СОДЕРЖАНИЕ

ЭССЕ

НЕСКОЛЬКО СЛОВ О ТАЙНОПИСИ

Вряд ли можно представить себе время, когда не существовала потребность или, по крайней мере, желание обмениваться информацией между двумя людьми таким образом, чтобы скрыть ее ото всех остальных. Следовательно, практика шифрованного письма должна насчитывать много веков. Поэтому Де ла Гиллетьер[1] в своем сочинении «Лакедемон древний и новый» явно ошибается, утверждая, что криптографию изобрели спартанцы. Он называет скиталу первым инструментом этого искусства, однако ее следовало упомянуть лишь как одно из многих средств криптографии, попавших в ранние анналы истории. Скиталы представляли собой два совершенно одинаковых деревянных цилиндра. Эфор вручал генералу, отправлявшемуся в по-

[1] Имя, под которым печатал свои произведения Гиллье де Сен Жорж (1625–1705) — французский литератор, историк искусства.

ход с войском, один цилиндр, а второй оставлял у себя. Если предоставлялась возможность установить связь, на скиталу плотно наматывали узкую полоску пергамента, не оставляя промежутков между витками. Сообщение записывалось поперек витков, после чего послание разворачивали и отправляли получателю. Если оно попадало в чужие руки, перехватившие его ничего не могли разобрать. Но если депеша приходила по назначению, то адресату, чтобы прочитать написанное, было достаточно намотать полоску пергамента на второй цилиндр. Тот факт, что этот простой способ шифрования сохранился до наших дней, скорее связан с историей использования скиталы, чем со своей эффективностью. Похожие методы секретной связи наверняка существовали со времен изобретения письменности.

Следует по ходу дела заметить, что ни в одном из трактатов на тему этой статьи, попавшихся нам на глаза, мы не встретили даже намека на метод расшифровки — за исключением методов, применимых к любым шифрам, — тайных сообщений, изготовленных с помощью пары скитал. Правда, мы читали истории о том, что перехваченные свитки получалось разгадать, однако это всегда происходило лишь по чистой случайности. Тем не менее получить разгадку можно с абсолютной точностью. После перехвата по-

лоски пергамента необходимо изготовить конус сравнительно большой длины, скажем, шесть футов, чья окружность в основании должна быть не меньше длины полоски кожи. Полоску необходимо плотно обмотать вокруг конуса, начиная с самого основания, не оставляя зазоров, затем, не позволяя полоске развернуться или виткам разойтись в стороны, постепенно сдвигать ее, перемещая к вершине конуса. Такой способ непременно выявит отдельные слова, слоги или буквы, умышленно связанные с другими. В конце концов пергамент достигнет точки на конусе, соответствующей толщине скиталы при написании тайного письма. А так как по мере продвижения к вершине конуса будут пройдены все возможные величины диаметра скиталы, ошибка полностью исключается. Установив диаметр скиталы, можно изготовить ее дубликат и легко прочитать зашифрованное сообщение.

Немногие поверят, если им сказать, что изобрести способ тайнописи, способный поставить исследователей в тупик, не так-то просто. Можно с уверенностью утверждать, что человеческий разум не в состоянии выдумать такой шифр, который не смог бы разгадать чужой дотошный ум. И все же относительно способности к расшифровке тайнописи между различными видами интеллекта существуют очень заметные различия. Нередко бывает, что из двух человек, на первый

взгляд равных по своим умственным способностям, один не может разгадать даже самый простой шифр, в то время как другой щелкает самые мудреные задачи как орехи. В целом можно заметить, что в таких исследованиях очень активно задействуются аналитические способности. По этой причине криптографические задачки было бы вполне уместно включить в учебные программы академий как тоник для укрепления важнейших умственных способностей.

Если бы два человека, не имеющие никаких навыков криптографии, захотели вести переписку, которую никто, кроме них, не смог бы прочитать, то скорее всего они быстро придумали бы какой-нибудь особый алфавит с одним на двоих ключом. Для начала они, возможно, решили бы, что «a» должно читаться как «z», «b» как «y», «c» как «x», «d» как «w» и так далее. Другими словами, они поменяли бы порядок букв в алфавите на обратный. Немного поразмыслив, они нашли бы такую схему слишком очевидной и решили бы воспользоваться более сложным способом. Первые тринадцать букв английского алфавита можно, например, записать под последними тринадцатью буквами в следующем порядке:

n o p q r s t u v w x y z
a b c d e f g h i j k l m;

При таком расположении «a» заменяет «n» и наоборот, «o» заменяет «b» и наоборот и так

далее. Такой шифр опять же выглядит очень систематично, а значит, легко угадывается, поэтому ключевой алфавит лучше построить совершенно произвольным образом. Например, «a» может представлять собой «p», «b» — «x», «c» — «u», «d» — «o» и так далее.

Партнеры по переписке, если только не осознáют свою ошибку, когда их шифр кто-нибудь разгадает, скорее всего довольствуются последним вариантом как якобы гарантирующим полную безопасность. А если нет, то перейдут от букв к использованию произвольных символов. Например: «(» будет представлять «a», «.» будет представлять «b», «:» — «c», «;» — «d», «)» — «e» и так далее.

Написанное таким образом письмо, несомненно, будет иметь очень замысловатый вид. Но если и этот подход не принесет удовлетворения, можно придумать и реализовать постоянно меняющийся алфавит. Приготовьте два круга из картона, один диаметром на полдюйма меньше другого. Наложите центр меньшего круга на центр большего круга и закрепите, чтобы он не проскальзывал. Прочертите радиус из общего центра до края меньшего круга и продолжите его до края большего круга. Начертите двадцать шесть радиусов, чтобы получить двадцать шесть секторов, В каждый сектор на нижнем круге впишите по одной букве английского алфавита, чтобы охва-

тить весь алфавит, причем буквы лучше вносить в совершенно произвольном порядке. Повторите то же самое на верхнем круге. Вставьте булавку в общий центр и, удерживая нижний круг на месте, проверните верхний. Остановив вращение верхнего круга, напишите письмо, опираясь на полученный шифр, используя, например, для буквы «a» букву, выпавшую против нее на большем круге, и так далее. Чтобы прочитать зашифрованное таким способом письмо, получатель должен иметь такие же круги с буквами и знать хотя бы одно сочетание букв на верхнем и нижнем круге, использованное автором письма. Ключом к шифру могут служить первые две буквы, с которых начинается письмо. Если письмо, например, начинается с букв «a» и «m», то выставив их друг против друга на верхнем и нижнем круге, адресат получит доступ ко всему алфавиту.

На первый взгляд эти различные виды шифра кажутся окутанными атмосферой непроницаемой тайны. Написанное столь хитрым способом выглядит неразрешимой загадкой. Некоторым людям эта задача может оказаться не по зубам, но для других, поднаторевших в разгадывании шифров, здесь нет никакой тайны. Читателю следует помнить, что основой искусства дешифровки служат общие принципы строения языка, не зависящие от конкретных правил составления шифра или соответствующего ключа. Сложность

разгадывания криптографической загадки далеко не всегда соответствует количеству труда или изобретательности, вложенных в ее создание. Ключ используется исключительно теми, кто придумал шифр и пользуется им. Когда шифр читает кто-то другой, на ключ вообще не обращают внимания. Отмычку подбирают без него. Приведенное выше описание различных методов криптографии показывает постепенное нарастание их сложности. Но эта сложность не более чем дымовая завеса. За ней не прячется ничего существенного. Сложность имеет отношение только к созданию шифра, но не к его разгадке. Способ шифрования, упомянутый последним, ни в коей мере не сложнее для расшифровки, чем первый. Степень сложности обоих способов здесь ни при чем.

Обсуждая аналогичную тему в одной из еженедельных городских газет примерно полтора года назад, автор этой статьи получил возможность рассказать о применении строгого подхода ко всем формам мышления, о его преимуществах и распространении даже на то, что считается проявлением фантазии в чистом виде, и как следствие — на разгадывание шифров. Автор взял на себя смелость утверждать, что разгадает любой шифр вышеописанного типа, присланный в редакцию. Это предложение неожиданно вызвало живой интерес у многочисленных чита-

телей журнала. Редактора завалили письмами со всех концов страны. Многие читатели настолько были уверены в невозможности разгадать их загадки, что даже стыдились предлагать редактору пари. В то же время участники не всегда в точности придерживались установленных правил. Во многих случаях криптографы выходили за начальные рамки, использовали иностранные языки, не делали пробелов между словами и предложениями, применяли в одном шифре по нескольку алфавитов. Один господин среднего уровня порядочности прислал головоломку, состоящую из разного рода крючков и загогулин, которую не осилил самый экзотический набор типографских шрифтов. Он смешал целых семь алфавитов и опустил все промежутки между буквами и строками. Многие загадки пришли в письмах со штампом Филадельфии. Несколько, касавшиеся предмета пари, были присланы непосредственно из этого города. Из примерно ста полученных шифрованных писем мы не смогли с ходу прочитать только одно. Последнее письмо оказалось обманом — мы полностью доказали, что оно содержало набор случайных букв и символов, не имевший никакого смысла. А что касается загадки, использовавшей семь алфавитов, мы имели удовольствие огорошить ее отправителя, быстро представив правильный ответ.

Наша еженедельная газета в течение нескольких месяцев занималась решением иероглифических и смахивающих на каббалу загадок, поступавших от криптографов со всех уголков страны. Однако за исключением самих авторов шифрованных посланий вряд ли нашелся хоть один человек, кто увидел в этом деле что-то еще, кроме чистой воды мистификации. В подлинность ответов на самом деле никто не верил. Один читатель утверждал, что загадочные письмена публиковались только для того, чтобы придать газете эксцентричности и привлечь внимание. Другой решил, что мы сами придумывали и сами же разгадывали шифры. Учитывая сложившуюся ситуацию, дальнейшие исследования в области некромантии было решено прекратить. Пользуясь предоставленной возможностью, автор этой статьи подтверждает честность намерений издания, опровергает обвинения во вздорности, которым оно подвергалось, и заявляет от своего имени, что все шифры составлялись и разгадывались из самых искренних побуждений.

Очень часто встречается следующий непритязательный способ тайной переписки. На карточку с неравномерными интервалами наносятся продолговатые пространства длиной примерно в обычное слово из трех слогов, набранное шрифтом боргес. Вторая карточка имеет такой же вид. Каждый участник переписки получает

по одной такой карточке. Когда нужно написать письмо, карточку-ключ кладут на бумагу и в пустые промежутки вписывают слова, имеющие значение. Затем карточку убирают и оставшиеся свободные места на бумаге заполняют другими словами, чтобы придать письму совершенно иной вид. Когда адресат получает шифрованное письмо, ему достаточно наложить на него свою карточку, которая скроет лишние слова, оставив только те, что имеют значение. Главное препятствие криптографии этого типа состоит в заполнении свободных мест таким образом, чтобы предложения не звучали вымученно. К тому же опытный наблюдатель всегда заметит разницу в почерке между вписанными через карточку словами и теми, что были добавлены позже.

В качестве еще одного средства шифрования иногда используется колода игральных карт. Сначала стороны договариваются о расположении карт внутри колоды. Например, сначала должны идти пики, затем червы, затем бубны и в последнюю очередь трефы. Разложив карты установленным образом, отправитель пишет на верхней карте первую букву своего письма, на второй карте — вторую букву, на третьей — третью и так далее, пока не закончатся карты в колоде. Таким образом он получит пятьдесят две буквы. После этого он тасует карты в заранее оговоренном порядке, например, берет три нижние карты и кла-

дет их сверху, затем берет одну сверху и кладет ее вниз и так далее установленное количество раз. Сделав это, он опять пишет на каждой карте по одной букве, продолжая письмо, пока не израсходует все пятьдесят две карты. Процесс повторяется, пока письмо не будет написано целиком. Получив колоду, партнер по переписке размещает карты в первоначальном виде, потом буква за буквой читает первую часть письма, записанную на пятидесяти двух картах. Затем тасует карты в условленном порядке и читает очередную часть письма на пятидесяти двух картах. И так, пока не прочитает все письмо. Препятствием для криптографии такого рода является сам характер отправления. Колода карт, пересылаемая одним человеком другому, наверняка вызовет подозрения. Несомненно, шифру лучше придать безобидный вид, чтобы он не выглядел как шифр, вместо того чтобы пытаться сделать его недоступным для разгадывания на случай перехвата. Опыт подсказывает, что самый хитроумный шифр, если он привлек к себе внимание, может быть и обязательно будет взломан.

Надежный способ секретной связи можно создать следующим образом. Пусть каждая сторона обзаведется экземпляром одного и того же издания книги (чем реже издание и менее известна сама книга, тем лучше). В шифрованном документе используются только цифры, указывающие

местоположение буквы в этом издании книги. Например, шифр может начинаться с цифр 121–6–8. Получатель открывает страницу 121 и находит шестую букву слева в восьмой строке сверху. Эта буква будет первой буквой письма, и так далее. Такой способ очень надежен, и все же тайное сообщение, зашифрованное с его помощью, тоже можно расшифровать. Кроме того, прочтение сообщения отнимает очень много времени, даже если книга-ключ находится под рукой.

Разумеется, криптография как серьезное средство передачи важной информации не вышла из употребления по сей день. Она по-прежнему широко используется в дипломатии. И даже сейчас, по мнению различных иностранных правительств, есть люди, занимающие официальные должности, чья реальная деятельность сводится к расшифровке тайных сообщений. Выше уже говорилось, что для решения криптографических задач — по крайней мере высшего порядка — требуются особые мыслительные способности. Поэтому услуги таких людей, хоть они бывают редко востребованы, как правило, хорошо вознаграждаются.

Пример современного использования шифра приводится в книге, опубликованной издателями из Филадельфии, господами Ли и Бланшаром, под названием «Очерки о выдающихся личностях Франции». В очерке о Берье говорит-

ся о письме, адресованном герцогиней дю Берри парижским легитимистам, в котором сообщалось о ее прибытии. К письму прилагалась длинная шифрованная записка, ключ для прочтения которой герцогиня забыла передать. «Острый ум Берье, — пишет биограф, — вскоре сам его обнаружил. Ключом служила фраза, заменявшая двадцать четыре буквы алфавита, — Le, gouvernement provisoire».

Утверждение, что Берье быстро нашел ключевую фразу, лишь доказывает, что автор очерка ничего не смыслит в криптографии. Месье Берье, разумеется, нашел ее, но сделал это лишь для того, чтобы утолить свое любопытство, уже разгадав загадку. Он не использовал ключ для дешифровки, но взломал замок другим способом.

В рецензии на книгу (опубликованной в апрельском номере журнала) мы отозвались об этой истории следующим образом: «Фраза Le, gouvernement provisoire была написана по-французски, и шифрованная записка была адресована французам. Расшифровка заняла бы больше времени, если бы ключ составили на иностранном языке. Мы предлагаем любому, у кого найдется время, отправить нам аналогичную записку, составив ключевую фразу на французском, испанском, немецком, греческом или на латыни (либо на любом диалекте этих языков) и обещаем разгадать, что в ней написано».