# CÓDIGOS VIA ESPAÇOS SHIFT

EnCoRI - 2023

Tatiana Miguel Rodrigues
Unesp - Bauru

**Definição 1.** *Se $\mathcal{A}$ é um alfabeto finito, então o $\mathcal{A}$-shift completo é a coleção de todas as sequências bi-infinitas de simbolos de $\mathcal{A}$. O $r$-shift completo (ou $r$-shift) é o shift completo sobre o alfabeto $\mathcal{A} = \{0, 1, 2, \cdots, r-1\}$.*

$$\mathcal{A}^{\mathbb{Z}} = \{x = (x_i)_{i \in \mathbb{Z}};\ x_i \in \mathcal{A},\ \forall i \in \mathbb{Z}\}.$$

**Definição 3.** *O tamanho de um bloco $u$ é o número de símbolos que ele contém, denotado por $|u|$. Se $u = a_1a_2\cdots a_k$ é um bloco não vazio, então $|u| = k$, enquanto $|\epsilon| = 0$.*

**Definição 4.** *Um $k$-bloco é simplesmente um bloco de tamanho $k$. O conjunto de todos os $k$-blocos sobre $\mathcal{A}$ é denotado por $\mathcal{A}^k$. Um sub-bloco (ou sub-palavra) de $u = a_1a_2\cdots a_k$ é um bloco da forma*

$$a_ia_{i+1}\cdots a_j, \text{ em que } 1 \leq i \leq j \leq k.$$

*Por convenção, o bloco vazio $\epsilon$ é sub-bloco de todo bloco.*

**Definição 5.** *Se $x \in \mathcal{A}^{\mathbb{Z}}$ e $i \leq j$, então denotamos o bloco de coordenadas em $x$ da posição $i$ até a posição $j$ por $x_{[i,j]} = x_i x_{i+1} \cdots x_j$. Se $i > j$, então $x_{[i,j]} = \epsilon$ (bloco vazio).*

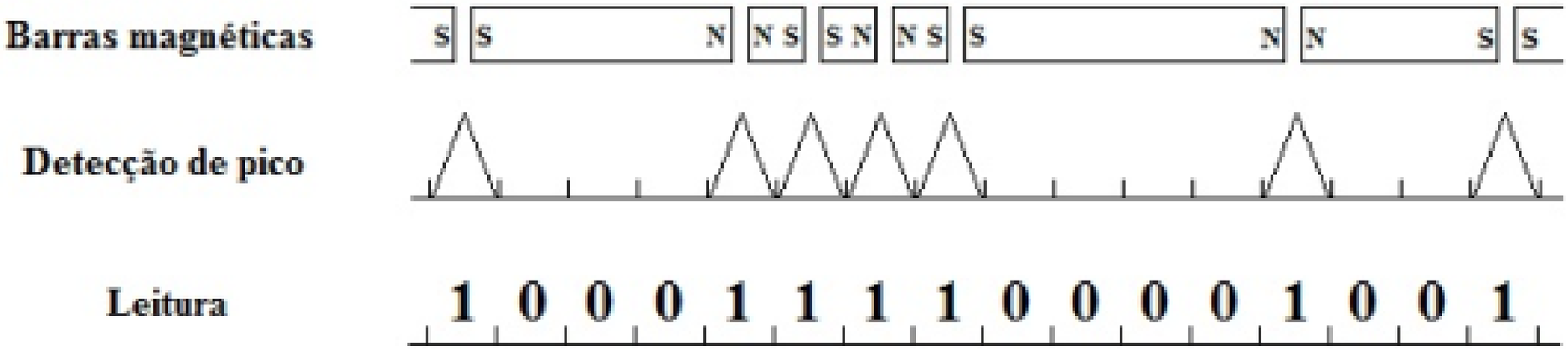
**Definição 6.** *Se $x \in \mathcal{A}^{\mathbb{Z}}$ e $w$ é um bloco sobre $\mathcal{A}$, dizemos que $w$ ocorre em $x$ se existem indices $i$ e $j$ tais que $w = x_{[i,j]}$.*

**Definição 7.** *Seja $\mathcal{F}$ uma coleção de blocos sobre $\mathcal{A}$ que serão chamados de blocos proibidos. Para qualquer $\mathcal{F}$, definimos $\mathsf{X}_{\mathcal{F}}$ como o subconjunto das sequências em $\mathcal{A}^{\mathbb{Z}}$ que não contém qualquer bloco em $\mathcal{F}$.*

**Definição 8.** *Um Espaço Shift é um subconjunto $X$ de um shift completo $\mathcal{A}^{\mathbb{Z}}$ tal que $X = \mathsf{X}_{\mathcal{F}}$, para alguma coleção $\mathcal{F}$ de blocos proibidos sobre $\mathcal{A}$.*

**Definição 9.** *Para cada par* $(d, k)$ *de inteiros não negativos, com* $d \leq k$, *existe um Espaço Shift chamado um* $(d, k)$ *espaço shift de tamanho limitado, denotado por* $\mathsf{X}(d, k)$, *e definido pelas restrições de que os* $1$*'s ocorrem infinitamente em cada direção e existem no mínimo* $d$ $0$*'s e no máximo* $k$ $0$*'s entre sucessivos* $1$*'s.*

**Definição 10.** *Um Espaço Shift do tipo finito é aquele que pode ser descrito por um conjunto finito de blocos proibidos, isto é,* $X = \mathsf{X}_{\mathcal{F}}$, *em que* $\mathcal{F}$ *é um conjunto finito.*


Barras magnéticas
S S N N S S N N S S N S N
Detecção de pico
Leitura
1 0 0 0 1 1 1 1 0 0 0 0 1 0 0 1

Baseados nas características físicas do meio magnético e na sensibilidade do equipamento eletrônico, cada sistema tem uma distância mínima de separação $\Delta$ entre mudanças de polaridade com o intuito de evitar a interferência entre símbolos

No método acima, o tamanho da *janela de detecção* deve ser no mínimo $\Delta$, isto é, $L \geq \Delta$, uma vez que 1's podem ocorrer em células adjacentes. Usando esquemas em que 1's são separados por pelo menos $d$ 0's, podem ser usadas janelas de detecção de tamanho $L = \Delta/d + 1$ e armanezar mais dados em cada faixa.

O bloco $10^n1 = 1000\cdots0001$ é lido como 2 pulsos separados por um intervalo de tempo, e o tamanho deste intervalo é $(n+1)/L$, em que $n$ é o número de 0's. Qualquer maneira de medir este intervalo pode resultar em um valor inexato para $n$. Esta falha é corrigida por um "loop" de reação toda vez que um pulso é lido, este "loop" é chamado de *Pulso de tempo*.

## Código FM

Um código FM (Frequency Modulation) é um esquema que controla o *Pulso de tempo* com a simples idéia de inserir um bit 1 entre cada para de bits de dados (0 e 1).

**Exemplo 2.** *Se a palavra-código original é* 10000011 *então o código FM associado é:*

$$\underline{1}1\underline{0}1\underline{0}1\underline{0}1\underline{0}1\underline{1}1\underline{1}$$

*O número de zeros da palavra é o número de vezes que tivemos a mudança de* 1 *para* 0*, deixando claro que na palavra acima não existe diferença entre* $\underline{1}$ *e* 1*. A palavra original é recuperada ignorando-se os* $\underline{1}$*'s.*

**Proposição 1.** *O código FM é um espaço* $\mathsf{X}(0,1)$ *shift do tipo finito.*

**Demonstração**: Da Definição 9 segue que o código FM é um $\mathsf{X}(0,1)$, e é do tipo finito pois $\mathsf{X}(0,1) = \mathsf{X}_{\mathcal{F}}$, em que $\mathcal{F} = \{00\}$.

Com o código FM, $n$ bits de dados são codificados em $2n$ bits, então podem ser armazenados em um pedaço de faixa de tamanho $2n\Delta$. Com relação ao tamanho da faixa este código pode ser melhorado pelo código MFM.

## Código MFM

Se sequências codificadas possuem ao menos $d$ 0's entre sucessivos 1's, então podemos encolher a janela de detecção e o tamanho da célula para $L = \Delta/(d+1)$ e ainda manter separação suficiente entre pulsos para evitar a interferência entre símbolos. Um método que usa esta ideia é chamado código MFM (Modified Frequency Modulation). Este código insere um $\underline{0}$ entre cada par de bits, a menos que ambos os bits sejam 0, neste caso é inserido um $\underline{1}$.

**Exemplo 3.** *Se a palavra-código original é* 10000011 *então o código MFM associado é:*

$$\underline{0}1\underline{0}0\underline{1}0\underline{1}0\underline{1}0\underline{0}\underline{1}0\underline{1}$$

**Proposição 2.** *O código MFM é um espaço* $\mathsf{X}(1,3)$ *shift do tipo finito.*

**Demonstração**: Devemos mostrar que em qualquer sequência no código MFM o número de 0's entre sucessivos 1's é no mínimo 1 e no máximo 3. Como o código MFM insere um 0 entre cada par de bits, segue que em qualquer sequência não há 1's vizinhos, logo entre sucessivos 1's há no mínimo um 0. Podemos verificar também que existem sequências com três 0's entre sucessivos 1's, por exemplo, ao bloco 101 associamos o bloco $\underline{0}1\underline{0}0\underline{1}$. Suponhamos que existam sequências com quatro 0's entre sucessivos 1's, assim teríamos as seguintes configurações: $\cdots 1\underline{0}0\underline{0}1\cdots$ ou $\cdots 1\underline{0}0\underline{0}1\underline{\cdots}$, que não ocorrem, uma vez que o código associado ao bloco 00 seria $0\underline{1}0$ e não $0\underline{0}0$, assim, o número máximo de 0's entre sucessivos 1's é três. Portanto, o código MFM é um espaço $\mathsf{X}(1,3)$ shift, e é do tipo finito pois $\mathsf{X}(1,3) = \mathsf{X}_{\mathcal{F}}$, em que $\mathcal{F} = \{11, 0000\}$.

No código MFM, como $d = 1$, pulsos não podem ocorrer em células adjacentes, assim usam-se células de tamanho $L = \Delta/2$ e mantêm-se a separação suficiente entre pulsos. Assim como no código FM, no código MFM $n$ bits de dados são codificados em $2n$ bits e podem ser armazenados num espaço de tamanho $2n\Delta/2 = n\Delta$, exatamente metade do espaço requerido no código FM, para a mesma informação. Mas este ganho não vem de graça, pois percebe-se que alguns dos 1's nas sequências do MFM são usados para a sincronização do tempo, mas o código MFM não controla totalmente o *pulso de tempo*.

[1] W. H. Gottschalk, G. A. Hedlund, Topological Dynamics, *Amer. Math. Soc. Colloquium Publ.* 36 (1955)

[2] J. Hadamard, Les surfaces a courbures opposées et leurs lignes geodesiques, *Journal de Mathematiques Pures et Appliqué.* 4 (1898), 27-73.

[3] D. Lind, B. Marcus, An introduction to symbolic dynamics and coding, *Cambridge University Press.* New York, 1995.

[4] M. Morse, A one-to-one representations of geodesics on a surface of negative curvature, *Amer. J. Math.* 43 (1921) 33-51.

[5] M. Morse, Recurrent geodesics on a surface of negative curvature, *Trans. Amer. Math. Soc.* 22 (1921) 84-100.

[6] S. Smale, Differentiable dynamical systems, *Bull. Amer. Math. Soc.* 73 (1967) 747-817.

# Criptografia e Fractais

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Alfabeto Nornal** | 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 |
| **Alfabeto Cifrado** | 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 |

Tabela 2.1: **Método de substituição utilizado por Júlio César. Fonte: Singh (2003).**

| **Alfabeto Nornal** | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 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 |
| 2 | 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 |
| 3 | 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 |
| 4 | 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 |
| 5 | 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 |
| 6 | 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 |
| 7 | 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 |
| 8 | 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 |
| 9 | 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 |

Tabela 2.2: **Quadro de Vigenère. Fonte: Singh (2003).**

Para a construção de um cripto-sistema não é suficiente criar uma função de uma-via , é necessário para que a mensagem seja decodificada seguramente, que seja enviada e recebida por um caminho eficiente e que se tenha um alçapão.

A ideia de alçapão surgiu com Diffie e Hellman em 1976 e consta de uma informação secreta que permite fácil inversão da regra de inversão

1. Geram-se dois números primos grandes $p$ e $q$ e define-se $n$ por $n = pq$. Os números p e $q$ devem ser mantidos em segredo.
2. Define-se $\varphi(n) = (p-1)(q-1)$. Procura-se, randomicamente, um inteiro grande $d$, relativamente primo com $\varphi(n)$, tal que $1 < d < \varphi(n)$. O número $d$ é a chave privada.
3. Calcula-se o inteiro $e$ tal que $1 \leq e \leq \varphi(n)$ pela fórmula $ed \equiv 1 \bmod \varphi(n)$.

4. Torna-se conhecida a chave pública $P$, que consiste no par de inteiros $(e, n)$.

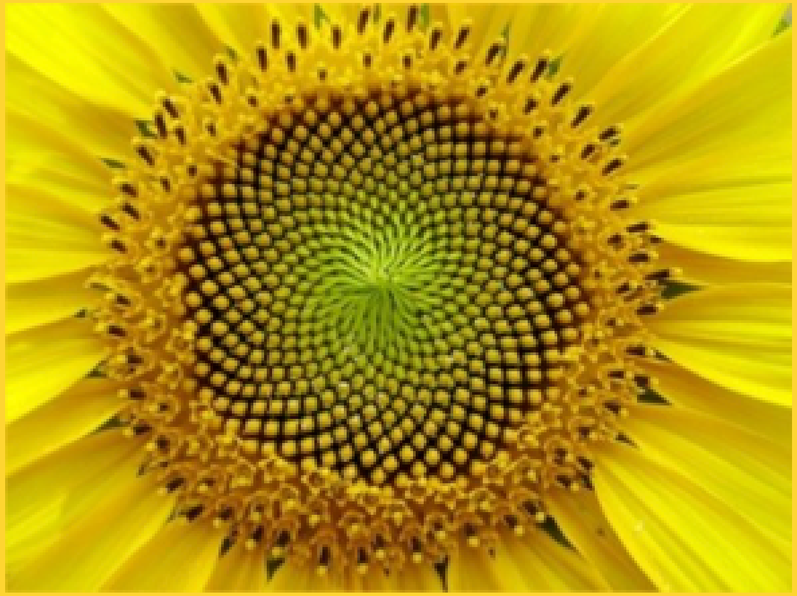
5. Representando por $M$ a mensagem a ser transmitida, como um inteiro no limite

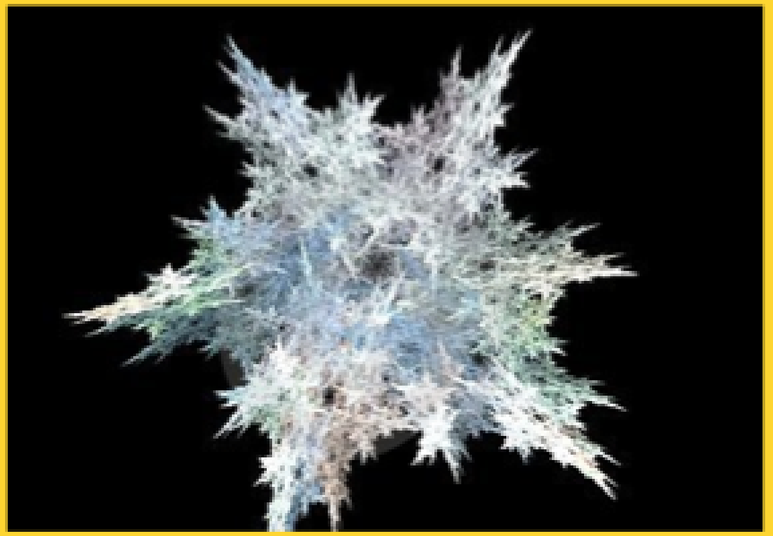
$\{1,..., n\}$; quebra-se $M$ em blocos se é grande demais.

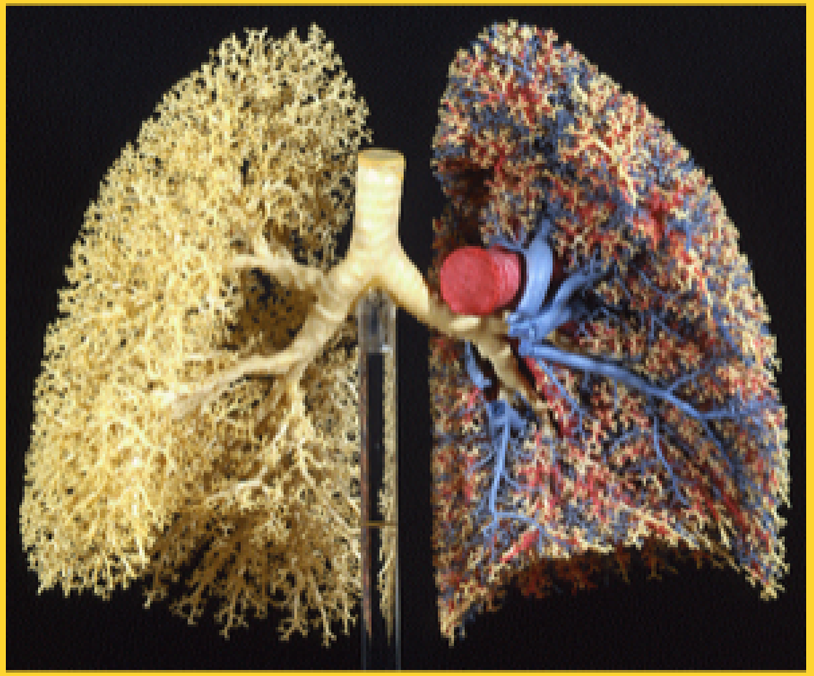
6. Codifica-se $M$ no criptograma $C$, pela regra $C \equiv M^e \bmod n$.

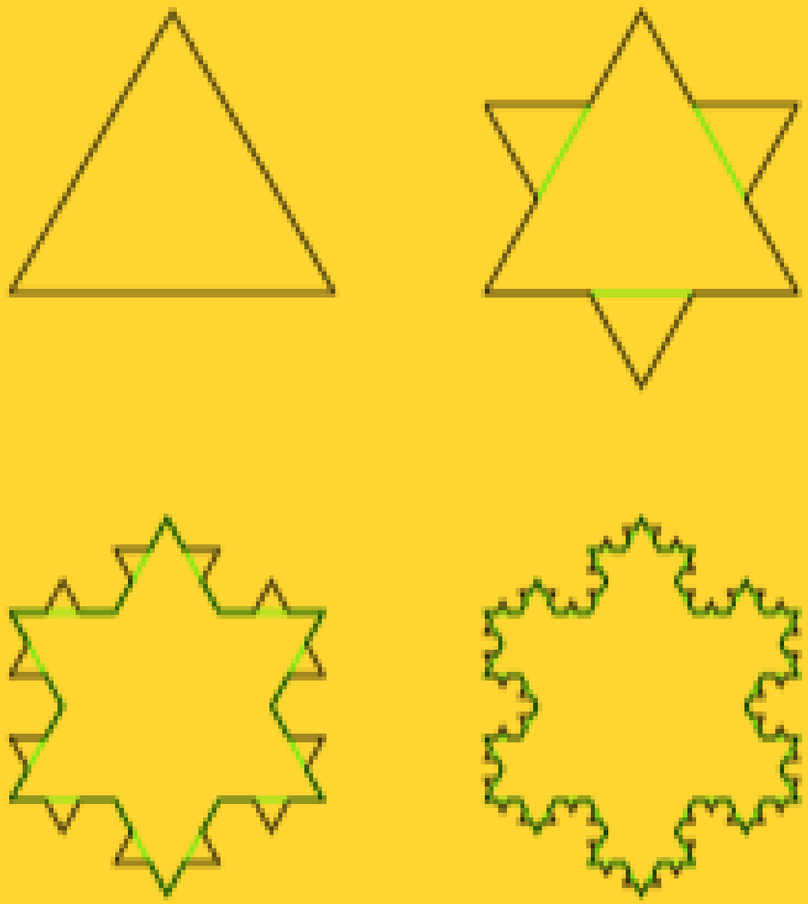
7. Decodifica-se C usando a chave privada $d$ pela fórmula $D \equiv C^d \bmod n$.

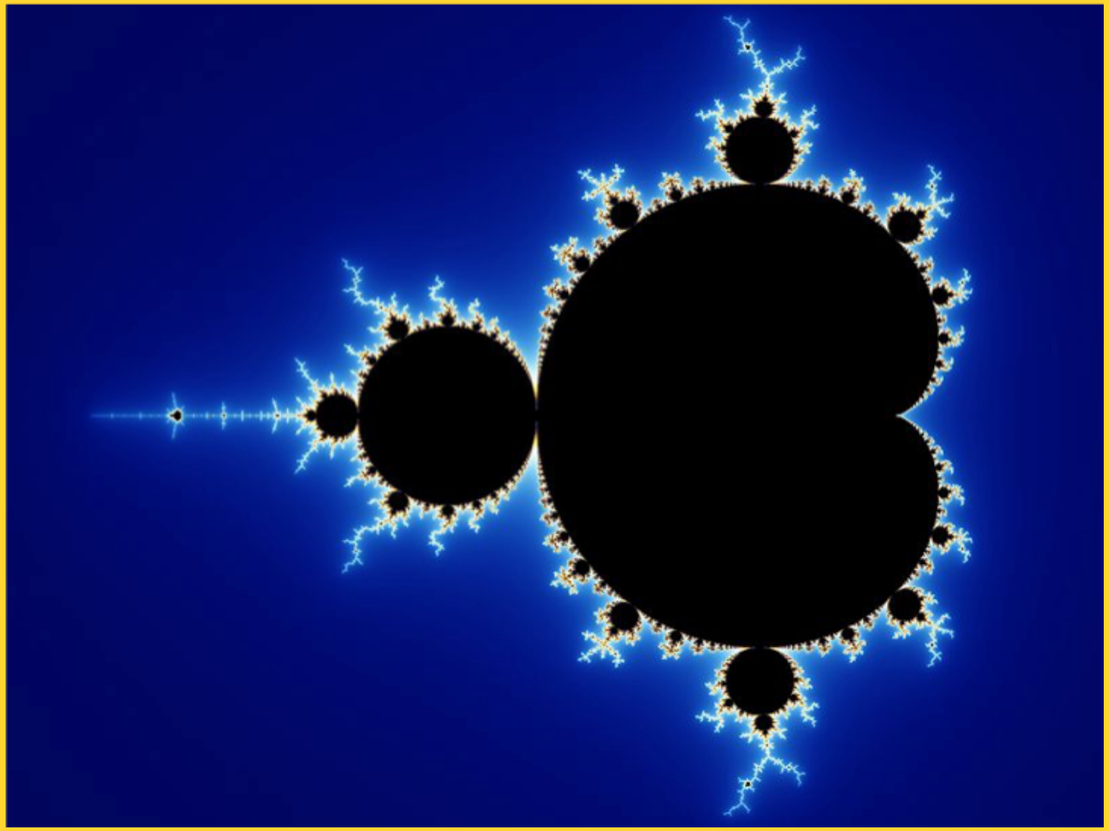
**Fractais**.... vem do latim **fractus** que significa fragmentar, quebrar, partir. Este termo foi criado pelo matemático francês **Bernoit Mandelbrot** (1975) e, a grosso modo, são **formas geométricas que se repetem iterativamente**, em escala decrescente de crescimento.

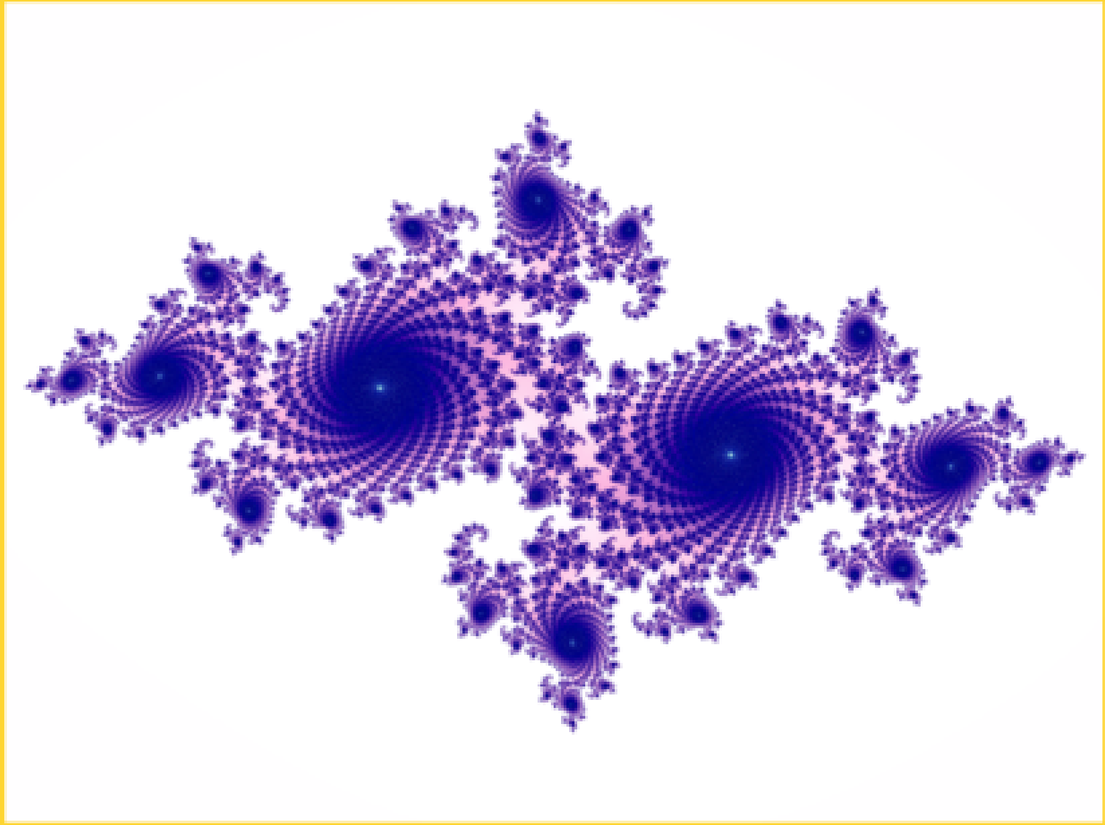












Na **auto-semelhança** há simetria escalar e a redução ocorre igualmente em todas as dimensões do fractal. Na auto-afinidade também há simetria escalar, mas o fator de redução pode ser diferente em algumas dimensões do fractal.

A **dimensionalidade fracionária** refere-se ao fato que as dimensões dos fractais pode ser uma fração e representa sua ocupação no espaço, ligada a seu grau de irregularidade e comportamento. Com ela torna-se possível medir partes de objetos cuja anormalidade ou tortuosidade impedem quantificação dentro dos padrões convencionais.

A **complexidade infinita** está relacionada às transformações decorrentes do processo de iterações sucessivas e ilimitadas que podem ocorrer na geração de um fractal

**Definição 29.** *Seja* $(\mathbf{X}, d)$ *um espaço métrico. Uma transformação em* $\mathbf{X}$ *é uma função* $f : \mathbf{X} \to \mathbf{X}$, *no qual associa exatamente um ponto* $f(x) \in \mathbf{X}$, *para cada ponto* $x \in \mathbf{X}$. *Se* $\mathbf{S} \subset \mathbf{X}$ *então* $f(\mathbf{S}) = \{f(x) : x \in \mathbf{S}\}$. $f$ *é injetora se* $x, y \in \mathbf{X}$ *com* $f(x) = f(y)$, *implica* $x = y$ *e é sobrejetora se* $f(\mathbf{X}) = \mathbf{X}$. *Caso* $f$ *possua ambas propriedades, então ela é bijetora e possui uma inversa, uma Transformação* $f^{-1} : \mathbf{X} \to \mathbf{X}$ *com* $f^{-1}(y) = x$ , *no qual* $x \in \mathbf{X}$ *é o único ponto de forma que* $y = f(x)$.

**Definição 30.** *Seja* $f : \mathbf{X} \to \mathbf{X}$ *uma transformação num espaço métrico. As iterações de* $f$ *são transformações* $f^n : \mathbf{X} \to \mathbf{X}$ *que, para* $n = 1, 2, \ldots,$ *definimos por:*

$$
\begin{aligned}
f^0(x) &= x, \\
f^1(x) &= f(x), \\
f^2(x) &= f(f^1(x)), \\
f^n(x) &= f(f^{n-1}(x)).
\end{aligned}
$$

**Definição 33.** *Uma Transformação* $w : \mathbb{R}^2 \to \mathbb{R}^2$ *da forma:*

$$w(x_1, x_2) = (ax_1 + bx_2 + e,\ cx_1 + dx_2 + f),$$

*nos quais* $a, b, c, d, e, f$ *são números reais, é chamada de transformação afim no plano.*

No caso, usaremos a seguinte notação:

$$w(x) = w\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix} = Ax + t.$$

A matriz A pode ser escrita da forma:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} r_1 \cos\theta_1 & r_2 \sin\theta_2 \\ r_1 \sin\theta_1 & r_2 \cos\theta_2 \end{pmatrix},$$

**Definição 38.** *Seja* $f : \mathbf{X} \to \mathbf{X}$ *uma transformação num espaço métrico. Um ponto* $x_f \in \mathbf{X}$ *de forma que* $f(x_f) = x_f$ *é chamado de ponto fixo de uma transformação.*

**Definição 39.** *Seja* $\mathbf{F}$ *um conjunto de transformações num espaço métrico* $\mathbf{X}$. $\mathbf{F}$ *é chamado de semigrupo se* $f, g \in \mathbf{F}$ *implica que* $f \circ g \in \mathbf{F}$. $\mathbf{F}$ *é chamado de grupo se é um semigrupo de transformações inversíveis, então* $f \in \mathbf{F}$ *implica* $f^{-1} \in \mathbf{F}$.

**Definição 40.** *Uma transformação $f : \mathbf{X} \to \mathbf{X}$ num espaço métrico $(\mathbf{X}, d)$ é chamada de contração se existe uma constante $0 \leq s < 1$ de forma que:*

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

*Qualquer número $s$ é chamado de fator de contração de $f$.*

**Teorema 7** (Teorema da Contração)**.** *Seja $f : \mathbf{X} \to \mathbf{X}$ uma contração num espaço métrico completo $(\mathbf{X}, d)$. Então $f$ possui exatamente um ponto fixo $x_f \in \mathbf{X}$ e ainda, para cada ponto $x \in \mathbf{X}$, a sequência $\{f^n(x) : \ n = 1, 2, \dots\}$ converge para $x_f$. Ou seja:*

$$\lim_{n \to \infty} f^n(x) = x_f, \quad \forall\ x \in \mathbf{X}.$$

# Espaço de Hausdorff

**Definição 24.** *Seja* $(\mathbf{X}, d)$ *um espaço métrico completo. Então* $\mathscr{H}(\mathbf{X})$ *denota o espaço no qual os elementos são subconjuntos compactos de* $\mathbf{X}$*, além do conjunto vazio.*

**Definição 25.** *Seja* $(\mathbf{X}, d)$ *um espaço métrico completo,* $x \in \mathbf{X}$*, e* $B \in \mathscr{H}(\mathbf{X})$*. Defina:*

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

*Então,* $d(x, B)$ *é a distância do ponto* $x$ *ao conjunto* $B$*.*

**Definição 26.** *Sejam* $(\mathbf{X}, d)$ *um espaço métrico completo e* $A, B \in \mathscr{H}(\mathbf{X})$. *Então,*

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

*é a distância do conjunto* $A \in \mathscr{H}(\mathbf{X})$ *ao conjunto* $B \in \mathscr{H}(\mathbf{X})$.

**Definição 27.** *Seja* $(\mathbf{X}, d)$ *um espaço métrico completo. Então a distância de Hausdorff entre os elementos* $A$ *e* $B$ *em* $\mathscr{H}(\mathbf{X})$ *é definido por:*

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

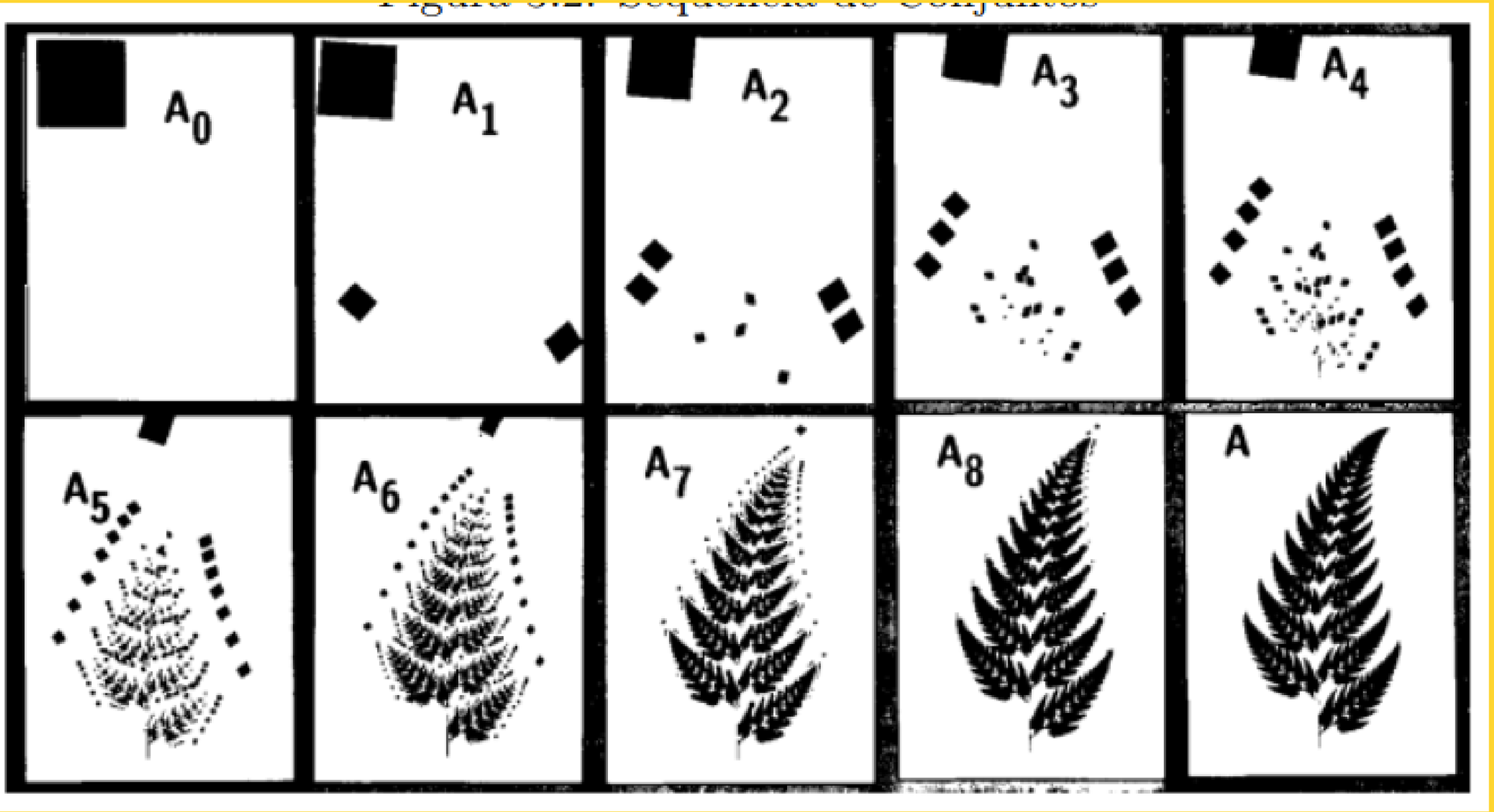
No qual, a notação $\vee$ é utilizada para denotar o máximo entre os elementos, então a distância de Hausdorff é o maior valor entre $d(A, B)$ e $d(B, A)$.

**Teorema 5** (Completude do espaço dos Fractais)**.** *Seja* $(\mathbf{X}, d)$ *um espaço métrico completo. Então* $(\mathscr{H}(\mathbf{X}), h)$ *é um espaço métrico completo. E ainda, se* $\{A_n \in \mathscr{H}(\mathbf{X})\}_{n=1}^{\infty}$ *é uma sequência de Cauchy, então*

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

*pode ser caracterizado como:*

$$A = \{x \in \mathbf{X} : \textit{existe uma sequência de Cauchy } \{x_n \in A_n\} \textit{ que converge a } x\}.$$


A0
A1
A2
A3
A4
A5
A6
A7
A8
A

Sejam $(\mathbf{X}, d)$ um espaço métrico e $(\mathscr{H}(\mathbf{X}), h(d))$ o espaço de Hausdorff associado a ele. Considerando agora a notação $h(d)$ para se referir a qual métrica está sendo considerada para a definição de $h$.

Apesar de ainda não ter sido apresentado uma definição formal de fractal, podemos dizer que fractal determinístico é um ponto fixo de uma contração em $(\mathscr{H}(\mathbf{X}), h(d))$, considerando que $(\mathbf{X}, d)$ seja geometricamente simples, assim como as contrações, que devem ser facilmente especificadas, como as descritas abaixo.

**Lema 3.** *Seja* $w : \mathbf{X} \to \mathbf{X}$ *uma contração num espaço métrico* $(\mathbf{X}, d)$. *Então* $w$ *é contínua.*

**Lema 4.** *Seja* $w : \mathbf{X} \to \mathbf{X}$ *uma contração contínua no espaço métrico* $(\mathbf{X}, d)$. *Então* $w$ *leva* $\mathscr{H}(\mathbf{X})$ *nele mesmo.*

**Lema 5.** *Seja* $w : \mathbf{X} \to \mathbf{X}$ *um contração num espaço métrico* $(\mathbf{X}, d)$ *com fator de contração* $s$. *Então,* $w : \mathscr{H}(\mathbf{X}) \to \mathscr{H}(\mathbf{X})$ *definido por*

$$w(B) = \{w(x) : x \in B\} \quad \forall\ B \in \mathscr{H}(\mathbf{X})$$

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

**Lema 7.** *Sejam* $(\mathbf{X}, d)$ *um espaço métrico e* $\{w_n : n = 1, 2, \ldots, N\}$ *contrações em* $(\mathscr{H}(\mathbf{X}), h)$. *Seja ainda* $s_n$ *o fator de contração de* $w_n$ *para cada* $n$. *Defina* $W : \mathscr{H}(\mathbf{X}) \to \mathscr{H}(\mathbf{X})$ *por*

$$W(B) = w_1(B) \cup w_2(B) \cup \cdots \cup w_N(B) = \bigcup_{n=1}^{N} w_n(B), \quad \forall\ B \in \mathscr{H}(\mathbf{X}).$$

*Então,* $W$ *é uma contração com fator de contração* $s = \max\{s_n : n = 1, 2, \ldots, N\}$.

**Definição 42.** *Um Iterated Function System (hiperbólico) ou Sistema de Funções Iteradas, consiste de um espaço métrico completo* $(\mathbf{X}, d)$ *junto com um conjunto finito de contrações* $w_N : \mathbf{X} \to \mathbf{X}$*, com os respectivos fatores de contração* $s_n$*, para* $n = 1, 2, \ldots, N$*. Utilizamos a sigla IFS para abreviá-lo e possui a notação* $\{\mathbf{X}; w_n,\ n = 1, 2, \ldots, N\}$ *e seu fator de contração é* $s = \max\{s_n : n = 1, 2, \ldots, N\}$.

**Teorema 8.** *Seja* $\{\mathbf{X}; w_n,\ n = 1, 2, \ldots, N\}$ *um IFS com fator de contração* $s$. *Então a transformação* $W : \mathscr{H}(\mathbf{X}) \to \mathscr{H}(\mathbf{X})$ *definida por*

$$W(B) = \bigcup_{n=1}^{N} w_n(B),$$

*para todo* $B \in \mathscr{H}(\mathbf{X})$, *é uma contração num espaço métrico completo* $(\mathscr{H}(\mathbf{X}), h(d))$ *com fator de contração* $s$. *Ou seja*

$$h(W(B), W(C)) \leq s \cdot h(B, C),$$

*para todo* $B, C \in \mathscr{H}(\mathbf{X})$. *Seu único ponto fixo* $A \in \mathscr{H}(\mathbf{X})$

$$A = W(A) = \bigcup_{n=1}^{N} w_n(A),$$

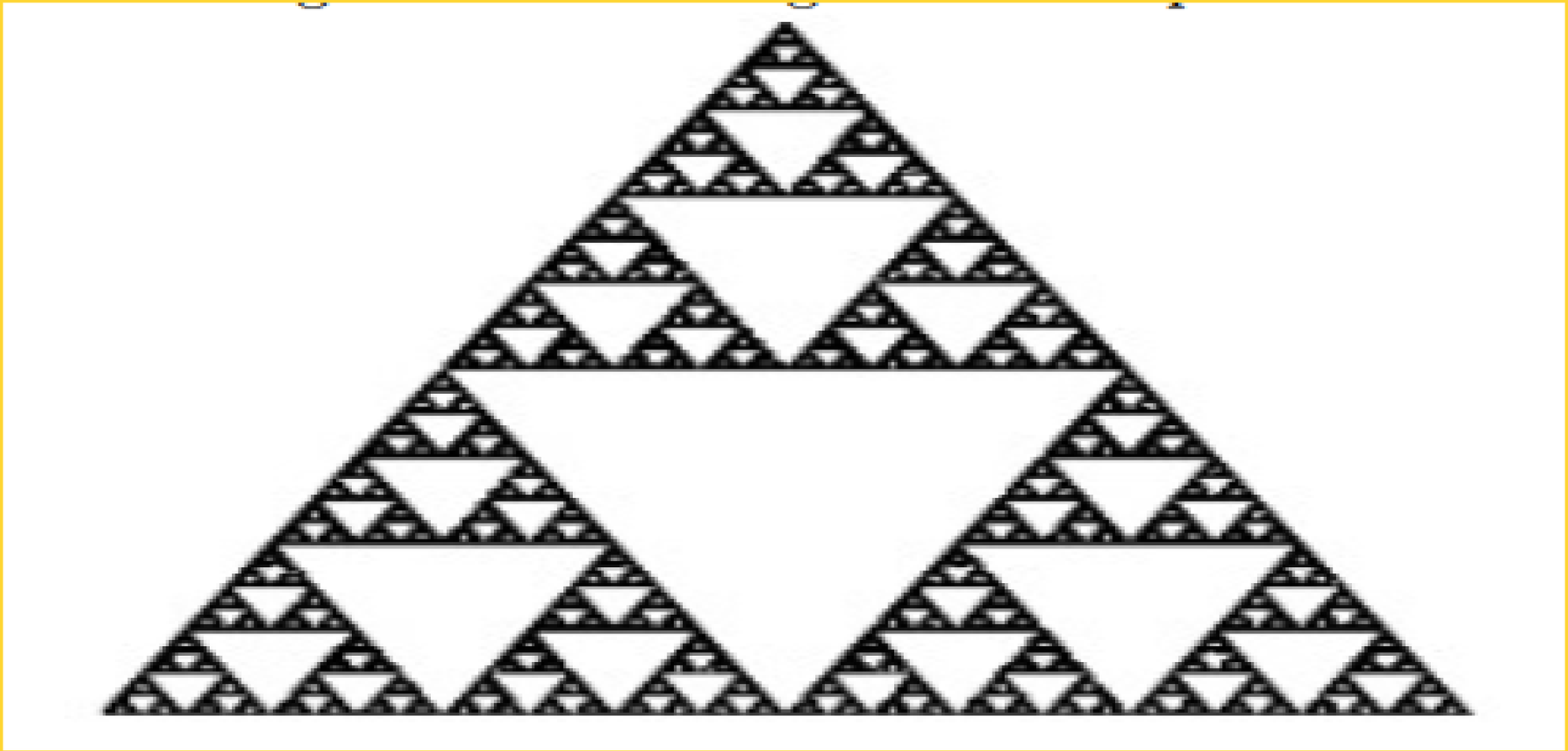
*é dado por* $A = \lim_{n\to\infty} W^n(B)$, *para qualquer* $B \in \mathscr{H}(\mathbf{X})$.

**Definição 43.** *O ponto fixo $A \in \mathscr{H}(\mathbf{X})$ descrito no Teorema 8 é chamado de atrator do IFS.*

Podemos dizer que os atratores dos IFS são um tipo de fractais

Sejam o espaço métrico $(\mathbf{X}, d)$, com $\mathbf{X} = [0,1] \times [0,1]$, e o IFS:

$$\begin{cases} w_1(x,y) = \left(\frac{x}{2}, \frac{y}{2}\right) \\ w_2(x,y) = \left(\frac{x}{2} + \frac{1}{2}, \frac{y}{2}\right) \\ w_3(x,y) = \left(\frac{x}{2} + \frac{1}{4}, \frac{y}{2} + \frac{1}{2}\right) \end{cases}$$



# Método Fractal

$$w_i(x,y) = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e_i \\ f_i \end{pmatrix}, \quad i = 1,2,\ldots,N$$

# Método proposto por Al Said e Said

$$w_i(x,y) = \begin{pmatrix} a_i & 0 \\ 0 & d_i \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} c_i \\ d_i \end{pmatrix}, \quad i = 1,2,\ldots,N$$

$$w_i(x,y,1) = \begin{pmatrix} a_i & 0 & c_i \\ 0 & b_i & d_i \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}, \quad i = 1,2,\ldots,N$$

$$H = \begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{pmatrix}$$

$$W(x,y,1)=\begin{pmatrix} A & 0 & C \\ 0 & B & D \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$$

$$A = a_4a_3a_2a_1,\ A\neq 1.$$
$$B = b_4b_3b_2b_1,\ B\neq 1,$$
$$C = a_4a_3a_2c_1+a_4a_3c_2+a_4c_3+c_4$$
$$D = b_4b_3b_2d_1+b_4b_3d_2+b_4d_3+d_4$$

# Algoritmo proposto

Para ocultar o valor do fractal atrator durante o processo de transmissão, é necessária uma chave secreta compartilhada, que está disponível apenas para o remetente e o destinatário.

Um protocolo de acordo com a chave DH é usado para gerar o número de iterações que irá criar o fractal atrator o qual por sua vez será usado para gerar a chave pública e criptografar a mensagem.

O esquema de chave pública fractal compreende 3 fases:

1)Geração da Chave

2) Encriptar

3) Decriptar

# Geração da Chave

$$W^n = \begin{pmatrix} A^n & 0 & (T_n(A))C \\ 0 & B^n & (T_n(B))D \\ 0 & 0 & 1 \end{pmatrix}$$

$$u \equiv A^n x + T_n(A)C$$

$$v \equiv B^n y + T_n(B)D$$

$$u' \equiv A^n x' + T_n(A)C$$

$$v' \equiv B^n y' + T_n(B)D$$

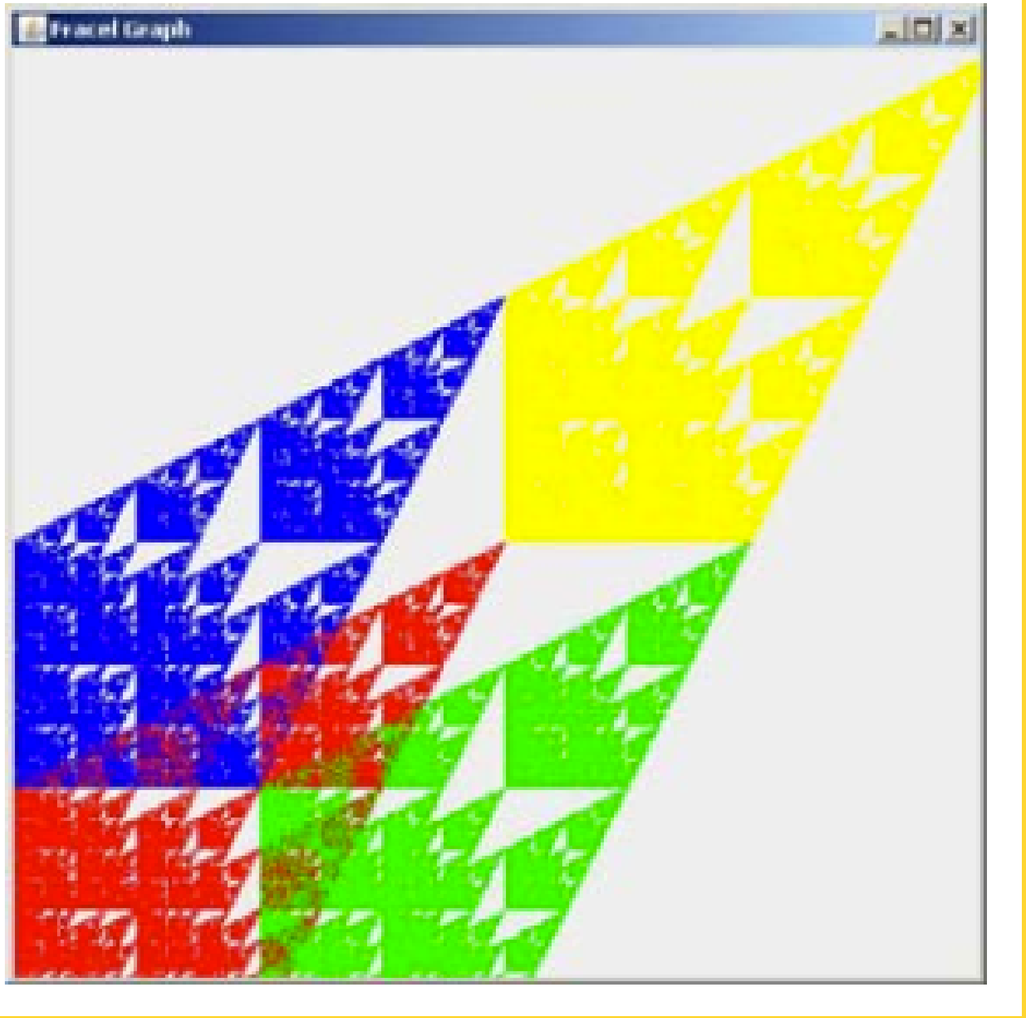
# Encriptar

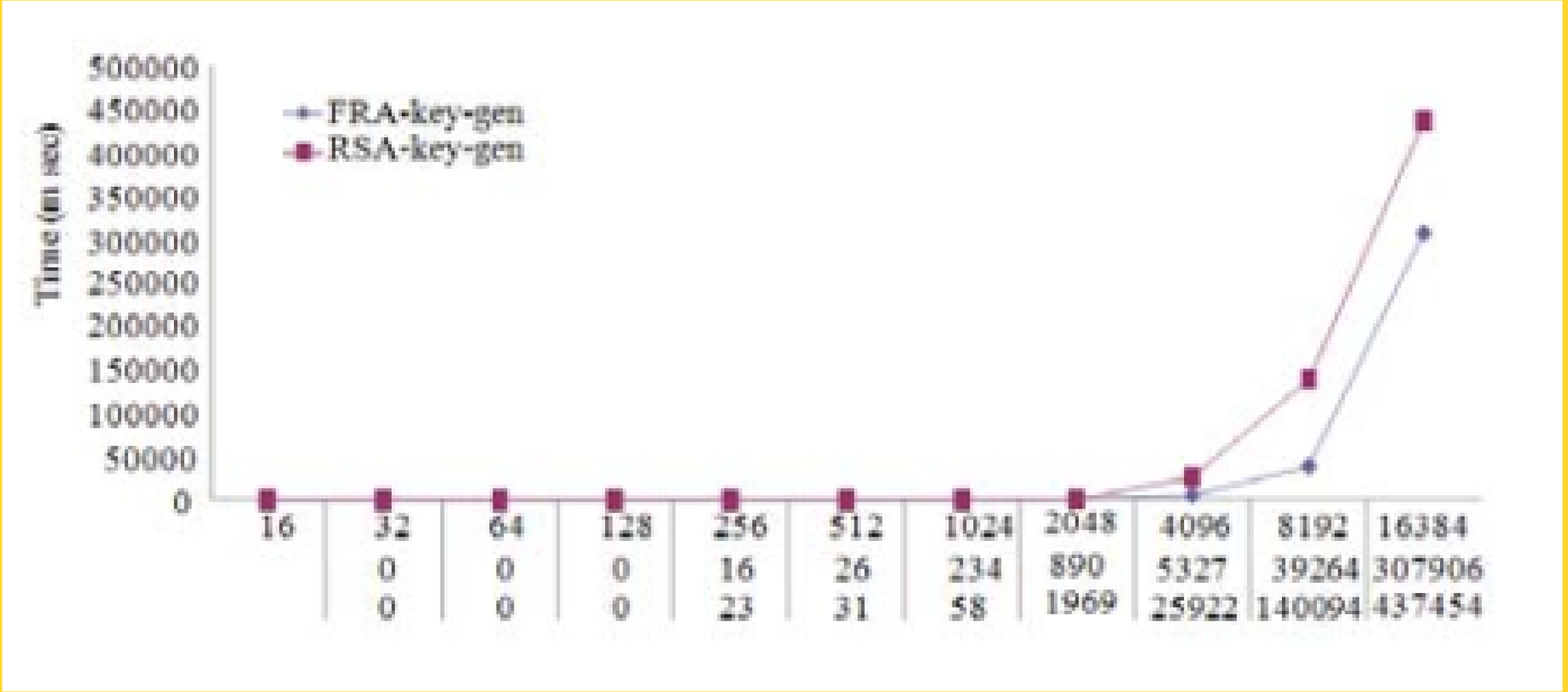
Determine a mensagem a ser criptografada e represente isso como pares

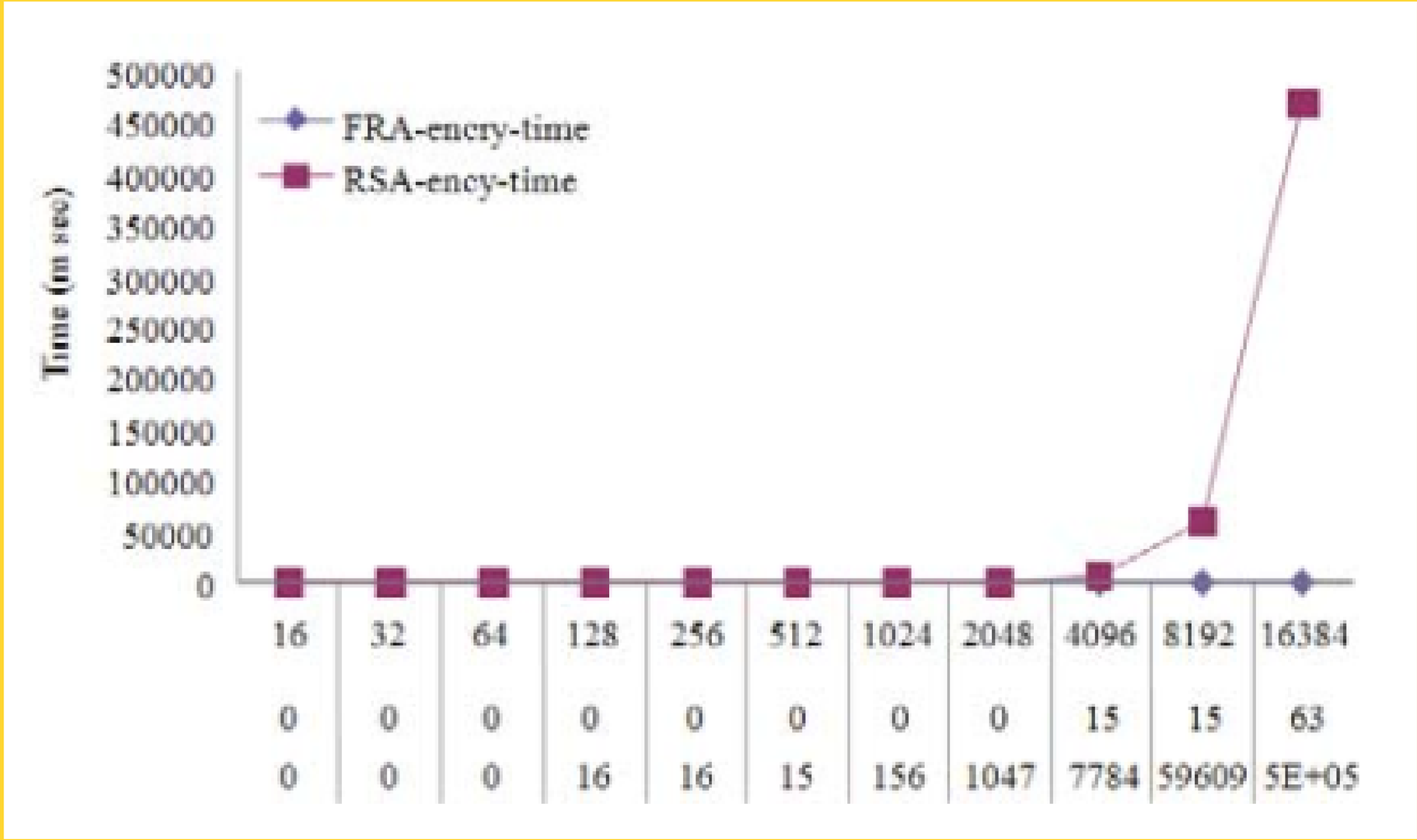
$$M = (m_1, m_2) = \left( \frac{s_1 - T_n(A)C}{(A^n x + T_n(A)C)(u' - T_n(A)C)} \right.$$
$$\left. \frac{s_2 - T_n(B)D}{(B^n y + T_n(B)D)(v' - T_n(B)D)} \right)$$

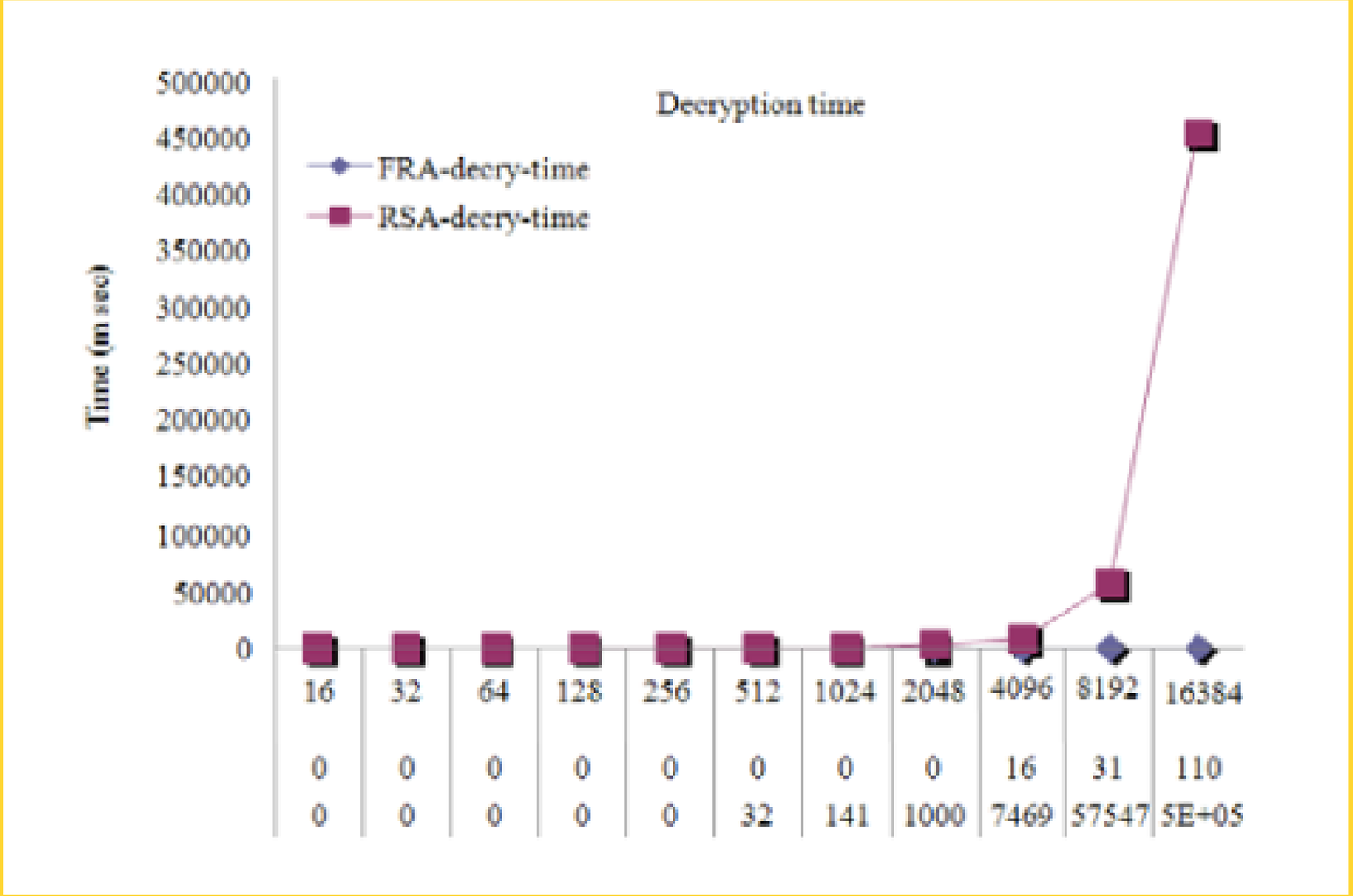
$$H = \begin{pmatrix} 0.5 & 0.5 & 0 & 0 \\ 0.5 & 0.5 & 0 & 0.25 \\ 0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & 0.25 & 0 \end{pmatrix}$$

$$W = \begin{pmatrix} 0.0625 & 0 & 0.5 \\ 0 & 0.0625 & 0.3125 \\ 0 & 0 & 1 \end{pmatrix}$$


Fractal Graph


Time (in sec)
500000
450000
400000
350000
300000
250000
200000
150000
100000
50000
0
FRA-key-gen
RSA-key-gen
16
32
64
128
256
512
1024
2048
4096
8192
16384
0
0
0
16
26
234
890
5327
39264
307906
0
0
0
23
31
58
1969
25922
140094
437454


500000
450000
400000
350000
300000
250000
200000
150000
100000
50000
0
Time (m sec)
FRA-encry-time
RSA-ency-time
16 32 64 128 256 512 1024 2048 4096 8192 16384
0 0 0 0 0 0 0 0 15 15 63
0 0 0 16 16 15 156 1047 7784 59609 5E+05


Decryption time
FRA-decry-time
RSA-decry-time
Time (m sec)
500000
450000
400000
350000
300000
250000
200000
150000
100000
50000
0
16 32 64 128 256 512 1024 2048 4096 8192 16384
0 0 0 0 0 0 0 0 16 31 110
0 0 0 0 0 32 141 1000 7469 57547 5E+05

Se os parâmetros do sistema criptográfico são baseados em números reais (um intervalo infinito contínuo), então o espaço de busca é enorme.

Assim, muitos ataques bem conhecidos falham em resolver os sistemas não lineares e encontrar o parâmetro de chave secreta de uma chave pública.

Mesmo que seja teoricamente possível, não é computacionalmente viável.

# Cripografia e Fractais: como isso ocorre.

A ideia é propor algoritmos que não estejam baseados em problemas de teoria dos números é um desafio para a área de segurança da informação.

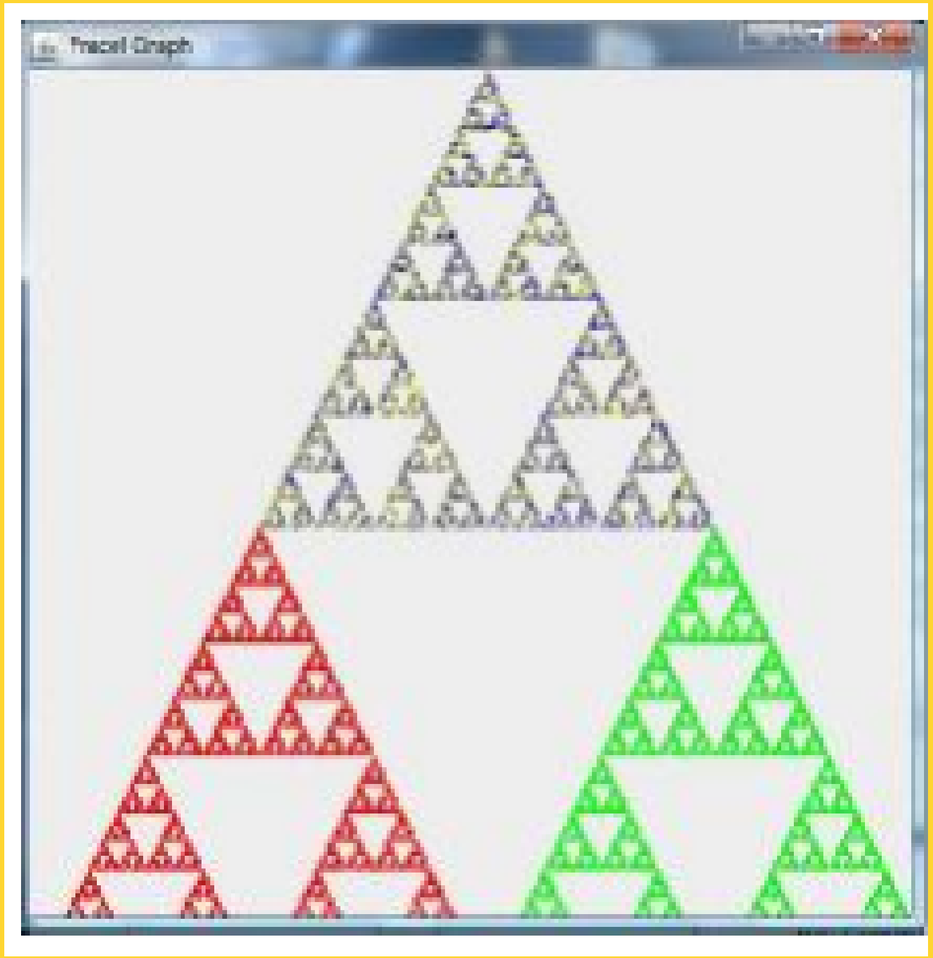
A ideia é propor algoritmos que não estejam baseados em problemas de teoria dos números é um desafio para a área de segurança da informação.

Um novo protocolo de acordo com a chave baseado na geração fractal usando IFS é proposto para concordar com uma chave de sessão e garantir a autenticidade da outra parte.

Este método baseado na escolha de um conjunto fractal conhecido e na resolução de suas funções afins recursivas as quais são usadas como uma raiz primitiva para gerar a chave pública.

Os fractais podem ser gerados pela iteração de uma ou mais transformações afins.

No protocolo proposto, o emissor e o receptor devem estar de acordo sobre o fractal usado no estabelecimento da chave.


Fractal Graph

O protocolo proposto: O protocolo envolveu duas partes, digamos Alice e Bob. Ambos devem gerar suas chaves públicas com base em suas chaves privadas selecionadas. A matriz W de Hutchinson deve ser feita e publicada antes da apresentação do protocolo de acordo, a fim de ser usado como um elemento primitivo no algoritmo. Se supusermos que Alice quer comunicar-se com Bob para estabelecer a chave de sessão, então eles realizarão os seguintes passos:

# Contas : )

# Análise de segurança

1. O domínio das funções fractais são definidos sem o subcorpo (0,1). Então, devido ao espaço de chave aberta e ao tamanho da chave baseada no protocolo fractal é comprovadamente capaz de resistir a alguns ataques conhecidos entre os protocolos tradicionais que se baseiam em campos finitos e lidam com o problema de log discreto e fatoração

## 2 - Ataque repetido:

Por meio da reutilização das informações obtidas no protocolo, um adversário poderia se passar pelo usuário legal. Mesmo que ele tenha obtido U ou U’ não é fácil para ele recuperar r ou s, pois são resultados de iterações e é demorado passar por todos os valores de n para n grande.

# 3-Autenticação Mútua:

O protocolo proposto consegue autenticação mútua entre duas partes. Na etapa 2 de o algoritmo, Alice calcula K usando suas chaves privadas x,y,s e Bob também calcula K' usando suas chaves privadas x',y',r; eles concordam com a chave de sessão se K=K', ou seja, o K' usando suas chaves privadas x',y',r; eles concordam com a chave de sessão se K=K', ou seja, a autenticação mútua é feita.

# 4- Ataque de chave de sessão conhecido:

No protocolo proposto, a chave de sessão é K= Ws*U’*(x,y,1), ou K’= Wr*U*(x’,y’,1),onde x,y,x',y',r e s são números aleatórios. Embora, o atacante possa saber chaves de sessão, como; U ou U', que representam a chave pública que é calculada usando a chave privada (s ou r) como uma iteração, e a constante de variação (x,y) ou (x’,y’), ele ainda não pode calcular a chave de sessão, porque a inclusão desses valores aleatórios pode ajudar para garantir um grande número de incógnitas sobre o número de equações.

Ou seja, resolver o sistema não linear numericamente resultou no acompanhamento de cumulativos erros de truncamento, e é considerado como demorado sobre o subcorpo infinito definido.

Portanto, é impossível encontrar a chave privada a partir da chave pública fornecida.

# Comparação da Perfomance

| | 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 |
| 8192 | 2377 | 22 | 1875 | 59722 |