А. И. Музыкантский, В. В. Фурин

Лекции по криптографии

МЦНМО

УДК 511+519.719.2
ББК 32.81в6
М89

Музыкантский А. И., Фурин В. В.
Лекции по криптографии
Электронное издание
М.: МЦНМО, 2014
68 с.
ISBN 978-5-4439-2075-7

Брошюра издана по материалам лекций по криптографии, прочитанных на факультете мировой политики МГУ им. М. В. Ломоносова. Основное внимание уделяется прикладным задачам, решаемым с помощью математических методов криптографии. Доступно рассказывается о том, что такое шифрование, криптографические протоколы, о роли криптографии в массовых информационных коммуникациях.

Первое издание было опубликовано в 2011 году.

Подготовлено на основе книги: *Музыкантский А. И., Фурин В. В.* Лекции по криптографии. — М.: МЦНМО, 2013. — 2-е изд., стереотип. — 68 с.

Издательство Московского центра
непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11,
тел. (499)241–74–83.
http://www.mccme.ru

ISBN 978-5-4439-2075-7

Оглавление

1. Основные понятия и математическая формализация

1.1. Основные понятия криптографии

В этой лекции мы познакомимся с одной из замечательных наук — криптографией. С незапамятных времен человечество обращалось к ней, когда возникала необходимость сохранить в тайне информацию. Можно постараться скрыть сам факт передачи информации, например, применить тайнопись при обычной переписке или проложить секретный канал между отправителем и получателем информации. Но сделать канал передачи информации полностью скрытым от недоброжелателей оказалось практически невозможно. Использовать только способ сокрытия передачи информации для защиты, например, важной государственной информации было ненадежно или очень дорого. Возникла задача использовать общедоступный канал связи, но при этом передавать нужную информацию в таком шифрованном виде, чтобы прочитать ее мог только адресат.

Для разработки методов преобразования информации (или шифрования) с целью ее защиты от незаконных пользователей и возникла наука ***криптография***.

Криптография на современном этапе — это область научных, прикладных, инженерно-технических исследований, основанная на фундаментальных понятиях математики, физики, теории информации и сложности вычислений. Криптография необходима в основном для сохранения государственной тайны, военной тайны, а также коммерческой, юридической, врачебной и т. д. При этом криптография, исторически возникшая именно как наука о методах шифровки и дешифровки, в дальнейшем, особенно с появлением компьютеров, включила в себя и многие другие задачи, возникающие в процессе организации обмена информацией.

Обеспечение конфиденциальности информации, уверенность в отсутствии изменений в передаваемой информации, установление подлинности источника передаваемых сообщений, невозможность отказа от факта совершения определенных действий — вот пример задач, решаемых современной криптографией.

В дальнейшем мы будем применять понятия, аналогичные военной терминологии. При отправлении сообщения обязательно есть *отправитель* и *адресат*, или *получатель*, кому направлено сообщение. Нежелательный для отправителя получатель сообщения будет именоваться *противником*, который пытается создать *угрозу сообщению*. *Атакой на шифр* будем именовать попытки противника разгадать наш шифр (иногда употребляется также термин *взлом шифра*). Возможность нашего шифра противостоять угрозам будем именовать *стойкостью шифра*.

В дальнейшем мы словом *дешифрирование* будем обозначать попытку взлома шифра незаконным получателем (противником); словом *расшифрование* мы обозначаем восстановление исходного текста из шифротекста его законным получателем.

Очень важно правильно понимать проблему соотношения цены информации, затрат на ее защиту и затрат на ее добывание. Если затраты на шифрование сопоставимы со стоимостью самой информации, то стоит задуматься об изменении способа шифрования. Аналогичны действия противника — если затраты на дешифровку выше стоимости информации, то стоит подумать о другом способе добычи информации. Отправитель сообщения должен понимать, что если материальные и людские затраты противника на дешифровку сообщения будут намного выше цены информации, содержащейся в сообщении, то он вряд ли возьмется за задачи дешифровки конкретных сообщений отправителя.

В мире разрабатываются специальные стандарты, которые позволяют отправителям сообщений, применяющих их в информационном обмене, с большой долей уверенности считать, что в течение определенного срока самые современные технические средства противников не смогут дешифровать информацию или, например, подделать зашифрованную электронную подпись отправителя.

Более подробно с основными понятиями криптографии можно ознакомиться в работе [2].

1.2. Из истории криптографии

1.2.1. От шифра Цезаря до машины «Enigma»

Одним из первых наиболее известных криптографических методов преобразования информации был шифр Сцитала, использующий метод перестановки букв. Брался жезл определенного диаметра, на него наматывалась лента и сообщение записывалось вдоль жезла

в несколько «строк». Далее лента разматывалась, и сообщение получалось зашифрованным. Чтобы прочитать сообщение, необходимо было иметь жезл такого же диаметра. Специальный метод дешифровки таких сообщений разработал Аристотель. Он использовал конус, для чего наматывал и двигал по нему ленту с сообщением. Когда появлялась возможность прочитать сообщение, на конусе делалась засечка, это и позволяло определить диаметр жезла, на котором сообщение было зашифровано.

Также интересным представляется шифр Цезаря, использующий метод замены. Отправитель и адресат договариваются о величине сдвига — определенном числе (у Цезаря обычно 3), после этого записывают алфавит по кругу (*а* после *я*, если алфавит русский, или *a* после *z*, если алфавит латинский) и заменяют букву в открытом тексте на букву, получившуюся в результате сдвига по кругу. Шифр можно было вскрыть в результате кропотливой работы с разными величинами сдвигов. Максимально мы можем использовать лишь 26 (в случае латинского алфавита) нетривиальных ключей.

В рассмотренных выше двух примерах появляется очень важное понятие криптографии — *ключ* (в шифре Сцитала это диаметр жезла, в шифре Цезаря — величина сдвига). Чтобы разгадать шифрованное сообщение, требуется не только получить само сообщение, знать метод шифрования, но и разгадать ключ.

Более сложный вариант шифрования был описан в рассказе «Пляшущие человечки» Артура Конан-Дойля. Для дешифровки Шерлоку Холмсу пришлось применять дополнительные методы (помимо перебора), такие, как частота появления тех или иных букв английского алфавита. Будучи знакомым со многими работами по дешифровке посланий, Эдгар По в рассказе «Золотой жук» писал: «...Едва ли разуму человека дано загадать такую загадку, которую разум его собрата, направленный должным образом, не смог бы разгадать».

Одним из первых, кто создал профессиональную службу по шифровке и дешифровке сообщений, был кардинал Ришелье. В 1628 году в почтамте Парижа был открыт «Черный кабинет». Его возглавил Антуан Россиньоль, который являлся автором шифра, используемого в будущем вплоть до наполеоновских войн. Ему принадлежит авторство доктрины: «Стойкость военного шифра должна обеспечить секретность за время, необходимое для выполнения приказа. Стойкость дипломатического шифра должна обеспечивать секретность в течение десятилетий».

С появлением электромеханических устройств появились новые возможности шифрования. Двадцатые и тридцатые годы XX века ста-

ли периодом расцвета конструирования различных шифровальных машин. В 1917 году Гильберт Вернам предложил очень эффективный способ шифрования сообщений. Шифруемое сообщение переводилось в двоичную кодировку, складывалось со значениями специальной телетайпной ленты-ключа и отправлялось по телеграфу адресату. Расшифровать сообщение, имея ленту-ключ, не представляло труда. В дальнейшем известным американским математиком Клодом Шенноном было доказано, что схема Вернама является абсолютно стойкой системой шифрования, при условии если длина ключа равна длине сообщения, ключ вырабатывается случайно и используется однократно.

Основной проблемой шифровальщиков стала выработка ключей и организация схемы обмена ими между отправителем и получателем сообщений. Так появились электромеханические шифраторы, состоящие из коммутационных дисков и механизма изменения их угловых положений. Наибольшую известность среди них приобрела немецкая шифровальная машина «Enigma», которая использовалась немецким командованием для нужд шифрования своих военных сообщений во время Второй мировой войны. Концепция работы «Enigma» была разработана немецким инженером Артуром Шербиусом, но принципы работы, устройство, да и сам факт существования этой шифровальной машины представляли собой высший государственный секрет Третьего Рейха.

Учитывая, что «Enigma» представляла собой одно из наивысших достижений «докомпьютерного» этапа развития шифровальной техники и что дешифровка ее кодов представляет собой одно из самых значительных достижений разведки союзников, которое оказало большое влияние на весь ход военных операций Второй мировой войны, имеет смысл сказать по этому поводу несколько слов.

1.2.2. Шифровальная машина «Enigma». Принцип действия и битва за шифры

«Enigma» (в русской транскрипции «Энигма») в переводе с древнегреческого означает «безымянный», «неназванный», «загадочный». Работы по применению шифровальной машины с подобным названием начались в Германии в глубокой тайне в 1928 году и активизировались с приходом к власти Гитлера. Работами руководил непосредственно германский Генеральный штаб. К началу Второй мировой войны работы по созданию военного варианта «Enigma» были закончены, машина прошла испытания и была принята на вооружение.

Рис. 1. Внешний вид шифровальной машины «Энигма»

«Enigma» относилась к классу электромеханических шифровальных машин. Ее конструкция была основана на системе из трех вращающихся барабанов, осуществлявших замену 26 букв латинского алфавита. Каждый барабан имел 26 входных контактов на одной стороне и столько же выходных контактов — на другой. Внутри каждого барабана проходили провода, связывавшие входные и выходные контакты между собой. Выходные контакты первого барабана соединялись с входными контактами второго. Когда оператор нажимал на какую-либо букву на клавиатуре машины, электрический ток подавался на входной контакт первого барабана, соответствующий этой букве. Ток проходил через первый барабан и поступал на выходной контакт, соответствующий какой-либо другой букве. Затем ток проходил последовательно через второй и третий барабаны и подавался на неподвижный рефлектор (от лат. reflecto — обращаю назад, отражаю). В конструкции рефлектора 26 контактов разбивались на пары, контакты внутри каждой пары были соединены между собой. Таким образом, рефлектор заменял букву на парную ей.

Ток, прошедший через рефлектор, подавался назад, на систему барабанов. Он вновь проходил через три барабана, но в обратном порядке. В конце концов на световом табло машины загоралась одна из 26 лампочек, соответствовавшая зашифрованной букве.

Самым важным свойством машины «Enigma» являлось вращение барабанов. Первый барабан после каждого преобразования буквы поворачивался на одну позицию. Второй барабан поворачивался на одну позицию после того, как первый совершал полный оборот, т. е. после преобразования 26 букв. Наконец, третий барабан поворачивался на одну позицию после того, как второй совершал полный оборот, т. е. после шифрования 676 букв.

Благодаря рефлектору «Enigma» на каждом шаге осуществляла перестановку букв внутри пар, и если, к примеру, буква N заменялась на S, то при том же положении роторов буква S менялась на N (ток шел по тем же проводам, но в другую сторону). Этим объяснялась особенность машины: для расшифровки сообщения достаточно было вновь пропустить его через машину, восстановив предварительно изначальное положение барабанов. Таким образом, начальное положение барабанов играло роль ключа шифрования. Это начальное положение устанавливалось в соответствии с текущей датой. Каждый оператор имел специальную книгу, задававшую положение барабанов для каждого дня. В целом получилась компактная, быстродействующая шифровальная машина, достаточно устойчивая к попыткам взлома применяемого шифра.

Очевидная слабость данной системы шифрования заключалась в том, что противнику достаточно было завладеть специальной книгой, задающей ключи шифрования, и самой машиной, чтобы дешифровать многие сообщения [5].

Немцам, несмотря на колоссальные усилия, не удалось сохранить в тайне работу над «Энигмой». Уже в 1932 году в специально созданном «Шифровальном бюро» в Варшаве начались работы над раскрытием тайны «Энигмы». Возглавлял группу молодой польский математик Мариан Ршевский, выпускник математического факультета университета в Познани. Группа имела в своем распоряжении устаревшую коммерческую шифровальную машину, купленную в Германии. Конечно, эта модель была очень далека от современных для той поры немецких военных шифровальных машин и принесла мало пользы. Поэтому главным моментом в работе ученых для решения задачи «Энигмы» было применение математики (теории групп и теории перестановок). Для раскрытия шифров «Энигмы» польские математики использовали перехваченные шифрованные сообщения и добились значительных успехов. Ими было теоретически воссоздано устройство машины, что позволило позже создать её реальную модель; были разработаны также методы восстановления ключей к шифрам на основе перехваченных сообщений.

Позднее, в 1939 году, перед началом войны все материалы по «Энигме» были поляками переданы во Францию и Англию. Англичане продолжили работы, раскрыв усовершенствования, которые были внесены в конструкцию последних немецких машин и систему кодов, используемую Германией. В этой работе, выполнявшейся большой группой ученых в местечке Блетчли в 70 км от Лондона, участвовал знаменитый математик Алан Тьюринг, широко известный как автор виртуальной «машины Тьюринга». Благодаря, главным образом, усилиям возглавляемой им группы были созданы механические вычислительные устройства, полным перебором отыскивавшие ключи к шифру на много порядков быстрее, чем это можно было сделать вручную. Подобное механическое устройство, но с возможностью его «программирования» с помощью бумажной перфоленты, созданное специально для дешифровки перехваченных сообщений «Энигмы» и названное «Colossus», некоторые исследователи считают *первым в мире по-настоящему программируемым компьютером*.

Математикам из Блетчли часто удавалось находить блестящие и в то же время простые решения, во много раз сокращавшие время вскрытия шифровок «Энигмы». Но их оригинальные идеи, в частности по организации «распределенных вычислений», приходилось воплощать по преимуществу с помощью карандаша и листа бумаги, что значительно затягивало время дешифровки перехваченных сообщений.

Наконец, осенью 1942 года, в результате спецоперации ВМС Англии, на германской подводной лодке U-571, которую немецкое командование считало затонувшей, была захвачена сама шифровальная машина «Enigma» и процесс дешифровки немецких секретных сообщений был поставлен англичанами на поток.

Вся эта работа по взламыванию немецких секретных шифров сохранялась в глубокой тайне, и немцы до самого конца войны даже не подозревали, что все их секретные сообщения становятся известны антигитлеровской коалиции. О том, какое значение придавало английское командование сохранению в секрете факта взлома немецких секретных шифров, говорит тот факт, что У. Черчилль никак не воспользовался знанием о предстоящем налете немецкой авиации на город Ковентри, сообщения о котором были перехвачены и заблаговременно расшифрованы англичанами. В результате город был подвергнут сильнейшей бомбардировке немецкой авиации, однако англичане сохранили в тайне свои возможности по дешифровке немецких секретных сообщений.