30 Централизованное тестирование

Задача. Трент поручил Алисе провести среди студентов тестирование по алгебре. Алиса придумала очень сложную задачу, в которой требуется найти многочлен $f(x)$ положительной степени с целыми коэффициентами. Боб предложил Алисе организовать проверку решения самими студентами. Боб написал программу, которая сравнивает найденное решение с искомым многочленом $f(x)$, внедренным в код программы. Алиса против проверяющей программы. Алиса опасается, что студент Виктор дизассемблирует код и восстановит $f(x)$, не решая задачу. Помогите Бобу переписать программу так, чтобы восстановить по ней $f(x)$ было вычислительно трудно.

Решение. Идея задачи принадлежит А. Маслову.

Пусть d — степень многочлена f, увеличенная на 1. Боб может выбрать различные целые $x_1, \ldots, x_d$ и найти соответствующие $y_1 = f(x_1), \ldots, y_d = f(x_d)$. Если для проверяемого многочлена h выполняется

$$h(x_i) = y_i, \quad i = 1, 2, \ldots, d,$$

то $h = f$, т. е. решение верное.

Если Боб явно задаст числа x_i, y_i в программе, то Виктор их восстановит и определит f как интерполяционный многочлен Лагранжа. Поэтому Бобу следует задать числа неявно.

Боб может выбрать циклическую группу G большого порядка q, в которой задача дискретного логарифмирования является трудной. Боб указывает в программе элементы

$$g^{x_i}, g^{x_i^2}, \ldots g^{x_i^d}, g^{y_i}.$$

По этим элементам вычислительно трудно найти x_i, y_i, но можно легко проверить решение задачи.

Для проверки решения $h(x) = a_d x^d + \ldots + a_1 x + a_0$ следует вычислить элемент

$$g^{a_0} \left(g^{x_i}\right)^{a_1} \ldots \left(g^{x_i^d}\right)^{a_d}$$

и сравнить его с g^{y_i}. Равенство означает, что $h(x_i) \equiv y_i \pmod{q}$. Отсюда, вообще говоря, не следует, что $h(x_i) = y_i$. Чтобы повысить гарантии Боб может использовать не одну, а несколько групп G различных порядков q. □