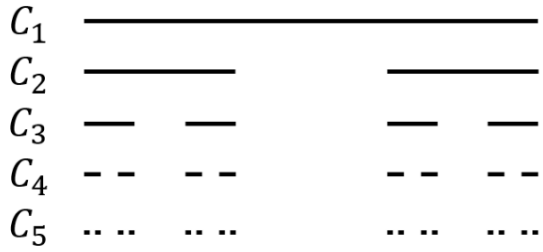

Figura 2: Iterações recursivas do Conjunto de Cantor

A estrutura foi utilizada como modelo experimental para investigação de padrões descontínuos e geração de sequências computacionais.



Figura 3: Apresentação do Processo de modelagem baseado em iterações do Conjunto de Cantor.

Triângulo de Sierpinski
Também foi realizada a construção computacional do Triângulo de Sierpinski.

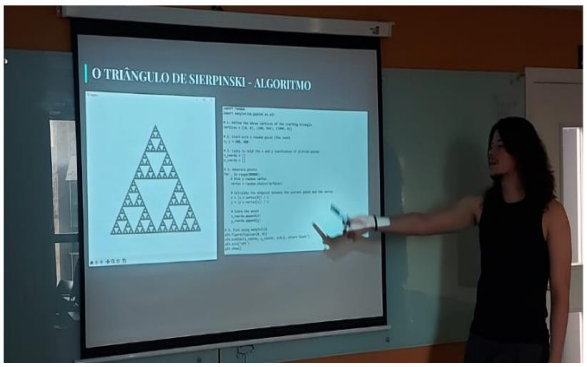

Figura 4 – Algoritmo gerador do Triângulo de Sierpinski

Conjunto de Julia

Uma das estruturas mais fascinantes da geometria fractal, intimamente relacionado ao famoso Conjunto de Mandelbrot. Eles representam um campo onde a matemática pura encontra a computação visual para descrever formas de complexidade infinita a partir de regras extremamente simples.

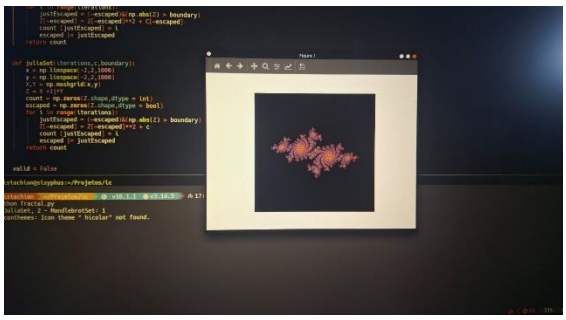

Figura 5 – Algortimo e fractal gerado – Conjunto de Julia

Criptografia

O processo de cifragem desenvolvido neste projeto fundamenta-se na intersecção entre sistemas dinâmicos, geometria fractal e operações lógicas computacionais para assegurar a confidencialidade da informação.

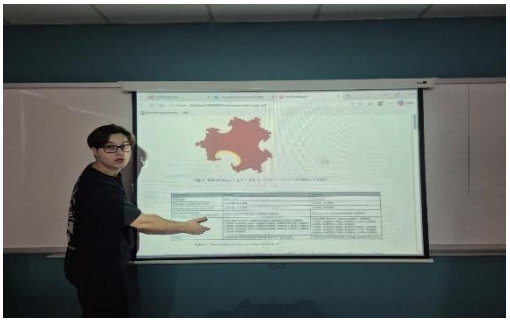

Figura 6 – Criptografando e descriptografando

Durante os seminários e implementações, os estudantes analisaram:

- auto-similaridade;
- recursividade;
- dimensão fractal;
- comportamento geométrico.

Esses estudos permitiram relacionar conceitos matemáticos abstratos com aplicações computacionais práticas.

Repositório Colaborativo

Como este trabalho caracteriza-se como uma iniciativa de iniciação científica de natureza continuada, o repositório do projeto no GitHub atua como um sistema de alimentação contínua de códigos.

A cada nova etapa de modelagem ou refinamento de algoritmo realizada pelos estudantes, o repositório é atualizado, garantindo que o progresso técnico da pesquisa seja um processo dinâmico, transparente e aberto à colaboração.

Repositório do projeto: https://github.com/marcosware/ic-fractais-computacao

CONCLUSÃO

A integração entre geometria fractal, sistemas dinâmicos e programação computacional demonstrou potencial para aplicações experimentais em criptografia visual e textual.

Embora o projeto ainda esteja em fase inicial de desenvolvimento, os resultados preliminares indicam que modelos baseados em caos e auto-similaridade podem contribuir para estudos futuros relacionados à segurança digital.

Além do aspecto técnico, a pesquisa evidenciou o potencial das metodologias ativas e da iniciação científica interdisciplinar na formação de estudantes das áreas de Matemática e Computação.

Como perspectivas futuras, pretende-se:

- implementar novos mapas caóticos;
- realizar testes estatísticos;
- investigar métricas de entropia;
- ampliar a análise computacional dos modelos;
- desenvolver aplicações experimentais para criptografia visual.

O estudo reforça a importância da integração entre Matemática, Computação e Educação Tecnológica na formação científica contemporânea.

AGRADECIMENTOS

Nossa gratidão aos Departamentos de Matemática e de Ciência da Computação do Instituto de Ciências Exatas e Informática (ICEI) da Pontifícia Universidade Católica de Minas Gerais (PUC Minas) e ao Departamento de Matemática do CEFET-MG. Este estudo é um reflexo do compromisso destas instituições com a excelência no ensino e na pesquisa.

REFERÊNCIAS

BACICH, Lilian; MORAN, José. **Metodologias Ativas para uma Educação Inovadora**. Porto Alegre: Penso, 2018.

MANDELBROT, Benoit. **The Fractal Geometry of Nature**. New York: W. H. Freeman, 1982.

NEGI, D. et al**. Secure data transmission through fractal-based cryptosystem: a Noor iteration approach**. 2025.

SHANNON, Claude E. Communication **Theory of Secrecy Systems. Bell System Technical Journal,** 1949.

STALLINGS, William. **Criptografia e Segurança de Redes**. 6. ed. São Paulo: Pearson, 2017.

DEANEY, Robert. **Chaos Theory and Dynamical Systems.** New York: Addison-Wesley, 1992.

PEITGEN, Heinz-Otto; JÜRGENS, Hartmut; SAUPE, Dietmar. **Chaos and Fractals: New Frontiers of Science.** New York: Springer, 2004.