1. Введение

1.1. Что такое бит?

Бит является фундаментальной единицей информации. Он может принимать значения 0

или 1. В течение сорока последних лет компьютеры работают сбинарными данными, то

есть с наборами битов (а не с цифрами от 0 до 9, как это принято у людей; можно

сказать, что компьютеры имеют только два пальца). Битыпозволяют кодировать целые

числа, символы, и т.д.. Вся информация, проходящая через компьютер, превращается

в биты.

8 бит образуют байт; это дает 256 комбинаций и позволяет кодировать числа от 0

до 255 или символы (включая разницу между прописными и строчными буквами,символы

с надстрочными знаками и другие).

1024 байта образуют один килобайт (кБ). 1024 используется вместо 1000 так как

1024 является степенью числа 2, то есть "круглым" числом, еслиработать по

основанию 2. 1024 килобайта образуют мегабайт (МБ), или 1048576 байт. 1024

мегабайта образуют гигабайт (ГБ), или 1073741824 байта. 1024 ГБобразуют терабайт

(ТБ). Дальнейшее умножение малоупотребительно, т.к. дорогостояще со всех точек

зрения. Типичная емкость жестких дисков широко распространенных внастоящее время

компьютеров составляет десять гигабайт. Развитая сеть может пропускать десять

мегабайт в секунду между двумя машинами.

1.2. Что такое криптографический ключ?

Криптографические операции, такие как шифрование и подписание данных электронной

цифровой подписью, могут быть осуществлены только определеннымилицами,

располагающими некоторыми секретами. В прошлые века этим секретом был сам способ

преобразования данных. Однако более рационально и более

эффективноконцентрировать этот секрет в виде набора битов, а сам алгоритм делать

общедоступным.

Действительно, сохранять в тайне алгоритм проблематично, и, кроме того,

необходима численная оценка его безопасности. Сам факт публикации

алгоритмапозволяет "бесплатно" получить признание его надежности

криптографическим сообществом.

Ключ, таким образом, является концентрацией секрета, этот набор битов является

"эссенцией" конфиденциальности.

1.3. Что такое полный перебор?

Взломать криптосистему, значит суметь осуществить некоторые операции, требующие

(в теории) знания секрета (ключа), не имея информации о последнем.Наиболее

полным взломом является взлом, в результате которого становится известен ключ,

что дает взломщику те же полномочия, что и законному владельцуключа.

Полный перебор является наиболее простым методом этой точки зрения: он состоит в

том, чтобы пробовать все ключи один за другим до тех пор, пока ненайдется

правильный. Этот метод является наиболее общим, и может быть распараллелен

(вычисления могут быть распределены на много машин). Кроме того,он наиболее

реалистичен: если рассматривать случай симметричной системы шифрования (которая

ставит в соответствие блоку, состоящему из несколькихбайтов, другой блок той же

длины, но преобразованный к "нечитаемому" виду при помощи ключа), достаточно

перехватить пару открытыйтекст/зашифрованный текст, то есть блок из несколько

байтов и соответствующих им зашифрованных. Например, если передается картинка в

формате JPG, то началосообщения представляет собой стандартный заголовок JPG,

формат которого всем хорошо известен.

С точки зрения статистики, надо перебрать примерно половину возможных ключей,

прежде чем найдется правильный. Если длина ключа составляет 56 битов,это

означает, что в среднем необходимо провести 2^55 итераций, что составит

36028797018963968.

1.4. Является ли полный перебор единственновозможным методом криптоанализа?

Нет. Но другие методы сильно зависят от конкретного алгоритма. Некоторые,

такиекак линейный или дифференциальный криптоанализ, требуют огромного числа пар

открытый/зашифрованный текст, представляя, таким образом, чисто

теоретическийинтерес.

Кроме того, существуют криптосистемы (в частности, системы асимметричные,

называемые еще "системами с открытым ключом"), для которых всесочетания битов не

образуют правильного ключа. Типичный пример - RSA, где ключ представлен большим

числом, полученным из двух больших простых чисел.Совокупность наборов из 1024

бит, которые являются двоичной записью этих чисел, гораздо меньше 2^1024. Полный

перебор абсурден в этом случае.

1.5. 128-битный ключ в два раза устойчивее квзлому, чем 64-битный?

НЕТ! Это распространенная ошибка. Каждый дополнительный бит удваивает количество

возможных ключей и затраты на полный перебор. Ключ длиной 128 битявляется в

18446744073709551616 раз более сложным для подбора, по сравнению с ключом длиной

64 бита (который уже не назовешь совсем легким).

1.6. PGP должно быть очень устойчив, так какиспользует ключи 1024 бита.

Стоп! Давайте разберемся! "1024 бит" в PGP - это ключ RSA или DSS, то есть ключ

асимметричного алгоритма. Атака методом полного перебора не самыйлучший вариант

в этом случае.

Кроме того, асимметричные алгоритмы относительно медленны, и "внутри" PGP

использует симметричный алгоритм (исторически IDEA,затем CAST) размер ключа

которого составляет 128 бит.

2. Текущее положение дел

2.1. Какова максимальная длина ключа длясимметричных криптосистем, которая

поддается программному взлому методомполного перебора?

Известно, что два ключа по 56 бит были подобраны полным перебором на обычных

компьютерах типа PC. Специализированная машина (построенная EFF) помогла

длявторого ключа, выполнив приблизительно треть общего объема вычислений.

Ключи были для алгоритма DES. Качественный ПК или рабочая станция могут

перебирать с максимальной скоростью нескольких миллионов ключей в секунду.

Еслипринять среднюю скорость один миллион ключей в секунду на машину, то легко

видеть, что для подбора ключа 10000 машин должны в среднем затратить 42 дня.

Полный перебор ключа длиной 64 бита для RC5 (для которого сложность полного

перебора несколько выше, чем для DES) в настоящее время продолжается, и

будетдлиться, по крайней мере, еще нескольких лет. Напоминаем, что подбор ключа

размером 64 бита, является в 256 раз более трудоемким, чем подбор ключа длиной

56 бит.

2.2. То же, с использованием специальнойаппаратуры?

Американская группа EFF, инвестировала 250000$ в создание специализированной

машины под названием "Deep crack" ("глубокий взлом"),которая в состоянии

перебрать все ключи алгоритма DES приблизительно за три дня. В ней использованы

специализированные процессоры, которые невозможноприменить для целей, отличных

от взлома DES (в частности, они ничего "не знают" о RC5).

Все остальные машины того же рода - из области слухов. DES используется уже

более 20 лет, и можно предположить, что, вероятно, машине EFF

предшествовалидругие прототипы, разрабатываемые секретными службами. В любом

случае, скоро уже 15 лет периодически упоминаются принципы построения такой

машины.

2.3. А для несимметричных криптосистем?

В принципе, существуют две математические задачи, используемые в асимметричных

шифрах: факторизация и дискретное логарифмирование. RSAиспользует первую, DSS

вторую. Другие упоминаемые задачи (вариации двух предыдущих, использование

эллиптических кривых, задача об укладке ранца,минимизация сети (задача

коммивояжера), обратное распознавание (permuted perceptrons problem - см.

примечания) относительно редко используются в настоящеевремя.

Рекорд факторизации датируется 22-ым августа 1999: число размером 155 десятичных

цифр (512 бит) было факторизовано за шесть месяцев вычислений напарке

приблизительно из 600 машин, некоторые из которых могут быть квалифицированны

как "быки" (в частности Cray с 2 ГБ памяти).Примененные алгоритмы гораздо более

сложны, чем полный перебор, и требуют большого количества оперативной памяти с

хорошей скоростью доступа.

Дискретное логарифмирование менее исследовано, на его взлом осуществлено меньше

инвестиций, чем на факторизацию. Рекорд - порядка 95 десятичных цифр.

2.4. Что относительно "кофейника"Шамира?

Представленный на Eurocrypt'99 в Праге (в начале мая 1999), этот аппарат

ускоряет физическими средствами исследование гладких чисел (то есть

полученныхпроизведением только маленьких простых чисел), которые получают обычно

методом решета. Эти числа являются основой нескольких алгоритмов факторизации и

решенийзадачи дискретного логарифмирования.

Сам аппарат еще не построен, описаны только его принципы. Существуют технические

проблемы для реализации прототипа (Arjen Lenstra высказал некоторыевозражения, с

которыми Adi Shamir согласился).

По общему мнению, этот метод позволил бы факторизовать число приблизительно в

600 бит, со средствами, которые позволили установить рекорд в 465 бит (вфеврале

1999), если все проблемы с реализацией будут решены. Отмечено, что решето заняло

приблизительно 60% времени для рекорда в 512 бит.

Все же шоу было очень увлекательным. Phil Zimmerman, автор PGP, заметил, что

очень доволен тем, что исследователи интересуются, как обстоят дела в

этихпроблемах, так как это увеличивает степень доверия к такого рода системам.

3. То, что будет возможным в будущем

3.1. Что такое закон Мура?

Закон Мура (Moore) является оценкой развития вычислительной техники во времени.

В базовом варианте он гласит, что для заданной стоимости (в широкомсмысле,

включая энергопотребление, производство оборудования, износ, стоимость хранения,

и т.д.) вычислительная мощность увеличивается в 8 раз каждые 3 года.Говоря более

точно, можно сказать, что через каждые три года, технологические достижения

позволяют разместить в 4 раза больше логических элементов вмикросхеме заданной

стоимости, одновременно ускоряя ее быстродействие в 2 раза.

Этот закон замечательно подтверждался в течение последних 15 лет. Следует

отметить, что центральные микропроцессоры компьютеров общего назначения

неполностью следуют этому закону, потому что они не могут так же быстро

увеличить размер шины данных (по соображениям обратной совместимости кода, а

такжепотому, что вычисления, которые эти процессоры обычно производят, имеют

дополнительные ограничения, делающие бесполезным использование слишком

большихрегистров).

Это касается, таким образом, систем, описываемых в терминах логических

элементов, специализированных на конкретном алгоритме. Таким образом, это посути

ASIC (Application Specific Integrated Circuit - специализированные микросхемы) и

FPGA (Field Programmable Gate Arrays - программируемые логическиеинтегральные

схемы); то есть перепрограммируемые цепи, выполняющие те же задачи, что и ASIC,

но вдвое более дорогие при заданной мощности, однакоявляющиеся многоцелевыми).

3.2. Какова предполагаемая стоимость полногоперебора с использованием

специализированного оборудования?

Если закон Мура будет продолжать выполняться (и не имеется веских оснований для

обратного, так как он учитывает качественные достижения, а не толькоувеличение

точности обработки кремния), можно достичь машины EFF (четверть миллиона

долларов, для 56 бит за 3 дня) и добавлять 3 бита каждые 3 года (3бита = 2^3 =

8; что дает в 8 раз больше возможных вариантов ключей).

Заметим, что для сохранения закон Мура, качественные достижения должны

происходить достаточно быстро, так как имеются пределы в увеличении

плотностиэлементов на кристалле кремния (замедление вследствие туннельного

эффекта). В ряде разрабатываемых методов предполагается осуществить замену

кремния наарсенид галлия, что позволит достичь более высокой плотности

элементов, замену алюминия медью, которая позволяет работать гораздо более

быстро, построениеоптической логики (оптический элемент переключается

приблизительно в 100 раз быстрее электронного, но его стоимость выше более чем в

100 раз).

Таким образом, можно считать, подобрать полным перебором 128-битный ключ так же

"легко", как сейчас 56-битный, станет возможным через 72 года. Этаоценка

является "наилучшей", в то время как многие исследователи этой тематики

полагают, что закон Мура будет выполняться в лучшем случае ещенесколько лет

(действительно, все качественные изменения, привнесенные за последних 15 лет,

были просто нереализованными, известными с 1975 года, и ихзапас почти исчерпан в

настоящее время).

3.3. А с использованием квантовыхкомпьютеров?

Квантовые компьютеры, реализуемые через суперпозицию состояний одной частицы,

являются более мощной вычислительной моделью, чем машина Тьюринга ипозволяют

осуществить многие операции (среди которых полный перебор ключей такого

"безграничного" алгоритма, как DES) за субэкспоненциальное время.

Квантовые компьютеры очень соблазнительны, но они не существуют. Был построен

двухбитовый квантовый регистр, но имеются достаточно мощныепрепятствия для

построения машины, способной сломать DES (главным образом, инициализация этого

монстра, которая не может быть распараллелена, и занимает,таким образом, 2^n

операций для ключа n битов).

Это не имеет большого значения для другого типа квантовой криптографии, который

служит для "неперехватываемой" передачи данных по оптоволокну(используя принцип

неопределенности Гейзенберга).

4. Различные слухи

4.1. NSA/DST/другие могут ломать ключи до128 бит.

Имеются очень сильные возражения против такого рода высказываний. Среди

классических можно выделить одно, предполагающее наличие процессора

сэнергопотреблением в 10 раз меньше, чем у классических (таким могли бы

располагать секретные службы, имеющие преимущество). Энергетические затраты

наполный перебор 128-битного ключа, если их перевести в тепловую форму,

заставили бы исчезнуть под водой Нидерланды в результате таяния полярных льдов.

Что касается 256-битных ключей, то если предположить, что затраты на анализ

одного ключа равны энергии перехода электрона с одной орбиты атома на другую,то

количества великодушно предоставляемой Солнцем энергии недостаточно для

осуществления такого перебора за разумное время.

Некоторые легко манипулируют количеством битов, легко относя 20 бит на

использование сверхпроводников или оптических элементов, 20 других наприменение

суперэффективных алгоритмов, и 30 последних потому что "это уже немного" (да,

просто помножим на 1 миллиард, это действительно"немного").

Напомню, что число битов экспоненциально. Это означает, что затраты на перебор

каждых n битов пропорциональны 2^n. Чтобы это было легче представить,напомним,

что:

64 бита: 18446744073709551616 возможных ключей

128 бит: 340282366920938463463374607431768211456 возможных ключей

256 бит:

115792089237316195423570985008687907853269984665640564039457584007913129639936

возможных ключей

4.2. NSA/DST/другие обладают квантовымикомпьютерами.

Очень маловероятно. Если это правда, то технологические достижения опережают

всех как минимум лет на 10. Другими словами, они располагали бы тогда

такойпродвинутой технологией, что сама идея дальнейшей борьбы была бы абсурдом.

Некоторые упоминают возможность получения внеземной технологии, либо через Людей

в Черном, либо непосредственно через Phil Zimmerman, их посла на этойпланете.

Как считают другие источники, квантовым компьютером располагала цивилизация

Атлантов (конечно, Атлантида была затоплена именно в результатеперебора ключа

"классическими" методами, см. выше).

Сталкиваясь с проявлениями абсурда и дилетантства в этой области, хочется

посоветовать держаться подальше от подобного рода спекуляций, чтобыневыглядеть

клоуном. Если хочется оценить что в состоянии сделать NSA, надо дать ему 3 года

времени в соответствии с законом Мура и хороший бюджет. Это позволитсделать

задачу с 64 битами решаемой. 80 бит останутся недостижимыми.

4.3. NSA/DST/другие достигли методов криптоанализа,недоступных другим.

NSA (в лице Don Coppersmith) объявил в 1987 году, что знали уже в 1977 о

дифференциальном криптоанализе, обнародованном Бихамом и Шамиром (E. Biham,

A.Shamir) именно в этом 1987 году. Алгоритм DES, разработанный в 1977,

специально защищен от такой атаки.

Тем не менее, уточним, что такая атака требует огромного количества пар

открытый/зашифрованный текст, и, в любом случае, нереальна. Кроме того, DES

небыл защищен против линейного криптоанализа, открытого в 1993 Matsui, что

ограничивает научное превосходство NSA 15 годами. Наконец, этот последний

способкриптоанализа также нереален, т.к. требует 64 ТБ известного открытого

текста, что в несколько десятков миллионов раз превышает объем Библии.

Подобные слухи ходили также про факторизацию, дискретное логарифмирование и

средства от прыщей. Легко можно встретить такие слухи в упоминаниях

омеждународных заговорах злодеев, которые хотят знать все обо всех в этом мире.

В любом случае, с определенного момента, гораздо дешевле установить видеокамеру

в вашем офисе, чем заставлять "молотить" квантовыйкомпьютер. Знаете ли Вы, что

восстановление изображения Вашего монитора возможно с дистанции 100 метров? То

же самое касается и сигналов клавиатуры,когда Вы печатаете. Необходимо иметь

хорошо спроектированную сетку Фарадея, чтобы защищаться от этого. Шифрование

позволяет установить защищенный каналмежду двумя точками, но не защищает сами

точки.

4.4. Я работаю на NSA/DST/других и поэтомупытаюсь убедить общественность, что

128-битное шифрование надежно.

Niark niark niark. Я обманщик, не так ли?

© Автор: Thomas Pornin (thomas.pornin@ens.fr); оригинал:

http://www.dmi.ens.fr/~pornin/faq-cle.html

©Владислав Мяснянкин, перевод на русский язык.

Примечания переводчика.

Пожалуйста, не присылайте мне замечания/комментарии по содержанию документа. Я

только перевел его. Пишите непосредственно автору (на французском или

английском языке) - адрес в заголовке.

EFF - Electronic Frontier Foundation http://www.eff.org/

NSA - National Security Agency http://www.nsa.gov/

DST - Direction de la Sйcuritй du Territoire

http://www.chez.com/icebreaker/dst/

Я не нашел русского термина для "Permuted Perceptrons Problem" и перевел как

"задача обратного распознавания". Если есть более правильный перевод - буду

рад услышать. Что это такое можно посмотреть например на

http://cgi.dmi.ens.fr/cgi-bin/pointche/papers.html?Po95a (на английском).

Если вы найдете неточности в употреблении терминов или предложите более

"благозвучный" вариант их перевода, это будет воспринято с благодарностью.

Неконструктивная критика и флейм пойдут на /dev/null.