Cryptography

JOACHIM VON ZUR GATHEN, JÉRÉMIE DETREY

4. Tutorial: Discrete logarithms

Exercise 4.1 (Exponentiation).

Given a group $(G, \diamond)$, where $\diamond$ denotes the group law operating on G, we take an element $g \in G$ of order ℓ.

We define the exponentiation of g over G with respect to the $\diamond$ operation as the map

$$\begin{array}{rccc} \exp_g : & \mathbb{Z} & \longrightarrow & G \\ & x & \longmapsto & g^x = \underbrace{g \diamond g \diamond \ldots \diamond g}_{x \text{ times}}. \end{array}$$

(i) Show that we can also see it as a map

$$\begin{array}{rccc} \exp_g : & \mathbb{Z}_\ell & \longrightarrow & G \\ & x & \longmapsto & g^x. \end{array}$$

Exercise 4.2 (Discrete logarithm in $\mathbb{Z}_n$).

We consider here the additive group $(\mathbb{Z}_n, +)$, where n is a positive integer.

(i) Given an element $g \in \mathbb{Z}_n$, define the map $\exp_g$ over $\mathbb{Z}_n$.

Take $n = 42$ and $g = 5$.

(ii) What is the additive order of g?

(iii) What is the discrete logarithm of 1 in base g? Namely, find an integer x such that $\exp_5(x) = 1$ in $\mathbb{Z}_{42}$.

(iv) Find a general way to compute discrete logarithms over $\mathbb{Z}_n$. Restrict yourselves to the case when g is coprime to n.

(v) Would $\mathbb{Z}_n$ be a wise choice for implementing the Diffie-Hellman key exchange?

Exercise 4.3 (Discrete logarithm in $\mathbb{Z}_n^\times$).

We now consider the multiplicative subgroup $(\mathbb{Z}_n^\times, \times)$ of integers modulo a positive integer n.

(i) Compute the discrete logarithm in base 2 of 3 in $\mathbb{Z}_{13}^\times$.

(ii) Same question in $\mathbb{Z}_{23}^\times$.

(iii) What is the discrete logarithm in base 2 of 3 in $\mathbb{Z}_{299}^\times$?
Hint: $299 = 13 \times 23$.