42 QuadDH

Задача. Пусть G — циклическая группа большого простого порядка. Трент разработал алгоритм `QuadDH`, который по образующему g группы G и ее элементу g^x находит g^{x^4}. Виктор всеми силами пытается заполучить описание алгоритма. Виктор считает, что с его помощью он сможет атаковать протокол Диффи — Хеллмана: по (g, g^x, g^y) находить g^{xy}. Восстановите ход рассуждений Виктора.

Решение. Пусть q — порядок группы G. Элемент $h \in G$ можно возвести в степень $e \in \{1, 2, \ldots, q-1\}$ менее чем за $2\log_2 q$ умножений в G, если использовать схему «возвести в квадрат – умножить». В частности, по этой схеме можно вычислить обратный к h элемент $h^{-1} = h^{q-1}$.

С помощью `QuadDH` можно найти

$$g^{(x+1)^4} = \texttt{QuadDH}(g^x \cdot g) \quad \text{и} \quad g^{(x-1)^4} = \texttt{QuadDH}(g^x \cdot g^{-1}),$$

затем определить

$$g^{8(x^4+x)} = g^{(x+1)^4} \cdot \left(g^{(x-1)^4}\right)^{-1}$$

и наконец

$$g^{x^3} = \left(g^{8(x^4+x)}\right)^{8^{-1}} \cdot g^{-x}$$

(вычисления в показателях ведутся по модулю q).

Фактически мы построили алгоритм `TripleDH`, который за два обращения к `QuadDH` и за полиномиальное (от $\log q$) число умножений в G находит g^{x^3} по (g, g^x).

С помощью `TripleDH` можно построить алгоритм `SqDH`:

$$g^{x^2} = g^{6^{-1}\left((x+1)^3-(x-1)^3-2\right)}.$$

Наконец, с помощью `SqDH` можно атаковать протокол:

$$g^{xy} = g^{2^{-1}\left((x+y)^2-x^2-y^2\right)}.$$

□

Обсуждение. Наш читатель `mathematic_by` предложил сразу строить `SqDH` по `QuadDH`, используя тождество

$$(x+1)^4 + (x-1)^4 = 2x^4 + 12x^2 + 2.$$