Escola Politècnica Superior **Universitat de Lleida**
Grau en Enginyeria Informàtica

Computational tools for problem solving

Lab list 5

Baby Step Giant Step Algorithm for the Discrete Logarithm Problem.

This assignment is about Shanks' baby step–giant step algorithm (BSGS) for computing discrete logarithms in the multiplicative group $\mathbb{Z}_p^*$ of a prime field. This group is cyclic of order $p-1$ and has generator g given by a primitive root modulo p: $\mathbb{Z}_p^* = \langle g \rangle$.

The discrete logarithm problem (DLP) in $\mathbb{Z}_p^*$ with generator g, consists of finding for a given $y \in \mathbb{Z}_p^*$, an integer $x \in \{0, \ldots, p-2\}$, denoted $\log_g(y)$, such that

$$y = g^x.$$

The BSGS algorithm is a meet-in-the-middle algorithm that computes x as $x = is - j$, where s is the integer $\lceil \sqrt{p} \rceil$ and $i, j \in \{0, \ldots, s\}$ are such that there is a match (collision) between both sides of the equivalent formulation $yg^j = g^{is}$. The left hand side is called the baby step side while the right hand side is the giant step side.

Example.

DL instance: Solve $2 = 10^x \bmod 19$.

BSGS solution:

i) $\mathbb{Z}_p^* = \{1, 2, \ldots, 18\}$ and $g = 10$ is generator since its order is the highest possible.

ii) Compute $s = \lceil \sqrt{19} \rceil = 5$.

iii) Compute the baby step set and giant step set

$$BS = \{(2 \cdot 10^j, j) : 0 \leq j \leq s\} = \{(2,0), (1,1), (10,2), (5,3), (12,4), (6,5)\}$$

$$GS = \{(10^{5i}, i) : 0 \leq i \leq s\} = \{(1,0), (3,1), (9,2), (8,3), (5,4), (15,5)\}\}$$

iv) A match of 5 is obtained for $(i, j) = (4, 3)$, then we have $x = 4 \cdot 5 - 3 = 17$.

Problem.

1) Write a code to compute discrete logarithms using BSGS.

2) Solve $3^x \equiv 12 \pmod{29}$, $13^x \equiv 19 \pmod{71}$ and $7^x \equiv 50 \pmod{143}$.