Сравнения

$$y^f \equiv x^{ef} \equiv x \pmod{pq}$$

показывают, что для нахождения x достаточно найти остаток от деления y^f на pq. (Числа выбраны так, что $x < pq$. При этом x не кратно ни p, ни q. Не подумайте, что это всерьез нас ограничивает: если p и q – большие числа, то вероятность того, что x нацело разделится на p или q, пренебрежимо мала. Кроме того, можно предусмотреть в алгоритме, чтобы в случае чего сообщение x было автоматически как-то так чуть-чуть изменено, без изменения его смысла, что x и pq станут взаимно просты.)

Почему многие надеются, что шифр RSA является шифром с открытым ключом? Да потому, что числа pq и e можно сделать общедоступными. Тогда зашифровать сообщение сможет любой, у кого есть компьютер (и какая-нибудь программа, позволяющая выполнять действия с многозначными числами). Расшифровать сообщение легко, если мы знаем число f. Но единственный известный ныне способ нахождения числа f требует нахождения чисел p и q, т.е. разложения произведения pq на множители. А эффективных алгоритмов решения этой задачи пока нет (удача 1994 года не в счет: если бы в числах p и q было не 64 и 65, а хотя бы по 300 цифр, то и ресурсов сети Internet не хватило бы!). Впрочем, нет сейчас и доказательства того, что никто никогда не научится быстро (математик сказал бы: «за время, полиномиальное от количества цифр») разлагать числа на простые множители.

Приложение

Как возводить в большую степень?

Чтобы возвести число x в 9007-ю степень, по определению, достаточно выполнить 9006 умножений. Но можно обойтись и меньшим числом операций: вычислить x^2, $\left(x^2\right)^2 = x^4$, $\left(x^4\right)^2 = x^8$,..., $\left(x^{2048}\right)^2 = x^{4096}$, наконец, $\left(x^{4096}\right)^2 = x^{8192}$ и воспользоваться формулой

$$x^{9007} = x \cdot x^2 \cdot x^4 \cdot x^8 \cdot x^{32} \cdot x^{256} \cdot x^{512} \cdot x^{8192},$$

которая основана на том, что в двоичной системе счисления 9007 имеет вид

$$9007_{10} = 10001100101111_2.$$

Понимаете? Мы разложили 9007 в сумму 1 + 2 + 4 + 8 + 32 + + 256 +512 + 8192 и смогли сильно сэкономить: обошлись 13-ю возведениями в квадрат на первом этапе вычислений и 7-ю умножениями на втором этапе. Всего 20 умножений вместо 9006. Огромная экономия! (Для придирчивого читателя отметим, что выше следовало бы говорить не об умножениях, а об умножениях по модулю pq: дабы количество цифр не росло катастрофически, мы всякий раз должны не только перемножать, но и брать остаток от деления на pq. Но сейчас разговор не об этом.)

Преимущества изложенного метода возведения в степень тем нагляднее, чем больше показатель степени. Например, если показатель степени состоит не из четырех цифр, как 9007, а из нескольких десятков или сотен цифр, то наивный способ не то что утомителен, а неосуществим ни на каких, даже самых мощных, компьютерах. А основанный на двоичной системе – работает и в такой ситуации!

Упражнение 43 (М1086). С числом разрешено производить две операции: «увеличить в 2 раза» и «увеличить на 1». За какое наименьшее число операций можно из числа 0 получить число а) 100; б) 9907; в) n, если в двоичной системе счисления n имеет вид $\overline{a_m a_{m-1} \ldots a_1 a_0}$?

Алгоритм Евклида

Алгоритм Евклида – это способ отыскания наибольшего общего делителя, основанный на формуле

$$\text{НОД}(a,b) = \text{НОД}(a - bq,\ b),$$

которая верна для любых целых чисел a, b, q. (Докажите эту формулу!) Подробно о нем рассказано в статье Н.Васильева «Алгоритм Евклида и основная теорема арифметики» (Приложение к журналу «Квант» № 6 за 1998 год). Собственно говоря, нам нужен даже не алгоритм Евклида, а основанный на нем способ решения линейных уравнений.

Итак, даны два взаимно простых числа e и m (в интересовавшем нас случае $m = \varphi(pq)$, но здесь это не важно). Нужно найти такие числа f и k, что

$$ef = 1 + km.$$

Если бы m было не очень большим, то можно было бы выполнить полный перебор всех m остатков. Но если m большое, то перебор нереален. Оказывается, алгоритм Евклида позволяет быстро решать эту задачу.

Чтобы объяснить, как он работает, рассмотрим пример: $e = 9007$, $m = 19876$. (Мы хотели взять сто-с-лишним-значное число m, но в последний момент струсили.) Уравнение

$$9007f = 1 + 19876k$$

можно записать в виде

$$9007f = 1 + 9007 \cdot 2k + 1862k,$$

т.е.

$$9007(f - 2k) = 1 + 1862k.$$

Обозначим $a = f - 2k$. Тогда

$$9007a = 1 + 1862k.$$

Заметьте: получилось уравнение того же типа, что и исходное, только коэффициенты стали меньше. Теперь следующий шаг:

$$1862 \cdot 4a + 1559a = 1 + 1862k,$$

т.е.

$$1559a = 1 + 1862(k - 4a).$$

Обозначим $k - 4a = b$, тогда

$$1559a = 1 + 1862b.$$

Далее,

$$1559(a - b) = 1 + 303b.$$

Обозначив $a - b = c$, получаем уравнение

$$1559c = 1 + 303b.$$

Дальше – так же:

$$44c = 1 + 303(b - 5c),\ \ d = b - 5c,\ \ 44c = 1 + 303d;$$

$$44(c - 6d) = 1 + 39d,\ \ x = c - 6d,\ \ 44x = 1 + 39d;$$

$$5x = 1 + 39(d - x),\ \ y = d - x,\ \ 5x = 1 + 39y.$$

Машина продолжила бы вычисления дальше, пока коэффициент при одной из неизвестных не стал бы равен 1. А мы остановимся уже здесь: очевидно, $x = 8$, $y = 1$ – одно из решений

(*Окончание см. на с. 37*)