ДИСТАНЦИОННОЕ ОБУЧЕНИЕ

Поздняков Сергей Николаевич

СЕКРЕТНАЯ НАУКА

В электронном приложении к этому номеру журнала представлена лекция С.Н. Позднякова, прочитанная в центре «Интеллект». Публикуем презентацию к этой лекции, которая может рассматриваться как развернутая аннотация, а также как самостоятельная публикация.

Симметричные алгоритмы шифровки

- КНИГА – БУКВА – КНИГА (К-Б, Н-У, И-К, Г-В, А-А)
- ДОМИНО – ИНОДОМ – ДОМИНО (циклический сдвиг на 3)
- ИСКЛЮЧАЮЩЕЕ ИЛИ ДЛЯ ДВОИЧНОГО КОДИРОВАНИЯ XOR (eXlusive OR)

1 XOR 1 = 0
0 XOR 0 = 0

1 XOR 0 = 1
0 XOR 1 = 1

x=10111001000101000101 – исходное сообщение в двоичной кодировке
y=00100101000101001110 – секретный ключ
z=10011100000000001011 – зашифрованное сообщение z = x XOR y
y=00100101000101001110 – тот же секретный ключ
u=10111001000101000101 – расшифрованное сообщение u = z XOR y

Криптографические протоколы

или как передать информацию без кодирования

- Как сосчитать общую сумму денег, не сообщая о своих средствах остальным?

- Каждый добавляет к сумме число и сообщает результат следующему по кругу
- Общая сумма, полученная на первом круге 8888

Криптографические протоколы

или как передать информацию без кодирования

- Как сосчитать общую сумму денег, не сообщая о своих средствах остальным?

- На втором круге каждый вычитает из общей суммы такое число, чтобы разность чисел на первом и втором круге равнялась количеству денег у него
- В результате получаем правильную сумму:
  (1230+888+3200+2010+1560) – (1215+880+3195+1980+1540)=
  = 15 + 8 + 5 + 30 + 20 = 78

Криптографические протоколы

доказательство с нулевым разглашением

- Вы нашли способ, как раскрасить в четыре цвета любую карту, но не хотите делиться секретом, пока вас не признают автором этой идеи

- Как доказать всем, что вы владеете этим методом, если его надо держать в секрете?

Криптографические протоколы

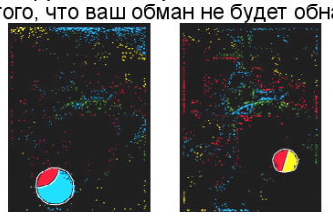
доказательство с нулевым разглашением

- Вы можете предложить проверить себя на раскраске любой карты.
- Однако для сохранения секретности вы не хотите показывать раскраску целиком, а только разрешаете посмотреть раскраску любых двух областей с общей границей (если они раскрашены в разные цвета, то раскраска правильная).
- Предположим для определённости, что у нашей карты имеется 100 таких границ. Сколько проверок нужно сделать, чтобы убедить проверяющего в том, что вы не обманщик (каждая новая проверка предполагает новую раскраску)?

Криптографические протоколы

доказательство с нулевым разглашением

- Если вы неправильно раскрасили области только вблизи одной границы, то обнаружить это будет 1 шанс из 100, то есть 0,99 – вероятность того, что ваш обман не будет обнаружен.



- Однако, если проверяющий сделает 1000 проверок, то вероятность обмана будет $0{,}99^{1000} \approx 0{,}000043$, то есть примерно 1 шанс на 25000. Это очень мало.

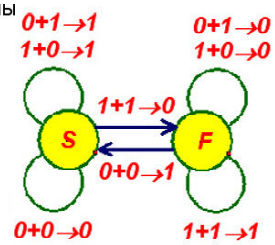
Односторонние функции

- Развитие сети Интернет привело к появлению таких понятий как «электронная подпись», «электронные деньги».
- На самом деле, это просто некоторые специальные способы шифрования, которые получили название шифров с открытой частью

- В основе этих шифров лежит понятие односторонней функции. Это такие функции, которые вычисляются быстро, но сделать обратные вычисления очень сложно.
- Может показаться, что это очень хитрые функции, о которых мы ничего не знаем. На самом деле односторонней функцией является уже умножение чисел: мы можем быстро (на компьютере) перемножить 60-значные числа, но разложить некоторые 120-значные числа на два множителя очень трудно.

Алгоритмы для выполнения операций сложения и умножения над длинными числами

- Пример автомата, вычисляющего сумму двоичных чисел произвольной длины



- Выполнение умножения для двоичных чисел сводится к операциям сдвига и сложения
- С десятичными числами действуем аналогично

Попробуем теперь разложить 120-значное число на множители

- Будем использовать метод пробных делителей. Для нахождения делителей числа N достаточно перебрать пробные делители до корня из N (так как дальше второй возможный делитель станет меньше первого, а такие уже проверялись)
- Наше число примерно равно 10^{120}. Возьмём компьютер, который вычисляет миллиард делений в секунду и посчитаем, сколько он будет работать, чтобы проверить 10^{60} (корень из 10^{120})
- В часе 3600 секунд (то есть не больше 10^4). Значит компьютер будет работать не меньше 10^{56} часов
- В сутках не более 100 часов, а в году не более 1000 суток, значит наш компьютер будет работать не менее 10^{51} лет
- Заметим, что время существования Вселенной оценивается в 10^{11} лет

Какова ситуация с практикой разложения на множители длинных чисел?

- «Установлен рекорд в области вычислительной криптографии. Германские математики решили очередную задачу из списка «Вызовов RSA», – им удалось разложить на множители число длиной 640 бит. Вычислительная сложность задачи лежит в основе главных криптографических алгоритмов с открытым ключом (RSA и Диффи-Хеллмана соответственно), поэтому новые результаты очень важны для оценки стойкости криптосхем, повсеместно применяемых ныне для защиты информации.

  Число RSA-640 было факторизовано сотрудниками BSI, германского Федерального агентства безопасности инфотехнологий. Этой же команде, заметим, принадлежат и несколько предыдущих рекордов – разложение на множители чисел RSA-200 и RSA-576. Для нахождения делителей, как и прежде, применялся традиционный алгоритм числового решета (general number field sieve), а вычисления первого этапа, «просеивания», были организованы на базе распределенной системы компьютеров Боннского университета, Института Макса Планка в Бонне и Института экспериментальной математики в Эссене (три месяца неустанной работы восьмидесяти процессоров Opteron 2,2 ГГц). Второй важный этап алгоритма, «матричный», то есть собственно поиск уникальной пары делителей числа, занял полтора месяца. По условиям конкурса «Вызов RSA», учрежденного американской компанией RSA Security, немцы получат денежный приз в размере 20 тысяч долларов. В списке этого конкурса осталось еще шесть позиций – от RSA-704 до RSA-2048, причем по мере усложнения задачи будет расти и вознаграждение – от 30 до 200 тысяч долларов».

Алгоритм RSA и быстрое возведение в степень

- Основан на возможности быстро возводить число в степень и считать остаток от деления нацело
- $a^{100}=a\cdot a\cdot a\ldots\cdot a$ требует 99 умножений
- Идея быстрого алгоритма:
  $a^{100}=(a^{50})^2 = ((a^{25})^2)^2 = ((a\cdot(a^{12})^2)^2)^2 = ((a\cdot(((a^3)^2)^2)^2)^2)^2$ требует 8 умножений (возведение в квадрат – это тоже умножение)

Алгоритм RSA и теорема Эйлера

- Эйлер обнаружил замечательное свойство остатков некоторых степеней целых чисел
- Обозначим через N количество всех взаимно простых с M чисел, меньших M. Например, если M=10, то N=4 (числа 1, 3, 7, 9 взаимно просты с числом 10)
- Тогда степень любого натурального и взаимно простого с M числа A^N при делении на M даёт остаток 1. Например, 3^4 при делении на 10 даст остаток 1.

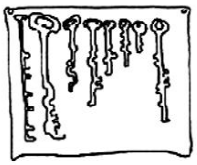
- Шифровка и дешифровка в алгоритме RSA делаются путём возведения в степень и деления нацело числа, кодирующего сообщение:

$$y=x^N \bmod M$$

Открытая и закрытая части шифра RSA

- Код RSA не является симметричным и для расшифровки требуется возводить в другую степень D – это и есть секретная часть кода. Она называется ключом и держится в секрете.

$$y=x^N \bmod M \qquad x=y^D \bmod M$$



- Ключ может быть найден, а шифр «взломан», если «взломщику» удастся разложить число M на множители
- Но в качестве числа M берут произведение двух длинных (около 60 цифр) простых чисел и разложить его на множители не просто

Секретное сообщение и электронная подпись

- Пользоваться шифром RSA можно так. Найти для себя «хорошее» число M, вычислить по нему N и D
- Числа M и N нужно объявить всем желающим писать вам секретные письма. Число D следует держать в секрете
- Посылающий вам письмо зашифрует его так: $y=x^N \bmod M$
- Дешифровать письмо нужно с помощью секретного ключа: $x=y^D \bmod M$. Никто другой письмо не прочитает. Для этого пришлось бы взломать код.

- Наоборот, вы можете использовать формулу $x=y^D \bmod M$ для шифровки сообщения. Тогда дешифровать её сможет любой по формуле $y=x^N \bmod M$
- Зачем это нужно? Чтобы все знали, что это ваше письмо. Чтобы подделать письмо, опять же надо взломать код

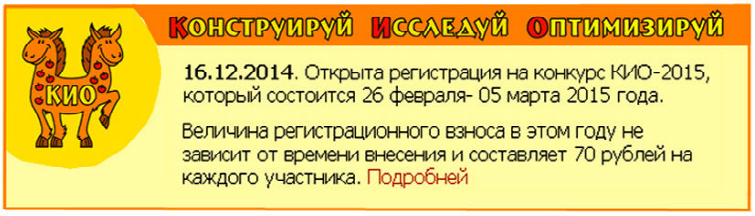
Что такое электронные деньги?

- Электронные деньги – это криптографический протокол, который позволяет посылать электронные письма (счета) в банк с тем, чтобы банк снял со счёта и перевёл другому лицу (продавцу) некоторую сумму денег

- Главное в том, чтобы банк не знал, для кого предназначаются деньги, иначе этот перевод нельзя будет назвать электронными деньгами
- В этом протоколе используется обмен письмами, подписанными электронными подписями, и дополнительная шифровка сообщений (затемняющий множитель)

Как сыграть в орлянку по телефону?

- А это вы должны придумать сами!
- А чтобы больше знать, читайте журнал «Компьютерные инструменты в школе»
- Узнать о новых нерешенных задачах вам поможет олимпиада «Конструируй, исследуй, оптимизируй!»
- Сайт олимпиады: go.kio.spb.ru



Поздняков Сергей Николаевич,
доктор педагогических наук,
профессор кафедры ВМ-2
СПбГЭТУ «ЛЭТИ».

© Наши авторы, 2014.
Our authors, 2014.