Ключи от тайны

Основы криптографии. Шифрование с помощью ключа

Юлия Волкова

Начало читайте в статье «**Тайны тайнописи**»

Иллюстрацию шифрования с помощью ключа можно увидеть практически в любом фильме «про шпионов», где самым ценным секретом сотрудника вражеской (или не вражеской) разведки является тот самый пресловутый ключ к шифровке. Поскольку ключ этот и у «Алекса», и у «Юстаса» должен быть, естественно, одинаковым, то для его передачи требуется надежный курьер. Однако любой, кому удастся этого курьера перехватить, подкупить или попросту обокрасть, сможет читать, изменять и фальсифицировать все, что было зашифровано, или, что более актуально в наши дни, заверено при помощи данного ключа. Задача «как доставить адресату секретный ключ без опасения, что его перехватят» не решена и до сих пор.

Почему же такое не «абсолютно надежное» средство сокрытия информации продолжает применяться? Потому, что у криптосистем, помимо надежности, имеются и другие важные параметры, например, скорость шифрования-дешифрования, которая при применении ключа достаточно высока (чего не скажешь об «абсолютно надежных» методах шифрования). Поэтому для сокрытия данных, которые вы храните сами, но опасаетесь, что они

попадутся на глаза постороннему, вполне пригодны крипторешения с секретным ключом. Но как средство передачи ценных данных методы эти могут оказаться довольно дорогими, главным образом из-за сложности передачи тайного ключа.

Откройте ключ

Проблема передачи ключа шифрования была решена в 1976 году, когда Уитфилд Диффи и Мартин Хеллман опубликовали статью «Новые пути криптографии», которая произвела в шифровальном сообществе настоящий бум. Они предложили **концепцию шифрования с открытым** (или асимметричным) **ключом**. Это была поистине революция, причем очень своевременная, поскольку ни один из известных в то время алгоритмов единственного вида — **симметричного шифрования с секретным ключом** — не соответствовал новым потребностям, вызванным лавинообразным ростом новых методов обмена сообщениями и, в частности, появлением глобальных сетей передачи информации.

Изюминкой новой идеи было предложение применить для шифрования односторонние функции, известные математикам еще со времен фараонов. Они обладают следующим свойством (сосредоточьтесь!): при заданном значении x относительно просто вычислить значение y=f(x), однако нет простого пути для вычисления значения x из известного y, даже если сама функция известна. Но если известен некий «потайной ход», то отыскание x не вызывает затруднений.

В схеме шифрования с открытым ключом применяется не один ключ, а пара: открытый (public key), используемый в процессе шифрования, и закрытый (private key), применяемый для дешифрации. Конечно, это не случайная пара случайных чисел, а пара, определенным образом взаимосвязанная. Ваш открытый ключ известен всему миру, а частный хранится в тайне. Любой, даже тот, о ком вы никогда и не слышали, может зашифровать предназначенные вам данные, воспользовавшись копией вашего открытого ключа. А вот прочитать их сможете только вы, поскольку задача выделения частного ключа из открытого нерешаема по определению.

Существует множество классов односторонних (или необратимых) функций, но далеко не всякая пригодна для использования в асимметричных криптосистемах. В самом определении необратимости присутствует неопределенность. Под необратимостью понимается не теоретическая необратимость, а *практическая невозможность вычислить обратное значение за обозримый интервал времени, используя современные вычислительные средства*.

Поэтому чтобы гарантировать надежную защиту информации, к системам с открытым ключом предъявляются два важных и очевидных требования. Во-первых, преобразование исходного текста должно быть необратимым и исключать возможность его восстановления на основе открытого ключа. И, во-вторых, невозможным на современном техническом уровне должно быть также и определение закрытого ключа на основе открытого.

Все системы, предлагаемые сегодня, опираются на один из следующих типов необратимых преобразований:

- разложение больших чисел на простые множители;
- вычисление логарифма в конечном поле;
- вычисление корней алгебраических уравнений.

Итак, если до 1976 года единственным способом пересылки секретной информации была симметричная криптография и организовать канал для передачи тайных ключей могли себе позволить только правительства, крупные банки и корпорации, то появление шифрования открытым ключом стало технической революцией, несущей стойкую криптографию в массы. Место дорогостоящего и труднореализуемого скрытого обмена заняла односторонняя функция.

Тогда, в конце 70-х, многие всерьез думали, что пришло время отправлять на заслуженный отдых связных и дипкурьеров, колесящих по планете и перевозящих ключи шифрования с угрозой для собственной жизни или свободы.

Современная история

Шифрование с открытым ключом представляет несомненный интерес, поскольку его легко применять, и оно решает ряд до его появления нерешенных проблем с авторизацией. Точнее, оно решает всего несколько таких проблем.

1. Идентификация пользователя. Мы пользуемся современными средствами связи, позволяющими отправителю оставаться неизвестным, но хотим быть уверенными в том, что тот, с кем мы общаемся, — действительно тот, за кого себя выдает. Для этого используется протокол идентификации. Таковых существует великое множество, и основаны они, в большинстве своем, на принципах RSA или дискретного логарифмирования.

2. Аутентификация документа. Автор удостоверяет документ при помощи цифровой подписи. Операция подписи добавляет к сообщению несколько бит, которые являются результатом некоей операции над самим документом и сведениями об авторе, биты эти, как правило, хэшируются с использованием одного из известных алгоритмов MD5 или SHA. Более того, любой, кто имеет доступ к документу, должен иметь и возможность проверить, действительно ли подпись под ним поставлена автором. Для этого используются схемы подписи, наиболее известной среди которых является Elgamal, — также построенная на решении задачи дискретного логарифмирования.

3. И, кроме того, как и шифрование с секретным ключом, шифрование с открытым ключом является криптосистемой, гарантирующей **конфиденциальность информации**.

Известно множество криптосистем с открытым ключом — это Elgamal (названная в честь ее изобретателя Тахира Эльгамаля), Diffie-Hellman (названная, правильно, в честь ее создателей), DSA — Digital Signature Algorithm (изобретенный Дэвидом Кравицом).

Наилучший пример криптосистемы с открытым ключом (и, несомненно, простейший) появился двумя годами позже, в 1978 г. Тогда извилистые коридоры зеркального лабиринта, в которых плелась паутина чистой математики и черной магии криптографического научного искусства, делают новый поворот. Его фирменный знак — статья Роналда Л. Ривеста, Ади Шамира и Леонарда Адлемана об изобретенной ими системе шифрования RSA. Статья подробно описывала алгоритм шифрования, основанный на математической сложности разложения числа на целочисленные множители. Частный ключ создается из тройки чисел **(p, q, d)**, где **p** и **q** — простые числа примерно одного размера, а **d** — простое число, связанное с **p–1** и **q–1**. Открытый ключ создается из пары **(n, e)**, где **n=pq**, а **e** — находится из выражения **ed=1 mod(p–1)(q–1)**.

Предположим, вам требуется передать некое сообщение, зашифрованное при помощи открытого ключа вашего адресата **(n, e)**. Вы сначала преобразуете исходное сообщение в целое число **m**, меньшее чем **n**, затем выполняете вычисления **c=me mod n** и передаете результат **c** адресату. Тот, имея частный ключ **(p, q, d)**, выполняет новые вычисления **cd mod n=med mod n=m**, получив в итоге исходное сообщение.

В алгоритме RSA секретной лазейкой является односторонняя функция, которая связывает целое число **x<n** с величиной **xe mod n**.

Авторы пообещали премию в сто долларов тому, кто первым расшифрует RSA-шифрованную фразу

«96861375462206147714092225435588290575999112457431987469512093081629 82251457083569314766228839896280133919905518299451578151 54».

Единственное, что требовалось для этого, — разложить на два сомножителя 129-значное число, приведенное в той же статье.

Это было сделано только через 17 лет. Для того чтобы расшифровать фразу The magic words are squeamish ossifrage, команде из 600 человек потребовалось 220 дней работы и1600 компьютеров, связанных через интернет. Я подозреваю, что затраты несколько превысили размер премии.

В отличие от RSA метод Эль-Гамаля, как и алгоритм Диффи-Хелмана, основан на проблеме дискретного логарифмирования. Вспомните школьные уроки математики. Мы достаточно легко (при помощи ручки и бумаги) возводили число в степень, а вот для восстановления аргумента функции по значению (то есть для нахождения логарифма) пользовались специальными таблицами, логарифмической линейкой или, позднее, калькулятором.

Не менее известны также криптосистемы на основе эллиптических кривых. Эллиптическая кривая — это множество точек **(x, y)**, описываемое уравнением:

y2 = x3 + ax + b,

а также бесконечно удаленная точка. Для точек на кривой довольно легко вводится операция сложения, которая играет ту же роль, что и операция умножения в криптосистемах RSA и Эль-Гамаля.

Задачу дискретного логарифма на эллиптической кривой можно описать так: дана точка **G** на эллиптической кривой порядка **r** (**r** — количество точек на кривой) и другая точка **Y** на этой же кривой. Нужно найти единственную точку **x** такую, что **Y** есть **x**-я степень **G**.

В каждой избушке — свои погремушки

Вот уже почти три десятилетия заинтересованные стороны наблюдают за развитием отношений между традиционной (конвенциальной) и асимметричной криптографией. И отношения эти, надо сказать, весьма непросты. Всплеск эйфории после появления асимметричной криптографии, ощущение, что теперь все под контролем и можно решать массу новых задач, продолжались лет пять, пока строились теоретические модели.

Практических задач в то время не решали, поскольку вели бюрократические игры с правительствами, возражавшими против такой «**криптографии для всех**». Противодействие государственных структур вполне понятно. Спецслужбы опасались не только безнаказанной торговли государственными секретами — пойди найди, что там было зашифровано открытым ключом и передано через интернет некоему X, проживающему в стране N. Несомненно, что во всем этом им не нравилась также невозможность перлюстрировать переписку — «черным кабинетам» тут работы не оказалось.

Когда игры закончились с незначительным перевесом в пользу государств, началась реальная работа. Все складывалось (точнее, перемножалось) отлично. На бумаге. На практике же обнаружились «овраги» на путях обмена открытыми ключами. Вот тут-то и пришел конец радужным надеждам. Возникла чрезвычайно серьезная проблема защиты открытого ключа. Ведь система работает правильно, только если используемый вами открытый ключ действительно принадлежит тому, кому предназначено сообщение. Если же ключ подделан, то послания ваши будет читать кто-то другой. В задачке

спрашивается, как проверить, какой ключ у вас в руках, — настоящий или поддельный? И вот тут-то чистая математика разложения на сомножители снова запутывается в абсолютно «ненаучной» проблеме, причем не менее сложной, чем в симметричной криптографии. Тамошняя внекриптографическая проблема — нахождение сверхнадежного канала для обмена ключами. Здесь — не менее заковыристая проблема достоверности ключа.

Защита информации как защита от подделки

В асимметричных криптосистемах вам не надо предохранять открытые ключи от раскрытия. Наоборот, вы заинтересованы в их широкой доступности. Но если ключ доступен всем, где гарантия, что это не фальшивка? Вот оно — самое слабое место криптосистем с открытым ключом. Кто докажет мне, что именно этот открытый ключ принадлежит именно этому человеку?

Итак, каков сценарий процесса?

В идеале — все элементарно. Если вы собираетесь написать кому-то секретное письмо, то загружаете открытый ключ адресата с сервера ключей, шифруете с его помощью письмо и отправляете его по электронной почте.

Не в идеале — в игре появляется третий участник, который некоторое время назад создал свой открытый ключ с идентификатором вашего потенциального адресата и подменил на сервере настоящий ключ на свою фальшивку. Вы, ни о чем не подозревая, использовали подделку. Теперь злоумышленник может перехватить и расшифровать ваше сообщение. Он даже может перешифровать письмо правильным открытым ключом и отправить по назначению, так что и малейшего подозрения ни у кого не возникнет. Просто, как в «черном кабинете», — отпарили конверт, прочли письмо, заклеили и вернули на почту.

Единственный способ избежать подобных ситуаций — получать открытые ключи непосредственно от их обладателей, то есть мы возвращаемся к проблеме защищенного канала передачи ключа.
Другой вариант — получить ключ от доверенного лица, о котором вам известно, что оно имеет достоверную копию требуемого открытого ключа. Этот посредник может даже удостоверить целостность ключа своей подписью, зашифрованной при помощи собственного частного ключа, то есть создать подписанный сертификат достоверности ключа. Он может также хранить и передавать желающим достоверную копию вашего открытого ключа, выступая между вами и вашими корреспондентами в качестве доверенного представителя. Придуманы и действуют различные по сложности реализации и надежности обороны структуры обмена открытыми ключами, изобретаются все более изощренные инструкции по «самообороне» от подделки вашего ключа и от использования подделанных ключей. Комплекс предлагаемых мер сильно напоминает детские сказки, в которых ключ — в яйце, яйцо — в утке, утка — в норе, нора — в горе, гора — на дне моря, и так до бесконечности. Вопрос о том, как защитить открытые ключи от подделки, — это непрестанная головная боль всей асимметричной криптографии, и большая часть всей системы завязана именно на разрешении этой единственной задачи, которая давно уже переросла в отдельную индустрию «защиты ключей для защиты информации».

Но если бы сложности асимметричных систем на этом и заканчивались, то можно было бы надеяться, что однажды появится такой сверхстойкий способ защиты, что шифрование раз и навсегда станет абсолютно устойчивым. К сожалению, не все так просто. Если в симметричных системах гарантией надежности служит скрытность самого шифра, то в асимметричных системах гарантией надежности шифра служит вычислительная сложность отыскания исходных переменных односторонней функции. Можно ли всерьез доверить свои нешуточные секреты подобным средствам? А что, если какой-нибудь непризнанный (или признанный) гений выдумает способ быстрого разложения чисел на множители? А что, если такой способ уже есть — где-нибудь в секретных лабораториях MI-6?

Новые решения — на стыке старых

В ходе единства и борьбы двух направлений криптографической науки родилась новая гибридная криптосистема с нескромным названием Pretty Good Privacy (PGP), объединившая в себе лучшие стороны как традиционной криптографии, так и шифрования открытым ключом. В алгоритме PGP удобство шифрования открытым ключом дополняется скоростью симметричных алгоритмов, которые работают почти в тысячу раз быстрее асимметричных. Шифрование открытым ключом, в свою очередь, снимает проблемы скрытой передачи ключей. Происходит некая синергетика — используемые совместно алгоритмы взаимно дополняются и улучшаются без какого бы то ни было ущерба безопасности.

В процессе PGP-шифрования информация сначала сжимается. Сжатие не только уменьшает время передачи и экономит объем памяти, но и, что гораздо важнее, повышает криптостойкость. Почему? Дело в том, что многие методы криптоанализа основаны на поиске устойчивых сочетаний (так называемых паттернов), которые всегда встречаются в тексте. Сжатие уменьшает их число, чем существенно улучшает сопротивляемость криптоанализу.

Затем PGP создает одноразовый ключ сеанса — симметричный ключ, применяемый только для одной операции. Ключ этот представляет собой псевдослучайное число, сгенерированное компьютером из импульсов, полученных им от случайных движений мыши и нажатий клавиш. При помощи этого ключа и очень надежного, быстрого симметричного алгоритма PGP шифрует сжатое сообщение, получая в итоге зашифрованный текст. После этого она шифрует и сам ключ сеанса, на этот раз по асимметричной схеме при помощи открытого ключа адресата. Данные о ключе сеанса передаются вместе с зашифрованным текстом.

Дешифровка выполняется строго в обратном порядке. Сначала PGP-программа получателя «вынимает» из сообщения данные о ключе сеанса, дешифрует его, используя закрытый ключ, и только потом дешифрует само сообщение.

Еще раз о ключах

Ключ — это, как правило, о-о-очень много бит (попробуйте представить себе число из 2048 бит), используя которые криптоалгоритм формирует зашифрованный текст. В асимметричной криптографии, как и в традиционной, разумеется, шифр тем надежнее защищен, чем больше ключ.

Однако размер асимметричного открытого ключа и размер тайного ключа в симметричной криптографии абсолютно несопоставимы. Так, считается, например, что 80-битный секретный ключ эквивалентен по стойкости 1024-битному открытому ключу. Стойкость 128-битного секретного ключа равна стойкости 3000-битного открытого. Несомненно, чем ключ больше, тем безопасность выше, но вряд ли можно сравнивать абсолютно различные алгоритмы, применяемые в каждом из типов криптографии. Все равно, что спрашивать — кто сильнее, кит или слон.

Поскольку пара (открытый — закрытый) ключей математически связана, то извлечение частного ключа всегда остается возможным, это только вопрос времени и вычислительных мощностей. Следовательно, нам нужен не просто сверхдлинный ключ, а ключ оптимальный: достаточно длинный, чтобы быть стойким, но достаточно короткий, чтобы не задерживать работу на века. Процесс выбора оптимального ключа основан на предположении о том, кто может попытаться «прочитать ваши файлы», насколько он настойчив, каким временем располагает, каковы его ресурсы.

Чем больше ключ, тем больше времени потребуется на его вскрытие. Если вы хотите спрятать государственный секрет на десятилетия, вы, вероятно, остановите свой выбор на очень длинном ключе. Но не обольщайтесь. Кто знает, сколько потребуется времени завтрашним компьютерам, чтобы вскрыть ваш ключ? Не забывайте, что было время, когда чрезвычайно надежным считался 56-битный симметричный ключ. А еще раньше полностью полагались на шифр Цезаря…

Цифровой автограф

С самого своего рождения, с шифра Цезаря и до PGP, криптография была поставлена на службу охраны секретов. Однако современный стремительный век, век, когда промедление в заключении сделки бывает началом разорения, а неподписанный вовремя контракт может оставить без работы все принадлежащие вам заводы, газеты и пароходы, все настойчивее требовал средств, позволяющих официальным лицам подписывать бумаги — финансовые договоры или политические соглашения — находясь от этих бумаг за тридевять земель. Требовалось, во-первых, обеспечить достоверность поставленной подписи (авторизация), убедиться, что сообщение не было изменено в пути (целостность), а также предотвратить возможность отказа отправителя от подписанной информации в будущем (неотречение).

Решение всех трех проблем называется электронной цифровой подписью (ЭЦП). Цифровая подпись, хотя и является, по своей сути, криптографической конструкцией, отлична от шифров, от нее требуется нечто большее, чем просто защита открытого текста.

ЭЦП служит той же цели, что и собственноручная подпись на бумажном носителе. Однако ручную подпись очень легко подделать. ЭЦП же подделать практически невозможно, кроме того, она делает еще и то, чего «бумажная» подпись не умеет, — подтверждает целостность информации и личность подписавшего.

Электронная подпись применяется сегодня гораздо чаще, чем чистое шифрование. Так, например, менеджера интернет-магазина, куда вы только что перевели со своего счета 10 000 долларов, не интересует, что кто-то узнает об этой покупке, но ему надо быть абсолютно уверенным, что он имел дело именно с вами. Равно как и вы желаете доказательств того, что перевели свои денежки в нужное место.

Интересно, что если бы электронную подпись изобрели во времена царя Салтана, то ткачиха с поварихой напрасно потеряли бы время, перехватывая письма Царицы и Салтана и подменивая грамотки в суме гонца.

Что дальше?

При слове «шифр» многие вспомнят Штирлица или Мату Хари, «пляшущих человечков» Конан Дойла или «Золотого жука» Эдгара По. Но, постойте, достижениями современной криптографии мы пользуемся ежедневно, иногда даже не подозревая об этом. Например, открывая доступ в интернет, программа-навигатор может спросить, нужен ли режим шифрования, и если вы ответите «да», она начнет создавать ключ шифрования. Второй не менее яркий пример — это банковские карточки. Те карточки, что лежат в наших с вами бумажниках, давно уже не магнитные — в них вшит процессор, который выполняет криптографические функции. Третий пример — цифровая подпись. Мы пользуемся ее возможностями, зачастую не осознавая, что это такое, и, тем более, не

понимая ее математических основ. Но, может, эти основы нам и ни к чему? Достаточно того, что мы признаем исключительное значение ЭЦП всегда, когда речь идет об использовании в бизнесе электронных документов.

Место криптографии сегодня — не только в офисе или банке, в государственном учреждении или войсковой части. Ее место — везде, где используются электронные средства коммуникаций. Еще сто лет назад все общение было частным. Если вам казалось, что вас подслушивают, вы могли уйти в другую комнату или отойти в сторонку. До недавнего времени для того, чтобы поинтересоваться, что это такое вы пишете вашей бабушке в Сестрорецк, требовалось затратить некоторое время и потрудиться перехватить, отпарить и вскрыть бумажный конверт. Для того чтобы узнать, о чем это вы болтаете по вечерам со своей девушкой, требовалось подключиться к телефонному кабелю и прослушивать, а, возможно, и стенографировать разговор. Для крупных операций «ручной» перехват был непрактичен и применялся только в тех случаях, когда цель оправдывала затраченные средства.

Но все изменилось с изобретением радио и цифровой связи. Теперь мы общаемся электронно. Ваши разговоры с девушкой никак не защищены. Звонок с мобильного телефона может быть перехвачен. Электронная переписка с бабушкой еще менее безопасна. Ни для кого не секрет, что современные средства позволяют — в огромных масштабах и незаметно — автоматически сканировать e-mail, отыскивая в огромном потоке некие ключевые слова.

Мне кажется, что, учитывая рост скоростей вычислений и вероятность появления искусственного интеллекта (или хотя бы того, что сегодня им называют), совсем не лишне ознакомиться с принципами и современными достижениями криптологии — науки о тайнописи и способах ее прочтения. Потому что вовсе не исключено, что в ближайшее время наши компьютеры будут общаться друг с другом лишь при помощи цифровых заклинаний, недоступных человеческому пониманию.

Криптография становится обычным делом, и с расширением областей ее применения (цифровая подпись, аутентификация и подтверждение подлинности и целостности электронных документов, безопасность электронного бизнеса, защита информации, передаваемой через интернет, и др.) будет возрастать и ее роль. Всем нам потребуется познакомиться с криптографией, и в будущем она станет «третьей грамотностью» наравне со «второй грамотностью» — владением компьютером и информационными технологиями. Помните, еще в документах древних цивилизаций говорилось, что тайнопись является одним из 64-х искусств, которым следует владеть как мужчинам, так и женщинам.

Тайны тайнописи

В ходе эволюции человек учился защищаться от холода, голода, диких зверей и капризов погоды. На каком-то из этапов своего развития он понял важность своевременного получения достоверной и правильно отобранной информации. И, наконец, осознал необходимость информацию эту защищать.

В условиях соперничества (военного, научного или коммерческого — не важно) знания существуют в двух формах — «у меня и у моего врага». И для того чтобы победить или хотя бы выжить, первую форму желательно довести до максимума, а вторую — до минимума. Защищая свою информацию, мы стремимся сохранить в тайне имеющийся у нас запас знаний, а рассекречивая чужую — увеличить этот запас за счет конкурентов.

История защиты информации начинается, по всей вероятности, где-то в то время, когда люди начали учиться общаться при помощи переписки. Естественно, им потребовались способы обеспечить ее секретность. Точных дат и достоверных данных о тайнописи в древности никто не приводит. Известно, например, что в Древней Греции голову раба брили, писали на его голове, ждали, когда волосы вновь вырастут, после чего

отправляли с поручением к адресату. Что и говорить, время было такое — расстояния большие, скорости малые, плюс-минус два месяца роли не играли. Знатокам поэзии хорошо известен такой довольно широко используемый в то время прием тайнописи, как акростих, в котором скрываемое сообщение образуют начальные буквы стихотворных строк.

Для создания скрытого сообщения можно применять специальные технические средства (передать в конкретную точку пространства по радиоканалу остронаправленным лучом, предельно сжать информацию и передать в мгновенном импульсе, написать бесцветными чернилами, проявляющимися лишь после некоторого физического или химического воздействия). Кто из нас не читал, как в царских застенках революционеры писали письма молоком…

Все вышеперечисленные и подобные им способы защиты информации относят к**стенографическим** (или **симпатическим**), при которых сама информация остается неизменной, ее стараются сделать невидимой и тем самым скрыть факт ее передачи. Методы эти развивались и усложнялись вместе с ходом технического прогресса. Вершиной развития этих методов можно считать, вероятно, технологию создания сверхминиатюрных фотографий — так называемых микроточек, — которая

появилась после Втор ой мировой войны. Такая микроточка размером с точку печатного текста могла содержать сотни документов, и найти ее в книге, журнале или газете было ненамного проще, чем иголку в стоге сена. Современная микросхемотехника сверхбольшой интеграции позволяет записать текст так мелко, что без электронного микроскопа прочесть его будет невозможно. Широкое распространение компьютеров позволяет применять другие способы сокрытия информации. Например, «нестандартное» форматирование дисков, запись на технические дорожки, замешивание информации в большие объемы данных и т. д.

Однако *явным недостатком* симпатических методов является то, что скрытность созданных с их помощью сообщений обеспечивается лишь на данном этапе развития техники. Любой способ создания симпатического текста будет вскоре разрушен. А что за секретность без гарантии стойкости?

Хитросплетения разума

Интересно, что в глубокой древности тайнопись считалась одним из 64-х искусств, которым следует владеть как мужчинам, так и женщинам. Сведения о способах шифрованного письма можно обнаружить уже в документах древних цивилизаций Индии, Египта, Месопотамии. Среди самых простых — **иероглифическое письмо**, написание знаков не по порядку, а вразброс по некоторому правилу.

Первое исторически достоверное применение технических средств шифровки приписывается древним грекам и датируется примерно V–VI веками до нашей эры. Таким техническим средством был специальный брусок, называемый «сцитал». Его оборачивали узкой полоской бумаги и писали сообщение вдоль бруска. Затем полоску снимали и отправляли адресату. Предполагалось, что прочесть сообщение, не зная толщины бруска — которая служила здесь ключом шифрования — было невозможно.

Кроме того, Эней в работе «Об обороне укрепленных мест» описывает так называемый «**книжный шифр**» и способ перестановки букв в тексте по специальной таблице. Известна также система шифрования под названием «**квадрат Полибия**», в которой каждая буква заменяется парой чисел — ее координатами в квадрате 5x5, куда предварительно в заранее заданном порядке вписаны буквы алфавита.

Уже тогда шифрованная переписка использовалась не только полководцами, но и церковью, и учеными. Жрецы шифровали тексты прорицателей, а ученые — свои открытия. Например, у Э. Шюре в книге «Великие посвященные» встречается фраза о том, что «с великим трудом и большой ценой добыл Платон один из манускриптов Пифагора, который никогда не записывал свое учение иначе, как тайными знаками и под различными символами».

Классический пример с шифром Цезаря описан во всех учебниках по криптографии: не доверяя гонцам, Юлий Цезарь шифровал свои депеши, используя способ, который впоследствии получит название **шифра прямой замены**. В своих письмах он заменял каждую A на D, каждую B на E, и т. д. И его послание мог дешифровать только тот, кто знал правило «смещения на 3».

Словом, к началу нашей эры люди знали о криптографии довольно много и использовали ее достаточно широко. Последующие 19 веков были потрачены на изобретение более или менее хитроумных способов шифрования, надежность которых во многом была призрачной и зависела, главным образом, от того, насколько им доверяли те, кто ими пользовался.

Довольно мало сведений о применяемых шифрах можно найти до эпохи Возрождения. Известен ряд **значковых шифров**, при котором буквы открытого текста заменяются специальными знаками (помните «танцующих человечков» Конана Дойля?). Таким является шифр Карла Великого, применявшийся в IX веке нашей эры. Известен так называемый «**еврейский шифр**», в котором замена букв осуществляется по подстановке, порядок которой определяется так: алфавит разбивается на две половины, буквы второй половины пишутся под буквами первой половины в обратном порядке. Буквы текста заменяют теми, которые стоят с ними в паре. Проверьте: применив этот метод к зашифрованному сообщению, вы получите исходный текст.

Арабский след

Период расцвета арабских государств (VIII век н. э.) — поистине эпоха великих открытий в области криптографии. Не зря ведь слово «шифр», как и слово «цифра», имеет арабские корни. В появившейся в 855 году арабской «Книге о стремлении человека разгадать загадки древней письменности» описываются различные системы защиты информации, в том числе и несколько классических шифралфавитов. Один такой шифралфавит, называвшийся «**дауди**» (по имени израильского царя Давида), использовался для шифрования трактатов по черной магии. Он был составлен из видоизмененных букв древнееврейского алфавита.

Следующие сведения о криптографии также относятся к арабскому миру. В 1412 году на свет появляется произведение Шехаба Калкашанди — 14-томная «Энциклопедия всех наук», содержащая и сведения о методах засекречивания переписки. Раздел под общим заголовком «Относительно сокрытия в буквах тайных сообщений» состоял из двух частей: одна касалась символических действий, намеков и иносказаний, во второй описывались симпатические чернила и криптология. Здесь не только впервые подробно

рассказывалось о **шифрах перестановок** и **шифрах замены**, но и упоминался шифр, использующий несколько замен букв открытого текста. Но не этим известна книга. Все остальное затмевается первым в истории описанием криптоанализа на основе частоты появления знаков в исходном и шифрованном текстах. Автор даже приводит список букв арабского алфавита с указанием частоты их встречаемости в текстах Корана. Уже тогда частотный анализ сообщения позволял достаточно просто раскрывать шифры простой подстановки.

К сожалению, криптоаналитические достижения Калкашанди арабами были вскоре забыты. Иначе невозможно объяснить исторический курьез, имевший место спустя почти 300 лет. Судите сами. В 1600 г. марокканский султан направил в Англию посольство, глава которого вскоре отослал на родину сообщение, зашифрованное без всяческих затей — шифром простой замены. Письмо это каким-то образом попало в руки одного араба, который, судя по оставленной им записке, потратил 15 лет на то, чтобы понять смысл написанного. Пятнадцать лет! Подобную задачу Калкашанди решил бы за несколько часов.

Видимость скрывает реальность

Вплоть до эпохи Возрождения черная магия и криптография в сознании людей были крепко связаны. Иного и быть не могло, ведь криптографию в Европе изначально использовали для того, чтобы скрыть от любопытных глаз содержание документов, описывающих колдовские рецепты, заговоры, гадания и заклинания. Алхимики засекречивали с помощью шифров формулы философского камня. В таких недоступных для посторонних областях, как астрология и алхимия, каждая планета и каждое химическое вещество обозначались как всем понятными знаками, так и схожими с криптографическими таинственными символами.В результате как заклинания и магические формулы вроде «абракадабры», так и зашифрованные письма походили с виду на чепуху, но в действительности имели глубокий смысл.

Можно как угодно относиться к суеверным страхам тех веков, связанным с шифрованием, но что действительно напоминает черную магию, так это криптоанализ, который даже внешне очень похож на гадание. Мне до сих пор извлечение смысла из шифрованного текста представляется точно таким же колдовским делом, как получение знаний из расположения звезд и планет, узора линий на ладони, внутренностей овец, рисунка из кофейного осадка на стенках чашки.

В эпоху Возрождения, в пору буйного расцвета наук и ремесел в итальянских городах-государствах, шифры стали широко применяться учеными для защиты приоритета научных открытий. Применявшиеся шифрсистемы были предельно просты — фразы писались по вертикали или в обратном порядке, гласные пропускались или заменялись точками, использовались иностранные алфавиты (например, древнееврейский и армянский), каждая буква открытого текста заменялась следовавшей за ней буквой.

Интересно, что в то время, когда простые люди шифрование считали колдовством и ведьмачеством, основные работы в области криптографии и криптоанализа выполнялись в лоне католической церкви. Так, в XIV веке на свет появляется книга сотрудника папской канцелярии Чикко Симонетти, где он подробно описывает шифры замены, в которых, для выравнивания частоты встречаемости букв в шифртексте, гласным буквам ставится в соответствие не один знак, а несколько. Здесь же впервые встречается описание так называемого «**лозунгового**» шифра, который в различных модификациях будет применяться и несколько веков спустя. Правило замены букв в нем определяется следующим образом: под алфавитом пишется ключевая фраза — лозунг, а затем буквы, которые в лозунге не встречаются.

Почти век спустя появляется книга «Трактат о шифрах», автор которой, Габриэль де Лавинд, секретарь папы Клементия XII, дает описание нового типа шифра, предполагающего замену букв несколькими символами, количество которых пропорционально встречаемости букв в открытом тексте. Имена, должности,

географические названия рекомендуется заменять специальными знаками. Это был самый ранний образец **номенклатора** — гибридной системы шифрования, которой в последующие 450 лет суждено было распространиться по всей Европе.

В 1466 году опять-таки в папскую канцелярию представляется трактат о шифрах архитектора и философа Леона Альберти, где предлагается способ маскировки сообщения в некотором безобидном вспомогательном тексте. Здесь же Альберти предлагает свой собственный шифр с нескромным названием «**шифр королей**». По сути, Альберти придумал **многоалфавитную замену** — новый вид шифрования, используемый в большинстве современных шифрсистем.

По идее Альберти, первую букву сообщения следовало заменять по одному признаку (алфавиту замены), например, a = p, b = m, c = f, ..., вторую — по второму, например, a = l, b = t, c = a, ..., третью — по третьему, например, a = f, b = x, c = p, ... и так далее. Порядок шифралфавитов устанавливался в соответствии с известным ключом. Многоалфавитные шифры явились большим шагом вперед, но на практике не использовались в течение более четырех столетий. Почему? Да потому, что многоалфавитная замена по сравнению с номенклатором отнимала слишком много времени, а «незначительная» ошибка при письме, например, пропуск буквы, приводила к таким искажениям, что получателю сообщения было не суждено расшифровать его даже при наличии верного ключа. Несколькими годами позже, значительно опередив свое время, Альберти изобрел **код с перешифровкой**, который стал широко применяться в странах Европы лишь 400 лет спустя.

В 1518 году в Германии появляется первая печатная книга по криптографии «Полиграфия». Ее автор, аббат Иоганнес Тритемий, развивает идею Альберти о многоалфавитной замене. Алгоритм шифрования выглядит следующим образом: создается таблица замены, первой строкой которой является собственно сообщение, второй — алфавит, третьей — алфавит, сдвинутый на один шаг, и т. д. При шифровании первая буква сообщения заменяется буквой, стоящей под ней в первой строке, вторая буква — буквой, стоящей во второй строке, и т. д.

В России, хотя тайнопись использовалась уже в XII–XIII веках, официальной датой появления криптографической службы считается 1549 год (царствование Ивана IV), а именно образование «посольского приказа», при котором имелось «цифирное отделение». Шифры использовались такие же, как на западе — значковые, замены, перестановки. Петр I позднее полностью реорганизовал криптографическую службу, создав Посольскую канцелярию. В это время появляются специальные коды для шифрования — «цифирные азбуки».

В начале XVI века Маттео Арженти, криптограф папской канцелярии, изобрел код, согласно которому могут заменяться не только буквы, но и слоги, слова, даже целые фразы. Где-то в это же время появляется и числовой код.

Следующим этапом развития криптографии можно считать 1563 год, когда в своей книге «О тайной переписке» итальянский естествоиспытатель Джованни Порта описал **биграммный шифр**, в котором осуществляется замена не одной буквы, а пары букв. В своей книге Порта приводит примеры списков вероятных слов из различных областей знания, существенно предвосхитив то, что впоследствии криптологи назовут «**методом вероятного слова**». Примерно в то же время французский посол в Риме Блез Виженер, познакомившись с трудами по криптографии, пишет книгу «Трактат о шифрах» (1585 г.), в которой он предлагает в качестве ключа применять открытый или шифрованный текст и высказывает мысль о том, что «все вещи в мире представляют собой шифр. Вся природа является просто шифром и секретным письмом». Позднее эту мысль повторят и Блез Паскаль, и отец кибернетики Норберт Винер.

Эра «черных кабинетов»

XVII век вошел в историю криптоанализа как эра «черных кабинетов». В это время в различных странах начали появляться первые службы дешифровки корреспонденции. В Англии Оливер Кромвель создает «Интеллидженс сервис», в состав которой входит подразделение по дешифровке. Не отстает и Франция. Там дешифровальное отделение было создано при Людовике XIV по предложению кардинала Ришелье. Его возглавил Антуан Россиньоль — автор **дипломатического шифра**, представляющего собой слогово-словарный код на 600 компонентов. Этот шифр французская армия будет использовать более ста лет. Известно, что даже Наполеон во время своих походов использовал шифры, являющиеся упрощенными вариантами шифра Россиньоля.

Не менее известен и «**шифр Ришелье**» — при его использовании текст сообщения разбивается на отрезки, буквы которых переставляются в определенном порядке. Россиньолю принадлежит также авторство известной доктрины о том, что «стойкость военного шифра должна обеспечить секретность донесения в течение срока, необходимого для выполнения приказа. Стойкость дипломатического шифра должна обеспечивать секретность в течение нескольких десятков лет».

В Германии создается специальное отделение под управлением графа Гронсфельда, который усовершенствовал **шифр Виженера**, заменив буквенный лозунг цифровым, цифры в котором обозначают число шагов, на которое букву шифруемого сообщения сдвигают вправо по алфавиту. Благодаря простоте применения этот шифр использовался в свое время чрезвычайно широко.

В России «черные кабинеты» действовали со времен правления императрицы Елизаветы. Так же, как в Англии и Австрии, они размещались в почтовых отделениях. В число их сотрудников входили специалисты по вскрытию конвертов и подделке печатей, переводчики и дешифровальщики.

Репутацией же самого лучшего «черного кабинета» по праву пользовался венский. Ежедневно в семь утра туда привозили почту, которая должна была утром доставляться иностранным посольствам в Вене. Письма вскрывали, растапливая сургучные печати, отмечали порядок страниц и передавали помощнику директора. Наиболее важные документы переписывались. Для экономии времени длинные письма читались вслух и записывались одновременно несколькими стенографистами. После копирования письма укладывались обратно в конверты, опечатывались поддельными печатями и уже к половине десятого утра возвращались на почту.

Скопированный материал попадал на стол к директору «черного кабинета», который отбирал особо интересную информацию и направлял ее ко двору, полицейским чиновникам, дипломатам и военачальникам. В штате «черного кабинета» работали переводчики со всех европейских языков, а когда появлялась потребность в новом языке, один из них срочно выучивал его.

Если же попадались шифровки, их подвергали криптоанализу. Шифры того времени представляют собой, в основном, коды различной степени сложности. Из других шифров заслуживает внимания так называемый «**масонский шифр**». Это довольно оригинальный значковый шифр, в котором знаки для замены букв извлекались из алфавита, написанного на двух крестах — прямом и косом.

От черной магии к чистой математике

В XVII—XVIII веках становится все более понятно, что защита информации — не столько искусство сочинения и отгадывания изощренных шифров, сколько точная наука. Все заметнее переход криптографии из области черной магии в область чистой математики. Мы почти ничего не знаем о том, занимались ли ведущие математики того времени проблемами шифрования и дешифрования, но есть данные, что некоторые из них владели криптографией. Среди них Блез Паскаль, сделавший ряд открытий в области комбинаторики и создавший метод индуктивного доказательства; Исаак Ньютон и Готфрид Лейбниц, разработавшие дифференциальное и интегральное

исчисление. Знаменитый английский философ Ф. Бекон предложил идею двоичного кодирования. Леонард Эйлер вел обширные исследования по перечислению и построению латинских квадратов, т. е. шифров многоалфавитной замены.

На протяжении первой половины XIX столетия непревзойденными трудами по криптологии считались работы Альберти и Порта. Изложенные ими концепции оставались актуальными до тех пор, пока в криптологии не происходило никаких существенных изменений. Связь поддерживалась с помощью гонцов, а основным видом шифрования оставался номенклатор. Но с изобретением С. Морзе в 1844 году телеграфа старые концепции быстро теряют свою актуальность. Рост скоростей передачи требовал увеличить скорость шифрования. Шифровальщики, вручную заменявшие буквы и слоги специальными символами, уже не могли справиться с нарастающим потоком информации.

Новые условия требуют новых идей

Прежде чем начать разговор о новых идеях, следует сказать несколько слов о мифической криптостойкости многоалфавитных шифров. Пока шифрование и дешифрация выполнялись вручную, многоалфавитность оставалась редким явлением, поскольку требовала чересчур много времени, и защитой многоалфавитности служила сама ее непопулярность. Используйся она чаще, и криптоаналитики, возможно, давно придумали бы способ дешифрации. Но мир того времени остановил свой выбор на номенклаторе, поэтому мифу о высокой криптостойкости многоалфавитных шифров была суждена долгая жизнь.

Эта жизнь длиною более четырех веков оборвалась в 1863 году, когда офицер прусской армии Фридрих Казисский опубликовал книгу «Искусство тайнописи и дешифрования», в которой изложил метод вскрытия многоалфавитного лозунгового шифра с повторяющимся лозунгом, который ранее считался абсолютно криптоустойчивым. Казисский предложил определять длину лозунга статистически, доказав, что расстояния между повторениями в шифртексте будут равны или кратны длине лозунга. После того, как число букв в лозунге определено, шифртекст разбивается на отрезки, равные длине лозунга, и задача сводится к вскрытию шифра простой замены, что не представляло особого труда для криптоналитиков того времени.

В 1883 году криптология получила новые идеи, изложенные в труде под названием «Военная криптография». Интересно, что его автор, Огюст Кергоффс,

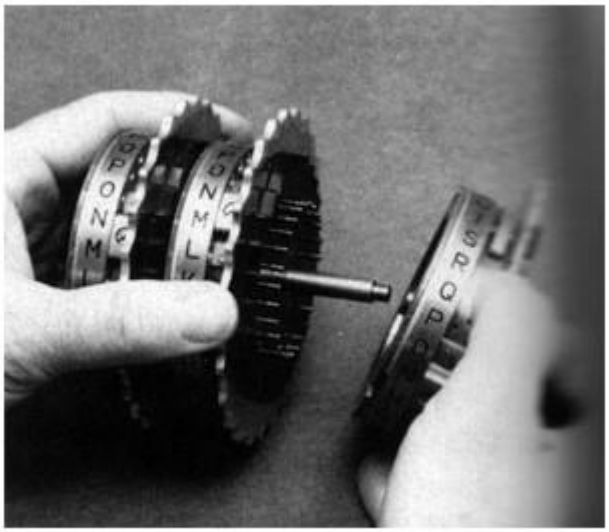
не был ни военным, ни профессиональным шифровальщиком, зато он преподавал иностранные языки и математику. Опираясь на знания в области лингвистики и математики, автор проводит сравнительный анализ шифров, на основе которого формулирует требования к шифрам и делает вывод, что практический интерес представляют только те шифры, которые остаются стойкими

даже при интенсивной переписке. Можно считать, что именно Кергоффс написал основы современной криптологии, один из главных принципов которой гласит, что стойкость криптографической системы зависит не от процесса шифрования, а от используемого ключа. Этот принцип не потерял своей актуальности и сегодня.

Не менее ценна мысль Кергоффса о том, что надежность шифра должны оценивать дешифровальщики. Разумеется, об этом догадывались и до него, но после закрытия «черных кабинетов» как-то позабыли. Во всяком случае, изобретатели новых шифров, вместо того чтобы вынести их на суд криптоаналитиков, стремились оценить их стойкость самостоятельно, подсчитывая число веков, необходимых для последовательного перебора всех возможных ключей, или старались доказать невозможность «пробить» какой-либо из элементов шифра. Кергоффс писал: «Я поражен тем, что наши ученые и профессора преподают и рекомендуют для применения в военное время системы, ключи к которым, несомненно, менее чем за час откроет самый неопытный криптоаналитик... Можно также полагать, что отсутствие серьезных работ по искусству прочтения тайнописи способствовало распространению самых ошибочных идей о стойкости наших шифрсистем».

Благодаря работам Кергоффса, во всех ведущих государствах мира уже в 80-х годах XIX века криптографию признают наукой и в обязательном порядке начинают преподавать в военных академиях. Для шифрования применяются **коды с перешифровкой**. Создаются и все шире используются механические шифровальные устройства. Однако в основе систем тех лет, как и в методах оценки их криптостойкости, математические принципы использовались недостаточно полно. Несмотря на это, революционные открытия в математике того времени сформировали фундамент для дальнейшего развития и усложнения систем шифрования и дешифрования. Зародившиеся тогда формальные языки и аксиоматические методы легли в основу тайнописи следующего века.

XX век — век двух мировых войн, век научно-технического прогресса, век социальных потрясений и передела государственных границ. На рубеже веков связь перестает быть исключительно почтовой, она становится электрической, появляется телеграф, а затем и радио. Это преобразило и криптографию, поскольку возможности доступа противника к шифрованному тексту расширились, появились возможности влиять на открытый текст. Вслед за изменением связи меняется и криптография, становясь сначала **электромеханической**, а затем **электронной**.



Во время Первой мировой войны главным (и зачастую единственным) средством шифрования были коды. Несмотря на то, что все участники боевых действий постоянно разрабатывали новые коды и улучшали старые, обеспечить их сохранность удавалось далеко не всегда, поэтому противники нередко были полностью осведомлены обо всем,

что содержалось в секретной переписке врага. С применением шифров связан ряд трагических событий, из которых упомянем лишь разгром двух русских армий — Ранненкампа и Самсонова в Восточной Пруссии в августе 1914 года, причиной которого была плохая организация закрытой связи, в результате чего переговоры по радио велись вообще без всякого шифра.

Война и радиосвязь полностью преобразили криптографию.

Шифрованный текст, переданный по радио, был доступен каждому, кто имел в своем распоряжении несложный приемник. И даже если этот текст нельзя было расшифровать сразу, — его можно использовать при анализе последующих сообщений. В этот период получили развитие методы дешифрования, основанные **на парах открытых и шифрованных текстов**; **на нескольких шифровках**, созданных с помощью одного ключа; **на переборе вероятных ключей**. Именно эти методы применялись англичанами для чтения секретной переписки немцев во время Первой мировой войны. Несмотря на то, что неоценимую помощь английским криптоаналитикам оказали водолазы, добывавшие кодовые книги с затонувших немецких подлодок, основой их работы был скрупулезный анализ перехваченных текстов. Находкой для криптографов было использование в качестве лозунгов пословиц, поговорок, патриотических призывов, а также стереотипные выражения, которые так любили употреблять в своих посланиях немецкие дипломаты. Если бы они только знали, как много информации дала взломщикам их кодов одна только фраза «Имею честь сообщить Вашему Превосходительству, что...»!

Все чаще использовались вероятностно-статистические методы, основанные на частоте появления знаков, биграмм, триграмм и т. д. И все же, методы работы криптоаналитиков оставались «человеческими» до 1917 года, до того момента, когда Гильберт Вернам предложил новый способ шифрования.

Год 1917 — революция в шифровании

В то время для передачи сообщений все шире и шире использовались телетайпы. Поэтому требовались методы, позволяющие шифровать текст не до того, как он попадает к телеграфисту, а непосредственно в момент передачи, и, соответственно, расшифровывать в момент приема. Очень хотелось поручить это дело машине. Как оказалось, колебания тока в линии передачи можно легко записать с помощью осциллографа и затем преобразовать в буквы передаваемого сообщения. Изменив соединения проводов телетайпа, телеграфисты получали сообщение, зашифрованное методом одноалфавитной замены.

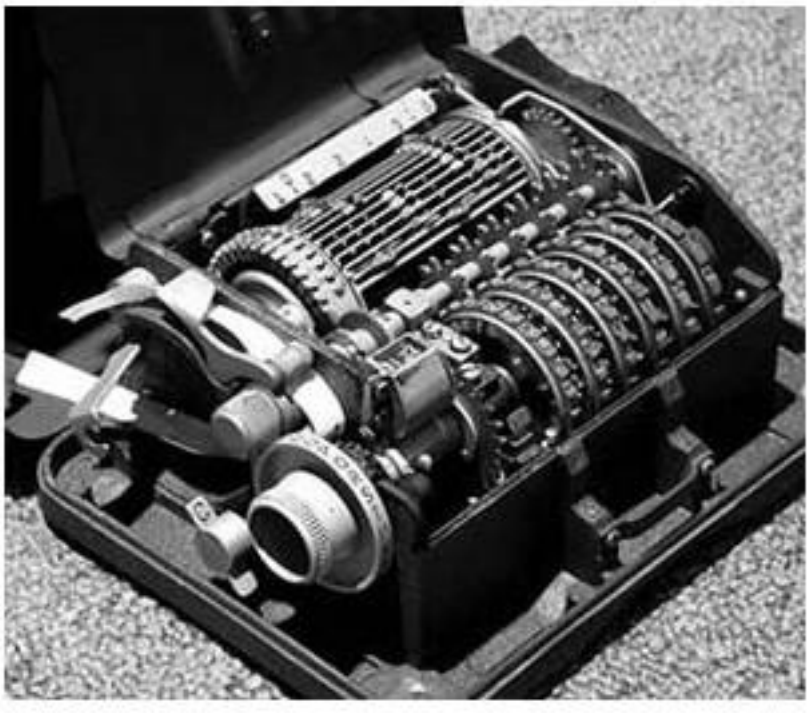
Все понимали, что такая защита чересчур слаба, но, не сумев придумать ничего другого, пользовались ей до тех самых пор, пока Вернам не предложил использовать для кодирования сообщений особенности телетайпного кода, в котором кодируемый знак выражается в виде пяти элементов. Каждый из этих элементов символизирует наличие («плюс») или отсутствие («минус») электрического тока в линии связи. Например, букве «А» соответствует комбинация «+ – – – –».

Подготовленное к отправке сообщение набивается на перфоленте: отверстие соответствует «плюсу» кода, его отсутствие — «минусу». В процессе передачи металлические щупы телетайпа проходят через отверстия, замыкая цепь, и посылают импульсы тока («+»). Там, где отверстия нет, и бумага не позволяет щупам замкнуть цепь, импульс не передается («–»).

Для шифрования Вернам предложил заранее готовить «гамму» — перфоленту со случайными знаками — и затем электромеханически складывать ее импульсы с импульсами знаков открытого текста. Полученная сумма представляла собой шифртекст. На приемном конце импульсы, полученные по каналу связи, складывались с импульсами той же самой «гаммы», в результате чего восстанавливались исходные импульсы сообщения. А если сообщение перехватывалось, то без «гаммы» расшифровать его было невозможно, противник видел только ничего не значащую последовательность «плюсов» и «минусов».

Дальнейшее усовершенствование метода, предложенного Вернамом, принадлежит будущему начальнику связи войск США Джозефу Моборну, объединившему хаотичность «гаммы», на которую опирался Вернам в своей системе «**автоматического шифрования**», с используемым в то время в войсках правилом «**одноразового шифрблокнота**». Идея Моборна заключалась в том, что каждая случайная «гамма» должна использоваться один, и только один раз. При этом для шифрования каждого знака всех текстов, которые уже переданы или будут переданы в обозримом будущем, должен применяться абсолютно новый и не поддающийся предсказанию знак «гаммы».

В период между двумя мировыми войнами в большинстве стран появляются **электромеханические шифраторы**.



Они были двух типов. Первый — устройство, состоящее из коммутационных дисков и механизма изменения их угловых положений. По обеим сторонам коммутационного диска размещены контакты, соответствующие алфавитам открытого и шифрованного текста. Контакты эти соединяются между собой согласно некоторому правилу подстановки, называемому коммутацией диска. Эта коммутация определяет замену букв в начальном угловом положении. При изменении углового положения диска изменяется и правило подстановки. Таким образом, ключ шифрования содержит пару неизвестных: схему соединения контактов и начальное угловое положение. Если после шифрования каждой буквы менять угловое положение диска — получим многоалфавитное шифрование. Еще

более сложное устройство получим, соединив последовательно несколько дисков, угловые положения которых меняются с различной скоростью.

Широко известная шифрмашина «**Энигма**»,

которой были оснащены германские войска времен Второй мировой войны, является типичным примером устройства на коммутационных дисках. Конструктивно «Энигма» походила на обычную пишущую машинку, только нажатие клавиши приводило не к удару молоточка по бумаге, а создавало электрический импульс, поступавший в схему криптопреобразования. Американская шифрмашина **М-209** — типичный пример второго типа шифратора, — **шифратора на цевочных дисках**.

Интересно, что Советский Союз производил шифрмашины обоих названных типов.
Таким образом, перед Второй мировой войной все ведущие страны имели на вооружении электромеханические шифрсистемы, обладающие высокой скоростью обработки информации и высокой стойкостью. Считалось, что применяемые системы недешифруемы, и криптоанализу больше делать абсолютно нечего. Как часто бывает, это мнение было впоследствии опровергнуто, и дешифровщики были непосредственными участниками военных действий.

Прежде чем перейти ко второй части и к рассказу о современных системах шифрования, упомянем теоретическое открытие, во многом предопределившее дальнейший путь развития криптографии. Речь идет о двух работах, написанных в начале сороковых годов прошлого века и существенно расширивших научные основы криптографии, — статье американца Клода Шеннона «Теория связи в секретных системах» и статье советского ученого В. А. Котельникова «Основные положения автоматической шифровки». Эти статьи полностью уничтожили радужные надежды и предубеждения, развеяли мифы и разрушили вековые легенды, сняли с криптографии покров тайны.

Шеннон доказал, что предложенный Вернамом в 1917 году метод шифрования с применением случайной комбинации знаков («гаммы»), объединенный с одноразовым шифрблокнотом, — единственная абсолютно стойкая система шифрования, при условии, что длина ключа равняется длине самого сообщения.

Подавляющее большинство систем шифрования являются лишь разумно стойкими, поскольку криптоаналитик, имея в своем распоряжении большой объем шифрованного текста и достаточно времени, может найти пути расшифровки сообщений. Одноразовый же шифрблокнот — абсолютно стойкий как в теории, так и на практике. Каким бы длинным ни был перехваченный текст, сколько бы времени ни отводилось на его исследование, криптоаналитик никогда не сможет вскрыть одноразовый шифрблокнот, использованный для получения этого шифртекста. И вот почему.

У криптоаналитика нет отправной точки для исследований, ведь «гамма» не содержит повторений, не используется дважды, не является связным текстом и не имеет структурных закономерностей. Криптоанализ бессилен. Остается только метод прямого перебора всех возможных ключей, который, по идее, в конечном счете обязательно приведет к открытому тексту. Однако успех, приобретенный этим путем, иллюзорен. И дело не только в том, что затраты времени колоссальны. Тотальное опробование действительно позволяет получить исходный текст. Но оно также даст и еще множество связных текстов той же длины. Кто возьмется определить, какой из них является истинным?

Говорят, что такой метод шифрования использовался не только в тайных операциях советской разведки и ЦРУ, но и при проведении правительственных переговоров по «горячей линии» Москва — Вашингтон.Однако в обмен на абсолютную стойкость метод этот требует чересчур больших вычислений, что не всегда оправданно. Иногда достаточно обеспечить криптостойкость на некоторое время (помните доктрину Россиньоля?). Как говорил Остап Бендер: «Мне не нужна вечная игла для примуса, я не собираюсь жить вечно».

Стойкость криптосистемы сегодня оценивается объемами вычислений, которые требуются для ее вскрытия. Считается, что ключ шифрования достаточно стоек, если все известные способы его отыскать настолько сложны, что требуют больше времени, чем простой перебор всех возможных ключей.

Все мы сегодня, иногда даже не подозревая об этом, применяем средства защиты информации. Мы шифруем сообщения электронной почты, пользуемся интеллектуальными банковскими карточками, ведем разговоры по закрытым каналам связи и т. д. Всякий раз возникает вопрос — надежна ли защита? Но и этот элементарный вопрос не так просто правильно сформулировать. Кто наш противник? Каковы его возможности? Какие он преследует цели? Как измерить стойкость защиты? Чего мы хотим от нее — скрыть факт переписки? зашифровать содержание? засекретить имена адресатов? не позволить противнику исказить информацию?

Над этими и многими другими проблемами работает современная криптография, новейшая история которой началась в 1978 г. с суммы в 100 долларов и числа «9686137546220614771409222543558829057599911245743198746951209308162982251457083569314766228839896280133919905518299451578151 54».

Продолжение читайте в статье «**Ключи от тайны**»