25 PIN, PIN, PIN,...

Задача. У Боба все больше пластиковых карточек. Для каждой карточки требуется помнить PIN-код — число x от 0 до 9999. Как обычно, при трех попытках ввода неверного PIN карточка блокируется. Боб не может запомнить x наверняка. Тем не менее, при предъявлении 7 или 8 PIN-кодов конкретной карточки Боб всегда может выбрать из них тройку, в которой обязательно окажется x. Боб решил действовать следующим образом:

1. Выбирается ключ k — натуральное число. Ключ записывается в очень защищенный блокнот.

2. PIN x зашифровывается, ему ставится в соответствие число $y = (x+1)^k \bmod 10009$. Шифртекст y сохраняется в другом, не очень защищенном блокноте.

Боб хочет организовать все так, чтобы каждому y соответствовало 7 или 8 вариантов x. Тогда Боб сможет отобрать три из них, включая правильный, и наверняка пройти аутентификацию с трех попыток. А вот Виктору, даже если он завладел двумя блокнотами, придется проверять не менее 7 вариантов. Как Боб должен выбирать k и как должно быть организовано расшифрование y?

Решение. Число $p = 10009$ простое, а $p - 1 = 2^3 \cdot 3^2 \cdot 139$.

Ключ k должен выбираться так, что НОД$(k, p-1) = 8$. Прямые расчеты показывают, что для всех таких k выполняется:

$$z^k \not\equiv \tilde{z}^k \pmod{p}$$

для любых различных $z, \tilde{z} \in \{10001, \ldots, 10008\}$. Поэтому результат зашифрования допустимого PIN-кода $x \in \{0, 1, \ldots, 9999\}$ может совпадать с (воображаемым) результатом зашифрования *только одного* недопустимого PIN-кода $\tilde{x} \in \{10000, 10001, \ldots, 10008\}$.

Определить x по $y = (x+1)^k \bmod p$ можно следующим образом:

1. Представить k в виде $8l$, где НОД$(l, p-1) = 1$.

2. Найти $z = y^{l^{-1} \bmod p-1} = (x+1)^8 \bmod p$.

3. Применить алгоритм Тонелли — Шенкса и найти квадратные корни из z по модулю p. Пусть z_1, z_2 — найденные корни.

4. Снова применить алгоритм Тонелли — Шенкса и найти квадратные корни из z_1, z_2. Пусть z_3, z_4, z_5, z_6 — новые корни.

5. Наконец, еще раз применить алгоритм Тонелли — Шенкса и найти квадратные корни из z_3, z_4, z_5, z_6. Пусть $x_1, x_2, \ldots, x_8$ — окончательные корни. Фактически это корни 8-й степени из z по модулю p.

6. Возвратить $(x_i - 1) \bmod p$, $i = 1, 2, \ldots, 8$.

□

Спасибо В. Палухе за ценные замечания.