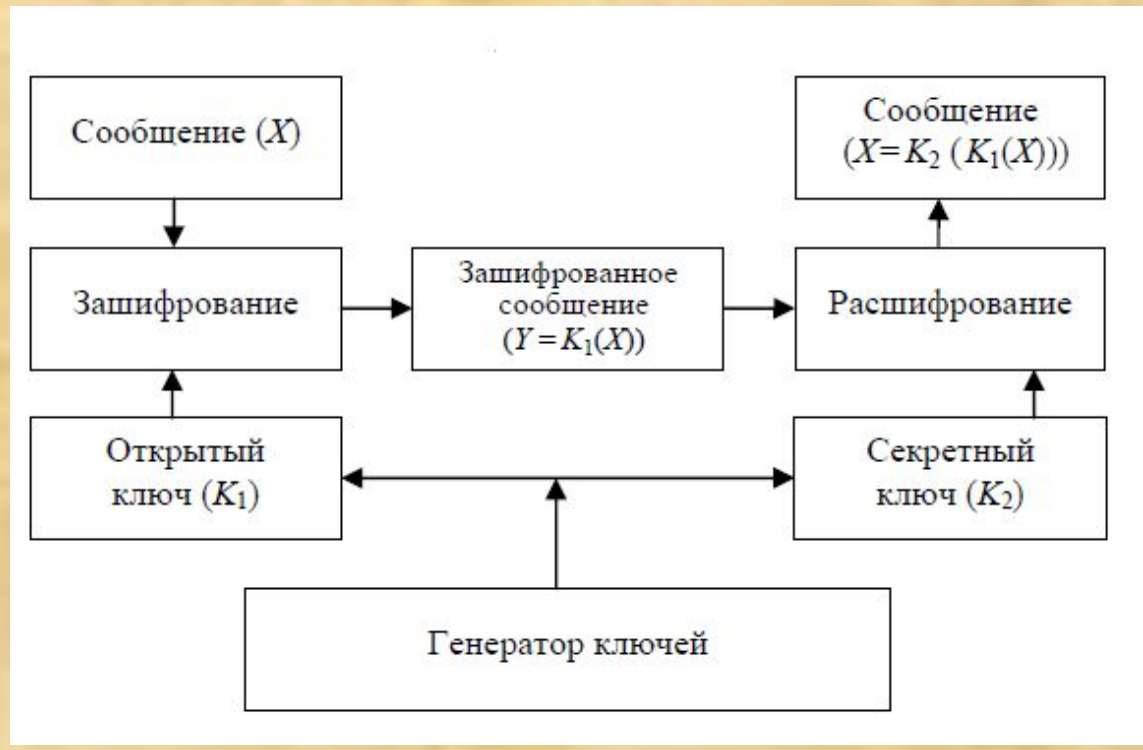
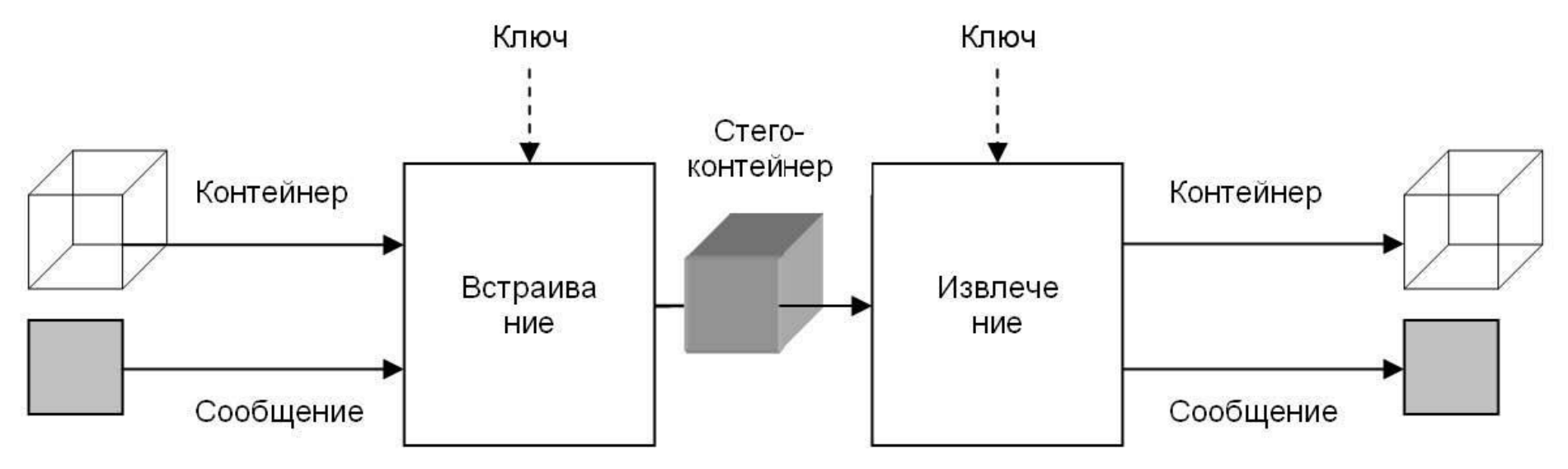
Возможные применения теории фракталов в криптографии

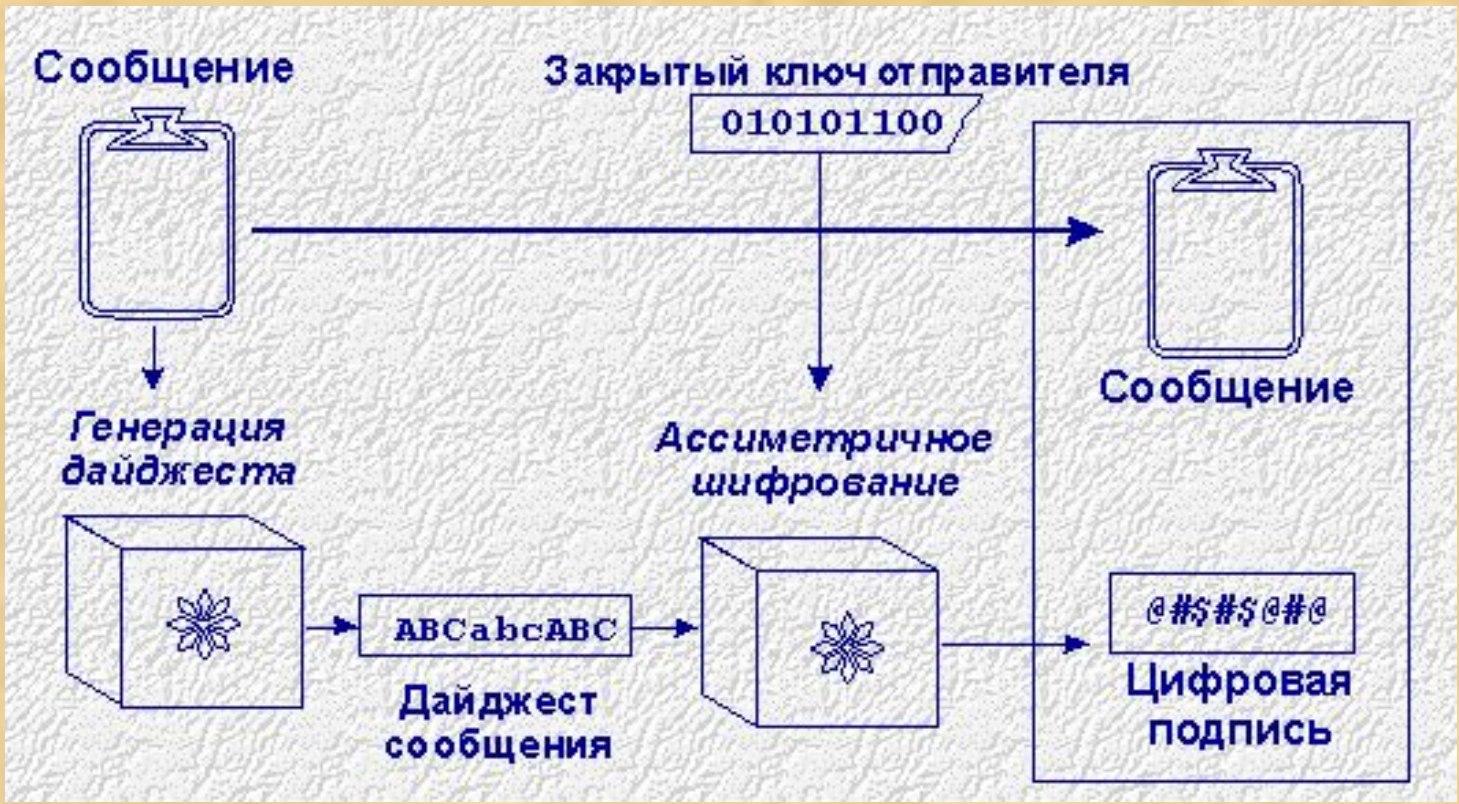
Ассиметричное шифрование с открытым ключом:



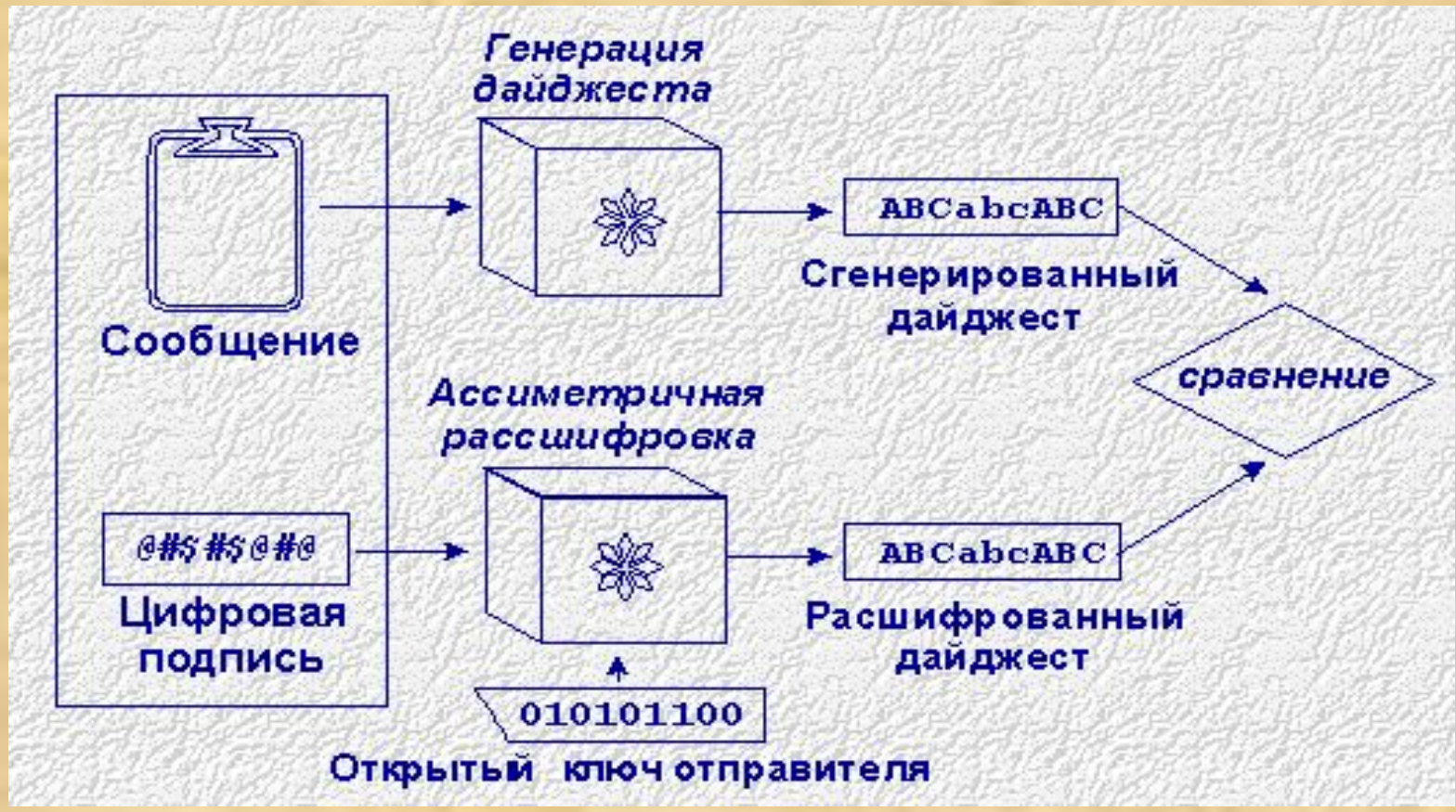
Общий принцип стеганографического сеанса:



Общая схема формирования цифрового конверта (закрытое сообщение + подпись)



Проверка правильности цифровой подписи, используя открытый ключ отправителя для расшифровки дайджеста сообщения.

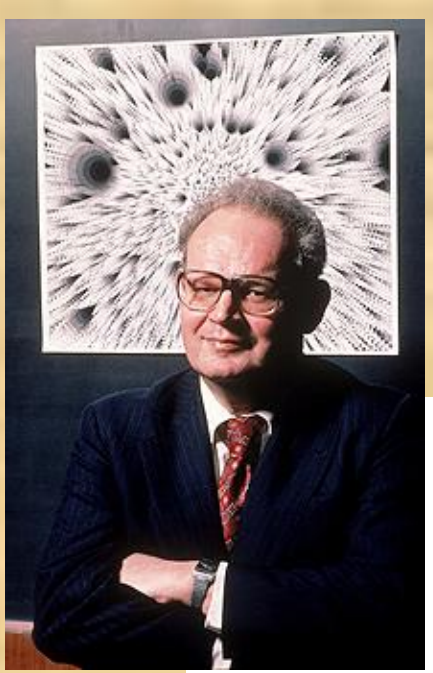


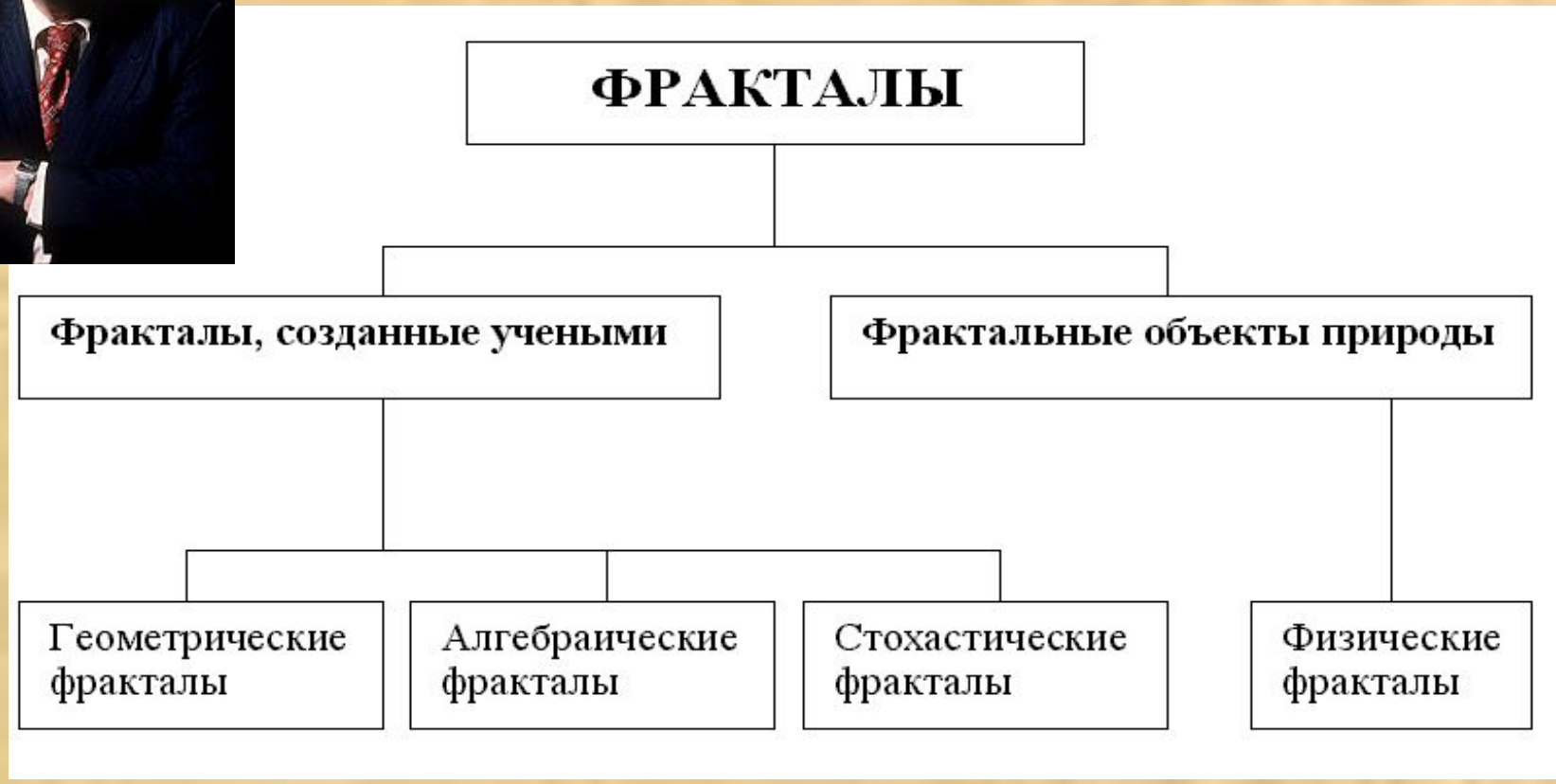
Для того, чтобы хеш-функция *H* считалась криптографически стойкой, она должна удовлетворять трём основным требованиям, на которых основано большинство применений хеш-функций в криптографии:

- Необратимость или стойкость к восстановлению прообраза: для заданного значения хеш-функции *m* должно быть вычислительно невозможно найти блок данных *X*, для которого $H(X)=m$.

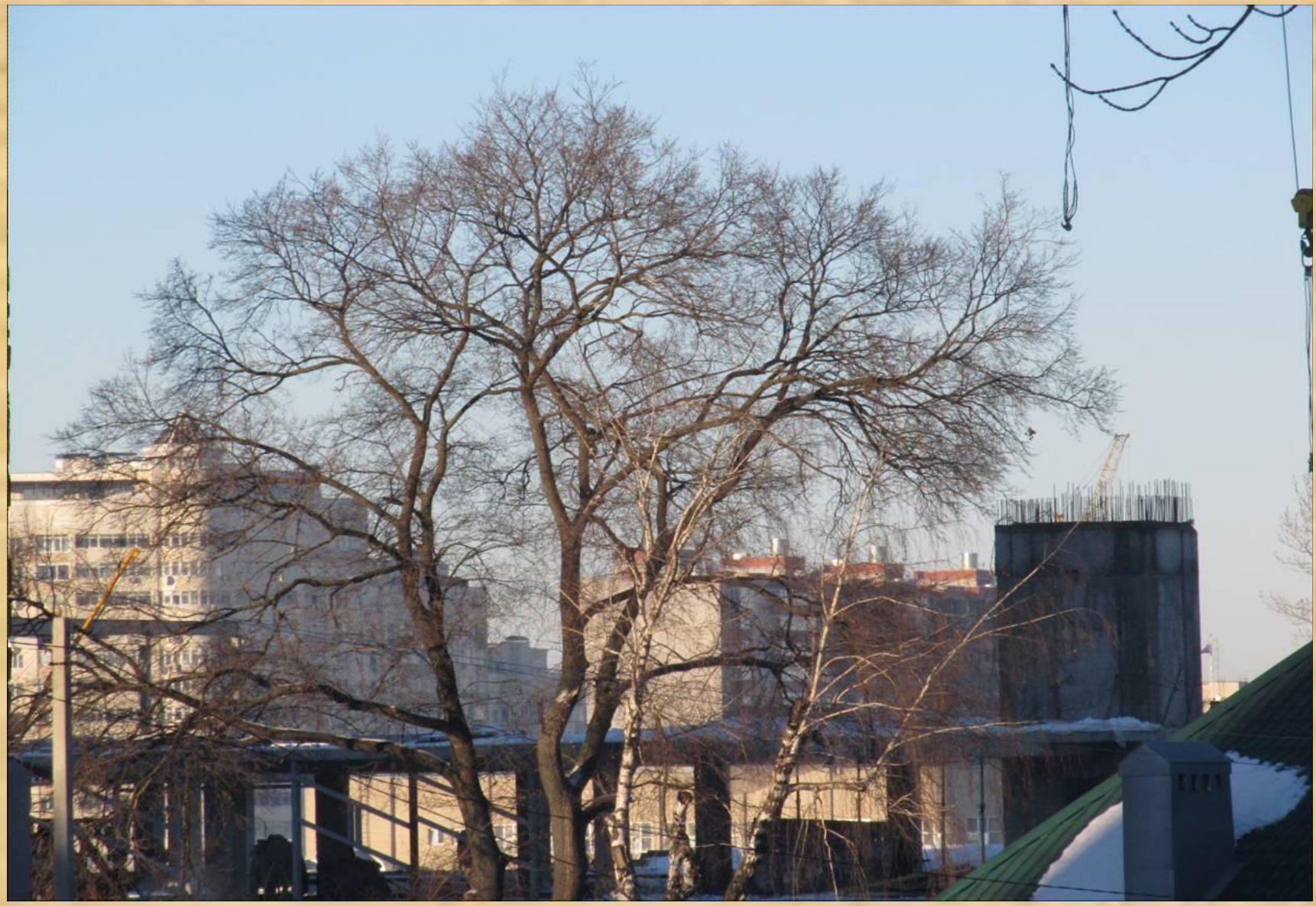
- Стойкость к коллизиям первого рода или восстановлению вторых прообразов: для заданного сообщения *M* должно быть вычислительно, невозможно подобрать другое сообщение *N*, для которого $H(N)=H(M)$.

- Стойкость к коллизиям второго рода: должно быть вычислительно невозможно подобрать пару сообщений *M*, и *M'*, имеющих одинаковый хеш.

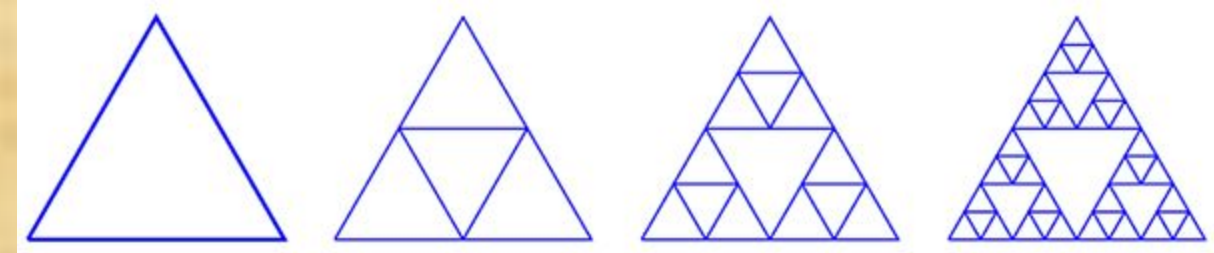


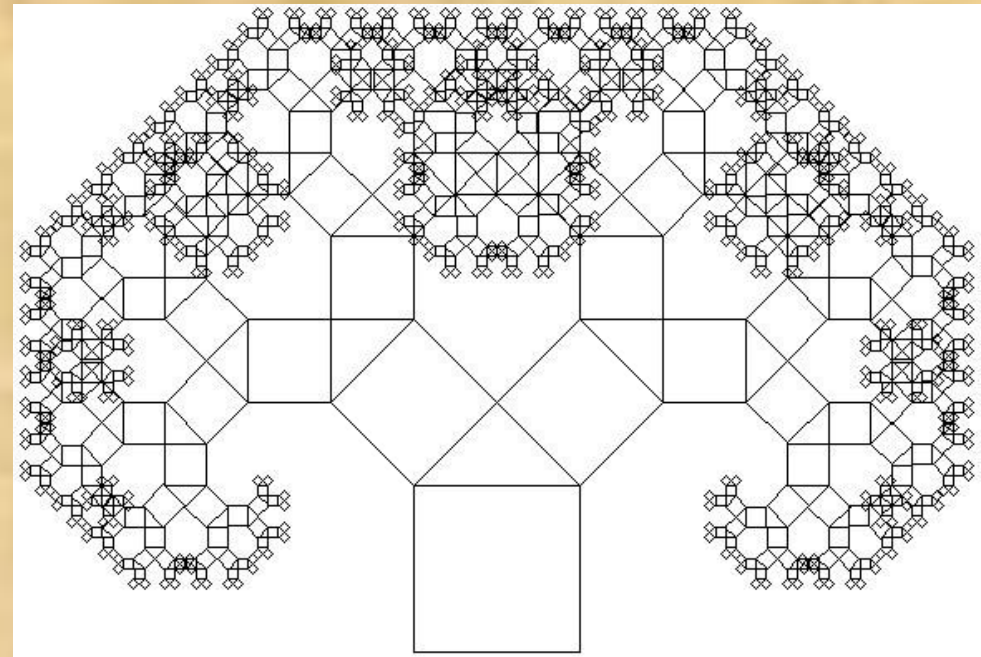

ФРАКТАЛЫ
Фракталы, созданные учеными
Фрактальные объекты природы
Геометрические фракталы
Алгебраические фракталы
Стохастические фракталы
Физические фракталы

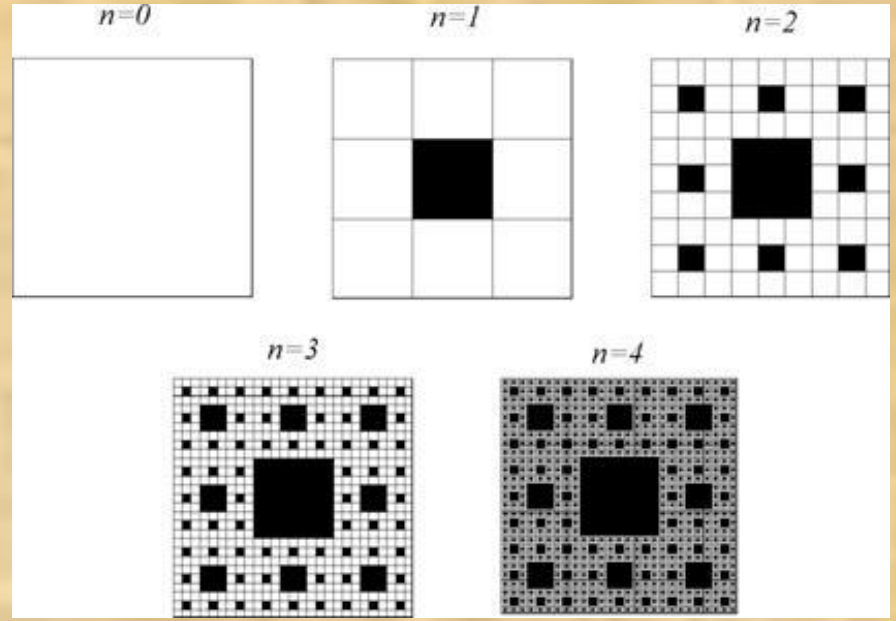
Фракталы в природе



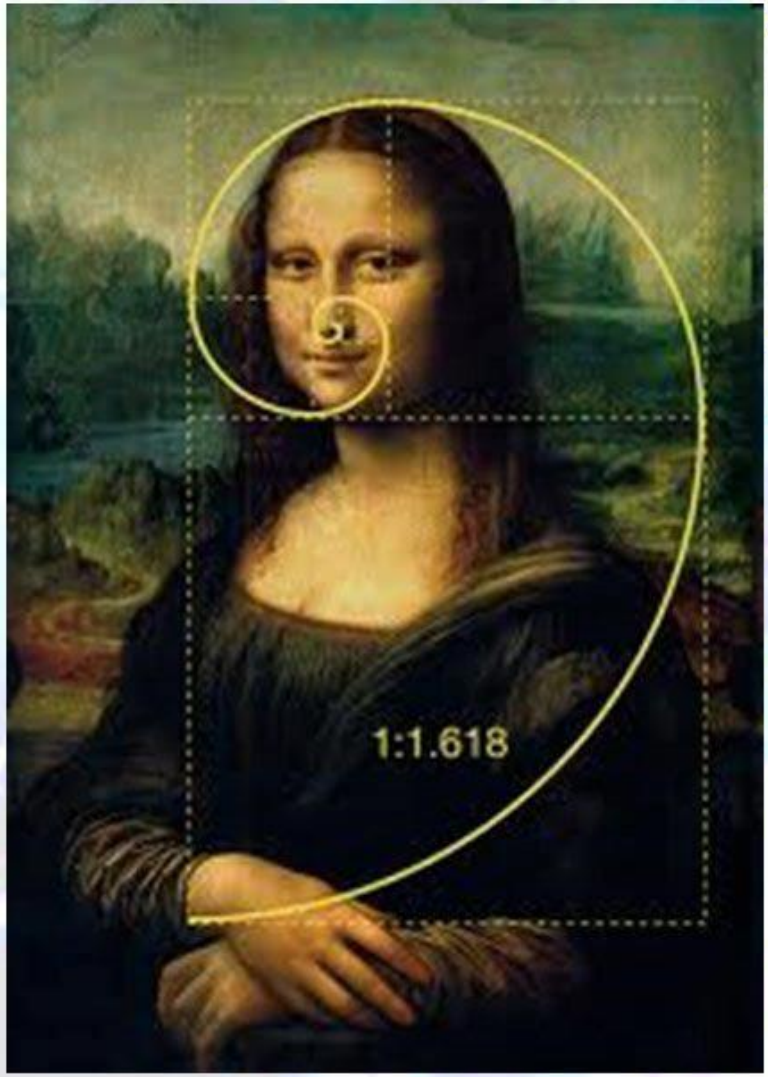
Геометрические фракталы

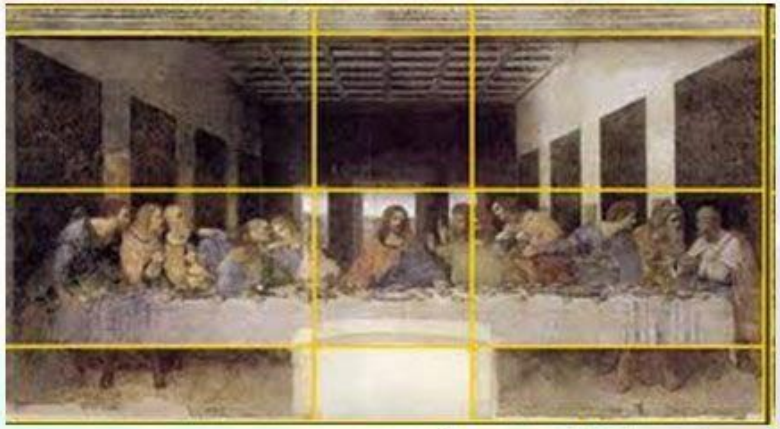


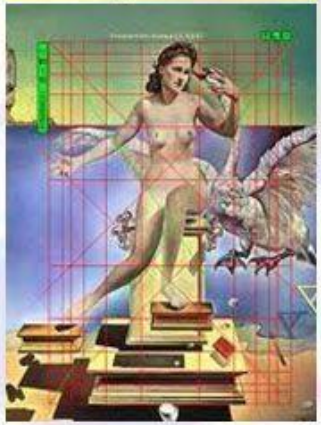





simone
PÉRÈLE

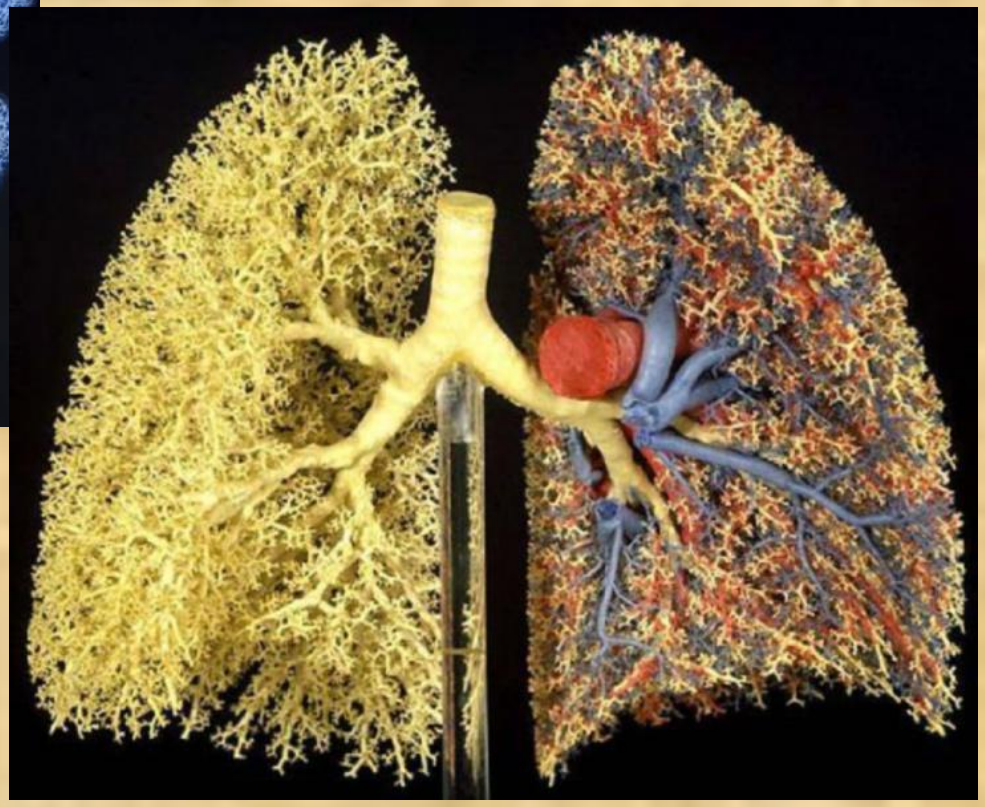

1:1.618

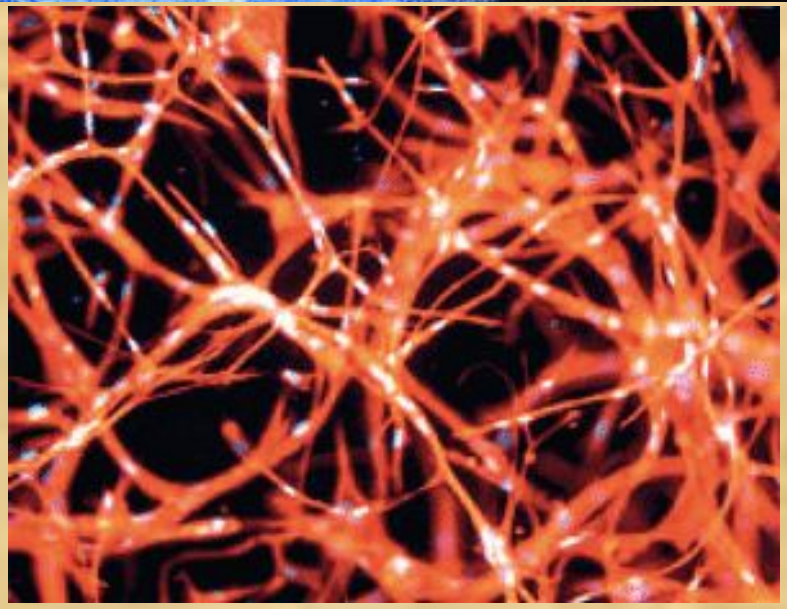




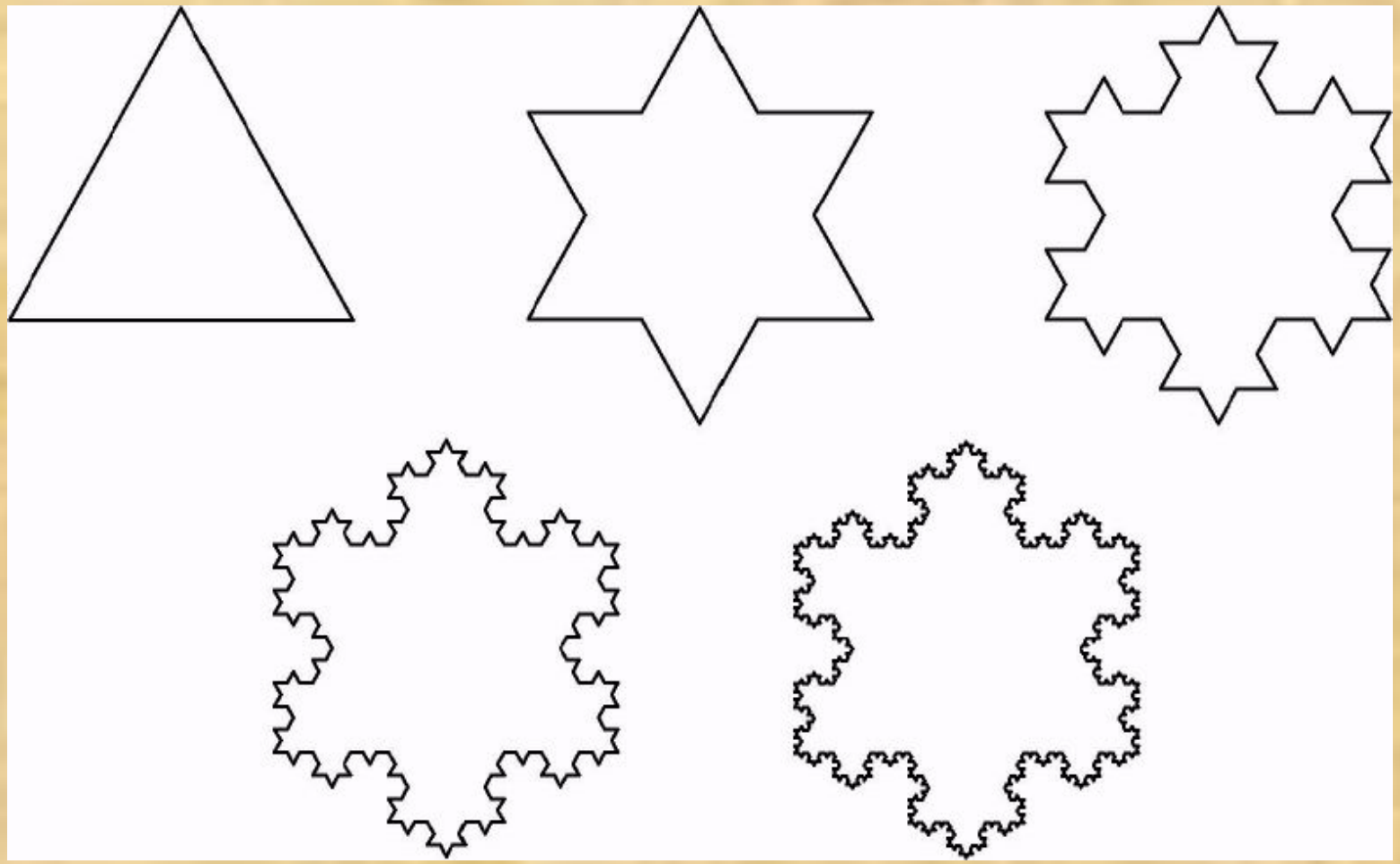
Кацусика Хокусай. Большая волна в Канагава

Винсент Ван Гог, «Звездная ночь»





Снежинка Коха



Алгебраические фракталы

$$X' = A * X + B * Y + E$$
$$Y' = C * X + D * Y + F$$

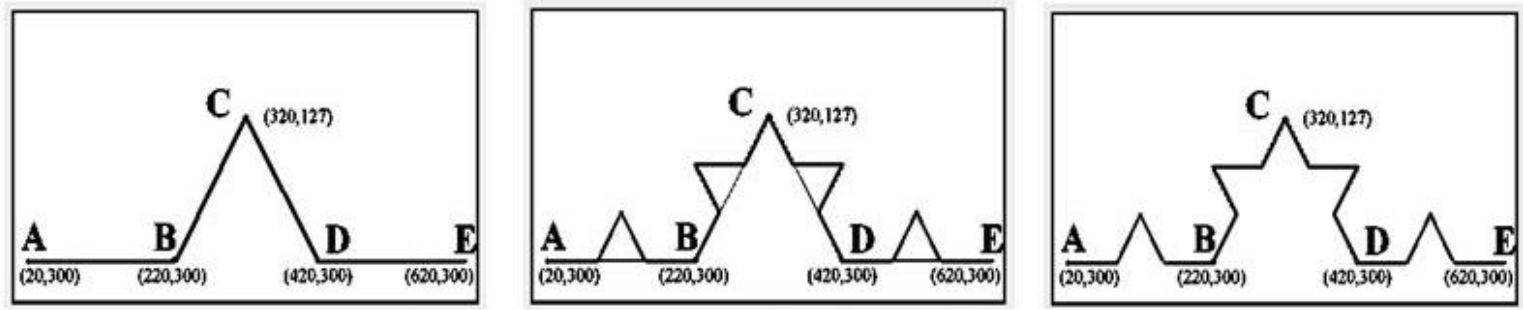
$$X' = (A1*X + B1*Y + C1) / (D1*X + E1*Y + F1)$$
$$Y' = (A2*X + B2*Y + C2) / (D2*X + E2*Y + F2)$$

$$X' = A1*X*X + B1*X*Y + C1*Y*Y + D1*X + E1*Y + F1$$
$$Y' = A2*X*X + B2*X*Y + C2*Y*Y + D2*X + E2*Y + F2$$

Алгоритм построения IFS -фрактала:

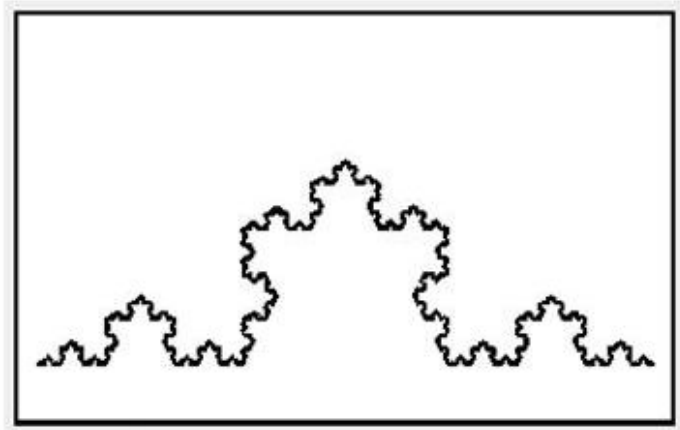
- Найти и закрасить начальную точку (X, Y) изображения.
- Выбрать одно из IFS-преобразований, найти координаты (X', Y') новой точки изображения и закрасить найденную точку.
- Принять $X = X'$ и $Y = Y'$.
- Повторить п.п. 2 и 3 алгоритма заданное число раз.

Построение IFS "снежинки" Коха.



Исходная заготовка на сетке координат 640 x 350.

База, преобразование, которому она подвергается и результат после одной итерации.



$$X' = 0.333*X + 13.333$$
$$Y' = 0.333*Y + 200$$

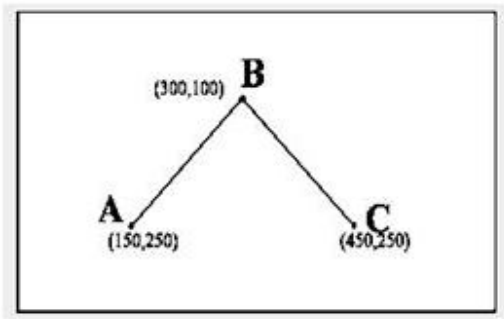
$$X' = 0.333*X + 413.333$$
$$Y' = 0.333*Y + 200$$

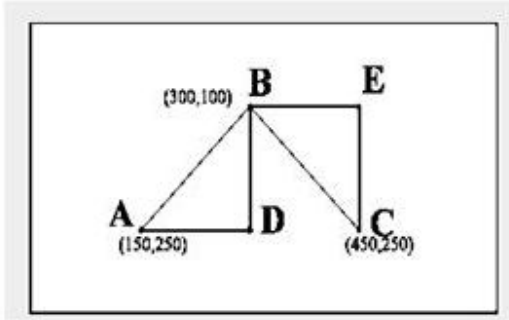
$$X' = 0.167*X + 0.289*Y + 130$$
$$Y' = -0.289*X + 0.167*Y + 256$$

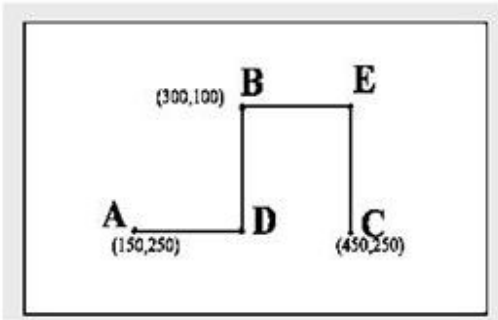
$$X' = 0.167*X - 0.289*Y + 403$$
$$Y' = 0.289*X + 0.167*Y + 71$$

Итоговая "снежинка" Коха и IFS (состоящее из 4-х преобразований), с помощью которых она была построена в том же прямоугольнике 640x350 за 10 итераций.

Построение IFS "дракона" Хартера-Хейтуэя.

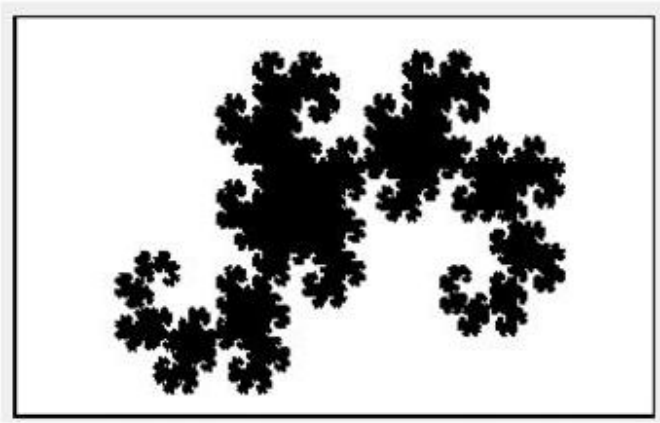






Исходная заготовка на сетке координат 640 x 350.

База, преобразование, которому она подвергается и результат после одной итерации.



X' = -0.5*X -0.5*Y + 490
Y' = 0.5*X -0.5*Y + 120

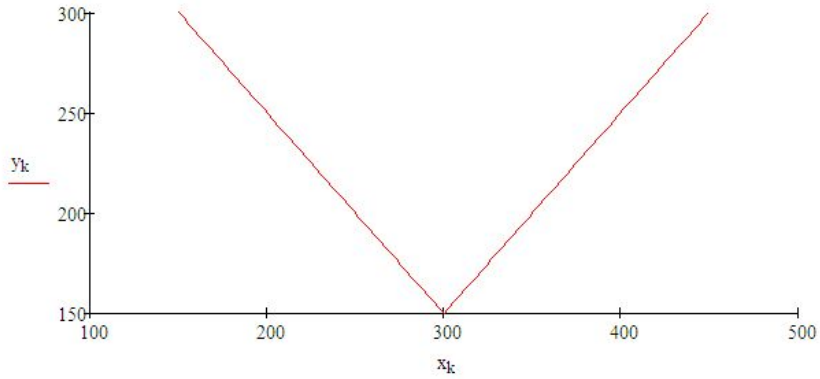
X' = 0.5*X -0.5*Y + 340
Y' = 0.5*X +0.5*Y - 110

Итоговый "дракон" Хартера-Хейтуэя и IFS (состоящее из 2-х преобразований), с помощью которых он был построен в том же прямоугольнике 640x350 за 512 итераций.

$a := 150 \qquad b := 450 \qquad n := 100 \qquad k := 0..n$

$$x_k := a + \frac{(b-a)}{n} \cdot k$$

$$y_k := \text{if}\left(x_k < 300, -x_k + 450, x_k - 150\right)$$

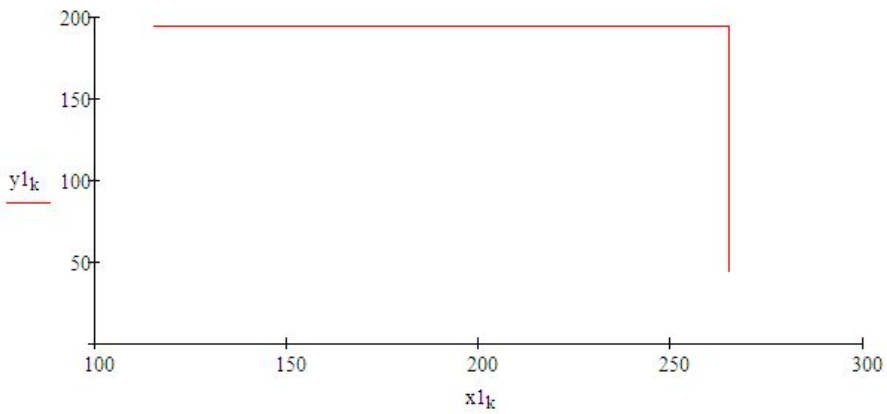


$$x1_k := -0.5\,x_k - 0.5\,y_k + 490$$

$$y1_k := 0.5\,x_k - 0.5\,y_k + 120$$

$x1_0 = 265 \qquad x1_n = 115$

$y1_0 = 45 \qquad y1_n = 195$

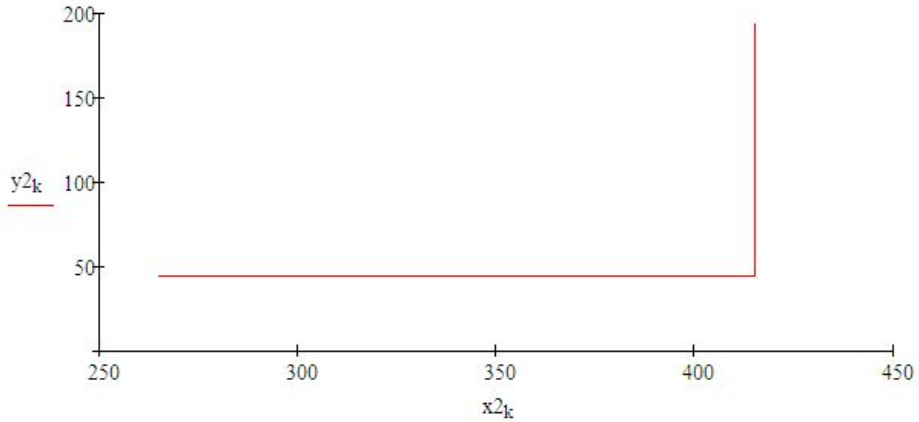


$$x2_k := 0.5\,x_k - 0.5\,y_k + 340$$

$$y2_k := 0.5\,x_k + 0.5\,y_k - 180$$

$x2_0 = 265 \qquad x2_n = 415$

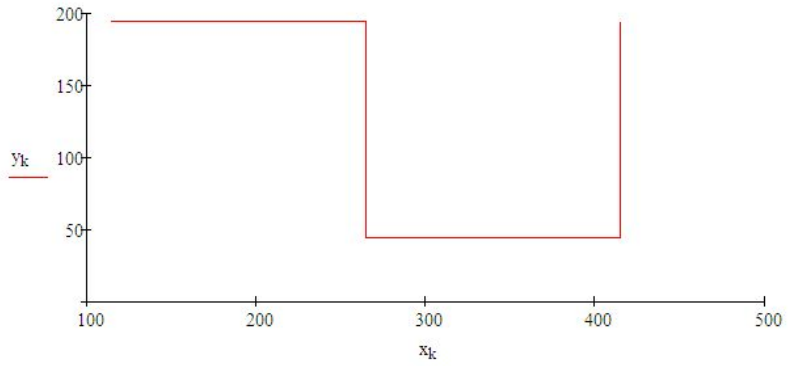
$y2_0 = 45 \qquad y2_n = 195$



$k := 0..2 \cdot n$

$x_k := \text{if}(k < n, x1_{n-k}, x2_{k-n})$

$y_k := \text{if}(k < n, y1_{n-k}, y2_{k-n})$

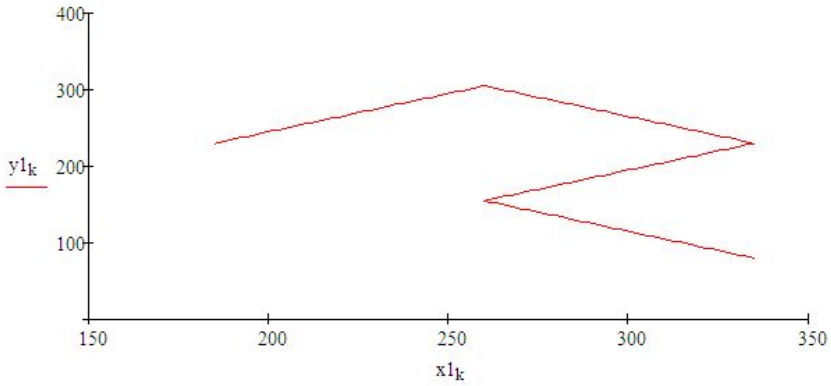


$x1_k := -0.5 x_k - 0.5 y_k + 490$

$y1_k := 0.5 x_k - 0.5 y_k + 120$

$x1_0 = 335$ $x1_n = 335$

$y1_0 = 80$ $y1_n = 230$

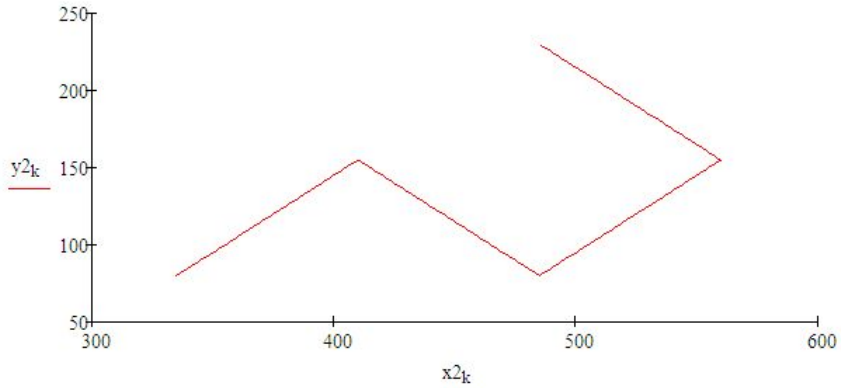


$x2_k := 0.5 x_k - 0.5 y_k + 375$

$y2_k := 0.5 x_k + 0.5 y_k - 75$

$x2_0 = 335$ $x2_n = 485$

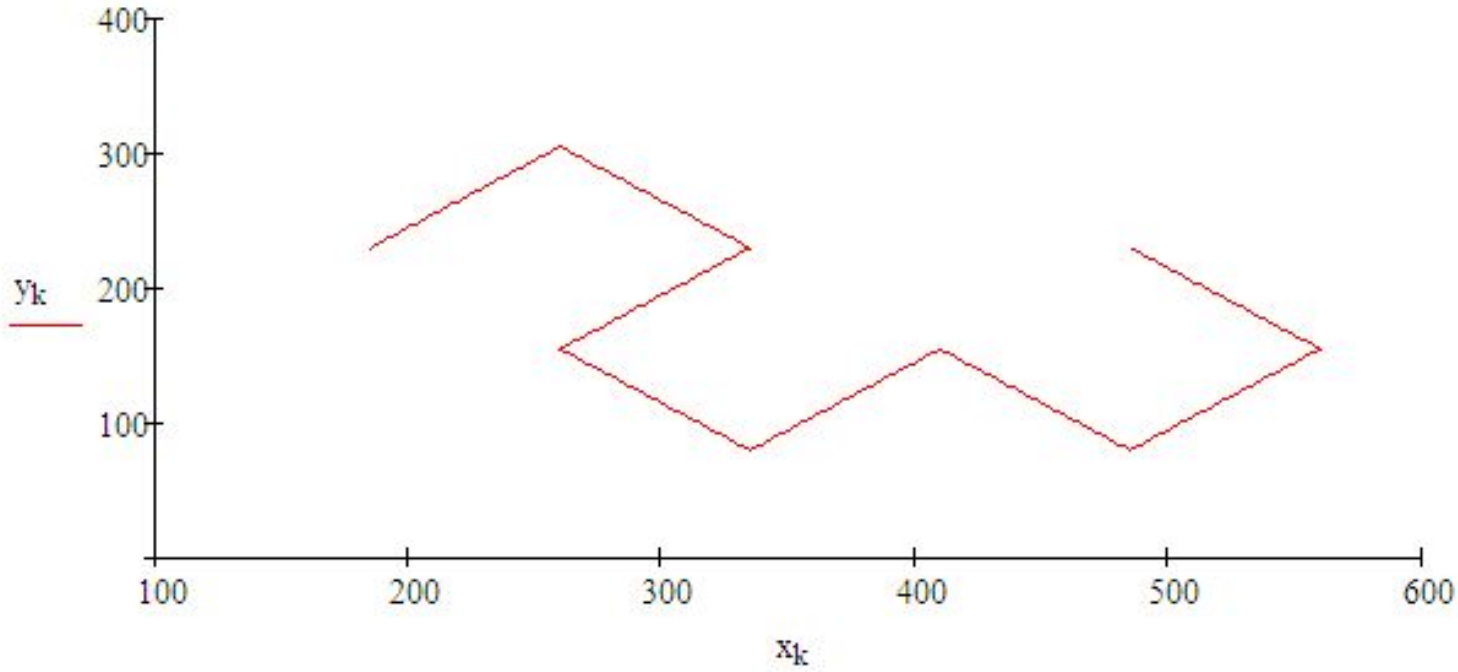
$y2_0 = 80$ $y2_n = 80$



$k := 0 .. 4 \cdot n$

$$x_k := \text{if}\left(k < 2n , x1_{2n-k} , x2_{k-2n}\right)$$

$$y_k := \text{if}\left(k < 2n , y1_{2n-k} , y2_{k-2n}\right)$$

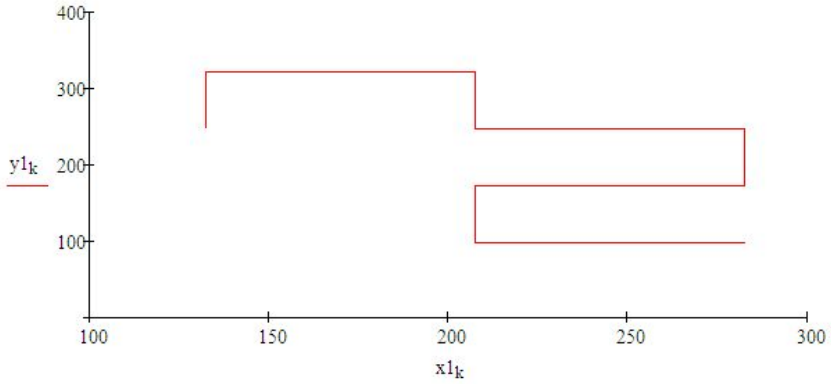


$x1_k := -0.5\,x_k - 0.5\,y_k + 490$

$y1_k := 0.5\,x_k - 0.5\,y_k + 120$

$x1_0 = 282.5 \qquad x1_n = 207.5$

$y1_0 = 97.5 \qquad y1_n = 172.5$

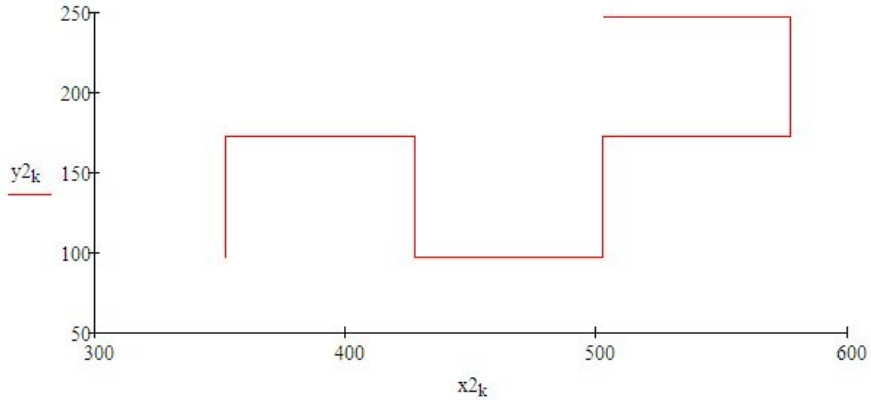


$x2_k := 0.5\,x_k - 0.5\,y_k + 375$

$y2_k := 0.5\,x_k + 0.5\,y_k - 110$

$x2_0 = 352.5 \qquad x2_n = 427.5$

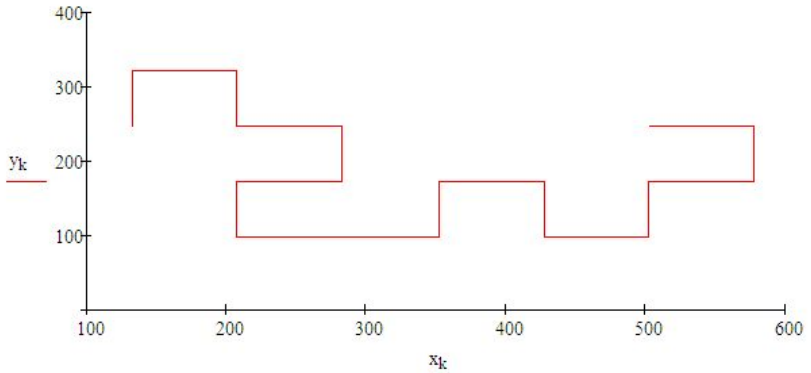
$y2_0 = 97.5 \qquad y2_n = 172.5$



$k := 0..8 \cdot n$

$x_k := \text{if}\left(k < 4n, x1_{4n-k}, x2_{k-4n}\right)$

$y_k := \text{if}\left(k < 4n, y1_{4n-k}, y2_{k-4n}\right)$

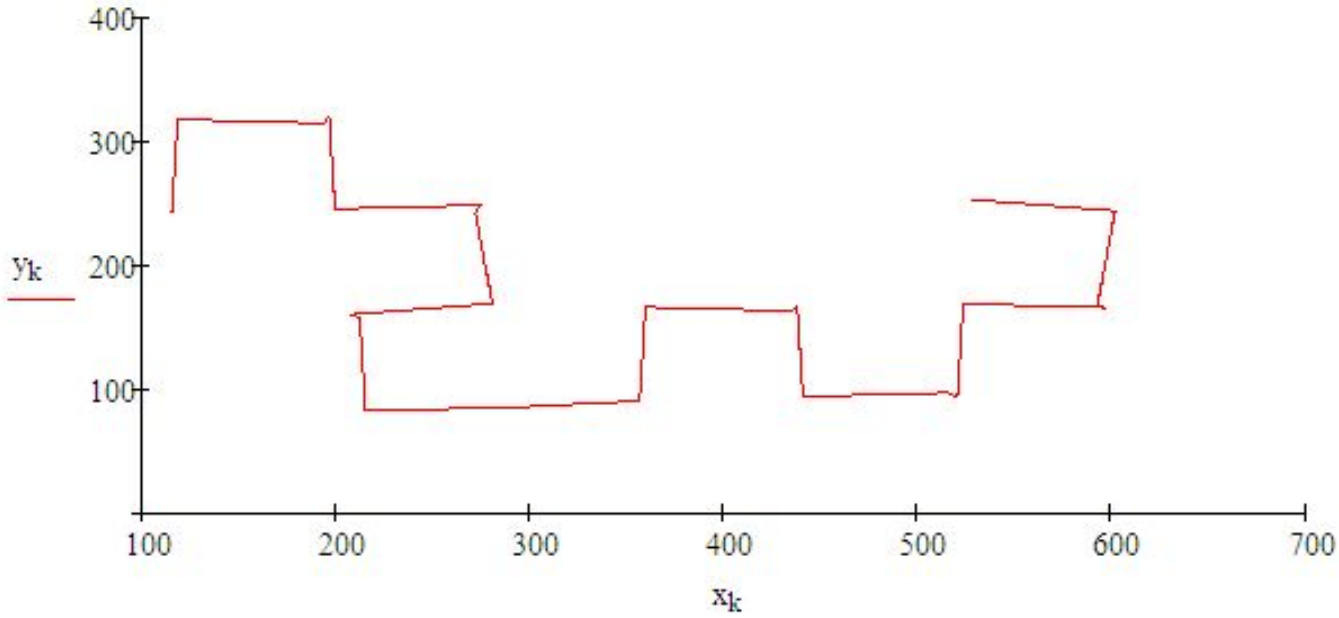


$x1_k := -0.52 x_k - 0.48 y_k + 490$ $\quad x2_k := 0.52 x_k - 0.48 y_k + 375$

$y1_k := 0.48 x_k - 0.52 y_k + 120$ $\quad y2_k := 0.48 x_k + 0.52 y_k - 110$

$k := 0 .. 8 \cdot n$

$x_k := \text{if}\left(k < 4n , x1_{4n-k} , x2_{k-4n}\right)$ $\quad y_k := \text{if}\left(k < 4n , y1_{4n-k} , y2_{k-4n}\right)$

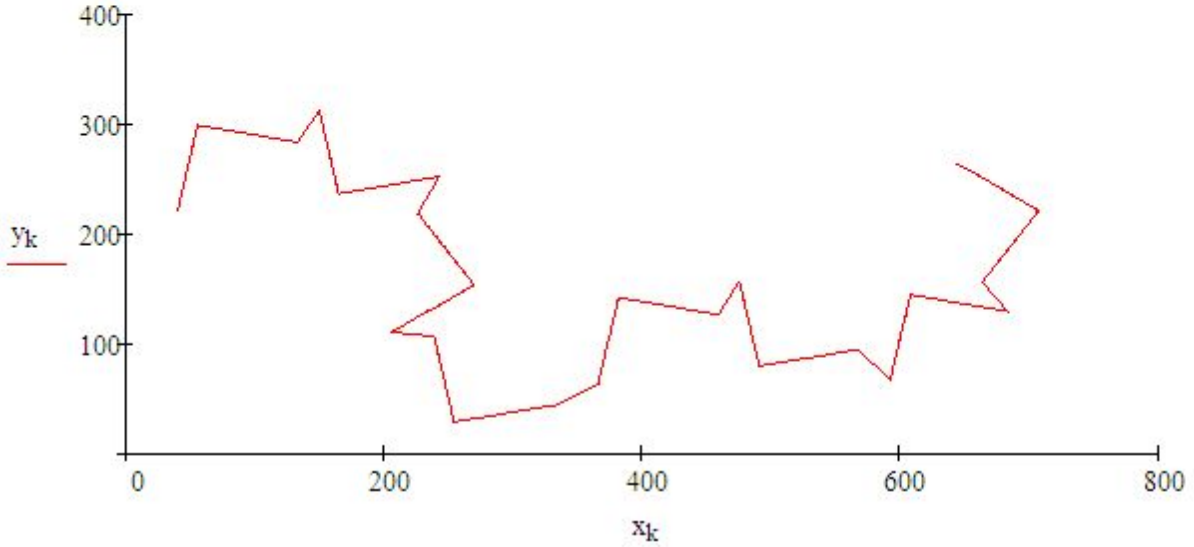


$x1_k := -0.6 x_k - 0.4 y_k + 490$ $x2_k := 0.6 x_k - 0.4 y_k + 375$

$y1_k := 0.4 x_k - 0.6 y_k + 120$ $y2_k := 0.4 x_k + 0.6 y_k - 110$

$k := 0 .. 8 \cdot n$

$x_k := \text{if}\left(k < 4n, x1_{4n-k}, x2_{k-4n}\right)$ $y_k := \text{if}\left(k < 4n, y1_{4n-k}, y2_{k-4n}\right)$

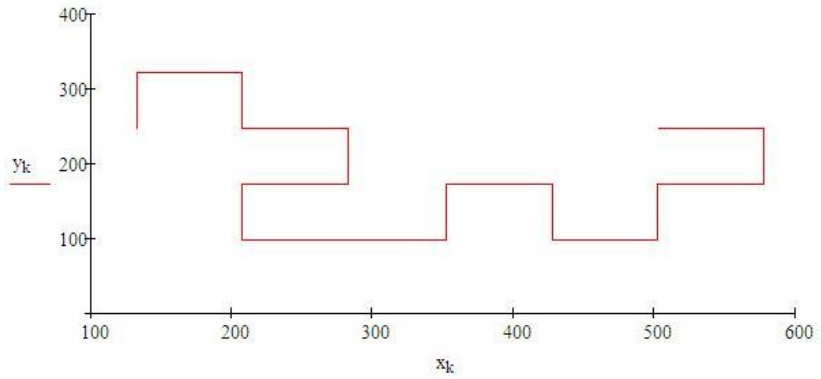


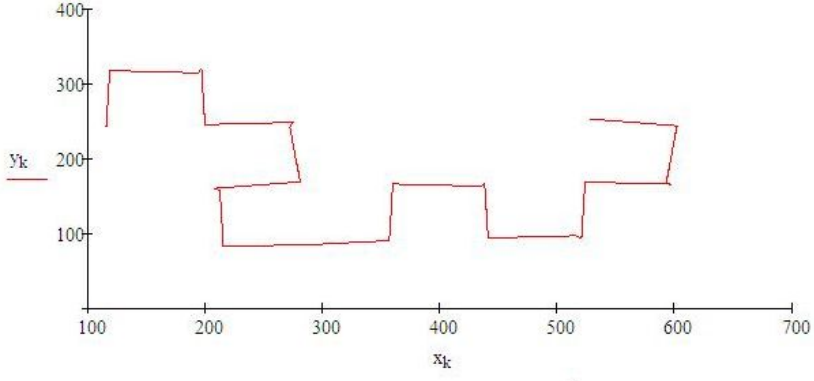
Mathcad - J3

Файл Правка Вид Вставка Формат Инструменты Символьные операции Окно Справка

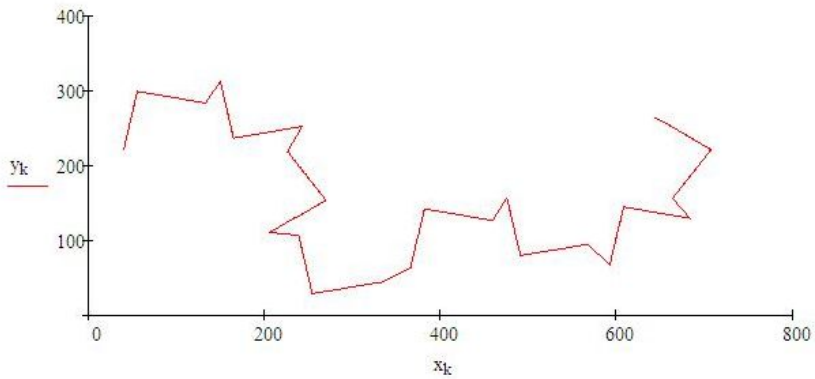
100%

Normal Arial 10



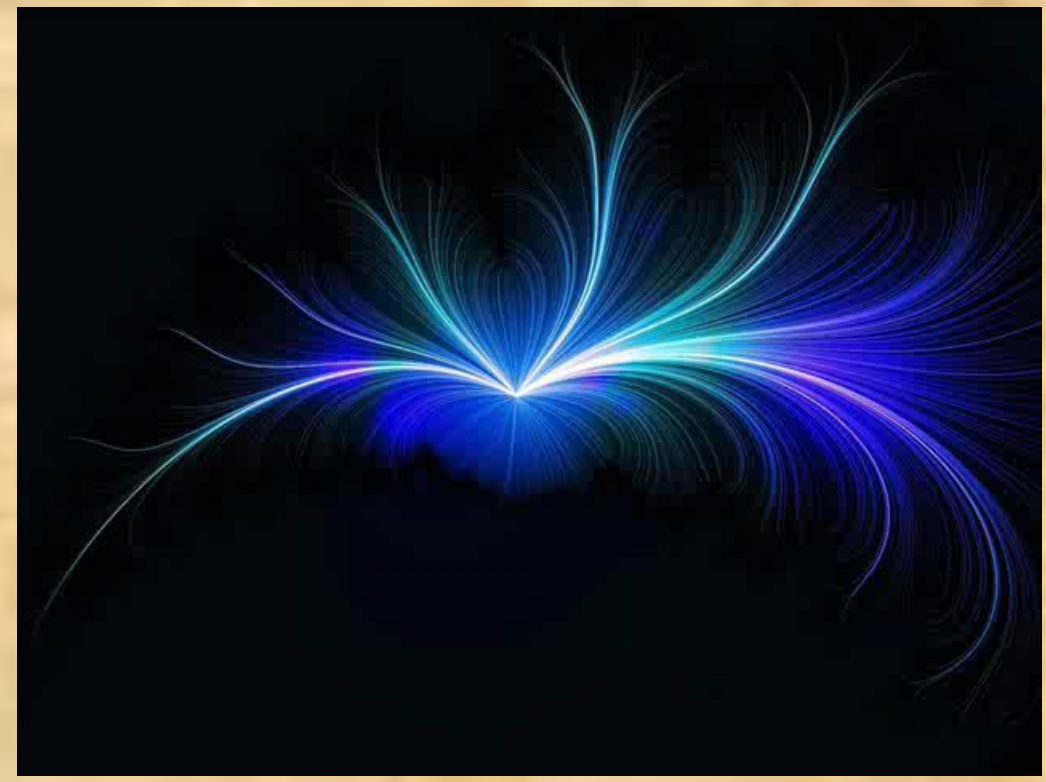


J3

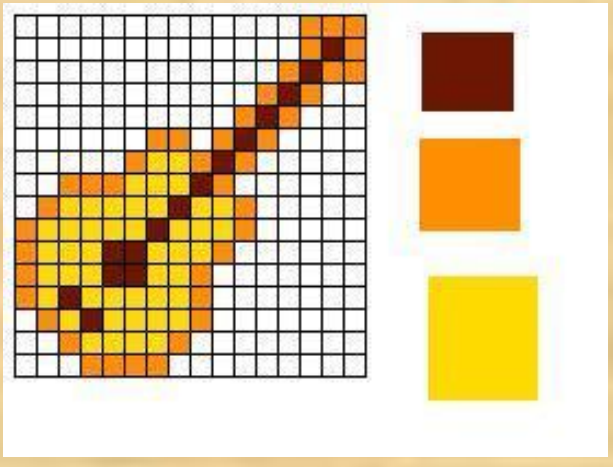


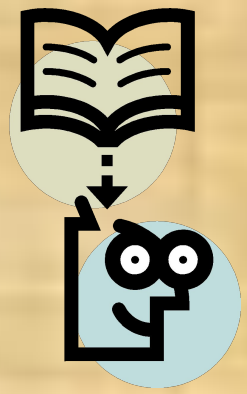
Нажмите F1, чтобы открыть справку.

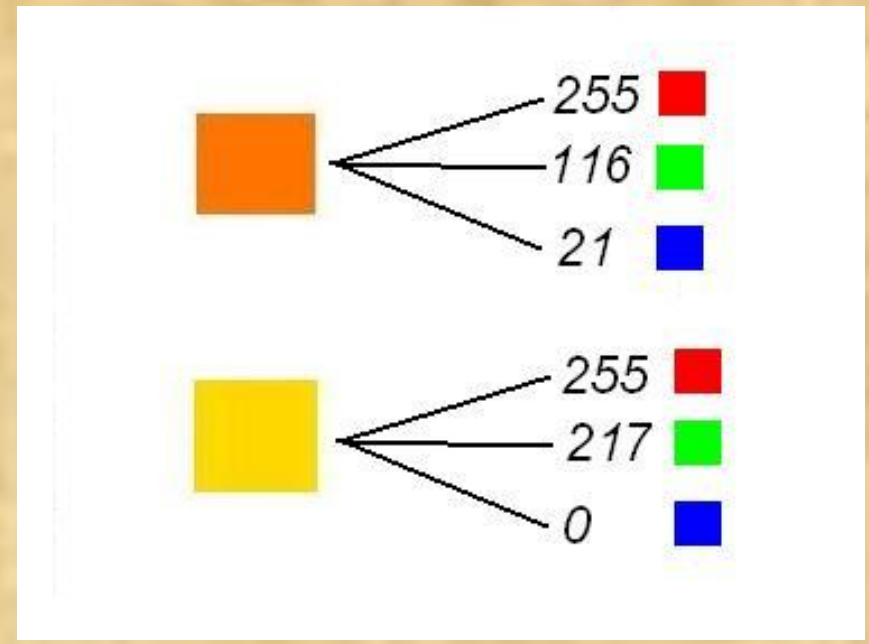
АВТО

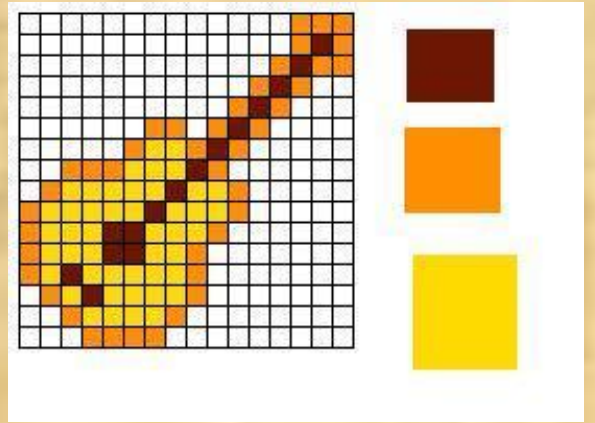


Шаг 0: RGB-формат





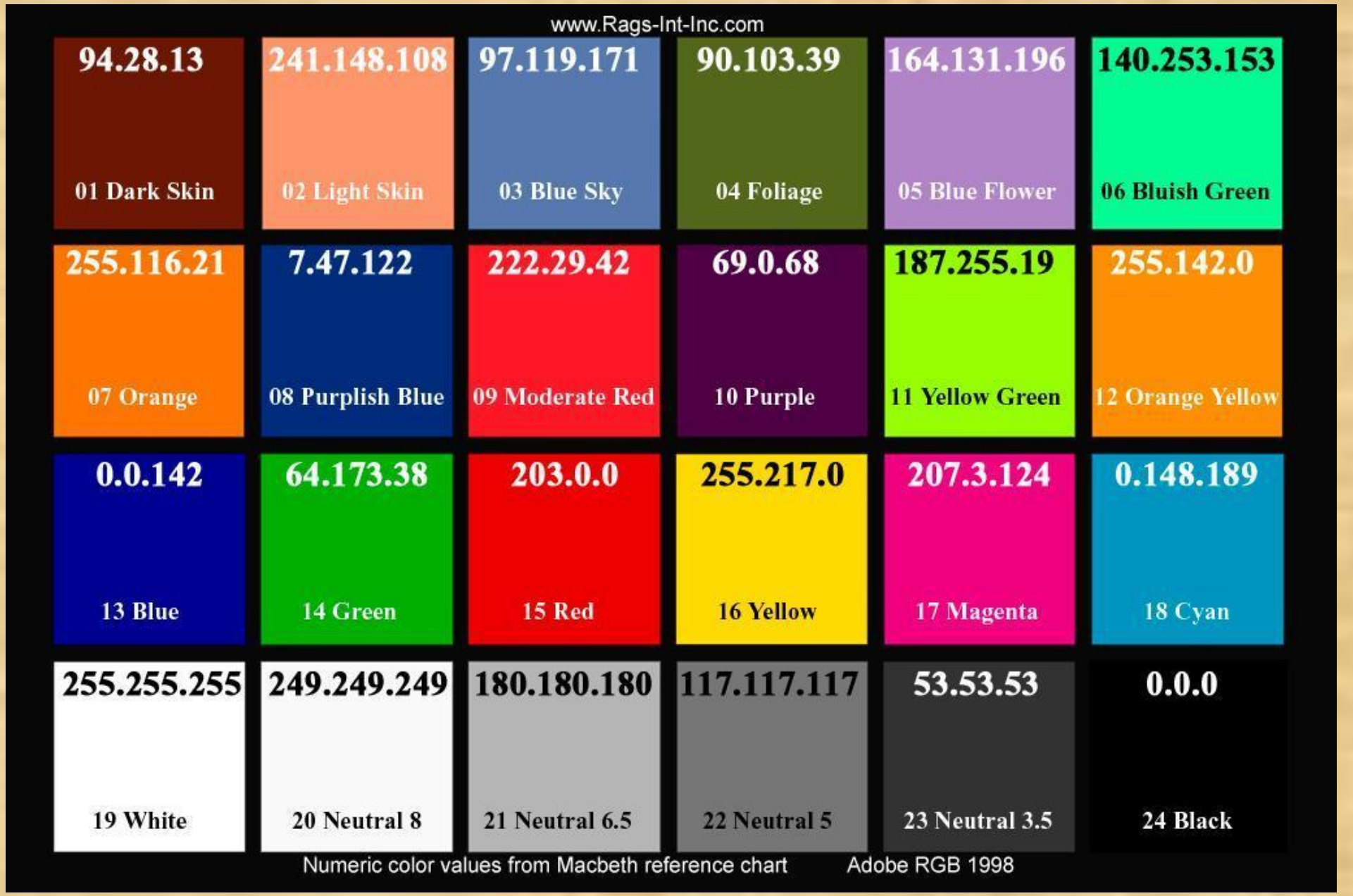




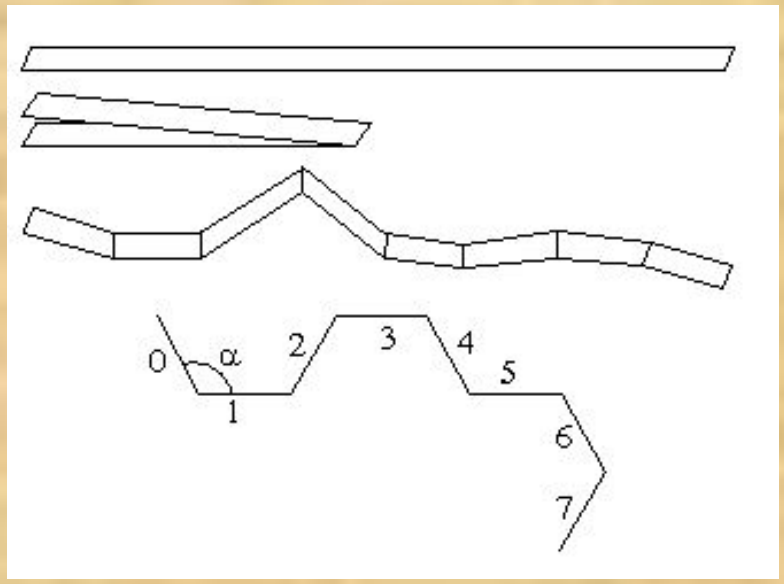
$$r := \begin{pmatrix}
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 94 & 255 \\
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 94 & 255 & 255 \\
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 94 & 255 & 255 & 255 \\
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 94 & 255 & 255 & 255 & 255 \\
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 94 & 255 & 255 & 255 & 255 & 255 \\
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 94 & 255 & 255 & 255 & 255 & 255 & 255 \\
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 94 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\
255 & 255 & 255 & 255 & 255 & 255 & 255 & 94 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\
255 & 255 & 255 & 255 & 255 & 255 & 94 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\
255 & 255 & 255 & 255 & 94 & 94 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\
255 & 255 & 255 & 255 & 94 & 94 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\
255 & 255 & 94 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\
255 & 255 & 255 & 94 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255
\end{pmatrix}$$

$$g := \begin{pmatrix}
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 142 & 142 & 142 \\
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 142 & 28 & 142 \\
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 142 & 28 & 142 & 142 \\
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 142 & 28 & 142 & 255 & 255 \\
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 142 & 28 & 142 & 255 & 255 & 255 \\
255 & 255 & 255 & 255 & 255 & 255 & 142 & 142 & 255 & 142 & 28 & 142 & 255 & 255 & 255 & 255 \\
255 & 255 & 255 & 255 & 255 & 142 & 217 & 217 & 142 & 28 & 142 & 255 & 255 & 255 & 255 & 255 \\
255 & 255 & 142 & 142 & 142 & 217 & 217 & 217 & 28 & 142 & 255 & 255 & 255 & 255 & 255 & 255 \\
255 & 142 & 217 & 217 & 217 & 217 & 217 & 28 & 217 & 217 & 142 & 255 & 255 & 255 & 255 & 255 \\
142 & 217 & 217 & 217 & 217 & 217 & 28 & 217 & 217 & 217 & 142 & 255 & 255 & 255 & 255 & 255 \\
142 & 217 & 217 & 217 & 28 & 28 & 217 & 217 & 217 & 142 & 255 & 255 & 255 & 255 & 255 & 255 \\
142 & 217 & 217 & 217 & 28 & 28 & 217 & 217 & 142 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\
142 & 217 & 28 & 217 & 217 & 217 & 217 & 217 & 142 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\
255 & 142 & 217 & 28 & 217 & 217 & 217 & 217 & 142 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\
255 & 255 & 142 & 217 & 217 & 217 & 217 & 142 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\
255 & 255 & 255 & 142 & 142 & 142 & 142 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255
\end{pmatrix}$$

$$b := \begin{pmatrix}
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 0 & 0 & 0 \\
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 0 & 13 & 0 \\
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 0 & 13 & 0 & 0 \\
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 0 & 13 & 0 & 255 & 255 \\
255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 0 & 13 & 0 & 255 & 255 & 255 \\
255 & 255 & 255 & 255 & 255 & 255 & 0 & 0 & 255 & 0 & 13 & 0 & 255 & 255 & 255 & 255 \\
255 & 255 & 255 & 255 & 255 & 0 & 0 & 0 & 0 & 13 & 0 & 255 & 255 & 255 & 255 & 255 \\
255 & 255 & 0 & 0 & 0 & 0 & 0 & 0 & 13 & 0 & 255 & 255 & 255 & 255 & 255 & 255 \\
255 & 0 & 0 & 0 & 0 & 0 & 0 & 13 & 0 & 0 & 0 & 255 & 255 & 255 & 255 & 255 \\
0 & 0 & 0 & 0 & 0 & 0 & 13 & 0 & 0 & 0 & 0 & 255 & 255 & 255 & 255 & 255 \\
0 & 0 & 0 & 0 & 13 & 13 & 0 & 0 & 0 & 0 & 255 & 255 & 255 & 255 & 255 & 255 \\
0 & 0 & 0 & 0 & 13 & 13 & 0 & 0 & 0 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\
0 & 0 & 13 & 0 & 0 & 0 & 0 & 0 & 0 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\
255 & 0 & 0 & 13 & 0 & 0 & 0 & 0 & 0 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\
255 & 255 & 0 & 0 & 0 & 0 & 0 & 0 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\
255 & 255 & 255 & 0 & 0 & 0 & 0 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255
\end{pmatrix}$$

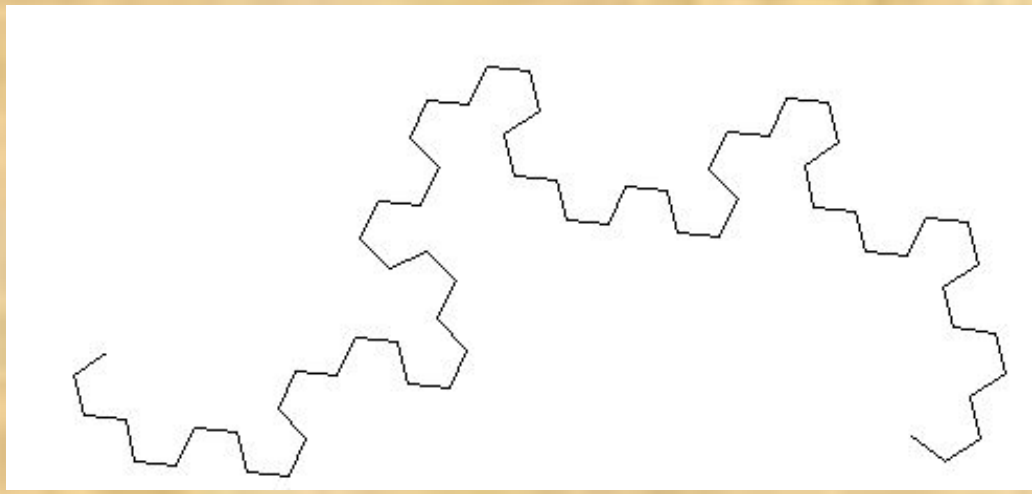

www.Rags-Int-Inc.com
94.28.13
01 Dark Skin
241.148.108
02 Light Skin
97.119.171
03 Blue Sky
90.103.39
04 Foliage
164.131.196
05 Blue Flower
140.253.153
06 Bluish Green
255.116.21
07 Orange
7.47.122
08 Purplish Blue
222.29.42
09 Moderate Red
69.0.68
10 Purple
187.255.19
11 Yellow Green
255.142.0
12 Orange Yellow
0.0.142
13 Blue
64.173.38
14 Green
203.0.0
15 Red
255.217.0
16 Yellow
207.3.124
17 Magenta
0.148.189
18 Cyan
255.255.255
19 White
249.249.249
20 Neutral 8
180.180.180
21 Neutral 6.5
117.117.117
22 Neutral 5
53.53.53
23 Neutral 3.5
0.0.0
24 Black
Numeric color values from Macbeth reference chart
Adobe RGB 1998

Дракон Хартера-Хейтуэя **из полоски бумаги**



n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
d_n	1	1	0	1	1	0	0	1	1	0	0	0	1	0	0	1

$$d(16) = d(8) = d(4) = d(2) = d(1) = 1,$$
$$d(12) = d(6) = d(3) = -1,$$
$$d(10) = d(5) = 1.$$



Пример работы основного алгоритма.

Текст 1.

Есть близнецы. Для земнородных -
Два божества. То Смерть и Сон.
Как брат с сестрою дивно сходных
Она угрюмей, кротче Он.

в двоичной кодировке

..... 1111000011001010000110000001010.....

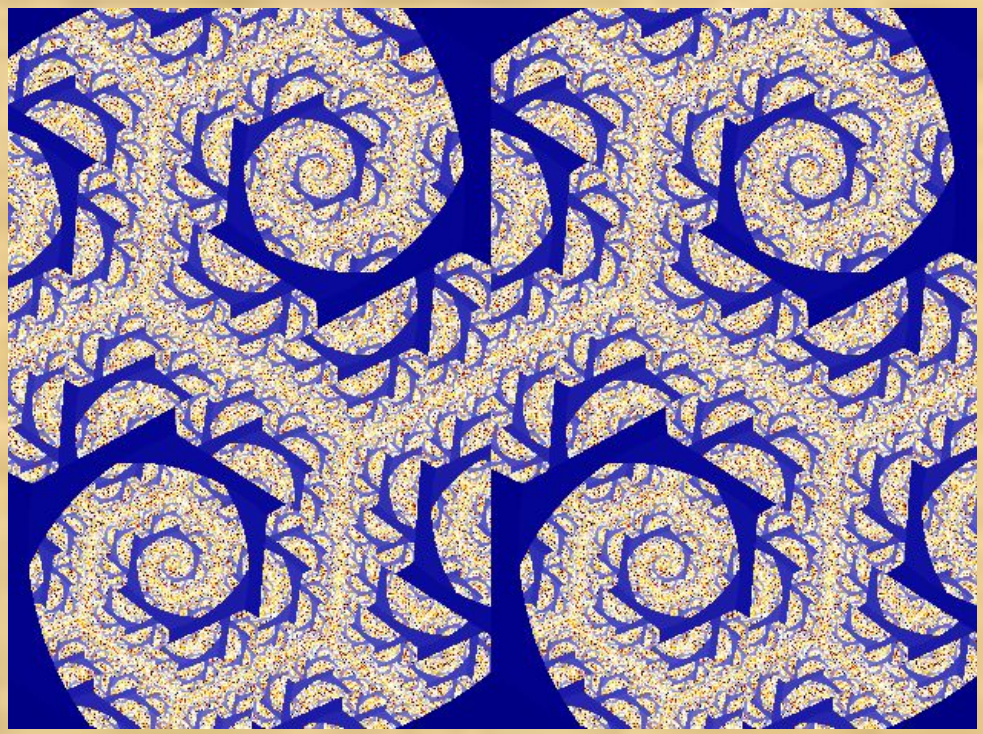
Текст 2.

Есть близнецы. Для земнородных -
Две божества. То Смерть и Сон.
Как брат с сестрою дивно сходных
Она угрюмей, кротче Он.

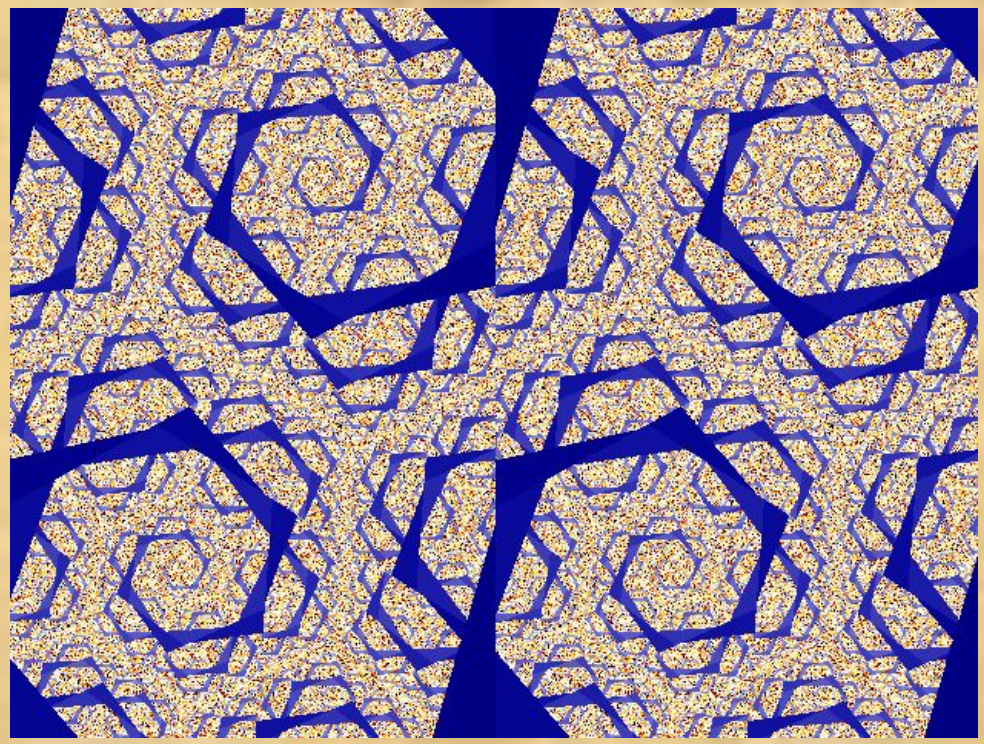
в двоичной кодировке

.....1111000011001010000110010001010.....

В стандартной двоичной кодировке буквы «а» и «в» отличаются всего лишь на бит.



Фрактал, соответствующий Тексту 1.



Фрактал, соответствующий Тексту 2.

Спасибо за внимание!