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

Computational tools for problem solving

Lab list 7

Baby Step Giant Step Algorithm for the Discrete Logarithm Problem

This coding exercise consists in an implementation of Shank's Baby Step – Giant Step algorithm (BSGS) for the computation of Discrete Logarithms in a (multiplicative) cyclic group $\mathbb{Z}_p^*$. This group has order $p-1$ and a (multiplicative) generator g is given by a primitive root modulo p: $\mathbb{Z}_p^* = \langle g \rangle$.
The Discrete Logarithm problem $\log(y)$ in $\mathbb{Z}_p^*$ with given generator g is to find the solution the solution $x \in \{1, \ldots, n\}$ of

$$y = g^x.$$

The BSGS algorithm is a meet-in-the-middle algorithm that computes x as $x = is - j$ by finding a match in each hand side of the equivalent formulation $yg^j = g^{is}$, where s is an integer near $\sqrt{p}$. The left hand side is the Baby Steps, and the r.h.s. is the Giant Steps.

Example:

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

BSGS solution:

i) $\mathbb{Z}_{19} = \{0, 1, 2, \ldots, 18\}$,

$$\mathbb{Z}_{19}^* = \{1, 2, \ldots, 18\},$$

$g = 10$ since the (multiplicative) order of 10 $\pmod{19}$ is the highest possible value $18 = \varphi(19)$.

ii) Since $\sqrt{19} \sim 5$, set $s = 5$ and let i, j run in $0, \ldots, 5$.

iii) Compute the lists L1: $(2 \cdot 10^j \mod 19, j)$ and L2: $(10^{5i} \mod 19, 5i)$:

$$\begin{array}{lllllll} L1: & (1,0) & (3,5) & (9,10) & (8,15) & (5,20) & (15,25) \\ L2: & (2,0) & (1,1) & (10,2) & (5,3) & (12,4) & (6,5) \end{array}$$

iv) Since the match happens when the 1st position equals to 5, then $x = 20 - 3 = 17$.

Problem 1.

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

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