

12+

СЕРГЕЙ КИРНИЦКИЙ

Криптография без иллюзий

ОТ СТЕНЫ НЕДОВЕРИЯ К ТРЁМ
ОПОРАМ



Сергей Кирницкий

Криптография без

иллюзий. От стены

недоверия к трём опорам

<https://litres.ru/74269844>

ISBN 9785007066129

Аннотация

Можно ли построить уверенность, начав с нуля? Философы называют это трилеммой обоснования; инженеры сталкиваются с ней каждый раз, когда два незнакомца пытаются договориться через враждебную сеть. Это книга о том, что криптография не создаёт доверие — она лишь перевозит и размножает крупницу, заложенную вне математики. У этой крупницы ровно три источника: сверить лично, довериться авторитету, опереться на общее прошлое. Понять это — значит перестать ждать чуда и начать выбирать осознанно.

Содержание

Введение. Письмо незнакомцу	5
Часть I. Обещание	9
Глава 1. Замок без ключа, ключ без замка	11
1.1. Почтовый ящик	12
1.2. Что обещает асимметрия	14
1.3. Подпись и шифрование — два глагола	17
1.4. Соблазн	20
Глава 2. Человек посередине	24
2.1. Мэллори, владеющая каналом	25
2.2. Письмо доходит «правильно»	28
2.3. Аутентифицировать вход, не выход	31
2.4. Первое появление Стены	34
Часть II. Стена	38
Глава 3. Нельзя получить нечто из ничего	40
3.1. Аутентификация из нуля невозможна	41
3.2. Трилемма Мюнхгаузена	44
Конец ознакомительного фрагмента.	45

Криптография без иллюзий

От стены недоверия к трём опорам

Сергей Кирницкий

Иллюстрация на обложке Created with Grok

© Сергей Кирницкий, 2026

ISBN 978-5-0070-6612-9

Создано в интеллектуальной издательской системе Ridero

Введение. Письмо незнакомцу

Каждый день ты делаешь то, что ещё сто лет назад сочли бы либо фокусом, либо безумием. Набираешь номер карты в поле на чужом сайте и нажимаешь «оплатить». Пишешь пароль, который не знает никто на свете, и отправляешь его — куда-то. Говоришь близкому человеку что-то, предназначенное только ему, хотя между вами лежат тысячи километров провода, стекла и чужих машин, о существовании которых ты даже не подозреваешь.

И это работает. Секрет доходит. Не к соседу, не к случайному прохожему в цифровой толпе, а именно туда, куда ты целился, — к человеку или к службе, которых ты чаще всего и в лицо-то никогда не видел. Ты делаешь это между делом, не задерживая дыхания, как открывают кран: повернул — потекло.

Остановись на секунду и посмотри на это глазами того, кому такое показали впервые. Ты вручаешь запечатанное письмо толпе — толпе, в которой не знаешь никого. Ты не знаешь, кто примет конверт и передаст дальше, кто стоит на перекрёстках, в чьих руках он побывает по дороге. А рук этих — не одна и не две: твоё письмо перелетает из города в город, от посредника к посреднику, и ни одного из них ты не выбирал и ни одному не давал разрешения. Толпа кишит чужими, и любой из них держит письмо хотя бы мгновение — успел

бы и вскрыть, и подменить, и просто прочесть. И всё же ты почему-то уверен, что распечатает его один-единственный адресат — тот, кому оно написано.

Как это вообще возможно?

Вопрос звучит наивно — так наивно, что взрослый человек стесняется его задать вслух. Есть же шифрование; про него все слышали; на замочек в углу экрана можно ткнуть пальцем; значит, всё в порядке. Но наивные вопросы обычно и есть настоящие — те, мимо которых мы привыкли проходить, потому что кто-то однажды сказал, что тут всё решено. За спокойным словом «шифрование» прячется не одна загадка, а несколько, и они вложены друг в друга, как коробки. Снаружи — «как спрятать письмо от чужих глаз». У этой загадки есть красивый ответ, и мы к нему придём; он и вправду похож на фокус. Но чуть глубже лежит другая, и она куда упрямее: откуда ты знаешь, что письмо уходит именно тому, кому ты его пишешь? Что запечатанный конверт, который толпа несёт куда-то в темноту, ляжет в руки твоего адресата, а не того, кто лишь назвался им?

Ведь ты никогда его не видел. Не слышал его голоса. Между вами — только линия, по которой бегут сигналы, и на дальнем её конце кто-то говорит: «это я». Почему ты веришь?

Вот с этого вопроса всё и начнётся. Не «надёжен ли замок» — замки давно надёжны, — а «твой ли это замок вообще». Обещаю сразу и честно: к последней странице ты не

получишь на него ответа «да» или «нет». Больше того — сам вопрос к тому времени изменится. Он не растворится в тумане, а станет точнее: из простого «можно ли доверять незнакомцу?» вырастет другой, на который уже можно опереться и с которым можно жить. Пока я не скажу, во что именно он превратится, — иначе испорчу дорогу. А дорога здесь важнее пункта назначения. Мы пройдем её так, как проходит всякий, кто однажды всерьёз задумался: от простого удивления к неудобной правде и дальше — к правде, которая освобождает.

Одно слово всё же назову заранее, потому что оно простое и понадобится нам с самого начала. Опора. Когда ты веришь, что на том конце линии — именно твой человек, эта вера на чём-то держится. Где-то под ней есть опора — что-то, что ты когда-то увидел своими глазами, услышал своими ушами, получил из рук в руки или просто однажды решил считать надёжным. Достаточно почувствовать: у всякого доверия под ногами есть опора, даже когда ты её не замечаешь, — как не замечаешь пола, пока он тебя держит.

И всё же ты пишешь. Каждый день, десятки раз, ты доверяешь свои секреты незнакомцам за стеклом экрана — и почти всегда оказываешься прав. Это не глупость и не слепая удача. Люди отправляли важное в руки посыльных, гонцов и почтмейстеров задолго до всякой электроники и чаще всего не ошибались — не потому, что мир был безопасен, а потому, что вера их на чём-то стояла. Стоит на чём-то и твоя.

Возьми же в руку это письмо — к тому, кого ты никогда не видел. Мы отправим его в путь. И по дороге, шаг за шагом, разберёмся, на чём держится тихая, привычная вера, что оно дойдёт.

Часть I. Обещание

...контакт, который может состояться между любыми двумя людьми — независимо от того, общались ли они когда-либо прежде.

— Уитфилд Диффи, Мартин Хеллман. «Новые направления в криптографии» (1976)

Кажется, что безопасность — это вопрос удачно выбранного инструмента. Найди достаточно хитрый замок — и любой разговор, даже с человеком, которого ты никогда не видел, станет непроницаем для чужих. В этой вере есть своя логика: вся многовековая история секретной переписки — это история замков, которые становились всё изощрённее, пока их всё равно не вскрывали. Асимметрия, с которой начинается современная криптография, поначалу встает в этот же ряд — просто очередной замок, самый хитрый из всех, почти магия.

Но у неё есть свойство, которого не было ни у одного замка прежде: её можно показать всем и ничего при этом не отдать. Замок, выставленный на площади, — и ключ, который остаётся только у тебя. Из этого свойства растут сразу две вещи, и спутать их опасно: умение спрятать письмо от посторонних и умение доказать, чья рука его написала. Прятать и удостоверять — не одно и то же, хотя фокус проделывает и то, и другое как будто одним движением

руки.

И всё же за самой красивой версией этого фокуса остаётся вопрос, который он не закрывает. Замок можно выставить на всеобщее обозрение — но откуда тот, кто собирается им воспользоваться, знает, что замок и вправду твой? Этот вопрос пока полежит в стороне. Дорога к нему начинается с предмета, знакомого до скуки: с почтового ящика, в щель которого письмо бросает кто угодно, а вынуть его может только владелец.

Глава 1. Замок без ключа, ключ без замка

Тысячи лет тайна держалась на общем секрете. Двое, желавшие говорить так, чтобы третий не понял, должны были сперва сойтись на чём-то, известном только им, — слове, шифре, уговоре о том, как переставлять буквы. И всякий раз всё упиралось в одну и ту же заминку: этот общий секрет сначала надо было как-то передать. Передать до разговора, по какому-то каналу, который сам ещё ничем не защищён, — курьером, при встрече, шёпотом на ухо. Замок и ключ были, по сути, одним предметом: кто умел запереть, тот умел и отпереть, а потому ключ приходилось делить на двоих.

Идея, что запирать и отпирать могут разные ключи, звучит поначалу как трюк с двойным дном — будто где-то припрятан подвох. Если посторонний способен закрыть замок, почему тот же посторонний не способен его открыть? И всё же именно на этой несимметричности держится разговор с незнакомцем. Прежде чем разбирать её как устройство, стоит один раз пережить её на предмете, который висит в каждом подъезде.

1.1. Почтовый ящик

Обычный почтовый ящик в подъезде — вещь, которую ты видел тысячу раз. Металлическая дверца, за ней полость, а в дверце прорезана узкая щель. В эту щель письмо может опустить кто угодно — сосед, почтальон, случайный человек, заглянувший с улицы. Ему не нужно ни разрешения, ни ключа: щель для того и сделана, чтобы принимать. А открыть дверцу и достать накопившееся может только один — тот, у кого ключ от неё. Щель работает в одну сторону. Опустить письмо — свободно; вынуть — только хозяину.

В этой обыденности спрятана большая идея, и на ней стоит задержаться чуть дольше, чем она просит. Смотри: чтобы бросить письмо, тебе не нужно ничего секретного. Ты не должен знать, есть ли у владельца ключ, какой он и где он его держит. Тебе довольно найти щель. Щель не спрашивает, кто ты: она не отличает хозяина от чужого, званого от незваного — принимает любое письмо от любого. Владеть ящиком и владеть ключом от него — разные вещи, и разведены они намеренно: тот, кто пользуется щелью, и тот, кто отпирает дверцу, могут не знать друг друга в лицо и никогда не встретиться.

Вот это и есть асимметрия — раньше, чем мы произнесли слово. У ящика словно два разных «ключа» с разными правами. Один общедоступен — это сама щель, ею пользуются

все подряд. Другой единственный — это ключ от дверцы, он у хозяина. И, что здесь важнее всего, они не две половины одного секрета, поделённого поровну, а пара с несимметричными правами: то, чем *кладут*, и то, чем *достают*. Именно это веками и казалось невозможным. Раз замок заперт, рассуждали все, — значит, есть тот, кто умеет его отпереть; и чтобы позволить кому-то запереть, приходилось выдать ему заодно и способ отпереть. Здесь запирающий и отпирающий разведены начисто: сколько ни заглядывай в щель, открыть её дверцу нельзя.

Чтобы почувствовать, до чего это устройство необычно, оглядись по сторонам. Почти все замки вокруг тебя устроены наоборот. Дверь в квартиру: один и тот же ключ и запирает, и отпирает, — а потому копию этого ключа ты отдаёшь только тем, кому доверяешь целиком, и сам миг передачи копии всегда чуть тревожен. Навесной замок на гараже, замочек на дневнике, дверца сейфа — та же история: кто может закрыть, тот может и открыть. Симметрия здесь настолько привычна, что её перестали замечать. И на этом ровном фоне почтовый ящик делает нечто тихо-странное: из обыденных предметов он едва ли не единственный уже развёл два права, которые прочие держат слитно, в одном ключе.

А теперь сделай следующий шаг сам — он напрашивается. Раз щель нужна каждому, кто захочет тебе написать, её место снаружи, на виду. Общедоступную половину не прячут; напротив, чем она заметнее, тем лучше делает свою ра-

боту. В этом смысле она похожа вовсе не на секрет, а на адрес. Адрес на конверте не берегут как тайну — его сообщают всем, от кого ждут вестей; он затем и существует, чтобы его знали. Открытая половина пары — вещь того же рода: её назначение в том, чтобы быть известной. Не «утаить», а «объявить».

В этом и странность: спрятанный адрес — бесполезный адрес; чем больше людей его знают, тем лучше он служит владельцу. Тайна, которую выгодно разглашать, звучит как противоречие в терминах — и всё же ровно так ведёт себя открытая половина пары.

Пока запомним только это простое узнавание — оно ещё пригодится. Та часть пары, которой пользуются другие, — не тайна, а адрес, и держать её естественно на виду. Но заметь, за чем именно мы сейчас проследили: за одним-единственным умением ящика — прятать брошенное в него от чужих глаз. У самой асимметрии есть и второе умение, совсем другого сорта; и спутать эти два умения — первая из ошибок, которых стоит остерегаться.

1.2. Что обещает асимметрия

Второе умение асимметрии живёт в другом предмете. Ящик прячет — это вся его забота: что опустили в щель, то и укрыто от посторонних глаз, и совершенно неважно, кто опустил. Но есть нужда прямо противоположная: не спрятать

написанное, а, наоборот, оставить его открытым для всех и при этом намертво связать с тем, кто его написал. Для этого служит не ящик, а печать.

Вспомни сургучную печать на старом письме. Она не прячет ни строчки — письмо под ней прочтёт всякий, кому хватит духу сломать сургуч. Печать делает другое: пока она цела, она свидетельствует, чья рука закрыла конверт и что с тех пор его никто не вскрывал. Ящик отвечает на вопрос «кто это увидит?»; печать — на вопрос «от кого это пришло?». Два предмета, две разные работы, и смешивать их так же нелепо, как ждать, что дверной замок сам расскажет тебе, кто ломился в дверь, пока тебя не было.

Ценность печати вовсе не в том, что она что-то скрывает, — а в том, что её нельзя подделать и что она привязана к одному человеку. Перстень с гербом оставляет оттиск, который видит всякий; но оставить такой оттиск может лишь владелец перстня. Оттиск открыт для глаз и закрыт для подделки: любой прочтёт, чей он, и никто не проставит его от чужого имени. Ровно этого мы и хотим от подлинности — чтобы происхождение письма было на виду, а присвоить его чужому было невозможно.

Назовём обе услуги точно — дальше всё будет держаться на этом различии. Первая услуга — тайна: содержимое укрыто от чужих. Вторая — подлинность: удостоверено, чья рука за письмом стоит. Это не два положения одного тумблера, не «режим А» и «режим Б» одной и той же кнопки.

Это два разных обещания, которые асимметрия раздаёт порознь, и каждое можно получить без другого.

Здесь легко оступиться, потому что в обиходе обе услуги сливаются в одно смутное слово — будто есть единая кнопка «сделать безопасно», и, нажав её, ты получаешь всё сразу. Говорят «тут всё зашифровано, значит, надёжно» — и в этом коротком «надёжно» незаметно просят сразу двух разных вещей: чтобы чужой не прочёл и чтобы свой оказался и вправду своим. Просят двух, а проверяют, в лучшем случае, одно.

Письмо можно спрятать безупречно — и всё же не знать, от кого оно. Вообрази послание, запечатанное так плотно, что ни одна живая душа, кроме адресата, не разберёт ни слова: тайна идеальна. Но идеальная тайна ни слова не говорит о том, чья рука это письмо составила; под непроницаемой обёрткой может сидеть кто угодно. Письмо, запечатанное от всех глаз и подписанное «твой навсегда», трогает нежностью строк — а чья это рука, нежность не доказывает ничем. Спрятать — не значит удостоверить.

И наоборот. Письмо можно удостоверить безупречно — и не прятать при этом вовсе. Публичное объявление, скреплённое подписью, которую нельзя подделать, читают все желающие: тут нет ни крупицы тайны, зато в авторстве нельзя усомниться. Так работает манифест, прибитый к дверям на виду у города, — важно не спрятать текст, а не дать отпереться от подписи под ним. Удостоверить — не значит спрятать.

Отсюда следствие простое, но неуютное: провал одной услуги не лечится успехом другой. Сколько ни наращивай тайну, она не прибавит ни капли уверенности в том, кто перед тобой; сколько ни укрепляй подлинность, она не укроет от чужих глаз ни строчки. Перед нами две отдельные оси, и двигаться по одной можно, не сместившись по другой ни на шаг. Идеально спрятанное письмо бывает от самозванца; идеально подписанное прочитано всеми.

Запомни это различие — это развилка, к которой мы ещё вернёмся не раз. Почти всё, что случится с нами дальше, случится оттого, что две услуги слишком легко принять за одну: успех в одной обманчиво сходит за успех во всём. Пока довольно того, что ты видишь их порознь — ящик, который прячет, и печать, которая удостоверяет: два предмета, а не один.

1.3. Подпись и шифрование — два глагола

Услугу удобно обратить в глагол — тогда сразу видно, что у неё есть дополнение, предмет, на который она направлена. Тайна — это глагол «спрятать»: спрятать *что*. Подлинность — глагол «доказать»: доказать *кто*. Разные глаголы правят разными дополнениями, и подставить одно на место другого нельзя — как нельзя спрятать «кто» или доказать «что»: выйдет бессмыслица уже на уровне грамматики, ещё до вся-

кой техники.

Эта грамматика проступает и в мастерской, там, где абстракция обростает конкретикой. Открой набор инструментов, которыми сегодня подписывают и шифруют, и встретишь два ключа с почти близнецовыми именами: ed25519 и X25519. Они выросли из одной математической семьи — общий предок, общая порода, — и всё же тебе твёрдо скажут: этот, ed25519, — чтобы подписывать; тот, X25519, — чтобы двоим сойтись на общей тайне, под которой потом прячут переписку. Их держат порознь и дают им разные имена вовсе не из педантизма. Один делает глагол «доказать»: скрепляет письмо подписью, которую никто другой не оставит. Другой делает работу, ведущую к «спрятать»: помогает двоим условиться о секрете, невидимом для третьего. Одна кровь — противоположные ремёсла.

Близнецовость имён — ловушка для глаза, и попадаются в неё постоянно. Но инструмент попасться не даёт: подсунь ключ не к тому глаголу — и всё встанет, потому что каждый ключ умеет ровно своё и наотрез отказывается делать чужое. Разведение, которое на словах выглядит придиркой, в работе оказывается жёстким: два ключа не взаимозаменяемы, как не взаимозаменяемы «доказать» и «спрятать».

И чем ближе сходство, тем слаще соблазн его не заметить. Именно родственность этих ключей и подталкивает обойтись одним: раз они так похожи, рассуждает уставший человек, к чему держать оба? Ловушка тем и коварна, что стоит

на подлинном сходстве, а не на обмане: различие тонко, а родство очевидно.

Вот тут и караулит искушение срезать угол: «возьму один ключ, тот, которым подписываю, и в него же стану шифровать — меньше хозяйства». Мысль понятная — и совершенно ложная. Просить ключ подписи хранить тайну — категорическая ошибка: ошибка не в расчёте, а в самом роде вещи. Подпись доказывает *кто*; шифрование прячет *что*. Требовать от подписи, чтобы она ещё и прятала, — всё равно что требовать от сургучной печати, чтобы она заодно заклеила конверт: печать не для того сделана, у неё другое ремесло. Или возьми подпись под договором: весь её смысл в том, чтобы стоять на виду рядом с текстом, который она заверяет; попросить эту подпись сделать договор нечитаемым для других — значит не понять, зачем подпись вообще ставят. Она свидетельствует и не скрывает; заставить её скрывать нельзя ни нажимом, ни хитростью — можно только сломать само различие, на котором держится смысл обеих услуг.

И заметь тонкость: ключ подписи — совершенно исправный ключ, он безупречно делает своё дело. Ошибка не в ключе, а в глаголе, который ему навязали. Исправность инструмента не делает его пригодным для чужой работы; печать не становится клеем оттого, что она исправна. Различие тайны и подлинности, минуту назад казавшееся философской тонкостью, оборачивается вполне практическим запретом: два глагола не складываются в один, сколько ни хочется ужать

связку ключей до одного. И это лишь первый случай, где успех в одном глаголе легко принимают за безопасность в обоих; таких подмен впереди ещё немало, и почти каждая начинается ровно с этой — с молчаливой веры, что раз одно сделано хорошо, то и второе как-нибудь сделается само.

Теперь у тебя в руках весь механизм. Две услуги, разведённые по двум предметам; два глагола, разведённые по двум ключам; и в каждой паре — открытая половина, которую незачем стеречь: тайны в ней нет с самого начала. Инструмент понят до конца — со всей его силой и со всеми границами. И самое лёгкое, что напрашивается сделать с этой открытой половиной, лежит прямо под рукой.

1.4. Соблазн

Так сделай же этот лёгкий шаг. Раз открытая половина — не секрет, а адрес, значит, и хранить её незачем: опубликуй, выведи на самом видном месте, и любой, кто захочет написать тебе тайно, возьмёт её оттуда и напишет. Не нужно встречаться, не нужно шептать пароль на ухо, не нужно искать надёжного курьера и вздрагивать за него всю дорогу. Довольно один раз объявить свой адрес всему свету — и тайная переписка с кем угодно вдруг становится возможной.

Вспомни, чего это стоило раньше. Двое, желавшие говорить тайно, сперва добывали общий секрет: сходились на условленном слове, переписывали от руки одинаковые таб-

лицы шифра, заучивали порядок, в котором будут путать буквы. И всё это добро надо было ещё и вручить друг другу — в запечатанном пакете с оказией, при короткой встрече в условленном месте, через человека, которому оба соглашались верить. Пакет мог потеряться в пути, встреча — сорваться, память — подвести; обряд был так хлопотен и ненадёжен, что тайна выдыхалась ещё прежде, чем начаться. Секрет, чтобы сделаться общим, должен был сперва проехать по свету — и вся затея держалась на этой доставке.

Остановись на миг и почувствуй, что здесь только что случилось. Вся тяжесть, которую человечество веками волокло на плечах, — необходимость сперва как-то доставить секрет по пути, который сам ещё ничем не защищён, тот самый узел, о который спотыкались все до единого, — эта тяжесть будто испарилась. Секрет больше не надо возить. Да и возить-то нечего: то, что нужно другим, ты и так отдаёшь всем, а то, что нужно тебе, не отдаёшь никому и никуда не везёшь. Задача, казавшаяся вечной, решается не хитрым курьером и не замком покрепче, а простым отказом от самой доставки.

И до чего это красиво в своей простоте. Прежде, чтобы сказать что-то тайное незнакомцу на другом конце земли, ты был обязан завести с ним сперва общую тайну — а как заведёшь её с тем, кого в глаза не видел? Замкнутый круг, из которого не было выхода: чтобы говорить тайно, нужен общий секрет, а чтобы передать общий секрет, нужно уже уметь говорить тайно. Теперь выхода искать не приходится:

круг разомкнулся сам, стоило лишь перестать прятать то, что и не требовалось прятать. Публичность ключа — не досадная уступка, не слабость, за которую придётся расплачиваться; напротив, именно она и есть решение. Чем шире ты раздал свой адрес, тем большему числу людей открыл дорогу к себе — и ни на волос не убавил собственной безопасности, ведь отдал ты ровно то, что и создано для раздачи.

Раздавать его можно сколь угодно щедро. Печатай открытую половину на визитной карточке, вписывай в справочник, ставь в конце каждого письма, вывешивай хоть на дверях — любая копия ничем не хуже первой, ведь утекать тут нечему: то, что не было тайной, невозможно выдать. Один и тот же объявленный адрес служит разом всем — и первому встречному, и тысячному; а ты для тысячного не сделал ни на грош больше, чем для первого. Один-единственный жест — и дорога к тебе открыта целому свету, до каждого, кто когда-нибудь захочет тебе написать.

Читатель уже кивает — и правильно делает, ведь придраться не к чему. Вывод безупречен на каждом шаге: две услуги разведены, два глагола разведены, открытая половина затем и создана, чтобы быть открытой, — стало быть, открой её и живи спокойно. Есть особое облегчение в том, как трудная задача вдруг оказывается решённой — не с боем, не ценой изнурительного труда, а от одного смещения взгляда, после которого прежнее препятствие перестаёт быть препятствием. Мысль ложится под ноги твёрдой почвой; на ней хо-

чется выпрямиться во весь рост и оглядеть поле, которое ещё недавно казалось непроходимым. И отсюда, с этой высоты, видно далеко — а всё видимое говорит одно и то же: задача, мучившая столько поколений подряд, наконец закрыта. Закрыта чисто, без остатка, и притом почти даром.

Замок, который незачем прятать, незачем и охранять. Повесь его на виду — и цель твоего ящика открыта каждому, кто захочет написать тебе тайно; ящик стоит посреди города, дверца заперта, ключ при тебе, и это выглядит не уязвимостью, а самым решением. Тот, кто веками искал безопасный способ доставить секрет, вдруг обнаруживает, что доставлять больше нечего: он просто повесил свой замок на площади и стал ждать писем.

И только одно легонько царапает — даже не мысль, а её лёгкость. Тяжесть, которую волокли столько поколений, не может ведь взять и раствориться без следа — а она, похоже, растворилась, и вдобавок задаром. Слишком гладко. Но сколько ни ищи, изъян не находится: замок на виду, ключ при тебе, незнакомец пишет — и всё сходится, всё на своих местах. Читатель стоит на твёрдой почве и кивает; почва под ним кажется совершенно надёжной.

Глава 2. Человек посередине

Раз ключ публичный, самое страшное — что его узнают: так подсказывает осторожность, приученная веками прятать. Но узнать публичное — не беда по определению; на то оно и публичное. Ключ можно напечатать на визитке, выбить на памятнике, разослать всем подряд — и ничего не случится. Осторожность сторожит не ту дверь.

Опасность сидит там, куда взгляд не заглядывает, — не в том, что кто-то прочтёт открытый ключ, а в том, что кто-то встанет между тобой и собеседником и будет решать, какой ключ ты вообще увидишь. Не подслушать разговор, а владеть самим каналом, по которому он идёт. Подслушивающий бессилён изменить то, что течёт мимо него; хозяин канала меняет само течение — и в этом вся пропасть между ними. И самое неприятное: письмо, прошедшее через такие руки, приходит без единого следа — правильное, целое, именно такое, какого ждёшь. Проверять его на выходе бесполезно; проверять надо было на входе.

Труба, по которой течёт наш разговор, кому-то принадлежит. Вопрос не в том, чиста ли вода, а в том, чьи руки на кране.

2.1. Мэллори, владеющая каналом

Обычный образ врага — тот, кто прислонился ухом к стене. Он снаружи, он пассивен, он ловит то, что случайно протекает наружу; всё, что от него защищает, — сделать стену толще. С таким врагом криптография справляется играючи: запри содержимое покрепче, и подслушивать станет нечего. Именно этот образ и подсовывает осторожность, когда речь заходит про открытый ключ, — будто вся угроза в том, что кто-то его подсмолит.

Настоящий противник устроен иначе, и знакомство с ним стоит завести сразу, пока привычная картинка не успела прирасти намертво. Назовём противника по имени: Мэллори. Мэллори не прижимается к стене — стена принадлежит ей. Она не ловит то, что течёт по каналу; она решает, что по нему потечёт. Между Бобом, который хочет написать Алисе, и самой Алисой стоит не любопытное ухо, а хозяйка трубы — та, через чьи руки проходит каждое письмо и каждый ключ и которая вольна пропустить, задержать или подменить всё, что сочтёт нужным. Она не гостья на канале; канал — её дом.

Разница кажется мелкой, а меняет она всё. Пассивный враг работает с тем, что ему досталось; Мэллори выбирает, что достанется тебе. Ты думаешь, что держишь в руках ключ Алисы, — но между тобой и Алисой стоит Мэллори, и ты держишь ровно то, что она тебе протянула. Вся даль-

нейшая игра пойдёт против этого противника, а не против подслушивающего: каждая попытка отнять у хозяйки трубы её власть решать, что ты увидишь, будет кончаться одним и тем же — обнаружением, что власть эта никуда не делась, лишь переехала на этаж выше или спряталась поглубже. Пока в голове сидит подслушивающий, ни одна из настоящих трудностей не встанет в полный рост.

Канал — это не отвлечённая линия между двумя точками, а всё, через что письмо и ключ реально проходят по дороге к тебе: сеть, несущая биты, сервер, что их пересылает, справочник, куда ты полез за чужим ключом, программа, которую кто-то вручил тебе, чтобы этим ключом пользоваться. Любые руки на этом пути годятся на роль Мэллори. Ей незачем быть всемогущей и видеть всё сразу — довольно оказаться на одном-единственном отрезке между тобой и собеседником и распоряжаться тем, что через него проходит. Хозяйка трубы — не мифическая всесильная тень, а вполне земное место, где кто-то встал между вами двоими, — и всё, что ты видишь, проходит через его руки.

И вот тут наконец видно, куда на самом деле смотрела осторожность и почему промахнулась. Опубликовать ключ и вправду ничего не стоит: его открытость — не рана. Ключ, лежащий на виду у всех, ровно так же годен, как ключ, врученный из рук в руки; в самой публичности нет ни грана слабости. Слабость в другом, и она совсем не там, где её сторожили: открытость ключа не говорит ни слова о том, чей он.

Лежит ключ, подписанный именем Алисы, — но подпись под именем может вывести и Мэллори, и по виду ключа этого не различить. Трюк с публикацией сработал без осечки против того врага, для которого его придумали, — против подслушивающего. Против хозяйки трубы он не значит ничего.

Тут же стоит оговорить и то, чего Мэллори не делает. Она не садится ломать замок. Ни здесь, ни дальше в этой книге никто не вскроет шифр перебором, не подберёт ключ, не найдёт трещину в самой математике. Замок цел и держит честно — просто хозяйка трубы, вместо того чтобы биться о него лбом, тихо ставит на его место свой собственный, а твой убирает в карман. Ей незачем взламывать то, что можно обойти. Ломать замок — значит работать там, где противник силён и готов к удару; обходить — значит уйти туда, где он и не думал обороняться. Криптографию не взламывают — её обходят. Там, где ждёшь героического взлома, чаще находишь буднично подменённый ключ.

Пока это лишь имя и роль: хозяйка трубы, решающая, что по ней течёт. Угроза названа, но ещё не осязаема — её легко выслушать и не поверить нутром, отмахнуться как от теоретической страшилки. Чтобы вежливое недоверие сменилось холодком узнавания, атаку придётся проиграть руками, шаг за шагом, и дойти до самой её жуткой черты — до того, что всё при этом выглядит совершенно, безупречно правильно.

2.2. Письмо доходит «правильно»

Проиграем всё по шагам — медленно, как разбирают по записи чужую шахматную партию, чтобы поймать тот единственный ход, после которого позиция уже проиграна, хотя доска ещё выглядит целой.

Боб хочет написать Алисе — тайно, так, чтобы прочла только она. Для этого ему нужен её открытый ключ: тот самый ящик со щелью, в который бросить письмо может любой, а вынуть — одна Алиса. Боб просит ключ, шлёт запрос по каналу. Но канал принадлежит Мэллори. Запрос доходит до неё, и вместо ключа Алисы она протягивает Бобу свой собственный, аккуратно надписав его именем Алисы. Боб получил ключ, на котором стоит нужное имя, — с чего бы ему усомниться. Первый шаг сделан, и он безупречен на вид.

Боб пишет письмо и запирает его этим ключом — тем, что считает ключом Алисы. Запертое, оно уходит обратно в трубу и снова попадает к Мэллори — но теперь запертым её собственным замком, который она, разумеется, отпирает без малейшего труда: замок-то её. Мэллори читает письмо целиком. Второй шаг: тайна, ради которой всё затевалось, уже нарушена, а Боб об этом не знает и знать не может.

Дальше — самое изящное, и здесь стоит задержаться. Мэллори не обрывает связь, не глотает письмо, не оставляет Алису без вести — любое из этого выдало бы её мгновенно.

но, потому что молчание там, где ждут ответа, само по себе неправильность. Вместо этого она берёт прочитанный текст и запирает его заново — на сей раз настоящим ключом Алисы, который у неё, хозяйки трубы, конечно, тоже есть, ведь этот ключ открытый и достался ей так же легко, как всем. Запертое письмо она отправляет дальше. Третий шаг: письмо продолжает путь, будто с ним ничего не случилось.

Алиса получает письмо и отпирает его своим ключом — и оно открывается. Открывается чисто, без заминки, без единого следа чужого касания. Представьте конверт, который кто-то вскрыл над паром, прочёл и запечатал снова той же печатью, тем же воском, ровно тем же оттиском, — так, что и под лупой не отличить от нетронутого. Именно это Мэллори проделывает с письмом, только воск у неё безупречен всегда: перешифровать правильным ключом — не то же, что подделать печать похоже: это значит запечатать её тождественно. Четвёртый шаг завершён, и на нём вся хитрость становится видна разом.

Оглядим сцену. Что видел каждый её участник? Боб просил ключ Алисы — и получил ключ под именем Алисы. Боб отправил тайное письмо — и оно ушло. Алиса получила письмо — и оно открылось её собственным ключом, тем самым, что лежит у неё и больше ни у кого. С точки зрения обоих всё прошло идеально: запрошено — получено, заперто — доставлено, открыто — прочитано. И если Алиса напишет ответ, он пойдёт той же дорогой, через тот же двой-

ной замок — ключ Боба подменён точно так же, — так что разговор может течь месяцами в обе стороны, оставаясь для Мэллори открытой книгой. Ни одной неправильности, за которую мог бы зацепиться глаз.

Вот отчего по спине проходит холодок. Мы привыкли, что взлом оставляет след: сломанную печать, царапину на замке, письмо, которое не открывается или открывается не тем ключом, — что-нибудь да не так. Ищешь неправильность — по ней и ловишь врага. Но здесь ловить нечего. Атака Мэллори не производит неправильности; она производит безупречную правильность. Алиса получает сообщение *под своим* ключом — потому и не подозревает. Всё валидно, всё сходится, всё на месте — и всё прочитано.

И дело не в том, что Боб с Алисой беспечны. Будь они сколь угодно осторожны, осторожности не за что зацепиться: нет галочки, которая не встала бы, нет проверки, которая не прошла бы, нет тревожного знака, который мог бы вспыхнуть. Ключ пришёл с верным именем; письмо заперлось и отперлось; ответ дошёл. Всякая мыслимая проверка правильности даёт зелёный свет — потому что подделка правильна во всём, кроме единственного, чего ни одна такая проверка не спрашивает.

Именно эта черта делает человека посередине по-настоящему жутким, а не просто досадным. Против врага, оставляющего следы, есть хотя бы надежда: будь внимательнее, проверяй тщательнее, лови несоответствие. Против врага без

следов внимательность бессильна. Значит, если ловить, то не письмо и не здесь. Ловить надо было раньше и не то — но что именно и в какой момент, ещё предстоит понять.

2.3. Аутентифицировать вход, не выход

Раз письмо чисто, а обман всё же случился, обман сидит не в письме. Где-то среди четырёх шагов есть точка, в которой ещё можно было всё спасти, — и найти её важнее, чем возмущаться самим фактом обмана. Интуиция по старой привычке сторожит приходящее и тычет пальцем в конец: проверьте то, что дошло, — не подменили ли, не подделали ли по дороге. Но письмо, дошедшее до Алисы, подменять было незачем; оно настоящее, заперто её настоящим ключом, и любая проверка на её конце скажет одно: всё в порядке. Алиса уже ничего не исправит — не потому, что проверяет плохо, а потому, что всё случилось задолго до неё.

Прокол — раньше и не там. Он произошёл в ту секунду, когда Боб принял ключ, надписанный именем Алисы, за ключ Алисы. Всё, что было после, — как Боб запер письмо, как оно шло, как открылось у Алисы, — лишь послушно доводило до конца ошибку, сделанную в самом начале. Утечка случилась не на приёме письма, а на его шифровании: в тот момент, когда Боб взял чужой замок и поверил, что он Алисин.

Это и есть сдвиг рычага. Интуиция ставит рычаг провер-

ки на выход — туда, где сообщение приходит, — и жмёт изо всех сил, а рычаг не поднимает ничего, потому что стоит не в той точке. Перенеси его на вход — на миг, когда ключ только пришёл и ещё не пущен в дело, — и вдруг видно, что именно здесь, и только здесь, у Боба была власть всё изменить. Спрашивать стоило не «цело ли пришедшее письмо», а «тот ли ключ я беру, прежде чем хоть что-то им запирать».

Правило шире одной сценки. Проверять надо ключ, когда его получаешь, а не сообщение, когда оно пришло. Миг приёма ключа — единственная точка на всём пути, где ещё можно было остановить Мэллори; дальше математика делает своё дело безупречно — и, приняв подделку за подлинник, делает его в пользу Мэллори. Криптография не ошибается — она честно служит тому ключу, который ей дали. Дали чужой — честно служит чужому, с той же силой и тем же прилежанием, что служила бы своему.

Теперь можно назвать точно, чего именно недоставало на входе. Боб ведь проверил бы ключ, если бы знал, что проверять; вся беда в том, что привычный вопрос звучит мимо цели. Мы спрашиваем: правильный ли это ключ? — рабочий ли, не испорчен ли, отпирает ли то, что должен. И на это ключ Мэллори отвечает безукоризненно: он совершенно правильный, настоящий рабочий ключ — только Мэллорин. Валидность — свойство математическое, и у подделки оно безупречно. А спросить следовало иное: чей это ключ? Принадлежность лежит не в математике, а снаружи неё —

и именно её никто не проверил, потому что никто о ней не спросил.

Разница здесь та же, что между двумя вопросами к предъявленному документу: хорошо ли он сделан — и того ли он человека. Можно до буквы выверить водяные знаки, чёткость печати, целостность ламината и остаться совершенно спокойным — придраться не к чему; и всё это время не спросить единственно важного: а лицо на нём — того, кто стоит перед тобой? Ключ Мэллори — безупречный документ на чужое имя.

Вот он, поворот: вопрос не «правильный ли ключ», а *чей* он. Стоит вслушаться, до чего это разные вопросы. Первый весь внутри математики, и математика же на него отвечает — да, ключ рабочий. Второй — снаружи, и внутри математики ответа на него нет вовсе: сколько ни разглядывай сам ключ, нигде в нём не написано, кому он принадлежит. Мэллори не подсунула плохой ключ — она подсунула хороший ключ не того человека. И пока Боб проверяет качество ключа вместо его принадлежности, он будет попадаться снова и снова, как бы придирчиво ни проверял, — потому что придирчивость его направлена на вопрос, в котором подделка неотличима от подлинника.

Вопрос поставлен — и в нём уже слышна следующая трудность. Хорошо, спрашивать надо «чей». Но чем на это ответить? Сам ключ о своей принадлежности молчит; письмо молчит; канал в руках Мэллори и подавно. Чтобы узнать, чей

ключ, придётся к чему-то обратиться за порукой — и вот при первой же честной попытке что-то начинает подозрительно напоминать круг.

2.4. Первое появление Стены

Спросим прямо: чем же ответить на «чей»? Боб держит ключ, надписанный именем Алисы, и хочет удостовериться, что ключ и вправду её. Что он может сделать?

Он может сверить ключ с чем-то — скажем, с коротким отпечатком, который Алиса заранее дала ему на бумажке. Может спросить кого-то — общего знакомого, справочник, посредника, которому доверяет, — тот ли это ключ. Может вспомнить что-то — например, что этим самым ключом они с Алисой уже переписывались месяц назад, и тогда всё сходилось. Пути разные, все по-своему разумны. Но приглядимся, на чём стоит каждый.

Сверить с бумажкой можно, лишь если веришь, что бумажка — от Алисы, а не подsunута Мэллори по дороге. Спросить посредника можно, лишь если веришь, что посредник честен и сам не обманут той же хозяйкой трубы. Вспомнить прошлую переписку можно, лишь если веришь, что тогда, месяц назад, на том конце была Алиса, а не Мэллори с самого начала. Куда ни ткни, ответ на «чей?» опирается на что-то, чему Боб уже доверяет. Проверка не рождает доверие из пустоты — она его тратит: берёт уже имеющуюся

у Боба уверенность в чём-то одном и ставит её порукой за новый ключ. Опору не создают проверкой — проверкой её расходуют.

Всё держится на одном коротком слове — *уже*. Каждый способ проверить требует доверия, которое есть у Боба прежде проверки, готовым, до первого сличения. И если заранее у Боба нет ничего, чему он верит, — ему попросту не из чего исходить: не с чем сверять, некого спрашивать, нечего вспоминать. Пустые руки так и останутся пустыми, сколько ими ни води над ключом. Первую уверенность неоткуда добыть проверкой, потому что проверка ею кормится.

Вот теперь круг виден во весь рост, и форма у него неприятно правильная. Чтобы установить доверие к ключу, нужно доверие к чему-то ещё. А откуда взялось то, другое доверие? Из проверки — которая опять-таки на что-то опиралась. Спросил справочник — но кто поручился за справочник? Кто-то или что-то, чему Боб поверил ещё раньше; а за того поручителя — кто? Ответ всякий раз отступает на шаг назад и там снова протягивает руку за опорой. Куда ни отступай, под ногой обнаруживается ещё одна опора, которую саму надо на чём-то держать. Доверие всё время занимают у доверия, как занимают денег, чтобы отдать прежний долг. И нигде в этой цепочке не видно первого звена — того, что держалось бы само, ни на что не опираясь. Боб пытается вытащить себя из трясины за собственные волосы, и ни одна прядь не закреплена на твёрдом.

Тут стоит остановиться и не спешить. Заманчиво решить, что мы просто не додумали: ещё немного смекалки, ещё один хитрый приём — и круг разомкнётся, найдётся способ проверить ключ, ничего не занимая. Может быть. Но закрадывается и другая, трезвая догадка: а вдруг это не наша нерасторопность, а свойство самой задачи? Вдруг «установить доверие с нуля» — не трудное дело, а невозможное в том же смысле, в каком нельзя приподнять пол, на котором стоишь? Разница огромна. Если это наша нерасторопность — надо думать дальше. Если свойство задачи — думать дальше бесполезно, и честнее это признать.

И стоит сразу отвести соблазн мрачного вывода. Это открытие — вовсе не про то, что доверять нельзя никому. Круг ничего не запрещает; он лишь показывает, где сидит настоящая трудность — не в математике, отработавшей без единого сбоя, а вне её, в одном вопросе о том, чей ключ. Мы всего только нашли точное место, где кончается власть шифра и начинается что-то иное, чему пока не подобрано имени.

Доказывать догадку рано. Но она уже поменяла воздух в комнате: мы искали лазейку в приёме, а наткнулись, похоже, на что-то не поддающееся — на первую тень стены. И у этой стены пока нет имени; и у того, чего недостаёт Бобу, — у того самого «нечто, чему он уже доверяет», за что можно было бы зацепить всю постройку, — имени тоже нет.

Труба по-прежнему в чужих руках, и всё, что приходит по ней, приходит правильно — только теперь мы знаем,

что как раз в этой правильности и прячется обман. Лёгкая мысль, с которой всё началось, — раз ключ публичный, до-вольно его опубликовать, — не пережила и четырёх шагов: публикация не стоит ничего, а вся тяжесть переехала на один простой с виду вопрос — чей это ключ? — на кото-рый нельзя ответить честно, не заняв где-то уже готового доверия. А занять его, эту первую уверенность, пока реши-тельно неоткуда.

Круг сомкнулся: чтобы установить доверие, нужно до-верие. И всё же не верится, что он смыкается наглухо, — ведь как-то же люди узнают друг друга, как-то же тайные письма доходят до тех, кому посланы. Где-то должна быть лазейка, через которую в этот круг просачивается первое доверие. Есть ли она взаправду — или мы принимаем за ла-зейку собственную, ещё не додуманную мысль?

Часть II. Стена

«А что, если бы ключом человека было само его имя — и, чтобы написать ему тайно, довольно было бы знать, *кто* он, а вовсе не какой у него ключ?» — вопрос Ади Шамира, 1984

Круг «чтобы установить доверие, нужно уже иметь доверие» легко принять за головоломку, которую просто ещё не разгадали, — за узел, который развяжет тот, кто окажется достаточно умён. У области за плечами полвека блестящих идей, изящных протоколов, имён, ставших легендой, — и трудно поверить, что среди всего этого не нашлось приёма, распутывающего такой простой на вид узелок. Эта вера — последняя из иллюзий, с какими читатель сюда пришёл, и проверить её стоит не отмахиваясь, а честно, до конца.

Проверка приводит к неуютному различению. Одно дело — сказать «мы пока не знаем, как»; совсем другое — «так не бывает, и вот почему». Круг доверия оказывается не пробелом в знании, а тем самым разветвлением, о которое философия спотыкается не первое тысячелетие: любая попытка что-либо обосновать сваливается в одну из немногих ловушек, и выхода мимо них нет. Там, где инженер ждёт трюка, обнаруживается теорема.

Дальше дорога идёт вниз. Лучшие умы области с этим выводом не смирялись — они строили обходы, каждый

по-своему остроумный, и каждый по-своему проваливался. Пройти их придётся один за другим: не чтобы позлорадствовать над чужой неудачей, а чтобы увидеть то, что видно только снизу. Стена, в которую они били, — не забор, который перелезают. Это несущая конструкция: убрать её нельзя, не обрушив всё, что на ней стоит.

Глава 3. Нельзя получить нечто из ничего

Между «мы не нашли решение» и «решения не существует» лежит пропасть. Первое — приглашение стараться сильнее: ещё одна бессонная ночь, ещё один умник — и замок поддастся. Второе — знание другого сорта, редкое и дорогое; его не добывают упорством, потому что упорство здесь бьёт в пустоту. Мало какие вопросы удаётся перевести из первого разряда во второй, и почти всегда это событие в истории мысли. Вопрос о ключе незнакомца — из тех немногих, что такой перевод допускают, и проделать его можно прямо на глазах у читателя.

Для такого перевода довольно предельно голой сцены: двое, у которых нет ровно ничего общего, а между ними канал, которым распоряжается чужой. Подделку в этой сцене не отличить от подлинника — и не по слабости средств, а по самому её устройству. Инженерная тупиковость здесь — частный случай куда более старой развилки, у которой ровно три исхода и четвёртого нет. А из развилки растёт переворот взгляда: то, что мы привыкли считать производством защиты, на поверку — перевозка. По трубе течёт лишь то, что в неё залили.

3.1. Аутентификация из нуля невозможна

Поставим опыт в самом чистом его виде. Комната, в ней двое — Алиса и Боб, — и между ними нет ничего: ни общего пароля, ни встречи в прошлом, ни знакомого, который поручился бы за одного перед другим, ни единого бита, который был бы у обоих и только у них. Всё, что их связывает, — канал, и канал этот принадлежит Мэллори. Она не подслушивает из-за угла; она и есть труба, по которой идёт каждое слово. Она читает, задерживает, подменяет, сочиняет — всё, что проходит, проходит через её руки.

Теперь Алиса хочет доказать Бобу, что письмо от неё. Что она может послать? Любую последовательность знаков. Пароль, придуманный на ходу, — но Боб его прежде не слышал и не отличит настоящий от выдуманного. Ответ на секретный вопрос — но общего секрета у них нет, вопрос задать не из чего. Результат самого изощённого обмена репликами, какой сумеют выдумать инженеры, — пожалуйста. Но что бы Алиса ни отправила, оно идёт по трубе Мэллори, и Мэллори видит его целиком. А раз видит — может отправить Бобу ровно то же самое от собственного имени. Всё, чем Алиса доказывает «это я», Мэллори повторяет знак в знак, доказывая «это я» с тем же успехом. У Боба на входе оказываются два неразличимых голоса, и нет ни приметы, по которой

один отличался бы от другого.

А если Боб не станет ждать пассивно и начнёт проверять сам — задаст встречный вопрос, потребует отклика, устроит допрос? Это ничего не меняет, потому что вопрос Боба тоже идёт по трубе. Мэллори принимает его, передаёт настоящей Алисе, получает от неё честный ответ и вручает Бобу — сидя посередине, работая переносчиком в обе стороны. Боб допрашивает Алису через Мэллори и получает подлинные ответы Алисы, заверенные Мэллори. Активность на входе не выручает: сколько ни спрашивай, спрашиваешь ты через ту же трубу.

Соблазнительно решить, что беда в недостаточно хитром протоколе: добавить обмен туда, лишний шаг сюда — и Мэллори не успеет, где-нибудь да проговорится. Стоит прочувствовать до конца, почему это не помогает. Сколько бы ходов ни было в протоколе, все они на виду у хозяйки трубы; что в каждый момент доступно Алисе, в тот же момент доступно и Мэллори, знак в знак. Мэллори встаёт посередине неотличимо не потому, что мы плохо старались, а потому, что при нулевом общем у подделки и у подлинника ровно одно и то же содержание. Различить их — значит извлечь из письма то, чего в нём попросту нет. Нарращивать хитрость здесь — всё равно что взвешивать всё точнее предмет, у которого нет веса: прибор ни при чём, весить нечего.

Можно повернуть то же самое и другой стороной. Чтобы Боб отделил Алису от Мэллори, ему нужен хотя бы один

признак, который есть в письме настоящей Алисы и которого не окажется в копии. Но копия на то и копия: Мэллори переносит в неё каждый признак без остатка — она ведь держит оригинал целиком в руках. Единственное, чего ей не скопировать, — то, чего в письме нет вовсе, что живёт где-то помимо канала. А по условию помимо канала у Алисы с Бобом нет ровным счётом ничего. Отличать, стало быть, нечем: всякий признак либо переезжает в копию вместе со всем прочим, либо его не существует. Третьего между этими двумя не помещается.

И вот тут проходит граница между двумя сортами незнания. «Мы ещё не нашли трюк» — неверный диагноз: он обещает, что где-то трюк лежит и ждёт своего часа. Не лежит. Не спрятан, не потерян, не дожидается следующего гения — его не существует, как не существует самого большого числа. Начать с чистого нуля и получить на выходе уверенность в том, *чей* перед тобой голос, нельзя — ни ловким алгоритмом, ни грубой силой, ни изобретательностью, которой пока недостало. Это не край наших умений. Это край самой задачи.

Странно только, что тупик знаком. Инженер упёрся в него, ворочая ключи и каналы, — но точно такой же тупик много раньше нашли те, кто ни о каких ключах не думал, а спрашивал куда проще: почему вообще хоть чему-то можно верить.

3.2. Трилемма Мюнхгаузена

Есть старая картинка: барон Мюнхгаузен тонет в болоте и, чтобы спастись, хватает сам себя за косичку и вытягивает наружу — вместе с конём. Смешно ровно потому, что так нельзя: опору не добыть из того самого, что тонет. Над этой невозможностью думали задолго до любых ключей и додумались до неё в общем виде — как до предела всякого обоснования вообще.

Возьмите любое утверждение и спросите: почему оно верно? В ответ дадут другое утверждение — основание. Спросите то же про основание. И вот здесь, куда бы вы ни двинулись дальше, дорога расходится ровно на три, а четвёртой тропы нет.

Первая — круг. Основание опирается на то, что само нужно в обосновании: первое верно, потому что верно второе, а второе — потому что верно первое. Круг бывает широким, в десяток звеньев, так что подвох не разглядеть сразу, — но рано или поздно цепь замыкается на себя, и всё сооружение висит в воздухе, держась за собственный хвост. Ничего оно не удостоверяет: внутри круга можно с равным правом доказать и утверждение, и обратное ему.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.