

# Современные информационные технологии

Биологический институт  
Томский государственный  
университет

Лекция 3

**Криптография и защита информации**

# Дмитрий Владимирович Курбатский

старший преподаватель каф. ихтиологии и гидробиологии,  
научный сотрудник ЛМБ БИ ТГУ, магистр биологии

- Зоологический музей (к. 123)
  - Компьютерный класс (к. 028)
- Главный корпус
- Группа ВКонтакте «Курсы "Информатика" и "Информационные технологии"»:  
[vk.com/i\\_it\\_bi\\_tsu](https://vk.com/i_it_bi_tsu)
  - Персональный раздел:  
[zoo.tsu.ru/kdv](http://zoo.tsu.ru/kdv)
  - [Рейтинг на сайте Professorrating.ru](http://Professorrating.ru) Рейтинг на сайте

# Ссылки по теме

- [Математический аппарат и алгоритмы криптографии \(сайт СПб ГУ ИТМО\)](#)
- Общество шифропанков – [www.cypherpunks.ru](http://www.cypherpunks.ru)
- Проект "openPGP в России" – [www.pgpru.com](http://www.pgpru.com)
- Низкоуровневое программирование, исследование программ и их защита – [www.wasm.ru](http://www.wasm.ru) [*в дауне, искать сборники материалов*]

# Блок 1

Из истории шифров

# Термины

- **Алфавит** – непустое множество дискретной природы (конечное либо счётное).
- **Символ** – элемент алфавита.
- **Формальная грамматика** (или просто грамматика) — способ описания формального языка, то есть выделения некоторого подмножества из множества всех слов некоторого конечного алфавита.

# Шифр

- Имеет ключ
- Подчиняется принципам Керкгоффса
- != кодирование

# Принципы Керкгоффса

1. Система должна быть физически, если не математически, невскрываемой.
2. Нужно, чтобы не требовалось сохранение системы в тайне; попадание системы в руки врага не должно причинять неудобств.
3. Хранение и передача ключа должны быть осуществимы без помощи бумажных записей; корреспонденты должны располагать возможностью менять ключ по своему усмотрению.
4. Система должна быть пригодной для сообщения через телеграф.
5. Система должна быть легко переносимой, работа с ней не должна требовать участия нескольких лиц одновременно.
6. Наконец, от системы требуется, учитывая возможные обстоятельства её применения, чтобы она была проста в использовании, не требовала значительного умственного напряжения или соблюдения большого количества правил.

# Кодирование

- – процесс преобразования сигнала из формы, удобной для непосредственного использования информации, в форму, удобную для передачи, хранения или автоматической переработки.
- – как правило, взаимно-однозначный.

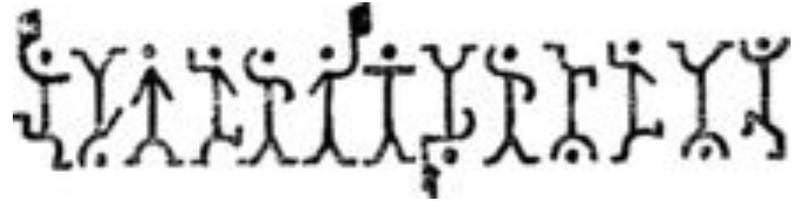
Примеры:

- Азбука Морзе
- Тюремный код
- Слэнг и жаргон
  - Язык офеней
- Индейцы-шифровальщики

# Шифры подстановки

- Одноалфавитный шифр подстановки (шифр простой замены) — шифр, при котором каждый символ открытого текста заменяется на некоторый, фиксированный при данном ключе символ того же алфавита.
  - Аффинный шифр
  - Шифр Цезаря  
АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ  
ГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВ
  - Атбаш  
А В С D E F G H I J K L M N O P Q R S T U V W X Y Z  
Z Y X W V U T S R Q P O N M L K J I H G F E D C B A
  - Шифр с использованием кодового слова  
А В С D E F G H I J K L M N O P Q R S T U V W X Y Z  
W O R D А В С E F G H I J K L M N P Q S T U V X Y Z

# Варианты



- Однозвучный шифр (омофоническая замена) подстановки похож на одноалфавитный за исключением того, что символ открытого текста может быть заменен одним из нескольких возможных символов.
  - Исторические шифры
  - Книжный шифр (стихи, книги)
  - [Шифр Виженера](#)
- Шифр с использованием неалфавитных или искусственных символов (*вовсе и не шифр!*)
- Шифрование 2..n групп символов, слов



# Шифры перестановки

- Поворотная решётка

1	2	3	7	4	1
4	5	6	8	5	2
7	8	9	9	6	3
3	6	9	9	8	7
2	5	8	6	5	4
1	4	7	3	2	1

# Взлом простых шифров

- частотный анализ
- семантический анализ
- вычисление длины ключа

# Связанные понятия

- Закон Ципфа

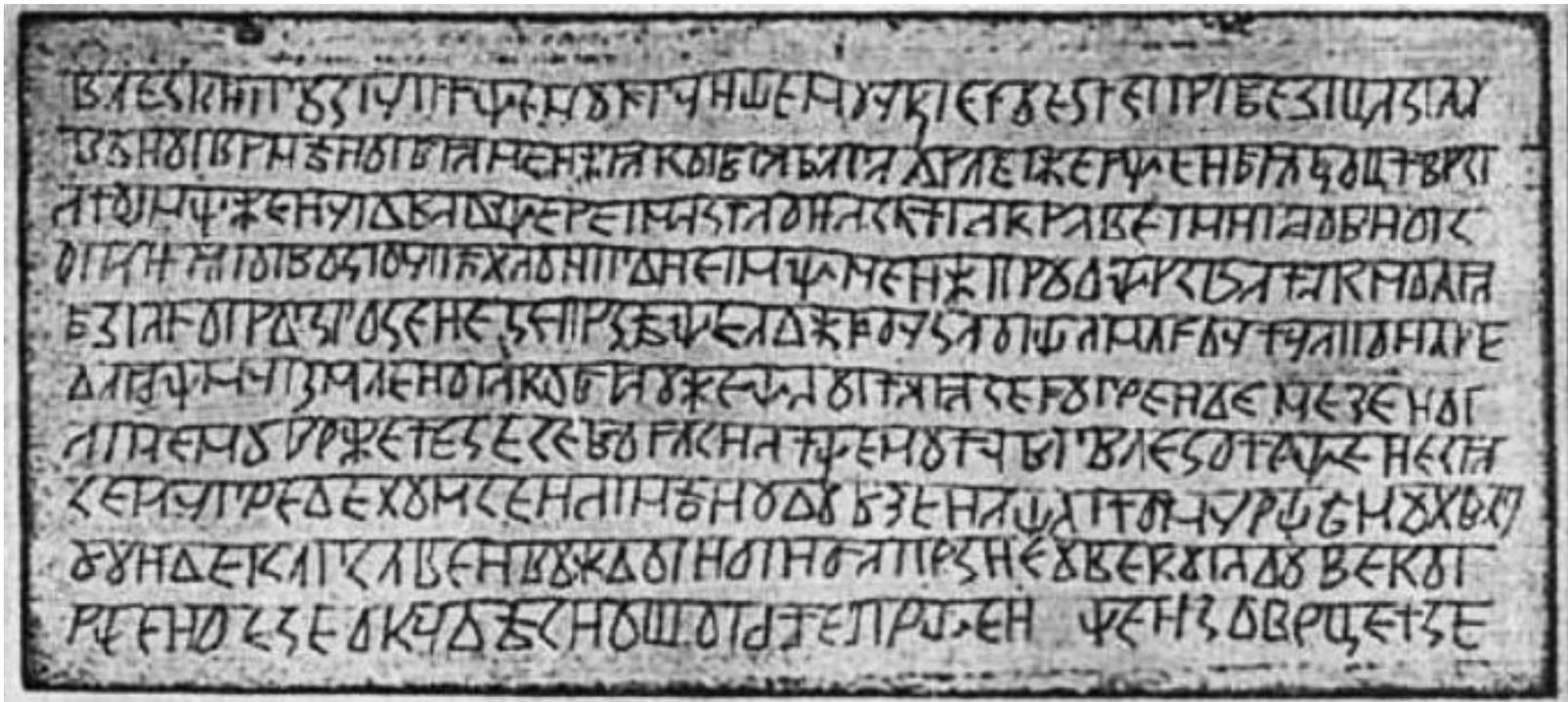
- эмпирическая закономерность распределения частоты слов естественного языка
- Если все слова языка (или просто достаточно длинного текста) упорядочить по убыванию частоты их использования, то частота  $n$ -го слова в таком списке окажется приблизительно обратно пропорциональной его порядковому номеру  $n$ .
- Например второе по используемости слово встречается примерно в два раза реже, чем первое, третье — в три раза реже, чем первое, и т. д.

- Информационная энтропия

- мера неопределённости или непредсказуемости информации, неопределённость появления какого-либо символа первичного алфавита.
- При отсутствии информационных потерь численно равна количеству информации на символ передаваемого сообщения.



# «Велесова книга»



# Связанные понятия

- [Частотный словарь](#)
- [Список Сводеша](#)
- [Марковские цепи](#)

# Блок 2

Современные аспекты  
криптографии

# Термины

- **Криптография** — наука о методах обеспечения конфиденциальности и аутентичности информации.
- **Криптоанализ** — наука, изучающая математические методы нарушения конфиденциальности и целостности информации.
- Криптография и криптоанализ составляют **криптологию**, как единую науку о создании и взломе шифров.
- **Криптоаналитик** — человек, создающий и применяющий методы криптоанализа.
- **Криптографическая атака** — попытка криптоаналитика вызвать отклонения в атакуемой защищенной системе обмена информацией. Успешную криптографическую атаку называют взлом или вскрытие.
- **Криптографическая стойкость** — способность криптографического алгоритма противостоять криптоанализу.

# Термины

- **Открытый** (исходный) **текст** — данные (не обязательно текстовые), передаваемые без использования криптографии.
- Шифротекст, **шифрованный** (закрытый) **текст** — данные, полученные после применения криптосистемы (обычно — с некоторым указанным ключом).
- **Ключ** — параметр шифра, определяющий выбор конкретного преобразования данного текста.
- **Шифр**, криптосистема — семейство обратимых преобразований открытого текста в шифрованный.

# Термины

- **Шифрование** — процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа, в результате которого возникает зашифрованный текст.
- **Дешифрование** (дешифровка) — процесс извлечения открытого текста без знания криптографического ключа на основе известного зашифрованного.
- **Расшифровывание** — процесс нормального применения криптографического преобразования зашифрованного текста в открытый.

# Термины

- **Аутентификация** (*Authentication*) — процедура проверки подлинности.
- **Авторизация** – процедура предоставления субъекту определённых прав.
- **Идентификация** – процедура распознавания субъекта по его идентификатору.



Человек-оркестр / The Band / L'homme orchestre (Серж Корбер Serge Korber) [1970 Франция комедия мюзикл BDRip-AVC] Du (USSR) + 2x MVO +

Страницы: 1

[ответить](#) [Список форумов](#)

Автор

holoff

Download

**Скачать раздачу по magnet-ссылке · 2.96 GB**

Для скачивания .torrent файлов необходима [регистрация](#)  
[Как скачивать](#) · [Что такое torrent \(торрент\)](#)

Сайт не распространяет и не хранит электронные версии произведений, а лишь предоставляет создаваемому пользователями каталогу ссылок на [торрент-файлы](#), которые содержат хеш-сумм

THE BAND | L'HOMME ORCHESTRE

# Проблемы

- Проблема конфиденциальности — проблема защиты информации от ознакомления с ее содержимым со стороны лиц, не имеющих права доступа к ней.
- Проблема целостности — проблема несанкционированного изменения информации.
- Проблема аутентификации — проблема подтверждения подлинности сторон (идентификация) и самой информации в процессе информационного взаимодействия. Информация должна быть аутентифицирована по источнику, времени создания, содержанию данных, времени пересылки и т. п.
- Проблема невозможности отказа от авторства — проблема предотвращения возможности отказа субъектов от некоторых из совершенных ими действий.

# Контрольные суммы

	$k_{13}$	$k_{12}$	$k_{11}$	$k_{10}$	$k_9$	$k_8$	$k_7$	$k_6$	$k_5$	$k_4$	$k_3$	$k_2$	$k_1$
<b>EAN-13</b>	1	3	1	3	1	3	1	3	1	3	1	3	1
<b>UPC-12</b>													
<b>EAN-8</b>													

$$(3+0+0+0+0+7+4) + (2+0+0+0+3+7)*3 = 50$$

$$50 \bmod 10 = 0$$

*=> код считан верно*



# Хэширование

- *hashing*
- преобразование по определённому алгоритму входного массива данных произвольной длины в выходную битовую строку фиксированной длины

варианты названия:

- хэш-функции
- функции свёртки

варианты названия результата:

- хэш
- хеш-код
- дайджест сообщения (*message digest*).

# Требования

- Необратимость: для заданного значения хеш-функции должно быть вычислительно неосуществимо найти соответствующий блок данных.
- Стойкость к коллизиям первого рода: для заданного сообщения  $M$  должно быть вычислительно неосуществимо подобрать другое сообщение  $N$ , для которого  $H(M) = H(N)$ .
- Стойкость к коллизиям второго рода: должно быть вычислительно неосуществимо подобрать пару сообщений, имеющих одинаковый хеш.

# Связанные понятия

- Коллизии
- Парадокс дней рождения
  - 23 человека ~ 50 %
  - откуда для хэшей – не  $2^N$ , а только около  $2^{(N/2)}$
- Лавинный эффект
  - MD5(0110 0001 0110 0001 0110 0001 0110 0001) = '74b87337454200d4d33f80c4663dc5e5'
  - MD5(0110 0001 0110 0011 0110 0001 0110 0001) = 'ca7de9e17429612452a717a44c36e688'
  - MD5(0110 0001 0110 0001 0110 0001 0110 0011) = '3963a2ba65ac8eb1c6e2140460031925'

# Применение хэширования

- Сверка данных
  - Парольная защита
- Проверка на наличие ошибок

Имя файла	Тип	Размер	Дата
Sabayon_Linux_10_amd64_K	iso	2 231 369 728	12.09.2012 07
Sabayon_Linux_10_amd64_K.iso	md5	63	28.02.2013 22
Sabayon_Linux_10_amd64_K.iso	pkglist	34 341	28.02.2013 21

- Ускорение поиска данных



SHA256: 273a138e4d66b5aa8d86f2f5fc1e7aa64145cc031a67458b6613d4f0a0188ab2

Имя файла: filename

Показатель выявления: 1 / 56

Дата анализа: 2016-01-10 14:53:13 UTC (1 месяц, 1 неделя назад)

Имя торрента № Объем Готово Состояние

Леонтьев А.Н. - Правила ...		28.3 Мб	100.0%	В очереди р
Unformat. 2.0		6.95 Мб	100.0%	Ошибка: Им
(trumpet) J.B.Arban-Vollst...		61.7 Мб	100.0%	Ошибка: Им

Общие Трекеры Пирры Части Файлы Ск

Загружено: [Progress bar]

Доступно: [Progress bar]

### Параметры передачи

Прошло:	38 нед. 4 дн.	Осталось:
Загружено:	28.3 Мб	Отдано:
Скорость приёма:	0.0 Кб/с (в среднем 58.9 Кб/с)	Скор. отдачи:
Лимит приёма:	∞	Лимит отдачи:
Состояние:	В очереди раздач	

### Общие

Расположение: D:\Загрузки\Леонтьев А.Н. - Правила дорожного движе

Общий объём: 28.3 Мб (28.3 Мб готово)

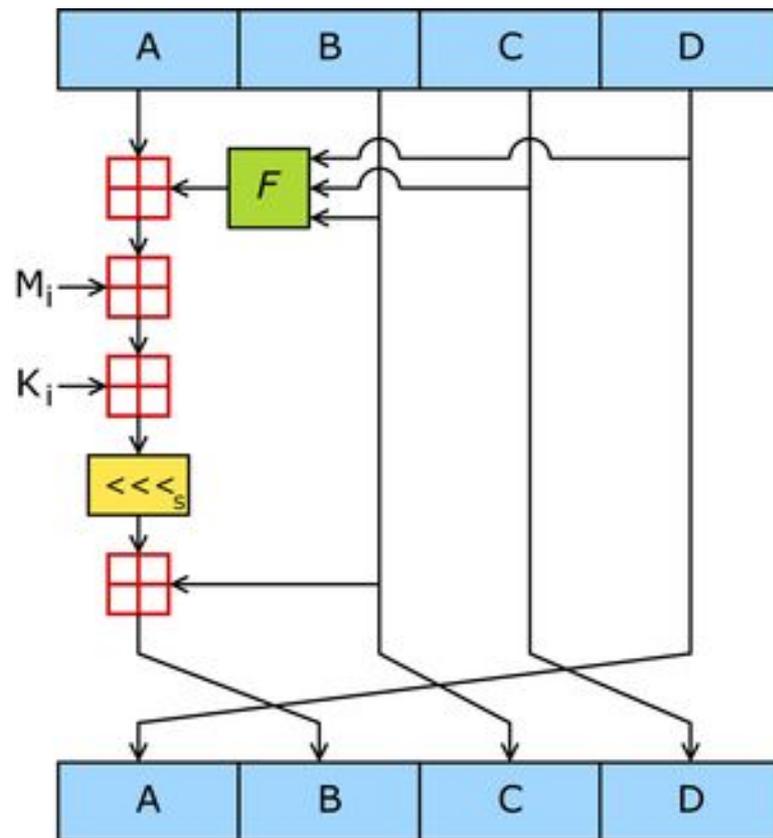
Создано: 11.08.2011 15:47:28 с помощью uTorrent/2000

Хеш-сумма: F000E7D0 255A25F6 F259BDBF 10A2FEB2 4BFBEA30

Описание: <http://rutracker.org/forum/viewtopic.php?t=3687651>

# Разновидности хэширования

- [Код Рида — Соломона](#)
- [Контрольные суммы](#)
  - CRC32
  - контрольная цифра
- [Криптографические хэш-функции](#)
  - [MD5](#) 😞
    - 128b
  - [SHA-2](#) 😊
    - 224..512b
  - Whirlpool
  - [ГОСТ Р 34.11-94](#)
    - 256b
  - [ГОСТ Р 34.11-2012](#)



# Базовая модель передачи данных



# Перехват данных

- активный
- пассивный

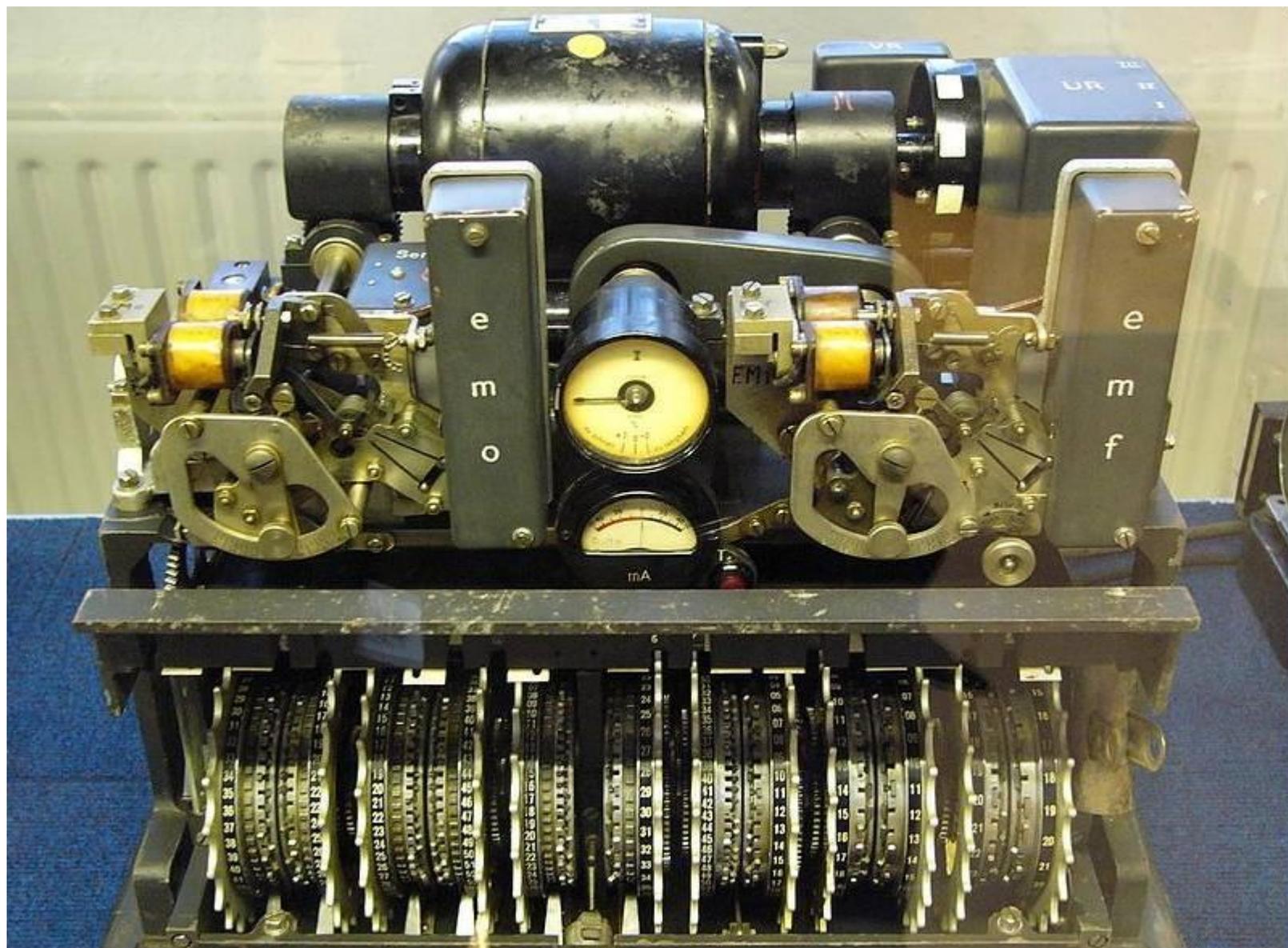
# Немного терминологии

- Гаммирование
  - функция XOR
    - $0111 \oplus 1100 = 1011$
  - вычеты по модулю
    - $(2+10) \bmod 11 = 1$
- Случайные и псевдослучайные числа

# Невзламываемый шифр

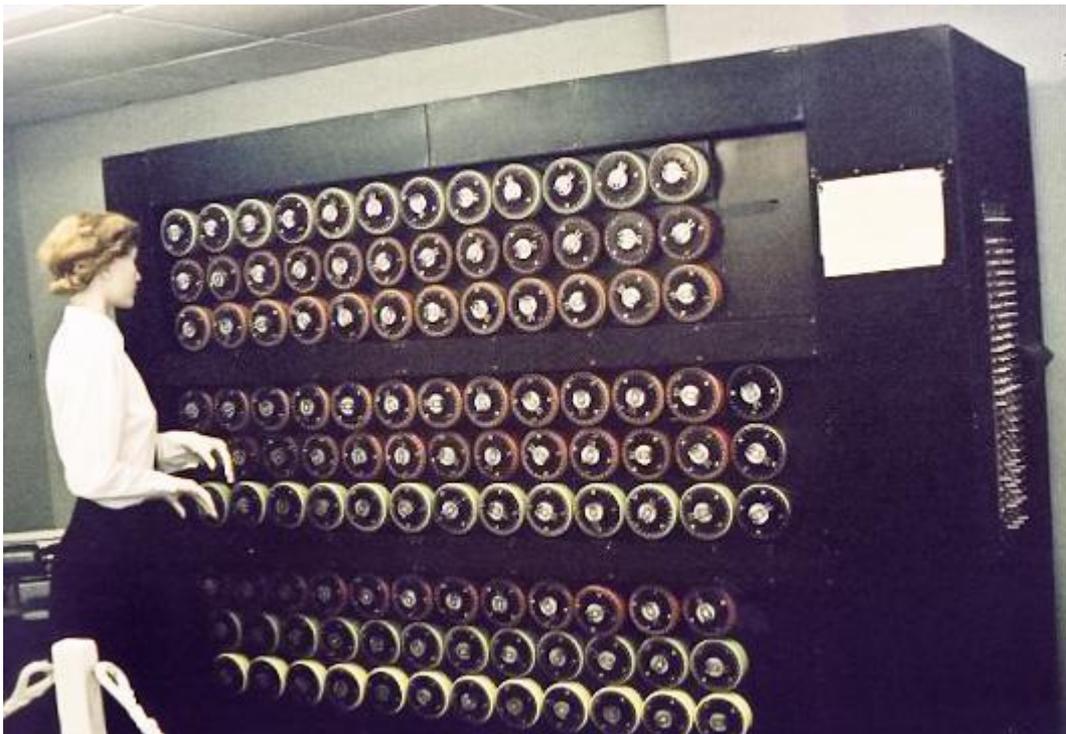
- [шифр Вернама](#), одноразовый блокнот
- Пример:  
Ключ           EVTIQWXQVVOPMCXREPYZ  
Открытый текст   ALLSWELLTHATENDSWELL  
Шифротекст       EGEAMAIBOSCOIQPAJATJK  
Шифрограмма   EGEAM AIBOS OIQPA JATJK
- Ключ должен:
  1. быть истинно случайным;
  2. совпадать по размеру с заданным открытым текстом;
  3. применяться только один раз.
- Хорош при 2 частично защищённых каналах или 1 надёжном.

# Машина Лоренца



# Машина «Энигма»

- Криптологическая бомба



# Криптостойкость

- Абсолютно стойкие криптосистемы

Требования:

- ключ генерируется для каждого сообщения (каждый ключ используется только один раз)
- ключ статистически надёжен (то есть вероятности появления каждого из возможных символов равны, символы в ключевой последовательности независимы и случайны)
- длина ключа равна или больше длины сообщения
- исходный (открытый) текст обладает некоторой избыточностью (что является критерием оценки правильности расшифровки)

- Достаточно стойкие криптосистемы

Основаны на:

- вычислительная сложность полного перебора
- известные на данный момент слабости (уязвимости) и их влияние на вычислительную сложность.

# Время полного подбора

• Кол-во знаков	Кол-во вариантов	Стойкость	Время перебора
• 1	36	5 бит	менее секунды
• 2	1296	10 бит	менее секунды
• 3	46 656	15 бит	менее секунды
• 4	1 679 616	21 бит	17 секунд
• 5	60 466 176	26 бит	10 минут
• 6	2 176 782 336	31 бит	6 часов
• 7	78 364 164 096	36 бит	9 дней
• 8	2,821 109 9x10 <sup>12</sup>	41 бит	11 месяцев
• 9	1,015 599 5x10 <sup>14</sup>	46 бит	32 года
• 10	3,656 158 4x10 <sup>15</sup>	52 бита	1 162 года
• 11	1,316 217 0x10 <sup>17</sup>	58 бит	41 823 года
• 12	4,738 381 3x10 <sup>18</sup>	62 бита	1 505 615 лет

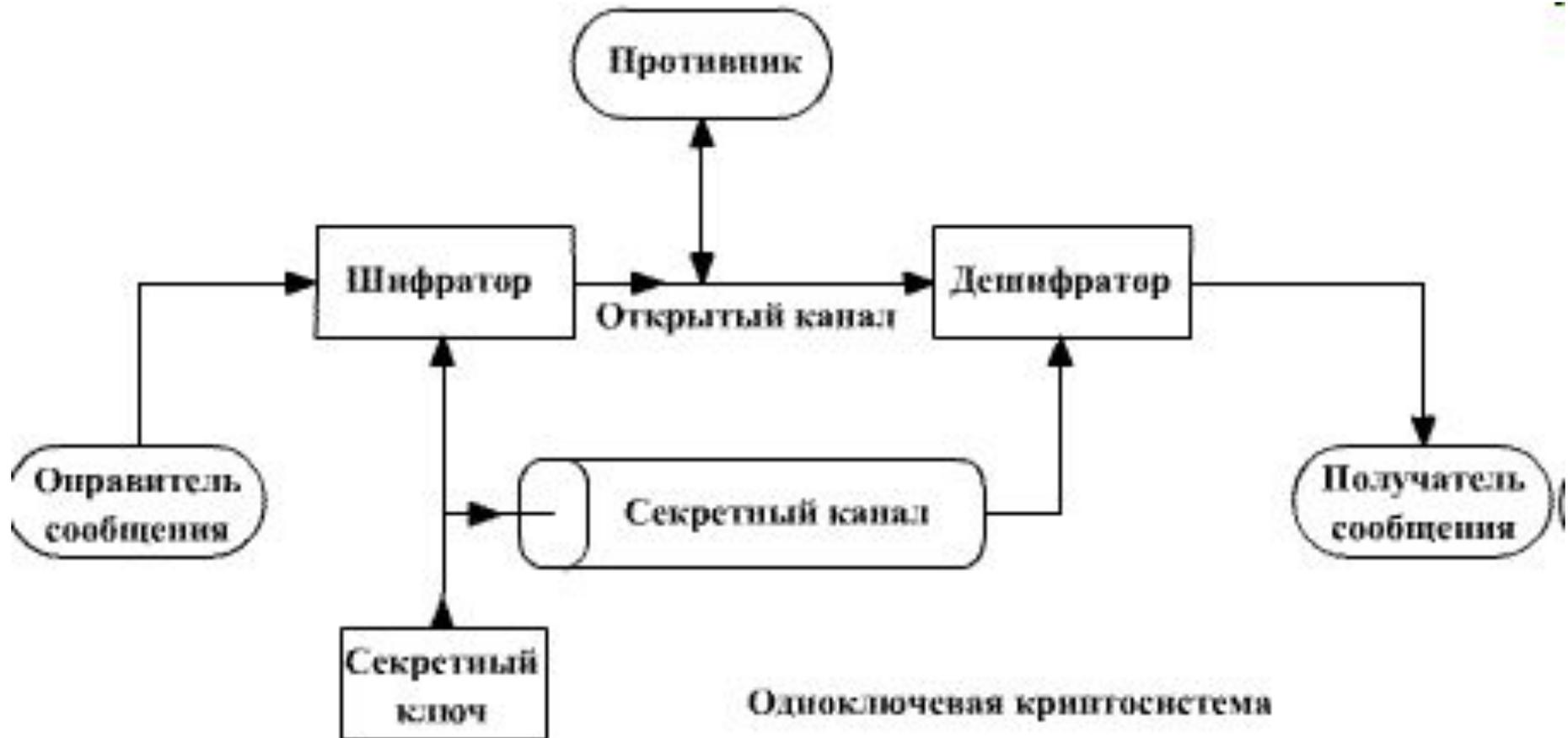
# Оценка секретных систем

- Количество секретности
- Объем ключа
- Сложность операции зашифрования и расшифрования
- Разрастание числа ошибок
- Увеличение объема сообщения

# По типу

- Симметричный шифр – использует один ключ для шифрования и дешифрования.
- Асимметричный шифр – использует два различных ключа.
- [Гибридные криптосистемы.](#)
- Хэш-функция

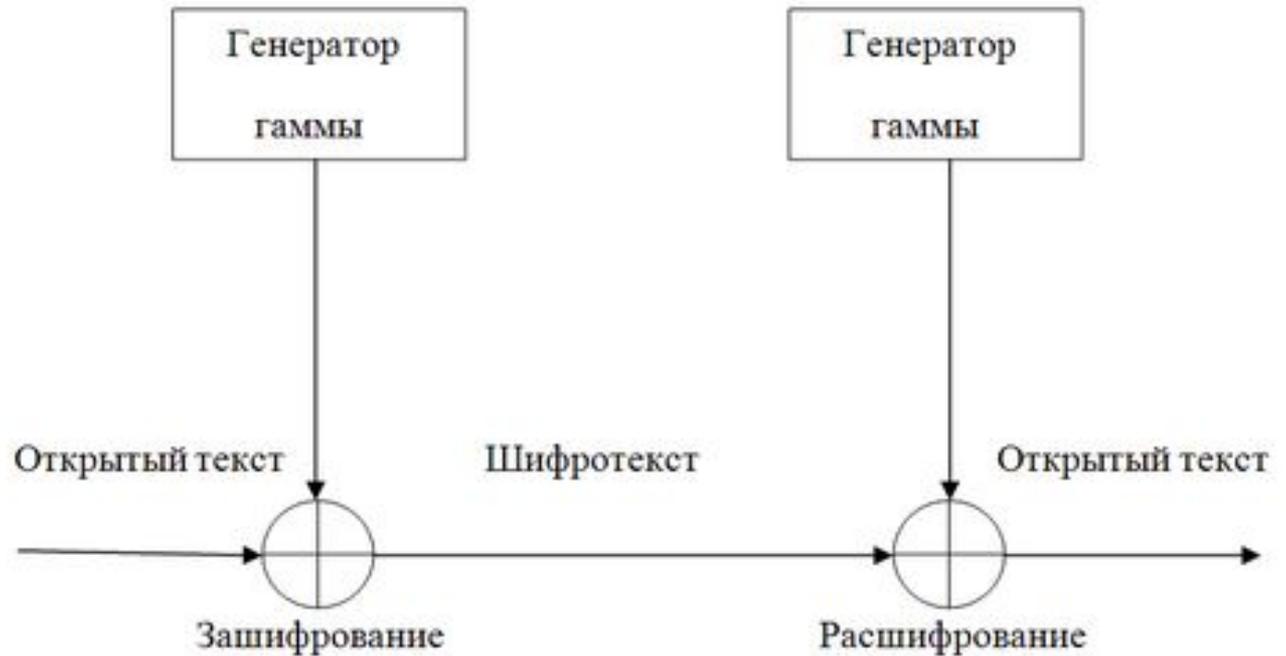
# Симметричное шифрование



# По поточности

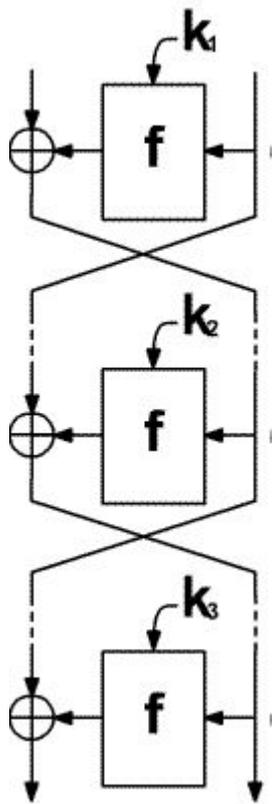
- Блочный шифр – шифрует сразу целый блок текста, выдавая шифротекст после получения всей информации.
- Поточный шифр – шифрует информацию и выдает шифротекст по мере поступления.

# Поточные шифры

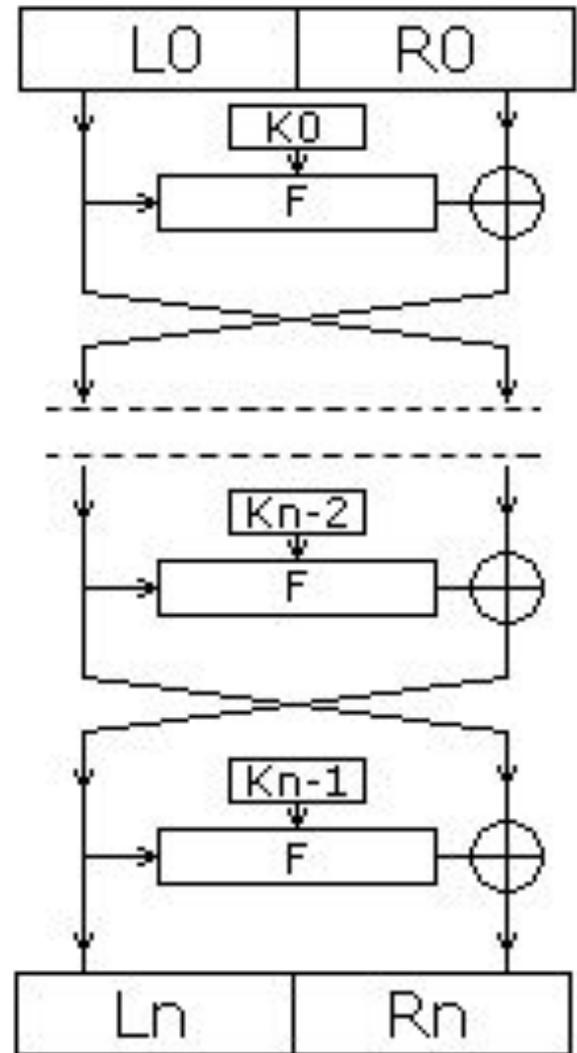
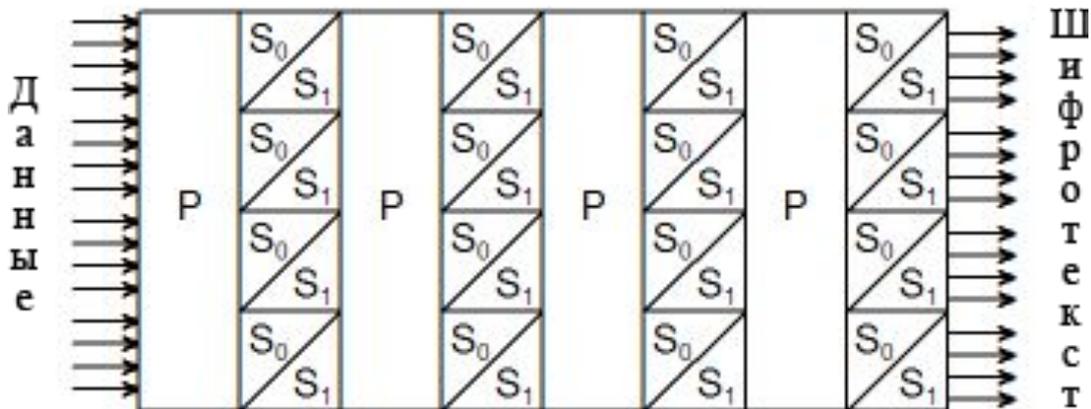


- Простые
- Синхронные
- Самосинхронизирующиеся
- На регистрах сдвига с линейной обратной связью (РСЛОС)
- И ещё сложнее

# Блочные шифры

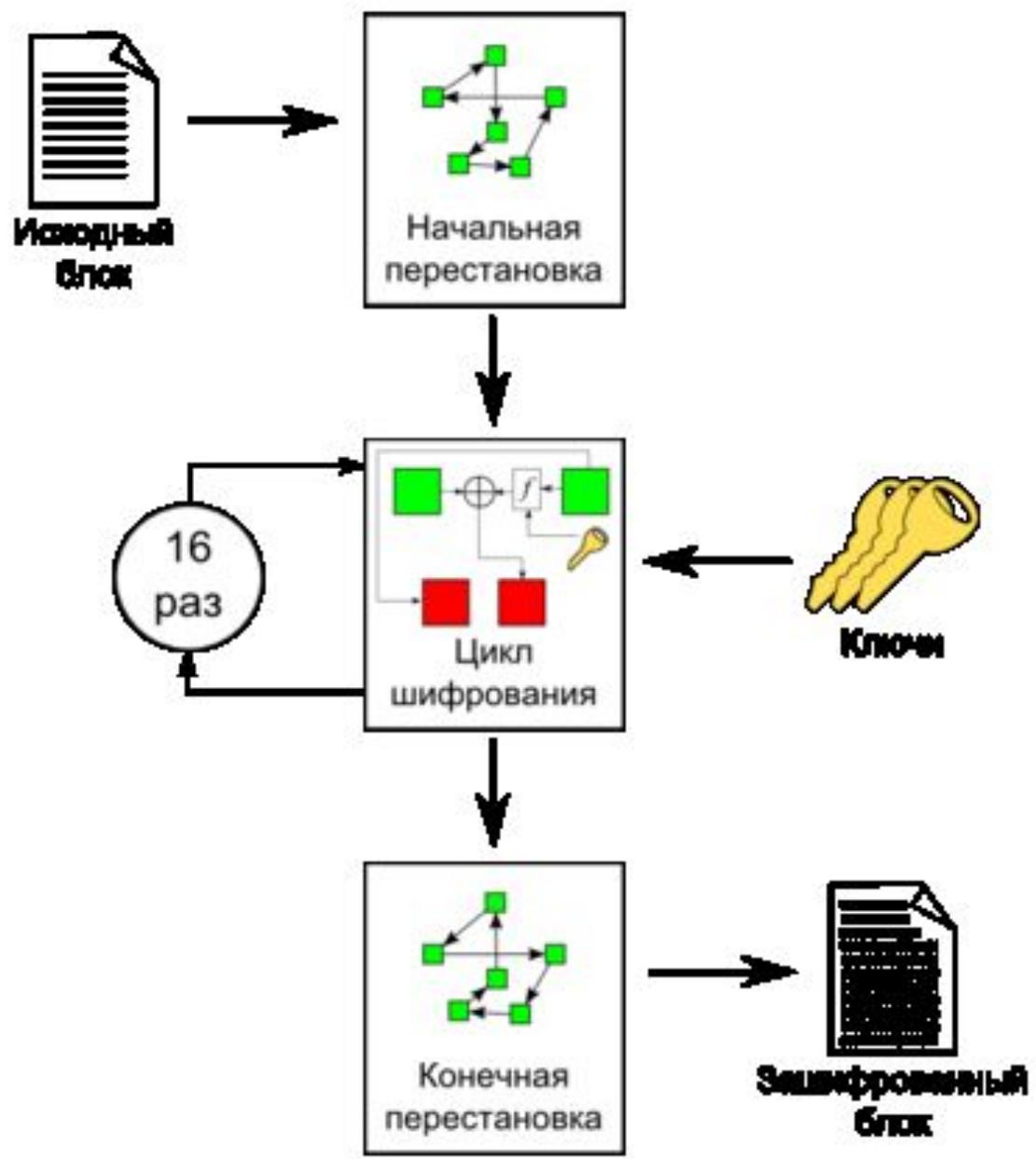


- часто: 1 блок = 64 бит
- принцип итерирования
- [конструкция Фейстеля](#)
- [SP-SP-сеть](#)
- ИНВОЛЮЦИЯ



# Стандарт Стандарт DES

- *data encryption standard*
- блочный, 64 бит
- ключ – 56 бит (64 бит включают биты чётности)
- шифр Фейстеля
- 16 итераций
- федеральный стандарт США (*был*)



# AES

- *Advanced Encryption Standard*
- блочный, 128 бит
- ключ – 128..256 бит
- SP-сеть
- 10..14 раундов
- современный стандарт США (и не только)

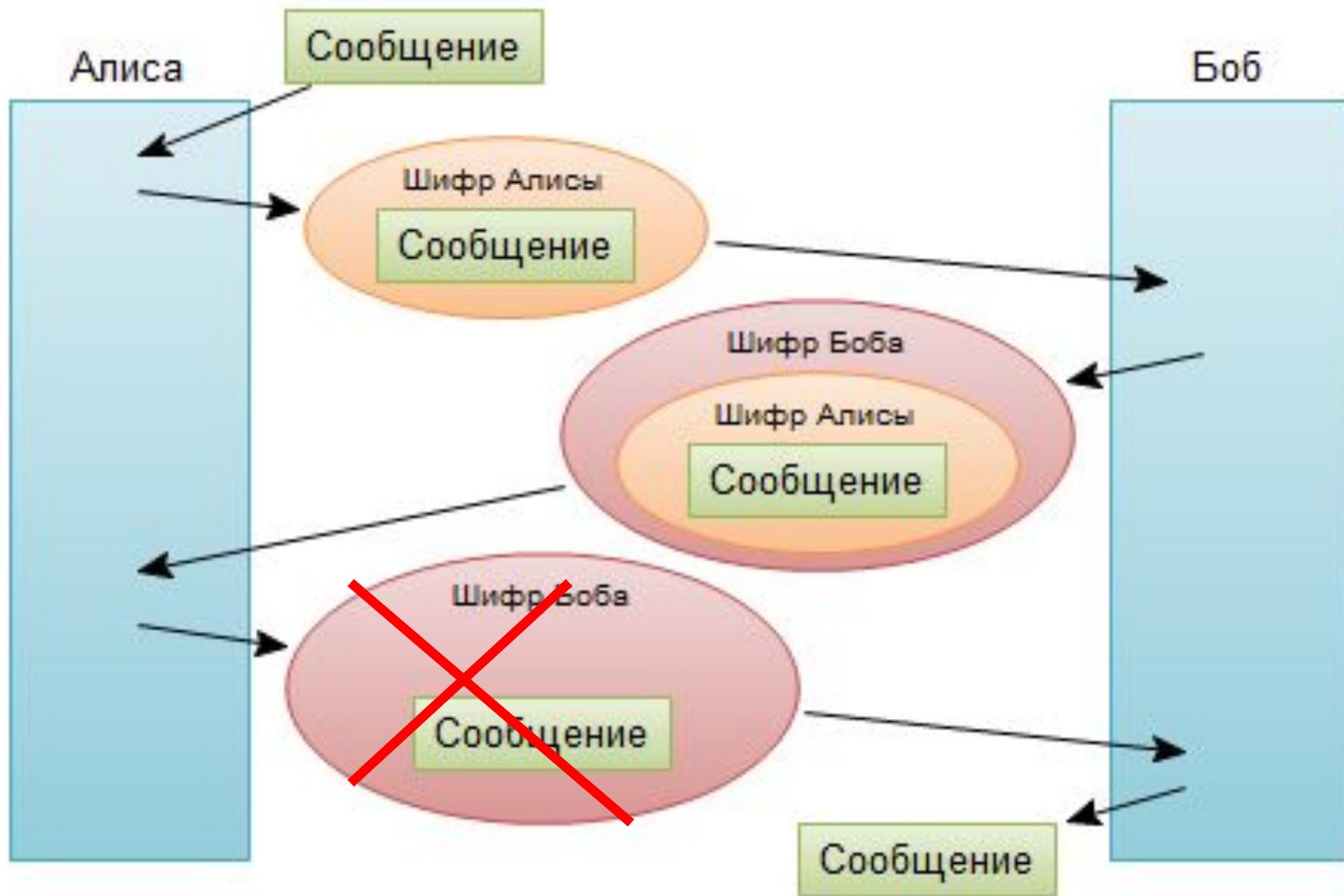
# ГОСТ 28147-89

- блочный, 64 бита
- ключ – 256 бит
- 32 итерации
- включает циклический сдвиг
- стандарт России

# Ещё термины

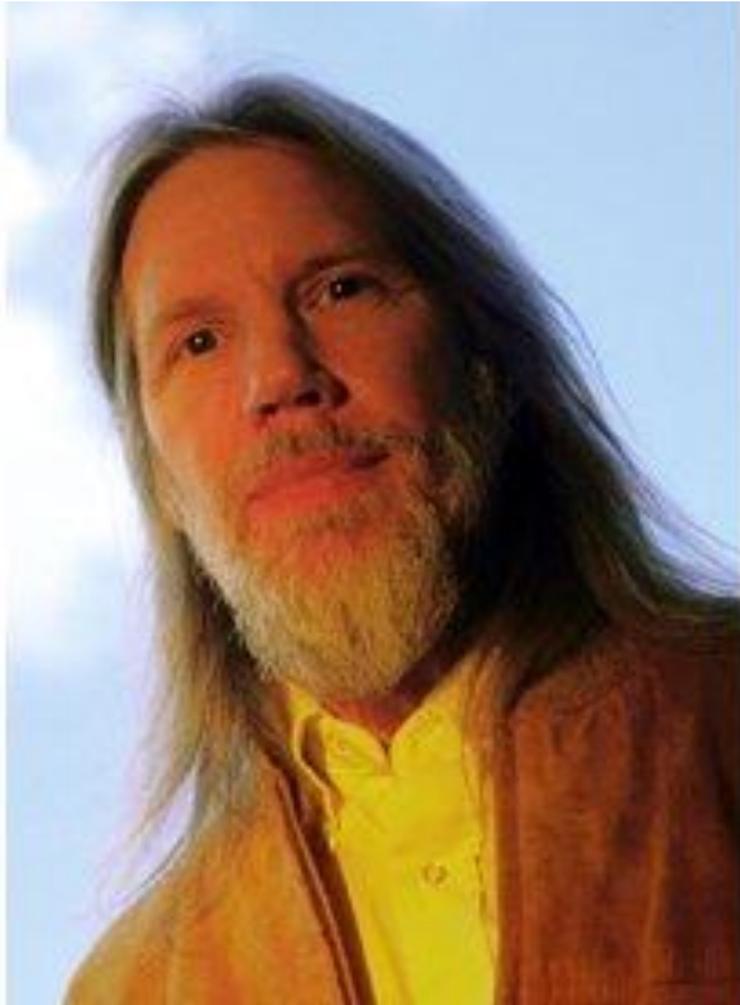
- аутентичный канал
- сеансовый ключ
- долговременный ключ
- цифровой конверт
- цифровая подпись
- код аутентификации сообщения (КАС, *message authentication code, MAC*)
- код целостности сообщений (КЦС, *message integrity check, MIC*) или имитовставка

# Алгоритм Диффи – Хеллмана

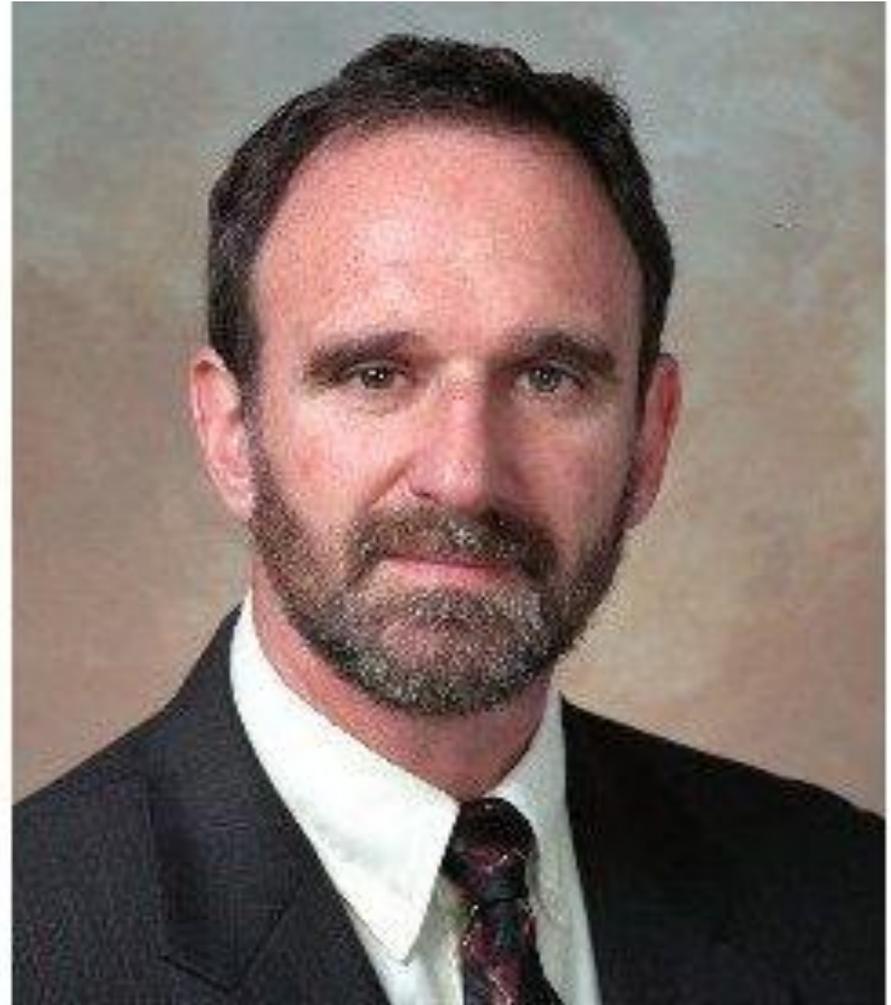


- [Очень хорошая статья](#) на тему.

# Алгоритм Диффи – Хеллмана



- Уитфилд Диффи
- *Bailey Whitfield 'Whit' Diffie*



- Мэ́ртин Хэ́ллман
- *Martin E. Hellman*

# Алгоритм Диффи – Хеллмана

- **Алгоритм обмена ключами**

- Односторонняя функция

- $f(x) = Y^x \pmod{P}$

- Пример:

$$2^2 \pmod{3} = 1$$

- $P$  должно являться простым числом

- $Y$  должно являться первообразным корнем по модулю  $P$

- $P, Y \sim 10^{300}$

$$5^x \pmod{7} = 2$$

$$x = ?$$

# Алгоритм Диффи – Хеллмана

<b>Этап 1</b>	<p>Оба участника договариваются о значениях <math>Y</math> и <math>P</math> для общей односторонней функции. Эта информация не является секретной. Допустим были выбраны значения <math>7</math> и <math>11</math>. Общая функция будет выглядеть следующим образом: <math>7^x \pmod{11}</math></p>	
<b>Этап 2</b>	<p>Алиса выбирает случайное число, например <math>3</math>, хранит его в секрете, обозначим его как число <math>A</math></p>	<p>Боб выбирает случайное число, например <math>6</math>, хранит его в секрете, обозначим его как число <math>B</math></p>

# Алгоритм Диффи – Хеллмана

<b>Этап 3</b>	Алиса подставляет число <b>A</b> в общую функцию и вычисляет результат $7^3 \pmod{11} = 343 \pmod{11} = 2$ , обозначает результат этого вычисления как число <b>a</b>	Боб подставляет число <b>B</b> в общую функцию и вычисляет результат $7^6 \pmod{11} = 117649 \pmod{11} = 4$ , обозначает результат этого вычисления как число <b>b</b>
<b>Этап 4</b>	Алиса передает число <b>a</b> Бобу	Боб передает число <b>b</b> Алисе

# Алгоритм Диффи – Хеллмана

<b>Этап 5</b>	Алиса получает <b>b</b> от Боба, и вычисляет значение $\mathbf{b^A \pmod{11} = 4^3 \pmod{11} = 64 \pmod{11} = 9}$	Боб получает <b>a</b> от Алисы, и вычисляет значение $\mathbf{a^B \pmod{11} = 2^6 \pmod{11} = 64 \pmod{11} = 9}$
<b>Этап 6</b>	Оба участника в итоге получили число <b>9</b> . Это и будет являться ключом.	

# Алгоритм Диффи – Хеллмана

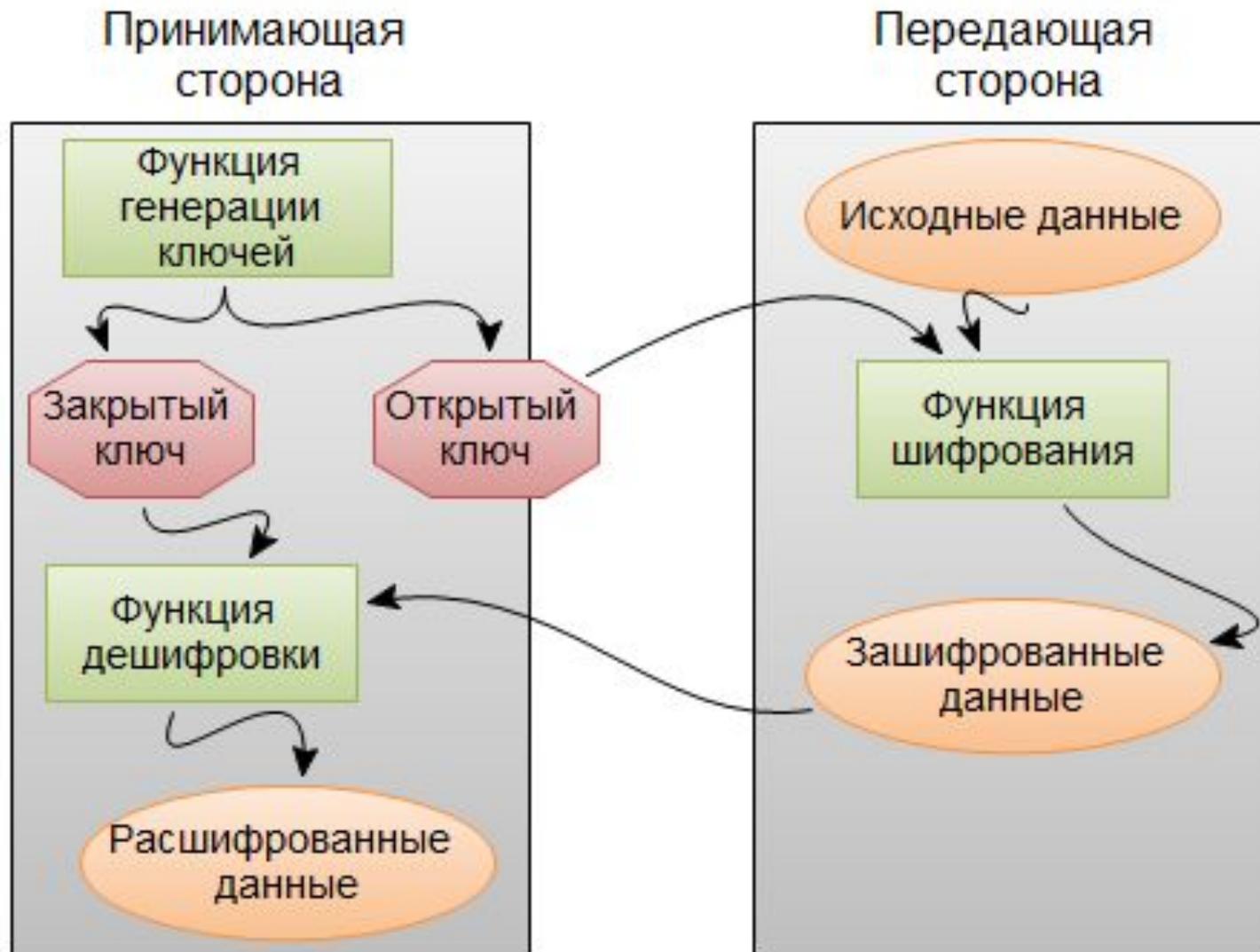
Чтобы получить ключ, необходимо знать

- Значения  $a$  и  $P$ , и секретное число Боба  $b$
- *или* значения  $b$  и  $P$ , и секретное число Алисы  $a$ .

# Ассиметричное шифрование

- Асимметричный шифр, двухключевой шифр, шифр с открытым ключом — шифр, в котором используются два ключа, шифрующий и расшифровывающий.
- Открытый ключ — тот из двух ключей асимметричной системы, который свободно распространяется. Шифрующий для секретной переписки и расшифровывающий — для электронной подписи.
- Секретный ключ, закрытый ключ — тот из двух ключей асимметричной системы, который хранится в секрете.

# Ассиметричное шифрование



# Асимметричная система



# Асимметричная система



# Применение АС

- Как самостоятельное средство для защиты передаваемой и хранимой информации.
- Как средство распределения ключей.
- Как средство аутентификации пользователей.

# Преимущества АС

- Не нужно предварительно передавать секретный ключ по надёжному каналу.
- Только одной стороне известен ключ шифрования, который нужно держать в секрете.
- Пару ключей можно не менять значительное время.
- В больших сетях число ключей в асимметричной криптосистеме значительно меньше, чем в симметричной.

# Недостатки АС

- В алгоритм сложнее внести изменения.
- Более длинные ключи.
- Шифрование-расшифрование с использованием пары ключей проходит на два-три порядка медленнее, чем шифрование-расшифрование того же текста симметричным алгоритмом.
- Требуются существенно бóльшие вычислительные ресурсы, поэтому на практике асимметричные криптосистемы используются в сочетании с другими алгоритмами.

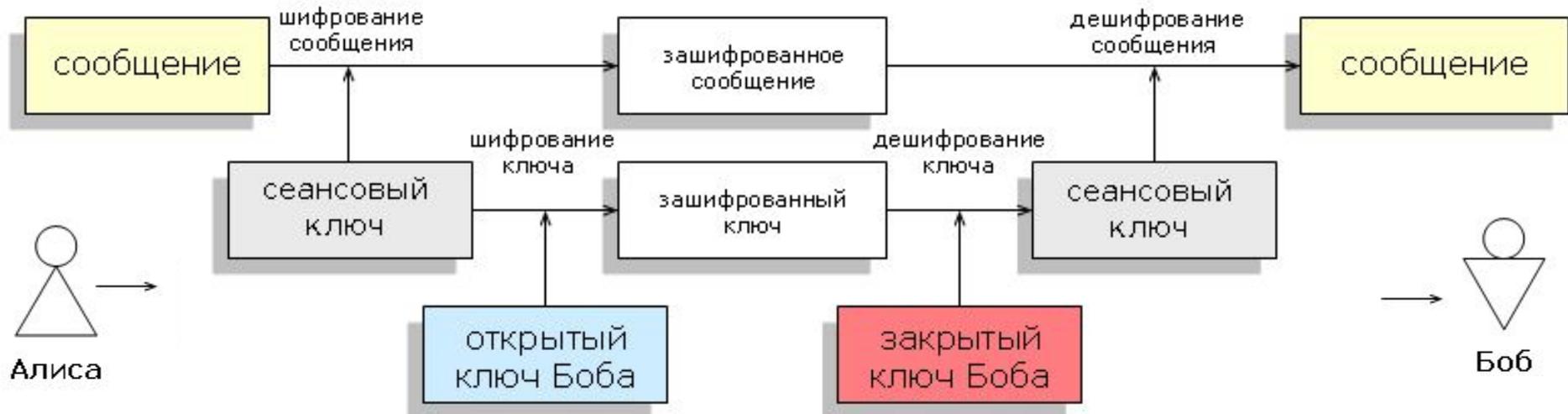
# Связанные понятия

- Задача дискретного логарифмирования (EGSA)
- Задача факторизации Задача факторизации, то есть разложения числа на простые множители (RSA)
- Эллиптические кривые

# Асимметричные алгоритмы

- RSA (*Rivest-Shamir-Adleman*)
  - используется в PGP, S/MIME, TLS/SSL, IPSEC/IKE
- DSA (*Digital Signature Algorithm*)
- Elgamal (Шифросистема Эль-Гамала)
- Diffie-Hellman (Обмен ключами Диффи — Хелмана)
- ECDSA (*Elliptic Curve Digital Signature Algorithm*) — алгоритм с открытым ключом для создания цифровой подписи.
- ГОСТ Р 34.10-2001

# Гибридные криптосистемы



# Методы взлома

- Криптоанализ
  - [дифференциальный](#)
  - [линейный](#)
- Полный перебор
  - метод ветвей и границ
  - распределённые вычисления
  - [радужные таблицы](#)
- Социальная инженерия
  - фишинг
  - терморектальный криптоанализ

# Методы криптоанализа

- Атака на основе шифротекста
- Атака на основе открытых текстов и соответствующих шифротекстов
- Атака на основе подобранного открытого текста (возможность выбрать текст для шифрования)
- Атака на основе адаптивно подобранного открытого текста
- Атака на основе подобранного шифротекста
- Атака на основе подобранного ключа

# Блок 3

Практические аспекты  
криптографии

# Способы аутентификации

- Прямая передача пароля
- Использование хэша
  - в т.ч. через cookie
- Использование шифрования

# Способы взлома и кражи данных в сетях

- Сниффинг
- Фишинг
- Подмена IP-адресов
- Подмена DNS
- Воровство cookie
- Кейлоггеры
- Социальная инженерия

# Защита WiFi

- Парольная защита
  - WEP 😞
  - WPA / WPA2 PSK 😊
- Скрытие SSID
- Привязка по MAC

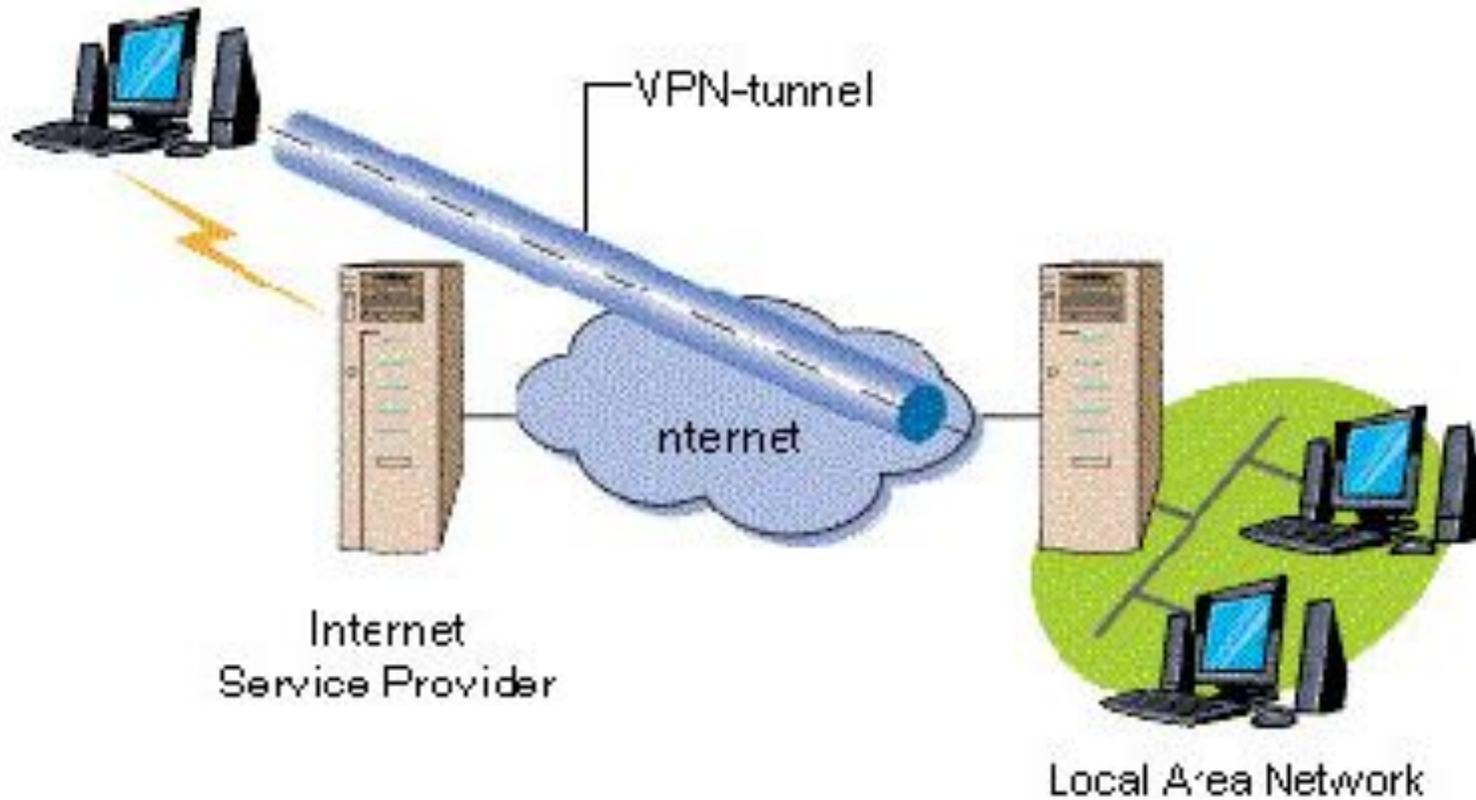
# HTTPS

- **SSL** (*secure sockets layer* — уровень защищённых сокетов)
- **TLS** (*Transport Layer Security* — безопасность транспортного уровня)  
– порт 443

# VPN

- *Virtual Private Network*
- виртуальная частная сеть

Remote Client



# SSH

- — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений.

# Шифропанк

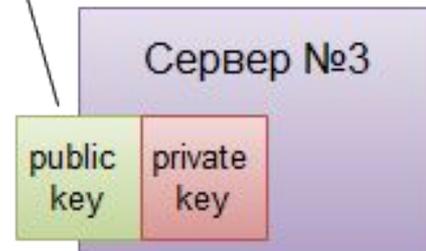
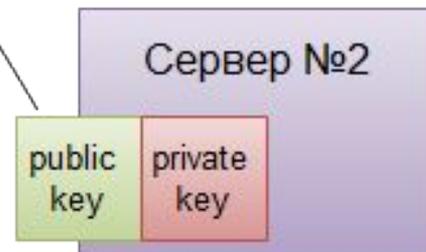
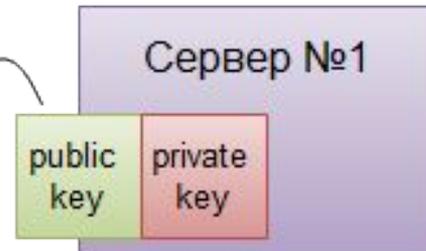
- [Статья про скрытие IP](#) Статья про скрытие IP
- [Ещё одна](#)

# TOR (*The Onion Router*)



- [Луковая маршрутизация](#) (*Onion routing*)

Исходный пакет

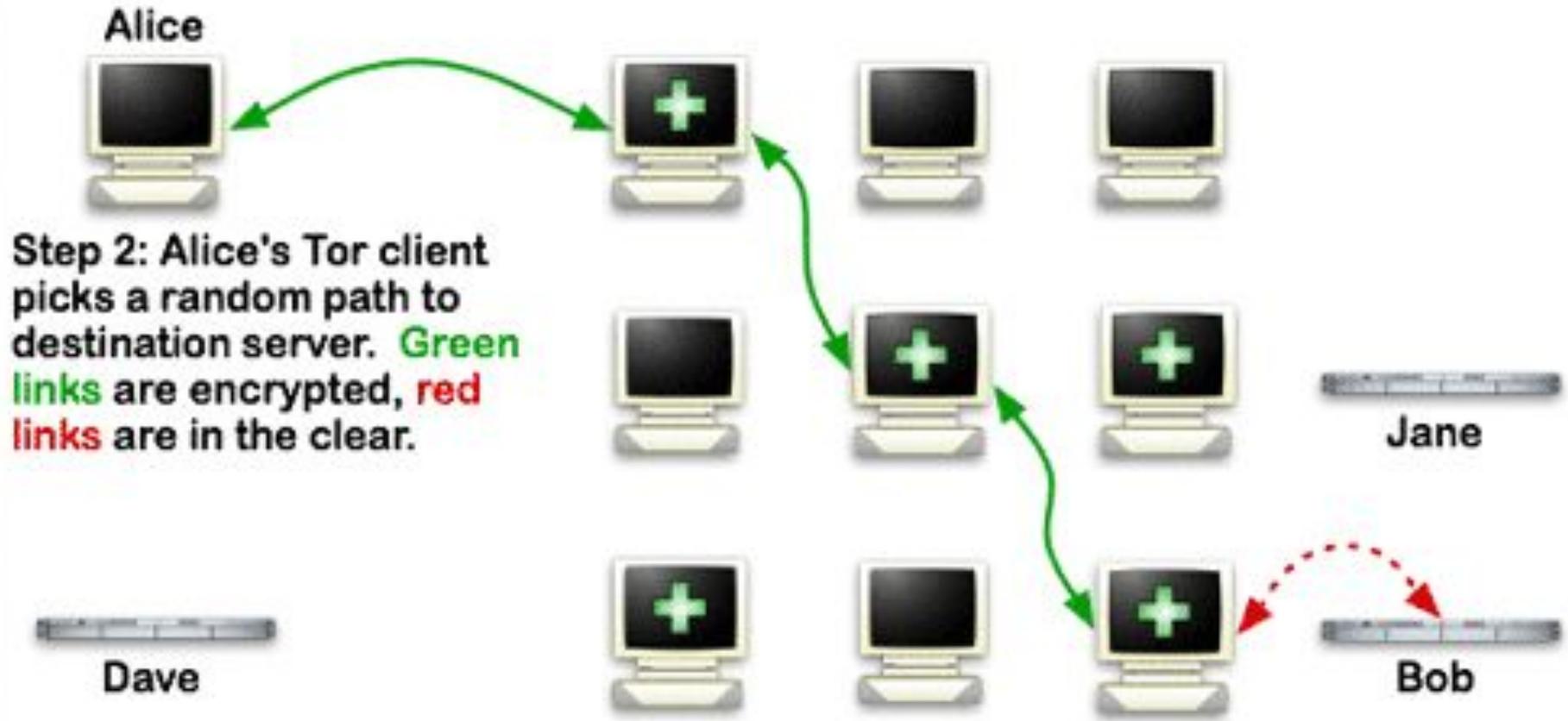
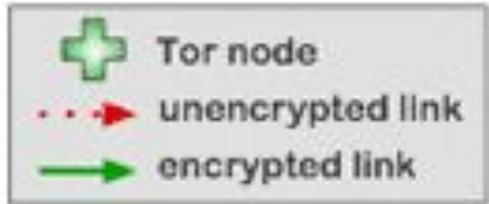


# How Tor Works: 1

-  Tor node
-  unencrypted link
-  encrypted link



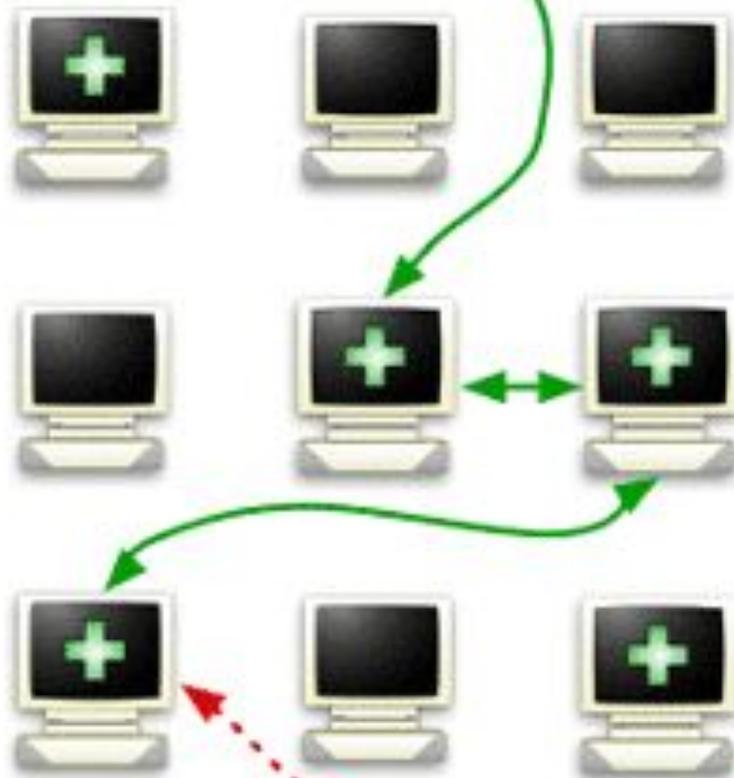
# How Tor Works: 2



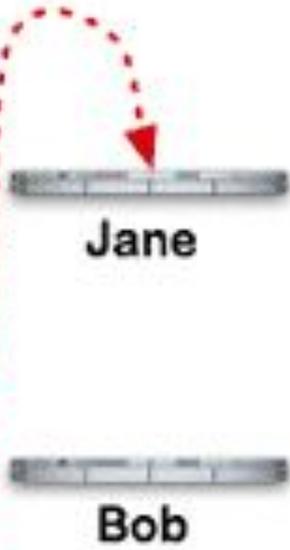
Step 2: Alice's Tor client picks a random path to destination server. **Green links** are encrypted, **red links** are in the clear.

# How Tor Works: 3

-  Tor node
-  unencrypted link
-  encrypted link

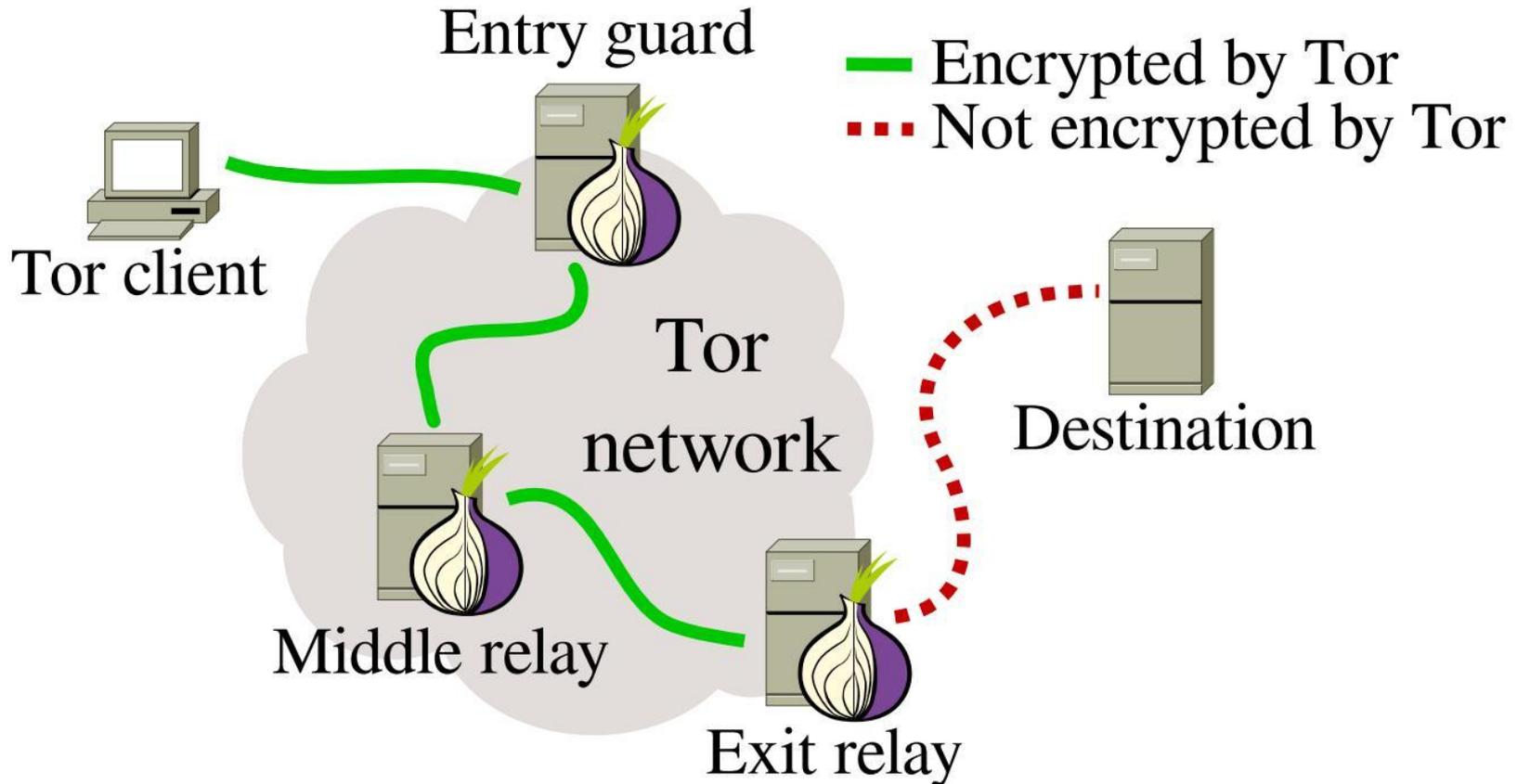


Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, **green links** are encrypted, **red links** are in the clear.



# TOR (*The Onion Router*)

- [Статья о безопасности в TOR](#) [Статья о безопасности в TOR](#)



# I2P

- *invisible internet project, IIP*
- чесночная маршрутизация
  
- Сеть
  - оверлейная
  - устойчивая
  - анонимная

# Электронная цифровая

## ПОДПИСЬ

### Назначение

- Контроль целостности передаваемого документа: при любом случайном или преднамеренном изменении документа подпись станет недействительной, потому что вычислена она на основании исходного состояния документа и соответствует лишь ему.
- Защита от изменений (подделки) документа: гарантия выявления подделки при контроле целостности делает подделывание нецелесообразным в большинстве случаев.
- Невозможность отказа от авторства. Так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец не может отказаться от своей подписи под документом.
- Доказательное подтверждение авторства документа: Так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец пары ключей может доказать своё авторство подписи под документом.

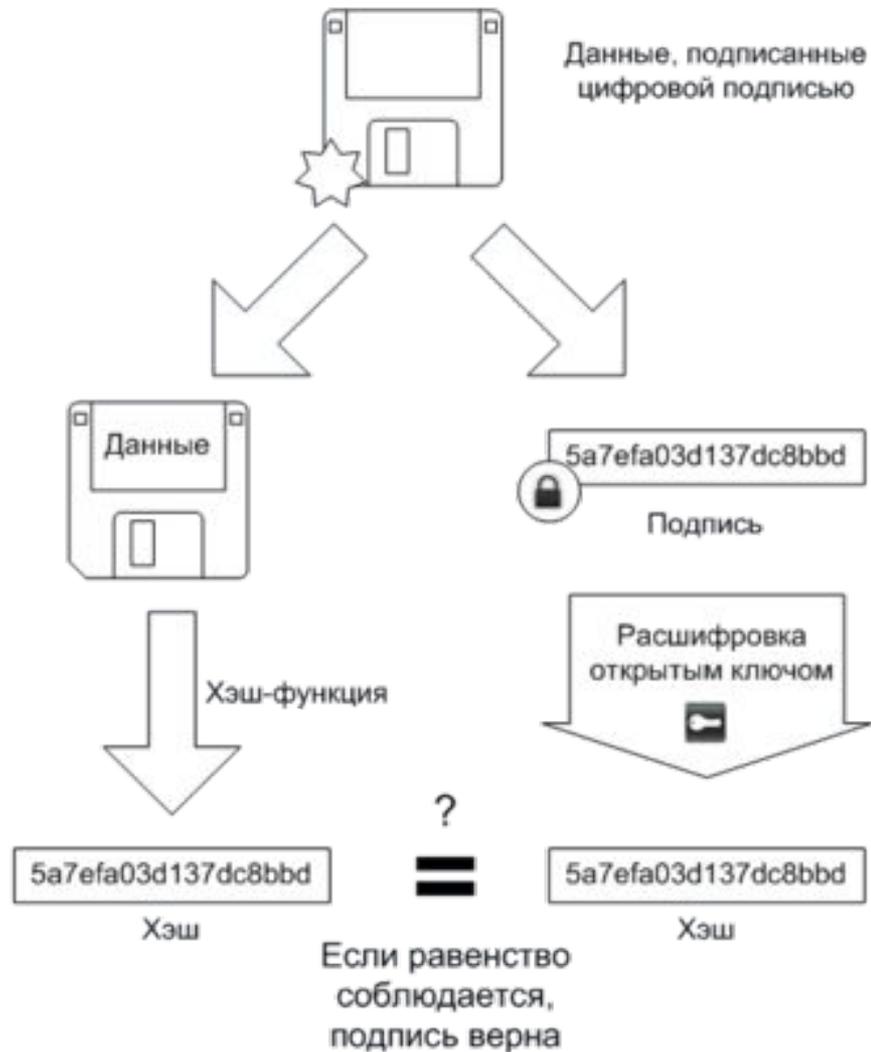
# Термины

- Имитозащита — защита от навязывания ложной информации. Имитозащита достигается обычно за счет включения в пакет передаваемых данных имитовставки.
- Имитовставка — блок информации, применяемый для имитозащиты, зависящий от ключа и данных.
- Электронная цифровая подпись, или электронная подпись — асимметричная имитовставка (ключ защиты отличается от ключа проверки). Другими словами, такая имитовставка, которую проверяющий не может подделать.
- Центр сертификации — сторона, чья честность неоспорима, а открытый ключ широко известен. Электронная подпись центра сертификации подтверждает подлинность открытого ключа.
- Хеш-функция — функция, которая преобразует сообщение произвольной длины в число («свёртку») фиксированной длины.

## Подписывание



## Проверка



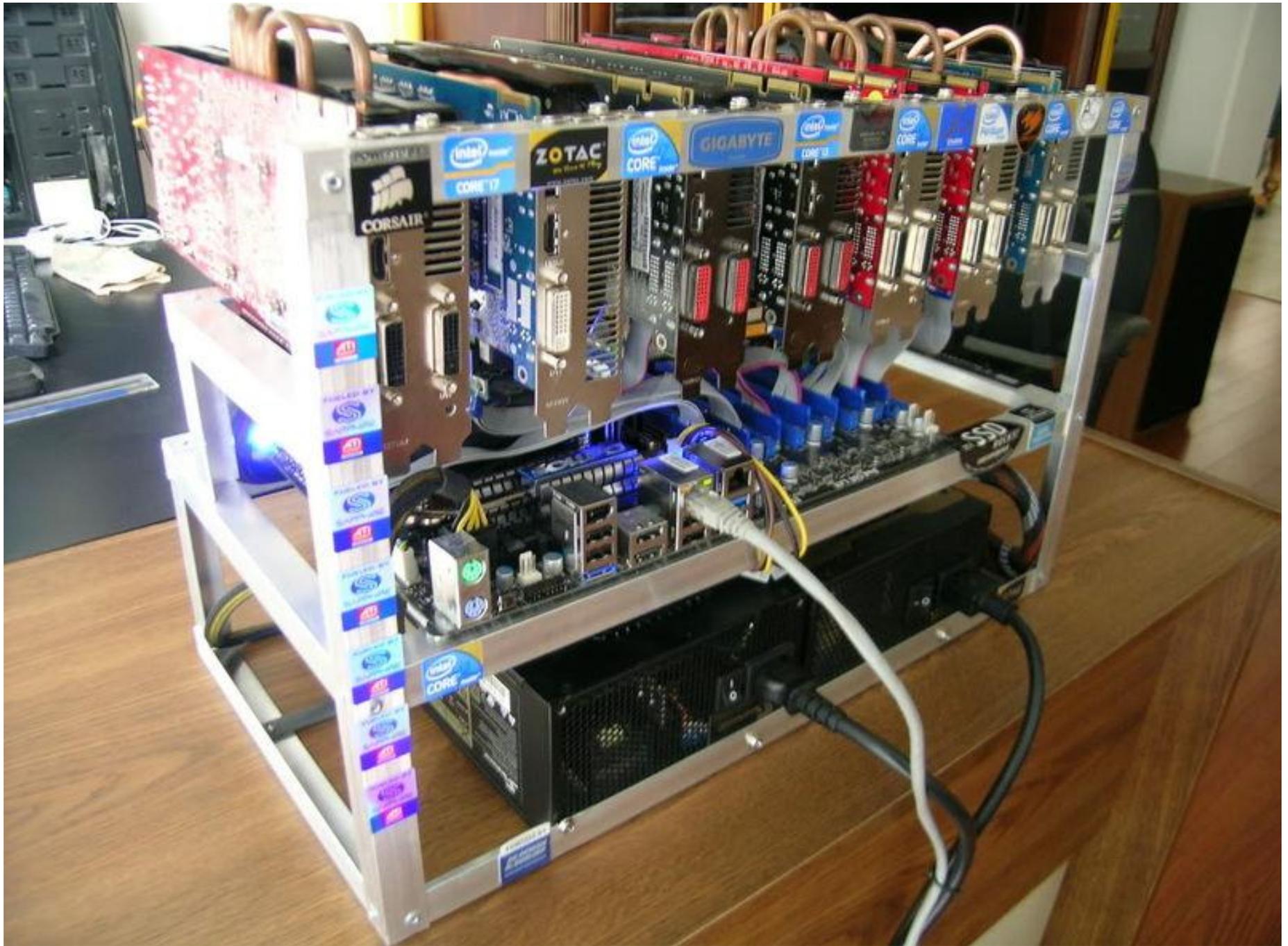
- [Сертификат открытого ключа](#)



# Биткойны

- Сатоши Накамото, 2008 г.
- Биткойн
  - сатоши
  - 1 сатоши = 0.00000001 BTC
- блокчейн (*blockchain*)
- кошелёк (*wallet*)
  - адрес
    - 1Jhbck6ziWRmQBp67GVDgLSJ9eFF5xNXgB
- подтверждение транзакции (*confirmation*)
- вознаграждение за транзакцию (*transaction fee*)
- майнинг
  - сложность майнинга (*mining difficulty*)
  - хэшрейт (*hash rate*)





# БИТКОЙНЫ

## Плюсы

- Нет инфляции
- Анонимность и приватность
- Децентрализованность
- Высокая скорость
- Публичность передвижения
- Не требуется регистрация
- Сверхмалые транзакции
- Требуется только наличие Сети

## Минусы

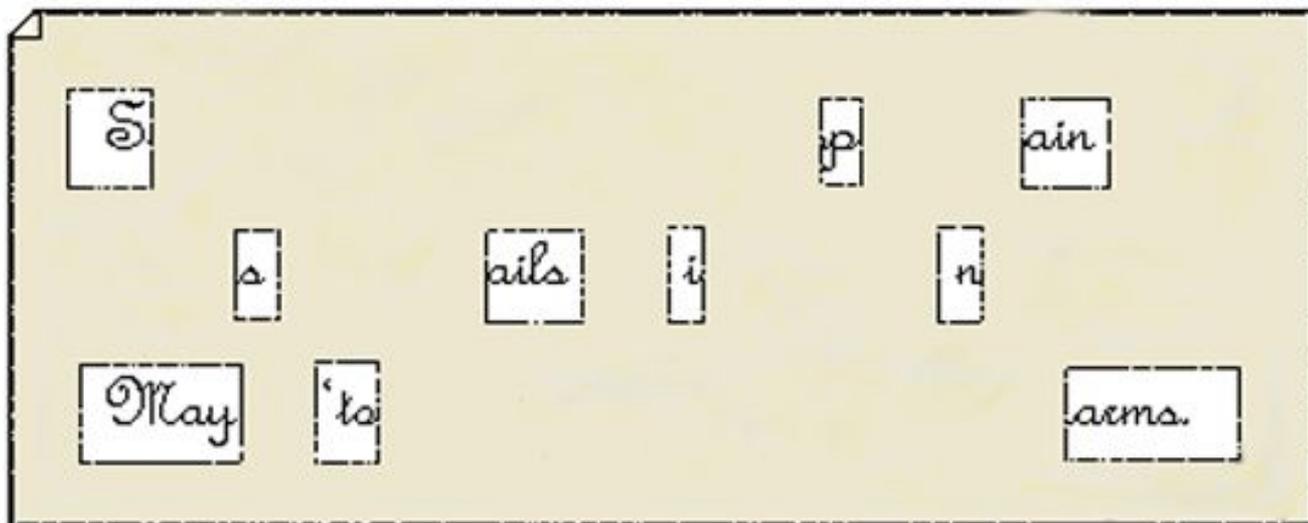
- Легко потерять
- Потенциальная уязвимость
- Нестабильный курс
- Большой размер базы транзакций
- Потенциальная нелегальность ИРЛ

# Стеганография

- Голова раба
- [RarJpeg](#)
- [RubberhoseFS](#)

# Решётка Кардано

Sir John regards you well and speaks again that  
all as rightly 'wails him is yours now and ever.  
May he 'tone for past d'lays with many charms.



- **Текст записки:**  
*Сэр Джон высоко ценит Вас и снова повторяет, что все, что доступно ему, теперь ваше, навсегда. Может ли он заслужить прощение за свои прежние промедления посредством своего обаяния.*
- **Шифрованное послание:**  
*В мае Испания направит свои корабли на войну.*

# Взлом программ

- Реверсивный инжиниринг
  - Грязный хак
  - Замена библиотеки
  - Генератор паролей
  - Дыры
  - Сервер паролей
- Защита от взлома
  - Шифрование и упаковка кода
    - Полиморфизм
  - Обфускация кода
  - Защита от отладки
  - Вынос проверки в Интернет

# Трояны-шифровальщики

- это очень, очень плохо.

# Расшифровка генома

- Гены
  - Экзоны
  - Интроны
- Повторы
  - тандемные повторы
  - диспергированные повторы
- Транспозоны
  - ретротранспозоны
  - ДНК транспозоны
- Псевдогены

# Ещё интересное

- Поросычья латынь

Isthay isay anay examplay ofay Oghay  
Atinlay. Asay ouyay ancaу eesay, it'say  
illysay, utbay otslay ofay unfay orfay  
ildrenchay.

- Вымершие и тайные языки

# Маньяк Зодиак

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
A	△	▣	P	/	Z	/	U	B	▣	Ж	O	R	π	ϣ	X	π	B
B	W	V	+	Э	G	Y	F	⊙	△	H	P	▣	K	Ю	Q	Y	Э
C	M	J	Y	Λ	U	I	K	△	Q	T	L	N	Q	Y	D	●	⊖
D	S	Φ	/	△	■	B	P	O	R	A	U	▣	F	R	L	Q	E
E	K	Λ	L	M	Z	J	Q	Я	\	ϣ	F	H	V	W	Э	▲	Y
F	▣	+	Q	G	D	△	K	I	⊖	⊙	Q	X	▲	●	⊕	S	Φ
G	R	N	L	Ю	Y	E	J	O	▲	Q	G	B	T	Q	S	■	B
H	L	D	/	P	■	B	▣	X	Q	E	H	M	U	Λ	R	R	К

- Крипτος

EMUFPHZLRFAXYUSDJKZLDKRNSHGNFIVJ  
YQTQUXQBQVYUVLLTREVJYQTMKYRDMFD  
VFPJUDEEHZWETZYVGWHKKQETGFQJNCE  
GGWHKK?DQMCQPFQZDQMMIAGPFXHQRLLG  
TIMVMZJANQLVKQEDAGDVFRPJUNGEUNA  
QZGZLECGYUXUEENJTBQLBQCRTBJDFHRR  
YIZETKZEMVDUFKSJHKFWHUKUWQLSZFTI  
HHDDDUVH?DWKBFUFPWNTDFIYCUQZERE  
EVLDFEZMOQQJLTTUGSYQPFEUNLAVIDX  
FLGGTEZ?FKZBSFDQVGOGIPUFXHHDRKF  
FHQNTGUAECNUVPDJMQCLQUMUNEDFQ  
ELZZVRRGKFFVOEEXBDMVPNFQXEZLGRE  
DNQFMPNZGLFLPMRJQYALMGNUVPDXVKP  
DQUMEBEDMHDAFMJGZNUPLGEWJLLAETG



•