Александр Альбов

Квантовая криптография

ПРОСТО

УДК 001, 501, 510
ББК 22.1
А 56

А 56 Александр Альбов. Квантовая криптография — СПб.: ООО «Страта», 2015. — 248 с.

ISBN 978-5-906150-35-6

Криптография существует уже несколько тысяч лет. Мастерство шифрования и дешифровки было востребованным издревле и в разных целях, будь то тайная любовная переписка монарших особ или радиограммы военных разведчиков из вражеского тыла. Книга рассказывает об истории этой шпионской науки, парадоксах и витках в ее развитии, приведших к новым революционным открытиям; об ученых, внесших мировой вклад в криптографическое дело.

Сегодня, когда информация приобретает едва ли не главную коммерческую ценность и политическое значение, искусство криптографии становится мощным средством в борьбе за влияние и превосходство. Грядет новый и решающий этап в эволюции вычислительных систем: эпоха квантовых компьютеров. Уже очень скоро информация, хранимая в наших базах данных, устремится в совсем другую реальность, странный и таинственный мир, открытый для нас Максом Планком век назад. Мир, в котором правят иные законы физики и живут иные частицы, делая его столь привлекательным для сокровенных человеческих тайн. Итак, мы снова ждем ответа на вопрос: грядет ли окончательная победа шифрования над дешифровкой в свете ожидаемого появления квантовых компьютеров?

ISBN 978-5-906150-35-6

ГЛАВА 1. ОСНОВНЫЕ ЭЛЕМЕНТЫ КОДИРОВАНИЯ

Сколько нужно ключей?

Принцип Керкгоффса

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, причём в такой степени, что стала синонимом «написания с использованием кода» или «закодированного письма». Однако если мы возьмём более строгое научное определение, то для второго метода правильным термином будет «шифровать» (или «расшифровывать», в случае обратного процесса) послание.

Давайте представим, что мы отправляем защищённое послание «АТАКОВАТЬ». Мы можем сделать это двумя основными путями: заменить слово целиком (кодирование), 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 другой части алфавита). 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 всё, 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 вперёд в алфавите русского языка, то он сможет с лёгкостью повторить процесс, двигаясь в обратном направлении, и успешно расшифровать послание.

Перевод текстов, написанных на вышедших из употребления языках, как, например, египетское иероглифическое или критское линейное письмо, был невозможен, пока не нашли способа приведения их в соответствие с каким-то известным языком. В обоих случаях это был древнегреческий.

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, находящейся далее в алфавите через определённое 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 жёсткие 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, приведённом выше, ключ — 2. Каждая буква исходного слова заменяется другой, которая расположена через две позиции в алфавите русского языка).

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 переведённый 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 условие: отправитель и получатель должны, по крайней мере, говорить на одном языке.

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 ключ. В случае трёх пользователей (A, B и C), необходимы три ключа: один для общения A и B, ещё один для пары A и C, а третий — для пары B и C. Точно так же четырём пользователям потребуется шесть ключей. Таким образом, если обобщить, то для n пользователей пользователей потребуется столько ключей, сколько существует комбинаций пар из n, то есть:

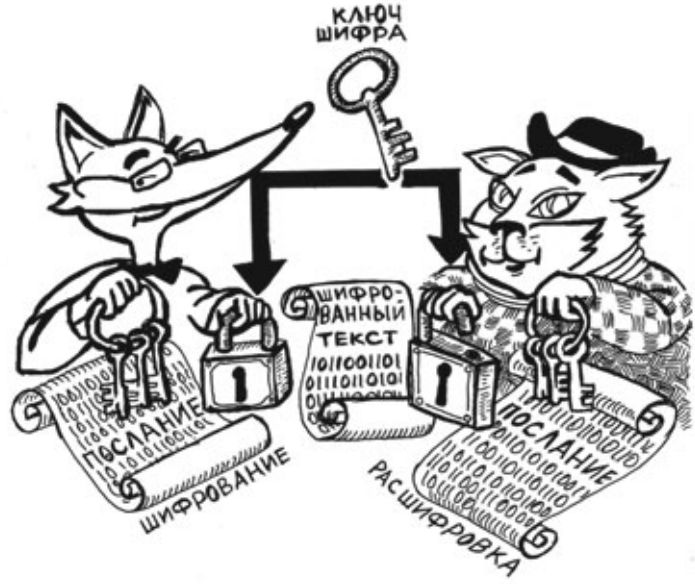
$$\binom{n}{2} = \frac{n(n-1)}{2}$$

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 пойдёт кругом:

17 999 999 997 000 000 000 .

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. Такой принцип был установлен в конце XIX столетия голландским лингвистом Огюстом Керкгоффсом фон Ниевенхофом и поэтому известен как принцип Керкгоффса.

Чтобы подвести итог сказанному, можно показать общую схему шифрования, определяемую следующими элементами: в схему входят отправитель и получатель послания, алгоритм шифрования и определённый ключ, который позволяет отправителю шифровать послание, а получателю расшифровывать его.



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, таким образом, используемая криптографическая система была уязвимой с обеих сторон. Этот тип криптографии, который зависит от ключа, имеющегося как у отправителя, так и у получателя, называется «шифрование закрытым ключом».

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

Как мы видели выше, 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.

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

ДОКТОР ОГЮСТ КЕРКГОФФС

Нидерландский лингвист, криптограф, профессор Парижской высшей школы коммерции во второй половине XIX века. Родился в 1835 году 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.

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 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.

ГЛАВА 2. КРИПТОГРАФИЯ ОТ АНТИЧНЫХ ВРЕМЁН ДО XIX СТОЛЕТИЯ

Скрытые послания

Транспозиционная криптография

Шифр Цезаря

Шифр Полибия

Частотный анализ

Шифр Марии Стюарт

Вклад Альберти

Квадрат Виженера

«Чёрные Кабинеты»

Неизвестный криптоаналитик

Шифр Гронсфельда

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 прочтении должен восприниматься как текст, а если возможность прочтения 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»).

СКРЫТЫЕ ПОСЛАНИЯ

Древнегреческий учёный Геродот упоминает в своей знаменитой «Истории», посвящённой описанию греко-персидских войн в V веке до н. э., два любопытных случая применения стеганографии, которые свидетельствуют о большой находчивости людей того времени.

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.

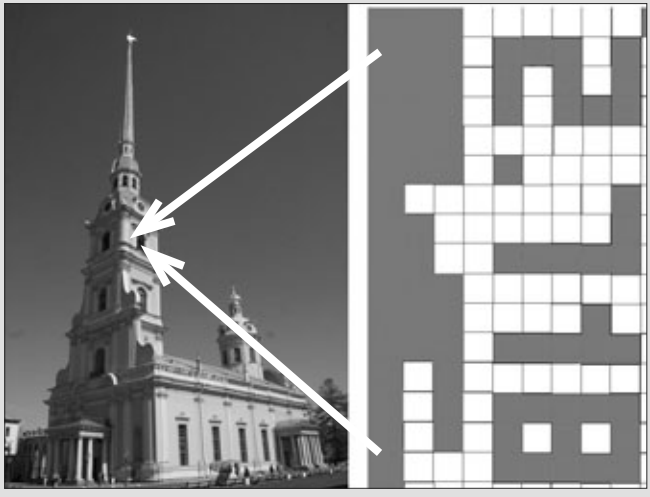
Второй пример, если это, конечно, происходило в действительности, имеет гораздо большую историческую важность, поскольку позволил Демарату, царю Спарты, находящемуся в ссылке в Персии, предупредить своих соотечественников о грядущем вторжении персидского царя Ксеркса. Эту историю Геродот рассказывает 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 чём 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».*

Распространённое стеганографическое средство, которое выдержало испытание временем, — это симпатические

СТЕГАНОГРАФИЯ НАШИХ ДНЕЙ

Хотя это и может показаться парадоксальным, но развитие новых технологий привело к возрождению стеганографии. К примеру, секретное послание можно запрятать в традиционный аудиофайл, причём слушатель не заметит никакой разницы в звучании. Файлы с изображениями также могут быть использованы для передачи скрытой информации. Пример цифровой стеганографии: число «е», основание натурального логарифма, до трёх знаков после запятой скрыто в крошечном фрагменте более крупного изображения. Слева — кажущаяся обычной фотография, справа — пикселы, вычлененные из одного маленького участка, в котором скрывается число 2,718.



(невидимые) чернила. Их применение описано в тысячах рассказов и фильмов. Используемые материалы — лимонный сок, сок растений и даже человеческая моча — обычно органического происхождения и с высоким содержанием 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 идёт о больших количествах посланий.

Во время холодной войны в полных драматизма шпионских триллерах герои часто отправляли послания при помощи средства, на котором буквы оказывались слишком мелкими для чтения невооружённым 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 снимок 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.

ТРАНСПОЗИЦИОННАЯ КРИПТОГРАФИЯ

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

Скитала позволяет полностью менять порядок букв в послании.

Чтобы получить представление об этом методе, который называется транспозицией, рассмотрим простой пример с перестановкой всего трёх букв: A, O и P. Не требуется никаких расчётов, чтобы выяснить, что эти буквы могут быть расставлены шестью возможными способами: AOP, APO; OAP, OPA; POA, PAO.

А = СООБЩЕНИЕ С ПОМОЩЬЮ СКИТАЛЫ
Б = СИМКЕООИО ЩТБСЬАЩ ЮЛЕП ЫНОС

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

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

10 x 9 x 8 x 7 x 6 x 5 x 4 x 3 x 2 x 1.

Такая операция называется факториал, выражается математическим обозначением **10!** И даёт 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 даёт наиболее высокий уровень безопасности, но что будет представлять собой ключ, который позволит расшифровать послание?!

Случайность процесса — это и его сила, и слабость.

Требовался способ шифрования, который дал бы ключи, являющиеся одновременно простыми, лёгкими для

РУКОВОДСТВО ДЛЯ ЮНЫХ ЛЕДИ

«Камасутра» — это легендарная книга, в которой, среди 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 четырёх различных умений, включая музыку, приготовление пищи и игру в шахматы. Для нас особый интерес представляет пункт сорок пять, потому что он посвящён 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 для латиницы 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 при расшифровке.

запоминания и передачи, но в то же время не требующие жертв, связанных с безопасностью. В результате начался поиск идеального алгоритма, и первых успехов в этом достигли римские императоры.

ШИФР ЦЕЗАРЯ

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 символом любого типа. В отличие от транспозиции, при замене необязательно пользоваться только буквами, из которых состоит послание. При транспозиции буква меняет позицию, но сохраняет свою роль. Та же самая буква имеет то же самое значение в исходном и в зашифрованном послании. При замене буква остаётся 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).

В первом веке до н. э. появился 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 неё: A заменялась на D, B на E, и т. д. W заменялась на Z, и, в конечном счёте, X, Y и Z заменяются на A, B и C.

КИНО И КОДИРОВАНИЕ

В классическом научно-фантастическом фильме «2001: Космическая Одиссея» (1968) Стэнли Кубрика на основе романа Артура Кларка наделённый 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. А может, это просто совпадение?

Кодирование и декодирование послания, зашифрованного таким методом, можно провести с использованием простой таблицы:

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

Здесь на примере латиницы мы видим изначальный алфавит (верхний ряд) и трансформированный (нижний ряд), который получился с использованием шифра Цезаря и заменой буквы на другую букву, расположенную через три позиции от неё дальше по алфавиту.

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 D. Классическое выражение AVE CAESAR (Здравствуй, Цезарь) будет зашифровано как DYH

ЕВКЛИД

Евклид (325—265 гг. до н. э.) — древнегреческий математик, автор первого из дошедших до нас трактатов по математике, считается отцом аналитической криптографии.

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 учёные давно знали и восхищались работами Евклида, но первое издание его работ в Европе появилось в Венеции только в 1482 году. Думается, нельзя считать совпадением то, что и арабы, и венецианцы были великими мастерами криптографии.

FDHVDU. И наоборот, зашифрованное послание WUHH после расшифровки даёт TREE (дерево).

В случае использования 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.

ШИФР ПОЛИБИЯ

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. Этот шифр — один из старейших среди тех, о которых мы имеем подробную информацию. Он основан на выборе пяти букв алфавита, чтобы те служили в виде «шапки» для столбцов и стояли первыми в строках таблицы пять на пять, затем ячейки таблицы заполняются буквами алфавита. Шифр сконструирован так, что каждая буква соответствует паре букв, в зависимости от строки и столбца таблицы, по которым они и определяются. Изначально использовался греческий алфавит, который включает 24 буквы, поэтому I и J из английского алфавита, состоящего из 26 букв, обычно объединяются в одной ячейке. Таблица заполняется в порядке, о котором договариваются отправитель и получатель. Обратите внимание, что в шифровальном алфавите должно быть 25 букв (5 × 5). Шифровальный алфавит также может быть размещён в таблице, где «шапкой» служат цифровые значения (например, цифры 1, 2, 3, 4, и 5). В таком случае получится следующая таблица:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I-J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Давайте рассмотрим пример двух версий использования шифра Полибия. Исходное послание — BLANKS. Из таблицы получаем:

B будет заменяться парой цифр 12
L будет заменяться парой 31
A будет заменяться парой 11
N будет заменяться парой 33
K будет заменяться парой 25
S будет заменяться парой 43

ШИФРОВАНИЕ СЛОВА БОЖЬЕГО

Средневековые криптоаналитики считали, что шифры присутствуют в Ветхом Завете, и они не ошибались. Существуют несколько фрагментов священных текстов, которые зашифрованы с помощью шифра замены, который называется Атбаш. Этот шифр состоит из замены любой буквы (n) на букву, которая находится на том же расстоянии от конца алфавита, на каком n находится от его начала. Например, в алфавите английского языка A меняется на Z, B на Y и т. д. В случае оригинала Ветхого Завета

Страница из еврейской библии (ранее XVIII века)

замены производятся буквами алфавита древнееврейского языка. Таким образом в Книге пророка Иеремии (25, 26) Babel (Вавилон) в зашифрованном виде пишется как Sheshakh.

Получается зашифрованное послание **123111332543.**

Эта система создания кодов может быть оформлена таким образом, чтобы ошибка отправителя и получателя оказалась маловероятной и код можно было легко обновлять. В нашем примере будет достаточно менять код каждый месяц: с JANUARY CIPHER (январский шифр) на FEBRUARY CIPHER (февральский шифр), потом MARCH CIPHER (мартовский шифр) и так далее — без необходимости для участников согласовывать друг с другом эти изменения после того, как код был изначально определён.

Надёжность и простота алгоритма, используемого для замены ключевого слова, на многие столетия сделали эту систему предпочитаемой системой шифрования.

В то время, по общему мнению, шифровальщики побеждали дешифровщиков.

ЧАСТОТНЫЙ АНАЛИЗ

Священная книга мусульман «Коран» состоит из ста четырнадцати глав (сур), каждая из которых излагает откровения пророка Магомета. Эти откровения были записаны при жизни пророка его сподвижниками и в дальнейшем собраны первым халифом Абу Бакром. Умар и Усман, второй и третий халифы соответственно, завершили его начинание.

Фрагментарная природа изначальных текстов привела к рождению ветви теологии, занимающейся датированием различных откровений. Среди других техник датирования учёные, занимающиеся изучением Корана, вычисляли частоту появления определённых слов, которые считаются появившимися только в течение периода написания. Если в откровении встречалось достаточно таких новых слов, то было разумно сделать вывод, что это относительно позднее откровение.

Эта инициатива оказалась первым специфическим инструментом криптоанализа, или дешифровки, из когда-либо изобретённых. Он называется «частотным анализом».

Первым человеком, который оставил письменное свидетельство об этой революционной технике, стал философ Аль-Кинди. Хотя он был астрономом, врачом, математиком

Рукопись Корана, Египет, возможно, Фатимиды, X век; выполнена восточным куфическим почерком коричневыми чернилами на пергаменте

АЛЬ-КИНДИ

Абу Юсуф Якуб ибн Исхак ибн Саббах аль-Кинди, употребительное сокращение имени — Аль-Кинди (около 801—873) — арабский философ, математик, теоретик музыки, астроном. Родился, по разным данным, в Куфе или в Басре, детство провёл в Басре, работал в Доме мудрости в Багдаде. Являлся фаворитом халифов ал-Мамуна (813—833) и ал-Мутасима (833—842), которые были покровителями представителей раннего калама — мутазилитов. При ал-Мутаваккиле подвергался гонениям. Аль-Кинди является автором большого числа трактатов по метафизике, логике, этике, математике, криптографии, астрологии, медицине, метеорологии, оптике, музыке.

В Западной Европе был известен под латинизированным именем Alkindus.

и лингвистом, больше всего его помнят благодаря занятиям криптоанализом. Если он и не был первым в этом деле, то определённо сыграл огромную роль в истории. До относительно недавнего времени о первопроходческой роли Аль-Кинди было известно очень мало.

В 1987 году экземпляр трактата Аль-Кинди, озаглавленного «О расшифровке криптографических посланий», всплыл в архиве в Стамбуле. В нём содержится очень краткое изложение первопроходческой техники.

> «*Один из способов расшифровки зашифрованного послания, если мы знаем, на каком языке оно написано, — это найти обычный незашифрованный текст, написанный на том же языке, причём достаточно длинный, потом сосчитать, сколько раз в нём появляется каждая буква. Букву, которая*

встречается наиболее часто, мы называем „первой"; букву, частота появления которой следует за первой, мы называем „второй"... и так далее, пока мы не охватим все встречающиеся в тексте буквы. Затем мы рассматриваем текст, расшифровкой которого занимаемся, и классифицируем встречающиеся в нём символы таким же образом. Находим символ, который встречается наиболее часто, и заменяем его „первой" буквой из нашего текста, делаем то же самое со „второй" и так далее, пока не охватим все символы в криптограмме, которую расшифровываем».

Выше в том же тексте Аль-Кинди упоминает, что при использовании способа шифрования, где применяется замена, каждая буква исходного послания «остаётся на своём месте, но меняет свою роль», и именно это постоянство, «сохранение позиции», делает возможным частотный криптоанализ. Гениальность Аль-Кинди изменила равновесие в среде шифровальщиков и дешифровщиков, и чаша весов, по крайней мере, на какое-то время, склонилась в пользу тех, кто подслушивает и подсматривает.

Подробный пример

Если идти от наиболее часто встречающейся к наименее часто встречающейся, то буквы в английских текстах используются следующим образом:

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

Процент появления каждой буквы представлен в следующей частотной таблице:

A 8,17%	H 6,09%	O 7,51%	V 0,98%
B 1,49%	I 6,97%	P 1,93%	W 2,36%
C 2,78%	J 0,15%	Q 0,10%	X 0,15%
D 4,25%	K 0,77%	R 5,99%	Y 1,97%
E 12,70%	L 4,03%	S 6,33%	Z 0,07%
F 2,29%	M 2,41%	T 9,06%	G 2,02%
N 6,75%	U 2,76%		

КРИПТОАНАЛИТИК ШЕРЛОК ХОЛМС И МЕТОД ПОДБОРА

В рассказе «Пляшущие человечки» Конан Дойл заставляет своего героя Шерлока Холмса столкнуться с шифром подстановки (замены) и обратиться к частотному анализу. Напомним, что Холмс «напряг свой мощный аналитический ум» и начал расшифровку с того, что выделил в записках короткое слово из четырёх букв и предположил, что это имя адресата (Илси). Так он получил первые три буквы шифра — И–Л–С. Затем он догадался, что слово побольше — ПРИХОДИ. С помощью полученных восьми букв он прочитал слово в ответном послании — НИКОГДА. Далее дело пошло проще, и, в конце концов, Холмс поймал преступника на его же уловку: послал ему записку, якобы от имени Илси, в которой зашифровал два слова: «ПРИХОДИ НЕМЕДЛЕННО». Арестовать злодея было делом техники.

Если послание зашифровано при помощи алгоритма замены, аналогичного тому, что обсуждался выше, оно может быть расшифровано в соответствии с частотой использования букв в исходном послании. Достаточно посчитать, сколько раз встречается каждая из букв в зашифрованном тексте, и сравнить их с частотной таблицей для языка, на котором писалось послание. Таким образом, если текст написан на английском языке и наиболее часто встречающаяся в зашифрованном тексте буква — это J, то она, вероятнее всего, соответствует букве E. Если второй по частоте появления

ШИФРОВКА ИЗ «ЗОЛОТОГО ЖУКА»

Уильям Легран, герой рассказа «Золотой жук» (1843) Эдгара Аллана По, нашёл место, где зарыт сундук с сокровищами, после расшифровки надписи на клочке пергамента. Легран использовал статистический метод, основанный на частоте появления букв, которые составляют текст на английском языке. Зашифрованное послание было следующим:

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶
60))85;1‡ (;:‡*8†83 (88)5*†;46 (;88*96*
?;8)*‡ (;485);5*†2:*‡ (;4956*2 (5*_4)8¶
8*;4069285);)6†8)4‡‡;1 (‡9;48081;8:8‡
1;48†85;4)485†528806*81 (‡9;48; (88;4 (
‡?34;48)4‡;161;:188;‡?;

Легран начал с предположения, что исходный текст был написан на английском языке. В английском языке чаще всего встречается буква «e». Затем он составил список букв, основываясь на частоте использования, от наиболее часто встречающейся к наименее часто встречающейся: a, o, l, d, h, n, r, s, t, u, y, c, f, g, l, m, w, b, k, p, q, x, z. Герой составил на основании криптограммы таблицу. В первом ряду — знаки зашифрованного послания, во втором ряду — частота их появления.

8	;	4	‡	)	*	5	6	(	†	1	0	9	2	:	3	?	¶	_
33	**26**	**19**	**16**	**16**	**13**	**12**	**11**	**10**	**8**	**8**	**6**	**5**	**5**	**4**	**4**	**3**	**2**	**1**

Поэтому «8» — это, скорее всего, буква «e». Затем герой нашёл три знака, которые могли бы обозначать the, определённый артикль, который также очень часто встречается в английском языке, что позволило Леграну перевести знаки «;», «4» и «8». Он догадался, что означает сочетание «;(88», поскольку знал, что обозначают три знака из четырёх. И, получив сочетание «t(ee», он сделал вывод о том, какую букву обозначает «(». Это может быть только «r», а в результате получилось слово

«tree» (дерево). Наконец, используя далее аналогичную криптоаналитическую технику и проявив немалое терпение, Легран составил следующий частичный шифровальный алфавит:

5	†	8	3	4	6	*	‡	(	;	?
a	d	e	g	h	i	n	o	r	t	u

Этого достаточно для расшифровки послания:
«A good glass in the bishop's hostel in the devil's seat forty-one de-grees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death's-head a bee line from the tree through the shot fifty feet out».

Русский перевод:
«Хорошее стекло в трактире епископа на чёртовом стуле сорок один градус тринадцать минут север-северо-восток главный сук седьмая ветвь восточная сторона стреляй из левого глаза мёртвой головы прямая от дерева через выстрел на пятьдесят футов».

является буква Z, то те же рассуждения приводят нас к выводу, что ей наиболее вероятно соответствует буква T. Процесс повторяется для всех букв зашифрованного текста.

Дешифровка с помощью частотного анализа — это история, полная драматизма, привлёкшая внимание немалого количества писателей. Возможно, самым известным произведением, основанным на крипто-анализе послания, является «Золотой жук» Эдгара По. Другие авторы, такие как Жюль Верн и Артур Конан Дойл, использовали подобные приёмы, чтобы добавить напряжения в сюжетные линии.

Даже свыше тысячи лет после появления идеи у Аль-Кинди она всё ещё очаровывает обычных людей своей находчивостью и оригинальностью.

Очевидно, что частотный метод не всегда может применяться столь непосредственным образом. Частоты в таблице, представленной выше, — это только средние показатели.

К примеру, в коротких текстах типа «Visit the zoo kiosk for quiz tickets» относительная частота появления букв очень сильно отличается от языковых характеристик в целом.

Поэтому для текстов, включающих менее 100 знаков, этот простой анализ используется крайне редко.

Однако частотный анализ не ограничивается изучением букв самих по себе. Хотя мы соглашаемся с тем, что маловероятным является наиболее частое появление буквы E в коротком зашифрованном тексте, мы с большей уверенностью можем считать, что пять наиболее часто встречающихся букв — это, вероятнее всего, A, E, I, O и T (пусть даже не знаем, какая из них которой соответствует). A и I никогда не встречаются в паре в английском языке, в то время, как другие буквы могут. Более того, также вероятно, что каким бы коротким ни был текст, гласные имеют тенденцию появляться перед и после скоплений других букв, в то время как согласные имеют тенденцию группироваться с гласными или с небольшим числом согласных. Таким образом, мы, возможно, сумеем отделить T от A, E, I и O.

По ходу успешной расшифровки писем станут появляться слова, в которых нам нужно расшифровать всего один или два знака, что позволит строить гипотезы о том, что это за буквы. Скорость дешифровки увеличивается по мере дешифровки большего количества писем.

ШИФР МАРИИ СТЮАРТ

8 февраля 1587 года шотландская королева Мария Стюарт была обезглавлена в замке Фотерингей после того, как её признали виновной в государственной измене. Расследование, которое привело к столь жестокому приговору, показало вне всяких сомнений: Мария и в самом деле действовала в сговоре с группой аристократов-католиков, которую возглавлял молодой Энтони Бабингтон. Заговорщики планировали покушение на английскую королеву Елизавету I с целью возвести Марию на трон католического государства, включающего и Англию, и Шотландию.

Решающие доказательства представила служба контрразведки Елизаветы, которую возглавлял лорд Уолсингем. Доказательства включали целый ряд писем, которыми обменивались Мария и Бабингтон. Из них было совершенно ясно,