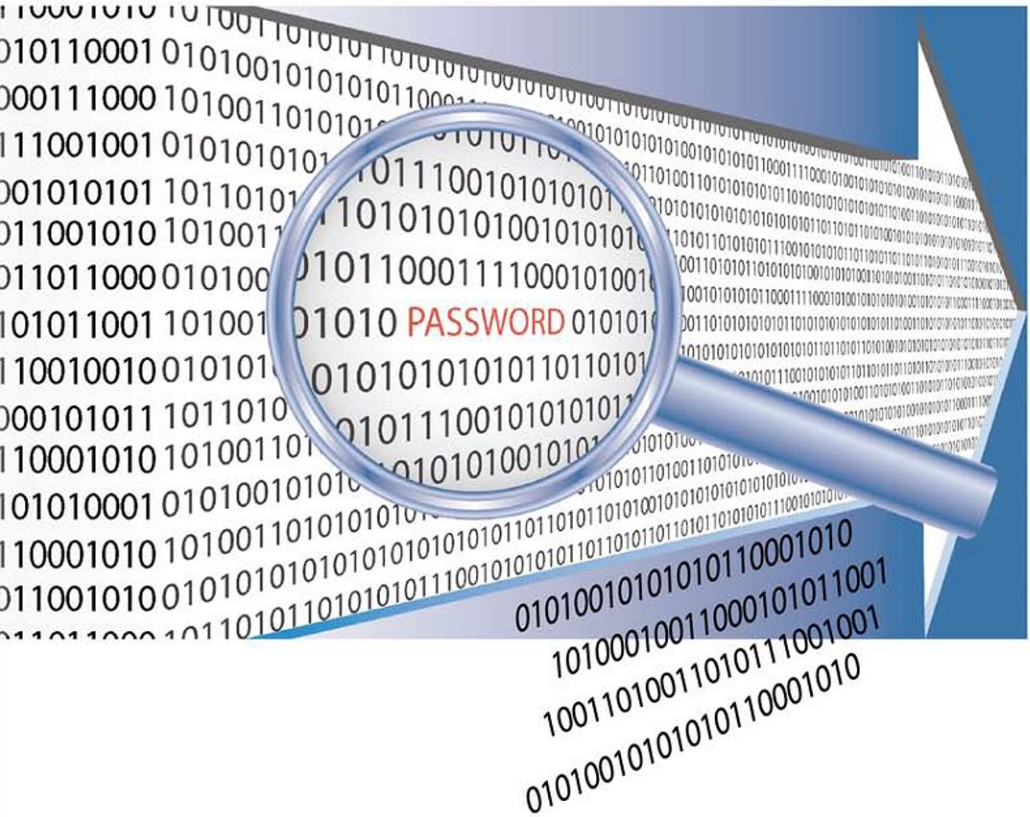
Виктор Де Касто

ПРОСТО
Криптография



ПРОСТО

УДК 001, 501, 510
ББК 22.1
К 28

К 28 Виктор Де Касто. **Просто криптография.** — СПб.: ООО «Страта», 2014. — 208 с.

ISBN 978-5-906150-15-8

Наверно, ничто не вызывает у людей большего любопытства, чем чужие тайны. Чем больше одни стремятся что-то скрыть, тем больше другие хотят это «что-то» узнать. В те давние времена, когда люди только научились писать, их тайны материализовались, представ в образе символов, иероглифов, букв, цифр. Но в таком виде они стали доступны другим. С этого момента началось извечное соревнование между шифровальщиками, пытающимися скрыть информацию, и криптоаналитиками, стремящимися расшифровать ее.

В книге рассказывается об истории криптографии: от примитивных систем шифрования и дешифровки, придуманных людьми еще в древние времена, до современных компьютерных алгоритмов — как существующих, так и тех, над которыми работают нынешние ученые-криптографы.

Книга предназначена для широкого круга читателей.

ISBN 978-5-906150-15-8

СОДЕРЖАНИЕ

ГЛАВА 1.
ИНФОРМАЦИЯ НУЖДАЕТСЯ В ЗАЩИТЕ

Криптография — это искусство
написания или взлома шифров.
Оксфордский словарь

Искусство создания посланий, которые могут быть поняты только отправителем и получателем, а любому другому лицу покажутся абсолютно бессмысленными, по всей видимости, является таким же древним, как сама письменность.

Историки знают о существовании ряда «нестандартных» иероглифов, которым более четырех с половиной тысяч лет. Хотя, конечно, вряд ли возможно с полной уверенностью сказать, представляют ли они попытку скрыть информацию или просто использовались в некоем религиозном ритуале... Зато хорошо известно о табличке из Вавилона, датированной примерно 2500 годом до н. э. На ней есть слова, в которых удален первый согласный и использован целый ряд необычных вариантов обозначения звуков. Исследования показали, что в тексте описан способ изготовления глазури для гончарных изделий, а это приводит нас к выводу: текст был написан купцом или мастером-гончаром, пожелавшим защитить от конкурентов секреты своего мастерства.

По мере распространения письменности и торговли возникли великие империи, которые часто вступали в пограничные конфликты со своими географическими соседями. В результате криптография и безопасная передача информации

стали делом особой важности не только для купцов, но и для правительств.

В нынешнее же время, в наш информационный век, обеспечение защиты связи и поддержание должного уровня секретности становятся гораздо важнее, чем прежде. Едва ли теперь существует какой-то поток информации, который бы каким-либо образом не кодировался и не шифровался.

Изначальная цель кодирования — техническое обеспечение связи. Например, текст конвертируется в бинарный (или двоичный) язык (систему счисления, использующую только цифры 0 и 1). После кодирования большая часть этой информации должна быть защищена от любого, кто может ее перехватить. Другими словами, кодированное послание требуется зашифровать. Наконец, законный получатель должен быть способен расшифровать полученное послание.

Кодирование, шифрование и дешифровка — это основные па в «танце информации», который повторяется миллионы раз в секунду, каждую минуту, каждый час каждого дня.

А «музыка», сопровождающая этот танец, — математика.

ОСНОВНЫЕ ЭЛЕМЕНТЫ КОДИРОВАНИЯ

Шифровальщики и специалисты по криптографии используют термин «кодировать» несколько в ином смысле, не так, как мы все. Для них кодирование — это метод написания с использованием кода, который состоит из замены одного слова другим. С другой стороны, использование шифра или шифрование включает замену букв или каких-то других отдельных знаков. С течением времени в широком сознании последняя форма сделалась превалирующей, причем в такой степени, что стала синонимом «написания с использованием кода» или «закодированного письма». Однако если мы возьмем более строгое научное определение, то для второго метода правильным термином будет «шифровать» (или «расшифровывать», в случае обратного процесса) послание.

Давайте представим, что мы отправляем защищенное послание «АТАКОВАТЬ». Мы можем сделать это двумя основными путями: заменить слово целиком (кодирование) или

заменить некоторые или все буквы, которые составляют это слово (шифрование). Простой способ кодирования слова — перевести его на язык, который не знают потенциальные любители подслушать или подсмотреть. В случае шифрования будет достаточно, например, заменить каждую букву другой (то есть стоящей в другом месте в алфавите). В этом случае необходимо, чтобы получатель знал использовавшуюся процедуру для того, чтобы декодировать или дешифровать текст, или послание потеряет смысл. Если мы уже договорились с получателем, что будем использовать тот или иной способ — переводить на другой язык или заменять каждую букву, — то все, что от нас требуется, — это сообщить нашему получателю о выбранном языке или количестве позиций, на которые мы продвинулись в алфавите для замены каждой буквы.

В приводимом примере, если получатель получает зашифрованное послание «ВФВЙРДВФЮ» и знает, что при замене каждой буквы мы сдвигались на две позиции вперед в алфавите русского языка, то он сможет с легкостью повторить процесс, двигаясь в обратном направлении, и успешно расшифровать наше послание.

ДВОИЧНЫЙ (БИНАРНЫЙ) КОД

Чтобы компьютер понял и обработал информацию, она должна быть переведена с языка, на котором записана, на так называемый бинарный или двоичный язык. Этот язык состоит всего из двух цифр: 0 и 1. Перевод чисел от 0 до 10 из десятичной системы в двоичную представлен в таблице.

Соответственно десятичное число 9770 будет выражаться с использованием двоичного кода как 10011000101010.

	Бинарный код
0	0
1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000
9	1001
10	1010

ПЕРЕВОД ИЛИ РАСШИФРОВКА?

К переводу текста, написанного на языке, в котором используется набор неизвестных обозначений (букв, знаков, символов), можно подходить как к обычной задаче дешифровки. Текст, который необходимо перевести, можно рассматривать как неизвестный текст, уже переведенный на наш язык, а алгоритмом шифрования будут правила грамматики и синтаксиса языка оригинала. Техники, используемые при решении обеих задач — перевод или дешифровка, — имеют много общего. В обоих случаях нужно соблюсти одно и то же условие: отправитель и получатель должны, по крайней мере, говорить на одном языке. Именно поэтому перевод текстов, написанных на вышедших из употребления языках, как, например, египетское иероглифическое письмо или критское линейное письмо, был невозможен, пока не был найден способ приведения их в соответствие с каким-то известным языком. В обоих случаях это был древнегреческий. На рисунке выше изображена табличка, найденная на Крите, на которой используется так называемое «линейное письмо Б».

Установленное нами разграничение между правилом шифрования (применяемая система) и параметром шифрования [меняющееся указание (инструкция), которое является специфическим для каждого послания или набора посланий] очень полезно, потому что потенциальному шпиону для расшифровки нужно знать и то, и другое.

Таким образом, шпион может знать, что ключ к шифру — это замена каждой буквы другой буквой, находящейся далее в алфавите через определенное количество позиций (x). Однако, если он не знает, какому числу соответствует x, то ему потребуется перепробовать все возможные комбинации для каждой буквы алфавита. В этом примере шифр очень простой, и испробовать все возможности — для чего требуется просто усердие — не так уж и сложно.

Эта техника дешифровки называется методом тотального перебора.

Однако в более сложных случаях этот тип взлома кода (криптоанализ) практически невозможен — по крайней мере, вручную. Более того, на перехват и расшифровку посланий обычно накладываются жесткие временные ограничения. Ведь информацию нужно получить и понять прежде, чем она станет бесполезной или широко известной другим.

Общее правило шифрования обычно называется алгоритмом шифрования, в то время как специфический параметр, используемый для шифрования или кодирования послания, называется ключом. (В примере шифрования, приведенном

СКОЛЬКО НУЖНО КЛЮЧЕЙ?

Какое минимальное количество ключей необходимо в системе с двумя пользователями? Тремя? Четырьмя? Чтобы два пользователя могли тайно общаться друг с другом, необходим только один код или ключ. В случае трех пользователей (A, B, C) необходимы три: один для общения A и B, еще один для пары A и C, а третий — для пары B и C. Точно так же четырем пользователям потребуется шесть ключей. Таким образом, если обобщить, то для ***n*** пользователей потребуется столько ключей, сколько существует комбинаций пар из количества пользователей ***n***, то есть:

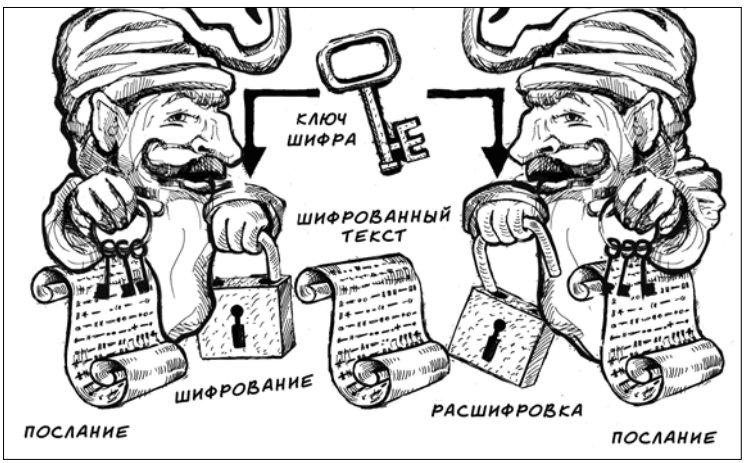
$$\binom{n}{2} = \frac{n(n-1)}{2}$$

В результате для относительно небольшой системы из 10000 связанных между собой пользователей потребуется 49995000 ключей. Если взять население земного шара, составляющее шесть миллиардов человек, то от количества ключей голова пойдет кругом: 17999999997000000000.

на стр. 6 —7, ключ — 2. Каждая буква исходного слова заменяется другой, которая расположена через две позиции после нее в алфавите русского языка.)

Очевидно, что для каждого алгоритма шифрования возможно огромное количество ключей, поэтому знание одного алгоритма может быть бесполезным, если мы не имеем представления, какой ключ нужен для расшифровки. Поскольку ключи обычно легче заменить и распространить, кажется логичным для обеспечения безопасности системы шифрования сосредоточиться на том, чтобы хранить ключи в тайне и уделять именно этому максимальное внимание. Этот принцип был установлен в конце XIX столетия голландским лингвистом Огюстом Керкгоффсом фон Ниевенхофом и поэтому известен как принцип Керкгоффса.

Чтобы подвести итог тому, что мы уже представили в этой книге, можно показать общую схему шифрования, определяемую следующими элементами:



То есть, в схему входят: отправитель и получатель послания, алгоритм шифрования и определенный ключ, который позволяет отправителю шифровать послание, а получателю расшифровывать его.

Далее мы увидим, как эта схема была модифицирована в недавнем прошлом из-за изменения природы и функции ключей, но пока будем придерживаться именно ее.

ДОКТОР ОГЮСТ КЕРКГОФФС

Нидерландский лингвист и криптограф, профессор Парижской высшей школы коммерции во второй половине XIX века. Родился в городе Нют, Нидерланды. Закончил Льежский университет, преподавал в Нидерландах и во Франции.

Автор книги «Военная криптография» (опубликована в 1883 году), в которой сформулировал ответы на вопросы, актуальность которых для криптографии обозначилась только в XX веке. В сжатой, системной форме Огюст Керкгоффс изложил требования к криптографическим системам, а также показал важнейшую роль криптоанализа для их проверки и подтверждения стойкости. Одно из требований теперь известно как «Принцип Керкгоффса».

В 1885 Керкгоффс заинтересовался искусственным языком волапюк, несколько лет был ведущим членом движения Волапюк и директором Академии волапюка. Он опубликовал несколько книг об этом искусственном языке и дал серию лекций во Франции, Испании и странах Скандинавии.

ПРИНЦИП КЕРКГОФФСА

В соответствии с принципом Керкгоффса, ключ — это основной элемент, обеспечивающий безопасность криптографической системы. До относительно недавнего времени ключи отправителя и получателя во всех возможных криптографических системах должны были быть идентичными или по крайней мере симметричными, то есть их необходимо было использовать и для шифрования, и для расшифровки послания. Поэтому ключ являлся общей тайной отправителя и получателя, и в связи с этим используемая криптографическая система всегда была уязвимой, так сказать, с обеих сторон. Этот тип

СКОЛЬКО НУЖНО КЛЮЧЕЙ?.. ЧАСТЬ 2

Как мы видели на с. 12, для классической криптографии требовалось огромное количество ключей. Однако в случае открытой (общедоступной) криптографической системы любым двум пользователям, которые обмениваются посланиями, требуются только четыре ключа: их соответствующие открытые и закрытые ключи. В этом случае количеству пользователей n требуется 2 n ключей.

криптографии, который зависит от ключа, имеющегося как у отправителя, так и у получателя, называется «шифрование закрытым ключом».

Это было свойством всех криптографических систем, изобретенных людьми с начала времен, независимо от используемого алгоритма и сложности. Сделать ключ одним и тем же для получателя и отправителя кажется единственно разумным и полностью соответствующим здравому смыслу.

В конце концов, разве может один человек кодировать послание в соответствии с одним кодом, а второй расшифровывать его в соответствии с другим и надеяться понять полученный текст? Тысячи лет это считалось полным абсурдом. Однако, как мы увидим ниже, всего пять десятилетий назад абсурд стал абсолютно возможным и теперь используется повсеместно.

В наши дни алгоритмы шифрования, которые используются в большинстве коммуникационных связей, состоят, как правило, из двух ключей: закрытого ключа, который уже стал обычным делом, и открытого ключа, который знают все. Механизм передачи состоит в следующем: отправитель получает открытый ключ получателя, которому он хочет отправить послание, и использует его для шифровки послания. Получатель использует

свой закрытый ключ для расшифровки полученного послания. Более того, эта система имеет очень важное дополнительное преимущество: ни отправителю, ни получателю не нужно заранее встречаться и договариваться ни о каких используемых ключах, поэтому безопасность системы гораздо выше, чем было возможно ранее. Эта полностью революционная форма известна как «шифрование открытым ключом» и сегодня составляет основу безопасности в коммуникационных сетях.

В основе этой революционной технологии лежит математика.

Фактически, как мы подробно выясним ниже, современная криптография держится на двух китах. Первый — модульная арифметика, а второй — теория чисел и в особенности та ее часть, которая занимается изучением простых чисел.

ТЕЛЕГРАММА ГЕРМАНСКОМУ ПОСЛУ

Криптография — это одна из областей прикладной математики, в которой наиболее очевиден контраст между первоначальной четкостью, лежащей в основе теории, и туманными последствиями ее внедрения и применения на практике.

А ведь иногда от успеха или провала в обеспечении защиты связи и коммуникаций зависит судьба целых наций. Одним из самых впечатляющих примеров того, как криптография изменила курс истории почти сто лет назад, является так называемое «дело о телеграмме Циммермана».

7 мая 1915 года, когда половина Европы была вовлечена в кровавый конфликт Первой мировой войны, немецкая подводная лодка торпедировала трансатлантический пассажирский лайнер «Лузитания», шедший под британским флагом недалеко от берегов Ирландии. Результатом стала одна из наиболее ужасных трагедий в истории: погибли 1198 гражданских лиц, 124 из которых были американцами.

Новость вызвала ярость в общественном мнении Соединенных Штатов Америки, и администрация президента Вудро Вильсона предупредила немецкое правительство, что если подобное повторится, США немедленно вступят в войну на стороне союзников. В дополнение к этому Вильсон потребовал, чтобы немецкие подводные лодки придерживались правил ве-

дения морской войны, установленных Гаагскими конвенциями 1899 и 1907 годов, что ставило под угрозу преимущество немецкого флота, применяющего по отношению к гражданским судам тактику неограниченной подводной войны.

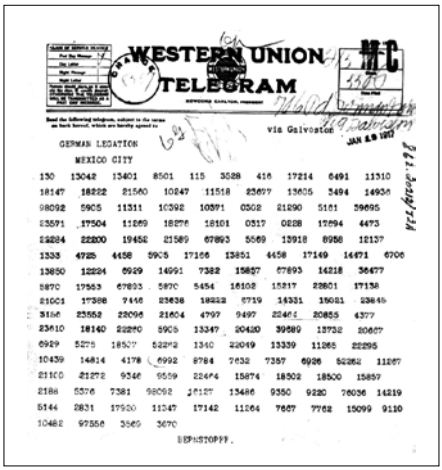
В ноябре 1916 года Германия назначила новым министром иностранных дел Артура Циммермана, имевшего репутацию прекрасного дипломата. Новость была положительно принята прессой США, которая посчитала это назначение благоприятным знаком для американо-германских отношений.

В январе 1917 года, менее, чем через два года после трагедии с «Лузитанией», когда война была в самом разгаре, посол Германии в Вашингтоне Иоганн фон Бернсторф получил от Циммермана следующую зашифрованную телеграмму с указанием тайно передать ее коллеге, германскому послу в Мексике, Генриху фон Эккардту:

«Мы намерены с первого февраля возобновить неограниченную подводную войну. Тем не менее, следует предпринять все попытки к тому, чтобы США и дальше сохраняли нейтралитет. Однако, если такие попытки окажутся безуспешными, мы предложим Мексике заключить союз на следующих условиях: совместное ведение боевых действий и совместное заключение мира; серьезная финансовая поддержка с нашей стороны и понимание нами стремления Мексики по возвращению утраченных территорий в Техасе, Нью-Мексико и Аризоне. Детали соглашения оставляются на ваше усмотрение [фон Эккардта].

Вы должны довести до сведения Президента [Мексики] о вышеуказанном с соблюдением максимальной степени секретности, как только станет точно известно о начале войны с США, и в дополнение к этому предложить ему по собственной инициативе пригласить Японию для немедленного присоединения к союзу и стать посредником между Японией и нами.

Пожалуйста, обратите внимание Президента на тот факт, что использование наших подводных лодок в полной мере открывает перспективу заставить Англию в течение нескольких месяцев заключить мир».



WESTERN UNION TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

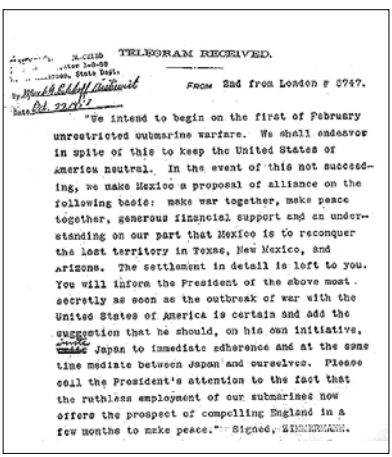
130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0502 21290 5161 39695
23571 17504 11269 18276 18101 0517 0828 17694 4473
22284 22200 19452 21589 67893 5569 13918 6958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17563 67893 5870 5454 16102 15217 22801 17158
21001 17388 7446 23638 18222 6719 14331 15021 23645
3186 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22220 5905 13347 20420 39589 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9546 9559 22464 15874 18502 18500 15857
2188 5576 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

Если бы содержание телеграммы сделалось достоянием общественности, это наверняка бы привело к началу войны между Германией и США.

Телеграмма Циммермана, отправленная послом Германии в Вашингтоне своему коллеге в Мексике, Генриху фон Эккардту

Кайзер Вильгельм II, разумеется, понимал, что после того, как немецкие подводные лодки начнут действовать с нарушением Гаагских конвенций, война сделается неизбежной, однако он надеялся, что к тому времени Великобритания капитулирует и США попросту не успеют включиться в завершившийся военный конфликт. К тому же, активная угроза со стороны Мексики у южных рубежей США заставит американцев сто раз подумать, прежде чем вступать в конфликт, происходящий вдали от их границ.



TELEGRAM RECEIVED.

FROM 2nd from London # 8747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

Та же телеграмма, но в расшифрованном виде

Но Мексике требовалось некоторое время для подготовки своих вооруженных сил. Поэтому было жизненно необходимо, чтобы тайные намерения Германии оставались неизвестными американцам достаточно долго.

Однако у британского правительства были другие планы. Вскоре после начала войны британцы перерезали подводные телеграфные кабели, которые соединяли Германию с западным полушарием напрямую. Таким образом связь должна была осуществляться через другие кабели — те, где британцы могли перехватывать сообщения. США пытались добиться переговоров об окончании войны и поэтому позволяли Германии продолжать передавать дипломатические послания. В результате послание Циммермана было получено немецким посольством в Вашингтоне в целости и сохранности.

Британское правительство отправило перехваченное послание в отдел, занимавшийся дешифровкой и взломом кодов, который назывался «комната № 40».

Немцы использовали свой обычный алгоритм шифрования, которым пользовалось Министерство иностранных дел, а также шифр, известный, как 0075, который эксперты из комнаты № 40 уже частично взломали. Указанный алгоритм включал замену слов (кодирование), а также букв (шифрование). Эта практика была подобна той, которая использовалась немцами в еще одном шифровальном инструменте того времени, шифре ADFGVX, который мы более подробно рассмотрим ниже.

Британцам не потребовалось много времени для расшифровки телеграммы. Правда, они не хотели сразу же доводить ее содержание до американцев. Для этого имелись две причины.

Во-первых, секретная телеграмма была отправлена под дипломатическим прикрытием, которое США обеспечивали немецким посланиям, а британцы эту привилегию напрочь проигнорировали. Во-вторых, если бы телеграмму сделали достоянием общественности, то немецкое правительство сразу же узнало бы, что его коды взломаны, и немедленно изменило систему шифровки.

Поэтому британцы решили сообщить американцам, будто бы раздобыли содержание телеграммы, полученной фон Эккардтом, чтобы таким образом убедить немцев, что телеграмма перехвачена уже расшифрованной, в Мексике.

В конце февраля правительство Вильсона передало содержание телеграммы прессе. Некоторые представители прес-

сы, в частности газеты, принадлежащие издательскому дому «Херст» (Hearst), который был настроен против возможной войны и прогермански, вначале отнеслись к ней весьма скептически. Однако к середине марта Циммерман публично признал авторство противоречивого послания. Чуть более двух недель спустя, 6 апреля 1917 года, Конгресс США объявил войну Германии.

Это решение имело далеко идущие последствия для Европы и мира...

В заключение отметим, что хотя телеграмма Циммермана и стала чрезвычайным событием своего времени, но это всего лишь одна историческая страничка, в которой важную роль сыграла криптография.

На протяжении этой книги мы увидим немало других примеров, разбросанных по столетиям и культурам.

Тем не менее, мы почти наверняка можем утверждать, что далеко не все знаем о самых важных исторических событиях.

Ведь благодаря своей природе история криптографии — это история тайн.

ГЛАВА 2.
КРИПТОГРАФИЯ ОТ АНТИЧНЫХ ВРЕМЕН ДО XIX СТОЛЕТИЯ

Как мы уже отмечали, криптография — это весьма древняя наука, вероятно, столь же древняя, как и сама письменность.

Однако это далеко не единственный возможный способ тайной передачи информации. В конце концов, любой текст при прочитывании должен восприниматься как текст, а если возможность прочитывания скрыта ото всех, кроме получателя, то мы достигли цели.

Наука о скрытой передаче информации путём сохранения в тайне самого факта передачи называется стеганографией (от греч. *στεγανοσ* — скрытый и греч. *γραφω* — пишу, буквально «тайнопись»). Вероятно, она возникла примерно в то же время и по тем же причинам, что и криптография.

СКРЫТЫЕ ПОСЛАНИЯ

Древнегреческий ученый Геродот, считающийся одним из величайших в мире историков, упоминает в своей знаменитой «Истории», посвященной описанию греко-персидских войн в V веке до н. э., два любопытных случая применения стеганографии, которые свидетельствуют о большой находчивости людей того времени.

ГЕРОДОТ ГАЛИКАРНАССКИЙ

Древнегреческий историк, живший в V в. до н. э., автор первого полномасштабного исторического трактата — «Истории», описывающего греко-персидские войны и обычаи многих современных ему народов. Труды Геродота имели огромное значение для античной культуры. Цицерон назвал его «отцом истории». Геродот — чрезвычайно важный источник по истории Великой Скифии, включающей десятки античных народов на территории современной Украины и России.

В первом примере, который содержится в «Талии», третьей книге «Истории», Гистией, тиран города Милет, приказал одному человеку побрить голову. Затем он написал на бритой голове послание и стал ждать, пока у мужчины снова вырастут волосы. После того, как они отросли, посыльного отправили в лагерь Аристагора. Добравшись туда, посыльный объяснил суть дела Аристагору, и волосы снова сбрили, открыв таким образом сообщение, которого здесь давно ждали.

Второй пример, если это, конечно, происходило на самом деле, имеет гораздо большую историческую важность, поскольку позволил Демарату, царю Спарты, находящемуся в ссылке в Персии, предупредить своих соотечественников о грядущем вторжении персидского царя Ксеркса. Эту историю Геродот рассказывает в «Полигимнии», седьмой книге «Истории»:

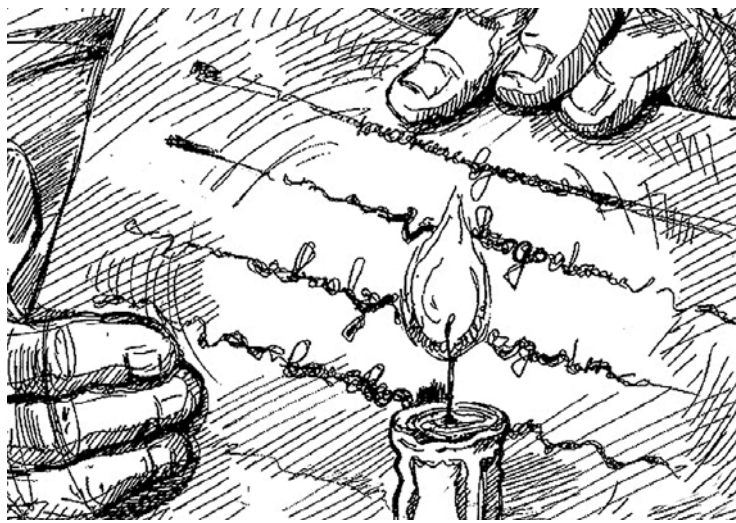
«Демарат не мог открыто предупредить их, поэтому ему пришла в голову такая мысль: он взял пару табличек [для письма], соскоблил с них воск и написал о планах царя на деревянной поверхности табличек. Затем он снова покрыл их расплавленным воском и таким образом скрыл сообщение.

В результате казавшиеся пустыми таблички не вызывали никаких подозрений у стражников в дороге.

Когда таблички наконец оказались в Лакедемоне (Спарта), тамошние жители не могли понять, в чем тут секрет, пока, насколько я понимаю, Горго [...] не предложила соскоблить воск с табличек, потому что под ним — как она подсказала — найдут написанное на дереве послание».

Стеганографическое средство, которое выдержало испытание временем, — это симпатические (невидимые) чернила. Их применение описано в тысячах рассказов и фильмов. Используемые материалы — лимонный сок, сок растений и даже человеческая моча — обычно органического происхождения и имеют высокое содержание углерода. Поэтому высохшие чернила имеют склонность к потемнению, когда оказываются под воздействием умеренно высоких температур, как, например, жар от пламени свечи.

Полезность стеганографии нет смысла оспаривать, хотя она делается совершенно непригодной, когда речь идет о больших количествах посланий. Более того, если ее использовать напрямик, без дополнительных ухищрений, у нее имеется один существенный недостаток: если послание однажды все-таки перехватят, содержание его сразу же станет



известным. По этой причине стеганография в основном используется как дополнение к криптографии, как средство усиления безопасности сверхсекретных передач.

Из приведенных примеров мы можем сделать вывод, что вооруженные конфликты являлись мощным стимулом и побудительным мотивом для развития безопасности информационных сообщений.

Поэтому неудивительно, что такие воинственные люди, как спартанцы (если верить Геродоту, они являлись мастерами стеганографии), также стали первопроходцами и в развитии криптографии.

ТРАНСПОЗИЦИОННАЯ КРИПТОГРАФИЯ

В вооруженном конфликте между спартанцами и афинянами за контроль над Пелопоннесом часто использовались длинные полоски пергамента, обернутые вокруг цилиндрической палки, которую называли ***скитала***. Послание писали на пергаментной полосе, которой оборачивали цилиндр. Даже если противник знал, какая использовалась техника шифрования (то есть алгоритм), если точные размеры скиталы не были известны, то любой, кто перехватывал сообщение, сталкивался с огромными трудностями для его расшифровки. Толщина и длина скиталы по сути являлись ключом шифровальной системы. Когда пергаментную полосу разматывали, послание становилось неподдающимся прочтению.

Скитала позволяет использовать криптографическую технику, при применении которой полностью меняется порядок букв в послании. Чтобы получить представление об этом методе, который называется транспозицией, давайте рассмотрим простой пример с перестановкой всего трех букв: А, О и Р. Не требуется никаких расчетов, чтобы выяснить, что эти буквы могут были расставлены шестью возможными способами: АОР, АРО, ОАР, ОРА, РОА и РАО.

Если говорить абстрактно, то процесс следующий: после того, как одна из трех возможных букв ставится на первое место, позволяя три различных варианта расстановки,

А = СООБЩЕНИЕ С ПОМОЩЬЮ СКИТАЛЫ
Б = СС О С ОПК БОИ ЩМТ ЕОА НЩЛ ИЬЫ ЕЮ

А – *послание , которое предстоит передать,* **Б** – *но если полоску бумаги развернуть, то получается полная чушь, набор ничего не значащих букв*

мы остаемся с двумя буквами, которые, в свою очередь, можно расставить двумя различными способами, чтобы получить новый общий результат: 3 × 2 = 6 вариантов расстановки. В случае более длинного послания, например, из 10 букв, количество возможных расстановок получается: 10×9×8×7×6×5×4×3×2×1. Такая операция называется факториал, выражается математическим обозначением ***10!*** и дает общий результат 3628800. Если говорить в общем, о количестве букв ***n***, то есть ***n!*** различных способов их перестановки. Таким образом, послание, которое состоит всего из 40 букв, может дать такое количество возможных способов перестановки букв, что расшифровать его вручную становится практически невозможно.

Неужели мы нашли идеальный криптографический метод?..

Увы, не совсем. По сути алгоритм перестановки (транспозиции) наугад дает наиболее высокий уровень безопасно-

С КРОШЕЧНЫМИ БУКВАМИ

Во время холодной войны в полных драматизма шпионских триллерах главные герои часто отправляли послания при помощи средства, на котором буквы оказывались слишком мелкими для чтения невооруженным глазом, – микрофильма. Техника родилась за несколько лет до начала холодной войны, в годы Второй мировой, когда немецкие агенты использовали стеганографическую технику, известную как микрофотоснимок, то есть фотоснимок с очень большим уменьшением. Он состоял из фотографии короткого текста, которая сводилась до размера точки, которую затем включали

в виде одного из многочисленных символов в безобидный текст.

сти, но что будет представлять из себя ключ, который позволит расшифровать послание?!

Случайность процесса — это одновременно и сила его, и слабость.

Требовался способ шифрования, который бы дал ключи, являющиеся одновременно простыми, легкими для запоминания и передачи, но в то же время не требующие в существенных объемах жертв, связанных с безопасностью.

В результате начался поиск идеального алгоритма, и первых успехов в этом достигли римские императоры.

РУКОВОДСТВО ДЛЯ ЮНЫХ ЛЕДИ

«Камасутра» — это легендарная книга, в которой, среди всего прочего, присутствует информация, которая требуется женщине, чтобы быть хорошей женой. Книгу написал примерно в IV веке до н. э. брахман Малланага Ватсьяяна. В ней рекомендуется до шестидесяти четырех различных умений, включая музыку, приготовление пищи и игру в шахматы. Для нас особый интерес представляет пункт сорок пять, потому что он посвящен искусству тайного письма, или «млекчита-викалпа». Автор рекомендует несколько способов, включая следующий: разделите алфавит пополам и наугад сгруппируйте по парам получившиеся буквы. При этой системе каждая пара букв представляет собой ключ. Например, один из вариантов в латинице может быть следующим:

A B C D E F G M L K J I H
T U V W X Y Z S R Q P O N

Чтобы написать тайное послание, требуется всего лишь заменять каждую букву A в изначальном тексте на T, G на Z, H на N и т. д., и наоборот.

ШИФР ЦЕЗАРЯ

«Veni, vidi, vici» (Пришел, увидел, победил).

Юлий Цезарь

Шифры, в которых используется замена (то есть шифры замены или шифры подстановки), развивались параллельно с шифрами, в которых используется перестановка (транспозиционными шифрами). В отличие от транспозиции, при строгой замене одна буква заменяется другой или любым типом символа. В отличие от транспозиции, при замене необязательно пользоваться только буквами, из которых состоит послание. При транспозиции буква меняет свою позицию, но сохра-

няет свою роль. Та же самая буква имеет то же самое значение в исходном послании и в зашифрованном послании. При замене буква остается на своей позиции, но меняет свою роль (та же самая буква или символ имеет одно значение в исходном послании и совсем другое — в зашифрованном послании). Один из первых известных алгоритмов подстановки — это так называемый шифр Полибия, названный в честь греческого историка Полибия (около 203 — около 120 гг. до н. э.), который оставил нам его описание. Его метод подробно описан в Приложении 1 в конце этой главы.

Примерно через полвека после шифра Полибия, в первом веке до н. э., появился еще один шифр, в котором используется принцип замены.

Он известен под названием «шифр Цезаря», поскольку Юлий Цезарь был одним из самых известных людей, которые его использовали. Шифр Цезаря — один из самых изученных в сфере криптографии и является исключительно полезным, потому что иллюстрирует принципы модульной арифметики, одной из математических основ написания закодированных посланий.

Шифр Цезаря основан на принципе, когда каждый символ в начальном тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите.

Например, в шифре со сдвигом 3 А была бы заменена на Г, Б станет Д, и так далее.

По словам великого историка Светония, автора «Жизни двенадцати Цезарей», Юлий Цезарь кодировал свои личные письма при помощи алгоритма замены следующего типа: каждая буква оригинала заменялась на другую, которая стояла в алфавите через три позиции после нее: A заменялась на D, B на E, и т. д. W заменялась на Z, и таким образом получалось, что X, Y и Z заменяются на A, B и C.

Кодирование и декодирование послания, зашифрованного таким методом, можно провести с использованием простого приспособления, подобного изображенному на рисунке.

Теперь рассмотрим процесс более подробно. В таблице, приведенной на следующей странице, мы на примере латини-

цы видим изначальный алфавит и трансформированный алфавит, который получился с использованием шифра Цезаря и заменой буквы на другую букву, расположенную через три позиции от нее дальше по алфавиту (в верхнем ряду показан исходный алфавит, в нижнем ряду — шифровальный алфавит).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Когда два алфавита, исходный и шифровальный, располагаются таким образом, то шифрование послания — это просто вопрос замены букв одного буквами другого. Ключ к шифру называется по букве, которая соответствует зашифрованной A (первой букве исходного алфавита). В данном случае это

КИНО И КОДИРОВАНИЕ

В классическом научно-фантастическом фильме «2001: Космическая Одиссея» (1968) американского кинорежиссера Стэнли Кубрика на основе романа Артура Кларка наделенный сознанием суперкомпьютер космического корабля, который называется HAL 9000, сходит с ума и пытается убить экипаж, состоящий из людей. А теперь проанализируйте слово HAL так, будто перед нами послание, зашифрованное при помощи шифра Цезаря с ключом B. В этом случае буква H будет соответствовать букве I, A соответствует B, а L соответствует M. Получится аббревиатура IBM, в то время — крупнейший производитель компьютеров в мире. Интересно, в фильме пытались рассказать об опасности, которую представляет искусственный интеллект? Или об опасности бесконтрольной власти коммерсантов? А может, это просто совпадение?

D. Классическое выражение AVE CAESAR (Здравствуй, Цезарь) будет зашифровано как DYH FDHVDU. И наоборот, зашифрованное послание WUHH после расшифровки дает TREE (дерево).

В случае использования только что описанного шифра Цезаря, при перехвате послания, если дешифровщик знает лишь, какой алгоритм использовался, но не знает ключа, то ему потребуется использовать все возможные варианты, пока не получится послание, имеющее смысл. Для этого, самое большее, ему потребуется проверить все ключи. Если алфавит состоит из n букв, то количество возможных замен даст n кодов.

ОТЕЦ АНАЛИТИЧЕСКОЙ КРИПТОГРАФИИ

Евклид — древнегреческий математик, автор первого из дошедших до нас трактатов по математике. Основная его работа «Начала» (в латинизированной форме — «Элементы») содержит изложение планиметрии, стереометрии и ряда вопросов теории чисел; в ней он подвёл итог предшествующему развитию математики и создал фундамент дальнейшего развития этой науки. Хотя в общественном сознании его работы больше всего ассоциируются с геометрией пространства, она связана и с арифметическими операциями с конечным количеством чисел, или модулями, и представляет собой один из основных трудов, изучаемых современной криптографией. Арабские ученые давно знали и восхищались работами Евклида, но первое издание работ Евклида в Европе появилось в Венеции в 1482 году. Думается, нельзя считать совпадением то, что и арабы, и венецианцы были великими мастерами криптографии.

МОДУЛЬНАЯ АРИФМЕТИКА И ШИФР ЦЕЗАРЯ

16=4? и 2=14? Это не ошибка и не какая-то странная система нумерации. Действие шифра Цезаря может быть сформулировано при помощи инструмента, который является обычным делом в математике и даже в еще больше степени в криптографии — модульной (или модулярной) арифметики, которую иногда называют часовой арифметикой. Эта техника ведет свое начало с работы греческого математики Евклида (325—265 гг. до н. э.) и является одной из основ современного обеспечения безопасности информации. В этом разделе мы представим базовые математические концепции, связанные с этим особым типом арифметики.

Возьмите классические аналоговые часы в качестве примера и сравните их с цифровыми. При аналоговом распределении часов круг разделен на 12 частей, которые мы запишем как 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11. Обозначение часов после полудня в аналоговых и цифровых часах представлено в таблице:

0	1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22	23

Мы, например, заявляем, что сейчас пятнадцать часов, но иногда говорим, что три часа пополудни.

Тот же самый принцип применяется при измерении углов.

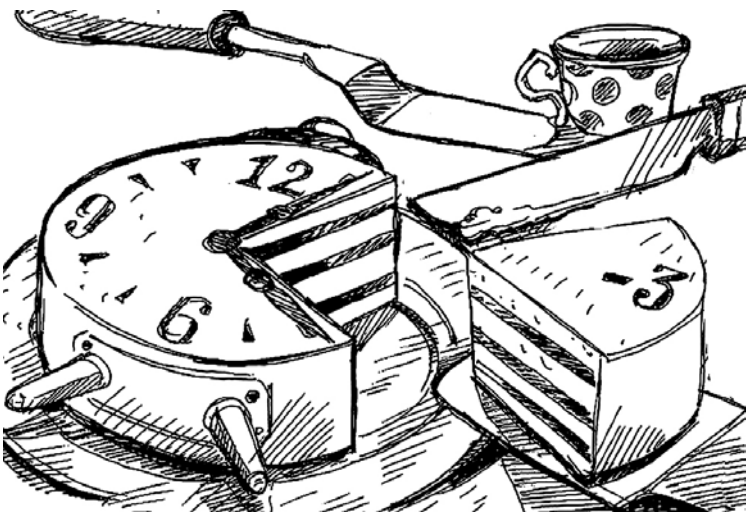
К примеру, угол 380° — это эквивалент углу в 20°, потому что вам требуется вычесть из первого значения полный оборот в 360°. Обратите внимание, что $380 = (1 \times 360) + 20$ и что 20 также представляет остаток при делении 380 на 360.

А какой угол является эквивалентом 750°?

После вычитания соответствующего количества полных оборотов мы находим, что эквивалентом угла в 750° является угол в 30°. Мы делаем вывод, что $750 = 2 \times 360 + 30$, а 30 — это остаток деления 750 на 360. Математическими обозначениями для этого являются:

$$750 \equiv 30 \pmod{360}$$

И мы говорим, что «750 конгруэнтно 30 по модулю 360».



А заменив градусы на часы, мы напишем: $14 \equiv 2 \pmod{12}$.

Мы спокойно можем представить себе часы и с отрицательными числами.

В таком случае, сколько будет времени, когда стрелка часов показывает на –7? Или, другими словами, чему конгруэнтно –7 по модулю 12? Давайте вычислим это, помня, что значение «0» в наших часах, состоящих из 12 частей, эквивалентно «12»:

$$-7 = -7 + 0 \equiv -7 + 12 = 5$$

Математика расчетов с нашими аналоговыми часами, состоящими из 12 частей, называется арифметикой по модулю 12. В общем и целом мы можем сказать, что $a \equiv b \pmod{m}$, если остаток деления между a и m — это b, при условии, что a, b и m — целые числа. Число b эквивалентно остатку деления a на m. Следующие утверждения эквивалентны

$a \equiv b \pmod{m}$
$b \equiv a \pmod{m}$
$a — b \equiv 0 \pmod{m}$
a — b — кратное m число.

Вопрос «Какое время аналогично 19 часам?» эквивалентен с математической точки зрения вопросу «Чему конгруэнтно

РАСЧЕТЫ С МОДУЛЯМИ

Проанализируем число 231 по модулю 17 при помощи калькулятора.

Вначале мы делим 231 на 17 и получаем:

13,58823529.

Затем, отбросив цифры после запятой, умножаем целое число в полученном результате $13 \times 17 = 221$.

Наконец мы производим вычитание 231—221 = 10, таким образом получая остаток после деления.

231 по модулю 17 — это 10. Результат выражается как $231 \equiv 10 \pmod{17}$.