UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Faculdade de Ciências e Tecnologia
Câmpus de Presidente Prudente

Sistema de Criptografia de Chave Pública Baseado em Sistemas de Funções Fractais (IFS)

Allan Hideick Tanaka

Orientadora: Prof.ª Dr.ª Tatiana Miguel Rodrigues

Programa: Matemática Aplicada e Computacional

Presidente Prudente, Julho de 2023

ALLAN HIDEICK TANAKA

Sistema de Criptografia de Chave Pública Baseado em Sistemas de Funções Fractais (IFS)

Dissertação apresentada ao Programa de Pós-Graduação em Matemática Aplicada e Computacional da Faculdade de Ciências e Tecnologia da UNESP para obtenção do título de Mestre em Matemática Aplicada e Computacional.

Área de Concentração: Matemática Aplicada e Computacional

Orientadora: Tatiana Miguel Rodrigues

Presidente Prudente, Julho de 2023

Tanaka, Allan Hideick
T161s Sistema de criptografia de chave pública baseado em Sistemas de Funções Fractais (IFS) / Allan Hideick Tanaka. -- Presidente Prudente, 2023
140 f.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Faculdade de Ciências e Tecnologia, Presidente Prudente
Orientadora: Tatiana Miguel Rodrigues

1. Matemática. 2. Criptografia. 3. Fractais. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Faculdade de Ciências e Tecnologia, Presidente Prudente. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

UNIVERSIDADE ESTADUAL PAULISTA

Câmpus de Presidente Prudente

CERTIFICADO DE APROVAÇÃO

TÍTULO DA DISSERTAÇÃO: Sistema de criptografia de chave pública baseado em Sistemas de Funções Fractais (IFS)

AUTOR: ALLAN HIDEICK TANAKA
ORIENTADORA: TATIANA MIGUEL RODRIGUES

Aprovado como parte das exigências para obtenção do Título de Mestre em Matemática Aplicada e Computacional, pela Comissão Examinadora:

Profa. Dra. TATIANA MIGUEL RODRIGUES (Participaçao Presencial)
Departamento de Matematica / Faculdade de Ciencias de Bauru

Prof. Dr. AGNALDO JOSE FERRARI (Participaçao Presencial)
Departamento de Matematica / Faculdade de Ciencias de Bauru

Prof. Dr. ROBSON RICARDO DE ARAUJO (Participaçao Presencial)
IFSP / Instituto Federal de Educação, Ciência e Tecnologia de São Paulo

Presidente Prudente, 14 de julho de 2023

Scanned with CamScanner

Dedico ao acaso da sorte que me fez chegar até aqui. A sorte pertence aos corajosos.

Agradecimentos

Agradeço à minha mãe, que me apoiou e deu suporte em todos os aspectos e momentos, me possibilitou estudar, sonhar e me fez crer que tudo é possível pelo esforço e dedicação.

Agradeço à minha esposa, que sempre me incentivou, auxiliou e me ouviu durante longas noites de conversas sobre o mesmo assunto. Foi paciente, carinhosa e esteve ao meu lado em todos os momentos, nunca desistindo nem por um segundo. Celebramos juntos cada vitória e compartilhamos cada derrota.

Aos meus sogros e cunhada, agradeço pelos conselhos e direcionamentos. Sem essas conversas, eu não teria concluído esse processo.

Expresso minha gratidão à minha orientadora, Prof.ª Dr.ª Tatiana Miguel Rodrigues, pela sua incrível visão de mundo, uma pessoa de personalidade extraordinária. Sempre esteve pronta e disposta, tanto durante a semana quanto nos finais de semana, fornecendo direcionamento, orientações e conselhos. Me ensinou muito, diretamente e indiretamente, de todas as maneiras possíveis, inclusive sobre como ser uma pessoa melhor. Levarei sua influência como referência pelo resto da minha vida.

Agradeço aos meus amigos, que caminharam ao meu lado desde a graduação. Estudamos juntos por dias a fio, trocamos ideias, tivemos diálogos e tiveram a paciência de ouvir cada detalhe do meu trabalho. Servimos uns aos outros como ombros em que pudemos nos apoiar, tornando tudo mais fácil e divertido.

À banca examinadora, Prof. Dr. Robson Ricardo de Araújo e Prof. Dr. Agnaldo José Ferrari pelas contribuições e sugestões.

À todos os professores do Departamento de Matemática da Unesp, pela sólida formação acadêmica.

À Univesp, pelo apoio financeiro.

Aprender como escapar. Escapar da voz alta, da linha que nunca desborda, do que se supõe centro. Aprender como sair: sair ao mundo, ao indeciso, deixar-se levar pelo movimento das coisas, acariciar as periferias. Aprender para nada. Aprender como inutilidade para enganar o tempo.

(SKLIAR, 2014)

Resumo

O presente trabalho compreende a uma aplicação da teoria fractal no grande campo da criptografia. Explorando conceitos preliminares para que fundamente o estudo em geral, prosseguindo teoricamente para a área da criptografia, trabalhando suas propriedades elementares e ramificações. Em seguida, é tratado de forma introdutória os principais resultados da Geometria Fractal, trilhando um caminho pelo conceito de *Espaço de Hausdorff*, *Distância de Hausdorff* e *Contrações no Espaço de Hausdorff*. Finalizando com a aplicação da Teoria Fractal em criptossistemas, propondo um método alternativo para a troca segura de chaves, baseado no *Protocolo Diffie-Hellman*.

Palavras-Chave: *Criptografia, Fractais, Sistema de Funções Iteradas, Criptossistemas*.

Abstract

The present work comprises an application of fractal theory in the broad field of cryptography. Exploring preliminary concepts to support the study in general, proceeding theoretically to the area of cryptography, working on its elementary properties and ramifications. Then, the main results of Fractal Geometry are treated in an introductory way, following a path through the concept of Hausdorff Space, Hausdorff Distance and Contractions in Hausdorff Space. Ending with the application of Fractal Theory in cryptosystems, proposing an alternative method for the secure exchange of keys, based on the Diffie-Hellman Protocol.

Keywords: *Cryptography, Fractals, Iterated Function Systems, Cryptosystems.*

Lista de Figuras

2.1 Um ponto x no espaço $\mathbb{R}$ 20
2.2 Uma função f em $X = C[0,1]$ 21
2.3 Representação dos pontos de uma sequência de Cauchy. 26
2.4 Representação Geométrica do Ponto Fixo 35
2.5 Conjunto convexo, estritamente convexo e não convexo 47

3.1 Diagrama de um criptossistema 63
3.2 Tabela ASCII 64
3.3 Cifra de fluxo 66
3.4 Cifra de bloco 66
3.5 Modelo de Criptografia Simétrica 67
3.6 Tabela de Vigenère 67
3.7 Modelo de Criptografia Assimétrica 73

4.1 O Conjunto de Cantor 86
4.2 O Triângulo de Sierpiński 86
4.3 Esponja de Menger 87
4.4 Distância entre ponto e conjunto 88
4.5 Distância entre conjuntos 89
4.6 Representação geométrica dos conjuntos A e B. 90
4.7 Contração f em um espaço métrico compacto. 101
4.8 Iteração da contração f convergindo para um ponto fixo $x_f \in X$. 101

5.1 Triângulo de Sierpiński 113
5.2 Curva do Dragão 113
5.3 Curva de Koch 113

5.4 Dragão de Levy 113
5.5 Samambaia de Barnsley 113
5.6 Árvore Fractal 113
5.7 Árvore Pitagórica 45º 123
5.8 Árvore Pitagórica 64º 124
5.9 Árvore Pitagórica 11º 127
5.10 Comparação de Performance - Java Net-Beans IDE 6.8 135
5.11 Comparação de Performance - Python 3.11 136

Lista de Tabelas

5.1 IFS para o Triângulo de Sierpiński 111
5.2 IFS para a Curva do Dragão 111
5.3 IFS para a Curva de Koch 111
5.4 IFS para o Dragão de Levy 111
5.5 IFS para a Samambaia de Barnsley 112
5.6 IFS para a Árvore Fractal 112
5.7 IFS para a Árvore Pitagórica 45º 123
5.8 IFS para a Árvore Pitagórica 64º 123

Conteúdo

Resumo **5**

Abstract **7**

Lista de Figuras **8**

Lista de Tabelas **10**

1 Introdução **15**

2 Conceitos preliminares **19**

2.1 Elementos de Espaços Métricos 19

2.1.1 Espaços Métricos Completos 25

2.1.2 Conjuntos compactos 29

2.1.3 Conjuntos conexos e desconexos 32

2.2 Elementos de Sistemas dinâmicos 33

2.2.1 Contrações no Espaço Euclidiano 36

2.2.2 Convexidade 45

2.3 Elementos de Teoria dos Números 51

2.3.1 Divisibilidade 52

2.3.2 Congruência 53

2.4 Elementos de Álgebra 57

2.4.1 Grupos 58

3 Criptografia **61**

3.1 Princípios básicos de criptografia 62

3.1.1 Processo de pré-codificação 63

3.2 Criptografia simétrica 65
3.2.1 Sigilo perfeito 68
3.3 Criptografia Assimétrica 71
3.3.1 O problema do logaritmo discreto 73
3.3.2 Protocolo de troca de chaves Diffie-Hellman 74
3.3.3 Criptografia RSA 76
3.4 Cenários de ataque e interceptação 82

4 Fractais **85**
4.1 Espaço de Hausdorff 87
4.1.1 A Completude do Espaço de Hausdorff 93
4.1.2 Transformações Contrativas 99
4.1.3 Contrações no Espaço de Hausdorff 102

5 Fractais e Criptografia **109**
5.1 Protocolo fractal de troca de chaves 109
5.1.1 A escolha do fractal 110
5.1.2 O protocolo proposto 114
5.2 Uma análise comparativa 129
5.2.1 De acordo com a quantidade de contrações do IFS 129
5.2.2 De acordo com a chave privada $s \in \mathbb{Z}$ 130
5.2.3 De acordo com as chaves privadas x e $y \in \mathbb{R}$ 133
5.2.4 Comparação de performance 135

Bibliografia **140**

Capítulo

1

Introdução

Um dos muitos encantos da matemática é a possibilidade de união entre dois mundos que, à primeira vista, parecem não estar relacionados, mas que funcionam juntos em completa harmonia. Partindo desse princípio, a motivação deste trabalho é a união da vasta área da Criptografia, que possui fundamentos ligados à Teoria dos Números, e da Teoria Fractal, que tem sua base na Geometria.

A Criptografia, proveniente do grego *kryptós*, que significa "escondido" ou "oculto", e *graphéin*, que significa "escrita", desempenha um papel fundamental desde os primórdios da humanidade, acompanhando o processo de evolução desde o início da escrita. Estudos indicam que o uso de mensagens codificadas remonta a 1900 a.C., quando um escriba egípcio utilizou hieróglifos fora da ordem padrão para representar sua inscrição, o que indica uma possível forma de codificação.

O uso militar da Criptografia foi amplamente explorado pelos espartanos há cerca de 2500 anos, que utilizavam um instrumento chamado *cítala*. O ditador romano *Júlio César* (100 a.C - 44 a.C) enviava mensagens codificadas pelo método da substituição para suas tropas durante as guerras, garantindo que, mesmo que o mensageiro fosse interceptado, o inimigo não seria capaz de compreender a mensagem original. Essa cifra ficou conhecida como a Cifra de César, que consistia na substituição das letras do alfabeto em uma ordem cíclica previamente combinada entre o imperador e as tropas.

O método de substituição foi amplamente utilizado como técnica criptográfica por um período de tempo. No século IX, os árabes desenvolveram um sistema de criptoanálise

simples que era capaz de quebrar facilmente a Criptografia de substituição. Esse sistema, conhecido hoje como *análise de frequência*, consistia na análise e identificação das letras mais frequentes no idioma em questão, substituindo-as pelas letras correspondentes na mensagem codificada.

Com a inutilização da Criptografia por substituição monoalfabética, a demanda por novos métodos aumentou exponencialmente. Nesse contexto, o diplomata francês *Blaise de Vigenère* (1523 - 1596), baseado nos trabalhos de *Leon Battista Alberti* (1404 - 1472), desenvolveu uma cifra polialfabética conhecida como a *cifra de Vigenère*, que utiliza 26 alfabetos diferentes para cifrar uma mensagem. Inicialmente, a cifra de Vigenère foi considerada indecifrável, mas foi quebrada pelo matemático inglês *Charles Babbage* (1791 - 1871) em 1854, utilizando um método semelhante à análise de frequência.

Durante muito tempo, o campo da Criptografia careceu de desenvolvimento. Em 1894, o rádio foi inventado pelo físico e inventor italiano *Guglielmo Marconi* (1874 - 1937), facilitando a comunicação entre os exércitos durante a Primeira Guerra Mundial, porém as mensagens eram facilmente interceptadas.

Em 1918, os alemães idealizaram uma máquina de cifragem amplamente utilizada pelo governo nazista durante a Segunda Guerra Mundial, chamada Enigma. A máquina consistia em um teclado para a inserção da mensagem original, um mecanismo que substituía as letras digitadas pelas letras cifradas e um indicador composto por lâmpadas que mostravam as letras da mensagem codificada. Além disso, a Enigma possuía rotores eletromecânicos para modificar periodicamente a chave de codificação.

O código da Enigma foi quebrado pelo matemático inglês *Alan Turing* (1912 - 1954), que utilizou uma generalização das contribuições dos poloneses para a quebra da Enigma e um sistema considerado precursor do computador. Os feitos de Turing lhe trouxeram grande reconhecimento como criptoanalista e matemático brilhante. Após esse período, muitos métodos criptográficos altamente eficazes foram desenvolvidos, entre eles, o conhecido e ainda utilizado RSA.

Mas o que a geometria da natureza, assim chamada pelo matemático polonês *Benoit Mandelbrot* (1924 - 2010), tem a oferecer para a arte de codificar mensagens? Em 1975, o termo *fractal*, do latim *fractus*, que significa "quebrado" ou "fragmentado", foi cunhado por Mandelbrot com o objetivo de identificar formas geométricas irregulares

e fragmentadas presentes no cotidiano. No entanto, diversos matemáticos famosos, como *Georg Ferdinand Ludwig Philipp Cantor* (1845 - 1918), *Giuseppe Peano* (1858 - 1932), *Niels Fabian Helge von Koch* (1870 - 1924) e *Wacław Sierpiński* (1882 - 1969), já trabalhavam com figuras que não se encaixavam na estrutura da Geometria Euclidiana conhecida. Essas figuras ficaram conhecidas como "monstros matemáticos".

De maneira informal, um objeto fractal é uma estrutura que apresenta fragmentação e irregularidades, que à primeira vista podem não fazer sentido, mas em uma escala ampla, revelam autossimilaridade. Ou seja, partes do fractal são réplicas do todo em diferentes escalas. Fractais podem ser observados em objetos da natureza, como as folhas das árvores, montanhas, raios, fumaças, nuvens e muitos outros. Dessa forma, a Geometria Fractal pode ser compreendida como uma extensão da Geometria Euclidiana comumente observada no dia a dia, caracterizada pela aleatoriedade, detalhes infinitos e autossimilaridade.

O estudo da Geometria Fractal permite uma mudança completa na forma como enxergamos a natureza em sua forma mais pura. A matemática envolvida nesse estudo proporciona interpretações fascinantes apenas observando a simples folha de uma samambaia. Portanto, as características singulares dos fractais e sua geometria complexa tornam-nos aliados valiosos como fundamentos matemáticos para garantir a segurança e a integridade de um criptossistema.

O trabalho foi motivado pela análise e de aspectos matemáticos dos fractais gerados por sistemas de funções iteradas (IFS) e sua aplicação na criptografia, em particular, os IFS possuem uma estrutura matemática complicada, especialmente na construção recursiva de tais funções, fornecendo melhores aproximações, as quais geram alguns aspectos muito úteis na área de criptografia.

Em relação à orientação e distribuição dos capítulos, o trabalho será dividido em etapas. No Capítulo 2, serão exploradas definições que servirão de base para o entendimento e o estudo da Criptografia e da Geometria Fractal, percorrendo um caminho pelos sistemas dinâmicos, teoria dos números, álgebra e espaços métricos.

O Capítulo 3 e o Capítulo 4 abordam, respectivamente, os fundamentos criptográficos e a Geometria Fractal, realizando um estudo detalhado dos principais resultados necessários para a união desses dois mundos, que será concretizada no Capítulo 5, onde

é apresentada uma aplicação, ou seja, um método criptográfico baseado na escolha de um fractal conhecido gerado por um sistema de funções iteradas (IFS).

Capítulo

2

Conceitos preliminares

Neste capítulo de conceitos elementares, busca-se situar o leitor no contexto do trabalho, proporcionando uma base sólida para a compreensão dos resultados apresentados ao longo do texto. Além disso, serão revisitadas definições essenciais que serão necessárias para o desenvolvimento do tema, assegurando sua clara compreensão. Também será feita uma breve contextualização histórica, situando o leitor na linha do tempo dos principais pensadores matemáticos que contribuíram com resultados relevantes sobre o tema.

2.1 Elementos de Espaços Métricos

A Teoria dos Espaços Métricos, de forma geral, trata da noção de distância entre pontos, conjuntos e elementos em geral. Suas bases foram estabelecidas no contexto do Cálculo Funcional em 1906 por *Maurice Fréchet* (1878 - 1973), um matemático francês, em seu trabalho intitulado *"Sur quelques points du calcul fonctionnel"*, no qual aborda espaços generalizados e contribuições para a formalização da noção de limite.

David Hilbert (1862 - 1943) também fez importantes contribuições nessa área. Em 1912, o termo "Espaços Métricos" foi utilizado pelo matemático alemão *Felix Hausdorff* (1868 - 1942) em seu trabalho sobre Teoria dos Conjuntos, intitulado *"Grundzüge der Mengenlehre"* (Princípios Básicos da Teoria dos Conjuntos). Hausdorff descreveu axiomas com base nas contribuições de Fréchet, que já eram conhecidos e utilizados

por *Henri Poincaré* (1854 - 1912). No entanto, a teoria dos espaços métricos, como a conhecemos hoje, foi desenvolvida em 1924 pelo matemático russo *Pavel Samuilovich Urysohn* (1868 - 1942).

Com base em Barnsley (1988) e Lima (2020) e Domingues (1982), o objetivo desta seção é explorar resultados que fundamentarão o estudo para a geometria fractal, pois a noção de medida, distância e espaço será fortemente usada na definição do contexto em que a teoria fractal está inserida.

Definição 1. *Um espaço X é um conjunto, e os pontos deste espaço são chamados de elementos do conjunto.*

Definição 2. *Seja X um conjunto. É chamado de topologia em X uma família z de subconjuntos de X com as seguintes propriedades:*

i. $\emptyset$ e X pertencem a z;

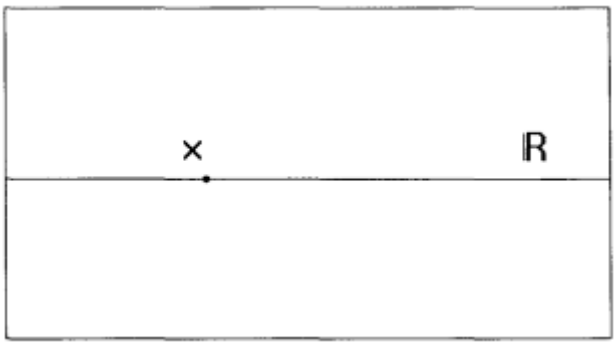
ii. A união de uma família arbitrária de membros de z pertence a z;

iii. A interseção de uma família finita de membros de z pertence a z.

Os membros de z são chamados de abertos. O par (X, z) é chamado de espaço topológico.

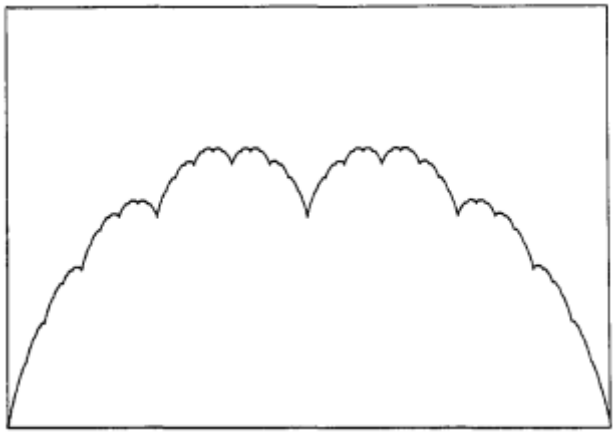
Exemplo 1. *Considere o espaço X como $\mathbb{R}$, $X = \mathbb{R}$. Um elemento de $\mathbb{R}$ é um ponto x na reta. Observe a Figura 2.1:*

Figura 2.1: Um ponto x no espaço $\mathbb{R}$



Fonte: Retirado de Barnsley (1988)

Figura 2.2: Uma função f em $X = C[0,1]$



Fonte: Retirado de Barnsley (1988)

Exemplo 2. *Considere X como o espaço das funções contínuas definidas no intervalo fechado $[0,1] = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$ na reta real $\mathbb{R}$, ou seja, $X = C[0,1]$. Um elemento de X é uma função $f : [0,1] \to \mathbb{R}$. Conforme ilustrado na Figura 2.2.*

Definição 3. *Um espaço métrico (X,d) é um espaço qualquer X com uma função real $d : X \times X \to \mathbb{R}$ que mede a distância entre elementos x e y de X. Para que (X,d) seja um espaço métrico, as seguintes propriedades devem ser verificadas:*

1. $d(x,y) = d(y,x)\ \forall\ x,y \in X$;
2. $0 < d(x,y) < \infty\ \forall\ x,y \in X,\ x \neq y$;
3. $d(x,x) = 0,\ \forall\ x \in X$;
4. $d(x,y) \leq d(x,z) + d(z,y),\ \forall\ x,y,z \in X$.

Exemplo 3. *Seja $X = \mathbb{R}^n$, isto é, elementos de $\mathbb{R}^n$ são do tipo $x = (x_1, \cdots, x_n)$, em que cada uma das coordenadas x_i, $i = 1, \cdots, n$ é um número real. Dados elementos $x, y \in \mathbb{R}^n$, define-se $d, d', d'' : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$:*

$$\begin{aligned} d(x,y) &= \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2} = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \\ d'(x,y) &= |x_1 - y_1| + \cdots + |x_n - y_n| = \sum_{i=1}^{n}|x_i - y_i| \\ d''(x,y) &= max\{|x_1 - y_1|, \cdots, |x_n - y_n|\} = max_{1 \leq i \leq n}|x_i - y_i|. \end{aligned}$$

Observe que $(X, d), (X, d')$ e (X, d'') são de fato, espaços métricos. Com efeito, para que d, d' e d'' sejam métricas em $X = \mathbb{R}^n$, se faz necessário demonstrar as quatro propriedades da Definição 3:

1. $d(x, y) = d(y, x)$

   Considere $x, y \in \mathbb{R}^n$, segue que:

$$\begin{aligned} d(x,y) &= \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2} \\ &= \sqrt{(y_1 - x_1)^2 + \cdots + (y_n - x_n)^2} \\ &= d(y,x). \end{aligned}$$

$$\begin{aligned} d'(x,y) &= |x_1 - y_1| + \cdots + |x_n - y_n| \\ &= |y_1 - x_1| + \cdots + |y_n - x_n| \\ &= d'(y,x) \end{aligned}$$

$$\begin{aligned} d''(x,y) &= max\{|x_1 - y_1|, \cdots, |x_n - y_n|\} \\ &= max\{|y_1 - x_1|, \cdots, |y_n - x_n|\} \\ &= d''(y,x) \end{aligned}$$

2. $0 < d(x, y) < \infty$

   Considere $x, y \in \mathbb{R}^n$, $x \neq y$, logo existe $i \in \{1, \cdots, n\}$, tal que $x_i \neq y_i$, logo:

$$d(x,y) = \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2} \geq \sqrt{(x_i - y_i)^2} = |x_i - y_i| > 0.$$

$$d'(x,y) = |x_1 - y_1| + \cdots + |x_n - y_n| \geq |x_i - y_i| > 0.$$

$$d''(x,y) = max\{|x_1 - y_1|, \cdots, |x_n - y_n|\} \geq |x_i - y_i| > 0.$$

3. $d(x,x) = 0$

   Para cada $x \in \mathbb{R}^n$, tem-se:

$$d(x,x) = \sqrt{(x_1 - x_1)^2 + \cdots + (x_n - x_n)^2} = \sqrt{0 + \cdots + 0} = \sqrt{0} = 0.$$

$$d'(x,x) = |x_1 - x_1| + \cdots + |x_n - x_n| = |0| + \cdots + |0| = 0.$$

$$d''(x,x) = max\{|x_1 - x_1|, \cdots, |x_n - x_n|\} = max\{0, \cdots, 0\} = 0.$$

4. $d(x,y) \leq d(x,z) + d(z,y)$

   Considere $x, y, z \in \mathbb{R}^n$, logo:

$$\begin{aligned} d(x,z) &= \sqrt{(x_1 - z_1)^2 + \cdots + (x_n - z_n)^2} \\ &= \sqrt{(x_1 - y_1 + y_1 - z_1)^2 + \cdots + (x_n - y_n + y_n - z_n)^2} \\ &\leq \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2} + \sqrt{(y_1 - z_1)^2 + \cdots + (y_n - z_n)^2} \\ &= d(x,y) + d(y,z). \end{aligned}$$

$$\begin{aligned} d'(x,z) &= |x_1 - z_1| + \cdots + |x_n - z_n| \\ &= |x_1 - y_1 + y_1 - z_1| + \cdots + |x_n - y_n + y_n - z_n| \\ &\leq |x_1 - y_1| + |y_1 - z_1| + \cdots + |x_n - y_n| + |y_n - z_n| \\ &= d'(x,y) + d'(y,z). \end{aligned}$$

$$\begin{aligned} d''(x,z) &= max\{|x_1 - z_1|, \cdots, |x_n - z_n|\} \\ &= max\{|x_1 - y_1 + y_1 - z_1|, \cdots, |x_n - y_n + y_n - z_n|\} \\ &\leq max\{|x_1 - y_1|, \cdots, |x_n - y_n|\} + max\{|y_1 - z_1|, \cdots, |y_n - z_n|\} \\ &= d''(x,y) + d''(y,z). \end{aligned}$$

Logo, d, d' e d'' são métricas, consequentemente $(X,d), (X,d')$ e (X,d'') são espaços métricos.

□

Definição 4. *Duas métricas d_1 e d_2 em um espaço X são equivalentes se existem constantes $0 < c_1 < c_2 < \infty$ tais que:*

$$c_1 d_1(x,y) \leq d_2(x,y) \leq c_2 d_1(x,y), \ \forall \ (x,y) \in X \times X.$$

Um fato interessante sobre métricas equivalentes é que qualquer par de métricas equivalentes dão a mesma noção de quais elementos do espaço estão próximos e quais estão distantes.

Definição 5. *Dois espaços métricos (X_1, d_1) e (X_2, d_2) são equivalentes se existe uma função $h : X_1 \to X_2$ invertível tal que a métrica $\tilde{d}_1$ em X_1 definida por:*

$$\tilde{d}_1(x,y) = d_2(h(x), h(y)), \ \forall \ x, y \in X_1.$$

é equivalente a d_1.

Definição 6. *Uma função $f : X_1 \to X_2$ de um espaço métrico (X_1, d_1) em um espaço métrico (X_2, d_2) é dita contínua se, para cada $\varepsilon > 0$ e $x \in X_1$, existe um $\delta > 0$ tal que:*

$$d_1(x,y) < \delta \Rightarrow d_2(f(x), f(y)) < \varepsilon.$$

Observe que se a função f é invertível e sua inversa f^{-1} é uma função contínua, então podemos afirmar que a função f estabelece um homeomorfismo entre os espaços X_1 e X_2. Isso é equivalente a dizer que os espaços X_1 e X_2 são homeomorfos.

Além disso, dizer que dois espaços são equivalentes não é simplesmente dizer que eles são homeomorfos. Para serem equivalentes, deve haver uma relação entre ε e δ satisfazendo a Definição 6, independentemente de x.

2.1.1 Espaços Métricos Completos

Os espaços métricos geralmente possuem um caráter geométrico simples, mas nem sempre. Existem algumas propriedades que ocorrem repetidamente em subconjuntos de espaços métricos e que auxiliam na descrição de conjuntos fractais e outros tipos de subconjuntos. Algumas dessas propriedades incluem conjuntos abertos, fechos, limites, completude, compacidade, entre outras. Portanto, a geometria fractal, objeto de estudo deste trabalho, busca descrever, classificar, analisar e observar subconjuntos de espaços métricos (X, d) de maneira coerente.

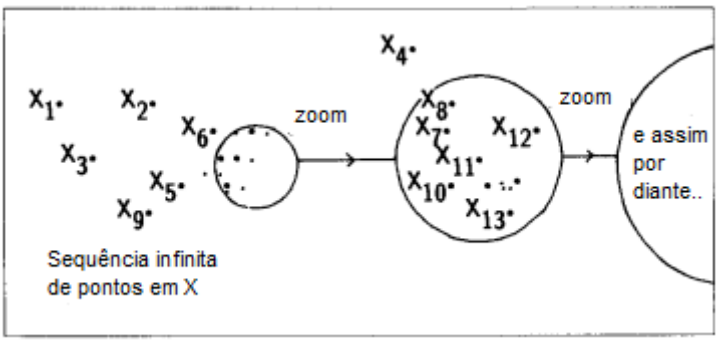
No estudo posterior sobre fractais, é necessário considerar um tipo específico de espaço métrico, conhecido como espaço métrico completo. No entanto, antes disso, é importante revisar alguns resultados.

Definição 7. *Uma sequência $(x_n)_{n=1}^{\infty}$ de pontos em um espaço métrico (X, d) é chamada de sequência de Cauchy se, para algum $\varepsilon > 0$, existe um inteiro $N > 0$, tal que*

$$d(x_n, x_m) < \varepsilon, \ \forall \ n, m > N.$$

Pode-se entender, de forma simplificada, que à medida em que a sequência progride, os pontos da sequência se aproximam. Para ilustrar a ideia, observe a Figura 2.3:

Figura 2.3: Representação dos pontos de uma sequência de Cauchy.



Fonte: Retirado de Barnsley (1988).

Note que, pelo fato de os pontos estarem se aproximando, isso não significa necessariamente que exista um ponto x para o qual a sequência esteja convergindo.

Definição 8. *Uma sequência $(x_n)_{n=1}^{\infty}$ de pontos em um espaço métrico (X, d) é dita convergente para um ponto $x \in X$ se, dado um $\varepsilon > 0$, existe um inteiro $N > 0$ tal que*

$$d(x_n, x) < \varepsilon, \ \forall \ n > N.$$

Neste caso, a sequência converge para o ponto $x \in X$, e tal ponto é chamado de limite da sequência, denotado por

$$x = \lim x_n$$

O limite x de uma sequência $(x_n)_{n=1}^{\infty}$ convergente possui a seguinte propriedade: Considere

$$B(x, \varepsilon) = \{y \in X \mid d(x, y) \leq \varepsilon\},$$

a bola fechada centrada em x e de raio ε. Qualquer bola centrada em x contém todos os pontos de x_n após um certo índice N, onde N se torna cada vez maior a medida que ε diminui.

Teorema 1. *Se uma sequência de pontos $(x_n)_{n=1}^{\infty}$ em um espaço métrico (X, d) converge para um ponto $x \in X$, então $(x_n)_{n=1}^{\infty}$ é de Cauchy.*

Demonstração. Seja (X, d) um espaço métrico e (x_n) uma sequência de pontos em (X, d) com limite a, isto é:

$$\lim x_n = a.$$

Dado $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$, tal que $n > n_0$ então $d(x_n, a) < \frac{\varepsilon}{2}$.

Tomando $m, n > n_0$, então:

$$d(x_m, x_n) \leq d(x_m, a) + d(x_n, a) < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Concluindo que (x_n) é de Cauchy.

□

Exemplo 4. *Considere uma sequência de números racionais (x_n) convergindo para um número irracional a, como por exemplo, $x_1 = 1$, $x_2 = 1.4$, $x_3 = 1.41$, $x_4 = 1.414$, $\cdots$. Com limite $\sqrt{2}$, i.e, $\lim x_n = \sqrt{2}$. Note que em $\mathbb{R}$ a sequência é convergente, porém, em $\mathbb{Q}$, (x_n) não é convergente. Logo, nem toda sequência de Cauchy é convergente.*

Definição 9. *Um espaço métrico (X, d) é completo se toda sequência de Cauchy $(x_n)_{n=1}^{\infty}$ em X tem limite $x \in X$.*

A Definição 9 garante que a sequência de Cauchy converge para um determinado ponto x, claro que $x = \lim_{n\to\infty} x_n$. Dado um espaço métrico (X, d) e uma sequência de Cauchy $(x_n)_{n=1}^{\infty}$ de pontos $x \in X$, se X é completo, então existe um ponto $x \in X$, tal que para $\varepsilon > 0$, a bola centrada em x e raio ε contém os pontos x_n da sequência para $n \to \infty$.

Exemplo 5. *Note que através do Exemplo 4, o conjunto $\mathbb{Q}$ não é um espaço métrico completo.*

Exemplo 6. *O conjunto $\mathbb{R}$ é um espaço métrico completo.*

De fato, considere (x_n) uma sequência de Cauchy em $\mathbb{R}$, logo, é bem sabido que (x_n) é limitada e que (x_n) possui subsequência convergente (x_{n_k}), desta forma, como (x_n) é de Cauchy e possui subsequência convergente, (x_n) também converge para o mesmo ponto, logo $\mathbb{R}$ é um espaço métrico completo.

Definição 10. *Seja S um subconjunto próprio de $\mathbb{R}^n$. O ponto a é dito interior de S se existe uma bola centrada em a de raio $r > 0$ contida em S. O conjunto de pontos interiores é chamado interior de S e é denotado por $int(S)$.*

Definição 11. *Um conjunto $S \subseteq \mathbb{R}^n$ é aberto se todos os seus elementos são pontos no interior de S, isto é, o conjunto S é aberto se e somente se $S = int(S)$.*

Exemplo 7. *i. O conjunto vazio é aberto, note que $int(\varnothing) = \varnothing$;*

ii. O conjunto $\mathbb{R}$ é aberto, pois tomando um ponto $x \in \mathbb{R}$, qualquer bola centrada em x de raio $r > 0$, estará contido no conjunto $\mathbb{R}$;

iii. Um intervalo aberto $A = (x, y)$ em $\mathbb{R}$ é um conjunto aberto.

Considere $a \in A$, tome $r = min\{y - a, a - x\}$, afirma-se que $(a - r, a + r) \subseteq A$.

Considere agora $b \in (a - r, a + r)$, se $b < a$, então $a - r < b < a$, com isto, segue que $a - b < r \leq a - x$. Logo:

$$x < b \leq a < y.$$

então $b \in A$, desta forma se $b = a$, então $b \in A$. O caso se $b > a$ é análogo.

Definição 12. *Seja $S \subset X$ um subconjunto de um espaço métrico (X, d). Um ponto $x \in X$ é chamado aderente a S se existe uma sequência $(x_n)_{n=1}^{\infty}$ de pontos $x_n \in S \setminus (x)$ tal que:*

$$\lim_{n\to\infty} x_n = x.$$

Definição 13. *Seja $S \subset X$ um subconjunto de um espaço métrico (X, d). O fecho de S, denotado $\overline{S}$ é definido:*

$$\overline{S} = S \cup \{pontos\ aderentes\ de\ S\}.$$

S é fechado se contém todos os pontos aderentes, isto é, $S = \overline{S}$. S é dito perfeito se for igual ao conjunto de todos seus pontos aderentes.

Exemplo 8. *Pensando no contexto do conjunto $\mathbb{R}$, note que um determinado conjunto F é fechado se $\mathbb{R}-F$ é aberto, logo observe que o intervalo $[a,b]$ é fechado, pois tomando $F=[a,b]$, então $\mathbb{R}-F=(-\infty,a)\cup(b,\infty)$.*

Perceba que $(-\infty,a)$ é aberto, de modo que tomando $-n<a$, onde $n\in\mathbb{N}$, segue que $x_k=(-k,a)$ é aberto, já que:

$$(-\infty,a)=\bigcup_{k=n}^{\infty}x_k.$$

De maneira análoga (b,∞) é aberto, portanto $\mathbb{R}-F$ é aberto e consequentemente $[a,b]$ é fechado.

Definição 14. *Seja $S\subset X$ um subconjunto de um espaço métrico (X,d). Um ponto $x\in X$ é dito ponto de fronteira de S se para cada $\varepsilon>0$, a bola $B(x,\varepsilon)$ contém um ponto em $X\setminus S$ e um ponto em S. O conjunto de todos os pontos de fronteira é dito a fronteira de S, denotado ∂S.*

2.1.2 Conjuntos compactos

Definição 15. *Seja $S\subset X$ um subconjunto de um espaço métrico (X,d). S é compacto se toda sequência infinita $(x_n)_{n=1}^{\infty}$ em S contém uma subsequência que converge para um ponto $p\in S$. Um espaço métrico (X,d) é compacto se o conjunto X é compacto.*

Exemplo 9. *Todo conjunto finito é compacto, pois seja K um conjunto finito, e considere $(x_n)=(x_1,x_2,\cdots)$ uma sequência de pontos de K, logo existe um termo x_r, tal que $(x_r,x_r,\cdots)$ é uma subsequência da sequência (x_n). Note que $(x_r,x_r,\cdots)$ converge para x_r, o que prova a afirmação.*

Definição 16. *Seja $S\subset X$ um subconjunto de um espaço métrico (X,d). S é limitado se existe um ponto $a\in X$ e uma constante $R>0$, tal que*

$$d(a,x)<R,\ \forall\ x\in S.$$

Definição 17. *(ε-rede) Seja $S\subset X$ um subconjunto de um espaço métrico (X,d). S é totalmente limitado se, para $\varepsilon>0$, existe um conjunto finito de pontos $\{y_1,y_2,\cdots,y_n\}\subset$*

S, dito ε-rede, tal que para qualquer $x \in S$, $d(x, y_i) < \varepsilon$ para algum $y_i \in \{y_1, y_2, \cdots, y_n\}$.

Proposição 1. *(Princípio da Casa dos Pombos) Sejam dois conjuntos A e B. Se $|B| < |A|$, então para cada função $f : A \to B$ existem pelo menos dois elementos do conjunto A que são levados a um mesmo elemento de B pela função f.*

Demonstração. Suponha por absurdo que nenhum elemento b do conjunto B possa ser obtido a partir de um elemento a do conjunto A. Por hipótese, tem-se que $f : A \to B$, e definição de função, para todo elemento do domínio é necessário ter uma imagem em B, de modo que $f(a) = b$.

Observe que desta forma, os conjuntos A e B possuem o mesmo número de elementos ou B possui mais elementos que A, o que é um absurdo, pois por hipótese $|B| < |A|$, conclui-se então que ao menos um elemento do conjunto A é imagem de pelo menos dois elementos do conjunto A.

□

Uma maneira mais simples de se entender o Princípio da Casa dos Pombos é a seguinte: Considere n casas de pombos e m pombos, de modo que $m > n$, considere também que os m pombos são colocados de forma aleatória nas n casas, como $m > n$, então pelo menos uma das caixas terá mais de um pombo.

Teorema 2. *Seja (X, d) um espaço métrico completo. Consideremos $S \subset X$, S é compacto se e somente se é fechado e totalmente limitado.*

Demonstração. ($\Leftarrow$)

Por hipótese, S é fechado e totalmente limitado. Seja $(x_i) \in S$ uma sequência infinita de pontos em S, como S é totalmente limitado, podemos definir uma coleção de bolas fechadas de raio $r = 1$, $B(x, 1)$, tal que S está contido na união de tais bolas, isto é:

$$S \subset \bigcup_{i=1}^{\infty} B_i$$

Pelo Princípio da Casa dos Pombos, uma determinada bola, B_1 por exemplo, contém uma infinidade de pontos x_n. Tomando N_1 tal que $x_{N_1} \in B_1$, note que $B_1 \cap S$ é

totalmente limitado, logo podemos cobrir $B_1 \cap S$ por um conjunto finito de bolas de raio $r = \frac{1}{2}$.

Novamente pelo Princípio da Casa dos Pombos, uma outra bola, B_2 por exemplo, também vai conter uma infinidade de pontos x_n, tomando N_2, tal que $x_{N_2} \in B_2$ e $N_2 > N_1$. Continuando com este raciocínio, teremos:

$$B_1 \supset B_2 \supset B_3 \supset \cdots \supset B_n \supset \cdots$$

Onde B_n tem raio $r = \frac{1}{2^{n-1}}$ e a sequência de inteiros $(N_n)_{n=1}^{\infty}$ tal que $x_{N_n} \in B_n$. Note que $(x_{N_n})_{n=1}^{\infty}$ é uma subsequência de (x_n) e é de Cauchy em S, como S é fechado, a sequência (X_{N_n}) converge para um ponto $x \in S$, logo, S é compacto.

$(\Rightarrow)$

Por hipótese, temos que S é compacto. Consideremos um $\varepsilon > 0$ e suponha que não exista uma ε-rede para S. Então existe uma sequência infinita de pontos $\{x_n \in S\}$ com $d((x_i, x_j) \geq \varepsilon$ para todo $i \neq j$. Porém, essa sequência possui uma subsequência convergente $\{x_{N_i}\}$. Sabemos que toda sequência que possui uma subsequência convergente, é de Cauchy, desta forma, temos um par de inteiros N_i e N_j tal que $N_i \neq N_j$, logo $d(x_{N_i}, x_{N_J}) < \varepsilon$.

Mas, $d(x_{N_i}, x_{N_J}) \geq \varepsilon$, o que é um absurdo. Desta forma não existe uma ε-rede para S.

□

Definição 18. *Seja $S \subset X$ um subconjunto de um espaço métrico (X, d). S é aberto se para cada $x \in S$ existe um $\varepsilon > 0$ tal que $B(x, \varepsilon) = \{y \in X \mid d(x, y) \leq \varepsilon\} \subset S$.*

Proposição 2. *Considere (X, d) um espaço métrico, então $S \subset X$ é aberto se, e somente se $X \setminus S$ é fechado.*

Demonstração. Suponha que $S \subset X$ é aberto, considere $\{x_n\}$ uma sequência em $X \setminus S$ com um limite $x \in X$. Devemos mostrar que $x \in X \setminus S$, para isto, assumimos que $x \in S$, logo, toda bola $B(x, \varepsilon)$ com $\varepsilon > 0$ contém um ponto $x_n \in X \setminus S$ que significa que S não é aberto, o que é um abusrdo, logo tal afirmação de que $x \in S$ é falsa, desta forma $x \in X \setminus S$, portanto $X \setminus S$ é fechado.

Supomos agora que $X \setminus S$ é fechado, consideremos $x \in S$, queremos mostrar que existe uma bola $B(x, \varepsilon) \subset S$, para isto, assumimos que não existe tal bola $B(x, \varepsilon) \subset S$. Logo, para cada inteiro $n = 1, 2, 3, \cdots$, temos um ponto $x_n \in B(x, \frac{1}{n}) \cap (X \setminus S)$, assim, $\{x_n\}$ é uma sequência em $X \setminus S$ com limite $x \in X$. Como $X \setminus S$ é fechado, podemos concluir que $x \in X \setminus S$, o que é um absurdo, pois $x \in S$. Desta maneira, a afirmação de que não existe uma bola $B(x, \varepsilon) \subset S$ é falsa, logo S é aberto.

□

2.1.3 Conjuntos conexos e desconexos

Definição 19. *Um espaço métrico (X, d) é dito conexo se os únicos subconjuntos de X que são simultaneamente abertos e fechados são o próprio X e $\varnothing$. Um subconjunto $S \subset X$ é conexo se o espaço métrico (S, d) é conexo. S é desconexo se não é conexo. S é totalmente desconexo se os únicos subconjuntos conexos de S não vazios sejam apenas conjuntos de pontos únicos.*

Definição 20. *Seja $S \subset X$ um subconjunto de um espaço métrico (X, d). S é conexo por caminhos se, para cada par de pontos x e y em S, existe uma função contínua $f : [0, 1] \to S$ do espaço métrico $([0, 1], d)$ no espaço métrico (S, d), tal que $f(0) = x$ e $f(1) = y$. Tal função f é chamada de caminho de x para y em S. Além disso, S é desconexo por caminhos se não é conexo por caminhos.*

Exemplo 10. *Todo subconjunto unitário de um espaço métrico (X, d) é conexo.*

Exemplo 11. *O subconjunto $\{0, 1\}$ de $\mathbb{R}$ é desconexo, pois tome $U = \{0\}$ e $V = \{1\}$, note que U e V são disjuntos, não vazios. A união entre os conjuntos $\{0, 1\}$ e U, assim como a união entre $\{0, 1\}$ e V são os seguintes conjuntos:*

$$U = \left]-1, \frac{1}{2}\right[\cap \{0, 1\} \text{ e } V = \left]\frac{1}{2}, 2\right[\cap \{0, 1\}.$$

Desta forma, U e V são ambos abertos em $\{0, 1\}$, o que justifica a afirmação.

Exemplo 12. *Considere no $\mathbb{R}^2$ o conjunto A definido como:*

$$A = \{(x, y) \in \mathbb{R}^2 | x \cdot y = 1\}.$$

Note que A é desconexo, pois sendo $G = \{(x, y) \in \mathbb{R}^2 \mid x, y > 0\}$ e $H = \{(x, y) \in \mathbb{R}^2 \mid x, y < 0\}$, então os subconjuntos:

$$U = \mathbb{R}^2 \cap G \text{ e } V = \mathbb{R}^2 \cap H,$$

formam uma desconexão do conjunto A.

2.2 Elementos de Sistemas dinâmicos

O que é um sistema dinâmico? Se um sistema é dinâmico, sua estrutura se altera conforme o tempo passa, e é exatamente isso que se busca compreender: o comportamento de um determinado sistema à medida em que o tempo t decorre, podendo ser discreto, ou seja, $t \in \mathbb{Z}$, ou contínuo, onde $t \in \mathbb{R}$.

Além disso, outro questionamento motivador pode ser elencado: como os fenômenos se alteram na natureza? *Galileo Galilei* (1564 - 1642), um célebre astrônomo e físico, e *Isaac Newton* (1643 - 1727), matemático e físico, são figuras de grande renome desde suas épocas e desempenharam papéis fundamentais na revolução que afirmava que a natureza obedece a leis imutáveis que podem ser descritas pela matemática. A revolução Newtoniana parte do pressuposto de que os princípios da natureza podem ser expressos em termos de matemática e física, o que permite prever e projetar eventos com certeza matemática. Com base em Baraviera; F. M. Branco (2012), Hasselblatt; A. Katok (2003) e Arrowsmith; C. M. Place (1990), apresentam-se a seguir alguns resultados importantes acerca dos Sistemas Dinâmicos.

Um sistema dinâmico é uma função φ definida em um conjunto A qualquer, nele mesmo, isto é,

$$\varphi : A \to A.$$

De acordo com Baraviera; F. M. Branco (2012), a dinâmica do sistema é o processo de iteração da função φ, ou seja, constitui-se do cálculo de $\varphi(x)$, onde $x \in A$, e, em seguida, a reaplicação de φ ao resultado para obter $\varphi(\varphi(x)) = \varphi^2(x)$. O índice 2 significa a segunda aplicação da função φ e uma convenção para evitar escrever expressões como a seguinte:

$$\varphi(\varphi(\varphi(\varphi(x)))).$$

Repete-se o processo até $\varphi^k(x)$, $k > 0$, isto é, a k-ésima aplicação de φ em x, tal notação não significa elevar a função $\varphi(x)$ a k-ésima potência.

O processo iterativo da função φ em um determinado ponto inicial x_0 gera um sistema dinâmico, desta forma, a ideia de um sistema dinâmico é analisar o comportamento futuro da função, é de se esperar que se $k < 0$, então buscamos compreender o comportamento passado de φ. Observe um exemplo com uma função básica logo abaixo.

Exemplo 13. *Seja $f : \mathbb{R} \to \mathbb{R}$ uma função definida por $f(x) = x^2$. Tome o ponto inicial como $x_0 = 2$, com o processo iterativo de f em $x_0 = 2$, gerando o seguinte sistema dinâmico:*

$$\begin{aligned}
&x_0 = 2\\
&f^1(x_0) = f(x_0) = (x_0)^2 = 2^2 = 4 = x_1\\
&f^2(x_0) = f(f(x_0)) = f(x_1) = 4^2 = 16 = x_2\\
&f^3(x_0) = f(f(f(x_0))) = f(x_2) = 16^2 = 256 = x_3\\
&\cdots\\
&f^k(x_0) = f(x_{k-1}) = (x_{k-1})^2
\end{aligned}$$

O conjunto formado pelos resultados das sucessivas iterações de um ponto é chamado de *órbita* desse ponto. Na função anterior, a órbita de $x_0 = 2$ é dada por: $\{2, 4, 16, 256, 65536, ...\}$.

Tal conjunto pode ser denotado como:

$$O(x) := \bigcup_{n\in\mathbb{N}} f^n(x).$$

Pode-se ter órbitas finitas com um número finito de elementos, ou órbitas infinitas com um número infinito de elementos.

Observe as órbitas dos seguintes pontos x_0 para a função $f(x) = x^2$ anterior:

(i.) Para $x_0 = 1$, obtêm-se o conjunto: $O(1) = \{1, 1, 1, 1, \cdots\}$

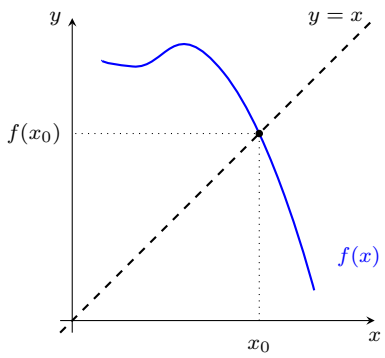
(ii.) Para $x_0 = \frac{1}{2}$, segue o conjunto: $O(\frac{1}{2}) = \{\frac{1}{2}, \frac{1}{4}, \frac{1}{16}, \cdots\}$

(iii.) Já para $x_0 = 3$, forma-se o conjunto: $O(3) = \{3, 9, 81, 6561, \cdots\}$

Em *(i.)*, a sequência dos elementos do conjunto é invariante. Assim, $x_0 = 1$ é um *ponto fixo*, desta forma, define-se:

Definição 21. *Um ponto x_0 tal que $f(x_0) = x_0$ é chamado de ponto fixo da função $f(x)$. Geometricamente, um ponto fixo de uma função é um ponto de interseção entre a reta $y = x$ com o gráfico da função $f(x)$, conforme a Figura (2.4).*

Figura 2.4: Representação Geométrica do Ponto Fixo



Fonte: O próprio autor

Já em *(ii.)*, a sequência de valores da órbita de $x_0 = \frac{1}{2}$ diminuem gradativamente, o mesmo ocorre com a função f para todo ponto x_0 tal que $|x_0| < 1$.

Por fim, em *(iii.)* a sequência dos elementos da órbita de $x_0 = 3$ cresce infinitamente. Neste caso, tem-se uma *órbita progressiva*. O mesmo ocorre com a função f para todo ponto x_0 tal que $|x_0| > 1$.

Definição 22. *Um ponto x_0 é periódico de período p se p é o menor inteiro tal que $f^p(x_0) = x_0$.*

Quando $p = 1$, segue que $f(x_0) = x_0$, então x_0 é simplesmente ponto fixo para a função f.

Exemplo 14. *Seja $f : \mathbb{C} \to \mathbb{C}$ uma função tal que $f(z) = z^2 + c$, onde $z \in \mathbb{C}$ e $c = a + bi$ é uma constante com $a, b \in \mathbb{C}$ e $i = \sqrt{-1}$.*

Tomando $z_0 = 0$ como ponto inicial, observe o que ocorre com as órbitas para alguns valores de c nessa função:

(i.) Para $c = -1$, tem-se: $-1, 0, -1, 0, -1, \cdots$;

(ii.) Para $c = i$, tem-se: $0, i, i-1, -i, i-1, -i, \cdots$

As sequências das órbitas de (i.) e (ii.) são *periódicas*. É dito que uma órbita é periódica se existem inteiros m, n com $m \geq n$, tais que $f^{m+n}(x_0) = f^n(x_0)$.

Logo abaixo, será explorado um resultado de grande importância que será utilizado ao longo de todo o processo de estudo. Trata-se do conceito de contrações.

2.2.1 Contrações no Espaço Euclidiano

Baseado em Hasselblatt; A. Katok (2003), define-se contrações no espaço euclidiano de acordo com a distância euclidiana, considerando X um espaço topológico com a métrica euclidiana. Dados $x = (x_1, x_2, \cdots, x_n)$ e $y = (y_1, y_2, \cdots, y_n)$ pertencentes a $\mathbb{R}^n$, segue:

$$d(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}.$$

Definição 23. *Uma aplicação $f : X \to X$ é chamada de Lipschitz ou continuamente Lipschitz com constante de Lipschitz λ se:*

$$d(f(x), f(y)) \leq \lambda \cdot d(x, y), \ \ x, y \in X. \tag{2.1}$$

É dito que f é uma contração ou λ-contração se $0 \leq \lambda < 1$ e λ é dito ser o fator de contração da aplicação f.

A atribuição do nome *Lipschitz* às aplicações f que satisfazem a propriedade acima é em menção ao matemático alemão *Rudolf Otto Sigismund Lipschitz* (1832 - 1903).

Exemplo 15. *Considere a função $f : X \to \mathbb{R}$, dada por $f(x) = x^2$. f é Lipschitz se o conjunto X for limitado.*

Com efeito, por hipótese, se X é limitado, existe uma constante A, tal que $|x| \leq A$, para todo $x \in X$. Logo:

$$\begin{aligned} |f(x) - f(y)| &= |x^2 - y^2| \\ &= |x - y| \cdot |x + y| \\ &\leq (|x| + |y|) \cdot |x - y|. \end{aligned}$$

Note que por hipótese $|x|, |y| \in X$, então $|x|, |y| \leq A$. Portanto:

$$|f(x) - f(y)| \leq 2A \cdot |x - y|.$$

Conclui-se que f é Lipschitz se $\lambda \leq 2A$.

□

2.2.1.1 Condições de contração para uma variável

A seguir, apresenta-se uma condição de contração que utiliza a derivada, no caso de uma única variável, mas antes, é necessário um resultado.

Teorema 3. ***(Teorema do Valor Médio)*** *- Se $g : [a, b] \to \mathbb{R}^m$ é contínua e diferenciável em (a, b), então existe um ponto $t \in [a, b]$ tal que:*

$$\|g(b) - g(a)\| \leq \|g'(t)\| \cdot (b - a).$$

Para que seja provado o resultado, será necessário o uso de dois fatos:

(i.) **(Teorema do Valor Médio para uma variável)** - Se $f : [a, b] \to \mathbb{R}$ é contínua em $[a, b]$ e diferenciável em (a, b), então existe $t \in (a, b)$ tal que $f(b) - f(a) = f'(t) \cdot (b - a)$;

(ii.) **(Desigualdade de Cauchy-Schwarz)** - Sejam $u, v \in \mathbb{R}$, $|\langle u, v \rangle| \leq \|u\| \cdot \|v\|$.

Munidos dos fatos anteriores, segue a demonstração do Teorema 3:

Demonstração. Sejam $v = g(b) - g(a)$ e $\varphi(t) =< v, g(t) >$.

Pelo item (i.), existe $t \in (a, b)$ tal que,

$$\begin{aligned}\varphi(b)-\varphi(a) &= \varphi'(t)\cdot(b-a)\\ &= (b-a)\cdot < v, g'(t) > .\end{aligned}$$

Aplicando o item (ii.):

$$\varphi(b)-\varphi(a) \leq (b-a)\cdot\|v\|\cdot\|g'(t)\|. \tag{2.2}$$

Por outro lado, segue que:

$$\begin{aligned}\varphi(b)-\varphi(a) &= < v, g(b) > - < v, g(a) >\\ &= < v, g(b)-g(a) >\\ &= < v, v >\\ &= \|v\|^2.\end{aligned}$$

Desta forma, pela Equação 2.2, tem-se que:

$$\begin{aligned}\|v\|^2 &\leq (b-a)\cdot\|v\|\cdot\|g'(t)\|\\ \|v\| &\leq (b-a)\cdot\|g'(t)\|\\ \|g(b)-g(a)\| &\leq (b-a)\cdot\|g'(t)\|.\end{aligned}$$

□

Proposição 3. *Seja I um intervalo e $f : I \to \mathbb{R}$ uma função diferenciável. Então f é Lipschitz se, e somente se, $|f'(x)| \leq \lambda$, para todo $x \in I$.*

Demonstração. Considere um intervalo fechado $[x, y] \subset I$. Como a função $f : I \to \mathbb{R}$ é diferenciável, então f é contínua no intervalo $[x, y]$ e derivável no intervalo aberto (x, y).

Pelo Teorema do Valor Médio para uma variável, se as condições acima são satisfeitas, então existe um ponto $c \in (x, y)$ tal que $f'(c) = \dfrac{f(x) - f(y)}{x - y}$, logo, é válido escrever:

$$f(x) - f(y) = f'(c) \cdot (x - y).$$

Como $f'(c) \leq \lambda$, segue que,

$$\begin{aligned} |f(x) - f(y)| &= |f'(c)| \cdot |x - y| \\ &\leq \lambda \cdot |x - y|. \end{aligned}$$

Logo, f é Lipschitz.

Por outro lado, suponha que f é Lipschitz, então existe $\lambda > 0$, tal que para quaisquer $x, y \in I$, vale que:

$$\begin{aligned} |f(x) - f(y)| &\leq \lambda \cdot |x - y| \\ \left| \frac{f(x) - f(y)}{x - y} \right| &\leq \lambda. \end{aligned}$$

Passando o limite de $x \to y$:

$$\left| \lim_{x \to y} \frac{f(x) - f(y)}{x - y} \right| \leq \lim_{x \to y} \lambda = \lambda.$$

Como f é derivável em I, então $|f'(x)| \leq \lambda$.

□

Proposição 4. ***(Princípio da Contração)***. *Seja $I \subset \mathbb{R}$ um intervalo fechado, possivelmente infinito, e $f : I \to I$ uma λ-contração. Então f tem um único ponto fixo x_0 e $|f^n(x) - x_0| \leq \lambda^n \cdot |x - x_0|$, para todo $x \in \mathbb{R}$, isto é, toda órbita de f converge para x_0, exponencialmente.*

Demonstração. Por hipótese, f é Lipschitz, desta forma, segue que:

$$|f(x) - f(y)| \leq \lambda \cdot |x - y|.$$

Iterando a função f, obtêm-se:

$$|f^n(x) - f^n(y)| = |f(f^{n-1}(x)) - f(f^{n-1}(y))| \leq \lambda \cdot |f^{n-1}(x) - f^{n-1}(y)|$$

$$|f^{n-1}(x)) - f^{n-1}(y))| = |f(f^{n-2}(x)) - f(f^{n-2}(y))| \leq \lambda^2 \cdot |f^{n-2}(x) - f^{n-2}(y)|$$

$$\cdots$$

$$|f^n(x) - f^n(y)| \leq \lambda^n \cdot |x - y|, \ \forall \ x, y \in, \mathrm{n} \in \mathbb{N}. \tag{2.3}$$

Então, para $x \in I$ e $m \geq n$, é valido escrever que:

$$|f^m(x) - f^n(x)| = |f^m(x) - f^{m-1}(x) + f^{m-1}(x) - f^{m-2}(x) + f^{m-2}(x) - \cdots + f^{n+1}(x) - f^n(x)|.$$

Aplicando a desigualdade triangular:

$$|f^m(x) - f^{m-1}(x) + f^{m-1}(x) - \cdots + f^{n+1}(x) - f^n(x)| \leq |f^m(x) - f^{m-1}(x)| + \cdots + |f^{n+1}(x) - f^n(x)|.$$

Equivalentemente:

$$|f^m(x) - f^{m-1}(x) + f^{m-1}(x) - \cdots + f^{n+1}(x) - f^n(x)| \leq \sum_{k=0}^{m-n-1} |f^{n+k+1}(x) - f^{n+k}(x)|.$$

Fazendo de forma separada, segue que:

$$\sum_{k=0}^{m-n-1} |f^{n+k+1}(x) - f^{n+k}(x)| = \sum_{k=0}^{m-n-1} |f^{n+k}(f(x)) - f^{n+k}(x)|.$$

Pela Equação 2.3, tem-se que:

$$\sum_{k=0}^{m-n-1} |f^{n+k}(f(x)) - f^{n+k}(x)| \leq \sum_{k=0}^{m-n-1} \lambda^{n+k} \cdot |f(x) - x|.$$

Portanto,

$$|f^m(x) - f^n(x)| \leq \sum_{k=0}^{m-n-1} \lambda^{n+k} \cdot |f(x) - x| = |f(x) - x| \cdot (\lambda^n + \lambda^{n+1} + \cdots + \lambda^{m-1}) = |f(x) - x| \cdot \frac{\lambda^n}{1-\lambda}.$$

Como λ está compreendido entre 0 e 1, ou seja, $0 < \lambda < 1$, e $m \geq n$ quando n tende ao infinito, temos que $|f^m(x) - f^n(x)|$ tende a zero. Portanto, a sequência $(f^n(x))$ é uma sequência de Cauchy, o que implica que ela converge. Além disso, para todo $x \in I$, o limite da sequência $(f^n(x))$ existe e está contido em I, uma vez que I é um conjunto fechado.

Considere agora a existência do ponto fixo. Seja x_0 o limite de $f^n(x)$, isto é,

$$\lim_{n\to\infty} f^n(x) = x_0.$$

Sabe-se que $x \in I$ e $n \in \mathbb{N}$, então:

$$|x_0 - f(x_0)| = |x_0 - f^n(x) + f^n(x) - f^{n+1}(x) + f^{n+1}(x) - f(x_0)| \text{ e}$$

$$|x_0 - f^n(x) + f^n(x) - f^{n+1}(x) + f^{n+1}(x) - f(x_0)| \leq$$

$$\leq |x_0 - f^n(x)| + |f^n(x) - f^{n+1}(x)| + |f^{n+1} - f(x_0)|,$$

$$|x_0 - f^n(x) + f^n(x) - f^{n+1}(x) + f^{n+1}(x) - f(x_0)| \leq$$

$$\leq |x_0 - f^n(x)| + |f^n(x) - f^n(f(x))| + |f(f^n(x)) - f(x_0)|.$$

Aplicando a Equação 2.3:

$$|x_0 - f^n(x) + f^n(x) - f^{n+1}(x) + f^{n+1}(x) - f(x_0)| \leq$$

$$\leq |x_0 - f^n(x)| + \lambda^n \cdot |x - f(x)| + \lambda^n \cdot |f^n(x) - x_0| \Rightarrow$$

$$|x_0 - f^n(x) + f^n(x) - f^{n+1}(x) + f^{n+1}(x) - f(x_0)| \leq$$

$$\leq (1+\lambda) \cdot |x_0 - f^n(x)| + \lambda^n \cdot |x - f(x)| \Rightarrow$$

$$|x_0 - f(x_0)| \leq (1+\lambda) \cdot |x_0 - f^n(x)| + \lambda^n |x - f(x)|.$$

Desta forma, se n tende ao infinito, isto é, $n \to \infty$, então:

$$|x_0 - f(x_0)| \leq (1+\lambda) \cdot |x_0 - x_0| + 0 \cdot |x - f(x)|$$

$$|x_0 - f(x_0)| \leq 0$$

$$0 \leq |x_0 - f(x_0)| \leq 0$$

$$x_0 = f(x_0).$$

Logo, x_0 é ponto fixo.

Por fim, considere a unicidade do ponto fixo x_0:

Seja dois pontos fixos $f(x_0) = x_0$ e $f(y_0) = y_0$, portanto, é válido que:

$$|f(x) - f(y)| \leq \lambda \cdot |y - x|,\ 0 < \lambda < 1,\ \forall\ x, y \in I.$$

Então,

$$|x_0 - y_0| = |f(x_0) - f(y_0)| \leq \lambda \cdot |x_0 - y_0|$$

$$|x_0 - y_0| \leq \lambda \cdot |x_0 - y_0| \Leftrightarrow (1-\lambda) \cdot |x_0 - y_0| \leq 0.$$

Como $\lambda < 1$, então $0 < \lambda < 1$, logo

$$|x_0 - y_0| \leq \lambda \cdot |x_0 - y_0| \Leftrightarrow (1-\lambda) \cdot |x_0 - y_0| \leq 0 \Leftrightarrow |x_0 - y_0| = 0 \Leftrightarrow x_0 = y_0.$$

Desta forma, o ponto fixo é único.

□

2.2.1.2 Condições de contração para várias variáveis

Veja agora o caso de várias varáveis para o princípio da contração.

Teorema 4. *Seja $X \subset \mathbb{R}^n$ fechado e $f : X \to X$ uma λ-contração. Então f tem um único ponto fixo x_0 e $d(f^n(x), x_0) \leq \lambda^n \cdot d(x, x_0)$ para todo $x \in X$.*

Demonstração. Inicialmente, será provada a existência de um ponto fixo x_0. Da hipótese de f ser Lipschitz, segue que:

$$d(f(x), f(y)) \leq \lambda \cdot d(x, y).$$

Ao iterar, obtêm-se:

$$d(f^n(x), f^n(y)) \leq \lambda^n \cdot d(x, y), \ \forall \ x, y \in X, \ n \in \mathbb{N}. \tag{2.4}$$

Afirma-se que $(f^n(x))$ é uma sequência de Cauchy. De fato, dados $m, n \in \mathbb{N}$, com $m \geq n$:

$$d(f^m(x), f^n(x)) \leq \sum_{k=0}^{m-n-1} d(f^{n+k+1}(x), f^{n+k}(x)) \leq \sum_{k=0}^{m-n-1} d(f^{n+k}(f(x)), f^{n+k}(x)).$$

Como a função f é Lipschitz, segue que:

$$d(f^m(x), f^n(x)) \leq \sum_{k=0}^{m-n-1} \lambda^{n+k} \cdot d(f(x), x) = d(f(x), x) \cdot \frac{\lambda^n}{1-\lambda}.$$

Quando $n \to \infty$, para $\lambda^n \to \infty$, a sequência $(f^n(x))$ é de Cauchy, e o limite $\lim_{n\to\infty} f^n(x)$ existe e está em x, pois é fechado. Denotando este limite por x_0, pela desigualdade triangular segue que:

$$\begin{aligned} d(x_0, f(x_0)) &\leq d(x_0, f^n(x_0)) + d(f^n(x_0), f^{n+1}(x)) + d(f^{n+1}(x_0), f(x_0)) \\ &\leq (1+\lambda) \cdot d(x_0, f^n(x)) + \lambda^n \cdot d(x, f(x)). \end{aligned}$$

Analisando quando n tende ao infinito e como $0 < \lambda < 1$, tem-se que:

$$d(x_0, y_0) \leq (1 + \lambda) \cdot 0 + 0 \cdot d(x, f(x)) \Rightarrow d(x_0, f(x_0)) = 0.$$

Logo,

$$f(x_0) = x_0.$$

Agora, será provado a unicidade do ponto fixo x_0.

Considere que exista dois pontos fixos x_0 e y_0, isto é, $f(x_0) = x_0$ e $f(y_0) = y_0$. Vale então que:

$$d(x_0, y_0) = d(f(x_0), f(y_0)).$$

Como a função f é Lipschitz, então:

$$\begin{aligned} d(f(x_0), f(y_0)) &\leq \lambda \cdot d(x_0, y_0) \\ d(x_0, y_0) &\leq \lambda \cdot d(x_0, y_0) \Leftrightarrow d(x_0, y_0) \cdot (1 - \lambda) \leq 0. \end{aligned}$$

Já que $0 < \lambda < 1$, então a desigualdade acima será válida se $d(x_0, y_0) = 0$, logo, $x_0 = y_0$.

Por fim, será provado que $d(f^n(x), x_0) \leq \lambda^n \cdot d(x, x_0), \forall\ x \in X$.

Considere que $d(f^n(x), f^n(y)) = d(f^n(x), f^n(x_0))$, pois y é um ponto qualquer tal que $y = x_0$.

Desta forma, pela Equação 2.4:

$$d(f^n(x), f^n(x_0)) \leq \lambda \cdot d(x, x_0).$$

Mas, como $y = x_0$, então:

$$d(f^n(x), f^n(y)) = d(f^n(x), f^n(x_0)).$$

Note que x_0 é ponto fixo, então $f^n(x_0) = x_0$, seguindo que:

$$d(f^n(x), x_0) \leq \lambda \cdot d(x, x_0).$$

□

Definição 24. *É dito que duas sequências* (x_n) *e* (y_n) *de pontos no* $\mathbb{R}^n$ *convergem exponencialmente uma para a outra se* $d(x_n, y_n) < c \cdot d^n$*, para algum* $c > 0$ *e* $d < 1$*,* $\forall\ n \in \mathbb{N}$*.*

2.2.1.3 O Teste de Derivada

Analogamente ao que foi feito para uma variável, a propriedade de contração pode ser verificada utilizando um teste de derivadas parciais contínuas para várias variáveis.

Seja $f : \mathbb{R}^n \to \mathbb{R}^m$ uma aplicação com derivadas parciais contínuas. Então a cada ponto pode-se definir a derivada ou a diferencial de $f = (f_1, f_2, \cdots, f_m)$ como uma aplicação linear definida pela matriz de derivadas parciais:

$$Df = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \frac{\partial f_2}{\partial x_1} & \frac{\partial f_2}{\partial x_2} & \cdots & \frac{\partial f_2}{\partial x_n} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \frac{\partial f_m}{\partial x_2} & \cdots & \frac{\partial f_m}{\partial x_n} \end{pmatrix}.$$

Define-se a norma de um diferencial como sendo a norma da matriz Df. Em Álgebra Linear, a norma de uma matriz é definida como:

$$\|A\| := max_{v \neq 0}\ \frac{\|A(v)\|}{\|v\|} = max_{\|v\|=1}\ \|A(v)\|.$$

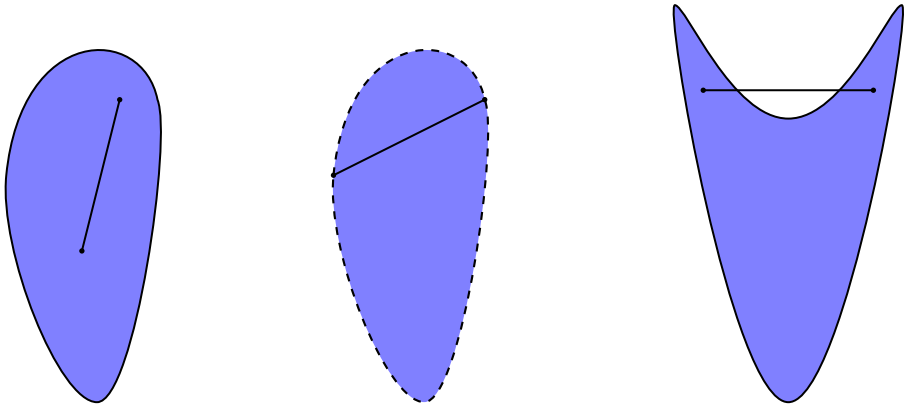
A partir de agora, será explorada uma classificação para conjuntos que desempenhará um papel importante no contexto em que o trabalho se situa: o conceito de convexidade.

2.2.2 Convexidade

Um conjunto convexo no $\mathbb{R}^n$ é um conjunto C, tal que para todo $a, b \in C$, o segmento de reta com pontos finais a, b está contido inteiramente em C. É dito que

um conjunto é estritamente convexo se para quaisquer pontos a, b no fecho de C, o segmento a partir de a até b está contido em C, exceto possivelmente para um ou ambos pontos finais. Geometricamente, observe a Figura 2.5:

Figura 2.5: Conjunto convexo, estritamente convexo e não convexo



Fonte: O próprio autor

Teorema 5. *Se $C \subset \mathbb{R}^n$ é aberto e convexo e $f : C \to \mathbb{R}^m$ é diferenciável com $\|Df(x)\| \leq M$, para todo $x \in C$, então $\|f(x) - f(y)\| \leq M \cdot \|x - y\|$ para $x, y \in C$.*

Demonstração. Considere um segmento de reta que "conecte" x e y, onde $x, y \in C$, dado por:

$$c(t) = x + t \cdot (y - x), \ t \in [0, 1].$$

Ainda, $c(t)$ está contido em C, que por hipótese, C é convexo.

Seja $g(t) := f(c(t))$, isto é, a função g é a aplicação de f em $c(t)$.

Pela Regra da Cadeia, segue que:

$$\begin{aligned} \|g'(t)\| &= \|Df(c(t)) \cdot c'(t)\| \\ &= \|Df(c(t)) \cdot (y - x)\| \\ &\leq M \cdot \|y - x\|. \end{aligned}$$

Note que $c(t) = x \Leftrightarrow t = 0$ e $c(t) = y \Leftrightarrow t = 1$, então:

$$f(x) = g(0) \text{ e } f(y) = g(1).$$

Portanto:

$$\begin{aligned} \|f(x) - f(y)\| &= \|g(0) - g(1)\| \\ &= \|g(1) - g(0)\|. \end{aligned}$$

Pelo Teorema 3:

$$\|g(1) - g(0)\| \leq \|g'(t)\| \cdot (1 - 0).$$

Assim, conclui-se que:

$$\|f(x) - f(y)\| \leq M \cdot \|y - x\|.$$

□

Corolário 1. *Se $C \subset \mathbb{R}^n$ é um conjunto aberto e convexo, e $f : C \to C$ uma aplicação com derivadas parciais contínuas e $\|Df(x)\| \leq \lambda < 1$ em todo ponto $x \in \mathbb{R}^n$, então f é uma λ-contração.*

Teorema 6. *Se $C \subset \mathbb{R}^n$ é um conjunto aberto e estritamente convexo, sendo $\overline{C}$ seu fecho, e $f : \overline{C} \to \mathbb{R}^n$ diferenciável sobre C e contínua sobre $\overline{C}$ com $\|Df(x)\| \leq \lambda < 1$, $\forall\, x \in C$, então f tem um único ponto fixo $x_0 \in \overline{C}$ e $d(f^n(x), x_0) \leq \lambda^n \cdot d(x, x_0),\ \forall\, x \in \overline{C}$.*

Demonstração. Para $x, y \in \overline{C}$, parametriza-se o segmento de reta unindo x e y pelo caminho $c(t) = x + t \cdot (y - x),\ t \in [0, 1]$ e seja $g(t) := f(c(t))$. Então $c((0, 1))$ está contido em C, pois é estritamente convexo.

Pela Regra da Cadeia,

$$\begin{aligned} \|Dg(t)\| &= \|Df(c(t)) \cdot c'(t)\| \\ &= \|Df(c(t)) \cdot (y - x)\| \\ &= \|D(c(t))\| \cdot \|y - x\|. \end{aligned}$$

Por hipótese,

$$\|Dg(t)\| \leq \lambda \|y - x\|.$$

Portanto, segue que:

$$\|f(y) - f(x)\| \leq \lambda \cdot \|y - x\|.$$

Pelo Corolário 1, f é uma contração. Consequentemente, f tem um único ponto fixo e além disso,

$$d(f^n(x), x_0) \leq \lambda^n \cdot d(x, x_0).$$

□

A partir de agora, serão analisados aplicações que não são contrações sobre qualquer domínio, mas sim sobre parte dele.

Proposição 5. *Seja f uma aplicação continuamente diferenciável com um ponto fixo x_0, onde $\|Df(x_0)\| < 1$. Então existe uma vizinhança fechada U de x_0, tal que $f(U) \subset U$ e f é uma contração de U.*

Observação 1. *Se f^{n_0} é uma contração e f é uma função Lipschitz em um espaço métrico (X, d), é sempre possível definir uma nova métrica d' em X, equivalente à métrica original, tal que f seja uma contração.*

Proposição 6. *Seja $f : X \to X$ uma transformação Lipschitz em um espaço métrico (X, d). Suponha que $f^{n_0} : X \to X$ seja uma contração em (X, d) para algum n_0. Então, existe uma métrica d' em X, equivalente à métrica d original, isto é, existem $c_1, c_2 > 0$, tais que:*

$$c_1 \cdot d(x, y) \leq d'(x, y) \leq c_2 \cdot d(x, y). \tag{2.5}$$

Tal que, para todo $x, y \in X$, f é uma contração no espaço métrico (X, d').

Demonstração. Por hipótese, f^{n_0} é uma contração em (X, d), logo existe $\lambda \in (0, 1)$, tal que:

$$d(f^{n_0}(x), f^{n_0}(y)) \leq \lambda \cdot d(x, y). \tag{2.6}$$

Defina

$$\begin{aligned}\tilde{d}(x,y) &= \sum_{i=0}^{n_o-1} \lambda^{\frac{-i}{n_0}} \cdot d(f^i(x), f^i(y)) \\ &= d(x,y) + \lambda^{\frac{-1}{n_0}} \cdot d(f(x), f(y)) + \cdots + \lambda^{\frac{-(n_0-1)}{n_0}} \cdot d(f^{n_0-1}(x), f^{n_0-1}(y)).\end{aligned}$$

Como f é Lipschitz, existe uma constante c, tal que:

$$d(f^i(x), f^i(y)) \leq c^i \cdot d(x, y).$$

Logo,

$$\tilde{d}(x,y) \leq \left[\sum_{i=0}^{\infty} \lambda^{\frac{-i}{n_0}} \cdot c^i\right] \cdot d(x,y).$$

Desta forma, pela Equação 2.6, $\tilde{d}$ é equivalente a d.

Veja agora que $\tilde{d}$ é uma contração. Observe que:

$$\begin{aligned}\tilde{d}(f(x), f(y)) &= \sum_{i=0}^{n_0-1} \lambda^{\frac{-i}{n_0}} \cdot d(f^{i+1}(x), f^{i+1}(y)) \\ &= \lambda^{\frac{1}{n_0}} \left[\sum_{i=0}^{n_0-1} \lambda^{\frac{-(i+1)}{n_0}} \cdot d(f^{i+1}(x), f^{i+1}(y))\right].\end{aligned}$$

Tomando $i + 1 = j$:

$$\begin{aligned}\tilde{d}(f(x), f(y)) &= \lambda^{\frac{1}{n_0}} \left[\sum_{j=1}^{n_0} \lambda^{\frac{-j}{n_0}} \cdot d(f^j(x), f^j(y))\right] \\ &= \lambda^{\frac{1}{n_0}} \left[\sum_{j=1}^{n_0-1} \lambda^{\frac{-j}{n_0}} \cdot d(f^j(x), f^j(y)) + \lambda^{-1} \cdot d(f^{n_0}(x), f^{n_0}(y))\right].\end{aligned}$$

Pela Equação 2.6, tem-se:

$$\begin{aligned}
\tilde{d}(f(x), f(y)) &\leq \lambda^{\frac{1}{n_0}} \left[\sum_{j=1}^{n_0-1} \lambda^{\frac{-j}{n_0}} \cdot d(f^j(x), f^j(y)) + \lambda^{-1} \cdot \lambda \cdot d(x, y) \right] \\
&\leq \lambda^{\frac{1}{n_0}} \left[\sum_{j=1}^{n_0-1} \lambda^{\frac{-j}{n_0}} \cdot d(f^j(x), f^j(y)) + d(x, y) \right] \\
&= \lambda^{\frac{1}{n_0}} [d(x, y) + \lambda^{\frac{-1}{n_0}} \cdot d(f(x), f(y)) + \cdots + \lambda^{\frac{-n_0-1}{n_0}} \cdot d(f^{n_0-1}(x), f^{n_0-1}(y))] \\
&= \lambda^{\frac{1}{n_0}} \cdot [\tilde{d}(x, y)].
\end{aligned}$$

Portanto, segue que:

$$\tilde{d}(f(x), f(y)) \leq \lambda^{\frac{1}{n_0}} \cdot \tilde{d}(x, y).$$

Como $\lambda^{\frac{1}{n_0}} \in (0, 1)$, consequentemente f é uma contração no espaço $(X, \tilde{d})$.

□

2.3 Elementos de Teoria dos Números

A Teoria dos Números estuda, em sua essência, as propriedades e características dos números inteiros, tema que se torna profundo e mais abstrato conforme se avança. Essa teoria tem suas raízes bem fundamentadas com os matemáticos gregos, incluindo grandes nomes como *Euclides de Alexandria* e *Diofanto de Alexandria*, este último conhecido por sua obra intitulada *"Arithmetica"*. Em um contexto mais moderno, destacam-se *Pierre de Fermat* (1607 - 1665), com suas valiosas anotações e o famoso *"Último Teorema de Fermat"*, *Leonhard Paul Euler* (1707 - 1783), que contribuiu grandemente para a teoria, deixando um legado como o *"Teorema de Euler"*, e *Carl Friedrich Gauss* (1777 - 1855), cuja célebre obra é intitulada *"Disquisitiones Arithmeticae"*. Neste trabalho, será apresentada uma breve introdução e os fundamentos necessários para o objetivo proposto, com base em Santos (2018).

2.3.1 Divisibilidade

Serão apresentadas algumas proposições e definições do conceito de divisibilidade com o objetivo de fundamentação. Entretanto, como são resultados elementares, suas demonstrações serão omitidas, o leitor pode consultá-las em Santos (2018).

Definição 25. *Considere $a, b \in \mathbb{Z}$, é dito que a divide b, denotado por $a \mid b$, se existir um inteiro c tal que $b = ac$. Se a não divide b, então denota-se por $a \nmid b$.*

Proposição 7. *Considere $a, b, c \in \mathbb{Z}$, se $a \mid b$ e $b \mid c$, então $a \mid c$.*

Exemplo 16. *Note que $3 \mid 12$ e $12 \mid 48$, logo $3 \mid 48$, e como não existe um inteiro c que satisfaz $15 = 4c$, então $4 \nmid 15$.*

Proposição 8. *Se $a, b, c, m, n \in \mathbb{Z}$, se $c \mid a$ e $c \mid b$, então $c \mid (ma + nb)$.*

Exemplo 17. *Note que $3 \mid 15$ e $3 \mid 42$, logo $3 \mid (8 \times 15 - 7 \times 42)$.*

Para demonstrar o resultado a seguir, é necessário enunciar o *Princípio de Eudoxius*, que segue: Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, então a é um múltiplo de b ou se encontra entre dois múltiplos consecutivos de b, isto é, correspondendo a cada par de inteiros a e $b \neq 0$ existe um inteiro q tal que, para $b > 0$, segue que, para b>0:

$$qb \leq a < (q + 1)b$$

e para b < 0:

$$qb \leq a < (q - 1)b.$$

Proposição 9. *Dados dois inteiros a e b, $b > 0$, existe um único par de inteiros q e r tais que:*

$$a = qb + r, \ \textit{com } 0 \leq r < b, \ (r = 0 \Leftrightarrow b \mid a).$$

onde q é dito quociente e r resto da divisão do inteiro a pelo inteiro b.

Demonstração. Pelo *Princípio de Eudoxius*, como $b > 0$, existe um q satisfazendo:

$$qb \leq a < (q+1)b,$$

o que implica que $0 \leq a - qb$ e $a - qb < b$. Definindo $r = a - qb$, note que é garantido a existência de q e r.

Com o objetivo de demonstrar a unicidade, suponha a existência de um par q_1 e r_1 satisfazendo:

$$a = q_1 b + r_1 \text{ com } 0 \leq r_1 < b,$$

que segue que $(qb+r)-(q_1b+r_1) = 0 \Rightarrow b(q-q_1) = r_1 - r$, o que implica que $b \mid (r_1 - r)$.

Mas, como $r_1 < b$ e $r < b$, tem-se que $|r_1 - r| < b$ e, portanto, como $b \mid (r_1 - r)$, deve ter $r_1 - r = 0$, que segue que $r = r_1$. Desta forma, $q_1 b = qb \Rightarrow q_1 = q$, uma vez que $b \neq 0$.

□

2.3.2 Congruência

Definição 26. *Seja a e b dois número inteiros. É dito que a é congruente a b módulo m, $m > 0$, se m divide $(a - b)$. Denota-se $a \equiv b \ mod \ m$. Se m não divide $(a - b)$, é dito que a é incongruente a b módulo m, isto é, $a \not\equiv b \ mod \ m$.*

Exemplo 18. *Note que 11 é congruente a 3 módulo 2, pois 2 divide $(11 - 3)$, em notação matemática:*

$$11 \equiv 3 \ mod \ 2 \Leftrightarrow 2 \mid (11 - 3).$$

Como 5 não divide 6 e $17 - 11 = 6$, segue que 17 é incongruente a 11 módulo 5, em notação matemática:

$$17 \not\equiv 11 \ mod \ 5 \Leftrightarrow 5 \nmid (17 - 11).$$

Proposição 10. *Sejam a, b números inteiros, então $a \equiv b \ mod \ m$ se, e somente se, existir um inteiro k, tal que $a = b + km$.*

É interessante para o estudo dominar os cálculos relacionados à congruência definida no conjunto dos números inteiros. Para isso, são necessários alguns resultados.

Proposição 11. *Sejam a, b, m, d números inteiros, com $m > 0$. As seguintes sentenças são verdadeiras:*

i. $a \equiv a \ mod \ m$, *(Propriedade Reflexiva);*

ii. *Se* $a \equiv b \ mod \ m$, *então* $b \equiv a \ mod \ m$, *(Propriedade Simétrica);*

iii. *Se* $a \equiv b \ mod \ m$ *e* $b \equiv d \ mod \ m$, *então* $a \equiv d \ mod \ m$, *(Propriedade Transitiva).*

Observação 2. *Note que podemos concluir pela Proposição 11 que a relação de congruência entre inteiros é uma relação de equivalência, pois satisfaz as propriedades reflexiva, simétrica e transitiva.*

Proposição 12. *Sejam a, b, c, m números inteiros, tais que $a \equiv b \ mod \ m$, então valem as sentenças abaixo:*

i. $a + c \equiv b + c \ mod \ m$;

ii. $a - c \equiv b - c \ mod \ m$;

iii. $ac \equiv bc \ mod \ m$.

Proposição 13. *Sejam a, b, c, d, m números inteiros tais que $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, então valem as sentenças abaixo:*

i. $a + c \equiv b + d \ mod \ m$;

ii. $a - c \equiv b - d \ mod \ m$;

iii. $ac \equiv bd \ mod \ m$.

Definição 27. *O conjuntos dos inteiros $\{r_1, r_2, \cdots, r_s\}$ é um sistema completo de resíduos módulo m se:*

i. $r_i \not\equiv r_j \ mod \ m$ *para* $i \neq j$;

ii. Para todo inteiro n, existe um r_i tal que $n \equiv r_i \ mod \ m$.

Pode-se interpretar um sistema completo de resíduos módulo m como o conjunto de números inteiros cujos restos pela divisão por m são os números $0, 1, \cdots, m-1$ sem repetições.

Exemplo 19. *O conjunto $\{0, 1, 2, 3, 4, 5, 6, 7\}$ é um sistema completo de resíduos módulo 8.*

Exemplo 20. *Considerando m um inteiro ímpar, o conjunto abaixo é um sistema completo de resíduos módulo m.*

$$\left\{-\frac{(m-1)}{2}, -\frac{(m-3)}{2}, \cdots, -1, 0, 1, \cdots, \frac{(m-3)}{2}, \frac{(m-1)}{2}\right\}.$$

Proposição 14. *Se k inteiros $r_1, r_2, r_3, \cdots, r_k$ formam um sistema completo de resíduos módulo m, então $k = m$.*

Proposição 15. *Se a, b, k, m são inteiros com $k > 0$, e $a \equiv b \ mod \ m$, então $a^k \equiv b^k \ mod \ m$.*

Exemplo 21. *Mostremos que o conjunto definido por $\{1^2, 2^2, 3^2, \cdots, m^2\}$, $m > 2$, não forma um sistema completo de resíduos módulo m.*

Solução. Para verificar tal afirmação, basta mostrar que o conjunto de números não são, dois a dois, incongruentes módulo m.

Para isto, tome dois números inteiros n e k, tais que $n > k$ e $n + k = m$, logo:

$$n^2 - k^2 = (n+k)(n-k) = m(n-k) \equiv 0 \ mod \ m,$$

levando que $n^2 \equiv k^2 \ mod \ m$.

Definição 28. *Seja n um inteiro positivo, define-se a função de Euler, denotada por $\phi(n)$ como sendo o número de inteiros positivos menores ou iguais a n que são coprimos com n, isto é, sendo $a \in \phi(n)$, $mdc(a, n) = 1$.*

Definição 29. *Um sistema reduzido de resíduos módulo m é um conjunto de $\phi(m)$ inteiros $r_1, r_2, \cdots, r_{\phi(m)}$, tais que cada elemento do conjunto é coprimo com m, e se $i \neq j$, então $r_i \not\equiv r_j \ mod\ m$.*

Exemplo 22. *Considere o conjunto de inteiros $G = \{0, 1, 2, 3, 4, 5, 6, 7\}$, o mesmo é um sistema completo de resíduos módulo 8, porém, um subconjunto de G, dado por $H = \{1, 3, 5, 7\}$ é um sistema reduzido de resíduos módulo 8, isto é, para se obter um sistema reduzido de resíduos módulo m, basta retirar os elementos do sistema completo de resíduos que não são coprimos com m.*

Proposição 16. *Seja a um número inteiro positivo tal que $mdc(a, m) = 1$. Se $r_1, r_2, \cdots, r_{\phi(m)}$ é um sistema reduzido de resíduos módulo m, então $ar_1, ar_2, \cdots, ar_{\phi(m)}$ é, também, um sistema reduzido de resíduos módulo m.*

Teorema 7. *(Teorema de Euler) Seja m um inteiro positivo e a um inteiro, tal que $mdc(a, m) = 1$, logo:*

$$a^{\phi(m)} \equiv 1 \ mod\ m.$$

Demonstração. Pela Proposição 16, sabe-se que os elementos $ar_1, ar_2, \cdots, ar_{\phi(m)}$ constituem um sistema reduzido de resíduos módulo m, ou seja, cada elemento ar_i é congruente módulo m a exatamente um dos elementos $r_j \leq j \leq \phi(m)$, portanto, o produto dos elementos ar_i deve ser congruente módulo m ao produto dos r_j, isto é:

$$ar_1 \cdot ar_2 \cdots ar_{\phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\phi(m)} \ mod\ m,$$

que segue:

$$a^{\phi(m)} r_1 \cdot r_2 \cdots r_{\phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\phi(m)} \ mod\ m.$$

Note que:

$$mdc\left(\prod_{i=1}^{\phi(m)} r_i, m\right) = 1,$$

podendo então cancelar $\prod_{i=1}^{\phi(m)} r_i$ de ambos os lados para se obter $a^{\phi(m)} \equiv 1 \ mod\ m$.

□

Exemplo 23. *Considere $m = 8$ e $a = 5$. Pelos exemplos anteriores, foi visto que o conjunto $g = \{1, 3, 5, 7\}$ forma um sistema reduzido de resíduos módulo 8, desta forma, pelo Teorema 16, o conjunto $h = \{5 \cdot 1, 5 \cdot 3, 5 \cdot 5, 5 \cdot 7\}$ forma também um sistema reduzido de resíduos módulo 8, ou seja, cada elemento do conjunto h é congruente módulo 8 a exatamente um dos elementos do conjunto g. Isto é:*

$$\begin{aligned} 5 \cdot 1 &\equiv 5 \ mod\ 8 \\ 5 \cdot 3 &\equiv 7 \ mod\ 8 \\ 5 \cdot 5 &\equiv 1 \ mod\ 8 \\ 5 \cdot 7 &\equiv 3 \ mod\ 8 \end{aligned}$$

Ao multiplicar membro a membro cada uma das congruências acima, obtêm-se:

$$5^4(1 \cdot 3 \cdot 5 \cdot 7) \equiv (1 \cdot 3 \cdot 5 \cdot 7) \ mod\ 8.$$

Podendo então cancelar o fator $(1 \cdot 3 \cdot 5 \cdot 7)$, pois $mdc(1 \cdot 3 \cdot 5 \cdot 7, 8) = 1$, de modo que resta:

$$5^4 \equiv 1 \ mod\ 8.$$

Note que, $4 = \phi(8)$, então $5^{\phi(8)} \equiv 1 \ mod\ 8$.

2.4 Elementos de Álgebra

A teoria algébrica remonta a 1900 a.C com os Babilônios, que deixaram resultados relevantes em várias áreas da Álgebra. Essa trajetória prosseguiu com os matemáticos gregos e recebeu imensas contribuições dos Árabes.

Os matemáticos italianos, como *Niccolò Fontana Tartaglia* (1500 - 1557), também deixaram suas contribuições na Álgebra. Ao seguir o percurso pelos nomes de grandes

matemáticos, destacam-se *René Descartes* (1596 - 1650), *Leonhard Euler* (1707 - 1783), *Joseph Louis Lagrange* (1736 - 1813), *Niels Henrik Abel* (1802 - 1829) e *Évariste Galois* (1811 - 1832). Este último, apesar de ter falecido jovem, deixou um grande legado matemático com a Teoria de Grupos e o *Teorema Fundamental de Galois*. Conforme Gonçalves (2017), serão apresentados alguns resultados elementares sobre a Teoria de Grupos, os quais serão fundamentais para a base deste trabalho.

2.4.1 Grupos

Definição 30. *Seja G um conjunto não vazio, onde está definida uma operação $*$ entre pares de G, denotada por:*

$$\begin{aligned} * \ : \ & G \times G \to G \\ & (x, y) \mapsto x * y \end{aligned}$$

O par $(G, *)$ é chamado de grupo se são válidas as seguintes propriedades:

1. *Propriedade associativa, $a * (b * c) = (a * b) * c$, $\forall\ a, b, c \in G$;*
2. *Elemento identidade, $\exists e \in G$, tal que $a * e = e * a$, $\forall\ a \in G$;*
3. *Elemento inverso, $\forall\ a \in G$, $\exists b \in G$, tal que $a * b = b * a = e$.*

Se um grupo $(G, *)$ verifica-se a seguinte propriedade:

$$a * b = b * a,\ \forall\ a, b \in G,$$

é dito que $(G, *)$ é um **grupo abeliano**, em menção ao matemático Norueguês Niels Henrik Abel (1802 - 1829).

Exemplo 24. *Note que o conjunto dos números inteiros $\mathbb{Z}$ é um grupo aditivo infinito.*

Exemplo 25. *Considere G o conjunto de retas no plano $\mathbb{R}^2$ com coeficiente angular não nulo, ou seja:*

$$G = \{f : \mathbb{R} \to \mathbb{R} : f(x) = ax + b, 0 \neq a, b \in R\}.$$

Note que se $f(x) = ax + b$, $a \neq 0$ *e* $g(x) = cx + d$, $c \neq 0$, *então:*

$$(g \circ f)(x) = g(f(x)) = acx + (bc + d),\ ac \neq 0.$$

Logo, a composição de funções $\circ$ *define uma operação no conjunto* G *que é associativa.*

Agora, observe que:

$$\begin{aligned} e &= I_{\mathbb{R}} : \mathbb{R} \to \mathbb{R} \\ & \quad x \mapsto y. \end{aligned}$$

é um elemento de G *e mais se,*

$$f^{-1}(x) = \frac{1}{a}x - \frac{b}{a},\ a \neq 0,$$

Assim,

$$f^{-1} \circ f = f \circ f^{-1} = I_{\mathbb{R}},\ \textit{onde}\ f(x) = ax + b,\ a \neq 0.$$

Logo, $(G, \circ)$ *é um grupo onde* $\circ$ *é a operação de composição entre funções.*
Se $f(x) = 2x + 4$ *e* $g(x) = 3x + 2$, *segue que:*

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) = g(2x + 4) = 6x + 14 \\ (f \circ g)(x) &= f(3x + 2) = 6x + 8. \end{aligned}$$

Perceba que o grupo $(G, \circ)$ *é um exemplo de grupo não abeliano contendo um número infinito de elementos.*

Capítulo

3

Criptografia

Com a influência do mundo globalizado e tecnológico, tornou-se possível realizar ações que anteriormente demandavam muito tempo e dinheiro. Por exemplo, uma importante reunião corporativa sobre estratégias de aumento de vendas de uma empresa multinacional, na qual os diretores residem em países diferentes, hoje em dia pode ser realizada com apenas um clique. O comércio digital proporciona o conforto de adquirir um item desejado diretamente do seu lar. No entanto, surge a questão: o que garante que tais ações sejam tão seguras contra interceptadores quanto a confidencialidade de um escritório particular ou uma transação presencial que não envolve a troca de dados entre o comprador e o vendedor?

Para explorar as facilidades que a tecnologia oferece, é necessário utilizar uma ferramenta que garanta a segurança e os princípios básicos de transmissão de dados. Nesse contexto, a criptografia se mostra como um grande aliado ao permitir o consumo de produtos digitais com segurança e eficiência. A criptografia é uma área que tem como um de seus objetivos modificar mensagens ou informações de modo a torná-las indecifráveis para pessoas indesejadas, garantindo assim que dados como informações de cartão de crédito do comprador ou estratégias confidenciais de uma empresa não sejam interceptados por pessoas mal-intencionadas.

Neste capítulo será explorado o fascinante campo da criptografia, abordando suas diversas ramificações com base em Coutinho (2015), Pellegrini (2019), Andria;

R. Gondim; R. Salomão (2019), Stinson; M. B. Paterson (2019), Reis (1989) e Silva (2019).

3.1 Princípios básicos de criptografia

A criptografia é um mecanismo de segurança de dados que estuda técnicas de transmissão e armazenamento seguros de informações, mesmo na presença de usuários indesejadas. É uma conceito utilizado para tornar dados ininteligíveis para usuários não autorizadas. Conforme Andria; R. Gondim; R. Salomão (2019), existem alguns termos criptográficos frequentemente utilizados, os quais serão empregados ao longo do texto.

1. **Texto plano ou simples, do inglês *plain text*:** Consiste em um conjunto de informações que ainda não passaram por nenhum tipo de criptografia, ou seja, o texto original;

2. **Encriptação:** É o processo de codificação de um texto plano;

3. **Texto cifrado ou encriptado:** Consiste em um conjunto de informações que foi criptografado, codificado, ou seja, o texto que passou pelo processo de criptografia;

4. **Decriptação:** É o processo de decodificação de um texto cifrado;

5. **Chave de codificação, do inglês *key*:** São elementos de informação ou algoritmos que compõem o processo de encriptação;

6. **Atacante, invasor ou ameaça:** É um usuário ou uma inteligência artificial não autorizada que tem o objetivo de acessar ou recuperar informações, quebrando a criptografia.

Formalmente, define-se um criptossistema por:

Definição 31. *Um criptossistema é uma quintupla* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$*, onde as condições abaixo são satisfeitas:*

(i.) $\mathcal{P}$ *é o conjunto finito de possíveis textos planos;*

(ii.) $\mathcal{C}$ *é o conjunto finito de possíveis textos cifrados;*

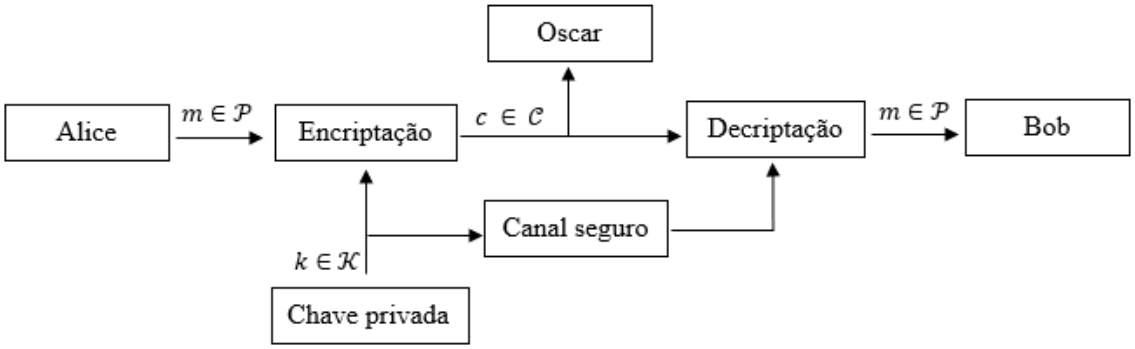
(iii.) $\mathcal{K}$ *é o espaço de chaves, um conjunto finito ou infinito de possíveis chaves;*

(iv.) Para cada $k \in \mathcal{K}$*, existe uma regra de encriptação* $crip_k \in \mathcal{E}$ *e uma regra de decriptação* $decrip_k \in \mathcal{D}$ *correspondente, onde para cada* $crip_k : \mathcal{P} \to \mathcal{C}$ *e* $decrip_k : \mathcal{C} \to \mathcal{P}$ *são funções tal que* $decrip_k(crip_k(m)) = m$ *para cada elemento do texto plano* $m \in \mathcal{P}$*.*

No item (*iv.*) tem-se que se um texto plano m é encriptado utilizando $crip_k$, então o texto cifrado obtido é decriptado com $decrip_k$, tendo como resultado o texto plano original m.

Para ilustrar ao leitor, considere que Alice e Bob desejam se comunicar em sigilo e Oscar é uma ameaça que não tem informações sobre as chaves privadas. O diagrama de um criptossistema é apresentado na Figura 3.1:

Figura 3.1: Diagrama de um criptossistema



Fonte: O próprio autor

3.1.1 Processo de pré-codificação

Suponha que dois indivíduos desejem se comunicar de forma sigilosa. As mensagens em texto plano são representadas por letras do alfabeto. Portanto, o processo de encriptação começa com a transformação do texto em dados numéricos, uma vez que os computadores compreendem e processam apenas código binário. Nesse sentido, é necessária a etapa de pré-codificação. Para isso, é utilizado um modelo de pré-codificação, como a tabela ASCII (American Standard Code for Information Interchange), que é amplamente empregada.

A Tabela ASCII é um sistema de representação que inclui letras, algarismos, sinais de pontuação, sinais matemáticos e sinais de controle. Conforme Andria; R. Gondim; R. Salomão (2019), a tabela é composta por um código binário de 7 bits, o qual codifica um conjunto de 128 caracteres. Essa tabela é representada em numeração de base binária, base decimal e hexadecimal. Para fins deste estudo, é mais conveniente trabalhar apenas com a base decimal, devido à maior facilidade de cálculo.

Exemplo 26. *Considere a pré-codificação do texto plano "UNESP" utilizando a Tabela ASCII disposta na Figura 3.2.*

Figura 3.2: Tabela ASCII

Binário	Decimal	Hexa	Glifo
0010 0000	32	20	
0010 0001	33	21	!
0010 0010	34	22	"
0010 0011	35	23	#
0010 0100	36	24	$
0010 0101	37	25	%
0010 0110	38	26	&
0010 0111	39	27	'
0010 1000	40	28	(
0010 1001	41	29	)
0010 1010	42	2A	*
0010 1011	43	2B	+
0010 1100	44	2C	,
0010 1101	45	2D	-
0010 1110	46	2E	.
0010 1111	47	2F	/
0011 0000	48	30	0
0011 0001	49	31	1
0011 0010	50	32	2
0011 0011	51	33	3
0011 0100	52	34	4
0011 0101	53	35	5
0011 0110	54	36	6
0011 0111	55	37	7
0011 1000	56	38	8
0011 1001	57	39	9
0011 1010	58	3A	:
0011 1011	59	3B	;
0011 1100	60	3C	<
0011 1101	61	3D	=
0011 1110	62	3E	>
0011 1111	63	3F	?

Binário	Decimal	Hexa	Glifo
0100 0000	64	40	@
0100 0001	65	41	A
0100 0010	66	42	B
0100 0011	67	43	C
0100 0100	68	44	D
0100 0101	69	45	E
0100 0110	70	46	F
0100 0111	71	47	G
0100 1000	72	48	H
0100 1001	73	49	I
0100 1010	74	4A	J
0100 1011	75	4B	K
0100 1100	76	4C	L
0100 1101	77	4D	M
0100 1110	78	4E	N
0100 1111	79	4F	O
0101 0000	80	50	P
0101 0001	81	51	Q
0101 0010	82	52	R
0101 0011	83	53	S
0101 0100	84	54	T
0101 0101	85	55	U
0101 0110	86	56	V
0101 0111	87	57	W
0101 1000	88	58	X
0101 1001	89	59	Y
0101 1010	90	5A	Z
0101 1011	91	5B	[
0101 1100	92	5C	\
0101 1101	93	5D	]
0101 1110	94	5E	^
0101 1111	95	5F	_

Binário	Decimal	Hexa	Glifo
0110 0000	96	60	`
0110 0001	97	61	a
0110 0010	98	62	b
0110 0011	99	63	c
0110 0100	100	64	d
0110 0101	101	65	e
0110 0110	102	66	f
0110 0111	103	67	g
0110 1000	104	68	h
0110 1001	105	69	i
0110 1010	106	6A	j
0110 1011	107	6B	k
0110 1100	108	6C	l
0110 1101	109	6D	m
0110 1110	110	6E	n
0110 1111	111	6F	o
0111 0000	112	70	p
0111 0001	113	71	q
0111 0010	114	72	r
0111 0011	115	73	s
0111 0100	116	74	t
0111 0101	117	75	u
0111 0110	118	76	v
0111 0111	119	77	w
0111 1000	120	78	x
0111 1001	121	79	y
0111 1010	122	7A	z
0111 1011	123	7B	{
0111 1100	124	7C	|
0111 1101	125	7D	}
0111 1110	126	7E	~

Fonte: Retirado de Andria; R. Gondim; R. Salomão (2019)

Obtêm-se então:

Texto plano: UNESP

Texto pré-codificado: 85 78 69 83 80

3.2 Criptografia simétrica

Um dos métodos mais simples para criptografar mensagens é a cifra de César. Essa cifra consiste na substituição de cada letra do alfabeto no texto original por uma letra correspondente em outra posição do alfabeto. Por exemplo, ao substituir cada letra pelo seu sucessor imediato no alfabeto, a palavra "CRIPTOGRAFIA" seria criptografada da seguinte forma:

DSJQUPHSBGJB

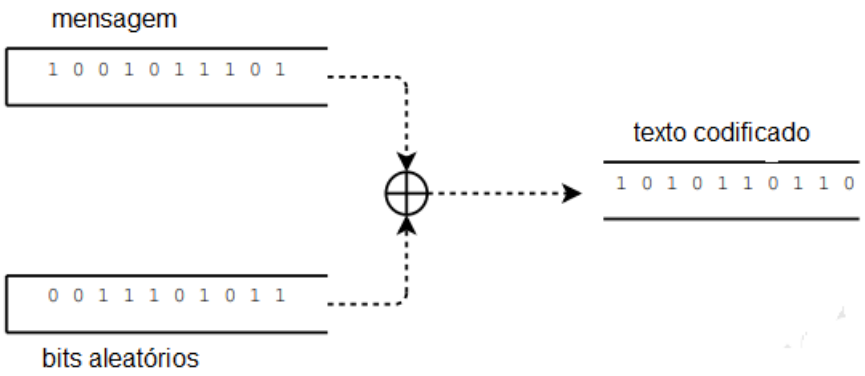
Para decifrar essa mensagem, o destinatário precisa conhecer o segredo, ou seja, a chave de decodificação. Sistemas criptográficos nos quais é necessário conhecer a chave para decifrá-los são chamados de *criptossistemas simétricos*. Nesses sistemas, a chave é comumente referida como chave secreta ou chave privada.

Os criptossistemas simétricos possuem duas funções com dois parâmetros. A função $crip(m, k)$ é utilizada para criptografar a mensagem, enquanto a função $decrip(m, k)$ é responsável pela decodificação da mensagem. Nesse caso, os parâmetros $m \in \mathcal{P}$ e $k \in \mathcal{K}$ representam a mensagem e a chave, respectivamente. É importante ressaltar que:

$$decrip(crip(m, k), k) = m.$$

De forma mais formal, de acordo com Pellegrini (2019), o código mencionado anteriormente, usado para cifrar mensagens, é conhecido como *cifras de fluxo*. Essas cifras transformam cada bit da mensagem desejada em um bit de um texto codificado, substituindo-o por um bit gerado por um processo pseudoaleatório, geralmente realizado por uma operação de *disjunção exclusiva* (XOR), como ilustrado na Figura 3.3. O padrão desse gerador é a chave privada que permite a criptografia e a decodificação das mensagens. Em uma cifra de fluxo, as funções $decrip(m, k)$ e $crip(m, k)$ são idênticas, ou seja, os participantes da comunicação compartilham a mesma chave privada.

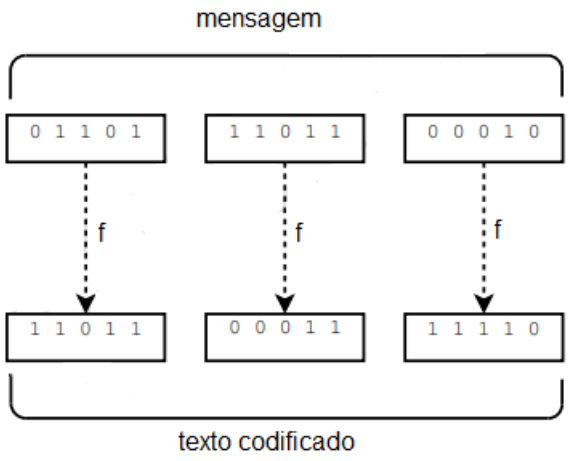
Figura 3.3: Cifra de fluxo



Fonte: Retirado de Pellegrini (2019).

É possível classificar as funções $crip(m, k)$ e $decrip(m, k)$ como *cifras de bloco*, que operam em blocos de bits de tamanho fixo. Nessas cifras, são realizadas transformações nos blocos de forma que se tornem difíceis de reverter ou decodificar. Uma representação visual desse processo pode ser observada na Figura 3.4.

Figura 3.4: Cifra de bloco

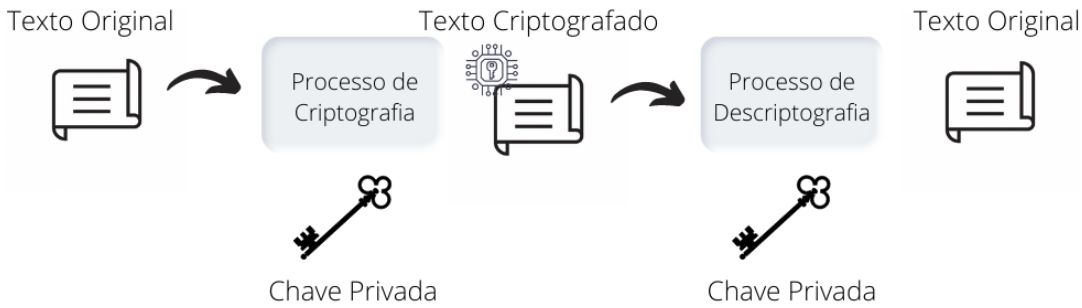


Fonte: Retirado de Pellegrini (2019)

A função f, também conhecida como função de criptografia, possui dois parâmetros: m para a mensagem e k para a chave privada. Dessa forma, $f(m, k)$ representa o processo de criptografia da mensagem, enquanto $f^{-1}(m, k)$ realiza a decodificação. É importante ressaltar que a função inversa f^{-1} deve ser difícil de calcular sem possuir a chave privada k.

Para facilitar a compreensão do leitor, a Figura 3.5 apresenta um modelo simétrico de um criptossistema.

Figura 3.5: Modelo de Criptografia Simétrica



Fonte: O próprio autor.

Um exemplo de criptografia simétrica é a *cifra de Vigenère*. Esse método consiste em uma sequência de cifras de César, onde o primeiro alfabeto é cifrado deslocando uma posição em relação ao alfabeto original, o segundo alfabeto desloca-se duas posições e assim por diante, como ilustrado na Figura 3.6. Além disso, é utilizada uma frase de transição como chave de codificação, na qual cada letra da chave indica a substituição a ser aplicada.

Figura 3.6: Tabela de Vigenère

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
01	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
02	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
03	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
04	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
05	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
06	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
07	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
08	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
09	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Fonte: Biblioteca de imagens do Google.

Para codificar uma mensagem utilizando a cifra de Vigenère, é necessário que ambos os envolvidos na transmissão da mensagem tenham conhecimento da chave de codificação. É importante observar que a chave deve ter o mesmo tamanho que o texto a ser codificado. Veja um exemplo em que a palavra "UNESP" será cifrada utilizando a palavra "CIFRA" como chave de codificação.

Para cifrar a primeira letra "U", é necessário identificar a primeira letra da chave de codificação, que é a letra "C" na Tabela de Vigenère. Para isso, procuramos a linha iniciada pela letra "C" e verificamos qual coluna, encabeçada pela letra "U", cruza com essa linha. Nesse caso, a letra cifrada correspondente é "W". Esse processo é repetido para o restante da palavra. Portanto, o processo de codificação é o seguinte:

Chave de codificação: CIFRA

Mensagem original: UNESP

Mensagem codificada: WVJJP

Dessa forma, utilizando a palavra "CIFRA" como chave de codificação, a palavra "UNESP" seria codificada como "WVJJP".

3.2.1 Sigilo perfeito

Um sistema de criptografia é considerado ter sigilo perfeito quando, mesmo que interceptadores obtenham acesso ao texto criptografado e tenham conhecimento dele, esse texto não fornece nenhuma informação sobre a mensagem original. Ou seja, se um intruso deseja obter a mensagem em texto claro, ter acesso ao texto criptografado não deve aumentar sua probabilidade de sucesso em obter a mensagem original. Formalmente, isso pode ser definido da seguinte forma:

Definição 32. *Seja $\mathcal{M}$ o espaço das mensagens, $\mathcal{C}$ o espaço dos textos criptografados e $\mathcal{K}$ o espaço das chaves. Um criptossistema tem sigilo perfeito se para todo $m \in \mathcal{M}$ e $c \in \mathcal{C}$, $Prob(m|c) = Prob(m)$, isto é, a probabilidade de m ocorrer dado que c ocorra é igual a probabilidade de m ocorrer.*

Teorema 8. *(Teorema de Bayes) Seja $\{A_1, A_2, \cdots, A_n\}$ uma partição do espaço amostral ω com $Prob(A_i) > 0$ para todo i, onde $1 \leq i \leq n$. Então, para todo evento B, com $Prob(B) > 0$ e para todo $1 \leq j \leq n$, tem-se que:*

$$Prob(A_j|B) = \frac{Prob(B|A_j)Prob(A_j)}{\sum_{i=1}^{n} Prob(B|A_i)Prob(A_i)}.$$

A demonstração do Teorema 8 pode ser encontrada e analisada em Ross (2010).

Enunciado o Teorema de Bayes, é possível prosseguir para um Lema equivalente a Definição 32, tal resultado segue abaixo:

Lema 1. *Um sistema de criptografia possui sigilo perfeito se e somente se, para todo* $m \in \mathcal{M}$ *e* $c \in \mathcal{C}$, $Prob(c|m) = Prob(c)$

Demonstração. Considere uma mensagem m qualquer e um texto criptografado c. Por hipótese:

$$Prob(c|m) = Prob(c)$$

Multiplicando por $\frac{Prob(m)}{Prob(c)}$, de modo que $Prob(c) \neq 0$:

$$\frac{Prob(c|m) \cdot Prob(m)}{Prob(c)} = Prob(m).$$

Pelo Teorema de Bayes, segue que:

$$Prob(m|c) = \frac{Prob(c|m) \cdot Prob(m)}{Prob(c)}$$

Desta forma:

$$Prob(m|c) = Prob(m).$$

□

O teorema a seguir demonstra uma limitação dos criptossistemas de sigilo perfeito: a quantidade de chaves deve ser igual à quantidade de mensagens possíveis. Portanto, quanto maior for a mensagem que os envolvidos desejam transmitir, maior deverá ser a chave privada correspondente.

Teorema 9. *Se um criptossistema tem sigilo perfeito, então* $|\mathcal{K}| \geq |\mathcal{M}|$.

Demonstração. Suponha por absurdo que $|\mathcal{K}| < |\mathcal{M}|$, considere distribuição uniforme sobre $\mathcal{M}$. Seja $c \in \mathcal{C}$ de modo que $Prob(c) > 0$, considere também $\mathcal{M}(\mathrm{c})$ definido de tal forma:

$$\mathcal{M}(\mathrm{c}) = \{\mathrm{m} \mid \mathrm{m} = \mathrm{Decrip_k(c)} \text{ para algum k} \in \mathcal{K}\}.$$

É bem sabido que para cada $m \in \mathcal{M}$, existe pelo menos um $k \in \mathcal{K}$ que satisfaça a condição de que $Decrip_k(c) = m$, desta forma, note que:

$$|\mathcal{M}(\mathrm{c})| \leq |\mathcal{K}|.$$

Mas, foi suposto que $|\mathcal{K}| < |\mathcal{M}|$, que segue que:

$$|\mathcal{M}(\mathrm{c})| \leq |\mathcal{K}| < |\mathcal{M}|.$$

Como $|\mathcal{M}(\mathrm{c})| < |\mathcal{M}|$, existe algum $m' \in \mathcal{M}$ tal que $m' \notin \mathcal{M}(\mathrm{c})$, logo:

$$Prob(m'|c) = 0$$

Como a distribuição sobre $\mathcal{M}$ é uniforme, então:

$$Prob(m'|c) = 0 \neq Prob(m') = \frac{1}{|\mathcal{M}|}.$$

Conclui-se, portanto, que um criptossistema em que $|\mathcal{K}| < |\mathcal{M}|$ não possui sigilo perfeito. Ou seja, é necessário que o espaço de chaves seja maior ou igual ao espaço de mensagens.

Observação 3. *Note que para criptossistemas simétricos, é possível que haja sigilo perfeito, o que implica em problemas com relação a tamanho e quantidade das chaves privadas $k \in \mathcal{K}$ que são necessárias para criptografar uma determinada mensagem $m \in \mathcal{M}$.*

3.3 Criptografia Assimétrica

Um dos principais desafios da criptografia simétrica é o uso de uma única chave privada para ambos os participantes da comunicação, o que torna o processo difícil quando os envolvidos estão distantes. Isso ocorre porque é necessário transmitir a chave privada em um canal seguro, o que pode ser comprometido por usuários não autorizados durante a transmissão da mensagem. Para solucionar esse problema, foram desenvolvidos os criptossistemas assimétricos, que permitem que o remetente e o destinatário se comuniquem de forma segura.

Para ilustrar de forma simples o funcionamento de um criptossistema assimétrico, considere o seguinte exemplo:

Exemplo 27. *Suponha dois indivíduos, Alice e Bob, que desejam se comunicar de forma segura. Inicialmente, Alice possui uma caixa, um cadeado C, e uma chave c que abre o cadeado C, sendo que apenas Alice possui essa chave. Por sua vez, Bob possui um cadeado B e uma chave b que abre o cadeado B, sendo que apenas Bob possui essa chave.*

Para iniciar a troca de mensagens, Alice escreve a mensagem desejada, coloca-a dentro da caixa, tranca a caixa com seu cadeado C e envia para Bob. Ao receber a caixa, Bob tranca a caixa com seu cadeado B e a devolve para Alice.

Em seguida, Alice pode abrir o cadeado C com sua chave c, e enviar novamente para Bob. Por sua vez, Bob é capaz de abrir o cadeado B com sua chave b e ler a mensagem de Alice, sem correr o risco de que a caixa seja aberta por terceiros.

Utilizando a teoria de grupos, pode-se pensar em uma modelagem matemática para o exemplo acima. Considere um grupo abeliano $(G, *)$ e um conjunto X, a operação $*$ é uma função:

$$* : G \times X \to X,$$

que associa $g * x \in X$ para cada par ordenado (g, x) de modo que:

1. Se $a, b \in G$, então $a * (b * x) = (a * b) * x$;
2. $e * x = x, \ \forall \ x \in X$;

3. $\forall \ \ a \in G$, $\exists b \in G$, tal que $a * b = b * a = e$.

Retomando o Exemplo 27, os cadeados C, B e as chaves c, b são elementos inversos no grupo $(G, *)$, desta forma, denotando $C = g \in G$, $c = g^{-1} \in G$ e $B = h \in G$, $b = h^{-1} \in G$, considerando ainda a mensagem x pertencente ao conjunto X onde G opera, tem-se a seguinte situação:

Alice		Bob
x	$\longrightarrow$	$g * x$
$h * (g * x)$	$\longleftarrow$	$a * x$
$(h * g) * x = (g * h) * x =$		
$= (g * h) * x$	$\longrightarrow$	$g^{-1} * [(g * h) * x] =$
		$g^{-1} * = [(g * h) * x] = h * x$
		$h^{-1} * (h * x) = x$

Fonte: O próprio autor, baseado em Andria; R. Gondim; R. Salomão (2019).

Em suma, em um sistema de criptografia assimétrica, os participantes envolvidos na transmissão da mensagem possuem um par de chaves, sendo uma pública e outra privada. A chave pública é utilizada para criptografar mensagens e pode ser divulgada livremente, sem comprometer a segurança do criptossistema. Por outro lado, a chave privada é usada para decriptar as mensagens e não pode ser compartilhada, nem mesmo entre os participantes envolvidos.

É importante destacar que a chave privada de cada participante não pode ser derivada a partir da chave pública. No método de criptografia assimétrica, qualquer pessoa pode utilizar a chave pública do destinatário para criptografar uma mensagem, porém, somente o destinatário, que possui a chave privada correspondente, poderá decriptar a mensagem com sucesso.

Definição 33. *Um criptossistema assimétrico depende de três algoritmos:*

(i.) Gen, que gera um par de chaves (p_k, q_k), a partir de um parâmetro de segurança n, onde p_k é a chave pública e q_k é a chave privada;

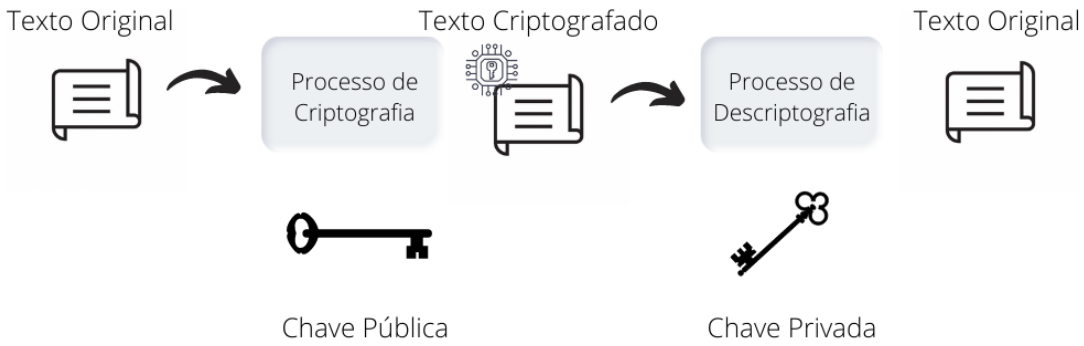
(ii.) Crip, que recebe como parâmetro uma chave pública p_k, uma mensagem m e calcula m para um texto cifrado c;

(iii.) Decrip, que recebe como parâmetro uma chave privada q_k, o texto cifrado c e calcula a mensagem original m.

Note que, $Decrip_{q_k}(Crip_{p_k}(m)) = m$.

Como exemplo, considere novamente o cenário em que Alice deseja se comunicar com Bob. Suponha que (C, c) e (B, b) sejam os pares de chaves pública e privada de Alice e Bob, respectivamente. Quando Alice precisa criptografar uma mensagem m para enviar a Bob, ela utiliza a chave pública B de Bob para realizar a criptografia. Ao receber a mensagem criptografada $B \cdot m$, Bob utiliza sua chave privada b para realizar a operação inversa e decriptar a mensagem, utilizando as propriedades do grupo associado. Dessa forma, ele é capaz de ler a mensagem original. Consulte a Figura 3.7 para uma ilustração visual desse processo.

Figura 3.7: Modelo de Criptografia Assimétrica



Fonte: O próprio autor

3.3.1 O problema do logaritmo discreto

Muitos criptossistemas assimétricos são fundamentados na dificuldade de resolver o clássico *problema do logaritmo discreto*. A segurança desses sistemas depende da dificuldade de resolver esse problema, que pode ser computacionalmente inviável ou extremamente demorado. O problema é definido da seguinte maneira:

Definição 34. *Seja G um grupo abeliano e $\alpha, y \in G$, onde y é uma potência de α. O logaritmo discreto de y na base α é o menor inteiro não negativo x tal que $\alpha^x = y$, denotado por* $\log_\alpha y = x$.

De maneira mais geral, a dificuldade do problema do logaritmo discreto reside em encontrar o valor do inteiro x. Em um grupo finito G, é fácil calcular α^x, mas realizar o processo reverso e encontrar o valor de x é praticamente inviável quando G é grande.

Uma abordagem utilizada por criptoanalistas para atacar criptossistemas baseados no problema do logaritmo discreto é a força bruta. Isso envolve testar todos os possíveis valores de x até encontrar o correto. No entanto, essa abordagem se torna praticamente impossível quando x pode ter milhares de dígitos, o que é comumente utilizado em criptossistemas dessa natureza. Essa característica garante a segurança e a integridade do sistema.

3.3.2 Protocolo de troca de chaves Diffie-Hellman

Um avanço significativo na área da criptografia foi alcançado em 1976 com as descobertas de Whitfield Diffie e Martin Hellman em seu trabalho intitulado "New directions in cryptography". Nesse trabalho, eles introduziram a chamada Chave de Diffie-Hellman, também conhecida como Protocolo Diffie-Hellman ou simplesmente Chave DH.

O Protocolo Diffie-Hellman permite a troca segura de chaves criptográficas entre duas entidades, mesmo em um canal de comunicação inseguro. Ele baseia-se em operações matemáticas complexas e propriedades dos números primos para garantir a confidencialidade das chaves compartilhadas.

Essa descoberta revolucionou a criptografia, abrindo caminho para o desenvolvimento de sistemas criptográficos assimétricos e a criação de algoritmos de troca de chaves seguras, que são amplamente utilizados hoje em dia para proteger a comunicação e as transações online. O Protocolo Diffie-Hellman se tornou um marco importante na história da criptografia moderna.

Em seus trabalhos, Diffie e Hellman propuseram um algoritmo baseado na dificuldade de calcular logaritmos discretos. O protocolo é realizado da seguinte maneira:

Considere dois sujeitos, Alice e Bob, que desejam trocar mensagens em sigilo. Primeiramente, ambos envolvidos definem em consenso uma raiz primitiva $a \in \mathbb{Z}_p^*$ de um número $p \in \mathbb{Z}$, onde p é primo, cujas potências geram todos os inteiros de 1 a $1 - p$, de modo que a e p não precisam ser mantidos em sigilo.

Alice escolhe um número qualquer x no intervalo $(1, p-1)$ e o mantém em segredo como sua chave privada. Então, Alice realiza o seguinte cálculo:

$$y_A = a^x \ mod \ p.$$

Logo em seguida, Alice pode enviar y_A para Bob utilizando um canal público qualquer.

O cálculo é análogo para Bob, é escolhido um número z aleatório de modo que $1 < z < 1 - p$, não podendo ser divulgado a ninguém. E realiza os cálculos:

$$y_B = a^z \ mod \ p.$$

E envia para Alice em um canal público qualquer.

Em posse de y_B, Alice calcula:

$$(y_B)^x \ mod \ p = (a^z)^x \ mod \ p = a^{xz} \ mod \ p = k.$$

De maneira similar, em posse de y_A, Bob realiza os cálculos:

$$(y_A)^z \ mod \ p = (a^x)^z \ mod \ p = a^{xz} \ mod \ p = k.$$

Dessa forma, Alice e Bob possuem a mesma chave compartilhada, sem a necessidade de divulgá-la em qualquer canal de comunicação, seja ele público ou possivelmente seguro. Esse protocolo permite que eles se comuniquem de maneira segura, garantindo a confidencialidade das mensagens trocadas.

Exemplo 28. *Seja o grupo $\mathbb{Z}_{11}$ e $a = 2$ uma raiz primitiva do primo $p = 11$. Alice escolhe $x = 5$ e realiza o cálculo:*

$$y_A = 2^5 \ mod \ 11 = 10,$$

e envia o y_A para Bob. Por sua vez, Bob realiza o cálculo análogo, escolhendo $z = 7$:

$$y_B = 2^7 \ mod \ 11 = 7,$$

e envia y_B para Alice. Em posse de y_B, Alice calcula:

$$7^5 \ mod\ 11 = (2^7)^5 \ mod\ 11 = 10,$$

Cabe a Bob, em posse de y_A, calcular:

$$10^7 \ mod\ 11 = (2^5)^7 \ mod\ 11 = 10.$$

Portanto, a chave privada $k = 10$ pode ser utilizada para que Alice e Bob se comuniquem em sigilo, mesmo sem terem divulgado suas chaves privadas x e z para ninguém, nem mesmo entre eles. Um invasor que tenha acesso ao canal de comunicação precisaria realizar um ataque de força bruta para determinar k, calculando as potências de 2 mod 11, o que não seria uma tarefa tão demorada. No entanto, para garantir a segurança do sistema, são escolhidos números primos com milhares de dígitos, o que torna o cálculo extremamente demorado.

Desta forma, o Protocolo Diffie-Hellman de troca de chaves é baseado no Problema do Logaritmo Discreto no grupo $G = \mathbb{Z}_p^*$, e a operação $*$ representa a multiplicação usual modular p, onde p é um número primo. Isso garante a segurança do sistema, mesmo que as chaves públicas sejam conhecidas por todos.

3.3.3 Criptografia RSA

O RSA (Rivest-Shamir-Adleman) é um criptossistema assimétrico amplamente conhecido e amplamente utilizado na comunidade. Ele foi o primeiro método criptográfico de chave pública desenvolvido e recebeu esse nome em homenagem aos seus criadores, R. L. Rivest, A. Shamir e L. Adleman, na época estudantes do Massachusetts Institute of Technology (MIT). O RSA foi criado em 1977 e ainda é usado em várias aplicações comerciais e softwares de navegação atualmente.

A segurança do sistema RSA é baseada na dificuldade de fatorar um número inteiro em dois números primos. Quando os números primos envolvidos são suficientemente grandes, o processo de fatoração se torna computacionalmente complexo. Por exemplo, um computador comum pode facilmente multiplicar dois números primos de 700 dígitos em questão de segundos, mas realizar a operação inversa, ou seja, fatorar o produto desses primos, exigiria realizar pelo menos 10^{700} divisões, o que demandaria uma quantidade enorme de tempo e esforço computacional.

De acordo com Pellegrini (2019), dado um número inteiro $n = p \cdot q$, onde p e q são primos distintos, a função de encriptação do sistema é dada no grupo $\mathbb{Z}_n$, elevando a mensagem m a um certo expoente e, isto é, $c = m^e \ mod \ n$, onde c representa a mensagem encriptada, e o processo de decriptação é o inverso, ou seja, $m = c^{e^{-1}}$. Note que, para que tais operações funcionem, é necessário que uma vez o expoente e escolhido, ele possua inverso $d = e^{-1}$, entretanto, no grupo $\mathbb{Z}_n$, nem todo elemento possuirá inverso.

O criptossistema RSA trabalha com exponenciação, pois é uma função que dependendo das condições, se torna de mão única, isto é, fácil de calcular, mas muito difícil de se reverter, logo, se faz preciso restringir $\mathbb{Z}_n$ a uma operação de multiplicação e mais ainda, é necessário encontrar os expoentes e e $d = e^{-1}$ que tenham inverso multiplicativo.

Dado um elemento $\alpha \in \mathbb{Z}_n$, o mesmo possui inverso se e só se é coprimo com n, isto é, $mdc(\alpha, n) = 1$, assim pode-se restringir o grupo $\mathbb{Z}_n$ ao conjunto dos elementos menores que n e coprimos com n:

$$\mathbb{Z}_n^* = \{\alpha \in \{1, 2, \cdots, n-1\} \ : \ mdc(\alpha, n) = 1\}.$$

O conjunto $\mathbb{Z}_n^*$ definido acima juntamente com a operação de multiplicação, forma um grupo no qual todos os elementos possuem inverso. A ordem do grupo é dada por $|\mathbb{Z}_n^*| = \phi(n)$, ou seja, a função de Euler definida no Teorema 7.

Como p é primo, por conta da construção da função ϕ, p deve ser coprimo com todos os elementos menores que ele, logo:

$$\phi(p) = p - 1.$$

Além disso, define-se a operação de multiplicação na função ϕ, logo:

$$\phi(\alpha\beta) = \phi(\alpha) \cdot \phi(\beta),$$

seguindo que $n = p \cdot q$, então:

$$\phi(n) = (p-1)(q-1).$$

Pelo Teorema de Euler 7, temos que para todo $n > 1$ e $\alpha \in \mathbb{Z}_n^*$, segue que:

$$\alpha^{\phi(n)} \equiv 1 \ mod \ n.$$

Pode-se então escolher os expoentes e e d em $\mathbb{Z}_{\phi(n)}^*$, escolhendo $e < \phi(n)$ ao acaso e calcula-se d da seguinte maneira:

$$e \cdot d \equiv 1 \ mod \ \phi(n).$$

Logo, pela Proposição 10, existe algum inteiro k, tal que:

$$e \cdot d = k \cdot \phi(n) + 1.$$

Desta forma, é possível encriptar $c = m^e$ e decriptar $c^d = m$:

$$\begin{aligned}
(m^e)^d &\equiv m^{k\phi(n)+1} \ mod \ n \\
&\equiv (m^{\phi(n)})^k m \ mod \ n \\
&\equiv (m^{k\phi(p)\phi(q)})m \ mod \ n \\
&\equiv (m^{\phi(p)})^{k\phi(q)} m \ mod \ n
\end{aligned}$$

Assim, pelo Teorema de Euler:

$$\begin{aligned}
(m^e)^d &\equiv (1)^{k\phi(q)} m \ mod \ n \\
(m^e)^d &\equiv m \ mod \ N.
\end{aligned}$$

Note que por conta de que n é formado pelo produto de dois primos p e q distintos, conforme mencionado anteriormente, o valor da função $\phi(n) = (p-1)(q-1)$.

Com o objetivo de ilustrar ao leitor o processo de encriptação e decriptação do sistema RSA, será descrito em etapas e em seguida elaborado um exemplo. Considere

que Bob queira codificar uma mensagem para Alice utilizando o RSA, primeiramente, Alice deve gerar sua chave pública:

1. Alice escolhe dois números primos p e q em sigilo, de preferência com muitos dígitos para garantir a segurança do sistema;
2. Realiza os cálculos $n = p \cdot q$ e $\phi(n) = (p-1)(q-1)$;
3. Após feitos os cálculos, escolhe ao acaso e de maneira que $1 < e < \phi(n)$, garantindo que $mdc(e, \phi(n)) = 1$;
4. Calcula sua chave secreta $d = e^{-1}\ mod\ \phi(n)$, a qual não deve compartilhar com ninguém;
5. A chave pública de Alice é o par ordenado de números (n, e).

Em posse da chave pública (n, e) de Alice, é necessário que Bob converta a mensagem em números inteiros e realize a encriptação de cada bloco da mensagem m de modo que $c = m^e\ mod\ n$, onde c representa a mensagem encriptada, logo em seguida, envia c para Alice.

Para decodificar, Alice realiza o cálculo $c^d\ mod\ n$, retornando cada bloco encriptado na mensagem original, sendo possível lê-la após converter os números inteiros em letras novamente.

Exemplo 29. *Considere que Bob deseja encriptar a palavra UNESP e enviar para Alice.*

(i.) Geração da chave pública de Alice

Para gerar a chave pública, Alice escolhe em sigilo $p = 37$ e $q = 41$, calculando:

$$n = 37 \cdot 41 = 1517 \text{ e } \phi(n) = (37-1)(41-1) = 1440.$$

Além disso, escolhe $e = 7$ aleatoriamente tal que $1 < e < \phi(n)$, gerando sua chave pública $(1517, 7)$, por fim, calcula sua chave privada, que será usada para decriptação:

$$d = 7^{-1}\ mod\ 1440 = 823.$$

(ii.) Pré-codificação

Para que Bob comece a encriptar uma mensagem para Alice, é necessário que faça a primeira etapa do processo é chamada de *pré-codificação*, pois o que se faz para codificar uma mensagem usando o RSA é calcular sua potência $mod\ n$ em relação a um expoente selecionado, para isto, precisamos que a mensagem seja um número inteiro.

Normalmente a maior parte das mensagens que serão transmitidas é em formato de texto, para isto, é necessário transformá-las em valores numéricos, especificamente em elementos do conjunto dos números inteiros para que possamos realizar o processo de encriptação. Para converter palavras em texto, pode-se utilizar a Tabela ASCII, ou qualquer outra tabela de conversão.

Convertendo a palavra "UNESP", utilizando a Tabela ASCII (Figura 3.2) na base decimal, tem-se:

$$8578698380. \tag{3.1}$$

Caso fosse utilizado alguma outra tabela de conversão, note que é necessário a utilização de números de no mínimo dois algarismos para que não haja ambiguidades como por exemplo, se o número 1 corresponder a letra A, o número 2 corresponder a letra B e o número 12 corresponder a letra L, se for escrito 12, não será possível saber se serão as letras AB ou a letra L.

A última etapa do processo de pré-codificação é dada pela divisão do número obtido em 3.1 em blocos de números menores que n, desta forma, obtêm-se:

$$857 - 86 - 983 - 80. \tag{3.2}$$

(iii.) Encriptação

Para encriptar, utiliza-se $c = m^e\ mod\ n$, de modo que a encriptação seja feita em cada bloco de (3.2) separadamente, mas tomando um certo cuidado para não unir os blocos encriptados novamente, pois se isto for feito, será difícil para decriptar a mensagem e retorná-la ao seu estado original.

Tomando os blocos como $m_1 = 857$, $m_2 = 86$, $m_3 = 983$ e $m_4 = 80$, realiza-se os seguintes cálculos utilizando a chave pública $(1517, 7)$ de Alice:

$$\begin{aligned} c_1 &= 857^7 \ mod \ 1517 = 549, \\ c_2 &= 86^7 \ mod \ 1517 = 1378, \\ c_3 &= 983^7 \ mod \ 1517 = 1024, \\ c_4 &= 80^7 \ mod \ 1517 = 364. \end{aligned}$$

Desta forma, a seguinte mensagem encriptada é enviada para Alice:

$$549 - 1378 - 1024 - 364.$$

Para decriptar, Alice precisará de sua chave privada $d = 823$ anteriormente obtida, e realizar os seguintes cálculos:

$$\begin{aligned} m_1 &= 549^{823} \ mod \ 1517 = 857, \\ m_2 &= 1378^{823} \ mod \ 1517 = 86, \\ m_3 &= 1024^{823} \ mod \ 1517 = 983, \\ m_4 &= 364^{823} \ mod \ 1517 = 80. \end{aligned}$$

Obtendo a seguinte mensagem:

$$857 - 86 - 983 - 80. \tag{3.3}$$

A qual é a mensagem original, unindo os blocos e convertendo novamente em letras, obtêm-se a palavra UNESP.

3.4 Cenários de ataque e interceptação

A criptoanálise é o estudo de técnicas e procedimentos para quebrar a cifra de criptossistemas. O papel do criptanalista é deduzir as chaves utilizadas na encriptação e, consequentemente, o texto plano. Na criptografia simétrica, há apenas uma chave de codificação privada que é utilizada tanto para encriptar quanto para decriptar o texto plano. Por essa razão, é necessário que seja seguro mesmo quando os algoritmos de encriptação e decriptação são conhecidos por um interceptador. Ou seja, a ameaça desconhece a chave privada utilizada, tendo apenas acesso aos processos criptográficos. O atacante pode ser classificado de duas maneiras:

1. **Atacante passivo:** Nesse caso, a ameaça possui apenas cópias dos elementos do criptossistema, representando uma ameaça apenas à confidencialidade da informação;

2. **Atacante ativo:** Esse tipo de ameaça tem a possibilidade de alterar alguns dos elementos do criptossistema, o que facilita o processo de quebra da cifra e representa uma ameaça tanto à integridade quanto à confidencialidade da informação.

Essas classificações são importantes para compreender as diferentes formas de ataques criptoanáliticos e avaliar a segurança dos criptossistemas utilizados.

De acordo com Stinson; M. B. Paterson (2019), existem vários tipos de ataques a criptossistemas, sendo os seguintes os mais comuns, nos quais um criptossistema deve garantir segurança:

1. **Ataque de texto cifrado (*Known cyphertext attack*):** Nesse tipo de ataque, o criptanalista tem acesso a uma grande parte do texto cifrado e seu objetivo é deduzir a chave privada utilizada, mesmo sem ter conhecimento do texto plano correspondente;

2. **Ataque de texto plano conhecido (*Known plaintext attack*):** Nesse tipo de ataque, o criptanalista tem acesso a algumas partes do texto cifrado e às correspondentes partes do texto plano. Seu objetivo é deduzir a chave privada utilizada;

3. **Ataque de texto plano escolhido (*Chosen plaintext attack*):** Nesse tipo de ataque, o criptanalista pode escolher parte do texto plano e obter o texto cifrado correspondente. O ataque é focado em pontos específicos da cifra, visando decriptar o restante do texto com base nas informações obtidas;

4. **Ataque de texto cifrado escolhido (*Chosen cyphertext attack*):** Nesse tipo de ataque, o criptanalista tem a capacidade de escolher parte do texto cifrado e obter o texto plano correspondente. O ataque é realizado na função de decriptação, visando decriptar o restante do texto com base nas informações obtidas.

5. **Ataque de força bruta (*Brute force attack*):** Nesse tipo de ataque, o criptanalista não possui informações que comprometam a integridade do sistema. Ele conhece apenas os métodos utilizados no criptossistema e busca percorrer todo o espaço de chaves, tentando deduzir a chave privada correta através de tentativas;

6. **Ataque homem do meio (*Man in the middle attack*):** Nesse tipo de ataque, o objetivo do criptanalista é infiltrar-se na comunicação entre dois indivíduos que estão utilizando um determinado criptossistema. O atacante tenta se passar por um dos indivíduos, buscando descobrir informações relevantes para facilitar a quebra do criptossistema. O invasor tenta obter acesso à comunicação e quebrar a autenticação usando chaves privadas geradas pelo mesmo criptossistema utilizado pelos indivíduos que ele deseja interceptar.

O ataque de texto plano escolhido e de texto cifrado escolhido são muito mais eficazes do que um ataque de texto cifrado. Dessa forma, um criptossistema que for vulnerável a um ataque de texto cifrado é considerado totalmente inseguro. Em muitos criptossistemas, se valores adequados não forem utilizados para garantir a integridade do sistema, um ataque de força bruta pode ser eficaz na tentativa de deduzir a chave privada.

A prevenção do ataque do "homem do meio" é realizada por meio de uma forte confirmação de autenticação digital. Os sistemas de criptografia de chave pública são bastante resistentes a esse tipo de ataque. Um método criptográfico é considerado com-

pletamente quebrado quando um atacante deduz a chave privada utilizada, permitindo o acesso às informações atuais e futuras.

Capítulo

4

Fractais

Fractais são formas geométricas distintas que não seguem um padrão específico em um contexto geral, mas podem ser classificados em três grupos de acordo com suas características individuais, método de geração e grau de autossimilaridade. Esses grupos incluem fractais definidos por meio de relações de recorrência, fractais aleatórios e aqueles definidos por sistemas de funções iteradas (IFS), que é o foco deste trabalho.

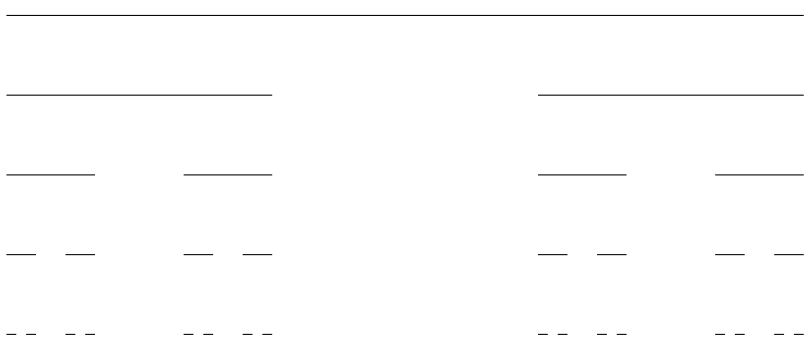
Os fractais gerados por IFS, também conhecidos como fractais determinísticos ou geométricos, possuem características como geometria de regra fixa, autossimilaridade exata e propriedades bem definidas. Alguns exemplos de fractais gerados por IFS clássicos incluem o *Conjunto de Cantor*, a *Curva de Koch*, a *Curva de Peano*, o *Triângulo de Sierpiński*, o *Tapete de Sierpiński*, a *Esponja de Menger*, a *Curva do Dragão*, entre outros.

Para despertar o interesse do leitor, é fascinante observar como alguns fractais clássicos são gerados. Um método especialmente intrigante para criar fractais é através da técnica de *remoção*, onde partes da figura geométrica são iterativamente removidas. Em 1883, *George Cantor* publicou um trabalho inovador sobre um conjunto específico que ficou conhecido como o Conjunto de Cantor ou a *Poeira de Cantor*, o qual é, de fato, um fractal renomado.

O método de construção do Conjunto de Cantor é bastante simples. Inicialmente, começa-se com um segmento de reta de comprimento unitário. Esse segmento é dividido em três partes iguais, e então a parte do meio é removida, resultando em

dois segmentos de comprimento $\frac{1}{3}$ cada. Em seguida, cada um desses dois segmentos é dividido novamente, e a parte do meio é removida novamente. Esse processo é repetido recursivamente, gerando assim o Conjunto de Cantor. Para uma melhor visualização, veja a Figura 4.1 abaixo:

Figura 4.1: O Conjunto de Cantor



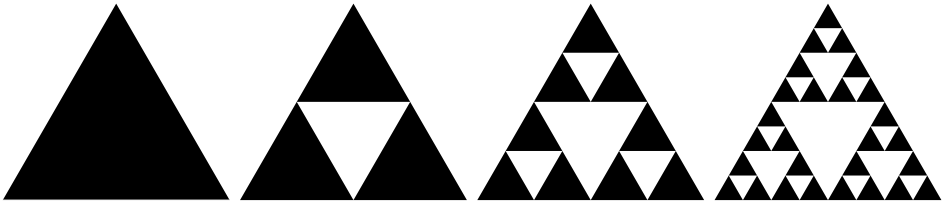
Fonte: O próprio autor

Um fractal que também pode ser gerado por remoção é o *Triângulo de Sierpiński*, que recebe esse nome em homenagem ao matemático polonês *Wacław Sierpiński*, que foi o primeiro a descrevê-lo.

O processo de construção do Triângulo de Sierpiński começa com um triângulo equilátero de lado unitário. A partir desse triângulo, um novo triângulo é removido, cujos vértices são os pontos médios dos lados do triângulo original. Isso resulta na primeira iteração do fractal. Em seguida, o mesmo processo é repetido para cada um dos três triângulos resultantes, gerando a segunda iteração, e assim por diante. Esse processo pode ser iterado n vezes.

Para uma melhor compreensão, observe a Figura 4.2 abaixo:

Figura 4.2: O Triângulo de Sierpiński



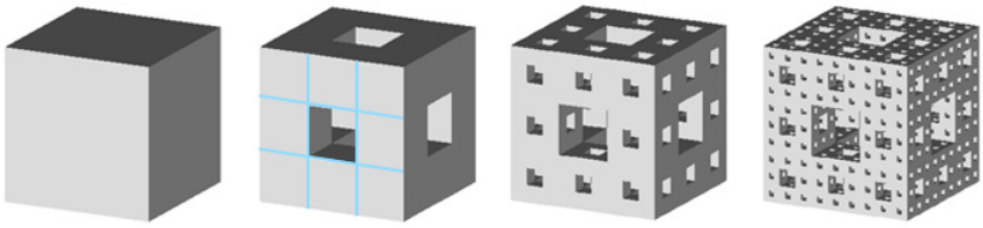
Fonte: O próprio autor

Um exemplo de fractal tridimensional que também pode ser gerado pelo método de remoção é a *Esponja de Menger*, idealizada pelo matemático austríaco *Karl Menger* (1902 - 1985). A construção desse fractal é realizada a partir de um cubo de aresta

medindo 1 unidade. Esse cubo é dividido em 27 cubos menores por meio de planos secantes e ortogonais às suas faces. Cada um dos cubos menores resultantes possuem arestas de comprimento $\frac{1}{3}$ de unidade. Em seguida, é removido o cubo central, bem como os cubos centrais de cada face. O processo é repetido recursivamente em cada um dos cubos restantes, gerando assim a Esponja de Menger.

Para uma melhor visualização, consulte a Figura 4.3 abaixo:

Figura 4.3: Esponja de Menger



Fonte: Biblioteca de imagens do Google

A Geometria Fractal é, sem dúvida, um objeto de estudo que desperta grande curiosidade matemática. Suas formas peculiares intriga a querer buscar uma compreensão mais aprofundada de sua construção matemática. Com base nisso, as próximas seções e subseções serão dedicadas à exploração de resultados que fornecerão fundamentos para o estudo.

4.1 Espaço de Hausdorff

Nas próximas seções, será apresentado um espaço adequado para trabalhar com os fractais, chamado de *Espaço de Hausdorff*, em homenagem ao matemático *Felix Hausdorff* (1868 - 1942). Esse espaço auxiliará no processo de compreensão de como os fractais definidos por sistemas de funções iteradas (IFS) são formados. Será verificado que o espaço de Hausdorff, também conhecido como *espaço dos fractais*, é um espaço métrico completo. Além disso, será estabelecido uma métrica para esse espaço, conhecida como *distância de Hausdorff*. Sem mais delongas, aos resultados.

Definição 35. *Considere um espaço métrico completo* (X, d)*. Denota-se* $\mathscr{H}$ *o espaço no qual os pontos são subconjuntos compactos não vazios de* X*, isto é*

$$\mathscr{H}(X) = \{K \subset X | K \text{ é compacto e } K \neq \varnothing\}.$$

Tal espaço $\mathscr{H}(X)$ é dito ser o Espaço de Hausdorff.

Neste ponto, é útil ter uma métrica claramente definida. Para aprofundar o estudo, pode-se introduzir a distância de Hausdorff. Essa distância mede a separação entre um elemento pertencente ao espaço métrico X e um elemento pertencente a $\mathscr{H}(X)$.

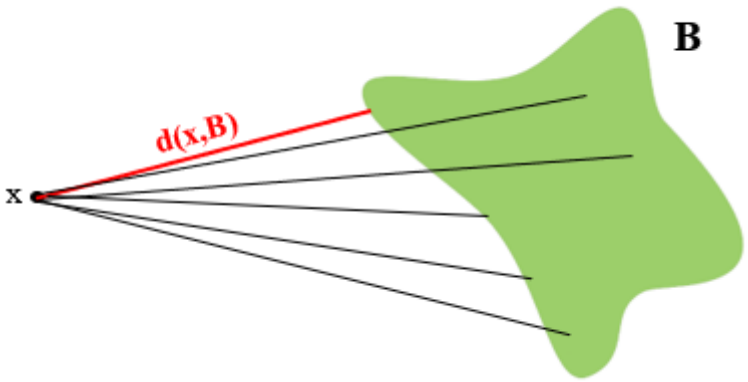
Observação 4. *Note que cada ponto do espaço de Hausdorff $\mathscr{H}(X)$ é um conjunto, logo, a distância entre pontos de $\mathscr{H}(X)$ será a distância entre conjuntos de pontos em um espaço métrico.*

Definição 36. *Considere um espaço métrico completo (X, d), $x \in X$, $B \in \mathscr{H}(X)$. Define-se a distância do ponto x ao conjunto B:*

$$d(x, B) = min\{d(x, y) \mid y \in B\}.$$

Para ilustrar tal definição, observe a Figura 4.4:

Figura 4.4: Distância entre ponto e conjunto



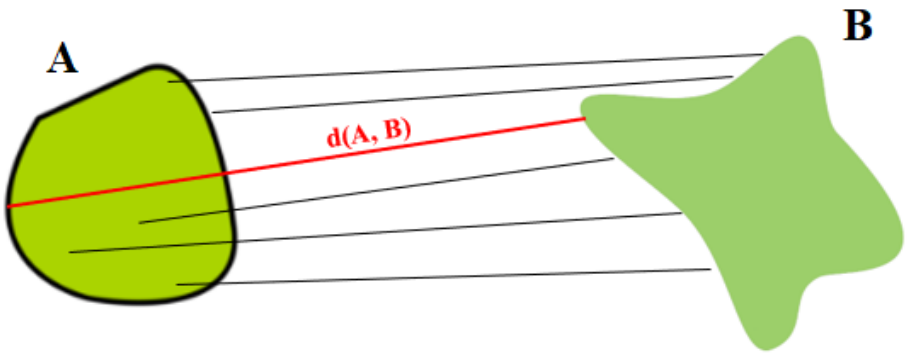
Fonte: O próprio autor

Definição 37. *Considere um espaço métrico completo (X, d), $A, B \in \mathscr{H}(X)$. Define-se a distância entre o conjunto A e o conjunto B:*

$$d(A, B) = max\{d(x, B) \mid x \in A\}.$$

Para ilustrar tal definição, observe a Figura 4.5:

Figura 4.5: Distância entre conjuntos



Fonte: O próprio autor

Proposição 17. *Seja (X, d) um espaço métrico completo. Será mostrado que se A, B e $C \in \mathscr{H}(X)$, então:*

$$d(A \cup B, C) = d(A, C) \vee d(B, C),$$

onde $\vee$ denota o máximo entre as distâncias.

Demonstração. Note que:

$$d(A \cup B, C) = max\{d(x, C) | x \in A \cup B\}.$$

Mas, segue que

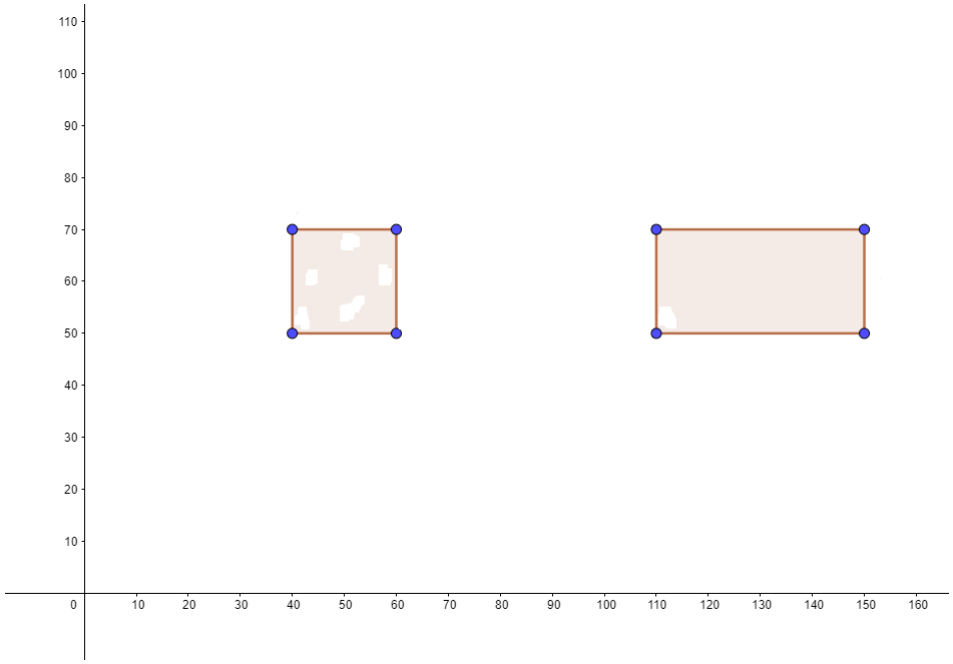
$$max\{d(x, C) | x \in A \cup B\} = max\{d(x, C) | x \in A\} \vee max\{d(x, C) | x \in B\}.$$

□

Para ilustrar a Definição 37, observe o seguinte exemplo:

Exemplo 30. *Considere dois conjuntos $A, B \in \mathbb{R}^2$ definidos tais que $A = [40, 60] \times [50, 70]$ e $B = [110, 150] \times [50, 70]$. Será calculada a distância entre o conjunto A e B.*

Figura 4.6: Representação geométrica dos conjuntos A e B.



Fonte: O próprio autor

Para calcular as distâncias de cada ponto $x \in A$ ao conjunto B, é feito de forma natural:

Para $x_1 = (40, 50) \Rightarrow d(x, B) = 70$

Se $x_2 = (60, 50) \Rightarrow d(x, B) = 50$

Se $x_3 = (40, 70) \Rightarrow d(x, B) = 70$

Se o $x_4 = (60, 70) \Rightarrow d(x, B) = 50$

Analisando a maior distância entre os pontos, tem-se que $d(A, B) = max\{d(x, B) \mid x \in A\} = 70$.

O cálculo de $d(B, A)$ *é análogo, é feito orientando pelo sentido inverso, como segue:*

Para $y_1 = (110, 50) \Rightarrow d(y, A) = 70$

Se o $y_2 = (150, 50) \Rightarrow d(y, A) = 90$

Se o $y_3 = (110, 70) \Rightarrow d(y, A) = 70$

Para $y_4 = (150, 70) \Rightarrow d(y, A) = 90$

Analisando a maior distância entre os pontos, tem-se que $d(y, A) = max\{d(y, A) \mid y \in B\} = 90$.

Concluindo que $d(B, A) = max\{d(y, A) \mid y \in B\} = 90$.

Com as definições dadas e exemplificadas, é possível definir a distância ideal para se trabalhar dentro do espaço de Hausdorff $\mathscr{H}(X)$, que segue:

Definição 38. *Considere um espaço métrico completo (X, d). Define-se a distância de Hausdorff entre dois pontos $A, B \in \mathscr{H}(X)$:*

$$h(A, B) = d(A, B) \vee d(B, A).$$

Proposição 18. *É possível mostrar que a distância de Hausdorff h é uma métrica no espaço de Hausdorff $\mathscr{H}(X)$.*

Demonstração. Para que h seja uma métrica, é necessário verificar as propriedades da Definição 3. Para isto, considere $A, B, C \in \mathscr{H}(X)$.

1. $h(A, B) = h(B, A)$.

   Note que, pela Definição 38, tem-se:

   $$h(A, B) = d(A, B) \vee d(B, A).$$

   Que é equivalente a:

   $$\begin{aligned} h(A, B) &= max\{d(A, B), d(B, A)\}, \\ &= max\{d(B, A), d(A, B)\}, \\ &= d(B, A) \vee d(A, B), \\ &= h(B, A). \end{aligned}$$

2. $0 < h(A, B) < \infty$.

   Note que A, B são elementos do espaço $\mathscr{H}(X)$, logo por definição são compactos e não vazios. Pela compacidade, segue que existem $a \in A$ e $b \in B$ tais que:

   $$d(A, B) = d(a, b).$$

Como d estabelece uma métrica em X, então é claro que $0 < d(a,b) < \infty$, logo $0 < h(A,B) < \infty$.

Por outro lado, como A e B são fechados, segue que se $A \neq B$, isto é, existe $a \in A$ tal que $a \notin B$, onde $d(A,B) > 0$, logo $0 < h(A,B) < \infty$.

3. $h(A,A) = 0$.

   Note que:

$$\begin{aligned} h(A,A) &= d(A,A) \vee d(A,A), \\ &= max\{d(A,A), d(A,A)\}, \\ &= max\{d(x,A) \mid x \in A\}, \\ &= 0. \end{aligned}$$

4. $h(A,B) \leq h(A,C) + h(C,B)$.

   Para verificar a desigualdade triangular, a priori note que $d(A,B) \leq d(A,C) + d(C,B)$, pois para todo $a \in A$:

$$\begin{aligned} d(a,B) &= min\{d(a,b) \mid b \in B\}, \\ &\leq min\{d(a,c) + d(c,b) \mid b \in B\}, \ \forall\ c \in C \\ &= d(a,c) + min\{d(c,b) \mid b \in B\} \ \forall\ c \in C. \end{aligned}$$

   Logo:

$$\begin{aligned} d(a,B) &\leq min\{d(a,c) \mid c \in C\} + max\{min\{d(a,c) \mid b \in B\} \mid c \in C\}, \\ &= d(a,C) + d(C,B). \end{aligned}$$

   Concluindo que:

$$d(A,B) \leq d(A,C) + d(C,B).$$

Com isto em mãos, similarmente:

$$\begin{aligned} d(B,A) &\leq d(B,C) + d(C,A), \\ h(A,B) &= d(A,B) \vee d(B,A) \leq d(B,C) \vee d(C,B) + d(A,C) \vee d(C,A), \\ &= h(B,C) + h(A,C). \end{aligned}$$

Concluindo que h é uma métrica em $\mathscr{H}(X)$.

□

4.1.1 A Completude do Espaço de Hausdorff

Até o momento, foi apresentado um espaço ideal para trabalhar com fractais e uma métrica bem definida que permite a medição dentro desse espaço. Portanto, o espaço métrico $(\mathscr{H}(X), h)$, que consiste em subconjuntos compactos não vazios equipados com a métrica de Hausdorff $h(d)$, será amplamente utilizado.

O objetivo agora é demonstrar a completude do espaço métrico $(\mathscr{H}(X), h)$. Para isso, serão necessárias algumas ferramentas adicionais.

Definição 39. *Seja $S \subset X$ e considere $\Gamma \geq 0$. Então, $S + \Gamma = \{y \in X \mid d(x,y) \leq \Gamma$ para algum $x \in S\}$. $S + \Gamma$ é chamado de dilatação de S por uma bola de raio Γ.*

Lema 2. *Seja A e B pertencente a $\mathscr{H}(X)$, onde (X,d) é um espaço métrico. Considere $\varepsilon > 0$. Então,*

$$h(A,B) \leq \varepsilon \Leftrightarrow A \subset B + \varepsilon \text{ e } B \subset A + \varepsilon.$$

Demonstração. De imediato, será mostrado que $h(A,B) \leq \varepsilon \Leftrightarrow A \subset B + \varepsilon$.

Suponha que $h(A,B) \leq \varepsilon$, isto é, $h(A,B) = d(A,B) \vee d(B,A) \leq \varepsilon$.

Se $d(A,B) \leq \varepsilon$, então $d(x,B) \leq \varepsilon$, para todo $x \in A$, por definição. Em particular, $d(x,y) \leq \varepsilon$ para algum $y \in B$. Logo $x \in B + \varepsilon$, que segue que $A \subset B + \varepsilon$. O mesmo ocorre para $d(B,A) \leq \varepsilon$, então $B \subset A + \varepsilon$.

Tomando $x \in A$, sabe-se que $d(A,B) = max\{d(x,B) \mid x \in A\}$, como $A \subset B + \varepsilon$, então para algum $y \in B$, vale que $d(x,y) \leq \varepsilon$.

Considere agora $\varepsilon_i > 0$, como $min\{d(x_i,y) \mid y \in B\}$, assim:

$$d(x_i,B) \leq \varepsilon_i.$$

Note que vale para todo $x_i \in A$, logo:

$$d(A,B) \leq \varepsilon_A, \text{ com } \varepsilon_A = max\{\varepsilon_1, \varepsilon_2, \cdots\}.$$

De maneira análoga, tem-se:

$$d(B,A) \leq \varepsilon_B, \text{ com } \varepsilon_B = max\{\varepsilon_1, \varepsilon_2, \cdots\}.$$

Tomando ε como $max\{\varepsilon_A, \varepsilon_B\}$, segue que:

$$d(A,B) \leq \varepsilon \text{ e } d(B,A) \leq \varepsilon.$$

Concluindo que $h(A,B) \leq \varepsilon$.

Procedendo de maneira análoga para $h(A,B) \leq \varepsilon \Leftrightarrow B \subset A + \varepsilon$, completa-se a demonstração.

□

Agora, considere $(A_n \mid n = 1, 2, \cdots, \infty)$ uma sequência de Cauchy de conjuntos compactos em $(\mathscr{H}(X), h)$. Isto é, dado $\varepsilon > 0$, existe um N, tal que $n, m \geq N$ implica que:

$$A_n + \varepsilon \supset A_m \text{ e } A_m + \varepsilon \supset A_n,$$

ou seja, $h(A_n, A_m) \leq \varepsilon$.

É necessário mostrar que existem sequências de Cauchy $(X_n)_{n=1}^{\infty}$ em X com a propriedade de que $X_n \in A$ para cada n. Em particular, o lema a seguir que permite a

estender uma subsequência de Cauchy $(X_{n_j} \in A_{n_j})_{j=1}^{\infty}$, tal que $X_{n_j} \in A_{n_j}$, para cada j, para uma sequência de Cauchy $(X_n \in A_n)_{n=1}^{\infty}$.

Lema 3. ***(O Lema da Extensão)*** *Seja (X, d) um espaço métrico. Considere $(A_n \mid n = 1, 2, \cdots, \infty)$ uma sequência de Cauchy de pontos em $(\mathscr{H}(X), h)$. Seja $(n_j)_{j=1}^{\infty}$ uma sequência infinita de inteiros:*

$$0 < n_1 < n_2 < n_3 < \cdots .$$

Suponha também uma sequência de Cauchy $(x_{n_j} \in A_{n_j} \mid j = 1, 2, 3, \cdots)$ no espaço métrico (X, d). Então existe uma sequência de Cauchy $(\tilde{x}_n \in A_n \mid n = 1, 2, \cdots)$, tal que $\tilde{x}_{n_j} = x_{n_j}$, para todo $j = 1, 2, 3, \cdots$.

Demonstração. Dado que (A_n) é uma sequência de Cauchy em $(\mathscr{H}(X), h)$, para todo $\varepsilon > 0$, existe $N_1 \in \mathbb{N}$ tal que, se $m, n > N_1$, então $h(A_m, A_n) < \dfrac{\varepsilon}{2}$. Desta forma, a partir do índice N_1, pode-se controlar A_m e A_n para que fiquem suficientemente próximos.

De modo semelhante, dado que (x_{n_j}) é uma sequência de Cauchy em (X, d), para todo $\varepsilon > 0$, pode-se escolher $N_2 \in \mathbb{N}$ tal que, se $j, k > N_2$, então $d(x_{n_j}, x_{n_k}) < \varepsilon/2$. O que permite controlar x_{n_j} e x_{n_k} para que também fiquem suficientemente próximos.

Considere $N = \max N_1, N_2$. Note que, para todo $j, k > N$, temos $n_j, n_k > N$.

Vamos mostrar que $(\tilde{x}_n)$ é uma sequência de Cauchy. Para isso, seja $\varepsilon > 0$ dado. Escolhemos $N' = \max N, N(\frac{\varepsilon}{2})$, onde $N(\frac{\varepsilon}{2})$ é um inteiro tal que $h(A_n, A_m) < \frac{\varepsilon}{2}$ para todo $m, n > N(\frac{\varepsilon}{2})$.

Agora, seja $n, m > N'$. Queremos mostrar que $d(\tilde{x}_n, \tilde{x}_m) < \varepsilon$. Observe que existem inteiros j, k tais que $n = n_j$ e $m = n_k$ (pois $n, m > N'$). Como (x_{n_j}) é uma sequência de Cauchy, temos que $d(x_{n_j}, x_{n_k}) < \frac{\varepsilon}{2}$ para $j, k > N'$.

Além disso, temos $h(A_{n_j}, A_{n_k}) < \frac{\varepsilon}{2}$ para $j, k > N'$. Agora, usando a desigualdade triangular, temos:

$$\begin{aligned}
d(\tilde{x}_n, \tilde{x}_m) &\leq d(\tilde{x}_n, x_{n_j}) + d(x_{n_j}, x_{n_k}) + d(x_{n_k}, \tilde{x}_m) \\
d(\tilde{x}_n, x_{n_j}) + d(x_{n_j}, x_{n_k}) + d(x_{n_k}, \tilde{x}_m) &\leq h(A_n, An_j) + d(x_{n_j}, x_{n_k}) + h(A_{n_k}, A_m) \\
h(A_n, An_j) + d(x_{n_j}, x_{n_k}) + h(A_{n_k}, A_m) &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.
\end{aligned}$$

Portanto, $(\tilde{x}_n)$ é uma sequência de Cauchy em (X, d). Além disso, temos $\tilde{x}_{n_j} = x_{n_j}$ para todo j, o que conclui a demonstração do lema.

Com base na Definição 39 e nos lemas 2 e 3, é possível elencar o teorema central desta subseção.

Teorema 10. ***(Completude do Espaço de Hausdorff)*** *Seja (X, d) um espaço métrico completo. Então $(\mathscr{H}(X), h)$ é um espaço métrico completo. Mais ainda, se $(A_n \in \mathscr{H}(X))_{n=1}^{\infty}$ é uma sequência de Cauchy, então:*

$$A = \lim_{n\to\infty} A_n \in \mathscr{H}(X).$$

Pode ser caracterizada como $A = \{x \in X \mid$ existe uma sequência de Cauchy $(x_n \in A_n)$ que converge para $x\}$.

Demonstração. Seja (A_n) uma sequência de Cauchy em $\mathscr{H}(X)$ e seja A definido como descreve o teorema. A prova será dividida em 5 itens:

(i.) $A \neq \varnothing$;

(ii.) A é fechado, logo completo já que X é completo;

(iii.) Para $\varepsilon > 0$ existe N tal que para $n \geq N$, $A \subset A_n + \varepsilon$;

(iv.) A é totalmente limitado, logo por (2.) é compacto;

(v.) $\lim A_n = A$.

Demonstração de (*i.*) Este item será provado verificando a existência de uma sequência de Cauchy $(a_i \in A_i)$ em X. Para isto, considere a sequência de inteiros positivos $N_1 < N_2 < N_3 < \cdots < N_n < \cdots$ tais que:

$$h(A_m, A_n) < \frac{1}{2^i} \text{ para } m, n > N_i.$$

Escolha $x_{N_1} \in A_{N_1}$, então, como $h(A_{N_1}, A_{N_2}) \leq \frac{1}{2}$, pode-se encontrar um $x_{N_2} \in A_{N_2}$, tal que $d(x_{N_1}, x_{N_2}) \leq \frac{1}{2}$. Assumindo que foi escolhido uma sequência finita $x_{N_i} \in A_{N_i}$, $i = 1, 2, \cdots, k$ para cada $d(x_{N_{i-1}}, x_{N_i}) \leq \frac{1}{2^{i-1}}$.

Como $h(A_{N_k}, A_{N_{k+1}}) \leq \frac{1}{2^k}$, e $x_{N_k} \in A_{N_k}$, pode-se encontrar $x_{N_{k+1}} \in A_{N_{k+1}}$ tal que $d(x_{N_k}, x_{N_{k+1}}) \leq \frac{1}{2^k}$. Por exemplo, seja $x_{N_{k+1}}$ um ponto em $A_{N_{k+1}}$ que é próximo

de x_{N_k}, por indução, é possível encontrar uma sequência infinita $(x_{N_i} \in A_{N_i})$ tal que $d(x_{N_i}, x_{N_{i+1}}) \leq \frac{1}{2^i}$.

Para verificar que (x_{N_i}) é uma sequência de Cauchy em X, seja $\varepsilon > 0$ e escolha N_ε tal que $\sum_{i=N_\varepsilon}^{\infty} \frac{1}{2^i} < \varepsilon$. Então para $m > n > N_\varepsilon$ tem-se:

$$d(x_{N_m}, x_{N_n}) \leq d(x_{N_m}, x_{N_{m+1}}) + d(x_{N_{m+1}}, x_{N_{m+2}}) + \cdots + d(x_{N_{n-1}}, x_{N_n}) < \sum_{i=N_\varepsilon}^{\infty} \frac{1}{2^i} < \varepsilon.$$

Pelo lema 3, existe uma subsequência convergente $(a_i \in A_i)$ para cada $a_{N_i} = x_{N_i}$. Então, o $\lim a_i$ existe e por definição está em A. Logo, $A \neq \varnothing$.

Demonstração de (*ii.*) Para mostrar que A é fechado, suponha que $(a_i \in A)$ é uma sequência que converge para um ponto a. Será mostrado que $a \in A$ e consequentemente que A é fechado.

Para cada positivo inteiro i, existe uma sequência $(x_{i,n} \in A_n)$ tal que:

$$\lim_{n\to\infty} x_{i,n} = a_i.$$

Existe uma sequência crescente de números inteiros positivos $(N_i)_{i=1}^{\infty}$, tal que $d(a_{N_i}, a) < \frac{1}{i}$, além disso, existe uma subsequência de inteiros (m_i), tal que $d(x_{N_i,m_i}, a_{N_i}) \leq \frac{1}{i}$, logo $d(X_{N_i,m_i}, a) \leq \frac{2}{i}$.

Ao tomar $y_{m_i} = x_{N_i,m_i}$ tem-se que $y_{m_i} \in A_{m_i}$ e $\lim_{i\to\infty} y_{m_i} = a$. Pelo lema 3, (y_{m_i}) pode ser estendido para uma sequência convergente $(z_i \in A_i)$, logo, $a \in A$, desta forma, A é fechado.

Demonstração de (*iii.*) Seja $\varepsilon > 0$, existe um N, tal que para $m, n \geq N$, temos $h(A_m, A_n) \leq \varepsilon$. Além disso, considere $n \geq N$, então para $m \geq n$, temos que $A_m \subset A_n + \varepsilon$.

É necessário verificar que $A \subset A_n + \varepsilon$, para isto, seja $a \in A$. Existe uma sequência $(a_i \in A_i)$ que converge para a, tomando N tão grande de modo que $m \geq N, d(a_m, a) < \varepsilon$.

Então, $a_m \in A_n + \varepsilon$ já que $a_m \subset A_n + \varepsilon$, como A_n é compacto, pode-se afirmar que $A_n + \varepsilon$ é fechado. Desta forma, como $a_m \in A_n + \varepsilon$, para todo $m \geq N$, a também deve pertencer a $A_n + \varepsilon$, concluindo que $A \subset A_n + \varepsilon$.

Demonstração de (*iv.*) Suponha que A não seja totalmente limitado, então, é possível encontrar uma sequência $(x_i)_{i=1}^{\infty}$ em A, tal que $d(x_i, x_j) \geq \varepsilon$, para $i \neq j$. Será mostrado que tal afirmação trará uma contradição.

Pelo Item (*iii.*), existe um n suficientemente grande, tal que $A \subset A_n + \frac{\varepsilon}{3}$, para cada x_i, logo existe um correspondente $y_i \in A_n$ para o qual $d(x_i, y_i) \leq \frac{\varepsilon}{3}$. Como A_n é compacto, note que alguma subsequência (y_{n_i}) de (y_i) converge.

Logo, pode-se encontrar pontos na sequência (y_{n_i}) tão próximos quanto se queira. Em particular, é possível encontrar dois pontos y_{n_i} e y_{n_j}, tal que $d(y_{n_i}, y_{n_j}) < \frac{\varepsilon}{3}$. Mas,

$$d(x_{n_i}, x_{n_j}) \leq d(x_{n_i}, y_{n_i}) + d(y_{n_i}, y_{n_j}) + d(y_{n_j}, x_{n_j}) < \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3}.$$

Logo, tem-se uma contradição pela maneira que (x_{n_i}) foi escolhido, assim, A é totalmente limitado, e pelo Item (*ii.*), é compacto.

Demonstração de (*iv.*) Pelo Item (*iv.*), segue que $A \in \mathscr{H}(X)$ e pelo Item (*iii.*) e pelo lema 2, a demonstração de que o $\lim A_i = A$ estará completa se for verificado que para $\varepsilon > 0$, existe um N tal que para $n \geq N$, $A_n \subset A + \varepsilon$.

Para tal verificação, seja $\varepsilon > 0$ e será determinado um N, tal que para $m, n \geq N$, tem-se $h(A_m, A_n) \leq \frac{\varepsilon}{2}$. Logo, para $m, n \geq N$, $A_m \subset A_n + \frac{\varepsilon}{2}$.

Seja $n \geq N$, será mostrado que $A_n \subset A + \varepsilon$. Considere $y \in A_n$, logo existe uma sequência crescente (N_i) de inteiros tal que:

$$n < N_1 < N_2 < N_3 < \cdots < N_k < \cdots .$$

E para $m, k \geq N_j$, $A_m \subset A_k + \frac{\varepsilon}{2^{j+1}}$. Note que $A_n \subset A_{N_1} + \frac{\varepsilon}{2}$. Como $y \in A_n$, existe um $x_{N_1} \in A_{N_1}$ tal que $d(y, x_{N_1}) \leq \frac{\varepsilon}{2^2}$. Repetindo o raciocínio, será encontrado uma sequência $x_{N_1}, x_{N_2}, \cdots$ tal que $x_{N_j} \in A_{N_j}$ e $d(x_{N_j}, X_{N_{j+1}}) < \frac{\varepsilon}{2^{j+1}}$.

Usando a desigualdade triangular sucessivas vezes, segue que:

$$d(y, x_{N_j}) \leq \varepsilon, \ \forall \ j,$$

além disso, (x_{N_j}) é uma sequência de Cauchy que converge para um ponto x em A. Mais ainda, $d(y, x_{N_j}) \leq \varepsilon$ implica que $d(y, x) \leq \varepsilon$, logo, foi mostrado que $A_n \subset A + \varepsilon$ para $n \leq N$.

Portanto, pelo item (*ii.*) A é compacto, que segue que $\lim A_n = A$, provando que $(\mathscr{H}(X), h)$ é um espaço métrico completo.

□

Note que, com a completude do espaço métrico $(\mathscr{H}(X), h)$ pode-se garantir que existe uma sequência de Cauchy que converge para um determinado ponto fixo, isto é, é possível controlar as iteradas de uma determinada transformação em $(\mathscr{H}(X), h)$.

4.1.2 Transformações Contrativas

Definição 40. *Uma transformação $f : X \to X$ definida em um espaço métrico (X, d) é dita ser uma contração se existe uma constante s, de modo que $0 \leq s < 1$, tal que:*

$$d(f(x), f(y)) \leq s \cdot d(x, y) \ \forall \ x, y \in X.$$

Tal constante s é chamada fator de contração da transformação f.

Pode-se interpretar a definição acima da seguinte forma: note que $0 \leq s < 1$, logo uma contração f é uma ferramenta para aproximar pontos do espaço, pois será feita a multiplicação da distância entre dois pontos por uma constante que está compreendida no intervalo $[0, 1)$.

Teorema 11. *(O Teorema da Contração) Seja $f : X \to X$ uma contração em um espaço métrico completo (X, d). Logo f possui exatamente um ponto fixo $x_f \in X$ e para qualquer ponto $x \in X$, a sequência $(f^n(x) : n = 0, 1, 2, \cdots)$ converge para x_f:*

$$\lim_{n \to \infty} f^n(x) = x_f, \ \textit{para cada } x \in X.$$

Demonstração. Considere $x \in X$. Seja $0 \leq s < 1$ um fator de contração para f, logo:

$$d(f^n(x), f^m(x)) \leq s^{m \wedge n} d(x, f^{|n-m|})(x), \tag{4.1}$$

para todo $m, n = 0, 1, 2, \cdots$, onde $x \in X$ é fixo, e $m \wedge n$ representa o mínimo entre dois números reais m e n. Em particular, para $k = 0, 1, 2, \cdots$, tem-se:

$$\begin{aligned} d(x, f^k(x)) &\leq d(x, f(x)) + d(f(x), f^2(x)) + \cdots + d(f^{(k-1)}(x), f^k(x)) \\ &\leq (1 + s + s^2 + \cdots + s^{k-1}) \cdot d(x, f(x)) \\ &\leq (1 - s)^{-1} \cdot d(x, f(x)). \end{aligned}$$

Substituindo na equação 4.1, segue que:

$$d(f^n(x), f^m(x)) \leq s^{m \wedge n} \cdot (1 - s)^{-1} \cdot d(x, f(x))$$

O que mostra que a distância entre os pontos de f^n estão se aproximando dado um inteiro k, logo, a sequência $(f^n(x))_{n=0}^{\infty}$ é uma sequência de Cauchy. Como X é completo por hipótese, a sequência de Cauchy possui um limite $x_f \in X$ para o qual a sequência converge:

$$\lim_{n \to \infty} f^n(x) = x_f.$$

Resta mostrar agora que x_f é um ponto fixo de f e ele é único. Como f é uma contração, f é contínua, então:

$$f(x_f) = f\left(\lim_{n \to \infty} f^n(x)\right) = \lim_{n \to \infty} f^{(n+1)}(x) = x_f.$$

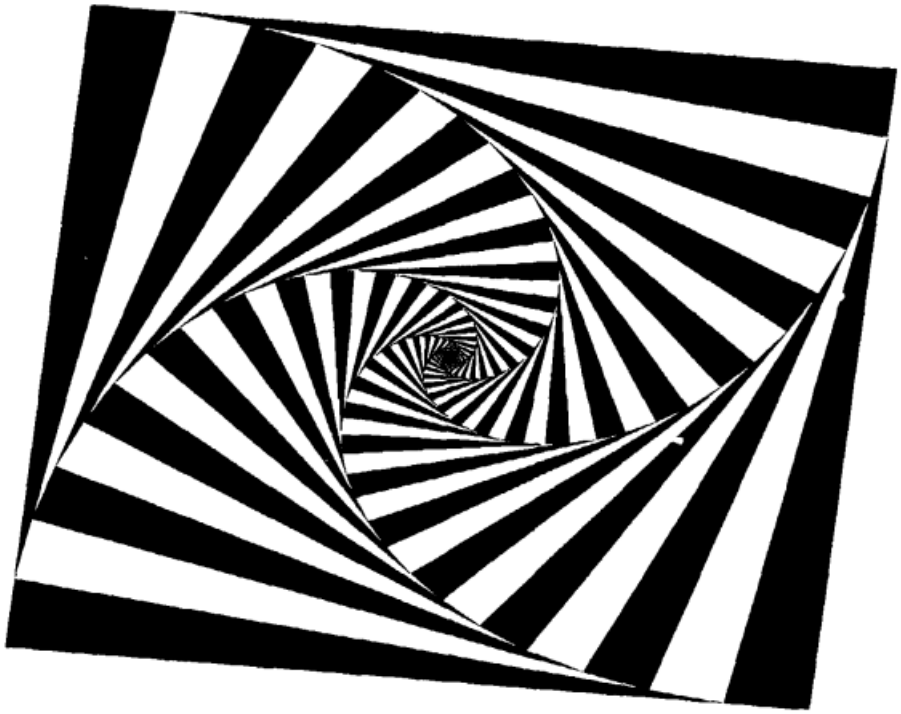
Suponha agora que existam dois pontos fixos x_f e y_f da contração f, logo pela definição de ponto fixo, $f(x_f) = x_f$ e $f(y_f) = y_f$, assim:

$$d(x_f, y_f) = d(f(x_f), f(x_f)) \leq s \cdot d(x_f, y_f).$$

O que implica que $(1 - s) \cdot d(x_f, y_f) \leq 0$, que segue que $d(x_f, y_f) = 0$, logo $x_f = y_f$, portanto o ponto fixo x_f é único.

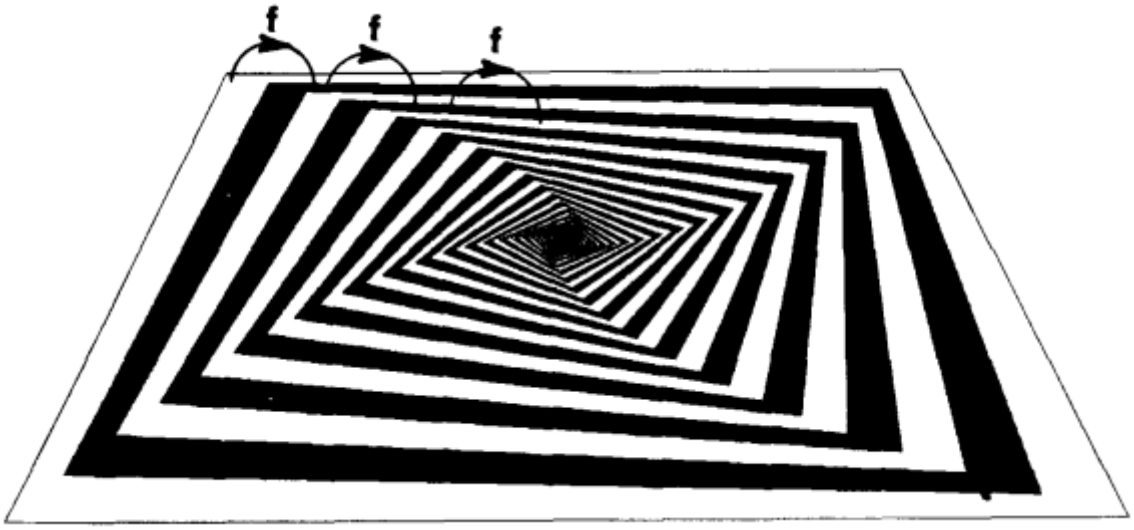
□

Figura 4.7: Contração f em um espaço métrico compacto.



Fonte: Retirado de Barnsley (1988)

Figura 4.8: Iteração da contração f convergindo para um ponto fixo $x_f \in X$.



Fonte: Retirado de Barnsley (1988)

Exemplo 31. *Considere as Figuras 4.7 e 4.8. Seja uma contração f em um espaço métrico compacto (X, d), note que durante as iterações f^n ocorrem algumas situações simples: A contração oscila entre as cores branco e preto, realiza a contração e uma translação, formando uma espécie de corredores transladados, convergindo para um ponto fixo $x_f \in X$ ao centro da imagem.*

4.1.3 Contrações no Espaço de Hausdorff

Até o presente momento, não foi explorada uma definição formal para os fractais, pois os resultados que foram estudados permitem afirmar que segundo Barnsley (1988), um *fractal determinístico* é um ponto fixo de uma contração f no espaço de Hausdorff $(\mathscr{H}(X), h(d))$. Será mostrado agora alguns resultados que fundamentarão melhor o conceito de fractal de uma maneira particular, isto é, será visto os fractais que são determinados por *sistemas de funções iteradas* (IFS), do inglês, *iterated function system.*

Lema 4. *Seja $w : X \to X$ uma contração em um espaço métrico (X, d), logo w é contínua.*

Demonstração. Considere um fator de contração $s > 0$ associado a contração w. Logo, pela definição de contração, dado um $\varepsilon > 0$, temos:

$$d(w(x), w(y)) \leq s \cdot d(x, y) < \varepsilon.$$

Considerando $\delta = \frac{\varepsilon}{s}$, tem-se que $d(x, y) < \delta$, logo w é contínua.

□

Lema 5. *Seja $w : X \to X$ uma contração contínua definida em um espaço métrico (X, d). Então $w : \mathscr{H}(X) \to \mathscr{H}(X)$, isto é, a imagem de w restrita a $\mathscr{H}(X)$ é o próprio espaço $\mathscr{H}(X)$.*

Demonstração. Suponha que S é um subconjunto compacto e não vazio de X. Nesse caso, ao examinar o conjunto $w(S)$ formado pelos elementos $w(x)$ para cada $x \in S$, observa-se que esse conjunto não é vazio. Demonstrando que $w(S)$ também é compacto, pode-se concluir que $w(S) \in \mathscr{H}(X)$. Isso implica que a função w mapeia elementos de $\mathscr{H}(X)$ para outros elementos de $\mathscr{H}(X)$.

Seja $(y_n = w(x_n))$ uma sequência infinita de pontos em S, então (x_n) é também uma sequência infinita de pontos em S. Como S é compacto, então existe uma subsequência (x_{N_n}) de (x_n) que converge para um determinado ponto $\tilde{x} \in S$, mas, como w é contínua, tem-se:

$$(y_{N_n} = f(x_{N_n})),$$

que é uma subsequência convergente de (y_n) que converge para $\tilde{y} = f(\tilde{x}) \in w(S)$. Desta forma, obtêm-se duas subsequências de sequências de pontos em S que convergem para pontos em $w(S)$, logo $w(S)$ é compacto.

□

De acordo com os lemas acima, segue o próximo resultado, que auxiliará ao trabalhar com contrações em $(\mathscr{H}(X), h)$ fora do espaço métrico usual (X, d).

Lema 6. *Seja $w : X \to X$ uma contração definida em um espaço métrico (X, d) com fator de contração s. Então $w : \mathscr{H}(X) \to \mathscr{H}(X)$ definida por:*

$$w(B) = \{w(x) \mid x \in B\} \ \forall \ B \in \mathscr{H}(X),$$

é uma contração em $(\mathscr{H}(X), h)$ com fator de contração s.

Demonstração. Pelos lemas 1 e 2, sabe-se que a contração $w : X \to X$ é contínua e $w : \mathscr{H}(X) \to \mathscr{H}(X)$. Considere então $B, C \in \mathscr{H}(X)$, logo pela definição da distância de Hausdorff:

$$\begin{aligned} d(w(B), w(C)) &= max\{min\{d(w(x), w(y)) \mid y \in C\} \mid x \in B\} \\ &\leq max\{min\{s \cdot (x, y) \mid y \in C\} \mid x \in B\} = s \cdot d(B, C). \end{aligned}$$

De modo análogo, $d(w(C), w(B)) \leq s \cdot d(C, B)$, então:

$$\begin{aligned} h(w(B), w(C)) &= d(w(B), w(C)) \vee d(w(C), w(B)) \leq s \cdot d(B, C) \vee d(C, B) \\ &\leq s \cdot h(B, C). \end{aligned}$$

Desta forma, dado $B, C \in \mathscr{H}(X)$, tem-se que $w : \mathscr{H}(X) \to \mathscr{H}(X)$ é uma contração em $(\mathscr{H}(X), h)$ com fator de contração s.

□

Lema 7. *Considere B, C, D e E elementos de $\mathscr{H}(X)$, então:*

$$h(B \cup C, D \cup E) \leq h(B, D) \vee h(C, E),$$

onde h é a distância de Hausdorff usual.

Demonstração. Perceba que:

$$\begin{aligned} d(B \cup C, D \cup E) &= max\{d(x, D \cup E) \mid x \in B \cup C\}, \\ &= max\{d(x, D \cup E) \mid x \in B\} \vee max\{d(x, D \cup E) \mid x \in C\}, \\ &= d(B, D \cup E) \vee d(C, D \cup E). \end{aligned}$$

Desta forma, para todo elemento $x \in B$, segue que:

$$\begin{aligned} d(x, D \cup E) &= min\{d(x, y) \mid y \in D \cup E\}, \\ &= min\{min\{d(x, y) \mid y \in D\},\ min\{d(x, y) \mid y \in E\}\}, \\ &\leq min\{d(x, y) \mid y \in D\} = D(x, D). \end{aligned}$$

O raciocínio é análogo para o elemento E, assim como foi feito com D. Logo, se a distância entre D e E for mais próxima de x, então $d(x, D \cup E) = d(x, D)$, se caso contrário, segue que $d(x, D \cup E) < d(x, D)$.

Observe que $d(B, D \cup E) \leq d(B, D)$ ao escolher o maior valor que $d(x, D)$ pode assumir, para qualquer $x \in B$. O mesmo ocorre para $x \in C$, logo $d(C, D \cup E) \leq d(C, E)$.

Mas, ao tomar $d(B, D) \vee d(C, E)$, note que será maior que $d(B, D \cup E)$ e $d(C, D \cup E)$, assim:

$$d(B \cup C, D \cup E) = d(B, D \cup E) \vee d(C, D \cup E) \leq d(B, D) \vee d(C, E).$$

De modo análogo, segue que:

$$d(D \cup E, B \cup E) = d(D, B \cup C) \vee d(E, B \cup C) \leq d(D, B) \vee d(E, C).$$

Podendo concluir então:

$$\begin{aligned} h(B \cup C, D \cup E) &= d(B \cup C, D \cup E) \vee d(D \cup E, B \cup C), \\ &= [d(B, D \cup E) \vee d(C, D \cup E)] \vee [d(D, B \cup C) \vee d(E, B \cup C)], \\ &\leq [d(B, D) \vee d(C, E)] \vee [d(D, B) \vee d(E, C)], \\ &= h(B, D) \vee h(C, E). \end{aligned}$$

Assim,

$$h(B \cup C, D \cup E) \leq h(B, D) \vee h(C, E).$$

□

O resultado a seguir é de extrema importância em relação à união de contrações no espaço de Hausdorff. Com o objetivo de elaborar novas contrações, o operador que será definido recebe o nome de *Operador de Hutchinson.*

Lema 8. *Seja (X, d) um espaço métrico. Considere $\{w_n \mid n = 1, 2, \cdots, N\}$ contrações em $(\mathscr{H}(X), h)$, onde s_n é o fator de contração para w_n para cada n. Define-se $W : \mathscr{H}(X) \to \mathscr{H}(X)$ da seguinte forma:*

$$W(B) = w_1(B) \cup w_2(B) \cup \cdots \cup w_N(B) = \bigcup_{n=1}^{N} w_n(B), \text{ para cada } B \in \mathscr{H}(X).$$

Então W é uma contração com fator de contração s dado por:

$$s = max\{s_n \mid n = 1, 2, \cdots, N\}.$$

Demonstração. Por indução o resultado é provado.

$$h(W(B), W(C)) = h(w_1(B) \cup w_2(B), w_1(C) \cup w_2(C)).$$

Pelo lema 7:

$$h(W(B), W(C)) \leq h(w_1(B), w_1(C)) \vee h(w_2(B), w_2(C))$$

Logo, pela definição de contração, conclui-se que:

$$h(W(B), W(C)) \leq s_1 h(B, C) \vee s_2 h(B, C) \leq sh(B, C).$$

□

Com os resultados anteriores bem fundamentados, pode-se definir um sistema de funções iteradas.

Definição 41. *Um Sistema de Funções Iteradas hiperbólico (Iterated Function System), consiste de um espaço métrico completo (X, d) junto com um conjunto finito de contrações $w_N : X \to X$, com os respectivos fatores de contração s_n, para $n = 1, 2, \cdots, N$, dado pelo maior fator de contração $s = max\{s_n : n = 1, 2, \cdots, N\}$. Denota-se o IFS como $\{X; w_n, n = 1, 2, \cdots, N\}$.*

Teorema 12. *Seja um IFS hiperbólico $\{X; w_n, n = 1, 2, \cdots, N\}$ com fator de contração s. Então a transformação $W : \mathscr{H}(X) \to \mathscr{H}(X)$ definida por:*

$$W(B) = \bigcup_{n=1}^{N} w_n(B),$$

para todo $B \in \mathscr{H}(X)$, é uma contração num espaço métrico completo $(\mathscr{H}(X), h(d))$ com fator de contração s, isto é,

$$h(W(B), W(C)) \leq s \cdot h(B, C), \ \forall \ \ B, C \in \mathscr{H}(X).$$

Além disso, seu único ponto fixo $A \in \mathscr{H}(X)$*,*

$$A = W(A) = \bigcup_{n=1}^{N} w_n(A),$$

é dado por $A = \lim_{n\to\infty} W^n(B)$*, para qualquer* $B \in \mathscr{H}(X)$*.*

Demonstração. Observe que o operador de Hutchinson $W : \mathscr{H}(X) \to \mathscr{H}(X)$ é uma contração pelo lema 8 com fator de contração dado pelo máximo entre as n contrações, isto é, $s = max\{s_n \mid n = 1, 2, \cdots, N\}$.

O Teorema 11 nos garante que, como W é uma contração, então seu ponto fixo A é único e, além disso, para qualquer elemento B de $\mathscr{H}(X)$, a sequência $\{W^n(B)\}$ converge para A. Logo, conclui-se que:

$$\lim_{n\to\infty} W^n(B) = A.$$

□

Definição 42. *O ponto fixo* $A \in \mathscr{H}(X)$ *descrito no Teorema anterior é dito o atrator do IFS.*

Observação 5. *Segundo Barnsley (1988), pode-se dizer que os atratores dos IFS são um tipo de fractais determinísticos.*

Exemplo 32. *Considere o sistema de funções iteradas (IFS), segundo a Definição 41,* $\{\mathbb{R}; w_n, n = 1, 2\}$*, dado por:*

$$w_1(x) = \frac{1}{3}x \ \ e \ \ w_2(x) = \frac{1}{3}x + \frac{2}{3}.$$

O operador de Hutchinson é dado por:

$$W(A) = w_1(A) \cup w_2(A), \ \forall \ A \in \mathscr{H}(\mathbb{R}).$$

Considere o conjunto inicial $C_0 = [0, 1]$*, logo, ao iterar o IFS note que o atrator é o Conjunto de Cantor, pois a sequência de conjuntos* (C_n) *é uma sequência de Cauchy em* $\mathscr{H}(\mathbb{R})$*, tal que:*

$$C_0 \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_n \supseteq \cdots$$

Como $\mathbb{R}$ é um espaço métrico completo, pelo Teorema 12:

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

Capítulo

5

Fractais e Criptografia

Este capítulo se baseia na análise dos aspectos matemáticos dos sistemas de funções iteradas (IFS) e sua aplicação na criptografia, mais especificamente nos sistemas de criptografia de chaves públicas, levando em consideração a eficiência e a segurança do método.

Desde 1990, vários pesquisadores têm observado uma relação intrigante entre Caos, Geometria Fractal e Criptografia. Os sistemas dinâmicos caóticos são altamente sensíveis às condições iniciais, apresentam uma geometria extremamente complexa e um comportamento aparentemente aleatório. Em particular, Sistemas de Funções Iteradas (IFS) possuem uma estrutura matemática complicada, especialmente na construção recursiva dessas funções, o que resulta em melhores aproximações e gera aspectos muito úteis na área de criptografia.

5.1 Protocolo fractal de troca de chaves

Para que haja comunicação efetiva e sigilosa entre os pares, a segurança da informação leva em conta o estabelecimento de um canal de transmissão seguro, no qual as mensagens, mesmo codificadas, possam ser trocadas, proporcionando um nível maior de segurança em um criptossistema. Ao considerar isso, surge um novo obstáculo para um invasor, pois caso um terceiro tente interceptar a comunicação entre dois indivíduos que utilizam um método criptográfico seguro e um canal de transmissão seguro, seria

necessário violar tanto o canal quanto o criptossistema para ter acesso às informações sigilosas.

Conforme mencionado no Capítulo 3, Diffie e Hellman foram os pioneiros no desenvolvimento de um protocolo seguro de troca de chaves, publicado no trabalho intitulado *New Directions in Cryptography*, conhecido como o Protocolo Diffie-Hellman. Essa publicação deu origem a diversos protocolos subsequentes, que se baseiam nos conceitos matemáticos relativamente simples e de difícil reversão apresentados por Diffie e Hellman.

O método fractal de troca de chaves proposto aqui, idealizado por Al-Saidi (2014), baseia-se no Protocolo Diffie-Hellman. A segurança desse método é fundamentada na construção recursiva de um fractal escolhido, gerado por IFS, que é utilizado como uma raiz primitiva para gerar a chave pública, combinado com o problema do logaritmo discreto. Inicialmente, é necessário escolher um fractal e resolver suas transformações afins de forma recursiva, com o número de iterações determinado pelo atrator do fractal, que é gerado pelo operador de Hutchinson.

5.1.1 A escolha do fractal

Existem vários fractais determinísticos que podem ser gerados por IFS. Com base em Barnsley (1988), serão listados aqui alguns que podem ser utilizados para o estabelecimento do protocolo fractal de troca de chaves proposto anteriormente. Ao restringir-se aos IFS hiperbólicos da forma $\{\mathbb{R}^2; w_n \mid n = 1, 2, \cdots, N\}$ e, por exemplo, ao utilizar 3 contrações, é possível determinar o seguinte IFS:

$$
\begin{aligned}
w_1(x_1, x_2) &= \begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\
w_2(x_1, x_2) &= \begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 1 \\ 50 \end{pmatrix} \\
w_3(x_1, x_2) &= \begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 50 \\ 50 \end{pmatrix}
\end{aligned}
$$

Ao iterar o IFS acima, é gerado o atrator conhecido como o *Triângulo de Sierpiński*, o que equivale a dizer que o IFS acima gera o fractal do Triângulo de Sierpiński. Utilizando uma notação geral para os IFS $\{\mathbb{R}^2; w_n \mid n = 1, 2, \cdots, N\}$, temos o seguinte:

$$w_i(x) = w_i(x_1, x_2) = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} e_i \\ f_i \end{pmatrix} = A_i x + t_i.$$

onde a_i, b_i, c_i e d_i são os elementos da matriz e e_i e f_i representam a translação do IFS. A seguir será mostrado alguns valores de IFS de fractais conhecidos, tais resultados são acompanhados de um valor p_i associados às contrações w_i, tais valores representam probabilidade e serão explicados posteriormente.

Tabela 5.1: IFS para o Triângulo de Sierpiński

w	a	b	c	d	e	f	p
1	0.5	0	0	0.5	1	1	0.33
2	0.5	0	0	0.5	1	50	0.33
3	0.5	0	0	0.5	50	50	0.34

Tabela 5.2: IFS para a Curva do Dragão

w	a	b	c	d	e	f	p
1	0.5	-0.5	0.5	0.5	0	0	0.5
2	-0.5	-0.5	0.5	-0.5	1	0	0.5

Tabela 5.3: IFS para a Curva de Koch

w	a	b	c	d	e	f	p
1	0.333	0	0	0.333	0	0	0.25
2	0.167	-0.289	0.289	0.167	0.333	0	0.25
3	0.167	0.289	-0.289	0.167	0.5	0.289	0.25
4	0.333	0	0	0.333	0.667	0	0.25

Tabela 5.4: IFS para o Dragão de Levy

w	a	b	c	d	e	f	p
1	0.5	-0.5	0.5	0.5	0	0	0.5
2	0.5	0.5	-0.5	0.5	0.5	0.5	0.5

Tabela 5.5: IFS para a Samambaia de Barnsley

w	a	b	c	d	e	f	p
1	0	0	0	0.16	0	0	0.01
2	0.85	0.04	-0.04	0.85	0	1.6	0.85
3	0.2	-0.26	0.23	0.22	0	1.6	0.07
4	-0.15	0.28	0.26	0.24	0	0.44	0.07

Tabela 5.6: IFS para a Árvore Fractal

w	a	b	c	d	e	f	p
1	0	0	0	0.5	0	0	0.05
2	0.42	-0.42	0.42	0.42	0	0.2	0.4
3	0.42	0.42	-0.42	0.42	0	0.2	0.4
4	0.1	0	0	0.1	0	0.2	0.15

Note que nas tabelas são fornecidos valores p_i associados às contrações w_i para $i = 1, 2, \cdots, N$, que representam probabilidades. Formalmente, para um IFS $\{X; w_n \mid n = 1, 2, \cdots, N\}$, existem N probabilidades $\{p_i \mid i = 1, 2, \cdots, N\}$ que satisfazem a propriedade de vetor de probabilidade:

$$\sum_{i=1}^{N} p_i = 1, \text{ com } p_i > 0.$$

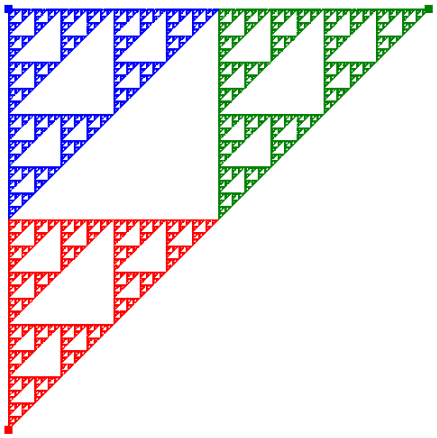
Os valores p_i desempenham um papel importante no contexto dos IFS em computação. Eles têm um papel crucial na geração das imagens dos atratores dos IFS, sendo aproximadamente determinados por:

$$p_i \approx \frac{|detA_i|}{\sum_{i=1}^{N} |detA_i|} = \frac{|a_i d_i - b_i c_i|}{\sum_{i=1}^{N} |a_i d_i - b_i c_i|},$$

onde $i = 1, 2, \cdots, N$. Note que p_i sempre será atribuído a valores pequenos e positivos, dependendo dos valores IFS para cada fractal.

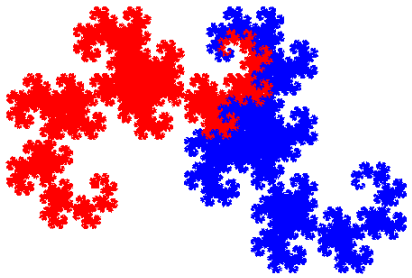
Para a geração das imagens dos atratores dos IFS, Barnsley (1988) propõe dois algoritmos: o Algoritmo Determinístico e o Algoritmo de Iteração Aleatória. Embora não sejam abordados em detalhes neste trabalho, ambos podem ser compreendidos mais aprofundadamente nos Capítulos 3 e 9 de Barnsley (1988). A seguir, são apresentadas algumas imagens geradas pelo software de uso público *IFS Construction Kit*, desenvolvido por *Larry Riddle*, que pode ser consultado em Riddle (2004–2022).

Figura 5.1: Triângulo de Sierpiński



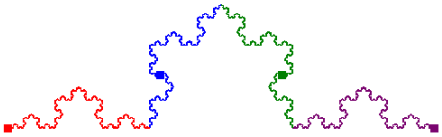
Fonte: O próprio autor

Figura 5.2: Curva do Dragão



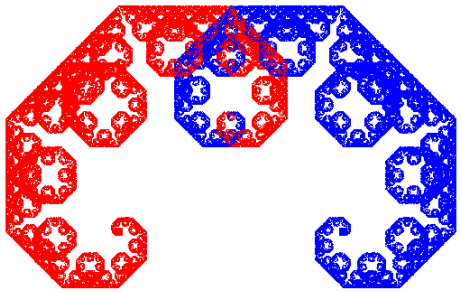
Fonte: O próprio autor

Figura 5.3: Curva de Koch



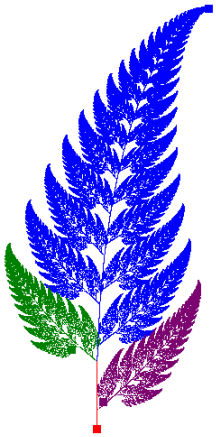
Fonte: O próprio autor

Figura 5.4: Dragão de Levy



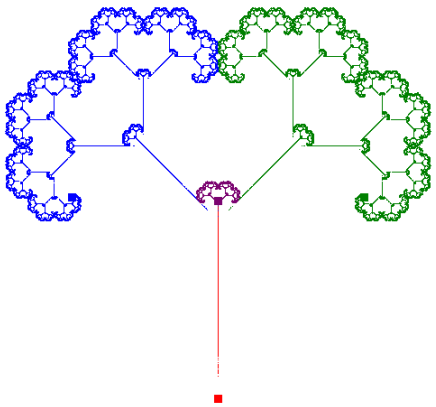
Fonte: O próprio autor

Figura 5.5: Samambaia de Barnsley



Fonte: O próprio autor

Figura 5.6: Árvore Fractal



Fonte: O próprio autor

5.1.2 O protocolo proposto

Considere um IFS da forma:

$$w_i(x,y) = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e_i \\ f_i \end{pmatrix},$$

onde $i = 1, 2, \cdots, N$, dependendo da quantidade de transformações afins utilizadas para gerar o fractal escolhido.

Para gerar o atrator fractal, isto é, a quantidade de iterações do sistema, é utilizado o operador de Hutchinson $W(B)$, $B \in \mathscr{H}(X)$:

$$W(B) = \bigcup_{i=1}^{N} w_i(B), \text{ para cada } B \in \mathscr{H}(X).$$

Reescrevendo e rearranjando o IFS em sua forma matricial e geral:

$$w_i(x,y) = \begin{pmatrix} a_i & 0 \\ 0 & b_i \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} c_i \\ d_i \end{pmatrix}, \tag{5.1}$$

onde $i = 1, 2, \cdots, N$. Uma coordenada aleatória Z dada pela tripla $(0, 0, 1)$ é adicionada com o objetivo de representar a translação do IFS, tornando a matriz 5.1 de ordem 3×3:

$$w_i(x,y,1) = \begin{pmatrix} a_i & 0 & c_i \\ 0 & b_i & d_i \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix},$$

onde $i = 1, 2, \cdots, N$.

Para calcular o operador de Hutchinson será feito um exemplo com quatro contrações w_1, w_2, w_3 e w_4, que é dado por $W = w_4 w_3 w_2 w_1$.

$$
\begin{aligned}
w_4 \cdot w_3 &= \begin{pmatrix} a_4 & 0 & c_4 \\ 0 & b_4 & d_4 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a_3 & 0 & c_3 \\ 0 & b_3 & d_3 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} a_4a_3 & 0 & a_4c_3 + c_4 \\ 0 & b_4b_3 & b_4d_3 + d_4 \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}
$$

$$
\begin{aligned}
w_4 \cdot w_3 \cdot w_2 &= \begin{pmatrix} a_4a_3 & 0 & a_4c_3 + c_4 \\ 0 & b_4b_3 & b_4d_3 + d_4 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & 0 & c_2 \\ 0 & b_2 & d_2 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} a_4a_3a_2 & 0 & a_4a_3c_2 + a_4c_3 + c_4 \\ 0 & b_4b_3b_2 & b_4b_3d_2 + b_4d_3 + d_4 \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}
$$

$$
\begin{aligned}
w_4 \cdot w_3 \cdot w_2 \cdot w_1 &= \begin{pmatrix} a_4a_3a_2 & 0 & a_4a_3c_2 + a_4c_3 + c_4 \\ 0 & b_4b_3b_2 & b_4b_3d_2 + b_4d_3 + d_4 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a_1 & 0 & c_1 \\ 0 & b_1 & d_1 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} a_4a_3a_2a_1 & 0 & a_4a_3a_2c_1 + a_4a_3c_2 + a_4c_3 + c_4 \\ 0 & b_4b_3b_2b_1 & b_4b_3b_2d_1 + b_4b_3d_2 + b_4d_3 + d_4 \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}
$$

A fim de simplicar a matriz $W = w_4w_3w_2w_1$, pode-se reescrever da seguinte maneira:

$$
W(x, y, 1) = \begin{pmatrix} A & 0 & C \\ 0 & B & D \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}, \text{ onde,}
$$

$A = a_4a_3a_2a_1$, $A \neq 1$;

$B = b_4b_3b_2b_1$, $B \neq 1$;

$C = a_4a_3a_2c_1 + a_4a_3c_2 + a_4c_3 + c_4$;

$D = b_4b_3b_2d_1 + b_4b_3d_2 + b_4d_3 + d_4$.

De um modo mais geral, é possível estabelecer o cálculo do Operador de Hutchinson para n contrações. Isso permite a utilização de fractais com IFS de n contrações, o que possibilita a incorporação de qualquer fractal gerado por um sistema de funções iteradas no método proposto. Vale ressaltar que ao realizar $W = w_n \cdots w_1$, obtém-se:

$$W = \begin{pmatrix} a_n \cdots a_1 & 0 & a_n \cdots a_2c_k + a_n \cdots a_3c_k + \cdots + a_{n+1} \cdots a_nc_k + c_k \\ 0 & b_n \cdots b_1 & b_n \cdots b_2d_k + b_n \cdots b_3d_k + \cdots + b_{n+1} \cdots b_nd_k + d_k \\ 0 & 0 & 1 \end{pmatrix}.$$

Onde,

- n é o número de contrações do sistema de funções iteradas;
- k é o número de elementos a_j que não aparecem nos termos da soma da entrada a_{13} da matriz W e o número de elementos b_j que não aparecem nos termos da soma da entrada a_{23} de W. Por exemplo, se $k = 1$, então $c_k = c_1$ ou $d_k = d_1$, se $k = 2$, então $c_k = c_2$ ou $d_k = d_2$ e assim por diante.

Logo, no protocolo proposto, é possível utilizar fractais com n contrações. Observe que o atrator do IFS é gerado realizando a n-ésima potência de W. Quanto maior for o número n de contrações do IFS utilizado para gerar o fractal, maior será a segurança do sistema.

Considere agora que Alice e Bob desejam estabelecer um canal seguro para se comunicarem em sigilo. De imediato, é necessário que ambos concordem em um fractal que será utilizado como um elemento primitivo, a fim de gerar suas chaves públicas a partir de suas chaves privadas previamente escolhidas. Portanto, eles devem seguir os seguintes passos:

1. De Alice para Bob:

   Como suas chaves privadas, Alice escolhe três números $x, y \in \mathbb{R}$ e $s \in \mathbb{Z}$, onde s é um número primo, em seguida, realiza o seguinte cálculo:

$$U = W^s(x, y, 1).$$

em seguida, envia U para Bob.

2. De Bob para Alice:

   De maneira análoga, Bob seleciona três números $x', y' \in \mathbb{R}$ e $r \in \mathbb{Z}$, onde r é um número primo, como suas chaves privadas, e realiza o cálculo:

$$U' = W^r(x, y, 1).$$

   em seguida, envia U' para Alice.

3. Gerando a chave pública

   Após Alice receber a chave U' de Bob, utilizando suas chaves privadas $x, y \in \mathbb{R}$ e $s \in \mathbb{Z}$ escolhidos previamente, realiza o seguinte cálculo para obter a chave pública K utilizada para se comunicarem em sigilo:

$$K = W^s \cdot U' \cdot (x, y, 1).$$

   Bob, em posse da chave U de Alice, realiza o procedimento análogo utilizando suas chaves privadas $x', y' \in \mathbb{R}$ e $r \in \mathbb{Z}$ escolhidas anteriormente:

$$K' = W^r \cdot U \cdot (x', y', 1).$$

   Ao final do procedimento, Alice e Bob compartilharão da mesma chave $K = K'$, sendo possível se comunicarem em um canal seguro.

Para ilustrar o protocolo ao leitor, segue um exemplo.

Exemplo 33. *Considere que Alice e Bob desejam se comunicar de forma sigilosa estabelecendo um canal seguro. Previamente, decidiram a utilização do fractal Curva de Koch, logo o IFS utilizado consistirá nos valores da Tabela 5.3.*

Com o fractal escolhido em consenso, o IFS é dado:

$$
\begin{aligned}
w_1(x,y) &= \begin{pmatrix} 0.333 & 0 \\ 0 & 0.333 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \\
w_2(x,y) &= \begin{pmatrix} 0.167 & -0.289 \\ 0.289 & 0.167 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0.333 \\ 0 \end{pmatrix}, \\
w_3(x,y) &= \begin{pmatrix} 0.167 & 0.289 \\ -0.289 & 0.167 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0.5 \\ 0.289 \end{pmatrix}, \\
w_4(x,y) &= \begin{pmatrix} 0.333 & 0 \\ 0 & 0.333 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0.667 \\ 0 \end{pmatrix}.
\end{aligned}
$$

Rearranjando e adicionando uma coordenada aleatória $(0, 0, 1)$ para representar translação, obtêm-se:

$$
\begin{aligned}
w_1(x,y,1) &= \begin{pmatrix} 0.333 & 0 & 0 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}, \\
w_2(x,y,1) &= \begin{pmatrix} 0.167 & 0 & 0.289 \\ 0 & -0.289 & 0.167 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}, \\
w_3(x,y,1) &= \begin{pmatrix} 0.167 & 0 & -0.289 \\ 0 & 0.289 & 0.167 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}, \\
w_4(x,y,1) &= \begin{pmatrix} 0.333 & 0 & 0 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}.
\end{aligned}
$$

Gerando a matriz de Hutchinson, por meio do operador de Hutchinson $W = w_4 w_3 w_2 w_1$:

$$W(x,y,1) = \begin{pmatrix} 0.003092583321 & 0 & -0.080165421 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix}.$$

Com a matriz W de Hutchinson determinada, Alice escolhe suas chaves privadas $x, y \in \mathbb{R}$ e $s \in \mathbb{Z}$, as quais:

$$x = 0.5,\ y = 1,5 \text{ e } s = 3.$$

Em seguida, gera $U = W^s(x,y,1)$:

$$\begin{aligned} U &= \begin{pmatrix} 0.003092583321 & 0 & -0.080165421 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix}^3 \\ &= \begin{pmatrix} 0.000000029577688302744511524 & 0 & -0.080414105951731617033 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix}, \end{aligned}$$

e envia U para Bob.

O processo para Bob é análogo para gerar $U' = W^r(x,y,1)$. Considerando que Bob escolheu os seguintes valores para $x', y' \in \mathbb{R}$ e $r \in \mathbb{Z}$:

$$x' = 0.75,\ y' = 1.25 \text{ e } r = 5.$$

$$\begin{aligned} U' &= \begin{pmatrix} 0.003092583321 & 0 & -0.080165421 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix}^5 \\ &= \begin{pmatrix} 0.000000000000282883128610881330 82 & 0 & -0.080414108330172300571 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix}, \end{aligned}$$

e envia U' para Alice.

Após Alice receber U', ela pode calcular sua chave pública $K = W^s \cdot U' \cdot (x, y, 1)$:

$$\begin{aligned} K &= W^s_{3\times 3} \cdot U'_{3\times 3} \cdot \begin{pmatrix} 0.5 \\ 1.5 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} -0.080414108330195048361783724085213377123850839538884026815 16 \\ 0.333 \\ 1 \end{pmatrix}. \end{aligned}$$

Em posse de U enviado por Alice, Bob faz o cálculo análogo para gerar sua chave pública $K' = W^r \cdot U \cdot (x', y', 1)$:

$$\begin{aligned} K' &= W^r_{3\times 3} \cdot U_{3\times 3} \cdot \begin{pmatrix} 0.75 \\ 1.25 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} -0.080414108330195048361783724085213377123850839538884026815 16 \\ 0.333 \\ 1 \end{pmatrix}. \end{aligned}$$

Note que $K = K'$, desta forma, Alice e Bob possuem uma chave em comum para comunicarem-se, sem ao menos publicar suas chaves privadas $x, y \in \mathbb{R}$, $s \in \mathbb{Z}$ e $x', y' \in \mathbb{R}$, $r \in \mathbb{Z}$.

Com o objetivo de realizar uma comparativa do método fractal de troca de chaves estabelecido, será feito uma sequência de exemplos com diferentes fractais, que seguem.

Exemplo 34. *Considere que dois envolvidos em um estabelecimento de canal seguro decidam utilizar o fractal Curva de Dragão, cujos valores estão dispostos na Tabela 5.2.*

Com o fractal escolhido, temos o seguinte IFS:

$$w_1(x,y) = \begin{pmatrix} 0.5 & -0.5 \\ 0.5 & 0.5 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

$$w_2(x,y) = \begin{pmatrix} -0.5 & -0.5 \\ 0.5 & -0.5 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Rearranjando e adicionando uma coordenada aleatória $(0, 0, 1)$ para representar translação, obtêm-se:

$$w_1(x,y,1) = \begin{pmatrix} 0.5 & 0 & 0.5 \\ 0 & -0.5 & 0.5 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix},$$

$$w_2(x,y,1) = \begin{pmatrix} -0.5 & 0 & 0.5 \\ 0 & -0.5 & -0.5 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}.$$

Gerando a matriz de Hutchinson, por meio do operador de Hutchinson $W = w_2 w_1$:

$$W(x,y,1) = \begin{pmatrix} -0.25 & 0 & 0.25 \\ 0 & 0.25 & -0.75 \\ 0 & 0 & 1 \end{pmatrix}.$$

Com a matriz W de Hutchinson determinada, Alice escolhe suas chaves privadas $x, y \in \mathbb{R}$ e $s \in \mathbb{Z}$, as quais:

$$x = 0.5,\ y = 1,5 \text{ e } s = 3.$$

Em seguida, gera $U = W^s(x, y, 1)$:

$$U = \begin{pmatrix} -0.25 & 0 & 0.25 \\ 0 & 0.25 & -0.75 \\ 0 & 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} -0.015625 & 0 & 0.203125 \\ 0 & 0.015625 & -0.984375 \\ 0 & 0 & 1 \end{pmatrix},$$

e envia U para Bob.

O processo para Bob é análogo para gerar $U' = W^r(x, y, 1)$. Considerando que Bob escolheu os seguintes valores para $x', y' \in \mathbb{R}$ e $r \in \mathbb{Z}$:

$$x' = 0.75,\ y' = 1.25 \text{ e } r = 5.$$

$$U' = \begin{pmatrix} -0.25 & 0 & 0.25 \\ 0 & 0.25 & -0.75 \\ 0 & 0 & 1 \end{pmatrix}^5 = \begin{pmatrix} -0.0009765625 & 0 & 0.2001953125 \\ 0 & 0.0009765625 & -0.9990234375 \\ 0 & 0 & 1 \end{pmatrix},$$

e envia U' para Alice.

Após Alice receber U', ela pode calcular sua chave pública $K = W^s \cdot U' \cdot (x, y, 1)$:

$$K = W^s_{3\times3} \cdot U'_{3\times3} \cdot \begin{pmatrix} 0.5 \\ 1.5 \\ 1 \end{pmatrix} = \begin{pmatrix} 0.20000457763671875 \\ -0.99996185302734375 \\ 1 \end{pmatrix}.$$

Em posse de U enviado por Alice, Bob faz o cálculo análogo para gerar sua chave pública $K' = W^r \cdot U \cdot (x', y', 1)$:

$$K' = W^r_{3\times3} \cdot U_{3\times3} \cdot \begin{pmatrix} 0.75 \\ 1.25 \\ 1 \end{pmatrix} = \begin{pmatrix} 0.20000457763671875 \\ -0.99996185302734375 \\ 1 \end{pmatrix}.$$

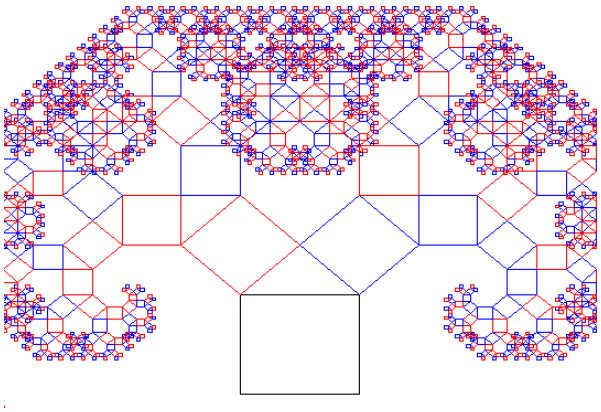
Conforme mencionado no início deste capítulo, é possível gerar diversos fractais usando IFS. Um exemplo de fractal é a árvore pitagórica, que é gerada por um processo iterativo envolvendo quadrados e triângulos retângulos. Devido à flexibilidade na angulação dessas formas geométricas, o fractal pode assumir várias representações. Na forma mais comum, os quadrados são dispostos em um ângulo de 45º, e isso pode ser alcançado usando o seguinte IFS com 3 contrações:

Tabela 5.7: IFS para a Árvore Pitagórica 45º

w	a	b	c	d	e	f	p
1	0.5	-0.5	0.5	0.5	0	1	0.25
2	0.5	0.5	-0.5	0.5	0.5	1.5	0.25
3	1	0	0	1	0	0	0.5

Com cerca de 10 iterarações do IFS acima, é possível gerar o seguinte fractal:

Figura 5.7: Árvore Pitagórica 45º



Fonte: O próprio autor

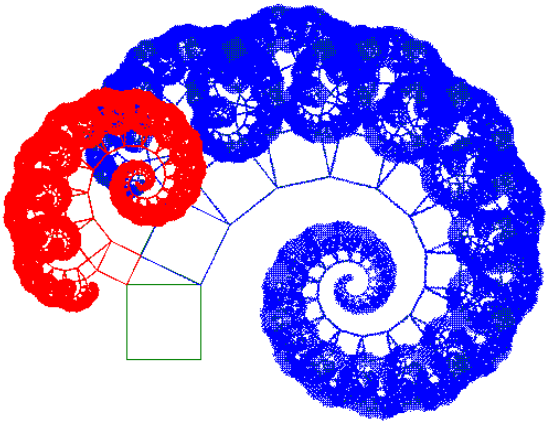
Alterando a angulação dos quadrados e triângulos retângulos para 64º, obtêm-se o seguinte IFS:

Tabela 5.8: IFS para a Árvore Pitagórica 64º

w	a	b	c	d	e	f	p
1	0.192	-0.394	0.394	0.192	0	1	0.096
2	0.808	0.394	-0.394	0.808	0.192	1.394	0.404
3	1	0	0	1	0	0	0.5

Com cerca de 30 iterações do IFS acima, é possível gerar o seguinte fractal:

Figura 5.8: Árvore Pitagórica 64º



Fonte: O próprio autor

Note que uma pequena alteração na angulação resulta em valores significativamente diferentes para o IFS, demonstrando a aleatoriedade do fractal.

Exemplo 35. *Considere que Alice e Bob queiram estabelecer um canal seguro de comunicação utilizando a Árvore Pitagórica com 64º de angulação como fractal.*

Com o fractal escolhido, temos o seguinte IFS:

$$w_1(x,y) = \begin{pmatrix} 0.192 & -0.394 \\ 0.394 & 0.192 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

$$w_2(x,y) = \begin{pmatrix} 0.808 & 0.394 \\ -0.394 & 0.808 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0.192 \\ 1.394 \end{pmatrix},$$

$$w_3(x,y) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Rearranjando e adicionando uma coordenada aleatória $(0,0,1)$ para representar translação, obtêm-se:

$$w_1(x,y,1) = \begin{pmatrix} 0.192 & 0 & 0.394 \\ 0 & -0.394 & 0.192 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix},$$

$$w_2(x,y,1) = \begin{pmatrix} 0.808 & 0 & -0.394 \\ 0 & 0.394 & 0.808 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix},$$

$$w_3(x,y,1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}.$$

Gerando a matriz de Hutchinson, por meio do operador de Hutchinson $W = w_3 w_2 w_1$:

$$W(x,y,1) = \begin{pmatrix} 0.155136 & 0 & -0.075648 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Com a matriz W de Hutchinson determinada, Alice escolhe suas chaves privadas $x, y \in \mathbb{R}$ e $s \in \mathbb{Z}$, as quais:

$$x = 0.5,\ y = 1,5 \text{ e } s = 3.$$

Em seguida, gera $U = W^s(x,y,1)$:

$$U = \begin{pmatrix} 0.155136 & 0 & -0.075648 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 0.003733685803155456 & 0 & -0.089204362046865408 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

e envia U para Bob.

O processo para Bob é análogo para gerar $U' = W^r(x,y,1)$. Considerando que Bob escolheu os seguintes valores para $x', y' \in \mathbb{R}$ e $r \in \mathbb{Z}$:

$$x' = 0.75,\ y' = 1.25 \text{ e } r = 5.$$

$$U' = \begin{pmatrix} 0.155136 & 0 & -0.075648 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}^5$$

$$= \begin{pmatrix} 0.000089859282672523479588274176 & 0 & -0.089530625432003717691623866368 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

e envia U' para Alice.

Após Alice receber U', ela pode calcular sua chave pública $K = W^s \cdot U' \cdot (x, y, 1)$:

$$K = W^s_{3\times3} \cdot U'_{3\times3} \cdot \begin{pmatrix} 0.5 \\ 1.5 \\ 1 \end{pmatrix} = \begin{pmatrix} -0.089538473518824511028506308512118517054234951 68 \\ 1 \\ 1 \end{pmatrix}.$$

Em posse de U enviado por Alice, Bob faz o cálculo análogo para gerar sua chave pública $K' = W^r \cdot U \cdot (x', y', 1)$:

$$K' = W^r_{3\times3} \cdot U_{3\times3} \cdot \begin{pmatrix} 0.75 \\ 1.25 \\ 1 \end{pmatrix} = \begin{pmatrix} -0.089538473518824511028506308512118517054234951 68 \\ 1 \\ 1 \end{pmatrix}.$$

Exemplo 36. *Alterando a angulação do fractal para 11º, obtemos um fractal ainda com 3 contrações, porém com valores diferentes, observe:*

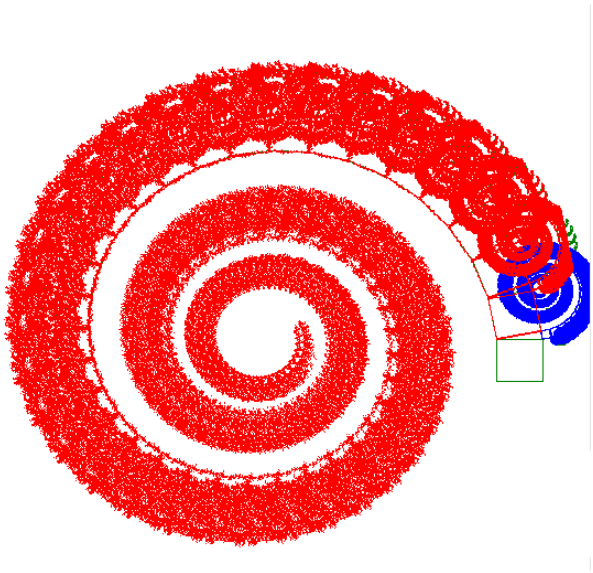
$$w_1(x, y) = \begin{pmatrix} 0.964 & -0.187 \\ 0.187 & 0.964 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

$$w_2(x, y) = \begin{pmatrix} 0.036 & 0.187 \\ -0.187 & 0.036 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0.964 \\ 1.187 \end{pmatrix},$$

$$w_3(x,y) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Com cerca de 100 iterações, obtém-se o seguinte fractal:

Figura 5.9: Árvore Pitagórica 11º



Fonte: O próprio autor

Dado o IFS em sua forma matricial, rearranjando e adicionando uma coordenada aleatória $(0,0,1)$ para representar translação, segue:

$$w_1(x,y,1) = \begin{pmatrix} 0.964 & 0 & 0.187 \\ 0 & -0.187 & 0.964 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix},$$

$$w_2(x,y,1) = \begin{pmatrix} 0.036 & 0 & -0.187 \\ 0 & 0.187 & 0.036 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix},$$

$$w_3(x,y,1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}.$$

Gerando a matriz de Hutchinson, por meio do operador de Hutchinson $W = w_3 w_2 w_1$:

$$W(x,y,1) = \begin{pmatrix} 0.034704 & 0 & -0.180268 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Com a matriz W de Hutchinson determinada, Alice escolhe suas chaves privadas $x, y \in \mathbb{R}$ e $s \in \mathbb{Z}$, as quais:

$$x = 0.255,\ y = 1,245 \text{ e } s = 5.$$

Em seguida, gera $U = W^s(x,y,1)$:

$$U = \begin{pmatrix} 0.034704 & 0 & -0.180268 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}^5 =$$

$$\begin{pmatrix} 0.000000050338199005510342017 & 0 & -0.18674892564108163886 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

e envia U para Bob.

O processo para Bob é análogo para gerar $U' = W^r(x,y,1)$. Considerando que Bob escolheu os seguintes valores para $x', y' \in \mathbb{R}$ e $r \in \mathbb{Z}$:

$$x' = 0.233,\ y' = 1.566 \text{ e } r = 7.$$

$$\begin{aligned} U' &= \begin{pmatrix} 0.034704 & 0 & -0.180268 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}^7 \\ &= \begin{pmatrix} 0.000000000060625696730000061476 & 0 & -0.18674893503036491074 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \end{aligned}$$

e envia U' para Alice.

Após Alice receber U', ela pode calcular sua chave pública $K = W^s \cdot U' \cdot (x, y, 1)$:

$$K = W^s_{3\times3} \cdot U'_{3\times3} \cdot \begin{pmatrix} 0.255 \\ 1.245 \\ 1 \end{pmatrix} = \begin{pmatrix} -0.18674893504168669922 \\ 1 \\ 1 \end{pmatrix}.$$

Em posse de U enviado por Alice, Bob faz o cálculo análogo para gerar sua chave pública $K' = W^r \cdot U \cdot (x', y', 1)$:

$$K' = W^r_{3\times3} \cdot U_{3\times3} \cdot \begin{pmatrix} 0.233 \\ 1.566 \\ 1 \end{pmatrix} = \begin{pmatrix} -0.18674893504168669922 \\ 1 \\ 1 \end{pmatrix}.$$

5.2 Uma análise comparativa

Com base nas considerações de Al-Saidi (2014), no protocolo proposto e na exemplificação com vários fractais, esta seção tem como objetivo realizar uma comparação entre os dados dos exemplos, a fim de analisar o nível de segurança do método, o custo computacional e a eficácia. Isso será feito considerando a quantidade de contrações que compõem o IFS dos fractais, a variação na escolha das chaves privadas $s \in \mathbb{Z}$ e $x, y \in \mathbb{R}$ e a performance do sistema. Essa análise proporcionará uma visão clara e reflexiva sobre o protocolo fractal de troca de chaves.

5.2.1 De acordo com a quantidade de contrações do IFS

Note que nos exemplos 33, 34 e 35, a quantidade de contrações de cada IFS é de 4, 2 e 3, respectivamente. Com base nessa análise, é possível realizar uma comparação entre as estruturas geradas durante a execução dos cálculos do método criptográfico.

Denotando as matrizes W de Hutchinson dos Exemplos 33, 34 e 35 por W_{34}, W_{35} e W_{36} respectivamente, ao realizar um recorte, tem-se:

$$W_{34}(x,y,1) = \begin{pmatrix} 0.003092583321 & 0 & -0.080165421 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix},$$

$$W_{35}(x,y,1) = \begin{pmatrix} -0.25 & 0 & 0.75 \\ 0 & 0.25 & 0.75 \\ 0 & 0 & 1 \end{pmatrix},$$

$$W_{36}(x,y,1) = \begin{pmatrix} 0.155136 & 0 & 0.075648 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Observe que, devido à matriz de Hutchinson ser gerada pelo produto matricial das contrações que compõem o IFS, quanto maior for a quantidade de contrações utilizadas para gerar um determinado fractal, maior será a quantidade de casas decimais nas entradas da matriz. Portanto, de acordo com Al-Saidi (2014), pode-se concluir que o fator de segurança do sistema é beneficiado, uma vez que qualquer erro de truncamento por parte de um invasor acarretará dificuldades na quebra do código.

5.2.2 De acordo com a chave privada $s \in \mathbb{Z}$

Pode-se ainda notar diferenças quando a chave privada s, que é um número inteiro primo, é escolhida com uma grande quantidade de dígitos. Com base em Al-Saidi (2014), durante a execução do método, quanto maior o número primo escolhido, maior é o fator de segurança do sistema. Observe o exemplo 33, em que é tomado $s = 3$:

$$\begin{aligned} W_{34} &= \begin{pmatrix} 0.003092583321 & 0 & -0.080165421 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix}^3 \\ &= \begin{pmatrix} 0.000000029577688302744511524 & 0 & -0.080414105951731617033 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

Observe agora quando $s = 13$:

$$W_{34} = \begin{pmatrix} 0.003092583321 & 0 & -0.080165421 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix}^{13}$$
$$= \begin{pmatrix} 2.3668913418741554658 \times 10^{-33} & 0 & -0.080414108330195048363 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix}.$$

Mais ainda, quando $s = 97$:

$$W_{34} = \begin{pmatrix} 0.003092583321 & 0 & -0.080165421 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix}^{97}$$
$$= \begin{pmatrix} 3.6406313358890869803 \times 10^{-244} & 0 & -0.080414108330195048363 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix}.$$

Observe que o número primo $s = 97$ ainda é consideravelmente pequeno em um sistema considerado seguro. Segundo Al-Saidi (2014), são utilizados números primos com cerca de 120 dígitos. É importante observar que quanto maior a chave privada s for, maior será a quantidade de casas decimais na entrada a_1 da matriz de Hutchinson.

Observe agora, quando s tem apenas 6 dígitos, $s = 104729$:

$$W_{34} = \begin{pmatrix} 0.003092583321 & 0 & -0.080165421 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix}^{104729}$$
$$= \begin{pmatrix} 7.428059900 \times 10^{-262837} & 0 & -0.080414108330195048363 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix}.$$

Por fim, conforme indicado por Al-Saidi (2014), observe quando s possui 157 dígitos, $s = 6864797$
$660130609714981900799081393217269435300143305409394463459185543183397656052122$
$559640661454554977296311391480858037121987999716643812574028291115057151$.

Esse número primo é conhecido como o 13º *Primo de Mersenne*. Ele recebe esse nome em homenagem ao matemático, teórico musical, teólogo e filósofo francês Marin Mersenne (1588 - 1648). Os números primos de Mersenne são números da forma $M_n = 2^n - 1$, em que n é um número primo pertencente ao conjunto dos números naturais.

Após a grandiosa contribuição de Mersenne, diversos matemáticos utilizaram os resultados desse célebre matemático para descobrir muitos números primos com um grande número de casas decimais.

Para fins de simplificação, será exibido o número em sua notação científica aproximada:

$$W_{34} = \begin{pmatrix} 0.003092583321 & 0 & -0.080165421 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix}^t$$

onde, $t = 6.864797660130609714981900799081393217269435300143305409394 4 \times 10^{156}$. Resultando em:

$$W_{34} = \begin{pmatrix} 1.28623849848907 \times 10^z & 0 & -0.080414108330195 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix},$$

onde, $z = 172284357170636576280279742097425485335538287523688568471778485315306501602263753173319079509926967743011403057983068391555372235989707190770393811007535327 70$.

Logo, note que o número de casas decimais aumenta drasticamente quando s possui mais de 120 dígitos. Além disso, não é viável descartar as casas decimais, uma vez que é necessário armazenar esses elementos para levar em consideração possíveis erros de truncamento e arredondamento realizados pelo invasor durante uma tentativa de quebra do processo criptográfico.

5.2.3 De acordo com as chaves privadas x e $y \in \mathbb{R}$

O mesmo ocorre para as chaves privadas x e y, que são representadas por números reais. Ao trabalhar no intervalo infinito $(0, 1)$, é possível utilizar chaves privadas x e y com um número infinito de casas decimais. Isso proporciona um aumento significativo no fator de segurança do sistema, pois, ao calcular a chave pública K, a quantidade de casas decimais nas entradas da matriz aumentam exponencialmente.

Realizando um recorte dos valores do Exemplo 33, tem-se como Matriz de Hutchinson:

$$W_{34} = \begin{pmatrix} 0.003092583321 & 0 & -0.080165421 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix}.$$

Além disso, temos as chaves privadas escolhidas por Alice:

$$x = 0.5,\ y = 1.5 \text{ e } s = 3.$$

Por fim, a matriz $U = W^s(x, y, 1)$:

$$\begin{aligned} U &= \begin{pmatrix} 0.003092583321 & 0 & -0.080165421 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix}^3 \\ &= \begin{pmatrix} 0.000000029577688302744511524 & 0 & -0.080414105951731617033 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix}, \end{aligned}$$

Para determinar sua chave pública K, Alice utiliza a matriz U' gerada por Bob, que é dada por:

$$
\begin{aligned}
U' &= \begin{pmatrix} 0.003092583321 & 0 & -0.080165421 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix}^5 \\
&= \begin{pmatrix} 0.000000000000282883128610881330 82 & 0 & -0.080414108330172300571 \\ 0 & 0 & 0.333 \\ 0 & 0 & 1 \end{pmatrix}.
\end{aligned}
$$

Assim, Alice gera sua chave pública K através da seguinte expressão:

$$
\begin{aligned}
K &= W^s_{3\times 3} \cdot U'_{3\times 3} \cdot \begin{pmatrix} 0.5 \\ 1.5 \\ 1 \end{pmatrix} \\
&= \begin{pmatrix} -0.080414108330195048361783724085213377123850839538884026815 16 \\ 0.333 \\ 1 \end{pmatrix}.
\end{aligned}
$$

Os valores escolhidos $x = 0.5$ e $y = 1.5$ são números pequenos. Segundo Al-Saidi (2014) e Al-Saidi; M. R. M. Said; A. M. Ahmed (2011), O sistema é considerado seguro quando são utilizados valores de x e y no intervalo $(0, 1)$, com cerca de 120 dígitos após a vírgula.

Observe a chave pública K quando se utiliza as chaves x e y com cerca de 120 casas decimais:

$x = 0.525489205869525489205869525489205869525489205869525489205869525489$
$205869525489205869525489205869525489205869525489205869,$

$y = 0.214785367514568743968579615757142789214785367514214785367514214785$
$367514214785367514214785367514214785367514214785367514.$

$$
K = U_{3\times 3} \cdot U'_{3\times 3} \cdot \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} -8.041411 \times 10^{-326} \\ 0.333 \\ 1 \end{pmatrix}
$$

Observe que o número de casas decimais aumenta significativamente com números x e y de 120 dígitos. No entanto, realizar um grande aumento na quantidade de dígitos dos números x, y e s como chaves privadas e apropriar-se de fractais com um grande número de contrações, possibilitaria a realização de muitos testes e aumentaria consideravelmente a segurança do sistema.

5.2.4 Comparação de performance

Nos trabalhos de Al-Saidi (2014) e Al-Saidi; M. R. M. Said; A. M. Ahmed (2011), a simulação do tempo de geração de chaves utilizando o fractal Triângulo de Sierpinski foi executada pela autora utilizando a linguagem de programação Java, por meio do aplicativo "NetBeans IDE 6.8". O experimento foi conduzido em um computador com as seguintes configurações: processador Intel Core 2 Duo, 3.0GHz e 2GB de memória RAM. Os resultados obtidos em termos de tempo em segundos foram os seguintes:

Figura 5.10: Comparação de Performance - Java Net-Beans IDE 6.8

	Fractal key agreement		**DH protocol**	
No. of Bits	Generating time	Key agreement time	Generating time	Key agreement time
128	57	0	13	10
256	90	0	50	12
512	103	0	73	29
1024	152	4	139	164
2048	350	9	267	1124
4096	891	14	704	8235

Fonte: Retirado de Al-Saidi; M. R. M. Said; A. M. Ahmed (2011)

Entretanto, ao utilizar a linguagem de programação Python 3.11 com o auxílio do aplicativo "Visual Studio Code" para realizar os cálculos de geração das chaves públicas, utilizando um computador com processador AMD Ryzen 5 3500U 3.0GHz e 8GB de memória RAM, em termos de tempo em segundos foram obtidos os seguintes resultados:

Figura 5.11: Comparação de Performance - Python 3.11

Método Fractal	
Nº de Dígitos	Tempo de Geração de Chave Pública
128	0.059440 segundos
256	0.097465 segundos
512	0.191955 segundos
1024	0.360122 segundos
2048	0.814773 segundos
4096	1.632744 segundos

Fonte: O próprio autor

Considerando apenas o tempo de geração das chaves para esta análise, é possível fazer duas comparações de desempenho entre o sistema implementado em Java e Python

Com base nos valores disponibilizados por Al-Saidi; M. R. M. Said; A. M. Ahmed (2011), o tempo de geração das chaves utilizando Java foi de 57 segundos para valores com 128 dígitos, 90 segundos para 256 dígitos, 103 segundos para 512 dígitos, 152 segundos para 1024 dígitos, 350 segundos para 2048 dígitos e 891 segundos para 4096 dígitos.

Ao utilizar a linguagem Python, os tempos obtidos foram de 0.059 segundos para valores com 128 dígitos, 0.097 segundos para 256 dígitos, 0.192 segundos para 512 dígitos, 0.360 segundos para 1024 dígitos, 0.814 segundos para 2048 dígitos e, por fim, 1.63 segundos para 4096 dígitos.

Ao analisar o sistema na maior quantidade de dígitos, o método de geração de chaves implementado em Python levou aproximadamente 0.18% do tempo necessário para gerar as chaves em Java, o que representa uma diferença drástica no tempo de execução.

É importante ressaltar as diferenças entre os computadores utilizados, principalmente em relação ao processador e à memória RAM, que podem ter impacto no tempo de geração das chaves.

A segunda comparação envolve o método fractal de troca de chaves implementado em Python e o protocolo Diffie-Hellman implementado em Java. Ao analisar as tabelas, nota-se uma diferença significativa no tempo de geração das chaves, embora seja menor

em comparação com o método fractal apresentado por Al-Saidi; M. R. M. Said; A. M. Ahmed (2011).

Uma análise completa do sistema envolveria a execução do protocolo completo, incluindo a geração de chaves e a transferência entre os participantes utilizando as duas linguagens de programação. No entanto, essa análise ultrapassa o escopo deste trabalho e poderia ser objeto de estudo em trabalhos futuros.

Bibliografia

Al-Saidi; M. R. M. Said; A. M. Ahmed, N. M. G. Efficiency analysis for public key systems based on fractal functions. *Journal of Computer Science*, v. 7, n. 4, p. 526–532, 2011. ISSN 1549-3636.

AL-SAIDI, N. M. G. An improved key agreement protocol based on fractal theory. *Eng. and Tech Journal*, v. 32, n. 1, 2014.

Andria; R. Gondim; R. Salomão, S. *Introdução à Criptografia com Curvas Elípticas*. [S.l.]: IMPA, 2019.

Arrowsmith; C. M. Place, D. K. *An Introduction to Dynamical Systems*. [S.l.]: Cambridge University Press, 1990.

Baraviera; F. M. Branco, A. T. *Sistemas Dinâmicos: uma primeira visão*. [S.l.]: Campinas - SP: UNICAMP/IMECC, 2012.

BARNSLEY, M. F. *Fractals Everywhere, 1a. edição*. [S.l.]: Academic Press, Dublin, 1988.

COUTINHO, S. C. *Criptografia*. [S.l.]: IMPA, 2015.

DOMINGUES, H. H. *Espaços métricos e introdução à topologia*. [S.l.]: Atual, 1982.

GONçALVES, A. *Introdução à Álgebra, 6a. edição*. [S.l.]: IMPA, 2017.

Hasselblatt; A. Katok, B. *A First Course in Dynamics With a Panorama of Recent Developments*. [S.l.]: Cambridge University Press, 2003.

LIMA, E. L. *Espaços Métricos, 6a. edição*. [S.l.]: IMPA, 2020.

PELLEGRINI, J. C. *Introdução à Criptografia e seus Fundamentos*. [S.l.]: Notas de aula, 2019.

REIS, V. L. M. *Criptografia, Segurança de Dados e Privacidade: Até que ponto pode-se confiar na discrição dos computadores?* Dissertação — UFRJ, Rio de Janeiro - RJ, 1989.

RIDDLE, L. *IFS Construction Kit Home*. 2004–2022. <https://larryriddle.agnesscott.org/ifskit/index.htm>.

ROSS, S. *Probabilidade: um curso moderno com aplicações*. [S.l.]: Bookman, 2010.

SANTOS, J. P. O. *Introdução à teoria dos números, 3a. edição*. [S.l.]: IMPA, 2018.

SILVA, V. B. *Números Primos e Criptografia: do Conceito ao Sistema RSA*. Dissertação — Universidade Federal do Tocantins, Arraias - TO, 2019.

Stinson; M. B. Paterson , D. R. *Cryptography: Theory and Practice, 4º edition*. [S.l.]: CRC Press, 2019.