Глава 5 | Засекреченные биты

Как создаются криптостойкие шифры

Средства шифрования в руках террористов и прочих

13 сентября 2001 года, Нью-Йорк, США. Пламя все еще бушует над обломками Всемирного торгового центра. В это время представитель штата Нью-Хэмпшир Джадд Грег докладывает Сенату о случившемся. Сенатор повторяет предупреждения, сделанные ФБР несколько лет назад: одним из самых серьезных препятствий для работы спецслужб является «возможность обмениваться зашифрованной информацией людям, намеренным принести вред стране». «Мы привыкли, – продолжал сенатор Грег, – что можем взломать большинство шифров с помощью наших средств и интеллекта».[1] И не более того. «Технология превзошла возможности криптоаналитиков».[2] Даже либеральный гражданский специалист по шифрованию Фил Циммерманн, чьи общедоступные программы для шифрования с 1991 года применяли борцы за права человека во всем мире, признал, что террористы в принципе могли шифровать свою переписку. «Я всего лишь допускаю, – заявил Фил Циммерманн, – что некто, планирующий настолько дьявольское действие, мог бы пожелать скрыть свои приготовления с помощью технологий шифрования».[3]

Шифрование (криптография) – это искусство кодирования сообщений, так что они не могут быть прочитаны противником или любителями читать чужие письма. Чтобы расшифровать сообщение, требуется знать последовательности символов – «ключ», которым оно было зашифровано. Зашифрованное сообщение может быть доступно

---

1 Стенограмма заседания Конгресса, 13 сентября 2001 года, с. S9357.

2 Джон Шварц (John Schwartz) «Disputes on electronic messages: Encryption takes on new urgency» (Диспуты по электронным сообщениям: второе рождение шифрования), *New York Times* от 25 сентября 2001 года.

3 Там же.

кому угодно, но без ключа его содержимое так же остается в тайне, как если бы сообщение хранилось в закрытом сейфе. Пока нет ключа – подходящего ключа – сейф (или сообщение) продолжает хранить свою тайну.

Когда требовалось, была и «совместная общественная деятельность, которая спроектировала и реализовала программное обеспечение и построила среду, обеспечивающую существование технологий шифрования», – утверждал сенатор Грег. Эта деятельность регулировалась законодательством. Создатели программ для шифрования должны были предоставить правительству лазейки для обхода защиты и декодирования сообщений. Но программы создавались по всему свету и могли распространиться в мгновение ока, как это произошло с программами Циммерманна. Для создания доступных правительству США «черных ходов» в программах Соединенные Штаты должны были бы использовать «американский рынок как средство» формирования зависимости иностранных поставщиков и вынудить их действовать по американским правилам.

К 27 сентября законодательная инициатива сенатора приобрела четкие формы. Ключи для шифрования сообщений следовало хранить у правительства под строгим секретом. Это будет «квази-правовая сущность», как постановил Верховный суд США, вынесший также решение о случаях, в которых ключи могли бы быть открыты. Борцы за права человека немедленно возмутились и выразили сомнение в том, что идея хранения ключей у третьей стороны вообще может работать. «Это ничего, – парировал сенатор в конце сентября. – Ничто не совершенно. Если мы не попытаемся, то ничего не сможем сделать. Если попытаемся, то приобретем, по крайней мере, фундамент для создания чего-то более совершенного».[1]

Спустя три недели сенатор Грег внезапно приостановил движение своей законодательной инициативы. «Мы не работаем над законопроектом о шифровании и не намерены этого делать», – заявил представитель сенатора 17 октября 2001 года.[2]

24 октября 2001 года Конгресс принял Акт о патриотах, давший ФБР существенно новые возможности в борьбе с терроризмом. Но в Акте нет ни слова о шифровании. После инициативы сенатора Грега власти США не предприняли никаких серьезных попыток законодательно контролировать разработку программного обеспечения для шифрования.

---

[1] Там же.

[2] Деклан МакКалло (Declan McCullagh) «Senator backs off backdoors» (Сенатор ведет скрытые действия), *Wired News* от 17 октября 2001 года.

Почему бы не контролировать шифрование?

В 1990-х ФБР сделало контроль шифрования своим правовым приоритетом. Инициатива сенатора была довольно мягкой формой законопроекта, разработанного ФБР и предложенного к рассмотрению избираемым Комитетом Сената по разведке (United States Senate Select Committee on Intelligence, SSCI) в 1997году.[1] В тексте проекта, в частности, содержалось предложение о заключении в тюрьму сроком на пять лет того, кто продавал программы для шифрования, не обеспечивающие представителями власти возможность немедленного декодирования сообщений.

Как могли меры, представлявшиеся необходимыми для борьбы с терроризмом в 1997 году, выпасть из поля зрения законодателей через четыре года после наиболее разрушительной террористической атаки, когда-либо предпринятой в отношении Соединенных Штатов?

Осенью 2001 года ни в законодательстве о криптографии, ни в соответствующей дипломатии не произошло существенных сдвигов. Никаких других оснований считать применение технологий шифрования террористами или организованной преступностью малозначительной проблемой также не было найдено. Сформировалось лишь еще одно важное явление в сфере практической криптографии – бурный рост числа коммерческих транзакций, совершенных через Интернет. И Конгресс внезапно осознал, что для экономики просто необходимо разрешить банкам и их клиентам, авиалиниям и пассажирам, аукциону eBay и магазину Amazon применять средства шифрования. Каждый, кто совершает коммерческие операции через Интернет, нуждается в криптографических средствах обеспечения безопасности сделки. Многим людям во всем мире стали вдруг понадобились надежные средства шифрования, и от этого зависела вся мировая экономика.

Напряжение между обеспечением надежности коммерческих операций и предотвращением тайной переписки между преступниками ощущалось около десяти лет. Сенатор Грег был одним из последних инициаторов ввода ограничений применения технологий шифрования. Национальный совет США по научным исследованиям (United States National Research Council, NRC) в 1996 году выпустил отчет на 700 страницах, в котором были указаны достоинства и недостатки использования криптографических средств. В заключении отчета указы-

[1] «Тот, кто после 31 января 2000 года будет продавать на внутреннем или внешнем рынке криптографические продукты, не содержащие свойств или функций, позволяющих официально уполномоченным лицам получить немедленный доступ к открытому тексту или расшифровать данные, может быть наказан тюремным заключением на срок до пяти лет с наложением штрафа или без оного», 105-е заседание Палаты представителей Конгресса, отчет 695, 104–108, часть 4 Акта о безопасности и свободе при помощи шифрования 1997 года, раздел 2803.

валось, что попытки контролировать технологии шифрования будут неэффективны и что вред, нанесенный этими действиями, превысит возможные выгоды.[1] Отчет не убедил представителей служб разведки и обороны страны. Директор ФБР Луи Фри, выступая перед Конгрессом в 1997 году, заявил, что «ограничивающее законодательство является выражением нашего общего мнения о том, что широкомасштабное применение криптостойких <не предоставляющих правительству ключ> средств шифрования окончательно сведет к нулю все наши возможности по борьбе с терроризмом и организованной преступностью».[2]

Даже четыре года спустя после атаки 11 сентября для нужд экономики не было предложено ни одной альтернативы повсеместному распространению криптографического программного обеспечения и использованию его на компьютерах коммерческих организаций или граждан, совершающих электронные сделки. В 1997 году рядовые граждане (так же, как и выборные представители власти) не могли что-то купить во время интернет-сеанса. Члены семей конгрессменов едва ли были активными компьютерными пользователями. К 2001 году все это изменилось – цифровая экспансия набрала темп. Компьютер стал обычным потребительским товаром, Интернет вошел в дома американцев – и вместе с ним пришла опасность кражи персональной (в том числе, финансовой) информации. Пользователи не хотели, чтобы их даты рождения, номера кредиток или идентификаторы социального страхования появились в Интернете для всеобщего обозрения.

Почему шифрование настолько важно для интернет-коммуникаций, что Конгресс США позволил себе пренебречь террористической угрозой ради возможности применения технологий шифрования коммерческими организациями и отдельными потребителями? Прежде всего, в необходимости защиты информации нет ничего нового. Те, к примеру, кто отправляет письма в конвертах обычной почтой, достаточно уверены в конфиденциальности безо всякой криптографии.

Ответ связан с открытой архитектурой Интернета. Биты пересылаются по Сети не непрерывным потоком, а отдельными блоками – пакетами. Пакет состоит не больше, чем из 1500 байт (см. приложение). Пакеты данных можно сравнить не с конвертами, где адрес снаружи, а содержимое внутри, а с открытками, где вся информация на виду. По мере перемещения по Интернету пакеты путешествуют от одного промежуточного компьютера к другому. Эти узловые компьютеры называются *маршрутизаторами*. Каждый пакет данных при попадании к маршрутизатору сохраняется, проверяется, анализируется

---

[1] Национальный совет по научным исследованиям, Кеннет У. Дэм и Герберт С. Лин (Kenneth W. Dam, Herbert S. Lin) «Cryptography's Role in Securing the Information Society» (Роль криптографии в обеспечении безопасности информационного общества), National Academy Press, 1996.

[2] Выступление директора ФБР Луи Фри (Louis Freeh) перед сенатскими слушаниями по шифрованию 9 июля 1997 года.

и пересылается ближе к пункту назначения. Для оптоволоконных или медных кабелей можно обеспечить защиту и неприступность, но при пересылке данных по беспроводным каналам биты могут быть считаны из эфира, причем без всякой возможности узнать о факте считывания.

Отправить номер своей кредитки универмагу в простом сообщении электронной почты – примерно то же самое, что выйти на Таймс Сквер и объявить его во всеуслышанье. К 2001 году огромное количество кредитных номеров путешествовало в виде битов по оптволоконным кабелям или в эфире и не было никакой возможности помешать любителям шпионажа считать эти данные.

Способ обеспечения безопасности интернет-коммуникаций – чтобы никто, кроме адресата, не мог прочесть сообщение – заключается в шифровании данных. Только получатель должен иметь возможность декодировать сообщение. В этом случае любители шпионажа могут сколько угодно исследовать пакеты на пути между маршрутизаторами. Все, что получит излишне любопытный пользователь, – это бессмысленный набор битов.

В мире, где началась электронная коммерция, криптография больше не может быть тем, чем она была с античности до начала третьего тысячелетия: оружием, применяемым военачальниками и дипломатами для защиты жизненно важных государственных секретов. Даже в начале 1990-х Государственный департамент США постановил, что исследователь криптографических методов должен был регистрироваться подобно международному торговцу оружием. Нынче криптография гораздо больше похожа на инкассаторский броневик, чем на оружие. Она уже не военное снаряжение, а деньги.

Создание потребительской ценности этого прежде военного средства уже не просто технологический сдвиг. Оно породило и продолжает порождать переосмысление фундаментальных понятий о неприкосновенности частной жизни и о балансе между безопасностью и свободой в демократическом обществе.

«Вопрос в том, – рассуждает Рональд Ривест, профессор информатики Массачусетского технологического института и один из ведущих американских специалистов по криптографии, – смогут ли люди общаться, не находясь при этом под наблюдением правительства, даже если таковое наблюдение полностью одобрено судебным решением».[1] В атмосфере, создавшейся после 11 сентября 2001 года и породившей Патриотический акт, трудно было поверить, что Конгресс ответит на вопрос профессора Ривеста утвердительно. Однако рыночная действительность дала свой ответ.

---

[1] Заявление Рона Ривеста (Ron Rivest) на пресс-форуме, Массачусетский технологический институт 7 апреля 1998 года.

Чтобы удовлетворить нужды электронной коммерции, криптографическое программное обеспечение должно быть широко доступно. Оно должно работать быстро и надежно, обеспечивая устойчивость к взлому. Кроме того, хотя история криптографии насчитывает не менее четырех тысяч лет, ни один из методов шифрования до конца двадцатого века не мог быть использован для ведения электронной коммерции. Однако в 1976 году двое молодых математиков, даже не работающих в разведке, – вот уж где действительно должны развиваться методы шифрования! – опубликовали статью, описывающую кажущуюся абсурдной реальность. Две стороны разрабатывали секретные ключи, позволявшие обмениваться зашифрованными сообщениями – даже если стороны никогда не встречались, а сообщения пересылались по открытым каналам. Разработанный метод *шифрования с открытым ключом* позволил любому мужчине, женщине или ребенку передавать номера кредитных карт интернет-магазину **Amazon более безопасно,** чем какой-нибудь генерал мог передавать свои приказы, от которых зависело выживание или уничтожение нации, еще 50 лет назад.

История криптографии

Криптография (от греч. «тайнопись») почти ровесница письменности. Существуют шифрованные сообщения в египетских иероглифах, нанесенные за две тысячи лет до нашей эры. *Шифрование* – это метод преобразования сообщения в непонятную форму, так чтобы восстановление исходного сообщения было возможным. Светоний, биограф Юлия Цезаря, описал его метод шифрования писем к оратору Марку Цицерону, с которым Цезарь обсуждал планы на будущее в последние дни Римской республики: «Если нужно было сообщить что-нибудь негласно, он пользовался тайнописью, то есть менял буквы так, чтобы из них не складывалось ни одного слова. Чтобы разобрать и прочитать их, нужно читать всякий раз четвертую букву вместо первой, например D вместо A и т. д.».[1] Другими словами, Цезарь применял побуквенное шифрование:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC
```

Чтобы зашифровать сообщение по методу Цезаря, замените каждую букву верхнего ряда соответствующей буквой из нижнего ряда. К примеру, начало «Записок Цезаря» «**Gallia est omnis divisa in partes tres**» (Галлия по всей своей совокупности разделяется на три части) будет зашифровано следующим образом:

```
Открытый текст:        GALLIA EST OMNIS DIVISA IN PARTES TRES
Зашифрованный текст:   JDOOLD HVW RPQLV GLYLVD LQ SDUWHV WUHV
```

[1] Гай Светоний Транквилл «Жизнь двенадцати цезарей: Божественный Юлий», часть 56, «Наука», 1993.

Оригинальное сообщение называется *открытым текстом*, а кодированное – *зашифрованным текстом* (или *шифртекстом*). Сообщение расшифровывается с помощью обратной подстановки.

Этот метод называется *сдвигом Цезаря*, или *шифром Цезаря*. Запомнить правило применения метода легко: сдвиньте алфавит трижды. Конечно, можно выполнить сдвиг большее или меньшее число раз. Алфавит Цезаря является целой семьей шифров с числом вариаций 25, по одной для каждой из возможностей сдвига латинского алфавита.[1]

Шифр Цезаря довольно прост; противник, знающий, что применен шифр Цезаря, может легко декодировать сообщение, перебрав все варианты сдвига. Но метод Цезаря является представителем целого класса *шифров простой замены*, в которых одна буква сопоставляется другой по общему правилу (так что одна и та же буква всегда «переводится» одинаково).

Шифров замены может быть создано гораздо больше, чем шифров с применением сдвига. К примеру, можно установить такое соответствие букв английского алфавита:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
XAPZRDWIBMQEOFTYCGSHULJVKN
```

так что **A заменяется на X, B – на A, C – на P и т. д. Это простой способ** замены перестановкой символов алфавита. Число возможных перестановок равно

$26 \times 25 \times 24 \times \cdots \times 3 \times 2$,

то есть примерно 4×10^{26} вариантов, что в 10 тысяч раз больше числа звезд в нашей Вселенной. Такое число перестановок перебрать невозможно. Шифр простой замены должен быть очень надежным – так казалось.

Взлом шифров замены

Примерно в 1392 году некий английский автор – раньше считалось, что это великий английский поэт Джеффри Чосер, – составил письменное руководство по работе с астрономическим прибором. Части этого руководства, озаглавленного **«The Equatorie of the Planetis»** (Движение планет)[2], были закодированы с помощью шифра замены (рис. 5.1). Загадка является более простой, чем кажется на первый взгляд, при

[1] В римском алфавите не было символов «J», «U» и «W», поэтому Цезарю были доступны лишь 22 сдвига.

[2] Folio 30 verso of Peterhouse MS. 75.I. Обсуждение авторства Чосера см. Дерек Дж. Прайс (Derek J. Price) «The Equatorie of the Planetis» (Движение планет), Cambridge University Press, 1955 и Кари Энн Рэнд Шмидт (Kari Anne Rand Schmidt) «The Authorship of The Equatorie of the Planetis» (Авторство «Движения планет»), Chaucer Studies XIX, D.S. Brewer, 1993.

том что в ней не так уж много текста, с которым можно работать. Известно, что текст написан на средневековом английском; посмотрим, что можно извлечь из этого факта.

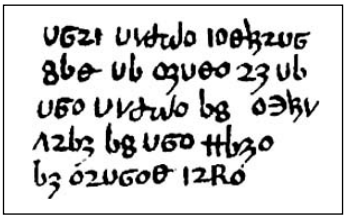

Рис. 5.1. *Зашифрованный текст из манускрипта «**The Equatorie of Planetis**»*

*Peterson **MS 75.1, том 30v. «The Equatorie of Planetis», манускрипт XIV века,** хранится в Кембриджском университете*

Хотя текст выглядит совершенно бессмысленным, в нем есть несколько ключевых элементов, за которые можно зацепиться. Например, определенные символы встречаются чаще других. В тексте насчитывается 12 символов 0 и 10 символов U; никакие другие символы не встречаются так же часто. В обычном тексте на английском языке чаще всего встречаются буквы **E и T, так что можно предположить, что упомянутые** символы соответствуют этим двум буквам. На рис. 5.2 показано, что произойдет, если предположить, что 0=**E** и U=**T. Сочетание** UG0 встречается дважды и представляет трехбуквенное слово **T?E. Это может** быть **TIE («связь») или TOE («носок обуви»), но слово THE (указательная частица)** кажется более вероятным; следовательно, G=**H.**

Рис. 5.2. *Зашифрованный текст из манускрипта «**The Equatorie of Planetis**»**: предполагается, что два наиболее часто встречающихся символа** представляют собой буквы **E и T***

Если это верно, то что это за четырехбуквенное слово в начале текста, начинающееся с TH? Это не THAT (местоимение «тот»), так как оканчивается пока неизвестным символом, и не THEN («тогда»), поскольку третий символ тоже неизвестен. Возможно, здесь зашифровано слово THIS (местоимение «этот»).

И еще есть двухбуквенное слово, начинающееся с T, встречающееся дважды во второй строке. Это должно быть TO (предлог «в» или обозначение неопределенной формы глагола). Результаты частичной расшифровки показаны на рис. 5.3.

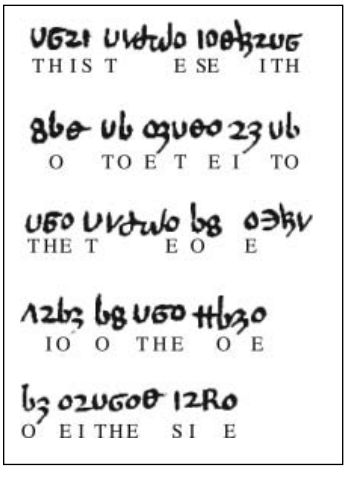

Рис. 5.3. *Зашифрованный текст из манускрипта «**The Equatorie of Planetis**»: **расшифрованы другие символы***

Расшифровка пошла на лад. Возможно, последние два слова – это EITHER SIDE, так что оставшиеся символы, зная средневековый английский и общую тематику текста, можно расшифровать без труда. Полностью декодированная фраза выглядит так: «THIS TABLE SERVITH FOR TO ENTRE IN TO THE TABLE OF EQUACION OF THE MONE ON EITHER SIDE» (данные из этой таблицы необходимо ввести в таблицу положений луны с любой стороны) (рис. 5.4).

Данный метод расшифровки называется *статистическим анализом*: если в зашифрованном тексте просто одни буквы заменены другими, то их соответствие можно установить, подсчитав, как часто те или иные буквы встречаются в тексте. Впервые эта идея была высказана арабским философом и математиком Аль-Кинди, жившим в Багдаде в IX веке.

В эпоху Возрождения этот способ расшифровки превратился в разновидность изящного искусства и стал широко применяться в европейских правящих кругах. Известный результат излишнего доверия ненадежным шифрам замены – казнь Марии Стюарт, чья переписка

Рис. 5.4. *Зашифрованный текст из манускрипта «**The Equatorie of Planetis**» расшифрован полностью*

с заговорщиками попала в руки королевы Елизаветы I. Мария Стюарт поплатилась головой за доверие данному способу скрытия тайн; однако шифры замены были популярны вплоть до XIX века, хотя их ненадежность была выявлена еще тысячу лет назад. Сюжеты рассказа Эдгара Аллана По «Золотой жук» (1843) и рассказа Артура Конана Дойля «Пляшущие человечки» (1903) из историй о Шерлоке Холмсе основаны на статистическом декодировании шифров замены.

Секретные ключи и одноразовые шифры

В прикладной криптографии каждый случай взлома кода порождает новый способ защиты от взлома. Убедившись, как просто взломать шифр астрономического манускрипта, мы можем попробовать найти способ сделать шифр более *стойким*, как говорят криптологи. Например, можно заменять одну букву несколькими.

Метод, носящий имя французского дипломата XVI века Блеза де Виженера, использует множество шифров Цезаря. К примеру, можно взять 12 шифров Цезаря и использовать первый шифр для кодирования 1-й, 13-й и 25-й букв открытого текста, второй шифр – для кодирования 2-й, 14-й и 26-й букв и так далее. На рис. 5.5 показан пример шифра Виженера. Открытое сообщение, начинающееся со слова «SECURE...», превратится в «llqgrw...» – как показано на рис. 5.5, S заменяется соответствующим символом из первого ряда, E – из второго и так далее. После достижения нижнего ряда необходимо снова вернуться к первому ряду и повторять процесс замены, пока не будет зашифрован весь открытый текст.

Рис. 5.5. *Шифр Виженера. Ключ к шифру – сочетание «**thomasbbryan**» – находится во второй колонке. Каждый ряд представляет собой шифр Цезаря, в котором величина сдвига определяется соответствующей буквой ключа.* ***(thomasbbryan – Томас Б. Брайен, адвокат, применивший данный шифр для*** *переписки со своим клиентом Гордоном МакКеем в 1894 году)*

Архив Гарвардского университета

Чтобы применить шифр с рис. 5.5, не нужно пересылать корреспонденту всю таблицу. Вторая колонка таблицы образует сочетание «thomasbbryan», которое и является ключом. Корреспондентам необходимо только условиться о ключе. Затем на основе ключа создается подстановочная таблица для шифрования и дешифрования сообщений.

Если слово «SECURE» зашифровывается в «llqgrw», то каждая из букв E кодируется разными буквами шифртекста; также буква l шифртекста представляет различные буквы открытого текста – S и E. Таким образом, шифр Виженера делает бесполезной попытку дешифрования с помощью статистического анализа, который в то время был главным инструментом криптоаналитиков. Хотя идея кажется очень простой, открытие Блеза де Виженера явилось прорывом в криптографии, и в течение нескольких сотен лет шифр считался абсолютно стойким (то есть невзламываемым).

Криптологи моделируют операции пересылки зашифрованных данных с помощью шаблонных персонажей: Алиса отправляет сообщение, Боб его получает, а Ева – противник, который может подключиться к каналу связи.

Предположим, Алиса хочет передать Бобу сообщение (рис. 5.6). Здесь подходит метафора «замок–ключ»: Алиса помещает сообщение в ящик и запирает его ключом, который есть только у нее и у Боба (допустим, что замок ящика запирается и отпирается только ключом). Если Ева перехватит ящик по дороге, то не сможет открыть замок без ключа. А Боб, получив ящик, сможет открыть замок своим ключом. До тех

Рис. 5.6. *Стандартный сценарий пересылки зашифрованных данных. Алиса собирается передать сообщение Бобу и зашифровывает текст секретным ключом. Боб дешифрует текст с помощью своей копии ключа. Ева (противник) перехватывает зашифрованное сообщение и пытается восстановить исходный текст*

пор пока форма ключа хранится в тайне, не имеет значения тот факт, что посторонние могут осматривать ящик снаружи или даже узнать принцип конструкции замка. Аналогично, если некий текст закодирован шифром Виженера, восстановить текст, не зная ключ шифра, почти невозможно.

Или, по крайней мере, так считалось. В действительности, шифр Виженера был взломан в середине XIX века английским математиком Чарльзом Бэббиджем, которого ныне считают создателем вычислительных машин. Бэббидж выяснил, что если возможно угадать или как-то вычислить длину ключа и соотнести ее с цикличностью повторения шифра, то проблема взлома сводится к нахождению всего нескольких подстановок. Чтобы вычислить длину ключа, Бэббидж применил статистический анализ. Математик так и не опубликовал свой метод (возможно, под давлением службы разведки).[1] Независимо от Бэббиджа офицер прусской армии Вильям Казиский нашел способ взлома шифра Виженера и опубликовал его в 1863 году. С этого времени использование шифра Виженера перестало быть безопасным.

Надежный способ защиты от взлома шифра Виженера заключается в использовании ключа, длина которого равна числу символов в сообщении; таким образом, шифр не повторяется. Если нам необходимо зашифровать 100 символов, нужно взять 100 шифров Цезаря и расположить их в 100 рядов подобно таблице на рис. 5.5. Каждый ряд будет использован только один раз. Такой метод назван *шифром Вернама*, по имени работавшего после Первой мировой войны изобретателя и сотрудника телеграфной компании AT&T telegraph Гилберта Вернама; также метод широко известен под названием *одноразового шифра*.

[1] О работе Ч. Бэббиджа в этом направлении стало известно только в 1970-х.

Криптография в истории

Криптография (шифрование) и криптоанализ (дешифрование, взлом шифров) были в центре многих поворотных событий человеческой истории. Тесное переплетение дипломатии, войн и технологий шифрования увлекательно описаны в книгах Дэвида Кана (David Kahn) «The Codebreakers» («Взломщики кодов») и Саймона Сингха (Simon Singh) «The Code Book» (Книга шифров).

Термин «одноразовый шифр» происходит от одного из способов реализации его применения. Предположим, что и у Алисы, и у Боба есть по одинаковому блокноту, на каждой странице которого написан уникальный ключ шифра. Алиса зашифровывает сообщение ключом с первой страницы. Боб расшифровывает сообщение тем же ключом. После этого страницы из обоих блокнотов вырываются и уничтожаются. При этом важно заметить, что каждый ключ используется однократно и не создает статистических шаблонов, по которым был взломан шифр Виженера.

Одноразовые шифры применялись во время Второй мировой войны и в период «холодной войны» в форме брошюр, заполненных цифрами (рис. 5.7). В настоящее время власти также используют одноразовые шифры для важных сеансов связи. При этом генерируется множество ключей, передаваемых адресату на компакт-дисках (CD или DVD).

Одноразовый шифр, если им правильно пользоваться, не может быть взломан методами криптоанализа. В шифртексте просто не окажется шаблонов, которыми можно будет воспользоваться. В 1949 году Клод Шеннон открыл важную связь между теорией информации и криптографией.[1] (На самом деле, как раз исследования методов криптографии для военных нужд, которыми занимался Клод Шеннон, и привели к рождению его теории информации и связи.) Ученый математически доказал то, что казалось правильным интуитивно: в теории, одноразовый шифр является абсолютно стойким.

Но, как сказал Йоги Берра[2], «в теории нет разницы между теорией и практикой. На практике такая разница есть». Надежные одноразовые шифры трудно создавать. Если шифр содержит повторы или шаблоны, то, по Шеннону, одноразовый шифр перестает быть стойким. Более важным является то, что пересылка ключа между сторонами без потери или перехвата – трудная задача. Обыкновенно стороны долж-

[1] Клод Шеннон «Теория связи в секретных системах» по изданию: Клод Шеннон «Работы по теории информации и кибернетике», М., ИЛ, 1963.

[2] Йоги Берра (Yogi Berra) – знаменитый американский бейсболист, известный также своими ироническими высказываниями. – *Прим. перев.*

Рис. 5.7. *Немецкий одноразовый шифр, используемый для связи между Берлином и Сайгоном в 1940-е годы. На обложке предупреждение: «Использованные страницы могут содержать шифры сообщений, которые еще не были доставлены. Следует хранить страницы в течение времени, превышающего время доставки сообщений»*

Агентство национальной безопасности США

ны заранее передать ключи и надеяться на их успешную доставку. Длинные ключи труднее передать, чем короткие, так что появляется представляющий серьезную угрозу безопасности соблазн использовать ключи повторно.

КГБ СССР поддался этому искушению, что позволило разведкам Великобритании и США полностью дешифровать свыше трех тысяч дипломатических и агентурных сообщений в период с 1942 по 1946 годы.[1] Проект Агентства национальной безопасности США под названием **«VENONA» был рассекречен в 1995 году. Из открытых материалов стало** известно, что благодаря работе участников проекта были раскрыты агенты КГБ Клаус Фукс и Ким Филби. Советские сообщения шифровались в два этапа, с применением одноразовых шифров. Это невообразимо затрудняло работу криптоаналитиков, но из-за военных потерь и нехватки ресурсов шифры использовались повторно.

Поскольку практически реализовать абсолютно стойкий шифр трудно, в настоящее время почти все системы шифрования используют относительно короткие ключи. Однако не следует определять надежность только по длине ключа. Сегодня в Интернете можно найти программы, которые взламывают шифр Виженера, и ни один профессиональный шифровальщик не станет его применять. Современные сложные

[1] *www.nsa.gov/publications/publi00039.cfm.*

шифры – отдаленные потомки старых шифров замены. В современных средствах шифрования открытый текст обрабатывается не посимвольно, а блоками. Текст (точнее, битовая последовательность) преобразуется в соответствии с некоторым методом, зависящим от ключа. Сам ключ также является битовой последовательностью, которую Алиса и Боб должны хранить в тайне от Евы. В отличие от шифра Виженера, нет известных (по крайней мере, общественности) методов взлома современных шифров, а наиболее эффективный метод дешифрования сообщения заключается в «лобовой атаке» (brute-force attack) – полном и прямом переборе всех возможных ключей.

Объем вычислений, необходимый для восстановления текста из зашифрованного сообщения путем прямого перебора, экспоненциально возрастает с увеличением длины ключа. Увеличение длины на один бит удваивает объем вычислений на компьютере взломщика, почти не требуя дополнительного времени на шифрование и дешифрование. Именно это делает современные средства шифрования столь полезными: скорость компьютеров может расти – даже экспоненциально, – но объем вычислений для взломщика возрастает так же экспоненциально при использовании ключей все большего размера.

Уроки для эпохи Интернета

Прервем ненадолго повествование, чтобы обсудить некоторые уроки из истории криптографии – принципы, которые были четко формализованы в начале XX века. В конце XX века, когда криптография сильно изменилась благодаря современным компьютерным технологиям и новым алгоритмам шифрования, эти уроки все еще остаются актуальны. А их очень часто прогуливают!

Прорывы случаются, но вести доходят медленно

Марию Стюарт обезглавили, потому что ее переписка с заговорщиками против Елизаветы I была расшифрована при помощи статистического анализа, описанного Аль-Кинди за девять столетий до упомянутых событий. Еще более древние методы оставались в строю до наших дней даже в критических коммуникациях. Светоний описал шифр Цезаря в I веке н. э. Даже два тысячелетия спустя сицилийская мафия использовала эти шифры. Печально известному главарю мафии Бернардо Провенцано удавалось ускользать от итальянской полиции в течение сорока трех лет. Но в 2002 году у одного из соучастников Провенцано нашли несколько *pizzini* – небольших бумажных листков с зашифрованным текстом. Эти листки содержали часть переписки Бернардо с сыном Анжело[1], зашифрованной по методу Цезаря, точно как описано у Светония. Провенцано стал использовать более безопасный шифр,

[1] Росселла Лоренци (Rossella Lorenzi), «Discovery News», 2007 год.

но падение началось. Преступник был обнаружен в жилом доме на ферме и арестован в 2006 году.

Даже ученые не застрахованы от простейших ошибок. Хотя Чарльз Бэббидж и Вильям Казиский взломали шифр Виженера в середине XIX века, научный журнал «Scientific American» полвека спустя описал этот шифр как «невзламываемый» (impossible of translation).[1]

Зашифрованные сообщения обычно кажутся непереводимыми. Небрежный человек, наивный или умудренный опытом, глядя совершенно непонятную смесь букв и цифр, может попасть под ложное впечатление о безопасности. Но криптография – наука, и криптологи знают много способов взломать шифр.

Доверять хорошо, но лучше знать

Нет никаких гарантий того, что даже лучшие современные шифры не могут быть взломаны или уже не являются таковыми. Некоторые шифры имеют под собой серьезную математическую основу, но проверка ее «на прочность» требует серьезного прорыва в математике. Если кто-то и знает, как взломать современные шифры, то этот кто-то наверняка работает в Агентстве национальной безопасности или аналогичном учреждении, а тамошний народ не привык выступать на публике.

В отсутствие строгого доказательства криптостойкости шифра вам остается только полагаться на Главный принцип криптографии: *«Если множество умных людей не смогло решить проблему, значит это неразрешимая (в ближайшее время) проблема».*[2]

Конечно, этот принцип не очень хорош для практики – прорывы в науке по определению не происходят «по заказу» или «в ближайшее время». И когда они случаются, у криптографического сообщества в очередной раз начинают болеть головы. В августе 2004 года на ежегодной конференции по криптографии группа исследователей сообщила о взломе популярного алгоритма MD5, применяемого для компьютерных криптографических операций вроде проверки подписи (message digest), составляющих основу систем безопасности большинства веб-серверов, приложений, требующих ввода пароля, и офисных программных пакетов. Криптологи порекомендовали более безопасный алгоритм SHA-1, но и в нем спустя год обнаружились критические уязвимости.

---

[1] «A new cipher code» (Новый шифр), приложение к «Scientific American», v.58 (27 января 1917 года), с. 61. Из материалов заседаний Клуба инженеров Филадельфии (Библиотека деловой литературы Бейкер, историческое собрание, только по предварительной записи), *www.nku.edu/~christensen/Sciamericansuppl17january1917.pdf*.

[2] Чарли Кауфман, Радиа Перлман, Майк Специнер (Charlie Kaufman, Radia Perlman, Mike Speciner) «Network Security: Private Communication in a Public World» (Сетевая безопасность: частное общение в общественном мире), Prentice-Hall, 1995, с. 40.

Надежный алгоритм шифрования – нечто вроде Святого Грааля компьютерных наук.

Надежный алгоритм шифрования – нечто вроде Святого Грааля компьютерных наук. Каждая обнаруженная уязвимость в принятых шифрах порождает новые идеи по совершенствованию алгоритмов. Мы еще не приблизились к совершенству, но прогресс идет.

Мало иметь надежную систему – нужно ее использовать

Прежде чем выяснять, возможна ли абсолютно безопасная система шифрования, подчеркнем, что даже совершенная математическая модель не обеспечит полную секретность, если ей не следовать.

Блез де Виженер опубликовал свой метод шифрования в 1586 году. Однако военные шифровальщики старались уклониться от применения шифра Виженера, потому что этот метод довольно неудобен в обращении. Шифровальщики пользовались простыми шифрами замены, зная, что они давно взломаны, – надеялись на авось. К началу XVIII века в большинстве европейских стран были организованы так называемые черные кабинеты, через которые проходила вся дипломатическая почта для досмотра и шифрования. Спустя какое-то время дипломаты переключились на шифры Виженера и продолжали шифровать ими документы даже после публикации сведений по технологии взлома.

Сегодня ничего не изменилось. Технологическое решение – неважно, насколько оно хорошо на бумаге, – не будет использоваться, если оно неудобно или дорого. Применение уязвимых систем часто пытаются объяснить попытками избавиться от проблем, связанных с переходом на более безопасные альтернативы.

В 1999 году для защиты домашних и офисных беспроводных соединений был принят стандарт шифрования WEP (Wired Equivalent Privacy). В 2001 году в стандарте WEP были обнаружены серьезные недостатки, позволявшие довольно легко подключаться к беспроводной сети[1], что сразу стало всем известно. Несмотря на это, производители средств беспроводной связи продолжали продавать продукцию, основанную на стандарте WEP, в то время как «знатоки» убеждали покупателей, что «WEP – это лучше, чем ничего». Новый стандарт защищенных беспроводных соединений WPA (Wi-Fi Protected Access) был представлен в 2002 году, но производство новых, сертифицированных для использования со стандартом WPA средств связи началось только в сентябре 2003 года. Хакеры украли более 45 миллионов номеров кредитных карт клиентов сетевого ритейлера TJX, поскольку компания

[1] Никита Борисов, Ян Голдберг, Дэвид Вагнер (Nikita Borisov, Ian Goldberg, and David Wagner) «Intercepting Mobile Communications: The Insecurity of 802.11» (Перехват мобильной связи: уязвимость стандарта 802.11), материалы Седьмой ежегодной международной конференции по мобильным вычислениям и сетям, 16–21 июля 2001 года.

использовала уязвимый стандарт WEP вплоть до 2005 года. Стоимость пренебрежения безопасностью составила сотни миллионов долларов.

Похожим образом дело обстоит со множеством современных устройств типа смарт-карт, основанных на технологии RFID. В январе 2005 года компьютерные исследователи из университета Джона Хопкинса и организации RSA Data Security объявили о взломе автомобильной противоугонной сигнализации, основанной на технологии RFID, и электронной платежной системы, встроенной в миллионы автомобильных RFID-меток. На демонстрации была проведена закупка бензина на станции Exxon/Mobile. Представитель разработчика системы, корпорации Texas Instruments, заметил, что методы исследовательской группы «недоступны большинству исследователей» и заявил: «Не вижу никаких причин изменять наш подход».[1]

Когда шифрование было уделом только военных, начальник, определив факт взлома противником системы безопасности, мог приказать подчиненным использовать новый шифр. Опасность применения слабого шифрования в наши дни основана на трех факторах: высокой скорости распространения новостей об обнаруженных уязвимостях среди экспертов, низкой скорости реакции обывателей и широте распространения криптографического программного обеспечения. Когда университетский исследователь находит в алгоритме небольшую проблему, компьютеры по всему свету становятся уязвимыми, и нет никакого центрального командного пункта, который мог бы издать приказ о всеобщем обновлении программного обеспечения.

Противник знает вашу систему

Последний урок истории криптографии может показаться не столь очевидным. Он состоит в том, что метод шифрования, в особенности разработанный для широкого применения, следует считать более надежным, если он распространен и не был взломан, чем если метод хранится в секрете.

Фламандский лингвист Аугуст Керкхоффс привел этот принцип в своем эссе по военной криптографии в 1883 году.[2] Как он объяснил:

> Система не должна быть секретной и ее попадание в руки противника не должно вызывать беспокойства… Под системой я подразумеваю не

---

[1] «RFID crack raises spector [sic] of weak encryption: Steal a car – and the gas needed to get away» (Взлом RFID вскрывает спектр слабых шифрованных защит: кража автомобиля и топлива, чтобы уехать), *Computerworld* от 17 марта 2005 года, *www.computerworld.com/mobiletopics/mobile/technology/story/0,10801,100459,00.html*.

[2] Аугуст Керкхоффс (Auguste Kerckhoffs) «La cryptographie militaire» (Военная криптография), *Journal des sciences militaires*, т. IX, с. 5–38, январь 1883, с. 161–191, февраль 1883, *www.petitcolas.net/fabien/kerckhoffs/crypto_militaire_1.pdf*.

> ключ, но материальную часть системы: таблицы, словари или необходимые механизмы. Не следует волноваться попусту или подозревать в неблагонадежности работников или подчиненных, зная, что если система, требующая секретности, окажется в руках множества людей, то ее надежность не будет зависеть от степени причастности каждого из них.

Другими словами, если метод шифрования широко распространен, то нереально ожидать, что он надолго останется в секрете. Метод должен разрабатываться так, чтобы оставаться безопасным, даже если все его составляющие (кроме одной – ключа) станут известны.

Клод Шеннон повторил принцип Керкхоффса в своей статье по теории связи в секретных системах: «Предположим, что *противнику известна используемая система*». Клод Шеннон писал:

> Наше ограничение обычно в криптологических исследованиях. Оно является пессимистичным, но безопасно и в конечном счете реалистично, так как можно ожидать, что противник рано или поздно раскроет любую секретную систему.[1]

В современной практике безопасности Интернета принципом Керкхоффса часто пренебрегают. Новые компании нередко делают громкие заявления о создании совершенно нового закрытого метода шифрования, объясняя свой отказ выставить метод на суд общественности необходимостью хранения секрета ради безопасности. Криптологи обычно воспринимают такую «секретность на основе туманности» с большой долей скепсиса.

Даже серьезные организации иногда упускают из вида принцип Керкхоффса. Система защиты цифрового медиасодержания CSS (Content Scrambling System), используемая при записи на диски DVD (Digital Versatile Disc, цифровой многоцелевой диск), была разработана консорциумом киностудий и производителей электроники в 1996 году. Система CSS шифрует содержимое диска, чтобы ограничить неправомерное копирование. Метод шифрования хранился в секрете, чтобы предотвратить производство нелицензионных DVD-проигрывателей.[2] Алгоритм работы системы CSS, который никогда серьезно не исследовался профессиональными криптологами, оказался слабым и был взломан спустя три года после анонсирования. В настоящее время в Интернете можно без труда найти как программы для обхода защиты

---

[1] Статья «Теория связи в секретных системах» из сборника К. Шеннона «Работы по теории информатики и кибернетике». М., ИЛ, 1963.

[2] Джеффри А. Блум, Ингемар Дж. Кокс, Тон Калкер, Жан-Поль М. Ж. Линнарц, Мэтью Л. Миллер, С. Брендан Тро (Jeffrey A. Bloom, Ingemar J. Cox, Ton Kalker, Jean-Paul M.G. Linnartz, Matthew L. Miller, and C. Brendan Traw) «Copy Protection for DVD Video» (Защита от копирования DVD-видео), материалы IEEE, том 87, № 7, июль 1999 года, с. 1267–1276.

CSS, так и множество фильмов с дисков DVD со снятой защитой (более детально защита от копирования обсуждается в главе 6).

Принцип Керкхоффса закрепился в форме стандартов шифрования. Стандарт DES (Data Encryption Standard) был принят в качестве национального стандарта США в 1970-х и широко применялся в коммерческих и финансовых сферах. Стандарт успешно выдержал все попытки взлома, хотя закон Мура сделал процесс перебора всех ключей DES в настоящее время практически осуществимым. Новый стандарт шифрования AES (Advanced Encryption Standard) был принят в 2002 году после тщательной и открытой для общественности проверки.[1] Стандарты DES и AES широко используются и определенно обеспечивают достаточный уровень безопасности. Их алгоритмы шифрования были проверены как профессионалами, так и любителями, и не было замечено никаких серьезных уязвимостей.

Эти уроки так же актуальны сегодня, как и всегда. Но в наше время произошли фундаментальные изменения в криптографии. В конце XX века криптографические методы перестали быть исключительно государственными секретами, став потребительским товаром.

Открытие, навсегда изменившее криптологию

В течение четырех тысяч лет криптография была нацелена на то, чтобы Ева не могла прочитать *перехваченные* сообщения Алисы Бобу. Усилия по шифрованию оказывались тщетными, если ключ попадал в руки противника. Хранение ключа в тайне было делом чрезвычайно важным и довольно рискованным.

Если Алиса и Боб совместно выработали ключ при личной встрече, то как мог Боб сохранить ключ в тайне во время опасного путешествия? Безопасность ключа всегда была исключительно важным приоритетом военной и дипломатической службы. Пилотам и солдатам при угрозе гибели или плена предписывалось в первую очередь уничтожить блокнот с ключом. Раскрытие ключа могло стоить жизни тысячам людей. Безопасность ключа была всем.

Если Алиса и Боб никогда не встречались, то как они могли выработать общий ключ, *не имея* безопасных средств его передачи? Это было фундаментальным ограничением: безопасная связь была практически осуществима только для сторон, которые могли заранее встретиться или использовать общий безопасный метод обмена ключами (например, такой, как диппочта).

Если бы Интернет остановился на этом ограничении, то электронная коммерция никогда бы не получила такого распространения, как сей-

[1] Федеральное издание стандартов № 197, Advanced Encryption Standard, *csrc.nist.gov/publications/fips/fips197/fips-197.pdf*.

час. Пакеты битов, пересылаемые в вычислительных сетях, совершенно не защищены от перехвата.

Но в 1970-х ситуация изменилась. Уитфилд Диффи, 32-летний либеральный математик-теоретик, увлекся криптологией еще будучи студентом Массачусетского технологического института. 31-летний Мартин Хеллман был целеустремленным аспирантом Высшей научной школы Бронкса и профессором в Стэнфорде. Уитфилд Диффи путешествовал по стране в поисках единомышленников по математическим основам криптологии. Найти таких людей было нелегко, поскольку большинство серьезных криптологических исследований велось за закрытыми дверями Агентства национальной безопасности. Ральф Меркль, 24-летний аспирант в области информатики, разрабатывал новый подход к безопасности связи. Сделав одно из важнейших открытий в истории криптографии, Диффи и Хеллман нашли способ практической реализации идей Меркля, представив результат в статье «New Directions in Cryptography» («Новые направления в криптографии»).[1] Описание статьи гласило:

> Способ выработки сторонами секретного ключа, известного только им, путем обмена несекретными сообщениями.

Другими словами, пока Алиса и Боб могут связаться друг с другом, они могут выработать секретный ключ. Не имеет значения, может ли Ева или кто другой прослушивать канал связи. Алиса и Боб используют секретные ключи для шифрования, а Ева не может извлечь из перехваченной информации ничего, что помогло бы установить ключ. При этом Алисе и Бобу совершенно не обязательно встречаться или о чем-то уславливаться заранее.

Важность этого открытия невозможно переоценить. Секретная связь была монополией правительств со времени изобретения письменности – правительство, заинтересованное в сохранении своих секретов, всегда забирает лучших шифровальщиков. Есть и еще одна причина правительственной монополии: только у него достаточно средств, чтобы обеспечить выработку, защиту и передачу ключей. Если бы обычные люди заполучили средства выработки секретных ключей, кто угодно мог бы использовать шифрование. Нужно только знать, как создать ключи; для передачи и защиты ключей не нужны ни дипкурьеры, ни армии.

Диффи, Хеллман и Меркль назвали свое открытие «шифрованием с открытым ключом». Хотя вначале оно не было оценено по достоинству, открытие сделало возможной электронную коммерцию. Представьте себя на месте Алисы, а магазин Amazon – на месте Боба. Как вы могли бы встретиться, чтобы выработать общий ключ? И *есть ли вообще* физическое расположение у магазина Amazon? Если Алиса отправляет

[1] Уитфилд Диффи и Мартин Хеллман (Whitfield Diffie and Martin Hellman) «New directions in cryptography» (Новые направления в криптографии), *IEEE Transactions on Information Theory*, ноябрь 1976.

свой номер кредитной карты по защищенному соединению, шифрование выполняется на логическом узле, точнее, на двух узлах Интернета. Методы Диффи, Хеллмана и Меркля и сопутствующие технологии обеспечили возможность безопасных интернет-транзакций. Покупая товар в интернет-магазине, вы, возможно, сами того не зная, занимаетесь шифрованием. В ролях Алисы и Боба выступают ваш компьютер и сервер магазина.

В 1997 году стало известно, что аналогичные технологии шифрования с открытым ключом были разработаны за два года до открытия Диффи и Хеллмана сотрудниками британского Главного управления правительственной связи (Government Communication Headquarters, GCHQ) Джеймсом Эллисом, Клиффордом Коксом и Малькольмом Уильямсоном.[1]

Кажется совершенно невероятным, что стороны могут выработать секретный ключ посредством открытого канала связи. Могли ли Диффи, Хеллман и Меркль преуспеть в том, что научное сообщество пыталось создать, но потерпело неудачу? А вот и нет, никто и не пытался создать ничего подобного, поскольку казалось очевидным, что Алиса и Боб должны были каким-то тайным образом обменяться ключами.

Даже великий Клод Шеннон упустил из виду это решение. В своей статье, объединившей и поставившей на строго научную основу все известные криптографические методы, Шеннон не предполагал альтернативных возможностей безопасной коммуникации: «Ключ передается некоторым способом на приемный конец, причем предполагается, что его нельзя перехватить».

Стороны могут выработать секретный ключ, даже если все их сообщения перехватываются.

Это не обязательно. Стороны могут выработать секретный ключ, даже если все их сообщения перехватываются.

Базовая схема передачи Алисой ключа Бобу остается такой, как показано на рис. 5.6. Алиса отправляет Бобу зашифрованное сообщение. Боб дешифрует текст с помощью секретного ключа. Шпионка Ева *перехватывает* зашифрованное сообщение и пытается восстановить исходный текст.

Преимуществом подобной системы шифрования является *невозможность* для Евы восстановить текст иначе, чем прямым перебором всех возможных ключей. Здесь на помощь Алисе и Бобу приходит эффект экспоненциального роста. Предположим, к примеру, что стороны ис-

[1] Джеймс Эллис (James Ellis) «The History of Non-secret Encryption» (История несекретного шифрования), *www.cesg.gov.uk/site/publications/media/ellis.pdf*.

пользуют в качестве ключа набор из 10 десятичных цифр. Если компьютеры Евы обладают достаточным быстродействием для перебора всех возможных ключей, стороны могут начать использовать ключ из 20 цифр. В таком случае время, требуемое для перебора, возрастает в 10^{10} раз. Если компьютеры Евы могут перебрать ключи первого типа за 1 секунду, то для перебора ключей второго типа теми же средствами потребуется более 300 лет!

Перебор всех возможных значений всегда остается *единственным средством* нахождения ключа для Евы. Но если Алиса закодирует сообщение шифром замены или шифром Виженера, то шифртекст будет содержать статистические закономерности, которые существенно облегчат задачу Евы. Способ защиты состоит в том, чтобы обеспечить полное отсутствие статистических закономерностей в шифртексте.

Протокол соглашения о ключе

Решающее значение имеет концепция *односторонних вычислений* (*односторонней функции*) – вычислений, обладающих двумя важными свойствами: а) прямое вычисление выполняется быстро; б) обратное вычисление выполняется медленно (если вообще выполняется). Более точно, односторонняя функция принимает в качестве аргументов числа x и y и вычисляет третье число, которое обозначим $x \times y$. Если третье число известно, то даже при знании значения x очень трудно найти значение y. Единственный способ найти значение y – метод проб и ошибок. С увеличением количества разрядов числа y время перебора возможных значений возрастает экспоненциально, становясь практически бесконечным для чисел из нескольких сотен разрядов. Еще одно важное свойство односторонней функции Диффи-Хеллмана: результат выражения $(x \times y) \times z$ равен результату выражения $(x \times z) \times y$.

Протокол соглашения о ключе начинается с публичного объявления о способе вычисления $x * y$ и величине некоторого большого числа g[1]. Вся эта информация общедоступна. Зная ее, стороны могут создать защищенный канал связи по следующим шагам.

1. Каждая сторона выбирает случайное число. Обозначим число Алисы буквой a, число Боба – b. Это будут *закрытые ключи* сторон, известные только им.
2. Алиса вычисляет $g \times a$, а Боб – $g \times b$ (это не требует значительных вычислений). Результаты вычислений называются *открытыми ключами* (обозначим их A и B).
3. Алиса отправляет Бобу число A, Боб отправляет Алисе число B. Не имеет значения, сможет ли Ева получить копии открытых ключей.

[1] Частная односторонняя функция Диффи–Хеллмана – это остаток от деления xy на p, где p – стандартное фиксированное число.

4. После получения открытого ключа B Алиса вычисляет значение $B \times a$; аналогично, Боб вычисляет значение $A \times b$.

Хотя стороны выполняют вычисления с разными величинами, но получают одинаковые результаты. Боб вычисляет значение $A \times b$, то есть, $(g \times a) \times b$ (см. шаг 2). Алиса вычисляет $B \times a$, то есть, $(g \times b) \times a$. В соответствии с третьим свойством односторонней функции, $(g \times a) \times b = (g \times b) \times a$.

Уверены ли мы, что шифр с открытым ключом нельзя взломать?

Несмотря на объединенные усилия лучших математиков и программистов, направленные на достижение абсолютной надежности шифрования, никто еще не доказал математически, что шифр с открытым ключом нельзя взломать. Доверие шифрам покоится на главном принципе «этого еще никто не сделал». Если кто и знает метод быстрого дешифрования, то это, возможно, Агентство национальной безопасности, которое проводит свои исследования в режиме строгой секретности. Если Агентство и знает, то молчит. Возможно, некий изобретатель-одиночка нашел способ взлома, но предпочел славе деньги и тихо наживается, дешифруя финансовые транзакции. А мы остаемся в уверенности, что никто не может и не сможет взломать шифр с открытым ключом.

Это общее число (обозначим его K) является ключом, который стороны используют для обмена зашифрованными сообщениями на основе выбранной функции.

Здесь есть критическая точка. Предположим, что Ева прослушивает канал связи. Что может извлечь Ева из полученных данных? У нее есть A и B, она знает значение g из спецификации стандарта. Ева знает все алгоритмы и протоколы; наконец, она тоже читала статью Диффи и Хеллмана. Но, чтобы вычислить ключ K, Ева должна знать один из секретных ключей – a или b. Но только Алиса знает значение ключа a, и только Боб знает значение ключа b. При использовании чисел из нескольких сотен разрядов невозможно вычислить a или b, зная g, A и B, без перебора практически бесконечного количества возможных вариантов значений.

Выполнять генерацию ключей стороны могут на персональных компьютерах или с помощью специальной аппаратуры. Но даже самые мощные компьютеры не обладают достаточным быстродействием, чтобы третья сторона могла взломать шифр известными методами.