Криптографическая защита информации

Основные исторические периоды криптографии

I период (с 3-го тысячелетия до н.э.) – характеризуется господством моноалфавитных шифров.

II период (с IX века на Ближнем Востоке и с XV века в Европе до начала XX века) – ознаменовался введением в обиход полиалфавитных шифров.

III период (с начала до середины XX века) – характеризуется внедрением электромеханических устройств в работу шифровальщиков.

Основные исторические периоды криптографии

IV период (с середины до 70-х годов XX века) – период перехода к математической криптографии. В работе К. Шеннона появляются строгие математические определения количества информации, передачи данных, энтропии, функций шифрования. Обязательным этапом создания шифра считается изучение его уязвимости к различным известным атакам.

Современный период (с конца 1970-х годов до настоящего времени) – отличается зарождением и развитием нового направления – криптография с открытым ключом. Появление такого направления расширило рамки использования криптографии не только государством, но и частными лицами.

Основные определения

1. Шифр – совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, заданных алгоритмом криптографического преобразования.

2. Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного варианта из совокупности всевозможных для данного алгоритма.

3. Зашифрование – процесс преобразования открытых данных в зашифрованные с помощью шифра.

Расшифрование – процесс преобразования закрытых данных в открытые с помощью шифра.

4. Шифрование – процесс зашифрования или расшифрованая данных.

Основные определения

5. Дешифрование – процесс преобразования закрытых данных в открытые при неизвестном ключе и, возможно, неизвестном алгоритме.

6. Криптостойкость – характеристика шифра, определяющая его стойкость к дешифрованию (*определяется периодом времени необходимым для дешифрования*).

Требования к современным методам шифрования

1. Стойкость шифра противостоять криптоанализу должна быть такой, чтобы вскрытие его могло быть осуществлено только путем решения задачи полного перебора ключей.

2. Криптостойкость обеспечивается не секретностью алгоритма, а секретностью ключа.

3. Шифртекст не должен существенно превосходить по объему исходную информацию.

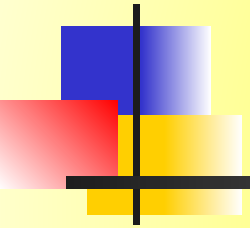
Требования к современным методам шифрования

4. Ошибки, возникающие при шифровании не должны приводить к искажениям и потерям информации.

5. Время шифрования не должно быть большим.

6. Стоимость шифрования должна быть согласована со стоимостью закрываемой информации.

Общая схема передачи шифрованных сообщений



Методы криптографии

Классификация криптоалгоритмов

по типу ключей:

- **Симметричные** – для шифрования и расшифровывания требуется один и тот же ключ
- **Асимметричные** – для шифрования требуется один ключ (открытый), а для расшифровывания другой (закрытый) ключ

по характеру воздействия над данными:

- **Перестановочные** – блоки информации (биты, байты, ...) не меняются сами по себе, а изменяется порядок их следования
- **Подстановочные** – изменяются сами блоки информации

в зависимости от размера блока информации:

- **Потоковые** – шифруются побитно. Результат шифрования не зависит от зашифрованного ранее входного потока
- **Блочные** – блок состоит из нескольких байт (обычно от 4 до 32). Результат шифрования зависит от данных всего блока

Классификация криптоалгоритмов

1. Шифрование
2. Кодирование
3. Другие методы

1. Шифрование - преобразование элементов открытого сообщения (символов, битов, байтов, …) на основе алгоритма и ключа.

2. Кодирование – преобразование информационного (смыслового) сообщения в комбинацию символов (чисел) в соответствии с некоторой таблицей.

Например: символы -> числа, (ASCII-код, азбука Морзе)
последовательность слов -> кодовое слово

1. Шифрование

1.1 Замена (подстановка)
- 1.1.1 Простая (одноалфавитная)
- 1.1.2 Многоалфавитная обыкновенная
- 1.1.3 Многоалфавитная гомофоническая
- 1.1.4. Полиграммная

1.2 Перестановка
- 1.2.1 Простая
- 1.2.2 По таблице
- 1.2.3 По маршрутам

1.3 Аналитические преобразования
- 1.3.1 Алгебра матрицы
- 1.3.2 По особым зависимостям

1.4 Гаммирование
- 1.4.1 С конечной гаммой
- 1.4.2 С бесконечной гаммой

1.5 Комбинированные методы

2. Кодирование

2.1 Смысловое

2.2 Символьное

2.3 Комбинированное

3. Другие методы

3.1 Рассечение – разнесение

3.2 Сжатие – расширение

3.3 Стеганография

1.1 Шифрование заменой

1.1.1 ***Простая замена*** задается *таблицей замен*

Алфавит исходного текста	А	Е	З	М	Н	. . .
	↓	↓	↓	↓	↓	↓
Алфавит шифротекста	Г	Ж	Р	И	Ф	. . .

Пример. Текст: **З А М Е Н А**

Шифр: **Р Г И Ж Ф Г**

1.1 Шифрование заменой

1.1.1 *Простая замена*

Шифр Атбаш: алфавит шифротекста получается путем **обратного порядка** исходного алфавита

Алфавит исходного текста	А Б В . . . Ю Я _
Алфавит шифротекста	_ Я Ю . . . В Б А

Шифр с кодовым словом: алфавит шифротекста начинается с символов кодового слова

Алфавит исходного текста	А Б В **Г** Д Е . . .
Алфавит шифротекста	**К О Д** Л В С . . .

1.1 Шифрование заменой

1.1.1 *Простая замена*

Шифр Цезаря: алфавит шифротекста получается путем **сдвига** исходного алфавита на 3 позиции

Алфавит исходного текста	**А** Б В **Г** **Д** . . . Ю Я _
Алфавит шифротекста	Ю Я _ **А** Б . . . Ы Ь Э

или

шифрование: $y_i = (x_i + k) \bmod N$

расшифровывание: $x_i = (y_i + N - k) \bmod N$

где x_i – i-й символ исходного текста

y_i - i-й символ шифротекста

k - константа (= 3)

N - количество символов алфавита

1.1 Шифрование заменой

1.1.1 *Простая замена*

Недостатки:

1. Сохранение статистических частот встречаемости символов в шифртексте как в открытом тексте.

2. Малое число возможных ключей шифрования.

Данные методы применяются редко, и только для шифрования коротких сообщений

1.1 Шифрование заменой

1.1.2 *Многоалфавитная обыкновенная*

Для замены символов исходного текста используют символы нескольких алфавитов

Алфавит открытого текста		А	Б.. Е	Ж	З.. М	Н ..
Алфавиты шифротекста	первый	17	23..97	47	76..32	55..
	второй	31	44..51	67	19..28	84..
	третий	48	63..15	33	59..61	34..

Пример. Текст: З А М Е Н А

Номер алфавита для шифрования: 1 2 3 1 2 3

Шифр: 76 31 34 97 84 48

При шифровании следующей буквы используют следующий алфавит

1.1 Шифрование заменой

1.1.2 *Многоалфавитная обыкновенная*

Шифра Вижинера:

Шифрование производится по формуле:

$$y_i = (x_i + k_i) \bmod N$$

где y_i - i-й символ шифртекста; k_i - i-символ ключа; x_i - i-й символ открытого текста (номер буквы в алфавите); N - длина используемого алфавита.

Расшифрование производится по формуле:

$$x_i = (y_i - k_i) \bmod N$$

1.1 Шифрование заменой

1.1.2 *Многоалфавитная обыкновенная*

Пример использования шифра Вижинера:

Открытый текст	Ключ	Преобразование	Текст
З	К	$y_1 = 8 + 11 \pmod{33} = 19$	П
А	Л	$y_2 = 1 + 12 \pmod{33} = 13$	М
М	Ю	$y_3 = 13 + 31 \pmod{33} = 11$	К
Е	Ч	$y_4 = 6 + 24 \pmod{33} = 30$	Э
Н	К	$y_5 = 14 + 11 \pmod{33} = 25$	Ш
А	Л	$y_6 = 1 + 12 \pmod{33} = 13$	М

1.1 Шифрование заменой

1.1.2 *Многоалфавитная обыкновенная*

Вариации шифра Вижинера:

- если ключ неограничен по длине и неповторяемый – ***шифр Вернама*** (одноразовые шифровальные блокноты)
- ***шифр Бофора*** – шифрование:

$$y_i = (x_i - k_i) \bmod N \quad \text{или} \quad y_i = (k_i - x_i) \bmod N$$

- **шифрование с автоключом** – в качестве ключа используются символы открытого текста или символы шифротекста

1.1 Шифрование заменой

1.1.2 *Многоалфавитная обыкновенная*

Шифрование с автоключом из открытого текста:

Пример шифрования

Открытый текст	Я	В	К	А	_	П	Р	О	В	А	Л	Е	Н	А
Код	31	2	10	0	32	15	16	14	2	0	11	5	13	0
Ключ	К	Л	Ю	Ч	Я	В	К	А	_	П	Р	О	В	А
Код	10	11	30	23	31	2	10	0	32	15	16	14	2	0
Строка 2 + строка 4	41	13	40	23	63	17	26	1434		15	27	19	15	0
Код шифра	8	13	7	23	30	17	26	14	1	15	27	19	15	0
Шифр	И	Н	З	Ч	Ю	С	Ъ	О	Б	П	Б	У	П	А

1.1 Шифрование заменой

1.1.2 *Многоалфавитная обыкновенная*

Шифрование с автоключом из шифротекста:

Пример шифрования

Шифр	И	Н	З	Ч	З	Ь	Ч	Д	Й	Ь	Б	Й	Ц	Ь
Код шифра	8	13	7	23	7	28	23	4	9	28	1	9	22	28
Ключ	К	Л	Ю	Ч	И	Н	З	Ч	З	Ь	Ч	Д	Й	Ь
Код	10	11	30	23	8	13	7	23	7	28	23	4	9	28
Строка 2 + 33 – строка 4	31	2	10	0	32	15	16	14	2	0	11	5	13	0
Код	31	2	10	0	32	15	16	14	2	0	11	5	13	0
Открытый текст	Я	В	К	А	_	П	Р	О	В	А	Л	Е	Н	А

Шифр И Н З Ч З Ь Ч Д И Ь Б И Ц Ь

1.1 Шифрование заменой

1.1.3 *Многоалфавитная гомофоническая*

Алфавиты шифротекста составлены так, чтобы символы зашифрованного сообщения имели статистически равную частоту встреч

Алфавит открытого текста		A	B	C	D	E	..	R	..	Y	Z
Алфавиты шифротекста	первый	f	N	Q	b	G	..	Z	..	K	t
	второй	*	N	Q	.	+	..	=	..	K	t
	третий	k	N	Q	b	]	..	a	..	K	t

Пример. Текст: R E A D E R

Номер алфавита для шифрования: 1 1 1 1 2 2

Шифр: Z G f b + =

При шифровании каждый символ заменяется по очереди символами соответствующего столбца

1.1 Шифрование заменой

Достоинство методов многоалфавитной замены

Маскирование в шифротексте частот появления символов открытого текста.

1.1 Шифрование заменой

1.1.4 *Полиграммная*

Шифр Плейфера

Относится к шифрам *полиграммной замены*, когда замене подвергается не отдельный символ, а группа символов.

Используется матрица замен (выступает в качестве ключа метода).

А	Х	Б	М	Ц	В
Ч	Г	Н	Ш	Д	О
Е	Щ	,	Х	У	П
.	З	Ъ	Р	И	Й
С	Ь	К	Э	Т	Л
Ю	Я	_	Ы	Ф	-

1.2 Шифрование перестановкой

1.2.1 *Простая перестановка*

Символы открытого текста переставляются в соответствии с задаваемым ключом шифра правилом

Пример. Ключ: 1-3-2

Текст: ПРО СТА Я_П ЕРЕ СТА НОВ КА

Шифр: ПОР САТ ЯП_ ЕЕР САТ НВО КА

В качестве ключа перестановки можно использовать последовательность символов. Для этого:

1) отсортировать символы ключа (в алфавитном порядке)
2) каждый символ ключа заменяется на номер позиции в отсортированном ключе

Ключевое слово: П Р О М Е Т Е Й

Отсортированный ключ: Е Е Й М О П Р Т

1 2 3 4 5 6 7 8

Числовой ключ: 6-7-5-4-1-8-2-3

1.2 Шифрование перестановкой

1.2.2 *Перестановка по таблице*

Символы открытого текста записываются построчно в матрицу перестановки согласно ключу1, а считываются из матрицы по столбцам согласно ключу2

Пример. Матрица перестановки 5x6
Ключ1: 5-1-3-2-4, ключ2: 2-1-6-5-3-4
Текст: СВЯЗНОЙ_ПРИЛЕТАЕТ_В_ПЯТНИЦУ

Шифротекст:
_ _ТЦВЙВЕИСЛН_ _ОИТТ_НППАУЯРЯЕ_З

Ключ2: 2-1-6-5-3-4

Ключ1: 5-1-3-2-4

	1	2	3	4	5	6
1	Й	_	П	Р	И	Л
2	В	_	П	Я	Т	Н
3	Е	Т	А	Е	Т	_
4	И	Ц	У	_	_	_
5	С	В	Я	З	Н	О

1.2 Шифрование перестановкой

1.2.2 *Перестановка по таблице*

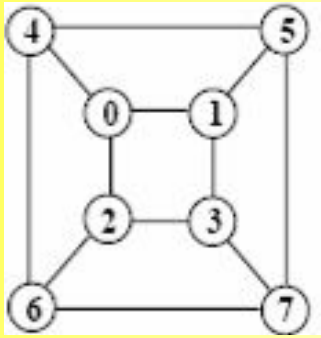
Модификации метода:

- направление записи исходного текста в матрицу (построчно, по столбцам, по спирали, по диагонали);
- направление чтения шифротекста из матрицы (построчно, по столбцам, по спирали, по диагонали);
- предварительное добавление дополнительных символов (пробелов) в исходный текст в соответствии с ключом перестановки;
- вместо двумерной использовать трехмерную таблицу (перестановка на кубике Рубика, объемная перестановка);

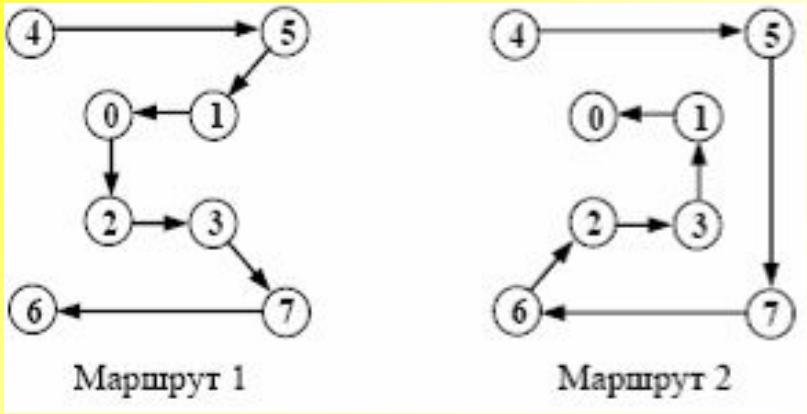
1.2 Шифрование перестановкой

1.2.3 *Перестановка по маршрутам*

Например, перестановка по гамильтоновым путям на графе *(гамильтонов путь – замкнутый путь, проходящий через все вершины графа строго по одному разу).*



1) Вершины графа нумеруют.
2) В вершины графа последовательно записывают символы открытого текста.
3) Получают шифр, путем считывания символов, согласно выбранному гамильтоновому пути.



1.2 Шифрование перестановкой

Недостатки:

1. Сохранение статистических частот встречаемости символов в шифротексте как в открытом тексте.
2. Малое число возможных ключей шифрования.

Достоинства:

Высокая скорость шифрования.

1.3 Аналитические преобразования

Основаны на понятии односторонней функции.

Функция ***Y = F(X)*** является односторонней, если она за сравнительно небольшое число операций преобразует элемент открытого текста **X** в элемент шифротекста **Y**, а обратная операция (вычисление $X = F_{обр}(Y)$ при известном шифротексте) является вычислительно трудоемкой.

В качестве односторонней функции можно использовать следующие преобразования:

- умножение матриц;
- решение задачи об укладке ранца;
- вычисление значения полинома по модулю;
- экспоненциальные преобразования и др.

1.3 Аналитические преобразования

1.3.1 *Метод алгебры матриц*

$$Y = A \cdot X$$

где X – вектор элементов открытого текста,
Y – вектор элементов шифротекста,
A – матрица преобразования (ключ).

Пример.

Шифрование

$$Y = A \cdot X = \begin{vmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{vmatrix} \cdot \begin{vmatrix} 2 \\ 0 \\ 19 \end{vmatrix} = \begin{vmatrix} 85 \\ 54 \\ 25 \end{vmatrix}$$

Расшифровывание

$$X = A^{-1} \cdot Y = \begin{vmatrix} 1 & -2 & 1 \\ -2 & 5 & -4 \\ 1 & -4 & 6 \end{vmatrix} \cdot \begin{vmatrix} 85 \\ 54 \\ 25 \end{vmatrix} = \begin{vmatrix} 2 \\ 0 \\ 19 \end{vmatrix}$$

1.3 Аналитические преобразования

1.3.2 *По особым зависимостям*

Метод ***укладки ранца***.

$C = |c_1, c_2, ..., c_n|$ - вектор чисел, ключ

Каждый символ X_i открытого текста представлен в виде *n* бит

$X_i = |x_1, x_2, ..., x_n|^T$, $x_k \in \{0, 1\}$.

Шифротекст получается как скалярное произведение $C*X_i$.

Пример.

Открытый текст	16	17	9	11	1	8
в двоичном виде	10000	10001	01001	01011	00001	01000
Вектор C =	1	3	5	7	11	
Шифр	1	12	14	21	11	3

1.3 Аналитические преобразования

1.3.2 *По особым зависимостям*

Метод ***полиномов***

Основан на преобразовании

$$y_i = \left(x_i^n + a_i \cdot x_i^{n-1} + \ldots + a_n \cdot x_i\right) \bmod p$$

где x_i – i-й элемент открытого текста,

y_i – i-й элемент шифротекста,

a_i – целые неотрицательные числа (ключ),

p – большое простое число.

1.4 Гаммирование

Гамма шифра – псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму.

Гаммирование – процесс наложения по определенному закону гаммы шифра G_i на открытые данные x_i (для шифрования) или закрытые данные y_i (для расшифровывания)

$$y_i = x_i \oplus G_i$$

$\oplus$ - операция поразрядного сложения по модулю 2, XOR (либо другая логическая операция)

1.4 Гаммирование

1.4.1 *С конечной гаммой*

Пример шифрования

Открытый текст	**Г А М Б И Т**
Код	**04 01 13 02 09 19**
Гамма шифра	**М О Д Е Л Ь**
Код	**13 15 05 06 12 29**
Операция сложения по модулю 33	**17 16 18 08 21 15**
Код шифра	**17 16 18 08 21 15**
Шифр	**Р П С З Ф О**

1.4 Гаммирование

1.4.1 *С бесконечной гаммой*

Пример шифрования

Открытый текст	**Г А М Б И Т**
Код	**04 01 13 02 09 19**
Гамма шифра	**07 06 09 04 05 08 07 09 …**
Код	**07 06 09 04 05 08 07 09 …**
Операция сложения по модулю 2	**03 07 04 06 12 27**
Код шифра	**03 07 04 06 12 27**
Шифр	**В Ж Г Е Л Ъ**

1.4 Гаммирование

- Гаммирование лежит в основе потоковых (побитных) криптоалгоритмов
- Криптостойкость определяется периодом псевдослучайной последовательности
- Гаммирование обладает высокой производительностью
- Простая аппаратная и программная реализация

1.5 Комбинированные методы

Последовательное использование нескольких различных методов шифрования для повышения криптостойкости шифрования.

Распространенные комбинации:

- подстановка + гаммирование
- замена + гаммирование
- гаммирование + гаммирование
- замена + перестановка

Стандарт шифрования данных DES (США), ГОСТ 28147-89 (Россия)

2. Кодирование

2.1 Смысловое

Замена одних смысловых данных (слов, фраз) на другие. Каждому специальному сообщению – свою систему кодирования.

«Имею 3 банки тушенки, привозите коробки» = «Вижу 3 танка, вызываю вертолеты»

2.2 Символьное

Сопоставление символам числовых кодов (для удобства передачи, хранения, обработки).

Примеры: код ASCII, азбука Морзе, код Хаффмена

2.3 Комбинированное

3. Другие методы шифрования

3.1 Рассечение – разнесение

Сообщение разбивается на блоки, которые хранятся в разных местах. Отдельный блок не позволяет раскрыть информацию.

3.2 Сжатие – расширение

Преобразование открытых данных с целью уменьшения объема памяти для их хранения. *Программы-архиваторы.*

3.3. Стеганография

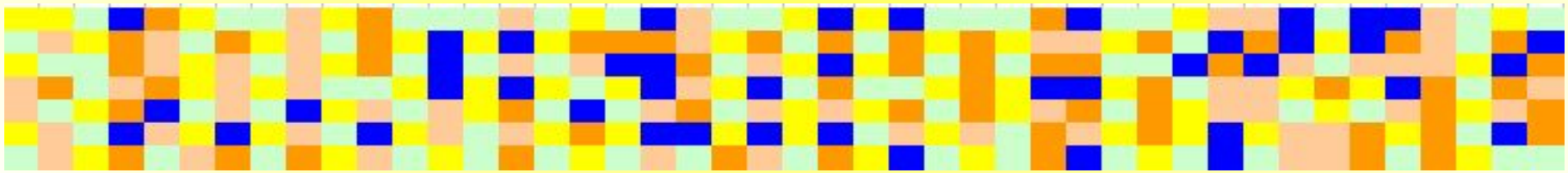
Методы маскировки, сокрытия факта присутствия конфиденциальной информации

Цифровая стеганография основана на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов.

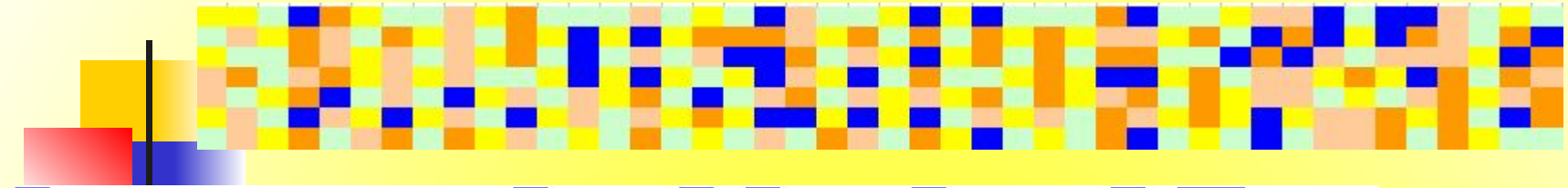
Как правило, данные объекты являются мультимедиа-объектами (изображения, видео, аудио, текстуры 3D-объектов) и внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека, не приводит к заметным изменениям этих объектов

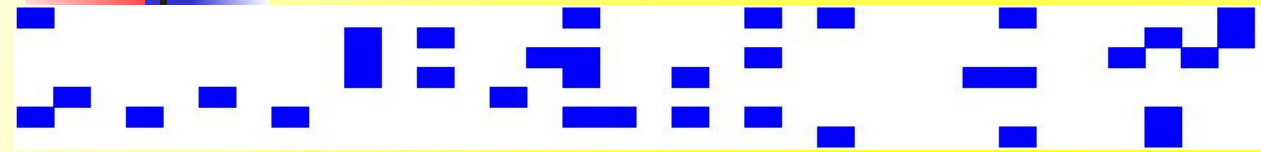
Пример:

(шифрованное сообщение содержится в цветовом шуме)

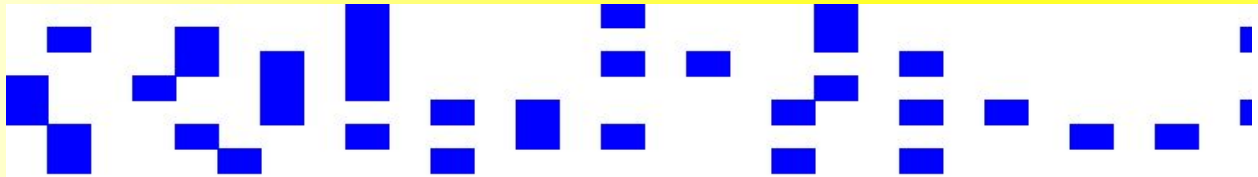


Расшифровка (взлом): по очереди оставляем один из 6-ти цветов, затем 2 из 6-ти (15 комбинаций), затем 3 из 6-ти (20 комбинаций)… - пока не получим расшифровку.





Оставили темно-синий цвет, вместо него - синий



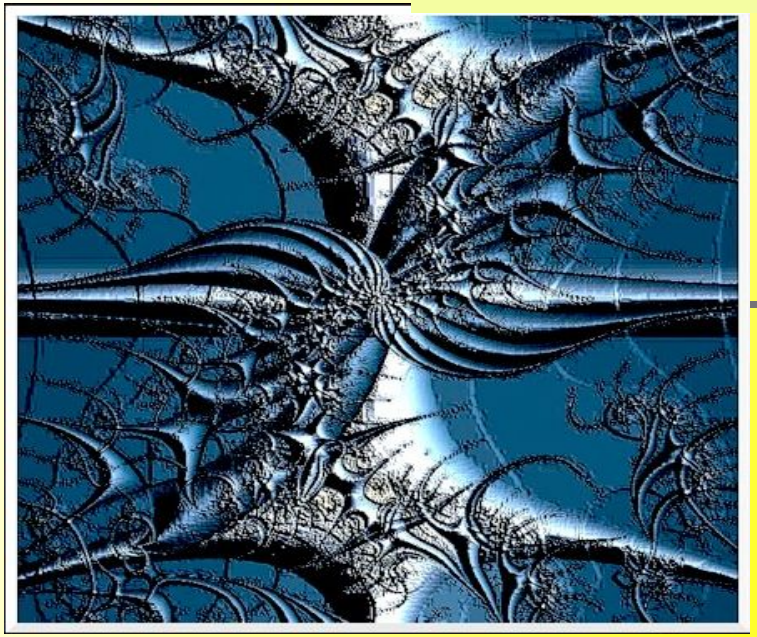
Оставили оранжевый цвет, вместо него - синий

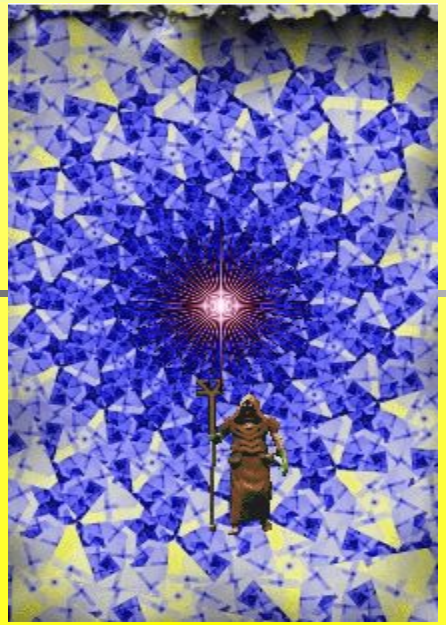
Оставили темно-синий и оранжевый цвет, вместо их - синий

Оставили светло-желтый и светло-зеленый, вместо их - синий

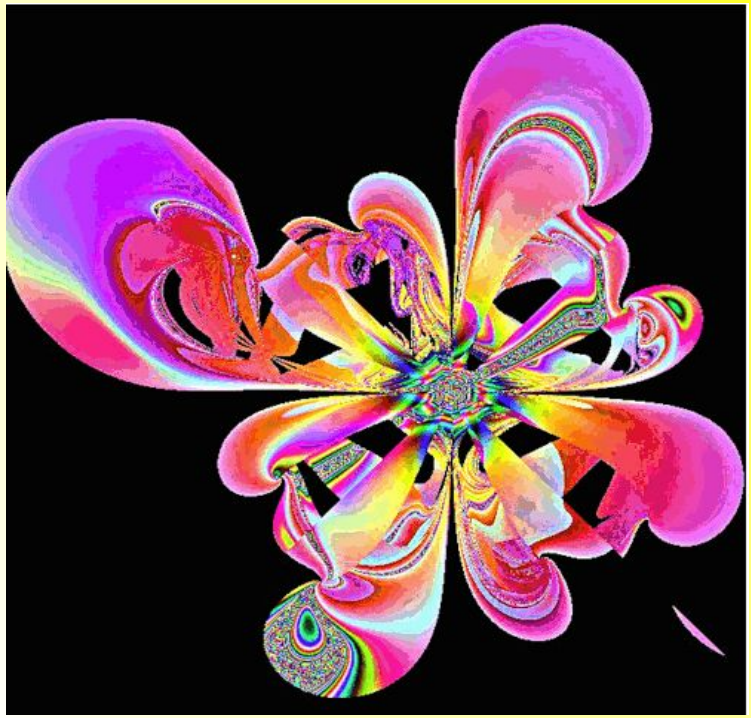
МЫ ЖИВЕМ ЗДЕСЬ

Примеры фракталов





На практике в стеганографии используются гораздо более сложные маскировки сообщения – не только цветом, но и формой элементов.



Хорошей базой являются **фракталы** – картины, которые строят сами компьютеры, используя уравнения с дробной размерностью.