47 DH-d

Задача. Пусть G — циклическая группа большого простого порядка q. Трент разработал машину `DH-d`, которая по образующему g группы G и ее элементу g^x находит g^{x^d}. Здесь d — небольшое натуральное число. Как с помощью машины `DH-d` решить задачу Диффи — Хеллмана: по (g, g^x, g^y) найти g^{xy}? Предложите решение с минимальным числом обращений к машине.

Решение. Элемент $[x] = g^x$ назовем неявным представлением $x \in \mathbb{F}_q$. Неявные представления можно складывать с помощью умножения в G:

$$[x + y] = g^x g^y = [x][y].$$

Более того, если x задано явно, то

$$[xy] = g^{xy} = [y]^x$$

(возведение в степень можно выполнить за полиномиальное от $\log q$ число умножений в G). В частности,

$$[x^d] = [x]^{x^{d-1} \bmod q}, \quad [x^{-1}] = [x]^{x^{q-3} \bmod q}.$$

Умножение $[xy]$ не сводится к вычислениям в G если и x, и y заданы неявно. Задача Диффи — Хеллмана как раз состоит в определении $[xy]$ по тройке $([1], [x], [y])$.

Машина `DH-d` вычисляет $[x^d]$ по $([1], [x])$. Следующий алгоритм, назовем его `SqDH`, позволяет за $d - 1$ обращение к машине найти $[x^2]$ по $([1], [x])$:

1. Для $a = 0, 1, \ldots, d-2$ вычислить

$$b_a = \texttt{DH-d}([1], [x][a]) = [(x+a)^d] = \left[\sum_{i=0}^{d} \binom{d}{i} a^i x^{d-i}\right] = b_0 \left[\sum_{i=1}^{d-2} \binom{d}{i} a^i x^{d-i}\right] [x]^{da^{d-1}} \left[a^d\right].$$

2. Составить систему уравнений

$$\left[\sum_{i=1}^{d-2} \binom{d}{i} a^i t_{d-i}\right] = \frac{b_a}{b_0 [x]^{da^{d-1}} [a^d]}, \quad a = 1, \ldots, d-2,$$

   и решить ее относительно $[t_2], \ldots, [t_{d-1}]$. Решить систему можно методом Гаусса, выполняя манипуляции с неявными представлениями элементов $\mathbb{F}_q$ по описанным выше правилам. Матрица системы имеет вид

$$M = (m_{ai}) = \left(\binom{d}{i} a^i\right), \quad a = 1, 2, \ldots, d-2, \quad i = 2, \ldots, d-1.$$

   Матрица обратима (над $\mathbb{F}_q$), поскольку делением строк на a^2 и столбцов на биномиальные коэффициенты она приводится к матрице Вандермонда (a^{i-2}). Таким образом, система уравнений будет иметь единственное решение и в этом решении $[t_i] = [x^i]$.

3. Возвратить $[t_2]$.

Решение задачи Диффи — Хеллмана можно найти с помощью двух обращений к `SqDH`, т. е. $2(d-1)$ обращений к `DH-d`:

$$[xy] = [4^{-1}((x+y)^2 - (x-y)^2)].$$

□

Комментарий. Развитие задачи QuadDH (см. `http://apmi.bsu.by/resources/tasks.html#42`). Сокращение числа обращений к `DH-d` подсказано участниками олимпиады NSUCRYPTO-2015. Остается открытым вопрос, можно ли затратить $< 2(d-1)$ обращений.