BabyDH 1

The following text is generated by ChatGPT

This question mainly tests the participants' abilities in reading academic papers and programming. It requires participants to have a certain understanding of lattice reduction algorithms and the Coppersmith method.

Description

The server simulates a DH key exchange between Alice and Bob, and we have obtained their public keys. Subsequently, as a third party, we can engage in a DH exchange with Alice and provide an additional Oracle that can leak the low-order bits of the x and y coordinates of the point negotiated between us and Alice. We need to reconstruct the complete coordinates of this point.

Solution

Based on the information provided in the question, we can construct the polynomial

$$f(x, y) = (My + y')^2 - ((Mx + x')^3 + a(Mx + x') + b)$$

, where x', y' are the leaked values, and $M = 2^{211}$.

We can use the Coppersmith method to find the small roots of this polynomial. The expected solution method involves adjusting the construction proposed by Jochemsz and May. However, relevant research has already been published in similar scenarios. Therefore, we only need to reproduce the construction outlined in the referenced paper to solve this problem.

Given the short time limit for this question, we can use the flatter tool to perform rapid lattice reduction. It has been observed that setting parameters m = 7, t = 1 . On a single-core Ubuntu virtual machine, takes approximately 25 seconds with a probability of completing the solution.