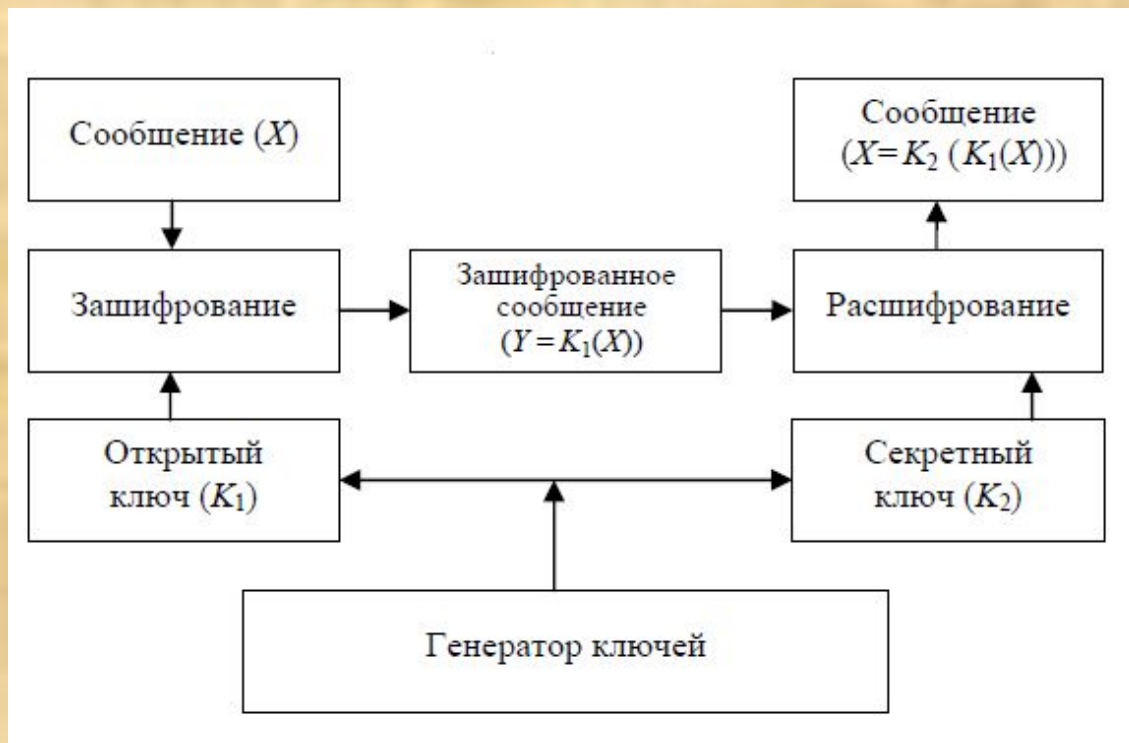
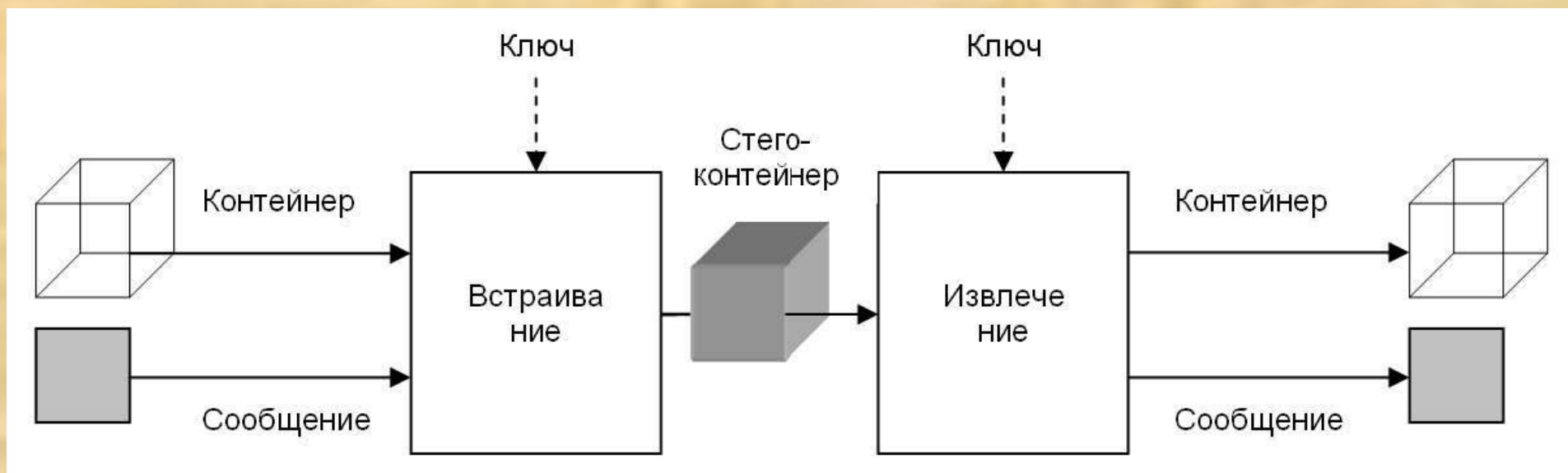


***Возможные применения
теории фракталов в
криптографии***

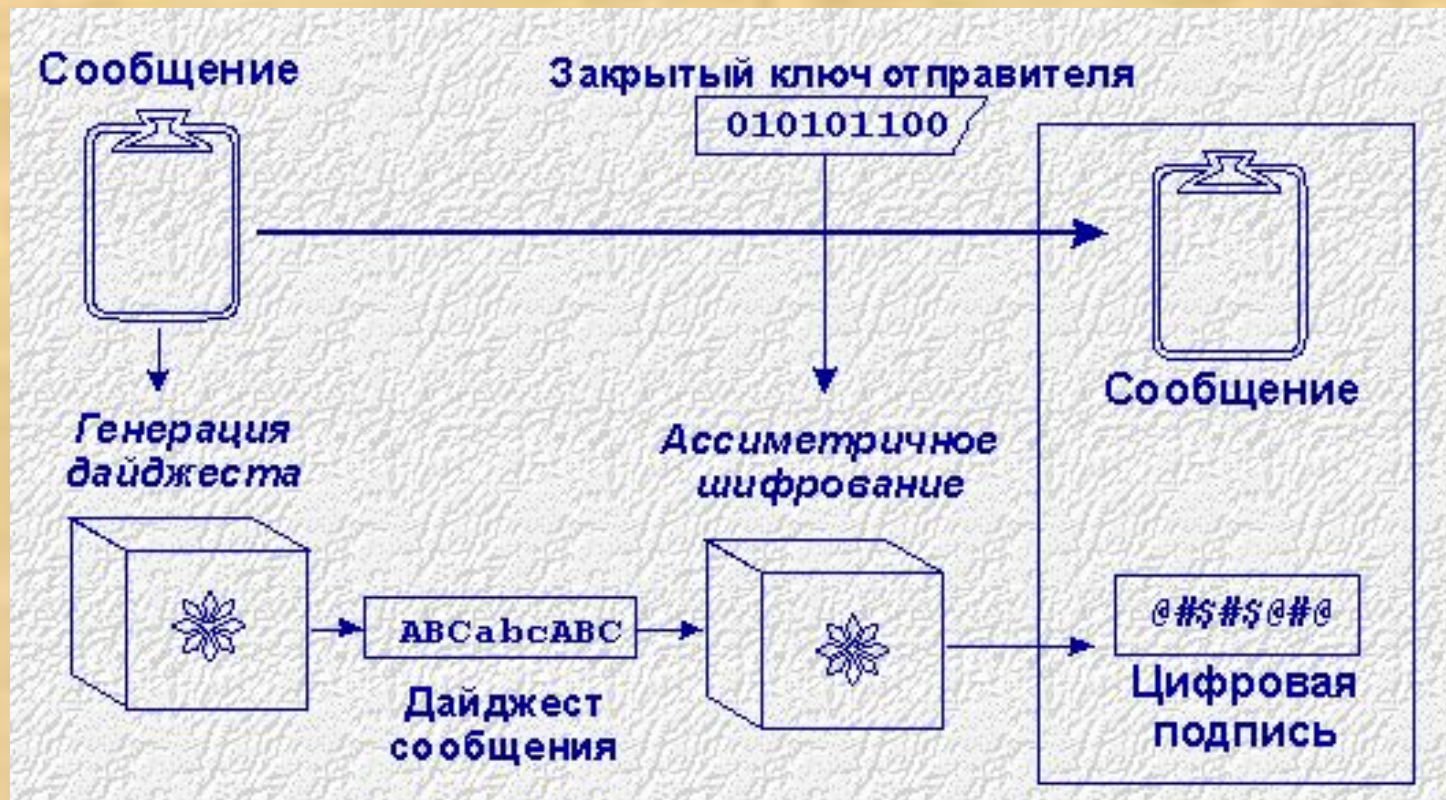
Ассиметричное шифрование с открытым ключом:



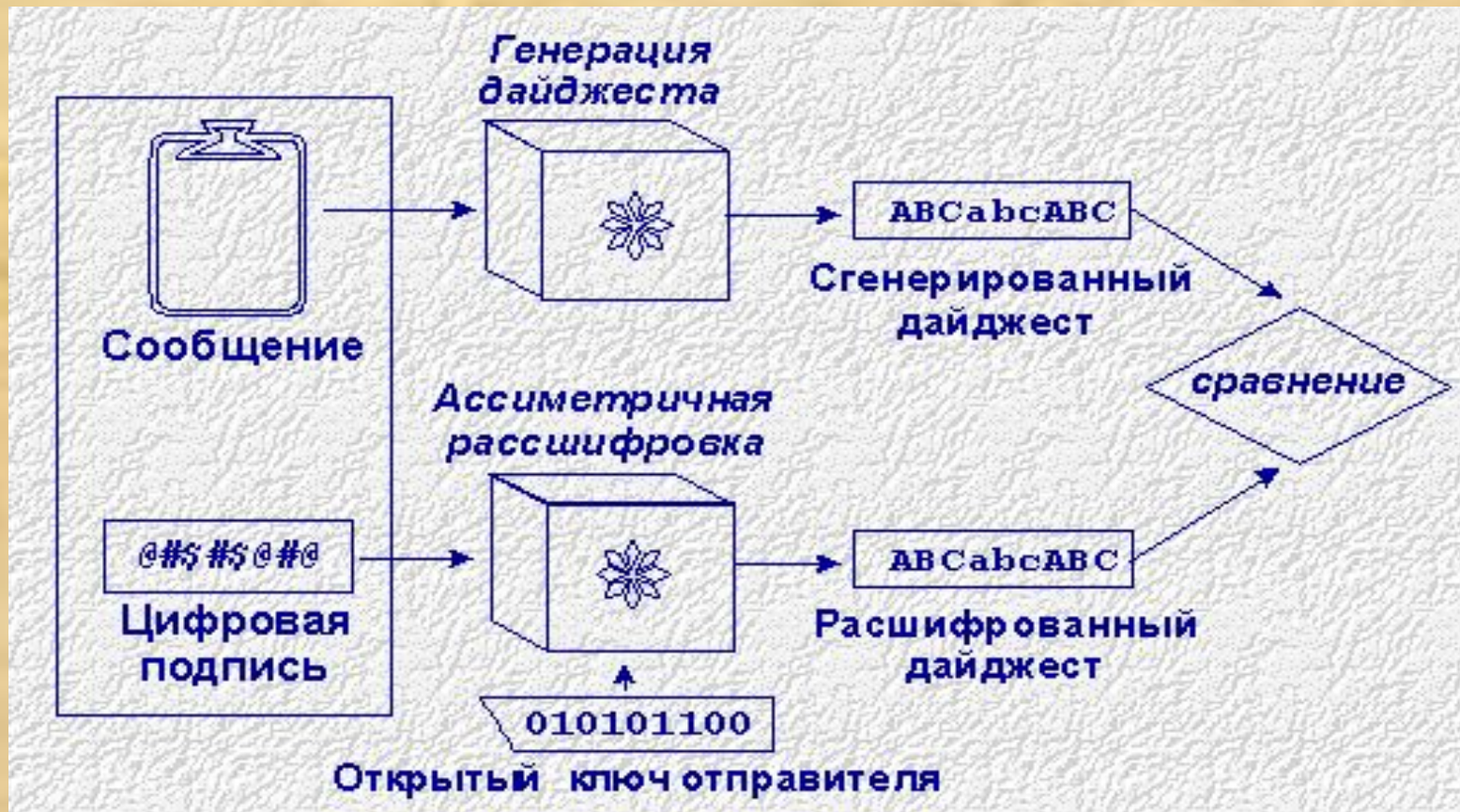
Общий принцип стеганографического сеанса:



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 t должно быть вычислительно невозможно найти блок данных X , для которого $H(X)=t$.
- 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.



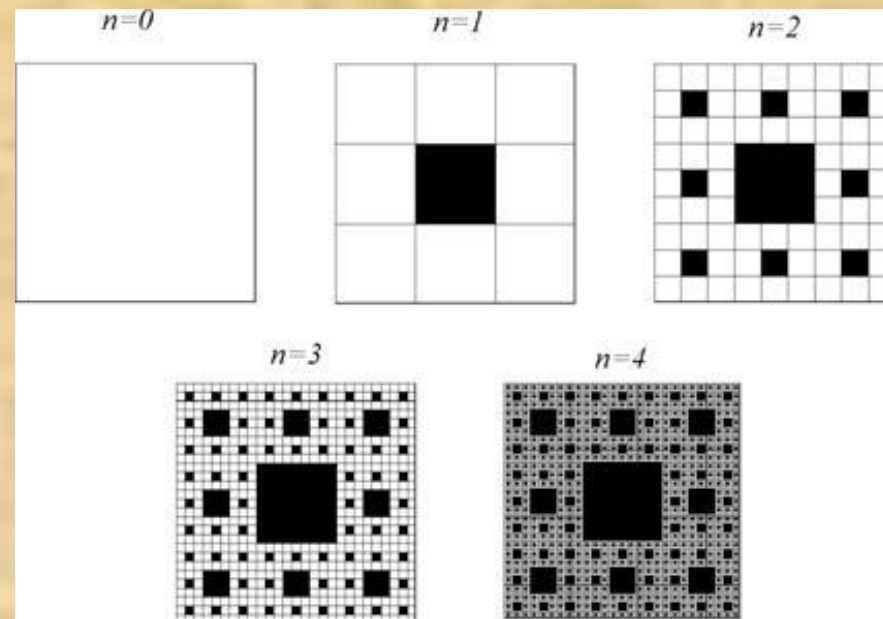
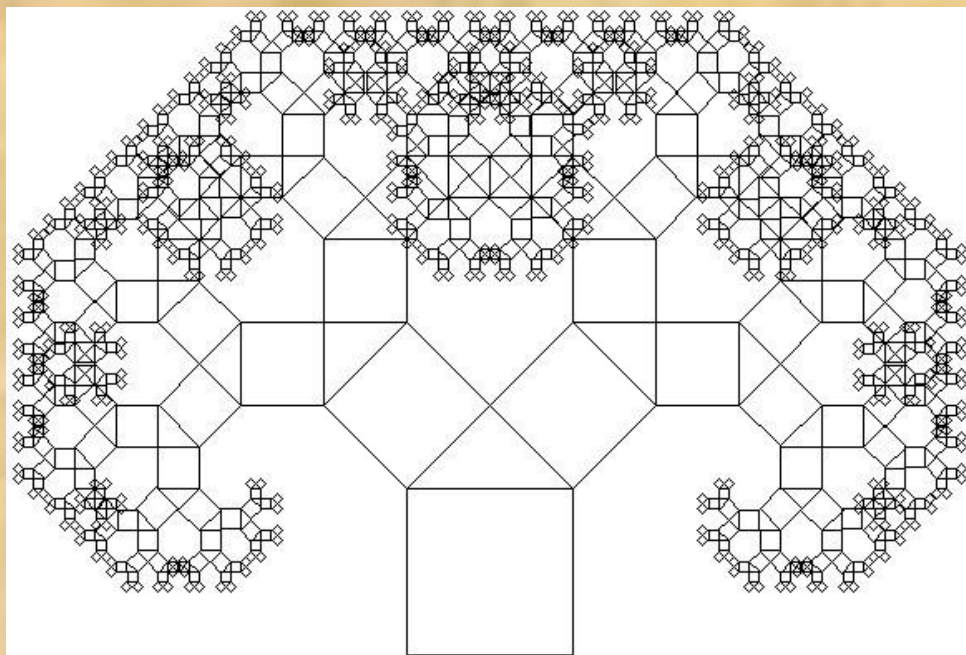
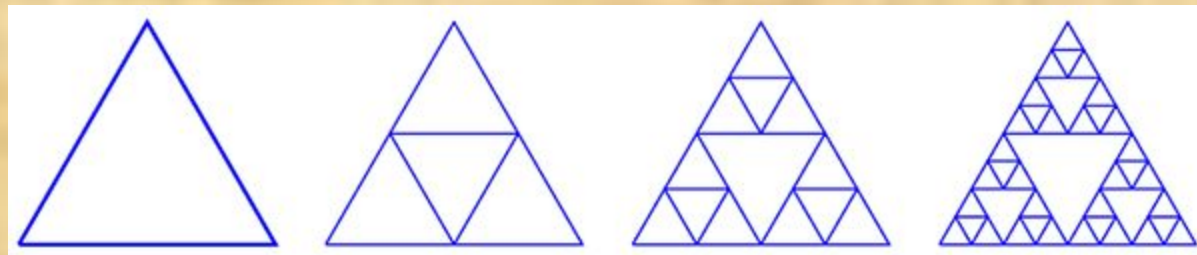
Фракталы в природе







Геометрические фракталы



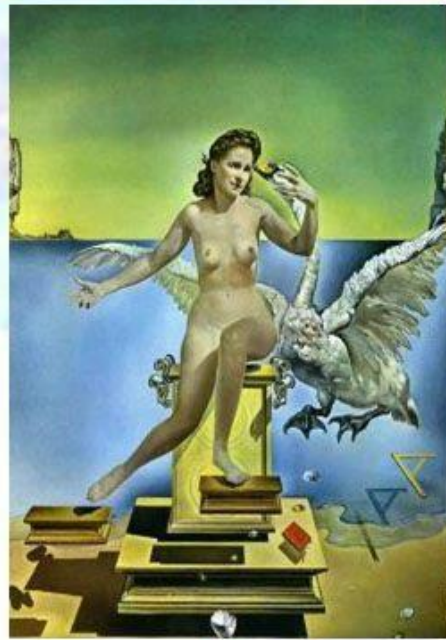
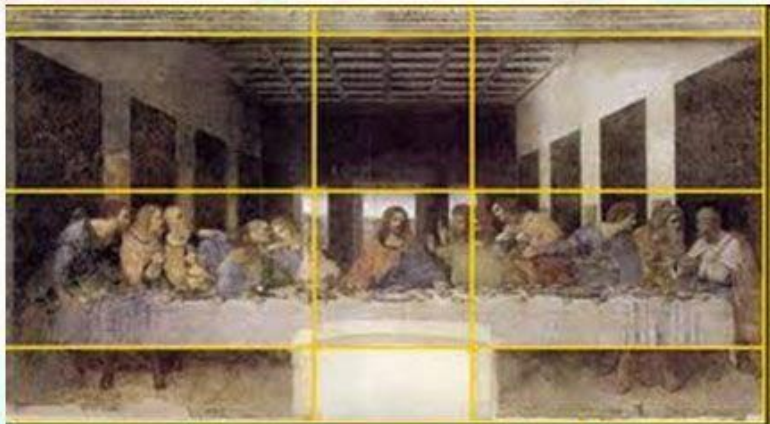
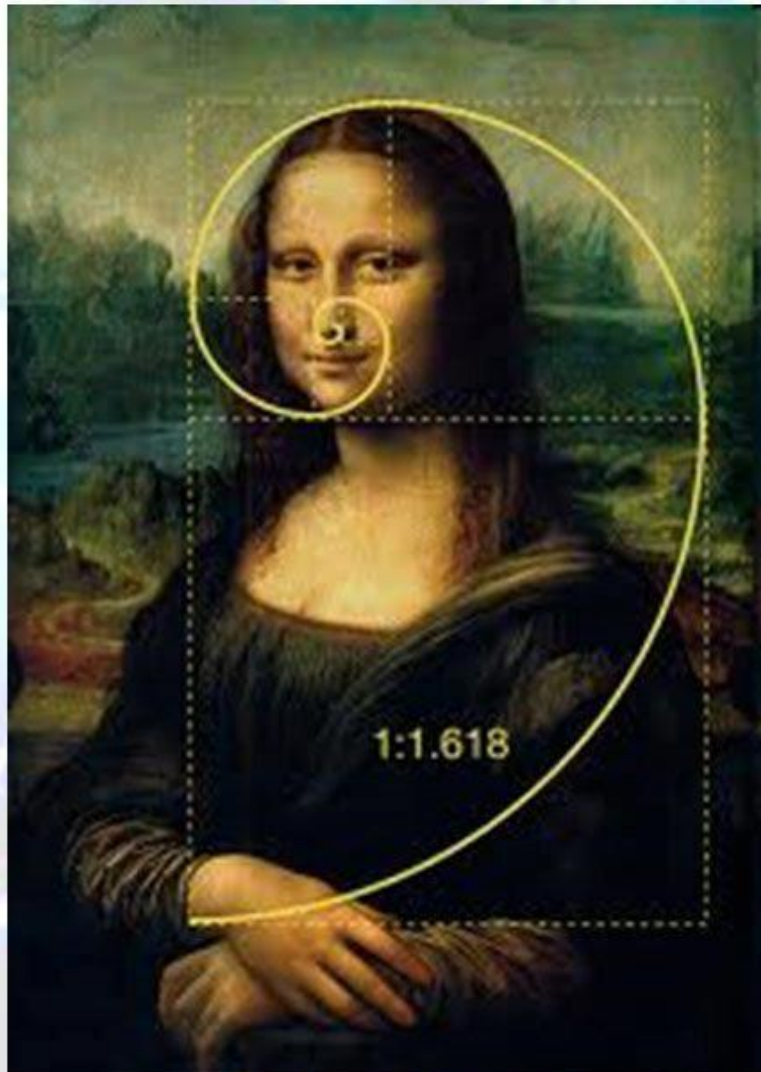


BE LIKE THE FRENCH. WEAR SEXY.

simone
PERELE





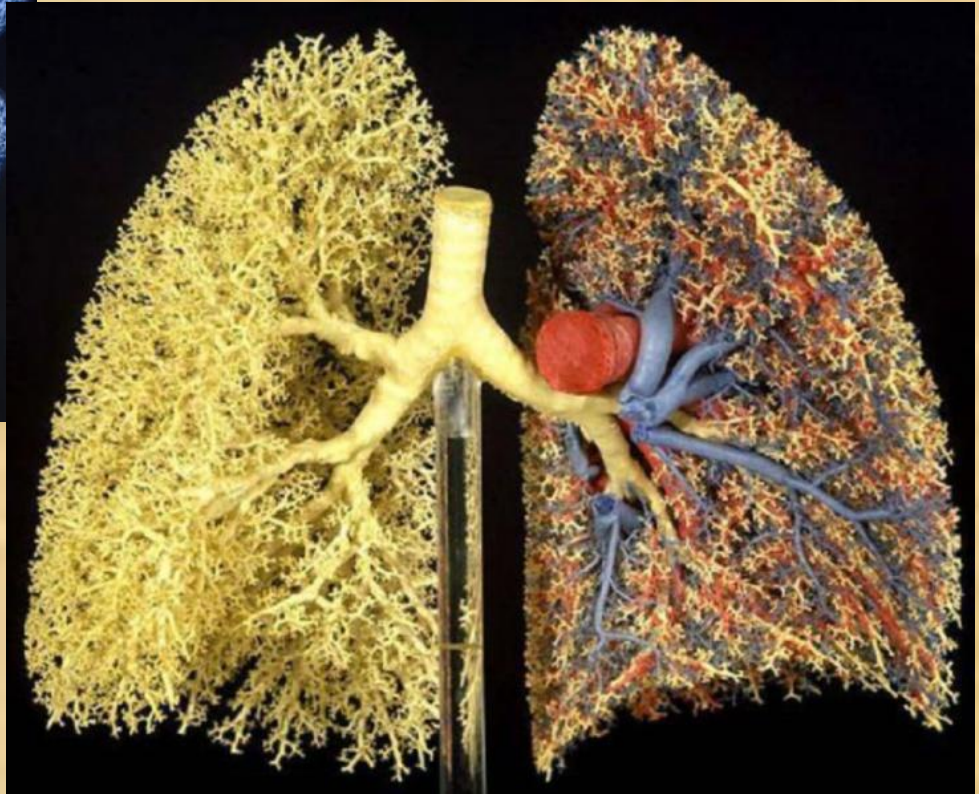
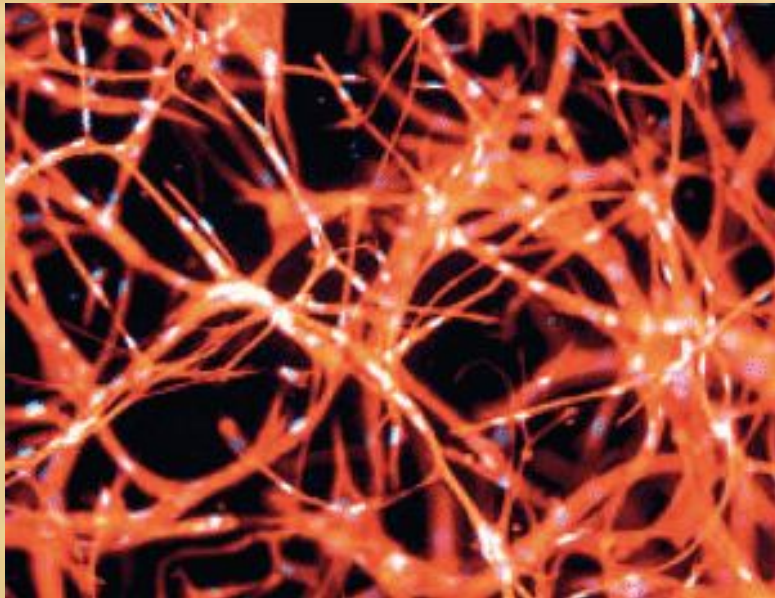
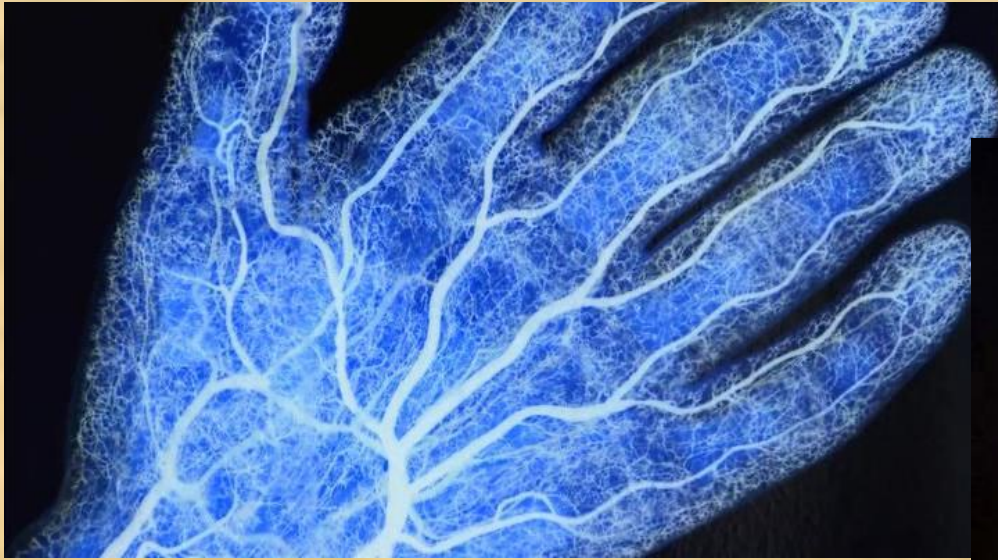




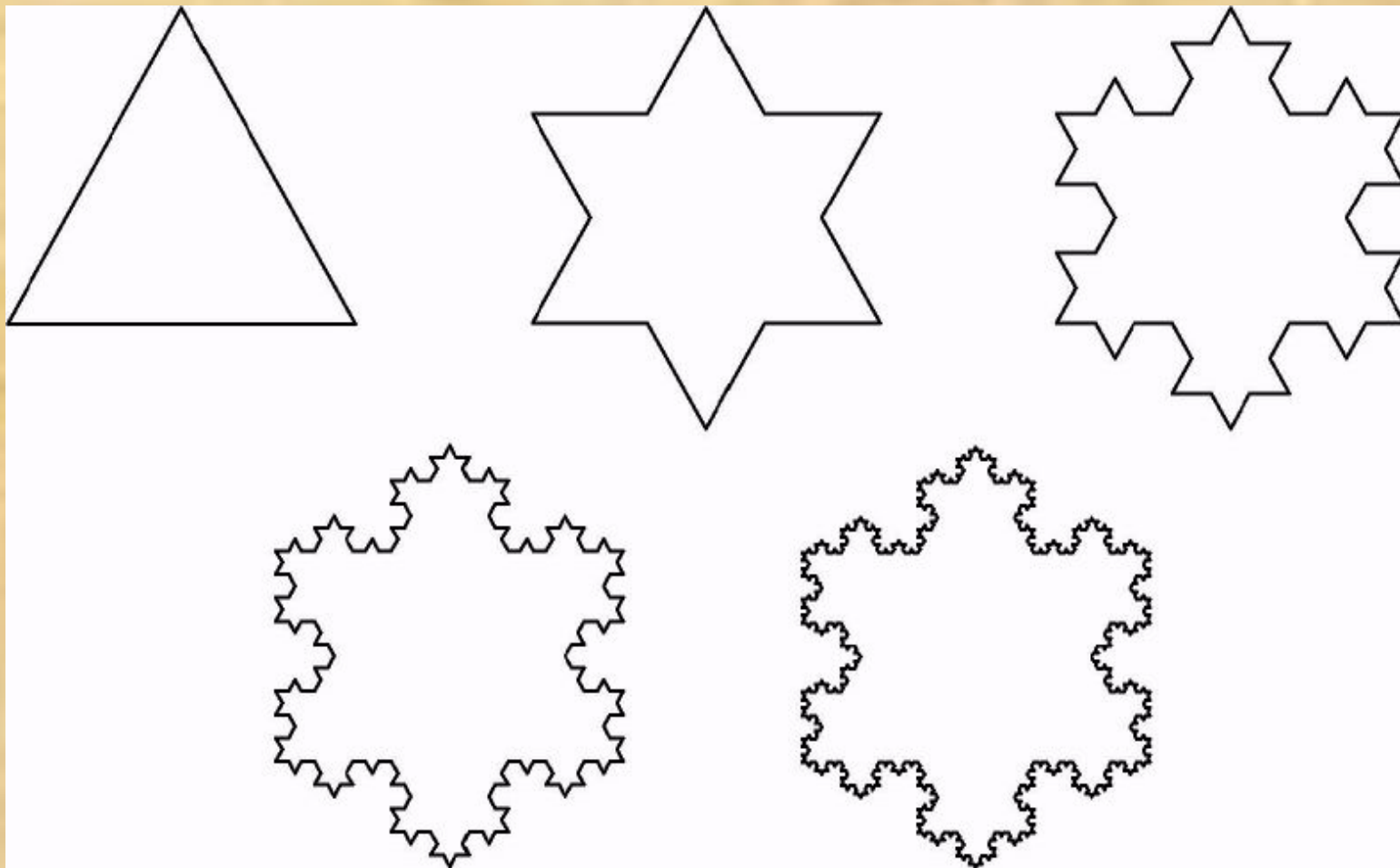
Кацусика Хokusай. Большая волна в Канагава



**Винсент Ван Гог, «Звездная
ночь»**



Снежинка Коха



Алгебраические фракталы

$$X' = A * X + B * Y + E$$

$$Y' = C * X + D * Y + F$$

$$X' = (A1 * X + B1 * Y + C1) / (D1 * X + E1 * Y + F1)$$

$$Y' = (A2 * X + B2 * Y + C2) / (D2 * X + E2 * Y + F2)$$

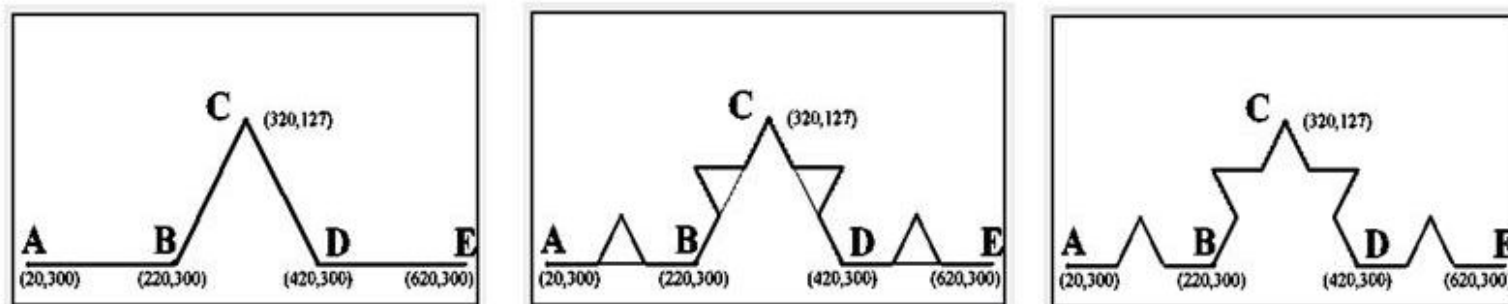
$$X' = A1 * X * X + B1 * X * Y + C1 * Y * Y + D1 * X + E1 * Y + F1$$

$$Y' = A2 * X * X + B2 * X * Y + C2 * Y * Y + D2 * X + E2 * Y + F2$$

Алгоритм построения IFS -фрактала:

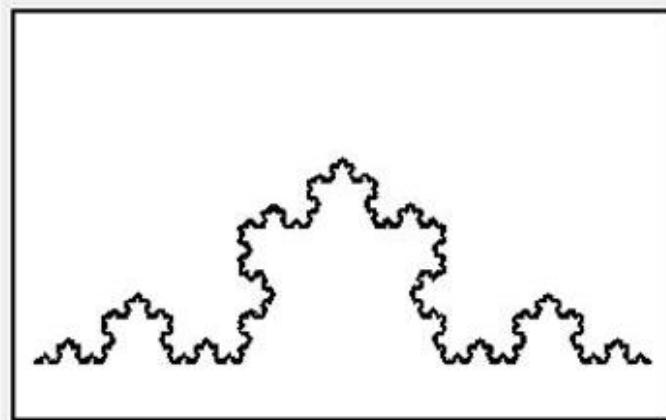
- Найти и закрасить начальную точку (X, Y) изображения.
- Выбрать одно из IFS-преобразований, найти координаты (X', Y') новой точки изображения и закрасить найденную точку.
- Принять $X = X'$ и $Y = Y'$.
- Повторить п.п. 2 и 3 алгоритма заданное число раз.

Построение IFS "снежинки" Коха.



Исходная заготовка на сетке координат 640 x 350.

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



$$\begin{aligned} X' &= 0.333 \cdot X + 13.333 \\ Y' &= 0.333 \cdot Y + 200 \end{aligned}$$

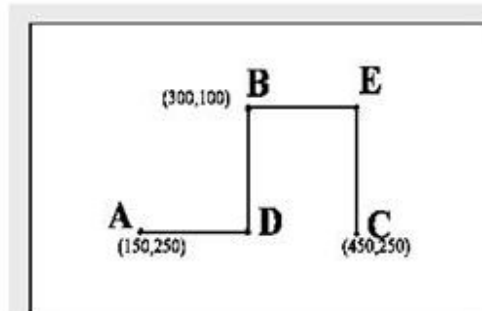
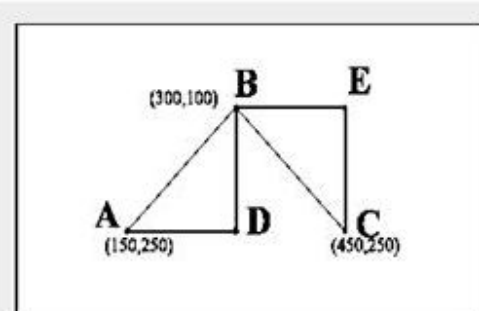
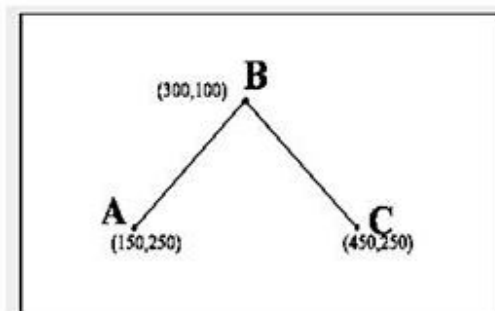
$$\begin{aligned} X' &= 0.333 \cdot X + 413.333 \\ Y' &= 0.333 \cdot Y + 200 \end{aligned}$$

$$\begin{aligned} X' &= 0.167 \cdot X + 0.289 \cdot Y + 130 \\ Y' &= -0.289 \cdot X + 0.167 \cdot Y + 256 \end{aligned}$$

$$\begin{aligned} X' &= 0.167 \cdot X - 0.289 \cdot Y + 403 \\ Y' &= 0.289 \cdot X + 0.167 \cdot Y + 71 \end{aligned}$$

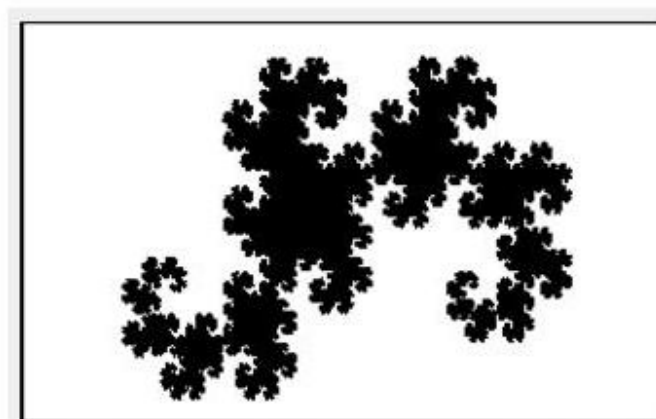
Итоговая "снежинка" Коха и IFS (состоящее из 4-х преобразований), с помощью которых она была построена в том же прямоугольнике 640x350 за 10 итераций.

Построение IFS "дракона" Хартера-Хейтуэя.



Исходная заготовка на сетке координат 640 x 350.

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



$$\begin{aligned} X' &= -0.5 * X - 0.5 * Y + 490 \\ Y' &= 0.5 * X - 0.5 * Y + 120 \end{aligned}$$

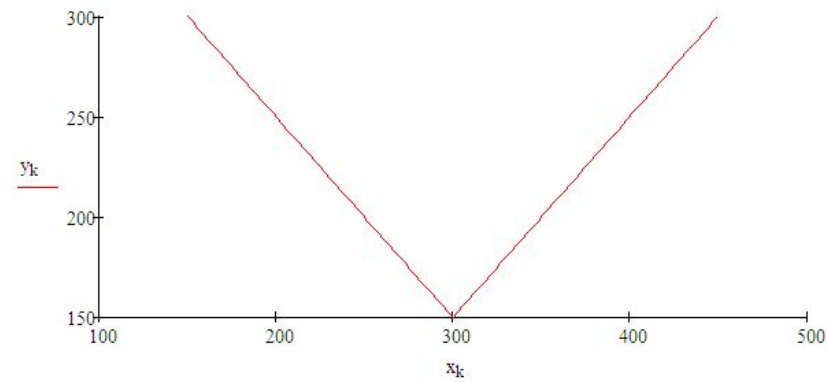
$$\begin{aligned} X' &= 0.5 * X - 0.5 * Y + 340 \\ Y' &= 0.5 * X + 0.5 * Y - 110 \end{aligned}$$

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 b := 450 n := 100 k := 0..n

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

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



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

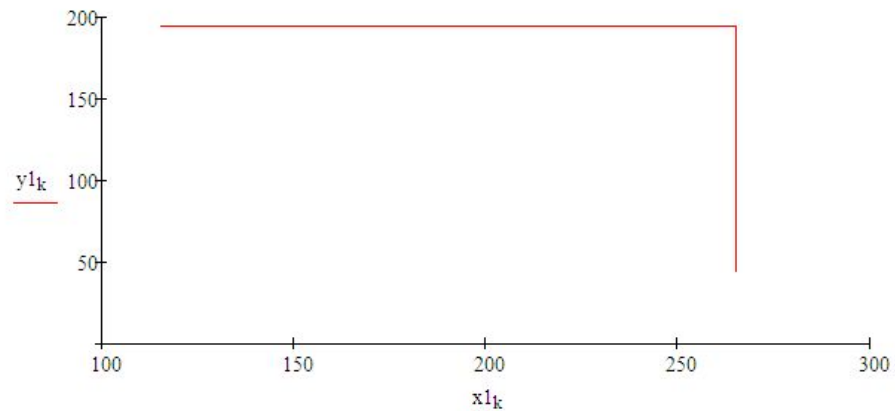
$$y1_k := 0.5x_k - 0.5y_k + 120$$

$$x1_0 = 265$$

$$x1_n = 115$$

$$y1_0 = 45$$

$$y1_n = 195$$



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

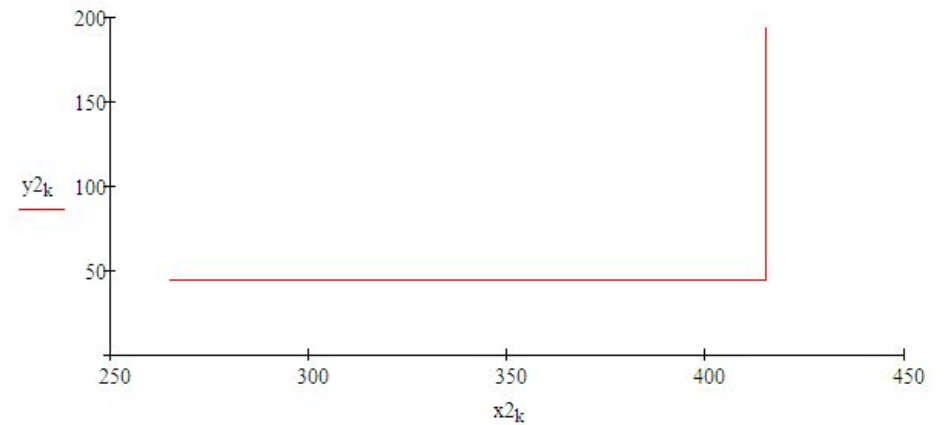
$$y2_k := 0.5x_k + 0.5y_k - 180$$

$$x2_0 = 265$$

$$x2_n = 415$$

$$y2_0 = 45$$

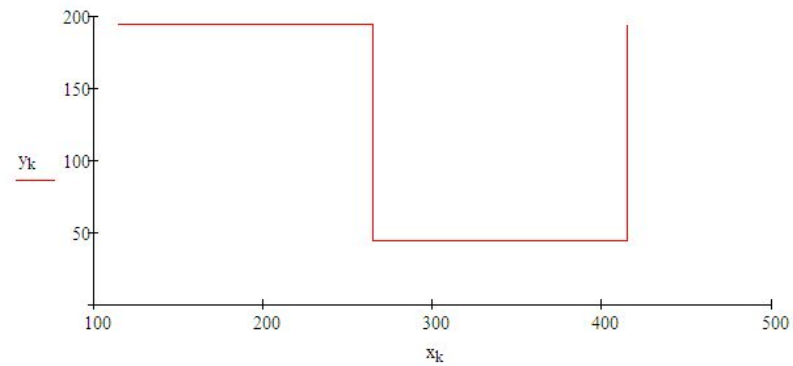
$$y2_n = 195$$



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

$$x_k := \text{if}(k < n, x_{1n-k}, x_{2k-n})$$

$$y_k := \text{if}(k < n, y_{1n-k}, y_{2k-n})$$



$$x_{1k} := -0.5x_k - 0.5y_k + 490$$

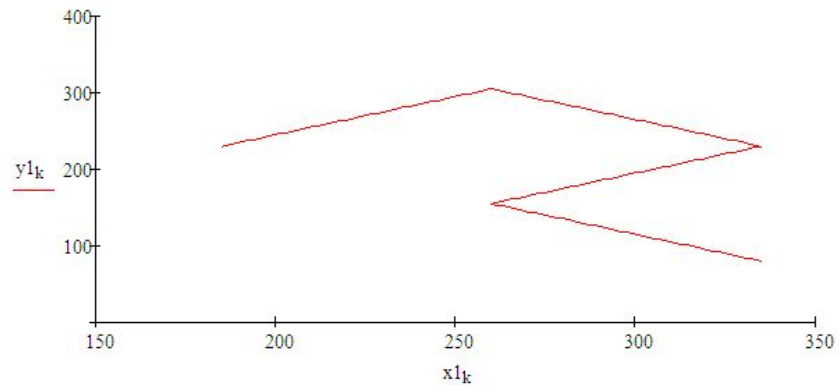
$$y_{1k} := 0.5x_k - 0.5y_k + 120$$

$$x_{10} = 335$$

$$y_{10} = 80$$

$$x_{1n} = 335$$

$$y_{1n} = 230$$



$$x_{2k} := 0.5x_k - 0.5y_k + 375$$

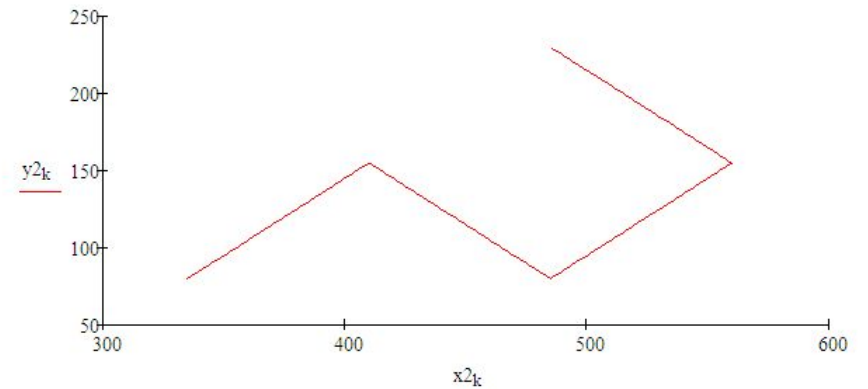
$$y_{2k} := 0.5x_k + 0.5y_k - 75$$

$$x_{20} = 335$$

$$y_{20} = 80$$

$$x_{2n} = 485$$

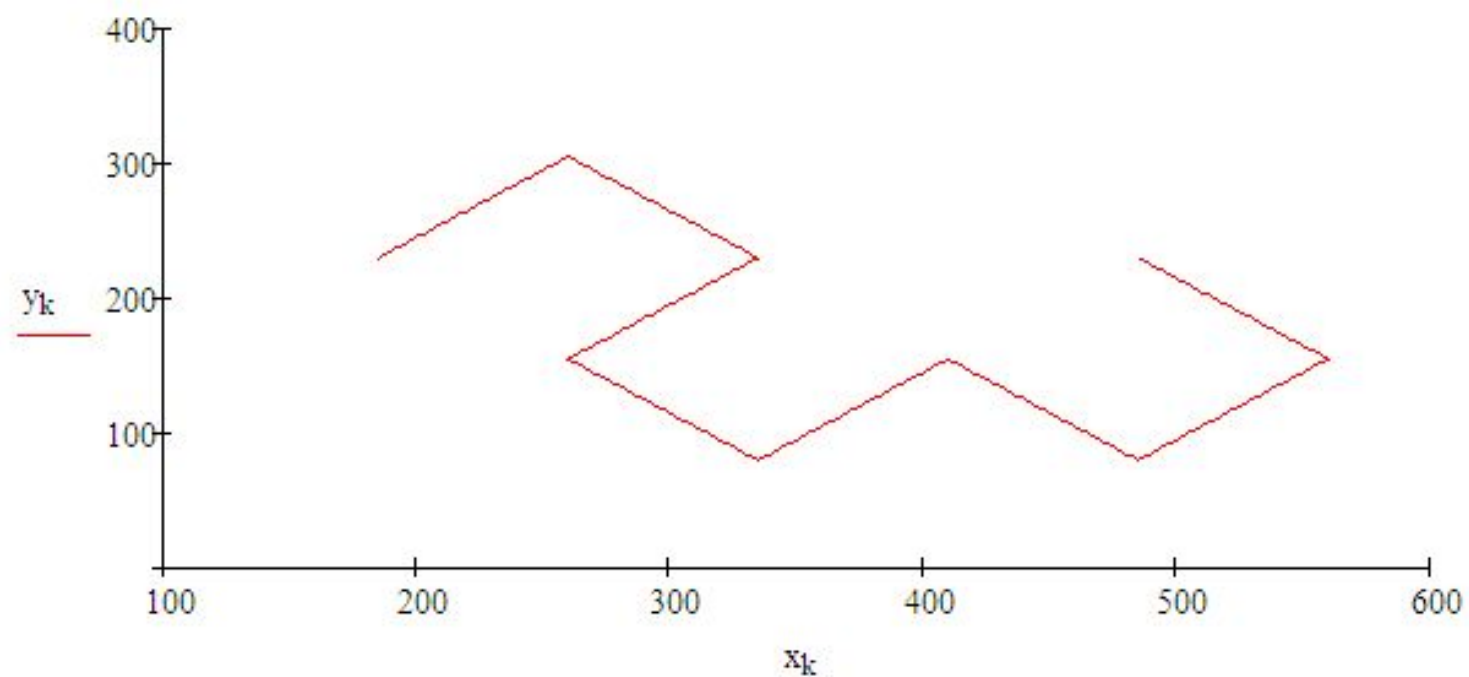
$$y_{2n} = 80$$



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

$x_k := \text{if}(k < 2n, x_{12n-k}, x_{2k-2n})$

$y_k := \text{if}(k < 2n, y_{12n-k}, y_{2k-2n})$



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

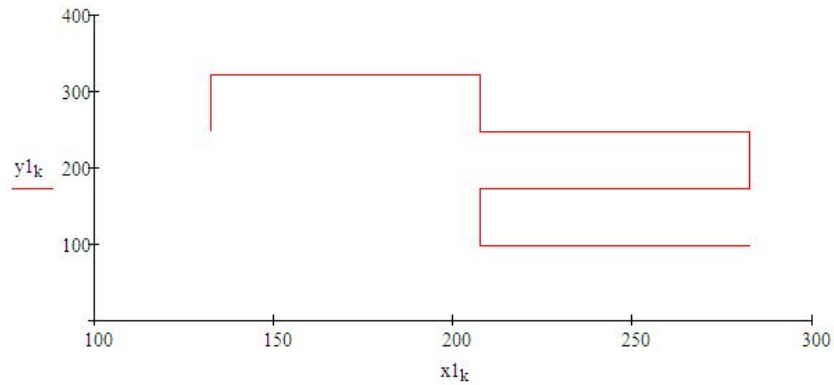
$$y1_k := 0.5x_k - 0.5y_k + 120$$

$$x1_0 = 282.5$$

$$x1_n = 207.5$$

$$y1_0 = 97.5$$

$$y1_n = 172.5$$



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

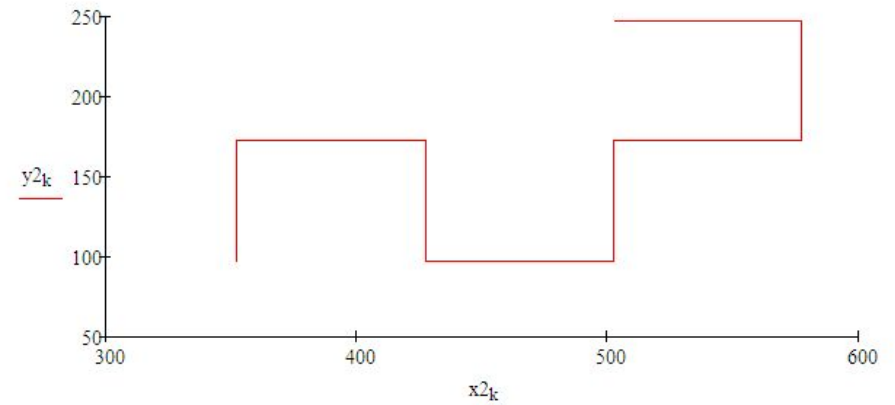
$$y2_k := 0.5x_k + 0.5y_k - 110$$

$$x2_0 = 352.5$$

$$x2_n = 427.5$$

$$y2_0 = 97.5$$

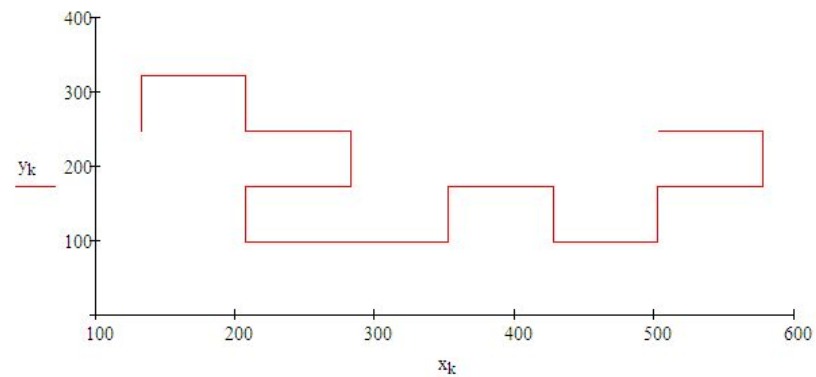
$$y2_n = 172.5$$



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

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

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



$$x1_k := -0.52x_k - 0.48y_k + 490$$

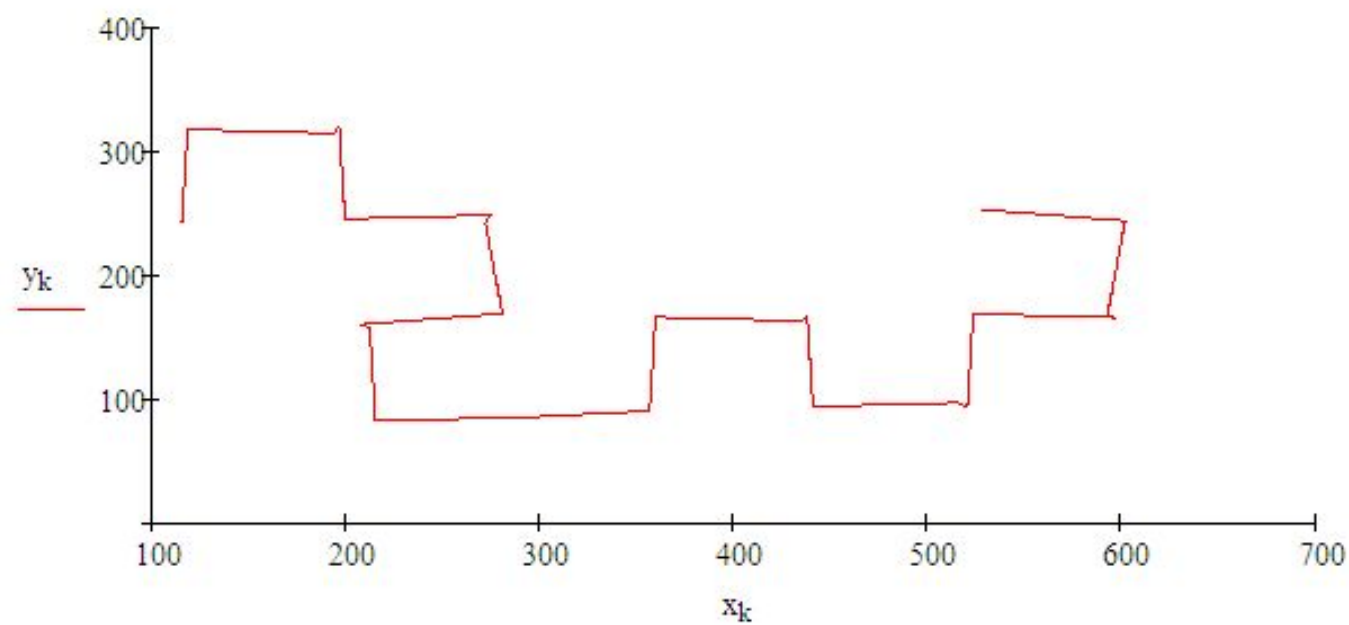
$$x2_k := 0.52x_k - 0.48y_k + 375$$

$$y1_k := 0.48x_k - 0.52y_k + 120$$

$$y2_k := 0.48x_k + 0.52y_k - 110$$

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

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



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

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

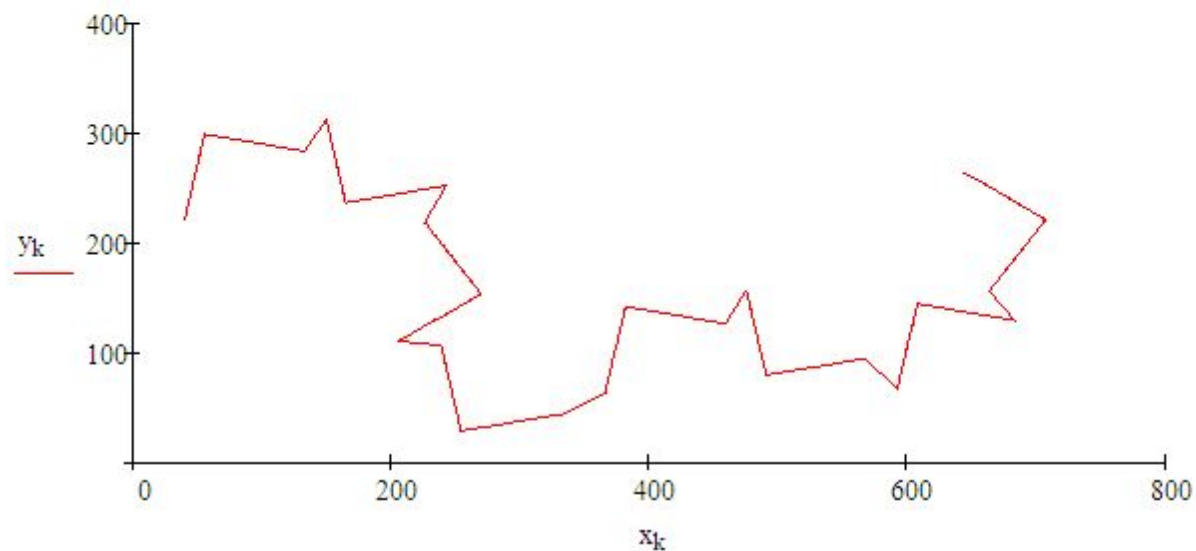
$$y1_k := 0.4x_k - 0.6y_k + 120$$

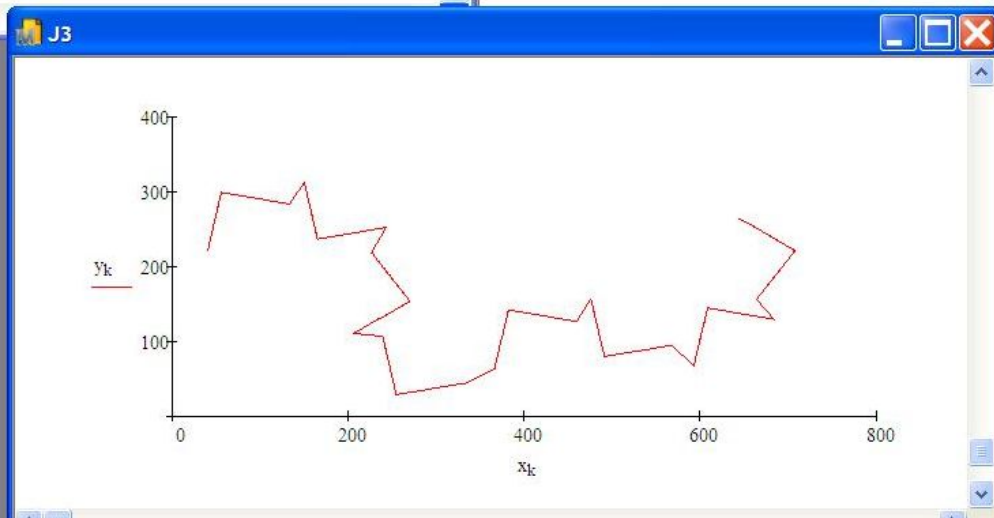
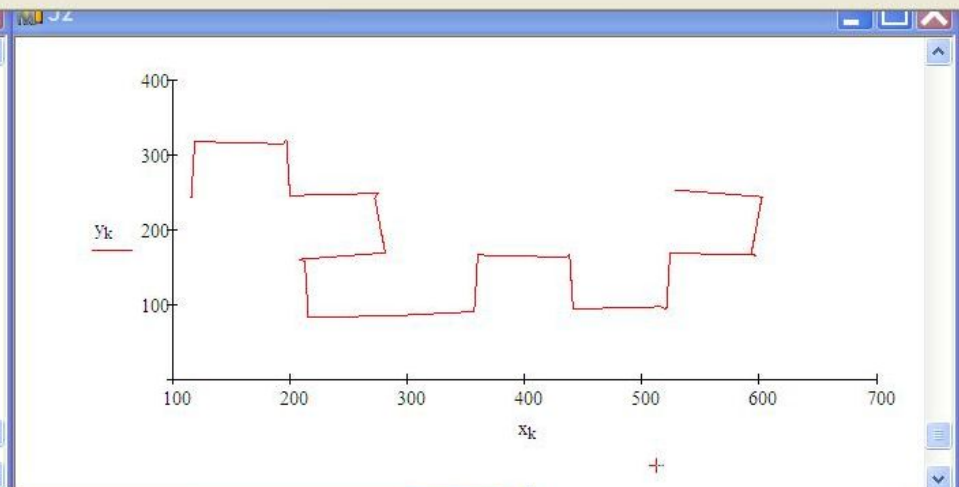
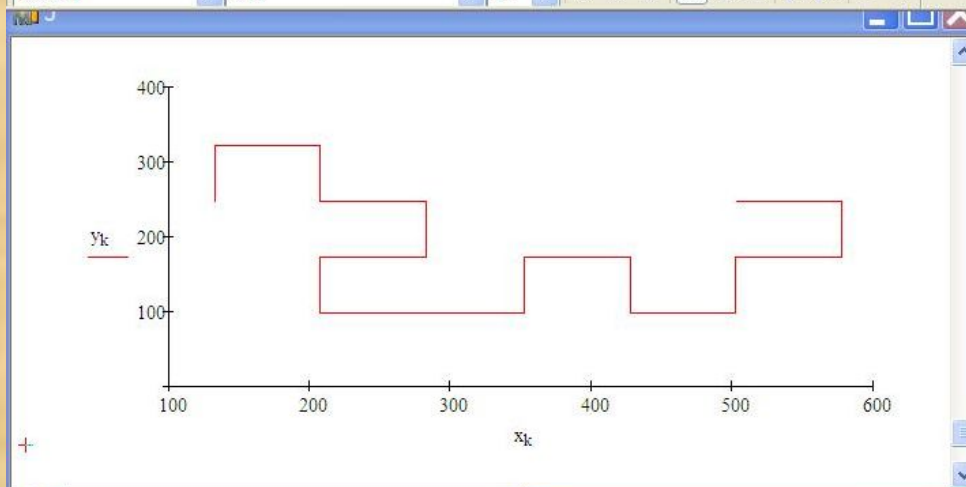
$$y2_k := 0.4x_k + 0.6y_k - 110$$

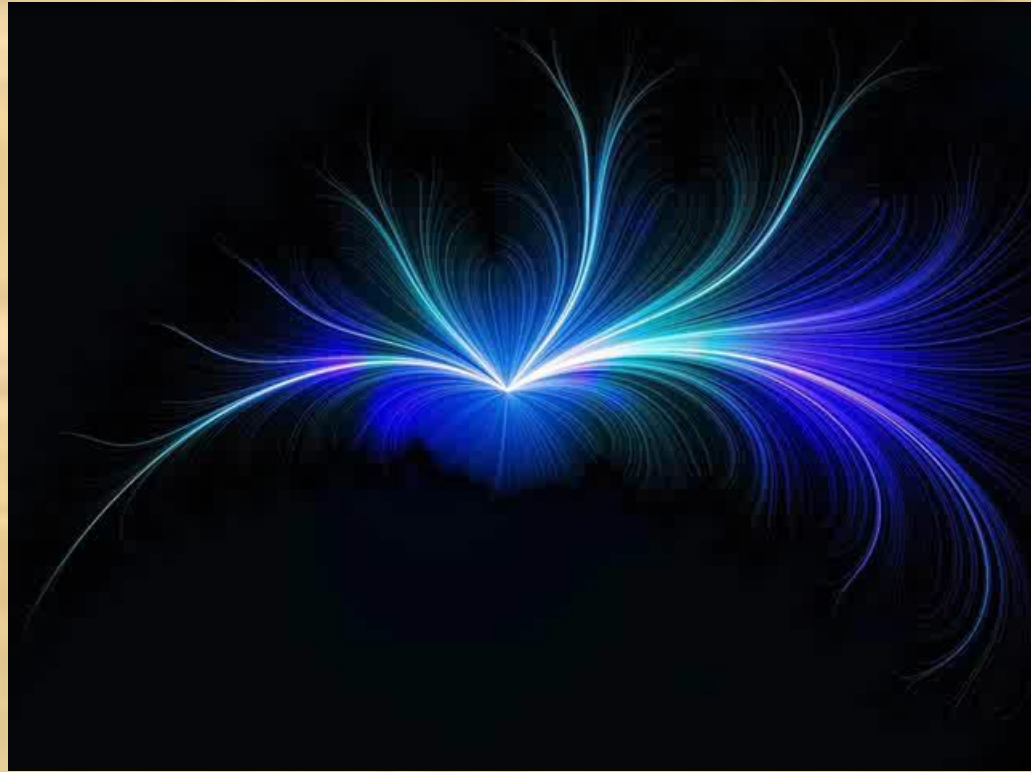
+

$$k := 0..8-n$$

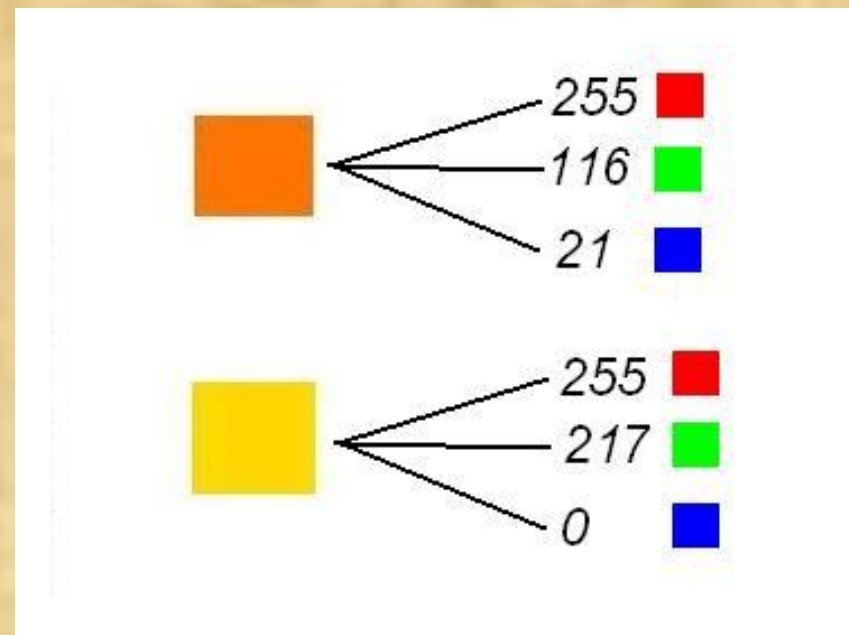
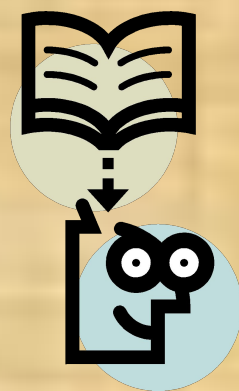
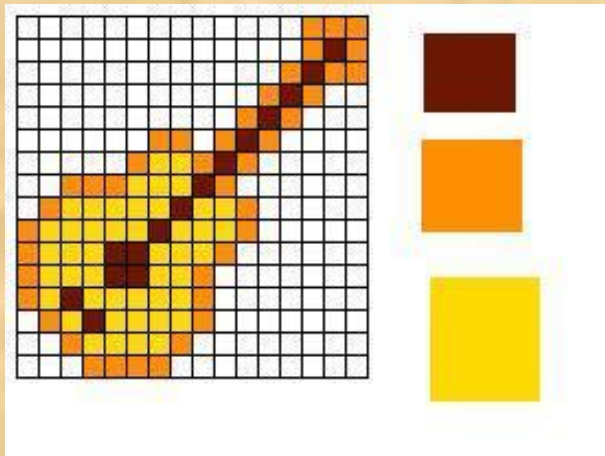
$$x_k := \text{if}(k < 4n, x1_{4n-k}, x2_{k-4n}) \quad y_k := \text{if}(k < 4n, y1_{4n-k}, y2_{k-4n})$$





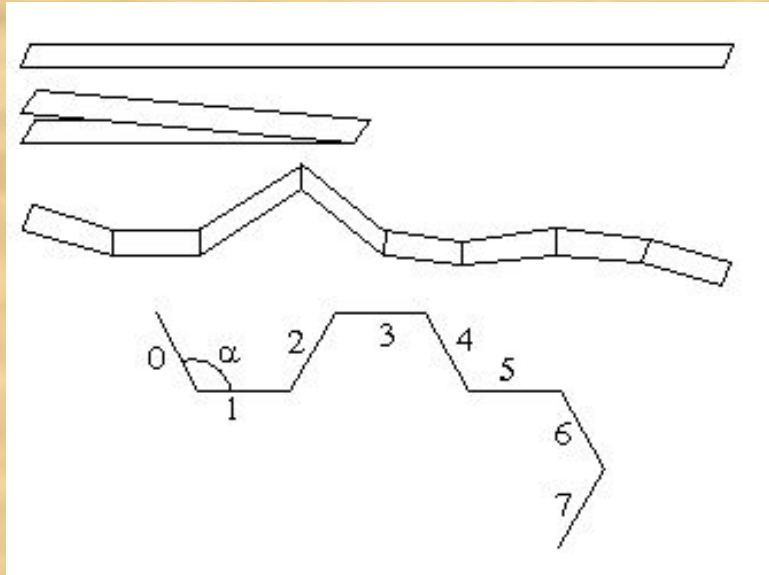


Шаг 0: RGB-формат



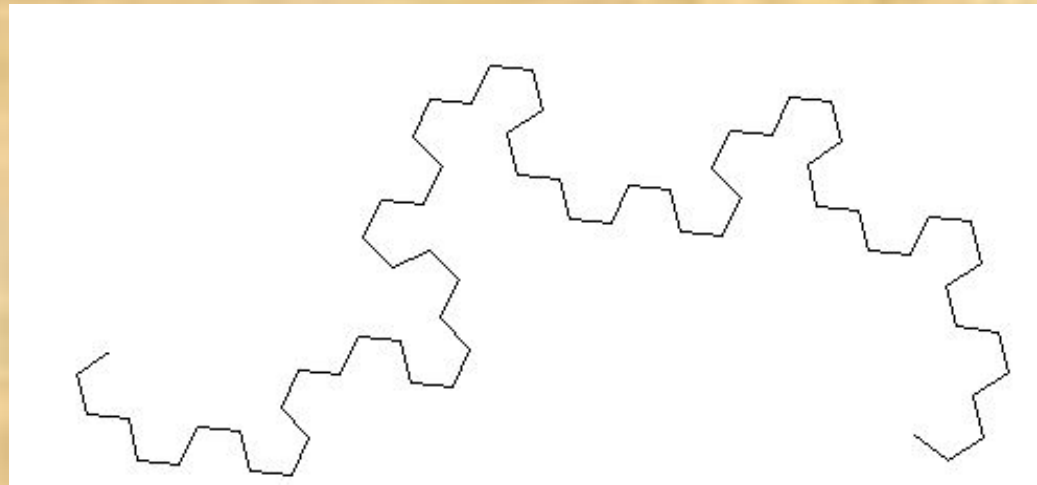
94.28.13 01 Dark Skin	241.148.108 02 Light Skin	97.119.171 03 Blue Sky	90.103.39 04 Foliage	164.131.196 05 Blue Flower	140.253.153 06 Bluish Green
255.116.21 07 Orange	7.47.122 08 Purplish Blue	222.29.42 09 Moderate Red	69.0.68 10 Purple	187.255.19 11 Yellow Green	255.142.0 12 Orange Yellow
0.0.142 13 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

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

$$\begin{aligned}d(16) &= d(8) = d(4) = d(2) = d(1) = 1, \\d(12) &= d(6) = d(3) = -1, \\d(10) &= d(5) = 1.\end{aligned}$$



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

..... 11110000110010**10000110000**001010.....

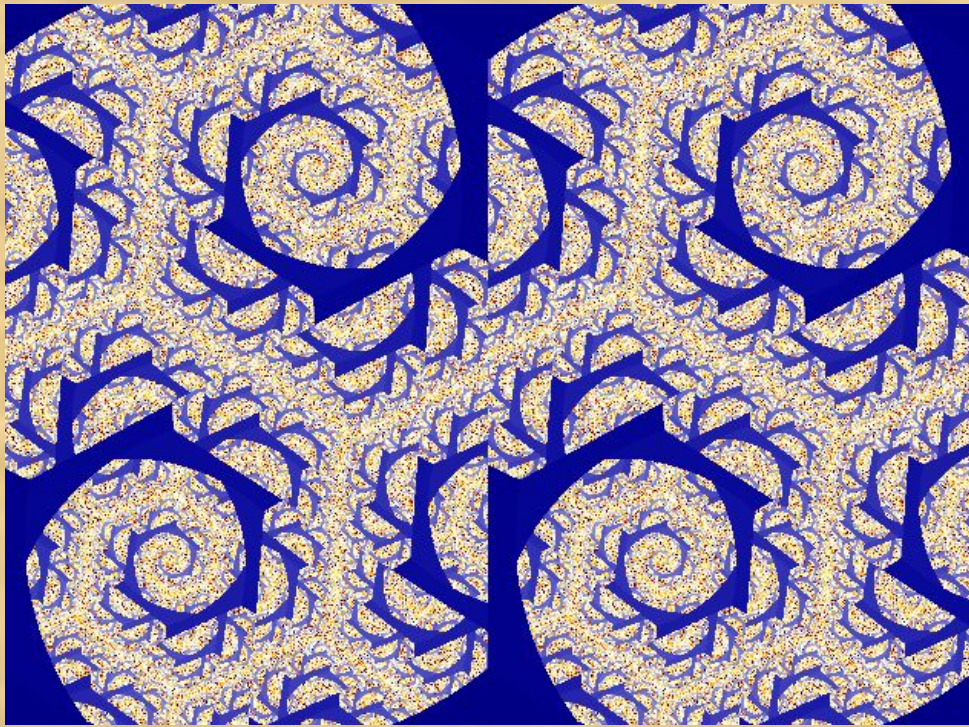
Текст 2.

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

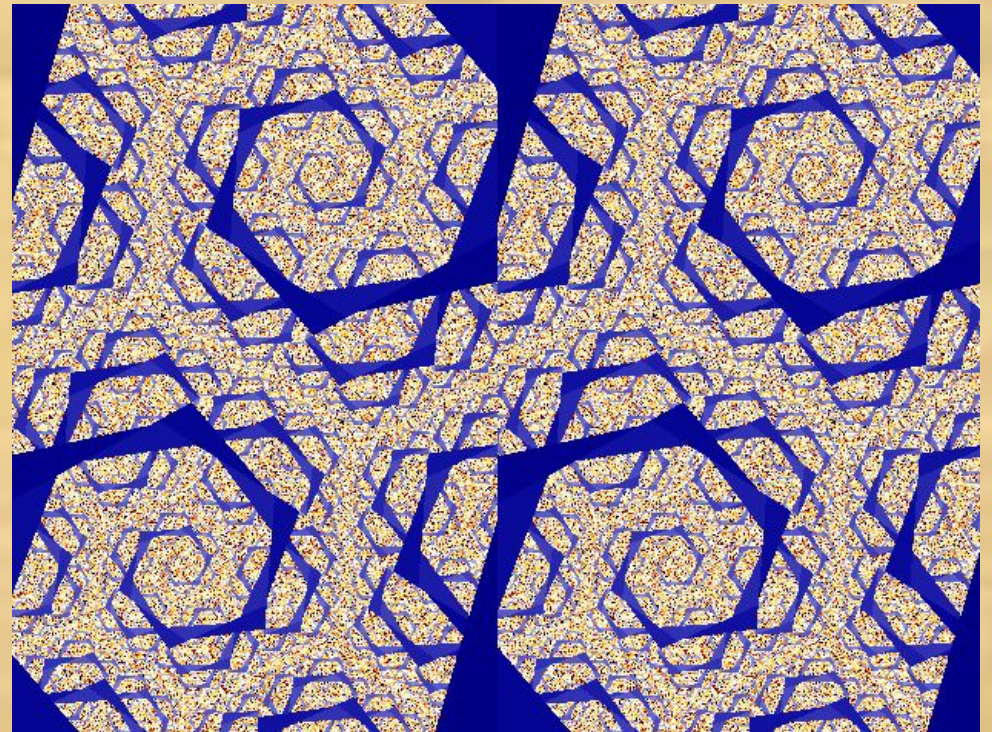
в двоичной кодировке

.....11110000110010**10000110010**001010.....

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



Фрактал, соответствующий
Тексту 1.



Фрактал, соответствующий
Тексту 2.

***Спасибо
за
внимание!***