3 Временной замок

Задача. Боб передает Алисе ключ K так, чтобы им можно было воспользоваться не сразу, а по истечении определенного времени. Для этого Боб выбрал простое $p = 2^{128} - 159$ и в течение месяца рассчитывал последовательность Фибоначчи по модулю p:

$$F_0 = 0, \quad F_1 = 1, \quad F_n = (F_{n-1} + F_{n-2}) \bmod p, \quad n = 2, 3, \ldots, 2^{64} - 1.$$

Последний элемент последовательности Боб использовал в качестве ключа: $K = F_{2^{64}-1}$. Компьютеры Алисы уступают компьютерам Боба и поэтому Боб считает, что для определения ключа Алисе потребуется не меньше месяца. Помогите Алисе найти ключ K раньше.

Решение. Будем использовать многочлены над полем из p элементов. При сложении, умножении и делении таких многочленов операции с их коэффициентами будем выполнять по модулю p.

Пусть $f_n(x) = a_n + b_n x$ — остаток от деления многочлена x^{n+1} на многочлен $x^2 - x - 1$. Имеем:

$$f_0(x) = 0 + 1 \cdot x, \quad f_1(x) = 1 + 1 \cdot x, \quad f_2(x) = 1 + 2 \cdot x, \quad f_3(x) = 2 + 3 \cdot x, \ldots$$

и вообще для $n \geq 1$:

$$f_n(x) = x f_{n-1}(x) \bmod (x^2 - x - 1) = b_{n-1} + ((a_{n-1} + b_{n-1}) \bmod p)x.$$

Отсюда следует, что $a_n = F_n$, $b_n = F_{n+1}$. Поэтому для определения K достаточно найти свободный член многочлена $x^{2^{64}} \bmod (x^2 - x - 1)$. Для этого можно воспользоваться следующим алгоритмом:

1. Установить $f(x) \leftarrow x$.
2. Для $i = 1, 2, \ldots, 64$ выполнить: $f(x) \leftarrow f(x)^2 \bmod (x^2 - x - 1)$.
3. Возвратить свободный член $f(x)$.

Выполнив алгоритм (например в системе компьютерной алгебры `Mathematica`), находим

$$K = 137973196247803287452671646795669768529$$

(или `67CCABC7CFFD05DBDEEC654ABB5D0951` в шестнадцатеричной системе счисления).

Интересно, что период последовательности (F_n) составляет $2(p+1)$. Период можно найти как порядок неприводимого над полем из p элементов многочлена $x^2 - x - 1$. Подробнее см. [Лиддл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988]. □