



## Как договориться при всех, чтобы никто не понял

*Шифрование с открытым ключом – приём, который кажется невозможным, пока не разберёшь его на красках*



Техника · 13–17 лет · 14 минут

Две тысячи лет шифрование требовало, чтобы стороны заранее встретились и договорились о ключе. В 1976 году показали, что это необязательно: двое могут при всех, на глазах у подслушивающего, прийти к общему секрету, которого он не узнает. На этом стоит весь интернет.

## Задача, которая кажется невозможной

Сформулируем строго, потому что в формулировке вся соль.

Двое хотят договориться о секретном числе. Они никогда раньше не встречались и не могут встретиться. Весь их разговор слышит третий — целиком, без пропусков, каждое слово. Третий записывает всё и никуда не спешит.

Нужно, чтобы в конце разговора у двоих было общее число, а у третьего его не было.

Первая реакция нормального человека: это невозможно. Всё, что сказал один, слышал и другой, и третий. Откуда у двоих возьмётся то, чего нет у третьего, если сведения у всех одинаковые?

Тем не менее это возможно, задача решена в 1976 году, и решение используется прямо сейчас — каждый раз, когда ты открываешь сайт с замочком в адресной строке.

## Как было раньше

Чтобы оценить масштаб, посмотрим на предысторию.

Две тысячи лет шифрование устроено одинаково: есть секретный ключ, известный обеим сторонам. Шифруют им же, расшифровывают им же. Юлий Цезарь сдвигал буквы на три позиции, и его полководцы знали, что на три.

Отсюда главная головная боль всей истории тайнописи — **распространение ключей**. Чтобы переписываться тайно, надо сначала передать ключ, и передать его тайно. Курьером, при личной встрече, заранее.

Для армии это решаемо: ключи развозят фельдъегеря. Для интернета — нет. Ты заходишь на сайт, который никогда не видел, с которым не договаривался, и должен немедленно установить защищённую связь. Никакого курьера не будет.

Именно эта задача и казалась нерешаемой в принципе.

## Разберём на красках

Решение проще всего понять на образе, который придумали сами авторы.



*Смешать краски легко, разделить обратно — нет*

Есть свойство, на котором всё держится: **смешать две краски легко, разделить смесь обратно — практически невозможно**. Глядя на зелёную банку, нельзя сказать, из какого именно жёлтого и какого именно синего её сделали.

Теперь сама процедура. Пусть двое — назовём их Аня и Боря, а подслушивает Витя.

**Шаг 1.** Аня громко, при всех, объявляет: берём за общую краску жёлтую. Витя это слышит. Пусть слышит.

**Шаг 2.** Аня втайне выбирает свою краску — скажем, красную. Никому не говорит. Боря втайне выбирает свою — синюю. Тоже никому.

**Шаг 3.** Аня смешивает общую жёлтую со своей красной, получает оранжевую и **открыто** отправляет банку оранжевой краски Боре. Витя видит оранжевую. Боря смешивает жёлтую со своей синей, получает зелёную и открыто отправляет Ане. Витя видит зелёную.

**Шаг 4.** Аня берёт полученную от Бори зелёную и подмешивает туда свою тайную красную. Боря берёт оранжевую и подмешивает свою тайную синюю.

И вот итог. У обоих получилась смесь из одних и тех же трёх красок: жёлтой, красной и синей. **Одинаковый цвет.** Это и есть общий секрет.

Что есть у Вити? Жёлтая, оранжевая и зелёная. Чтобы получить нужный цвет, ему не хватает либо красной, либо синей — а их никто никогда не передавал. Выделить красную из оранжевой он не может: смесь не разделяется.

Заметь изящество: секрет не передавался. Он **возник** у обоих независимо, из того, что каждый добавил своё.

#### Односторонняя функция

Действие, которое легко выполнить в одну сторону и практически невозможно обратить. Смешать краски — легко, разделить — нет. Перемножить два больших простых числа — секунда; разложить их произведение обратно на множители — задача, на которой ломаются суперкомпьютеры. Вся современная криптография стоит на существовании таких действий. Любопытно, что строго доказать существование односторонних функций до сих пор не удалось: мы пользуемся тем, во что очень обоснованно верим.

## Что стоит вместо красок

В настоящем протоколе вместо смешивания красок — возведение в степень с остатком от деления.

Идея та же. Легко: взять число, возвести в большую степень, поделить на простое число и оставить остаток. Трудно: по остатку восстановить, в какую степень возводили. Эта обратная задача называется дискретным логарифмом, и для больших чисел решения за разумное время не найдено.

Протокол называли по именам авторов — Диффи и Хеллман, 1976 год. Историческая справка, которую стоит знать: почти то же самое несколькими годами раньше придумали в британской разведке, но работа была засекречена и опубликована лишь в 1997-м. Открытие, сделанное в тайне, не изменило мир; сделанное открыто — изменило.

## Второй приём: замок без ключа

Из той же идеи вырос ещё один механизм, ещё более странный.



*Замок раздают всем, ключ не отдают никому*

У каждого есть **пара**: открытый ключ и закрытый. Открытый раздают всем желающим, публикуют, вешают на сайте. Закрытый не показывают никому.

Работает это так: зашифрованное открытым ключом расшифровывается только закрытым.

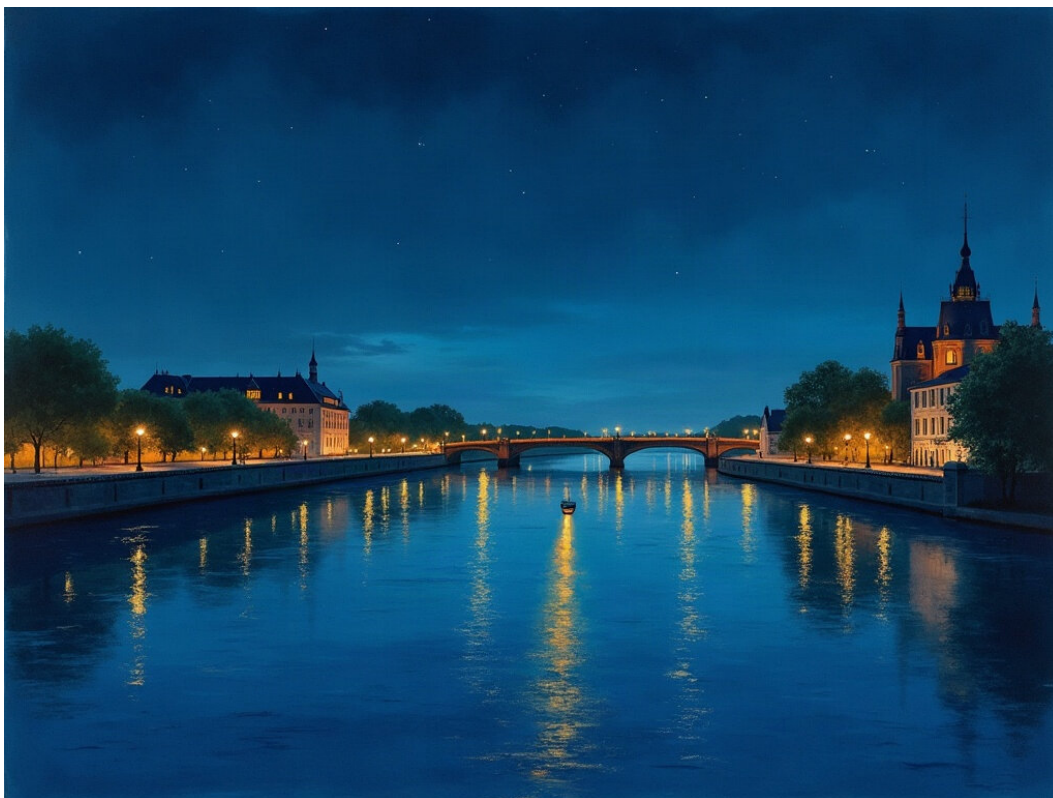
Образ понятный. Открытый ключ — это открытый висячий замок, который ты раздаёшь всем. Любой может положить письмо в коробку и защёлкнуть твой замок. После щелчка открыть коробку не может даже тот, кто её закрыл. Ключ есть только у тебя.

И у этого есть зеркальное применение, не менее важное. Если ты зашифруешь что-то своим **закрытым** ключом, расшифровать сможет любой обладатель открытого. Тайны никакой — зато доказано, что сообщение от тебя: больше ни у кого нет закрытого ключа.

Это называется электронной подписью, и на ней держатся обновления программ, банковские операции и вообще всё, где важно не скрыть, а удостоверить.

## Где здесь слабое место

Теперь честно о том, что обычно опускают.



*Каждое защищённое соединение начинается с такого обмена*

Описанный обмен защищает от **подслушивания**, но не от **подмены**. Представь, что Витя не просто слушает, а сидит посередине и пересылает сообщения. Аня думает, что говорит с Борей, а говорит с Витей. Боря думает то же самое. Витя договаривается с каждым по отдельности и читает всё.

Математика тут не помогает: с точки зрения протокола обмен прошёл безупречно.

Задача решается иначе — **удостоверением личности**. Должен существовать кто-то, кому обе стороны заранее доверяют и кто подтвердит: этот открытый ключ действительно принадлежит тому сайту. Такие поручители называются удостоверяющими центрами, их список защит в твой браузер, и именно их подпись проверяется, когда появляется замочек.

Заметь, во что упёрлись. Полностью избавиться от предварительной договорённости не вышло: её вынесли на уровень выше. Мы больше не обязаны заранее договариваться с каждым собеседником — но обязаны заранее доверять нескольким поручителям.

И это не формальность. Если поручителя взломают или заставят выдать ложное подтверждение, вся конструкция рухнет — причём незаметно для пользователя. Самое слабое место современной защищённой связи не в математике, а здесь.

#### Должны ли быть у государства ключи от переписки

**Должны.** Преступники пользуются теми же средствами, что и все. Если переписка недоступна никому, расследование тяжких преступлений упирается в стену. Разумный компромисс — оставить возможность доступа по решению суда, как с обыском в жилище.

**Не должны, потому что технически это невозможно избирательно.** «Дверь только для хороших» не существует: любая встроенная возможность доступа — это уязвимость, и рано или поздно ею воспользуется не тот, для кого она задумывалась. Ослабляя защиту для преступников, ослабляешь её для всех, включая больницы и энергосети.

Спор этот идёт с девяностых годов, называется «криптовойнами» и не закончен. Заметь особенность: одна сторона говорит о целях, другая — о технической осуществимости, и поэтому они плохо слышат друг друга.

## Почему это стоит знать

Несколько мыслей, выходящих за рамки техники.

**Невозможное иногда только кажется.** Задача об общем секрете при свидетелях выглядела логически безнадёжной — пока не заметили, что секрет не обязан передаваться, он может возникнуть.

**Асимметрия — мощная идея.** Всё строится на том, что действие в одну сторону дешёвое, а в обратную дорогое. Это встречается всюду: разбить легче, чем починить, соврать легче, чем проверить, сказать легче, чем сделать.

**Цепь доверия всегда где-то упирается в людей.** Математика безупречна ровно до того места, где начинается вопрос «а кому мы верим». Дальше — организации, законы и человеческая порядочность, и это самое хрупкое звено любой системы.

## Что именно происходит, когда ты открываешь сайт

Полезно увидеть, где всё описанное встречается в обычной жизни. За тот момент, пока страница загружается, происходит примерно следующее.

**Приветствие.** Браузер сообщает серверу, какие способы шифрования он умеет. Сервер выбирает общий и отвечает.

**Предъявление удостоверения.** Сервер присылает свой сертификат: открытый ключ плюс подпись поручителя, утверждающая, что этот ключ принадлежит именно этому домену. Браузер проверяет подпись по списку поручителей, зашитому у него заранее, и заодно смотрит срок годности и не отозван ли сертификат.

**Обмен по Диффи — Хеллману.** Стороны проделывают ровно то, что мы разбирали на красках, и получают общий секрет, которого нет ни у кого, кто слушал.

**Переход на быстрый шифр.** Дальше вся переписка идёт обычным симметричным шифром на этом общем секрете. Так делают потому, что асимметричные операции медленные: их используют только чтобы договориться, а сам разговор шифруют быстрым способом.

Весь обмен занимает доли секунды и повторяется при каждом новом соединении.

И ещё одна деталь, которую стоит знать. Современные версии протокола устроены так, что даже если завтра украдут закрытый ключ сервера, вчерашнюю записанную переписку прочесть не удастся: для каждого сеанса берутся новые одноразовые значения. Свойство называют прямой секретностью, и оно прямо отвечает на приём «записать сейчас, расшифровать потом» — который, между прочим, применяют вполне всерьёз в расчёте на будущие компьютеры.

## Главное в трёх строчках

- Двое могут получить общий секрет при полностью открытом разговоре: секрет не передаётся, а возникает у каждого независимо — как одинаковый цвет из одинакового набора красок.
- Всё держится на односторонних действиях: смешать легко, разделить нельзя; перемножить легко, разложить обратно — нет.
- Математика защищает от подслушивания, но не от подмены собеседника, поэтому в основании всё равно лежит доверие к поручителям — и это самое слабое звено.

### Вопросы для размышления

- Почему Витя, слышавший весь разговор целиком, не может повторить те же действия и получить тот же цвет?
- Электронная подпись ничего не скрывает. Зачем тогда шифровать сообщение своим закрытым ключом?
- Если в основании всё равно лежит доверие к поручителям, в чём тогда выигрыш по сравнению со старым способом с курьером и ключом?