

F. RECOVER SECRET KEY

PROBLEM DESCRIPTION

$$f(x) = k + a_1x + a_2x^2 + \cdots + a_{m-1}x^{m-1} \pmod{p}$$

給 n 組數對 (x_i, y_i) ，求常數 k 。

SOLUTION TECHINQUES

數學 / 高斯消去法

SOLUTION SKETCHES

高斯消去法。

我們可以證明，對於任兩數對：

$$y_i = k + a_1x_i + a_2x_i^2 + \cdots + a_{m-1}x_i^{m-1} \pmod{p}$$

$$y_j = k + a_1x_j + a_2x_j^2 + \cdots + a_{m-1}x_j^{m-1} \pmod{p}$$

可以推得：

$$y_i - ly_j = (k - lk) + a_1(x_i - lx_j) + a_2(x_i - lx_j)^2 + \cdots + a_{m-1}(x_i - lx_j)^{m-1} \pmod{p}$$

因此我們可以使用高斯消去法消去 $a_1 \sim a_{m-1}$ ，最後得到 k 。

TIME COMPLEXITY

每筆測資 $O(N^3)$ ， N 為數對的數量。

SOLUTION PROGRAM FOR REFERENCE

None due to live contest.