Оглавление

Содержание

Вступительное слово

От тайных дешифровальных колец до правительственных директив, задачи сокрытия и обнаружения информации в составе другой информации давно будоражили человеческий ум. Криптология – завораживающий предмет, с которым на практике сталкивался едва ли не всякий школьник. И вместе с тем имеются веские причины, по которым эта дисциплина на протяжении веков была окутана глубочайшей тайной, поскольку государства использовали ее для защиты своего самого секретного оружия. В военных и дипломатических делах к криптографии всегда относились в высшей степени серьезно. Не будет преувеличением сказать, что успехи и провалы криптографии влияли на исход войн и ход истории, и точно так же они определяют нашу современную историю.

Возьмем сражение при Энтитеме в ходе Гражданской войны в США, произошедшее в сентябре 1862 года близ Шарпсбурга, штат Мэриленд, в котором Федеральная армия под командованием Джорджа Макклеллана противостояла армии Конфедерации под командованием Роберта Ли. За несколько дней до него два солдата федералов нашли недалеко от лагеря листок бумаги, оказавшийся копией приказа Ли, в котором были подробно изложены планы вторжения в Мэриленд. Приказ не был зашифрован. Располагая этой информацией, Макклеллан точно знал местоположение рассеянных отрядов и смог уничтожить армию Ли, не дав им соединиться.

Успехи и провалы криптографии оказывали влияние и на более близкие к нам события. Сокрушительное поражение русской армии при Танненберге в августе 1914 года стало прямым следствием перехвата сообщений немцами. Удивительно, но сообщения русских передавались открытым текстом, потому что у полевых командиров не было ни шифров, ни ключей. Поэтому русские не могли безопасно координировать действия соседних подразделений.

50 лет холодной войны, последовавшей за Второй мировой войной, тоже стали результатом провала криптографии, на этот раз со стороны японцев в битве за Мидуэй в 1942 году. Американские криптоаналитики взломали японские коды и могли читать многие донесения Объединенного флота. Подобные истории – вотчина классической криптографии. Книга «Криптография с секретным ключом» как раз на этом поле и играет.

Никто не сможет лучше д-ра Фрэнка Рубина провести интересующегося читателя по всем закоулкам классической криптологии на любительском уровне, от математических истоков до социальных последствий. Д-р Рубин получил образование в области математики и информатики. Тридцать лет он проработал в компании IBM, в отделе автоматизации проектирования, и свыше 50 лет занимался криптографией. Д-р Рубин был редактором журнала «Cryptologia» и других изданий. Он автор десятков статей по математике и компьютерным алгоритмам, а также тысяч математических головоломок.

«Криптография с секретным ключом» – не просто новая версия классической книги Helen F. Gaines «Elementary Cryptanalysis». Здесь предмет рассматривается с древних времен до эры квантовых компьютеров. И, что немаловажно, описывается уникальный метод измерения стойкости шифра[1],[2].

Книга выходит в стратегически важный момент. Это своевременный и существенный вклад в понимание критической технологии. Неважно, испытывает ли читатель бескорыстный интерес к криптологии как таковой или занимается практической защитой информации, материал, изложенный на этих страницах, благодаря глубине и широте охвата, станет желанным источником полезной информации, а сама книга – ценным пополнением библиотеки.

– Рэндалл К. Николс, DTM

Рэндалл К. Николс – бывший президент Американской ассоциации криптограмм, отвечавший, в частности, за обзоры книг; директор программы сертификации беспилотных летательных систем на предмет кибербезопасности в Канзасском университете в Салине: заслуженный профессор отделения послевузовского образования в области кибербезопасности и компьютерно-технический экспертизы в колледже Ютики.

---

[1] И в книге R. K. Nichols «ICSA Guide to Cryptography», и в классическом труде Брюса Шнейера «Прикладная криптография» приведены методы оценки стойкости шифров и случайности. Первая посвящена в основном классической криптографии, вторая в большей степени современным шифрам (Nichols, 1999; Schneier, 1995).

[2] В «Криптографии с секретным ключом» лучше отобран и лучше изложен материал, чем в двух моих первых книгах по классической криптографии: «Classical Cryptography Course», т. I и II (LANAKI, 1998; 1999).

Предисловие

К идее написать эту книгу меня привели разные дорожки. Начну с моего школьного друга Чарли Роуза. Чарли работал в школьном книжном магазине. В один прекрасный день, заказывая книги для магазина, он обратил внимание на книгу Хелен Ф. Гейнс «Криптоанализ». Чарли захотел приобрести ее, да еще и с отраслевой скидкой. Но вот незадача – магазин должен был заказать как минимум три экземпляра.

Чарли нужно было найти еще двоих желающих купить книгу. Он пообещал, что мы все вместе прочтем ее, а затем будем придумывать криптограммы, которые другие должны будут решать. Я книгу купил, прочел и начал составлять криптограммы, а Чарли утратил интерес.

На обратной стороне обложки «Криптоанализа» был напечатан давно устаревший адрес Американской ассоциации криптограмм (www.cryptogram.org), но я все-таки нашел ее и вступил в ее члены. И начал решать разные типы криптограмм, которые публиковались в бюллетене для любителей «The Cryptogram». А спустя несколько лет стал заместителем редактора. И вот уже более 40 лет остаюсь членом Ассоциации.

В 1977 году был основан более профессиональный журнал по криптографии, «Cryptologia». Его можно найти в интернете по адресу https://www.tandfonline.com/toc/ucry20/current. Сначала я читал статьи, потом начал писать и в конце концов стал редактором. Както так получилось, что ко мне стекались все статьи разных фриков, и приходилось продираться сквозь хитросплетения нелогичной логики – вдруг где-то в глубине притаилась хорошая идея. И один раз такое случилось. Я превратил эту идею в статью для «The Cryptogram». Автор был так благодарен, что посадил в мою честь дерево в Израиле.

Этот опыт научил меня отделять статьи, которые просто плохо написаны или переоценивают стойкость шифра, от трудов совсем уж чокнутых авторов. И вот что я понял: любитель, придумавший слабый шифр, может его описать и разложить по шагам. Мечтатель не сможет излить смутные, но грандиозные плоды своего воображения на бумагу. Он будет изводить целые стопки бумаги, расписывая чудесные свойства своего шифра, но не в силах выписать его шаги. Он не способен превратить свои бессвязные мысли в конкретный алгоритм.

Начиная с 2005 года, я стал посещать курсы в колледже Марист по программе непрерывного образования. Вскоре я читал лекции по судоку, SumSum и другим головоломкам (я написал три книги о судоку), своим путешествиям по Танзании и Монголии, конструкции Эмпайр Стейт Билдинг, жизни Алана Тьюринга и другим темам. Я стал членом комиссии по учебным планам.

В 2018 году я вызвался прочесть двухсеместровый курс по криптографии. Подготовив почти 450 слайдов, я понял, что материала достаточно для книги. И, на мое счастье, обнаружилось, что годом раньше я уже начал писать как раз такую книгу. Вот эту.

Об этой книге

Для кого предназначена эта книга

Книга рассчитана на широкую аудиторию: массового читателя, криптографов-любителей, почитателей истории, студентов компьютерных специальностей, инженеров-электротехников, математиков и профессиональных криптографов. Это усложнило мне работу, потому что невозможно сделать все части книги одинаково интересными для всех. Для кого-то в некоторых частях окажется слишком много математики. А кому-то какие-то части покажутся чересчур элементарными. В этом разделе я попробую подсказать читателям, что, на мой взгляд, им стоит прочитать.

- **Массовые читатели** могут читать всё подряд до конца главы 8. Если математика покажется слишком сложной или изложение перенасыщенным техническими подробностями, просто пропускайте соответствующие страницы. Начиная с главы 9, материал становится более трудным. Дальше можно читать выборочно, только то, что кажется интересным. Быть может, имеет смысл прочитать главу 12, чтобы получить общее представление, не вдаваясь в детали.
- **Криптографы-любители**, вероятно, захотят прочитать книгу целиком, а затем более внимательно изучить разделы 4.2–5.11, 6.1–6.5, 6.7, большую часть главы 7, а также разделы 9.1–9.9 и главы «Развлечения» и «Задачи».
- **Почитатели истории** могут прочитать книгу целиком, пропуская всю математику, но обращая внимание на то, когда и кем были изобретены различные методы.
- **Студентам компьютерных специальностей** рекомендую уделить особое внимание разделам 5.6–5.11, главе 8 и главам 11–16.
- **Инженеров-электротехников** могут заинтересовать практические методы. Им стоит прочитать главы 2 и 4, где излагаются

основы, а затем разделы 7.2–7.8, главу 9 и главы 11–16, обращая особое внимание на главу 12.

- **Математикам** будут особенно интересны раздел 4.5, разделы 5.6–5.12, 10.4–10.7, 11.7–11.10, 12.3–12.6, главы 13–16, в особенности раздел 16.4.6, и глава 18.
- Для **профессиональных криптографов** интерес могут представлять разделы 7.8, 8.2, 10.5, 10.7, 11.4, 12.3–12.6, 13.8, 13.15, 14.2, 14.4, 15.4–15.14, 16.4, 16.5, и 18.12.

О шифрах

Я включил несколько развлекательных головоломок и более серьезных задач для читателей, которые хотят попробовать свои силы во вскрытии шифров. Для решения головоломок достаточно стандартных методов, описанных в книге.

При решении задач применяются методы, которые я придумал сам. Они достаточно просты, так что любитель сможет догадаться о методе и решить задачу. Я старался не вредничать и дать возможность интересующимся читателям найти решение. Не бойтесь – там нет ничего заумного или чрезмерно сложного. Никаких несуществующих слов или искаженных частот букв. И достаточно материала для решения.

Некоторые разделы начинаются символом * и заканчиваются символами **. Это факультативные разделы, которые могут содержать компьютерные алгоритмы или углубленную математику. Кто-то захочет их пропустить.

Форум на сайте liveBook

Приобретение этой книги открывает бесплатный доступ к платформе liveBook онлайнового чтения, созданной издательством Manning. Средства обсуждения на liveBook позволяют присоединять комментарии как к книге в целом, так и к отдельным разделам или абзацам. Совсем несложно добавить примечания для себя, задать или ответить на технический вопрос и получить помощь от автора и других пользователей. Для доступа к форуму перейдите по адресу https://livebook.manning.com/book/secret-key-cryptography/discussion. Узнать о форумах Manning и правилах поведения на них можно по адресу https://livebook.manning.com/discussion.

Издательство Manning обязуется предоставлять площадку для содержательного диалога между читателями, а также между читателями и автором. Но это обязательство не подразумевает какого-то конкретного объема присутствия со стороны автора, участие которого в работе форума остается добровольным (и не оплачивается). Мы рекомендуем задавать автору трудные вопросы, чтобы его интерес не угасал! Форум и архивы прошлых обсуждений остаются доступны на сайте издательства, до тех пор книга продолжает допечатываться.

Другие онлайновые ресурсы

Криптографические продукты, созданные автором, можно найти на его сайте по адресу www.mastersoftware.biz.

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге, – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте www.dmkpress.com, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу dmkpress@gmail.com; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу http://dmkpress.com/authors/publish_book/ или напишите в издательство по адресу dmkpress@gmail.com.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг, мы будем очень благодарны, если вы сообщите о ней главному редактору по адресу dmkpress@gmail.com. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Manning Publications очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты dmkpress@gmail.com.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

Об авторе

Фрэнк Рубин – обладатель степени бакалавра и магистра математики и доктора информатики. Он 28 лет проработал в подразделении автоматизации проектирования компании IBM, где разрабатывал специализированное программное обеспечение, которым инженеры IBM пользовались при проектировании компьютеров и электрических схем. Он владелец компании Master Software Corp., разрабатывающей криптографические продукты. Фрэнк – автор четырех патентов США по криптографическим методам. Он автор примерно 50 работ, опубликованных в реферируемых журналах по криптографии, а также нескольких внутренних документов IBM (руководств пользователя и проектных спецификаций). В области криптографии он известен, прежде всего, тем, что вскрыл цилиндрический шифратор Джефферсона. В информатике хорошо известен его метод арифметического кодирования, ставший одним из стандартных методов сжатия текстов, а также его алгоритм нахождения гамильтоновых путей. В чистой математике известна его идея применить распознаватель с конечным числом состояний к теории меры. Фрэнк опубликовал три книги по судоку, а также две «самиздатовских» книги по головоломкам SumSum. Он автор более 3500 задач, опубликованных в журналах «The Cryptogram», «Technology Review» и «Journal of Recreational Mathematics» (JRM), и единственный, удостоившийся специального выпуска JRM, посвященного исключительно его задачам.

1 Введение

Я занимаюсь криптографией больше 50 лет. За это время я очень многому научился. И в этой книге я хочу передать свои знания следующему поколению криптографов. Многие изложенные здесь сведения – новые открытия, которых вы не найдете ни в какой другой литературе.

Я знаю, что на тему криптографии уже написано много книг. И если я хочу, чтобы мою книгу читали, то должен предложить какие-то мысли, которых нет в других книгах, идеи, о которых другие авторы не знают или считают их невозможными. Книга должна стать **СЕНСАЦИЕЙ**. Поехали! Вот что я сделаю:

- расскажу простым нетехническим языком, как построить невскрываемый шифр;
- предложу свыше 140 шифров, готовых к применению. 30 из них невскрываемые;
- снабжу вас инструментарием и методами, позволяющими комбинировать и дополнительно укреплять шифры;
- опишу вычисление, которое позволит точно измерить стойкость шифра и гарантировать, что он невскрываемый;
- покажу, как построить и включить в проект коды, сжимающие данные;
- раскрою практический метод получения невскрываемого шифра с помощью одноразового блокнота;
- расскажу, как генерировать сразу много истинно случайных чисел;

- покажу, как находить очень большие и безопасные простые числа;
- научу добавлять необнаруживаемую закладку в шифр;
- раскрою потенциально фатальный дефект в квантовой криптографии;
- объясню, как бороться с гипотетическими ультракомпьютерами, которые, возможно, будут разработаны через несколько десятилетий (а, возможно, уже существуют, только это не афишируется).

Книга написана разговорным языком, как будто мы ведем дружескую беседу. Говоря «мы» или «нас», я имею в виду, что вы, читатель, и я, автор, совместными усилиями стараемся решить какую-то задачу или защитить какой-то секрет.

Эта книга – не научный труд. Я упоминаю о происхождении методов и идей, когда примерно знаю источники и даты, но многие знания я приобрел неформально. Вы почти не найдете ссылок, сносок и комментариев эрудита. Я хотел написать практически полезную книгу. Следуйте изложенным рекомендациям – и получите безопасный шифр. Сто пудов.

Иногда я включаю любопытные исторические факты – отчасти чтобы снять напряжение, а отчасти чтобы воссоздать историческую правду. Я знаю, что изучать криптографию – тяжкий труд. И надеюсь, что речь от первого лица, анекдот-другой и толика юмора помогут немного облегчить его.

В книге много нового материала. Приведены методы построения и взлома шифров, которые раньше нигде не публиковались. Есть даже несколько моих собственных математических открытий. Их вы найдете только в этой книге. Есть куча практических советов, как сделать то или другое, несколько компьютерных методов, рассказано, как можно ускорить вычисления или обойтись меньшей памятью.

Упор в книге сделан на особо безопасную криптографию. У вас имеется информация, которую необходимо сохранить в секрете от противника, располагающего суперкомпьютерами или даже квантовыми компьютерами. Из этой книге вы узнаете, как это сделать. Я представлю широкий набор инструментов, новых и давно известных, которые можно комбинировать бесчисленными способами, получая в итоге шифры сколь угодно высокой стойкости. Студенты, изучающие криптографию, и программисты, применяющие ее в работе, найдут здесь широчайший спектр практических методов, которые можно использовать для разработки новых криптографических продуктов и сервисов.

При всем при том я хочу, чтобы изложенный материал был доступен как профессионалам, так и любителям. Есть немало методов, которые можно реализовать, имея лишь листок бумаги и карандаш. Один такой метод описан в конце раздела 9.6.1. Эти методы пригодны для работы в полевых условиях, когда нет ни электричества, ни электронных устройств. Есть даже несколько шифров, доступных детям.

Любой человек может создать невскрываемый шифр.

И *вы* можете создать невскрываемый шифр. Нужно только знать, как это сделать. Если вы сумеете прочесть и понять эту книгу целиком или хотя бы наполовину, то сможете создать невскрываемый шифр. Эта книга научит любого желающего, как построить шифр, который устоит против атаки, всерьез организованной профессиональным криптографом, располагающим суперкомпьютером. Никакая другая книга не может этим похвастаться. На самом деле для разработки собственного безопасного шифра не нужно ничего, кроме карандаша и бумаги. Я собрал большую коллекцию методов и идей, начиная с XV века, и покажу вам, какие комбинации увеличивают стойкость шифра, а какие являются пустой тратой времени. Я вооружу вас проверенными временем приемами, дополнив их совсем новыми техниками, которые позволят возвести неприступную крепость.

Честное предупреждение: по образованию я математик, а по профессии специалист по информатике, так что без стеснения пользуюсь математической нотацией и математическими понятиями. Эта книга адресована не только инженерам и математикам, но и более широкой аудитории. Я буду объяснять всю необходимую математику, так что обращаться к другим источникам не придется. Если вы понимаете, что такое нижние индексы и показатели степени, если можете читать выражения, содержащие скобки, то никаких других математических знаний и не понадобится. Все сверх того – простые числа, модульная арифметика, операции над матрицами и математические кольца – я объясню здесь же.

Если вы не понимаете какую-то математическую идею, то есть три пути: (1) поверить мне на слово, (2) пропустить раздел целиком или (3) не использовать соответствующий криптографический метод. Есть достаточно других. И некоторые точно вас устроят.

Или просто впрягайтесь и читайте разделы, посвященные математике. Вы удивитесь тому, как много нового узнаете. Не расстраивайтесь, если не понимаете какую-то тему. Возможно, следующая окажется проще. Даже профессиональные математики понимают не всё.

2 Что такое криптография?

Краткое содержание главы:

- основные криптографические термины;
- что такое невскрываемый шифр;
- какие есть виды криптографии.

Криптографию часто называют «искусством тайнописи». Но этим она не исчерпывается. Криптография включает всё: от невидимых чернил до передачи сообщений с применением квантового запутывания фотонов. В частности, криптография включает придумывание и вскрытие кодов и шифров.

Разные авторы придают криптографическим терминам разный смысл, поэтому с самого начала договоримся о некоторых основных терминах.

Открытым, или *незашифрованным*, *текстом* называется сообщение или документ, который мы хотим сохранить в секрете. В традиционной криптографии сообщение было бы записано текстом на некотором языке, известном как отправителю, так и получателю. В век компьютеров это может быть файл любого типа, например: PDF (текст), JPG (изображение), MP3 (аудио) или AVI (мультимедиа).

Шифром называется метод или *алгоритм*, который искажает сообщение до неузнаваемости, например, изменяя порядок символов или заменяя одни символы другими. В общем случае шифры при-