O.V.K — X.T.R

ТАЙНОПИСЬ

КЛЮЧ, МЕРА И ПРИВЫЧКА



ИСТОРИЯ, УСТРОЙСТВО И ЗАЩИТА

O.V.K — X.T.R

ТАЙНОПИСЬ

КЛЮЧ, МЕРА И ПРИВЫЧКА

Изложение истории, устройства и правил —
от скиталы и чёрных кабинетов к машине и ключу,
и к тому, что защищает переписку ныне

НАСТОЛЬНОЕ ИЗДАНИЕ

«Тайна письма держится не на том, что способ неизвестен, а на том, что ключ не найден. Кто прячет способ — прячет от себя».

— из тетради шифровального стола



Книга писана для того, кто хранит написанное,
а не для того, кто читает чужое.
Приёмы изложены как приёмы,
границы — как границы,
и ничто не выдаётся за неприступное.

ОГЛАВЛЕНИЕ

ЧАСТЬ ПЕРВАЯ. ОСНОВАНИЯ

I. Что такое тайнопись 2
II. Слово и его происхождение 3
III. Три основания 4
IV. Древность: скитала и Цезарь 5
V. Аль-Кинди и счёт букв 6
VI. Возрождение: диск и таблица 7
VII. Чёрные кабинеты и телеграф 8
VIII. Чем тайнопись не является 9

ЧАСТЬ ВТОРАЯ. СТАРЫЕ ШИФРЫ

IX. Перестановка 11
X. Простая замена 12
XI. Как ломают замену 13
XII. Многоалфавитная замена 14
XIII. Как сломали Виженера 15
XIV. Одноразовый блокнот 16
XV. Роторные машины 17
XVI. Как сломали «Энигму» 18

ЧАСТЬ ТРЕТЬЯ. МЕРА И ЗАКОН

XVII. Шеннон и мера тайны 20
XVIII. Смешение и рассеяние 21
XIX. Ключ: длина и хранение 22
XX. Что значит «взломать» 23
XXI. Виды нападения 24
XXII. Случайность и её подделки 25
XXIII. Ошибки употребления 26
XXIV. Побочные пути 27

ЧАСТЬ ЧЕТВЁРТАЯ. НЫНЕШНЕЕ УСТРОЙСТВО

XXV. Шифры с общим ключом 29
XXVI. Отпечаток письма 30
XXVII. Два ключа 31
XXVIII. Подпись и удостоверение 32
XXIX. Как договариваются незнакомцы 33
XXX. Пароли и их хранение 34
XXXI. Переписка от края до края 35
XXXII. Что обещает квантовая машина 36

ЧАСТЬ ПЯТАЯ. ГРАНИЦА

XXXIII. Человек как слабое звено 38
XXXIV. Что видно и без содержания 39
XXXV. Не изобретай своего шифра 40
XXXVI. Чего тайнопись не может 41
XXXVII. Тайна и власть 42
XXXVIII. Правила пользующегося 43
XXXIX. Что сделать сегодня 44
XL. Заключение: ключ и привычка 45

ЧАСТЬ ПЕРВАЯ

ОСНОВАНИЯ

Откуда пошло ремесло, отчего тайна держится ключом,
а не скрытностью способа,
и как оно шло от скиталы до телеграфа

ГЛАВА ПЕРВАЯ

Что такое тайнопись

Тайнописью зовётся преобразование сообщения в такой вид, при котором прочесть его может лишь владеющий *ключом*, хотя бы способ преобразования был известен всем.

В определении этом важна вторая половина. Скрывать самый способ — занятие ненадёжное: способ утекает с человеком, с прибором, с перебежчиком. Ключ же есть вещь малая, сменяемая и хранимая.

Различим четыре слова. **Шифрование** — преобразование ключом. **Кодирование** — замена слов и понятий по условленной книге («сто восемнадцать» вместо «наступать»). **Сокрытие** — утаивание самого факта письма: невидимые чернила, точка в микрофильме, лишний пробел в рисунке. **Разбор** — чтение чужого без ключа.

Тайнопись отвечает на три различных нужды, и смешивать их не должно. *Тайна* — чтобы не прочли. *Целость* — чтобы не подменили ни буквы. *Удостоверение* — чтобы знать, кем написано. Древние знали одну лишь первую; ныне вторая и третья не менее важны.

Оттого книга разделена так. Часть вторая — старые шифры и то, как их ломали; третья — мера и общие законы; четвёртая — нынешнее устройство; пятая — границы и правила для человека, ибо на человеке всё и рушится.

ГЛАВА ВТОРАЯ

Слово и его происхождение

Греческое *kryptos* — скрытый, *graphein* — писать; отсюда *криптография*, скрытое письмо. Русское «тайнопись» есть точный перевод и слово более старое, чем принято думать: так называли и подмену букв в рукописях, и «литорею» — простую замену согласных, употреблявшуюся у нас с давних пор.

Отсюда же и родственные слова. *Криптоанализ* — разбор чужого письма без ключа; по-русски говорили «дешифрование» в отличие от «расшифрования», которое совершает законный получатель ключом.

Стеганография — от *steganos*, покрытый: сокрытие самого факта переписки. Геродот рассказывает о вестнике, коему обрили голову, написали на коже и дождались, покуда отрастут волосы; о дощечках, покрытых воском поверх надписи; о зайце с письмом в брюхе.

Различение это существенно и по сей день. Шифр прячет *содержание*; сокрытие прячет *наличие*. Первое законно и открыто; второе годится там, где опасно самое подозрение в переписке.

Наилучшее употребление — вместе: скрыть содержание шифром, а факт — обыкновенностью. Письмо, ничем не отличимое от тысяч прочих, привлекает менее, чем столбцы непонятных знаков.

ГЛАВА ТРЕТЬЯ

Три основания

Всё ремесло стоит на трёх положениях, и первое из них — главное правило, нарушаемое чаще прочих.

> Стойкость должна держаться на ключе,
> а не на скрытности способа.
> Полагай, что противник знает устройство.

Первое. Правило это высказал голландец Огюст Керкгоффс в 1883 году; Шеннон повторил его короче: *враг знает систему*. Способ рано или поздно станет известен — и тогда шифр, стоявший на тайне устройства, рухнет весь разом, тогда как смена ключа стоит недорого.

Второе. Стойкость есть *цена*, а не невозможность. Всякий шифр в принципе вскрываем перебором ключей; вопрос лишь в том, сколько это стоит времени и труда. Хороший шифр делает стоимость непомерной, а не вскрытие немыслимым.

Третье. Слабое место — не шифр, а *употребление*. Историю разбора чужих писем составляют не блестящие догадки, а повторённые ключи, стереотипные начала, ленивые операторы и украденные тетради. Об этом — глава двадцать третья.

Из трёх оснований выводится всё дальнейшее, и на них же держатся правила пятой части: *береги ключ, меняй ключ, не сочиняй своего шифра и не полагайся на то, что о твоём способе не догадаются*.

ГЛАВА ЧЕТВЁРТАЯ

Древность: скитала и Цезарь

Древнейшие шифры делятся на те же два разряда, что и все позднейшие: *перестановку* и *замену*.

Скитала. Спартанский жезл: на палку определённой толщины наматывали ремень и писали вдоль; размотанный ремень нёс бессвязные буквы. Ключом служила толщина палки. Это перестановка: буквы те же, порядок иной.

Шифр Цезаря. Замена буквы на отстоящую на три места: «а» на «г», «б» на «д». Светоний сообщает об этом как о простой привычке диктатора. Это замена: порядок тот же, буквы иные.

> ВСТРЕЧА В ПОЛДЕНЬ → ЁФХУЗЪГ Ё СТМИЗРЫ

Квадрат Полибия. Буквы располагали в таблице пять на пять, и всякая обозначалась парою чисел — строкою и столбцом. Сам по себе слаб, но он — родоначальник множества позднейших приёмов, ибо превращает буквы в числа.

Все три ныне ломаются в несколько минут и приводятся не ради употребления, а ради устройства: *перестановка, замена и превращение в числа* суть три первоначальных действия, из коих собраны и нынешние шифры.

ГЛАВА ПЯТАЯ

Аль-Кинди и счёт букв

Тысячу лет замена почиталась надёжной. Разрушил её арабский учёный Абу Юсуф аль-Кинди в девятом веке, написав «Трактат о дешифровке криптографических сообщений».

Мысль его проста и убийственна. Буквы всякого языка встречаются с разной частотой: в русском чаще всего «о», «е», «а», «и», «н», «т»; всякий текст несёт этот отпечаток. Замена меняет знаки, но не меняет *частот*: самый частый знак шифра и есть самая частая буква языка.

Отсюда порядок разбора: сосчитать знаки, сопоставить с частотами языка, испытать наиболее вероятные соответствия, опереться на двубуквенные сочетания и на короткие слова — и текст открывается, как правило, в четверть часа.

Замечательно и то, откуда это выросло: из богословской работы. Учёные того времени считали слова и буквы Корана, устанавливая подлинность и порядок сур; отсюда и явился счёт как орудие.

Урок отсюда пригодится и далее: *всякая закономерность исходного текста, пережившая шифрование, есть щель для разбора*. Хороший шифр должен уничтожать все закономерности, а не одну лишь читаемость.

ГЛАВА ШЕСТАЯ

Возрождение: диск и таблица

Ответом на частотный разбор стала *многоалфавитная* замена: пусть одна и та же буква переходит в разные знаки, смотря по месту.

Леон Баттиста Альберти около 1467 года устроил шифровальный диск: два кольца с буквами, вращаемые друг относительно друга; поворот менял соответствие посреди письма. За это его зовут отцом западной тайнописи.

Иоганн Тритемий в «Полиграфии» дал таблицу, где всякая строка есть алфавит, сдвинутый на одно место, — и предложил менять строку с каждой буквой.

Джованни Порта прибавил замену пар букв, а **Блез де Виженер** в 1586 году соединил всё это с *ключевым словом*: буква ключа указывает, какою строкою таблицы шифровать очередную букву.

Шифр этот прославился под именем Виженера и три века почитался невскрываемым — его так и звали, *le chiffre indéchiffrable*. Устройство его и способ разбора изложены в главах двенадцатой и тринадцатой.

Заметим общее: всякий раз, как разбор побеждал шифр, ответом было *прибавление разнообразия* — больше алфавитов, длиннее ключ, сложнее перемешивание. Это и есть закон необходимого разнообразия, знакомый по книге о кибернетике.

ГЛАВА СЕДЬМАЯ

Чёрные кабинеты и телеграф

С шестнадцатого века при дворах завелись *чёрные кабинеты* — учреждения, где вскрывали, читали и вновь запечатывали чужую почту.

Устроены они были основательно: мастера подделки печатей, чтецы на всех языках, писцы для скорых копий, разбиратели шифров. Венский кабинет славился тем, что письмо, поданное утром, к полудню возвращалось в почтовую сумку с нетронутою печатью.

Из этого ремесла вышли и славные разборы. Мария Стюарт была осуждена по письмам, писанным шифром замены и прочитанным Томасом Фелиппсом; в письмо, к слову, приписали и подложную строку — ранний пример того, для чего нужна *целость*, а не одна лишь тайна.

Телеграф в девятнадцатом веке перевернул дело. Сообщение перестало быть вещью, которую можно спрятать за пазухой: оно шло по проводу через чужие руки. Шифровать стало необходимо всякому купцу, а не одному послу.

Отсюда и перемена ремесла: от искусства писцов оно пошло к машинам, ибо телеграф требовал скорости, а скорость требовала устройства, а не выдумки. Об этом — глава пятнадцатая.

ГЛАВА ВОСЬМАЯ

Чем тайнопись не является

Отсечём лишнее, ибо на этом предмете наросло много вздора и много ложных надежд.

Она не есть сокрытие факта. Шифр прячет содержание; что вы кому-то писали, останется видно. Об этом — глава тридцать четвёртая, и это ныне важнее самого содержания.

Она не есть неприступность. Всякий шифр вскрываем перебором; вопрос в цене. Обещание «невзламываемого» есть первый признак невежества или обмана.

Она не есть кодовое слово вместо имени. Замена слов по условленной книге не даёт тайны: сообщение выдаёт себя длиной, повторами и обстановкой.

Она не защищает от того, кому вы пишете. Получатель прочтёт и может пересказать; ни один шифр этого не отменяет.

И она не спасает беспечного. Ключ на бумажке под клавиатурой, пароль из имени кошки, письмо, пересланное не тому, — всё это обходит любую стойкость.

Что же она даёт? *Возможность хранить и передавать написанное так, что чтение его посторонним стоит дороже, чем оно того стоит.* Этого довольно для всего, ради чего ею пользуются.

ЧАСТЬ ВТОРАЯ

СТАРЫЕ ШИФРЫ И ИХ РАЗБОР

Перестановка, замена, таблица и машина —
и всякий раз способ, коим их вскрывали;
ибо устройство шифра понимается через его слабость

ГЛАВА ДЕВЯТАЯ

Перестановка

✢

При перестановке буквы остаются те же, меняется лишь порядок. Простейший вид — запись по столбцам и чтение по строкам.

```
ВСТРЕЧАВПОЛДЕНЬ → таблица 5×3 →
ВЧПЕС АОНТВ ЛЬРВД (по столбцам)
```

Ключом служит ширина таблицы, а в шифрах поизящнее — порядок, в котором столбцы выписываются: он задаётся словом, буквы коего расставляются по алфавиту.

Слабость. Частоты букв сохраняются в точности: счёт даёт тот же отпечаток, что и обыкновенный текст этого языка. Оттого разбиратель немедленно узнаёт, что перед ним перестановка, а не замена, — и это половина дела.

Разбор. Испытывают ширины таблицы; при верной ширине в столбцах появляются осмысленные сочетания. Помогают и *вероятные слова*: если письмо военное, ищут «дивизия», «наступление», «час».

Перестановка сама по себе слаба, но полезна в соединении с заменою: она уносит соседство букв, которого замена не трогает. Это первый пример того, что в главе восемнадцатой названо *рассеянием*.

ГЛАВА ДЕСЯТАЯ

Простая замена

✢

При замене всякой букве назначен свой знак — постоянный на всё письмо. Ключом служит самое соответствие: для русского алфавита это перестановка тридцати трёх букв.

Число возможных ключей огромно — тридцать три факториал, число из тридцати шести цифр. Перебрать их нельзя ни ныне, ни впредь; и однако шифр этот ломается за четверть часа карандашом.

В этом — важнейший урок всей книги: *величина числа ключей ничего не говорит о стойкости*. Стойкость определяется не перебором, а тем, есть ли способ короче перебора. Здесь он есть — счёт букв.

Разновидности, придуманные для укрепления: пропуск пробелов; несколько знаков на частую букву (омофоны); пустышки, ничего не значащие; замена не букв, а пар. Все они затрудняют разбор и ни одна не отменяет его.

Сюда же относится и всё, что ныне зовут «шифром» в играх и головоломках: знаки пляшущих человечков, руны, цифровые подстановки. Это одна и та же простая замена в разных нарядах.

ГЛАВА ОДИННАДЦАТАЯ

Как ломают замену

Изложим разбор по порядку — не затем, чтобы читать чужое, а затем, чтобы понимать, отчего шифр негоден.

Первое: счёт. Сосчитать знаки. Если частоты неровны, как в языке, — перед нами замена; если ровны — многоалфавитный шифр; если совпадают с обычными в точности — перестановка.

Второе: соответствие. Самые частые знаки положить против самых частых букв языка: «о», «е», «а», «и», «н», «т».

Третье: сочетания. Опереться на пары и тройки: в русском часты «ст», «но», «то», «на», «ов»; редкая буква рядом с гласной укажет на «ъ», «ь», «ы».

Четвёртое: короткие слова. Однобуквенные суть «в», «и», «с», «а», «я»; двубуквенные — «не», «на», «по», «то».

Пятое: догадка и проверка. Подставить угаданное слово, посмотреть, что получится в прочих местах, отбросить негодное.

Вся сила приёма в том, что *ошибки исправляются сами*: неверная догадка порождает бессмыслицу в другом месте. Оттого разбор идёт быстро и не требует ни машин, ни счёта.

ГЛАВА ДВЕНАДЦАТАЯ

Многоалфавитная замена

Ответ на частотный разбор состоит в том, чтобы одна и та же буква переходила в разные знаки. Так устроен шифр Виженера.

Устройство. Берётся ключевое слово и подписывается под сообщением с повторением. Всякая буква сдвигается на столько мест, сколько указывает буква ключа под нею.

```
текст: В С Т Р Е Ч А
ключ: К Л Ю Ч К Л Ю
шифр: (сдвиг по букве ключа)
```

Отчего он крепче. Одна и та же буква текста при разных буквах ключа даёт разные знаки; частоты сглаживаются, и счёт букв, погубивший простую замену, ничего не даёт.

Три века он почитался невскрываемым. Между тем слабость его лежит на виду: ключ *повторяется*. Всё, что периодично, обнаруживается счётом; в этом и состоял разбор, изложенный в главе следующей.

Заметим наперёд: если бы ключ был длиною с сообщение и никогда не повторялся, шифр стал бы неприступным в точном смысле слова. Это и есть одноразовый блокнот из главы четырнадцатой.

ГЛАВА ТРИНАДЦАТАЯ

Как сломали Виженера

Разбор нашёл сперва Чарлз Бэббидж около 1854 года — и не напечатал; независимо и печатно изложил его прусский офицер Фридрих Касиски в 1863 году.

Первый шаг: найти длину ключа. Если в тексте попадаются одинаковые сочетания знаков, они, вероятнее всего, суть одинаковые куски текста, зашифрованные одинаковыми кусками ключа. Расстояния между ними кратны длине ключа; наибольший общий делитель этих расстояний и есть искомая длина.

Второй шаг: разделить. Зная длину, скажем, пять, выписывают всякую пятую букву в отдельный столбец. Внутри столбца работал один и тот же сдвиг — то есть перед нами простая замена, и её ломают счётом, как в главе одиннадцатой.

Уточнение дал позднее Уильям Фридман: *индекс совпадений* — мера того, насколько часто в тексте совпадают буквы, отстоящие на одно и то же расстояние. Он указывает длину ключа надёжнее совпадений сочетаний.

Урок всеобщий и годный за пределами шифров: *всякое повторение выдаёт устройство*. Оттого главные правила употребления — не повторять ключа и не начинать сообщений одинаково.

ГЛАВА ЧЕТЫРНАДЦАТАЯ

Одноразовый блокнот

Есть шифр, о котором доказано, что он неприступен, — и он же наименее употребим. Различить эти две стороны полезно всякому.

Устройство. Ключ — вполне случайная последовательность, *длиною с сообщение*, употребляемая *единожды*. Всякая буква складывается со своей буквой ключа. Придуман Гилбертом Вернамом в 1917 году; Шеннон доказал его совершенство в 1949-м.

Отчего он совершенен. При таком ключе всякий текст той же длины возможен с равной вероятностью. Перехватив шифровку, можно получить и «наступать в полдень», и «отступать на север» — при своём ключе для каждого. Стало быть, шифровка не несёт о тексте *никакого* сведения.

Отчего он неудобен. Ключ должен быть длиною с сообщение, вполне случайным, доставленным заранее по надёжному пути и уничтоженным после употребления. Дважды употреблённый ключ рушит всё: два письма, сложенные вместе, дают уравнение с двумя текстами и без ключа.

Именно так и вышло у советских шифровальщиков в сороковые годы, когда часть блокнотов была отпечатана дважды: американская работа «Венона» читала эти письма годами.

Отсюда мораль, годная для всей книги: *совершенство на бумаге не есть надёжность на деле*. Всё решает исполнение.

ГЛАВА ПЯТНАДЦАТАЯ

Роторные машины

Телеграф потребовал скорости, и на смену карандашу пришла машина. Устройство их таково, что заслуживает описания.

Ротор — колесо с двадцатью шестью (или тридцатью) контактами с каждой стороны, соединёнными внутри вперемешку: он есть простая замена, воплощённая в проводах. Но после всякой буквы ротор поворачивается — и замена меняется.

Несколько роторов ставятся друг за другом; второй поворачивается, когда первый сделает полный оборот, третий — когда второй, наподобие счётчика. Так получается многоалфавитный шифр с периодом в тысячи букв.

«Энигма», немецкая машина, имела сверх того *отражатель*, возвращавший ток обратно через роторы, и *коммутационную панель*, попарно менявшую буквы. Ключом были: набор и порядок роторов, начальные положения, положения колец и пары на панели.

Число сочетаний выходило астрономическое, и немцы полагали машину неприступной. Между тем в ней был изъян, происходивший от отражателя: *ни одна буква не переходила в себя*. Это малое обстоятельство и стало щелью, о чём в главе следующей.

ГЛАВА ШЕСТНАДЦАТАЯ

Как сломали «Энигму»

Работа эта — лучший пример того, что шифры ломают не догадкою, а сочетанием разбора, ошибок противника и машины.

Поляки. Марьян Реевский с товарищами ещё в тридцатые годы восстановили устройство машины и построили «бомбу» — прибор для перебора положений. В 1939 году они передали всё англичанам и французам; без этого дальнейшее было бы невозможно.

Блетчли-Парк. Алан Тьюринг и Гордон Уэлчман переустроили «бомбу» так, чтобы она искала не отдельные ключи, а *противоречия*: перебор шёл, покуда предположение не приводило к нелепости, и тогда отбрасывался целый разряд ключей разом.

Опоры. Работа держалась на *вероятных словах*: сводки погоды, начинавшиеся одинаково; «ничего не имею донести»; имена и звания. Немецкая исправность в переписке была лучшим союзником разбирателей.

Ошибки употребления. Повторение ключа сообщения дважды в начале; ленивые операторы, бравшие соседние буквы или инициалы подруг; повторные передачи того же текста иным ключом.

Итог поучителен вдвойне. Машина была хороша; погубили её *устройство отражателя* и *обиход*. И второе: разбор держали в такой тайне, что немцы до конца войны не знали о нём, — ибо разбор, о котором стало известно, перестаёт работать.

ЧАСТЬ ТРЕТЬЯ

МЕРА И ЗАКОН

Чем измеряется тайна, что значит «взломать»,
откуда берётся случайность
и отчего шифры рушатся не в устройстве, а в обиходе

ГЛАВА СЕМНАДЦАТАЯ

Шеннон и мера тайны

В 1949 году Клод Шеннон — тот же, что дал меру сведения, — напечатал работу о тайне сообщений, и с неё тайнопись сделалась наукою.

Он поставил вопрос строго: *сколько сведения о тексте несёт шифровка*. Совершенной он назвал тайну, при которой шифровка не несёт о тексте ничего: перехват не меняет вероятностей ни на волос. Он же доказал, что для этого ключ должен быть не короче сообщения и употребляться однажды.

Отсюда следствие, отрезвляющее и полезное: *всякий удобный шифр несовершенен*. Раз ключ короче сообщения, шифровка содержит достаточно сведения, чтобы ключ определялся однозначно — при неограниченном труде. Стойкость таких шифров есть стойкость по *цене*, а не по существу.

Он ввёл и *расстояние единственности* — длину шифровки, начиная с которой ключ определяется однозначно. Для простой замены в русском тексте это несколько десятков знаков; оттого короткие письма ломаются хуже длинных.

И третье его понятие, вошедшее в обиход, — смешение и рассеяние, о коих глава следующая. Ими описывается всё внутреннее устройство нынешних шифров.

ГЛАВА ВОСЕМНАДЦАТАЯ

Смешение и рассеяние

Шеннон указал два действия, из коих строится всякий добротный шифр, и вот они.

Смешение — связь между ключом и шифровкой должна быть запутанной: перемена одной буквы ключа должна менять шифровку непредсказуемым образом. Простая замена смешивает плохо: соответствие видно насквозь.

Рассеяние — всякий знак исходного текста должен влиять на многие знаки шифровки, а закономерности текста должны размазываться по всей длине. Перестановка рассеивает; замена — нет.

Отсюда общее устройство нынешних шифров: они складываются из *многих повторяемых кругов*, в каждом из коих есть замена (смешение) и перестановка либо перемешивание (рассеяние). Один круг слаб; десять или двадцать делают связь неуследимой.

Мерою хорошего перемешивания служит *лавина*: перемена одного знака во входе должна менять около половины знаков на выходе. Если этого нет, шифр негоден, сколь бы сложным ни выглядел.

Заметим, что здесь работает то же правило, что и в кибернетике: *разнообразие ответов должно покрывать разнообразие нападений*. Шифр, у которого перемешивание бедное, оставляет разбирателю щели, и щели эти находятся.

ГЛАВА ДЕВЯТНАДЦАТАЯ

Ключ: длина и хранение

Ключ есть единственное, что отличает вас от постороннего. Оттого всё, что о нём сказано, важнее устройства шифра.

Длина. Мерится в двоичных разрядах; всякий прибавленный разряд *удваивает* труд перебора. Ключ в сорок разрядов ныне перебирается быстро; в восемьдесят — трудно; в сто двадцать восемь — перебор невозможен при любых мыслимых средствах.

Заметим для ясности: невозможен не оттого, что дорого, а оттого, что не хватило бы вещества и времени вселенной, если считать по нынешним понятиям об энергии. Оттого длину ключа давно перестали считать слабым местом.

Происхождение. Ключ должен быть *случайным*, а не придуманным: человеческие выдумки предсказуемы, о чём в главе двадцать второй.

Хранение. Здесь и рушится всё. Ключ, лежащий рядом с шифровкой, есть отсутствие шифра. Отсюда правила: держать отдельно, беречь как деньги, менять по времени, иметь запасную копию в надёжном месте — ибо потеря ключа есть потеря написанного.

Смена. Всякий ключ имеет срок: чем больше им зашифровано, тем больше материала у разбирателя. Военные меняли ключи ежедневно; в нынешних устройствах это делается само собою при каждом соединении.

ГЛАВА ДВАДЦАТАЯ

Что значит «взломать»

Слово это в обиходе означает всё что угодно, а в ремесле имеет точный смысл, и различать надобно твёрдо.

> Шифр считается сломанным, если найден способ, дающий ключ или текст дешевле полного перебора, — хотя бы этот способ и был неисполним.

Отсюда две вещи, кажущиеся противными здравому смыслу. **Первая:** шифр может быть «сломан» и при этом оставаться пригодным — если найденный способ дешевле перебора вдвое, но всё ещё невыполним.

Вторая: шифр может быть безупречен и при этом бесполезен — если ключ можно достать иным путём: подкупом, кражей, побочными каналами, о коих глава двадцать четвёртая.

Оттого честная оценка звучит скучно: *«при таком-то нападении требуется столько-то работы»*. Всякое «взломан!» без указания рода нападения и цены есть газетный шум.

И правило для читателя новостей: спрашивать три вещи — *что именно сломано* (сам шифр, его применение или чужой прибор), *чего это стоило* и *что требуется от нападающего*. Обыкновенно оказывается, что сломано не то и не так.

ГЛАВА ДВАДЦАТЬ ПЕРВАЯ

Виды нападения

Стойкость измеряется не вообще, а против определённого рода нападения. Перечислим их по возрастанию силы нападающего.

Только шифровка. Есть перехваченное письмо и ничего более. Так работали разбиратели прошлых веков.

Известный текст. К шифровке известен и её исходный текст — хотя бы частью. Случается сплошь и рядом: сводки погоды, стандартные заголовки, «с уважением».

Подобранный текст. Нападающий может заставить зашифровать нужное ему. Кажется натяжкой — но именно так устроены многие нынешние нападения на устройства.

Подобранная шифровка. Он может подсунуть свою шифровку и увидеть отклик — хотя бы по тому, принята она или отвергнута.

Хороший шифр обязан устоять против всех четырёх. Правило это кажется чрезмерным — и оно спасло не одно дело: слабости, найденные в лаборатории при подобранном тексте, через десять лет оборачивались настоящими взломами.

Отсюда общий подход ремесла: *оценивать по сильнейшему мыслимому нападению, а не по вероятному*. Кто рассчитывает на слабого противника, готовится к вчерашней войне.

ГЛАВА ДВАДЦАТЬ ВТОРАЯ

Случайность и её подделки

Ключи, разовые числа и соли берутся из случайности; и здесь скрывается едва ли не больше провалов, чем в самих шифрах.

Человек не случаен. Прося назвать случайное число, получают семёрку; прося придумать пароль, получают имя и год. Об этом сказано в книге о ментализме, и это же губит ключи.

Машина не случайна сама по себе. Обыкновенные счётчики дают *псевдослучайность*: последовательность, вычисляемую по правилу из начального числа. Зная правило и начало, её воспроизводят целиком.

Отсюда знаменитые провалы: игорные заведения, где ставили по предсказанному; ключи, порождённые в приборе, у которого при запуске не было ничего непредсказуемого; и целые семейства ключей, оказавшиеся одинаковыми у тысяч устройств.

Как берут случайность. Из мира: тепловой шум, дрожание времени между событиями, движение мыши, шум датчика. Полученное перемешивают и выдают через испытанное устройство, которое всегда есть в нынешних системах.

Правило же для пользующегося одно: *не сочинять случайности самому* — ни ключей, ни паролей. Для этого есть готовые средства, и они лучше всякой выдумки.

ГЛАВА ДВАДЦАТЬ ТРЕТЬЯ

Ошибки употребления

История разбора чужих писем есть по большей части история чужой небрежности. Соберём её уроки.

Повторение ключа. Одноразовый блокнот, употреблённый дважды, перестаёт быть тайной; работа «Венона» тому свидетель.

Одинаковые начала. «Совершенно секретно», «Начальнику штаба», ежедневная сводка погоды — всё это вероятные слова, дающие опору разбирателю. «Энигма» пала не в последнюю очередь на них.

Повторная передача. То же сообщение, посланное дважды — старым ключом и новым, — выдаёт оба.

Ленивый оператор. Начальные положения роторов, взятые по соседним буквам или по инициалам; пароли из одного слова; ключ, не менявшийся год.

Смешение тайного и открытого. Один и тот же текст, посланный шифром и открыто, — готовая пара для разбора.

Отсюда правило, стоящее всей главы: *шифр ломают не там, где он силён, а там, где им пользуются*. Оттого добрая половина нынешней науки посвящена не шифрам, а тому, чтобы человек не мог употребить их неверно.

ГЛАВА ДВАДЦАТЬ ЧЕТВЁРТАЯ

Побочные пути

Есть нападения, обходящие шифр вовсе: они читают не сообщение, а *поведение прибора*, который его шифрует.

Время. Если проверка ключа или пароля идёт дольше при верном начале, чем при неверном, ключ подбирается по буквам, а не перебором целиком. Оттого сравнение секретов делают *постоянным по времени*.

Потребление тока. Работа с единицею и с нулём тратит разное количество тока; измерив потребление, восстанавливают ключ. Так вскрывали смарт-карты.

Звук и излучение. Ключ восстанавливали по звуку работающего вычислителя и по излучению проводов; и то и другое — не выдумка, а опубликованные работы.

Ошибки нарочно. Прибор подвергают перегреву или сбою питания; в наступившей неисправности он выдаёт то, чего не должен.

Для домашнего употребления всё это не самая близкая опасность; но урок отсюда общий и важный: *тайна живёт не в математике, а в вещи*. Оттого шифр, безупречный на бумаге, требует ещё и опрятного исполнения, о чём и сказано в главе тридцать пятой.

ЧАСТЬ ЧЕТВЁРТАЯ

НЫНЕШНЕЕ УСТРОЙСТВО

Шифры с общим ключом, отпечаток, два ключа и подпись;
как незнакомцы уславливаются о тайне,
как хранят пароли и что сулит новая машина

ГЛАВА ДВАДЦАТЬ ПЯТАЯ

Шифры с общим ключом

Первое семейство нынешних шифров — те, где обе стороны владеют *одним и тем же* ключом. Их зовут симметричными, и они прямые потомки роторных машин.

Устройство. Текст режется на куски равной длины (блоки), и всякий блок проходит через десяток-другой одинаковых кругов, в каждом из коих есть замена по таблице и перемешивание — то самое смешение и рассеяние из главы восемнадцатой.

Ходовые. Ныне повсеместно употребляется шифр, принятый в 2001 году по открытому состязанию, с ключом в 128 или 256 разрядов. Прежний, с ключом в 56 разрядов, был отставлен именно потому, что перебор стал по силам.

Способ применения важнее самого шифра. Один и тот же блок текста при простом применении даёт один и тот же блок шифра — и картинка, зашифрованная так, остаётся узнаваемой. Оттого употребляют *сцепление* блоков и разовое число, своё для всякого сообщения.

Целость вместе с тайной. Ныне принято, чтобы шифр разом и скрывал, и удостоверял: получатель узнаёт не только содержание, но и то, что ни один знак не подменён. Это отвечает второй нужде из главы первой, и пренебрежение ею стоило многих бед.

ГЛАВА ДВАДЦАТЬ ШЕСТАЯ

Отпечаток письма

✢

Особое орудие, без коего нынешнее устройство немыслимо, — *хэш*, или отпечаток: короткое число, вычисляемое из сообщения любой длины.

Свойства, которых от него требуют. Оно быстро вычисляется. По нему нельзя восстановить сообщение. Нельзя подобрать иное сообщение с тем же отпечатком. И перемена одного знака меняет отпечаток целиком — та самая лавина.

Для чего служит. Проверить, что файл не испорчен и не подменён. Сравнить два больших предмета, не пересылая их. Подписать сообщение, подписав его отпечаток. Хранить пароли, о чём в главе тридцатой.

Слабости. Ежели удаётся найти два разных сообщения с одинаковым отпечатком, отпечаток негоден. Так пали прежние: сперва один, затем другой — для второго было показано столкновение двух разных документов.

Отсюда правило обихода: *употреблять нынешние отпечатки, а не старые*, и не полагаться на «контрольную сумму» там, где нужна защита от умысла: сумма ловит случайную порчу, а не подделку.

ГЛАВА ДВАДЦАТЬ СЕДЬМАЯ

Два ключа

Три тысячи лет тайнопись стояла перед неразрешимым затруднением: чтобы переписываться тайно, надобно сперва условиться о ключе — а как условиться, не имея тайного пути?

Разрешение явилось в 1976 году: Уитфилд Диффи и Мартин Хеллман предложили *два разных ключа* — открытый, который раздают всем, и закрытый, который хранят. Написанное открытым читается лишь закрытым.

Годом позже Ривест, Шамир и Адлеман построили такую систему на трудности разложения больших чисел на множители: перемножить два больших простых числа легко, а разложить произведение обратно — неимоверно трудно.

Позднее выяснилось, что то же самое было открыто ранее в британской правительственной службе связи и держалось в тайне до девяностых годов. Обыкновенная судьба открытий в этом ремесле.

Цена. Такие шифры много медленнее и требуют куда более длинных ключей. Оттого их не употребляют для самого письма: ими *уславливаются об общем ключе*, а письмо шифруют быстрым шифром из главы двадцать пятой. Так устроено всё нынешнее.

ГЛАВА ДВАДЦАТЬ ВОСЬМАЯ

Подпись и удостоверение

Два ключа дают не только тайну, но и обратное: способ доказать, что писал именно ты.

Устройство. Отправитель вычисляет отпечаток сообщения и преобразует его *закрытым* ключом. Всякий, имея открытый ключ, может проверить, что подпись соответствует и сообщению, и ключу.

Что это даёт. Убеждение в том, кем написано; уверенность, что ни знака не переменено; и невозможность отпереться от написанного.

Чего не даёт. Тайны: подписанное читается всеми. Тайна и подпись — разные нужды, и делаются они разными действиями.

Затруднение. Откуда знать, что открытый ключ принадлежит именно тому человеку? Ответ — удостоверение: третья сторона, которой обе доверяют, подписывает своим ключом связь имени и ключа. Так устроены свидетельства в сети.

Слабость этого устройства известна: *доверие переносится на удостоверителя*. Если он обманут или подкуплен, подделка выйдет неотличимой. Оттого удостоверителей проверяют, а выданные ими свидетельства публикуют в открытых списках.

ГЛАВА ДВАДЦАТЬ ДЕВЯТАЯ

Как договариваются незнакомцы

Соберём сказанное в порядок, по которому сегодня устанавливается всякое защищённое соединение — когда вы открываете страницу с замочком.

Первое. Стороны предъявляют друг другу, что умеют, и уславливаются о шифре.

Второе. Сервер предъявляет свидетельство: свой открытый ключ, подписанный удостоверителем. Ваш прибор проверяет подпись и имя.

Третье. Стороны выводят общий тайный ключ, обмениваясь открытыми величинами. Подслушивающий видит обмен и не может вычислить получившегося ключа — в этом и состояла мысль Диффи и Хеллмана.

Четвёртое. Дальнейшая переписка идёт быстрым шифром на этом ключе, с проверкою целости всякого куска.

Пятое, важное: ключ существует лишь на время соединения и уничтожается. Оттого перехваченная ныне переписка не прочтётся и после кражи долговременного ключа. Свойство это зовут *совершенной прямой тайной*, и оно ныне обязательно.

Заметим: пользователь ничего этого не делает и не должен делать. Всё сказанное совершается в доли секунды; ему остаётся смотреть, что имя в свидетельстве — то самое, и не проходить мимо предупреждений.

ГЛАВА ТРИДЦАТАЯ

Пароли и их хранение

Пароль есть ключ, придуманный человеком, — и потому слабейший из ключей. Правила здесь просты и повсеместно нарушаются.

Как хранить у себя. Не в голове — голова придумывает предсказуемое и путает; не на бумажке под клавиатурой; а в хранилище паролей, защищённом одним длинным ключевым выражением, которое стоит помнить.

Каковы они должны быть. Длинные и разные для всякого места. Длина важнее вычурности: четыре случайных слова крепче, чем «P@ссв3т!» и запоминаются лучше.

Второй ключ. Где можно, ставить подтверждение вторым способом — прибором или ключом-брелоком. Это защищает и тогда, когда пароль украден.

Как хранить чужие. Тому, кто держит службу: никогда не хранить паролей открыто и не хранить их зашифрованными — хранить *отпечатки*, снятые нарочно медленной функцией и с *солью*, своей для всякого пользователя.

Соль — случайная добавка — делает бесполезными заранее составленные таблицы; медленность — невыгодным перебор. Утечки последних лет читаются как перечень тех, кто этого не сделал.

ГЛАВА ТРИДЦАТЬ ПЕРВАЯ

Переписка от края до края

Обыкновенная переписка через службу устроена так: письмо шифруется до сервера, там расшифровывается, хранится и вновь шифруется до получателя. Хозяин службы видит всё.

Оконечное шифрование устроено иначе: ключи есть лишь у собеседников, а служба переносит непрозрачные для неё свёртки. Прочесть их она не может, как бы её ни просили.

Что это даёт. Тайну содержания от службы, от взломщика её серверов и от того, кто предъявит ей требование. Ныне так работает несколько распространённых переговорных устройств.

Чего не даёт. Ничего не скрывает от собеседника: он прочтёт и может показать. Не скрывает *метаданных* — кто, кому, когда и сколько, о чём глава тридцать четвёртая. И не спасает, если самый прибор в чужих руках.

Проверка собеседника. Всё это держится на том, что ключ принадлежит тому, кому вы думаете. Оттого в таких устройствах есть сличение отпечатков ключей — и им стоит воспользоваться хотя бы раз, при встрече.

Правило же простое: *тайна переписки есть свойство устройства, а не обещание службы*. Спрашивать надлежит не «обещают ли», а «может ли служба прочесть, если захочет».

ГЛАВА ТРИДЦАТЬ ВТОРАЯ

Что обещает квантовая машина

О машине этой говорят много и большею частью неверно. Скажем трезво: что она угрожает сломать, чего не тронет и что уже делается.

Что под угрозой. Шифры с двумя ключами, стоящие на разложении чисел и на схожих задачах. Для них известен способ — работа Питера Шора 1994 года, — который на достаточно большой такой машине даёт решение быстро.

Что не под угрозой. Шифры с общим ключом и отпечатки. Для них известное ускорение лишь квадратично, и оно возмещается удвоением длины ключа. Ключ в 256 разрядов остаётся достаточным.

Чего пока нет. Машины нужного размера. Нынешние приборы далеки от того, что потребно; сроки называют разные, и всякий, кто говорит уверенно, говорит лишнее.

Что делают. Разрабатывают и уже принимают в употребление шифры, стойкие к такой машине; переход начат. Делают и потому, что перехваченное сегодня может быть прочтено через двадцать лет — для государственных тайн это существенно.

Для домашнего же обихода вывод скучен: *никаких действий не требуется*. Употребляйте нынешние средства и обновляйте их; переход совершится сам, как совершались прежние.

ЧАСТЬ ПЯТАЯ

ГРАНИЦА

Где рушится всякая стойкость, что видно и без содержания,
отчего не сочиняют своих шифров
и что делать сегодня

ГЛАВА ТРИДЦАТЬ ТРЕТЬЯ

Человек как слабое звено

Ни один известный шифр наших дней не был сломан в открытом бою. Ломают людей — и это не оборот речи, а сводка происшествий.

Выманивание. Письмо от мнимого начальства, срочность, страх, ссылка на власть — всё то, что описано в книге о внушении. Пароль отдаётся добровольно, и никакая тайнопись тут не при чём.

Усталость и спешка. Предупреждение о неверном свидетельстве, нажатое не глядя; вложение, открытое между делом; ключ, отправленный тем же путём, что и шифровка.

Удобство. Пароль, одинаковый везде; ключ, не защищённый паролем, «чтобы не мешал»; отключённое подтверждение, «потому что долго».

Принуждение. Ключ отдаётся под угрозой; о том, что никакая математика от этого не спасает, сказано в главе тридцать шестой.

Отсюда правило, определяющее всю пятую часть: *защита должна быть устроена так, чтобы правильное было и самым лёгким*. Средство, требующее ежедневного подвига, будет обойдено самим пользователем — и он будет прав.

ГЛАВА ТРИДЦАТЬ ЧЕТВЁРТАЯ

Что видно и без содержания

Шифр прячет содержание. Всё прочее остаётся на виду, и это прочее зовут *метаданными*.

Видно: кто с кем связывался, когда, как часто, сколь долго, откуда, какого размера были сообщения. Видно, к каким службам обращался прибор, хотя бы содержание и было закрыто.

Довольно ли этого? Более чем. По одним лишь связям устанавливаются знакомства, привычки, распорядок, отлучки и болезни — звонок в лечебницу и следом в аптеку говорит достаточно без всякого содержания.

Оттого в ремесле давно повторяют: *содержание говорит о том, что вы сказали; метаданные — о том, кто вы*. Второе для наблюдающего часто ценнее.

Что с этим делать. Устройства, скрывающие связь, существуют — посредники, луковичная маршрутизация, подмешивание пустого потока, — но все они дороги, медленны и неполны.

Честный вывод таков: *для домашнего обихода метаданные скрыть трудно*. Оттого разумнее не полагаться на их сокрытие, а помнить, что они есть, — и выбирать пути сообщения сообразно этому.

ГЛАВА ТРИДЦАТЬ ПЯТАЯ

Не изобретай своего шифра

Правило, которое всякий знающий повторяет новичку и которое всякий новичок нарушает.

> Всякий может придумать шифр,
> которого сам не сумеет вскрыть.
> Это не говорит о шифре ничего.

Слова эти принадлежат Шнайеру и суть точная правда. Свой шифр кажется крепким оттого лишь, что сочинитель не знает, с какой стороны его ломают, — а разбиратели знают.

Отчего же нельзя? Оттого, что стойкость устанавливается не доказательством, а *годами открытого разбора*. Нынешние шифры принимались по всесветным состязаниям, где сотни людей годами пытались их сломать; уцелевшие и служат.

То же и о собственном исполнении известного шифра: правильная запись формул не даёт защиты от побочных путей, от дурной случайности, от повторённого разового числа. Оттого берут готовые проверенные библиотеки, а не пишут своё.

Правило же для читателя короче: *употребляй общепринятое и обновляй его*. Собственная выдумка в этом деле есть не смелость, а неосторожность — и притом такая, о которой узнаёшь слишком поздно.

ГЛАВА ТРИДЦАТЬ ШЕСТАЯ

Чего тайнопись не может

Соберём пределы: они определяют, на что можно рассчитывать, а на что нет.

Она не скрывает факта переписки и не прячет метаданных.

Она не защищает прибор. Если в вашем устройстве чужая программа, она прочтёт написанное до шифрования и после расшифрования. Шифр защищает сообщение в пути и на хранении, а не работающий прибор.

Она не защищает от собеседника и от того, кому вы сами дали ключ.

Она не устоит против принуждения. Ключ отдают под давлением; никакая длина ключа этого не меняет.

Она не заменяет порядка. Копии, сроки, кто имеет доступ, что делать при утрате ключа — всё это устраивается людьми, а не шифром.

И она не вечна. Перехваченное сегодня хранится и может быть прочтено завтрашними средствами. Оттого для долгих тайн выбирают с запасом — и оттого же для житейских нужд запас этот не нужен.

ГЛАВА ТРИДЦАТЬ СЕДЬМАЯ

Тайна и власть

Спор о том, дозволительно ли гражданам иметь тайну, которой не может прочесть государство, идёт с тех пор, как шифры вышли из посольств в обиход. Изложим его честно, обеими сторонами.

Довод власти. Тайна укрывает не только честного: ею пользуются злоумышленники, и следствие оказывается бессильно там, где прежде помогала выемка почты. Отсюда требование «законного доступа» — особого ключа для властей.

Довод против. Ключ, существующий для одних, существует для всех: он может быть украден, продан, применён иным правительством. Устройство с нарочно оставленной дверью не бывает безопасным — это не мнение, а следствие устройства.

Из истории. В девяностые годы в Америке шифры причисляли к вооружению и запрещали к вывозу; предлагался и особый чип с ключом у властей — в нём вскоре нашли изъян. Ограничения были сняты, и нынешняя сеть выросла на открытой тайнописи.

Что тут можно сказать твёрдо. Никакой запрет не отнимает шифра у решительного злоумышленника: способ известен и умещается на странице. Отнимается он лишь у обыкновенных людей — у переписки, у больниц, у переводов денег.

Оттого спор этот не о преступности, а о том, *какой ценою покупается доступ*. Цена же — ослабление защиты у всех разом, и это стоит понимать прежде, чем становиться на сторону.

ГЛАВА ТРИДЦАТЬ ВОСЬМАЯ

Правила пользующегося

Соберём правила, вытекающие из всей книги. Все они скучны и все действуют.

Употребляй общепринятое. Проверенные средства, а не самодельные; не отключай их ради удобства.

Обновляй. Большая часть взломов совершается через давно исправленные изъяны. Обновление есть главнейшее из действий и притом самое дешёвое.

Береги ключ отдельно. Ключ рядом с шифровкой — отсутствие шифра. Пароли — в хранилище; долгие ключи — в двух местах, чтобы не потерять.

Ставь второй ключ там, где можно: он спасает при краже пароля.

Не пересылай ключа тем же путём, что и тайну.

Проверяй имя в свидетельстве и не проходи мимо предупреждений: они и есть тот самый случай, ради которого всё устроено.

Помни о человеке. Спешка, страх и уважение к начальству вскрывают больше тайн, чем все разбиратели вместе взятые.

ГЛАВА ТРИДЦАТЬ ДЕВЯТАЯ

Что сделать сегодня

Короткий порядок действий на один вечер, дающий больше, чем чтение десяти книг об этом предмете.

Первое. Завести хранилище паролей и перевести в него хотя бы важнейшие: почту, банк, служебные. Почта важнее прочего: через неё восстанавливают всё остальное.

Второе. Поставить подтверждение вторым способом на почту и на банк — лучше приложением или ключом-брелоком, чем сообщением на телефон.

Третье. Включить обновление везде, где оно выключено, и обновить прибор и оболочку.

Четвёртое. Включить шифрование хранилища на переносном приборе и на телефоне: потерянный прибор без этого есть открытая книга.

Пятое. Завести запас: копия важного — в двух местах, одна из них не в доме; и запись, как войти в хранилище паролей, оставленная в надёжном месте для близких.

Последнее из перечисленного — не о тайне, а о порядке: *потеря ключа губит написанное вернее чужого любопытства*. Оттого запас есть часть ремесла, а не отступление от него.

ГЛАВА СОРОКОВАЯ

Заключение: ключ и привычка

Сведём книгу к тому немногому, что стоит держать в памяти без справок.

Тайна держится *ключом*, а не скрытностью способа. Полагай, что устройство известно противнику; всё, что стоит на «о моём приёме не догадаются», рушится в первый же день.

Стойкость есть *цена*, а не невозможность. Хороший шифр делает чтение непомерно дорогим; совершенным же бывает лишь одноразовый блокнот, и цена его совершенства — неудобство, делающее его почти непригодным.

Шифры ломаются не в устройстве, а в *употреблении*: повторённый ключ, одинаковые начала, ленивый оператор, поддельная случайность. История двух тысяч лет говорит об этом на всякой странице.

И слабейшее звено — *человек*: спешащий, доверчивый, уставший. Оттого лучшая защита есть та, при которой правильное действие оказывается и самым лёгким.

Прочее в этой книге есть подробность к сказанному. Кто, берясь за новое средство, спросит: *где здесь ключ, кто им владеет, что видно постороннему и что будет, если ключ пропадёт*, — тот владеет ремеслом, хотя бы не помнил ни одного шифра из названных.

ТАЙНОПИСЬ

Ключ, мера и привычка

Изложение в сорока главах

O.V.K — X.T.R

Набрано и свёрстано
для настольного издания
формата 148 × 210 мм