5 Последняя теорема Ферма

Задача. Виктор утверждает что найденное Уайлсом доказательство последней теоремы Ферма содержит ошибку. Виктор присылает в журнал Selanna показатель $n > 2$, для которого он знает (?) решение уравнение $x^n + y^n = z^n$ в натуральных числах. Трент просит Виктора предъявить решение. Но Виктор отказывается это сделать, предлагая Тренту сначала анонсировать его открытие. Трент находится в затруднительном положении. Предложите криптографический протокол, который, с одной стороны, доказывал бы Тренту, что Виктор действительно знает решение, и, с другой стороны, не раскрывал бы это решение.

Решение. В нашем распоряжении оказалось следующее письмо. Публикуем его по разрешению Трента.

Уважаемый Виктор,

Предлагаю следующий протокол.

1. *Я выбираю различные большие простые p и q так, что n и $(p-1)(q-1)$ взаимно просты. Я отправляю Вам модуль $N = pq$.*
2. *Вы выбираете случайное $d \in \{1, 2, \ldots, N-1\}$ и отправляете мне замаскированное решение $X = dx \bmod N$, $Y = dy \bmod N$, $Z = dz \bmod N$. Если одно из полученных чисел X, Y, Z совпадает с 0, то Вы генерируете другое d или предлагаете мне выслать другой модуль N.*
3. *Я проверяю, что $X, Y, Z \neq 0$ и что $X^n + Y^n \equiv Z^n \pmod N$.*

Данный протокол обладает следующими свойствами.

Полнота. *По известному решению (x, y, z) Вы без труда сможете найти подходящую тройку (X, Y, Z).*

Корректность. *Нахождение подходящей тройки (X, Y, Z) без знания (x, y, z) представляется непростой задачей. Можно выбрать два элемента тройки, например X и Y, и определить Z как корень n-й степени из $X^n + Y^n$ по модулю N. Но извлечение корней по составному модулю при неизвестной факторизации модуля является трудной вычислительной задачей. На этой задаче базируется знаменитая криптосистема RSA. Возможно, существуют более простые способы нахождения (X, Y, Z), но они мне неизвестны.*

Важно, что кооординаты решения должны быть ненулевыми. Если снять это требование, то можно построить тривиальные решения, например $\{X = Z, Y = 0\}$.

Модуль N может оказаться не взаимно прост с x, y, z или d. В этом случае Вы получаете факторизацию N и предыдущие аргументы о корректности протокола не действуют. Но возможностью факторизации N можно пренебречь, потребовав, чтобы p и q были достаточно велики.

Неразглашение. *Важно не разгласить любое решение уравнения Ферма, в том числе решение (dx, dy, dz). Вы предъявляете остатки от деления компонент этого решения на N. Я не вижу эффективного способа определения исходного решения по остаткам.*

Приведенные аргументы не выглядят до конца исчерпывающими. Если у Вас есть возражения — давайте их обсудим. В противном случае предлагаю действовать по описанному протоколу.

С наилучшими пожеланиями, Трент.

Насколько нам известно, Виктор с Трентом больше не связывался. □