Миронов Илья Лазаревич

ЗАНЯТИЕ 3. СЕКРЕТНАЯ НАУКА

Секретная наука

Криптография - это одна из самых интригующих и таинственных областей современной науки, которая является не служанкой политиков и военных, а сама меняет окружающий нас мир. Со времен Юлия Цезаря и древних греков способы сокрытия тайн охранялись строже, чем государственные секреты, так как ключ от любого сейфа представляет ценность заведомо большую, чем содержимое одного сундука с драгоценностями.

Начиная от школьной записки и кончая контрольной цифрой на любой купюре, выпущенной Центральным Банком РФ, мы окружены тайнами, секретами и способами их сохранения. Всем знакомы два классических произведения художественной литературы, в которых главной пружиной сюжета являются шифры. Конечно, это «Золотой жук» Эдгара По и «Пляшущие человечки» Конан Дойля. Недаром они относятся к детективному жанру, так как раскрытие даже непритязательного шифра есть задача, сложнее и запутаннее расследования весьма изощренного преступления.

С точки зрения профессиональных криптоаналитиков, шифры вроде того, что разгадал Шерлок Холмс или которому пират Кидд доверил тайну своих сокровищ, ненадежны и неприемлемы для серьезных приложений. Разумеется, нужно соизмерять сложность используемого шифра, ценность шифруемых данных и усилия, которые может приложить охотник до чужих тайн для его взлома. Если вам потребуется так зашифровать свои файлы, чтобы их не смогла прочесть младшая сестра, то можно воспользоваться любым подстановочным шифром. Если вам противостоит серьезная организация или секретная служба крупного государства, то требования к надежности шифра многократно возрастают.

Вот один пример, обнажающий те этические проблемы, которые ставит криптография. В годы второй мировой войны англичанам удалось взломать немецкий шифр Enigma. Между прочим, для этого была построена машина, с полным правом претендующая на звание первого компьютера в мире. Сведения, получаемые в результате радиоперехватов и расшифровки немецких переговоров, представляли исключительную важность. И даже получив информацию о готовящейся бомбежке Ковентри, британские военные власти не стали предпринимать никаких мер, которые могли бы навести противника на мысль, что его планы раскрыты...

В этой статье мы коснемся нескольких аспектов современной криптографии, которые помогут вам создать представление о том, чем занимаются самые секретные отделы ведущих спецслужб мира. Хочется лишь предостеречь тех, кто, не встретив здесь ни одной формулы, сделает неправильный вывод о том, что криптография - это удел программистов и офицеров связи. На самом деле, целые отделы теории чисел развиваются, чтобы подкрепить математический аппарат криптографии, а многие статьи невозможно понять без солидной подготовки в алгебре, анализе и статистике.

DES, NSA etc.

Истории создания и взлома шифров могли бы стать основой для увлекательных романов, если бы они не хранились в архивах спецслужб под грифами наивысших уровней

секретности. Например, сам факт существования агентства по национальной безопасности - National Security Agency (NSA) в США являлся тайной в течение многих лет. Бюджет агентства засекречен и по сей день. Считается, что NSA является крупнейшим в мире работодателем для математиков, также как и самым большим покупателем компьютерного оборудования.

Поэтому, когда под контролем NSA был разработан и предложен в качестве стандарта алгоритм шифрации DES (Data Encryption Standard) в 1976 году, возникло необычайно много спекуляций и слухов относительно его надежности. Ведь главная проблема анализа стойкости алгоритмов шифрации заключается в том, что не существует никаких реальных методов формального доказательства того, что данный конкретный алгоритм надежен. С другой стороны, доказать слабость алгоритма весьма просто - для этого достаточно предъявить способ его взлома. Поэтому общепринятым методом подтверждения надежности алгоритма является его публикация и обсуждение научным сообществом. Если в течение достаточно долгого времени анализ авторитетных экспертов или организаций не обнаружил дырок в его защите, то такой алгоритм начинает пользоваться доверием.

DES является типичным алгоритмом блочной шифрации; он шифрует блоки по 64 бита. Блок из 64 бит поступает на вход алгоритма, блок той же длины зашифрованных данных является результатом работы алгоритма. DES - это симметричный алгоритм: один и тот же алгоритм и ключ используются для шифровки и расшифровки (за исключением незначительных различий в управлении ключом). Фактическая длина ключа составляет 56 бит (хотя ключ представляется в виде 64-битного числа, каждый восьмой бит используется для контроля четности и при шифрации игнорируется). Ключом может быть любое 56-битное число. В секретности ключа заключается вся защита, предоставляемая алгоритмом, так как, не зная ключа, расшифровать текст невозможно.

На элементарном уровне, алгоритм есть всего лишь комбинация двух стандартных методов шифрации: смешивания и распространения. Основные блоки, из которых состоит DES, состоят в однократном применении этих методов (подстановки и перестановки) с использованием ключа. Эта операция называется раундом. DES предусматривает 16 раундов, заключающихся в применении одних и тех же методов, использующих разные части ключа.

Стандарт DES в том виде, в котором он был опубликован, вызвал массу вопросов, касающихся его внутренней структуры. Почему были выбраны именно такие логические функции? Почему он совершает ровно 16 раундов? Почему длина ключа лишь 56 бит? Почему, наконец, DES рекомендован к применению только для защиты правительственной информации без грифа «секретно?

Как оказалось, на многие вопросы у NSA были свои ответы, которые оно предпочло не раскрывать в свое время научной общественности. Например, DES оказался специально защищен от применения дифференциального криптоанализа, предложенного в 1990 году и показавшего себя очень эффективным против других известных алгоритмов. Оказалось, еще в середине 70-х NSA было знакомо с этим методом, но оно не стало вводить его в научный обиход, желая использовать свое преимущество для взлома других способов шифрации.

Это дало повод предположить, что NSA, возможно, знало методы взлома DES, которые были встроены в него еще на этапе проектирования. Такое количество

сомнений, окружающих алгоритм и его создателей, спровоцировали беспрецедентную атаку со стороны виднейших специалистов в области криптографии на DES. Фактически, внимание, привлеченное этой проблемой, стало одним из катализаторов бурного развития криптографии в течение последних 20 лет. Вопреки всем усилиям, DES остается все еще очень надежным и превосходно зарекомендовавшим себя алгоритмом, для которого существуют очень эффективные аппаратные методы реализации.

Существует ли надежный шифр?

А существуют ли вообще шифры, которые было бы невозможно раскрыть? Оказывается, да. Более того, они уже давно применяются шпионами. Для таких шифров необходимо наличие идентичных копий одноразового блокнота у получателя и отправителя секретного сообщения. Представим себе блокнот, сплошь заполненный абсолютно случайными буквами. Отправитель использует одну букву из блокнота для шифрации одной буквы исходного сообщения. Шифрация состоит в сложении по модулю 32 номеров букв из блокнота и сообщения.

Например, если сообщение представляет собой строку

ПАКЕТВЫКРАЛ,

а соответствующие буквы из блокнота есть

ЕИАКПАФКАЬЯ,

то зашифрованный текст будет

ФИКПБВПФРЬК,

так как

П+Е mod 32= Ф,

А+И mod 32= И

...

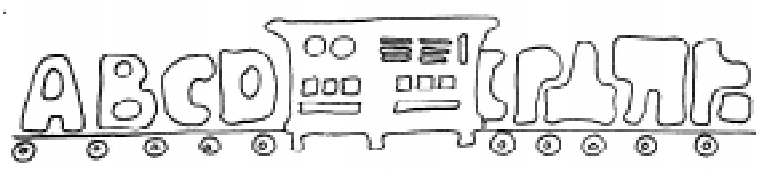
К сожалению, у этого абсолютно надежного метода есть несколько существенных недостатков. Во-первых, длина ключа оказывается равной длине шифруемого сообщения. Во-вторых, ключ должен использоваться не больше одного раза (шпионы обязаны уничтожать использованные страницы своих блокнотов), так как в случае повторного использования взлом кода становится весьма простой задачей. В-третьих, у получателя и отправителя должны быть совершенно одинаковые копии этих блокнотов, а если они смогли секретным образом передать такие блокноты, то почему бы им ни воспользоваться тем же каналом для передачи самого сообщения? Тем не менее, этот метод реально применяется, и в литературе можно встретить утверждение, что в «горячей линии» связи Кремль-Вашингтон используется похожий алгоритм.

Как передать информацию без кодирования

А нужны ли шифры вообще? Можно ли передавать информацию, не используя никакого кодирования? Криптография занимается изучением и таких вопросов, предлагая алгоритмы, с помощью которых можно обмениваться информацией, не раскрывая никаких тайн.

Представим, что в школе произвели тестирование IQ. Всем интересно сравнить свой результат с интеллектуальным коэффициентом одноклассников, но никто не хочет раскрывать свой IQ. Оказывается, школьники могут узнать средний IQ в своем классе, при этом ничей результат не раскрывается. Конечно, для этого им достаточно бросить бумажки в шляпу, а потом огласить результаты. А если они уже разъехались на каникулы и поддерживают связь только по электронной почте?

Для простоты будем считать, что среднее своих результатов хотят узнать четыре школьника Аня, Боря, Вася и Гена. Пусть Аня выберет любое случайное число R, прибавит его к своему результату и сообщит его по секрету Боре. Боря прибавит к полученному числу свой результат и пошлет его Васе в тайне от остальных



участников. Вася прибавит свой результат и сообщит его Гене. Гена, добавив к числу свой IQ, пошлет его Ане. Ане вычтет из полученного числа R, поделит его на четыре и объявит результат.

Можно заметить, что, если все честно следуют правилам, то полученный результат и будет средним IQ в классе. Конечно, Аня и Вася, сговорившись, могут узнать результат Бори. Немного модифицированная версия этого алгоритма (придумайте ее!) уберегает Борю от сговора любых двух участников. В таком алгоритме для выяснения точного результата одного участника требуется сговор всех остальных.

Как честно сыграть в орлянку

Пришло время рассказать одну историю.

Алиса и Боб хотят сыграть в орлянку, но у них нет монетки, которую можно было подкинуть. Алиса придумала простой способ подкидывания монетки в уме.

– Давай ты задумаешь случайный бит (0 или 1), я тоже задумываю случайный бит. Если наши биты равны, то выпал орел, если нет, то выпала решка, - предложила Алиса.

– А если кто-то из нас выберет свой бит не случайно? - поинтересовался Боб.

– Не имеет значения. Пока какой-нибудь из наших битов выбирается случайно, результат их сравнения тоже будет случаен, - ответила Алиса после недолгого раздумья. Боб признал правоту Алисы.

Вскоре после этого Алиса и Боб нашли книжку по искусственному интеллекту, валяющуюся на дороге. Хорошая девочка Алиса сказала: «Один из нас должен подобрать книгу и отнести ее в подходящее мусорное ведро». Боб согласился и предложил, чтобы они подкинули монетку в уме, чтобы определить, кто должен понести книгу.

– Если орел, то книгу понесешь ты, если решка, то я, - скала Алиса, - какой твой бит?

– 1, - ответил Боб.

– У меня тоже, - лукаво сказала Алиса, - мне кажется, тебе сегодня не повезло.

Не нужно объяснять, что в алгоритме подкидывания монетки в уме есть серьезная проблема. В действительности, алгоритм, предложенный Алисой, не гарантирует того, что биты, выбираемые игроками, независимы. По счастью, Алиса и Боб получили письмо от студента, интересующегося криптографией. Содержимое письма было слишком сложным, чтобы его кто-то смог понять, но конверт, в котором пришло письмо, оказался очень полезен.

В следующий раз, когда Алиса и Боб захотели подкинуть монетку, они сыграли в несколько модифицированную версию исходного алгоритма. Когда Боб задумал бит, он не стал его сообщать Алисе, а вместо этого записал его на клочке бумаги и положил в конверт. Затем Алиса объявила свой бит. После этого Алиса и Боб открыли конверт и сравнили бит Алисы с записанным битом Боба.

Результат сравнения битов оказывается случайным, если хотя бы один игрок играет честно. Алиса и Боб стали пользоваться таким чудесным алгоритмом и прожили долгую и счастливую жизнь.

Как же реализовать такой алгоритм на компьютере, не пользуясь никакими конвертами и записками? Для этого нам потребуется понятие односторонней функции. Односторонняя функция - это такая функция f, что по значению $f(x)$, вычислить x можно только перебором всех вариантов. Такую функцию построить сравнительно легко. Для этого необходимо предложить алгоритм, который бы полностью перемешивал биты x, применяя к ним достаточно много раз нелинейные преобразования, а множество значений функции состояло бы из нескольких сотен

бит. Кроме того, требуется, чтобы было вычислительно очень сложно подобрать такие значения x и y, чтобы выполнялось равенство $f(x)=f(y)$.

Итак, пусть Алиса и Боб согласовали функцию f. Боб загадывает случайное число x, вычисляет $y=f(x)$ и посылает y Алисе. Алиса пытается угадать, четное ли число x, и посылает свою догадку Бобу. Если Алиса угадала, то результатом игры считается орел, если нет, то решка. Боб сообщает результат игры и посылает x Алисе. Алиса проверяет, действительно ли $y=f(x)$.

Видно, что игра оказывается абсолютно честной: Алиса не имеет представления о четности x в силу односторонности функции f, а Боб не может подменить x после того, как Алиса высказала свою догадку, так как подобрать число с тем же значением функции f очень сложно.

Как сравнить записки, не раскрывая их содержимого

Давайте ознакомимся еще с одной историей, герои которой мучаются подозрениями, а искусное использование криптографических протоколов позволяет им совершенно честно узнать то, что они хотят, не скомпрометировав ничье имя.

Соседи по парте Андрей и Борис получили записки, в которых они приглашались на свидание. Зная смешливый характер девочек своего класса, они заподозрили, что эти записки одинакового содержания, и, придя на свидание, они встретят там друг друга.

- Боря, покажи мне свою записку, если там то же, что и у меня, то нам нужно будет кое-кого здорово проучить, - предложил Андрей.

– Нет, лучше ты мне свою покажи, - спрятав получше свою записку, сказал Боря.

– А если там не то же, что у тебя? Не буду я тебе свою записку показывать, - отказался Андрей, надеясь, что у него действительно состоится романтическое свидание.

– А то давай так. Ты вычислишь одностороннюю функцию f от своей записки, а я от своей. После этого мы их сравним и, если они равны, то никуда не пойдем, - предложил выход Боря.

– А если они разные, ты ничего не сможешь узнать про мою записку? - встревожился Андрей.

– Конечно нет, ведь мы будем использовать действительно ***односторонюю*** *функцию, - убежденно сказал Борис.*

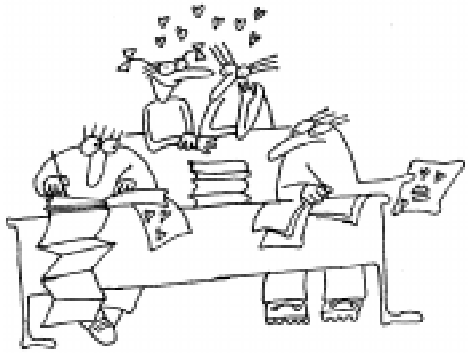
Помогая себе громким сопением, Андрей и Борис вычислили значения одной и той же односторонней функции f от текста своих записок, закодированного в двоичной системе счисления. У них получились числа длиной 128 бит.

– А как мы будем сравнивать наши числа? Ведь если кто-то из нас покажет другому свое число, то тот может запросто сказать, что у него число другое, хотя на самом деле они одинаковые, - задумался Андрей.

– И правда, что же делать? Хотя можно было бы вычислить односторонние функции от наших чисел, а потом ими обменяться, но уж больно не хочется еще раз вычислять эти длиннющие функции. - согласился Борис.

– Я придумал! Давай, каждый из нас будет по очереди называть биты своего числа. Я - первый бит, ты - второй, потом я - третий бит и так далее. У каждого из нас будет возможность проверить, совпадают ли наши числа, - воскликнул Андрей.

– Но ведь так мы узнаем только каждый второй бит другого числа. Если они отличаются, то это, конечно, означает, что числа разные, ну, а если они равны?



– Вероятность того, что у двух почти случайных чисел совпадут 64 бита, настолько мала, что на нее можно не обращать никакого внимания. А односторон

няя функция формирует почти случайные числа, не имеющие ничего общего с исходным текстов, - заверил Борю Андрей.

Так они и сделали, разрешив разом все свои сомнения.

И это все?

Из этой статьи вы могли узнать несколько элементарных примеров из криптографии, в которых, как в капле воды, отражаются многие понятия, появившиеся лишь в последние два десятка лет. Конечно, можно было бы также рассказать о том, как можно играть в покер по телефону, проводить выборы по радио (когда все слышат всех), расплачиваться цифровыми деньгами, которые невозможно подделать или скопировать. Но ведь где-то нужно остановиться.

Часть информации для этой статьи была почерпнута из книги Брюса Шнайера «Прикладная криптография», которая пока еще не переведена на русский язык. В этой книге описываются поразительные протоколы и алгоритмы, которые уже начинают применяться в высокотехнологичных устройствах, таких, как сотовые телефоны или «умные» кредитные карточки.

Надеюсь, что вам стала несколько ближе и понятнее криптография, наука о секретах и об алгоритмах, их стерегущих. Хотя конца спирали алгоритм шифрации - способ взлома не видно, каждый следующий виток становится еще круче и увлекательнее. Захотите - и вы тоже сможете принять участие в этой гонке.