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

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

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

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

Solution. We take an integer $x \in \mathbb{Z}$, and write x as $x' + k \cdot \ell$, where $x' \in \mathbb{Z}_\ell$. Since the order of g is ℓ, we have

$$\exp_g(x) = g^x = g^{x'+k\cdot\ell} = g^{x'} \diamond g^{k\cdot\ell} = g^{x'} \diamond 1_G = g^{x'} = \exp_g(x').$$

We can then restrict ourselves to exponents modulo ℓ. ○

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 $\mathbb{Z}_n$.

Solution. $\exp_g$ is simply the integer multiplication modulo n:

$$\exp_g : x \longmapsto x \cdot g \bmod n.$$

○

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

(ii) What is the additive order of g?

Solution. The order of g is 42, since 5 is coprime to 42. ○

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

Solution. $\log_5(1) = 17$, as $17 \cdot 5 \equiv 1 \pmod{42}$. ○

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

Solution. Since g is coprime to n, we can compute g^{-1}, the multiplicative inverse of g modulo n. Then, since $\exp_g(x) = x \cdot g$, we have $\log_g(y) = y \cdot g^{-1} = \exp_{g^{-1}}(y)$.

This corresponds to a change of base: 1 is another generator of $\mathbb{Z}_n$, and moreover $\log_1(y) = y$. We can then write

$$\log_g(y) = \log_g(1) \cdot \log_1(y) = \log_g(1) \cdot y.$$

And since $\log_g(1) \cdot g \equiv 1 \pmod{n}$, we have that $\log_g(1) = g^{-1}$. ○

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

Solution. Obviously not, since we can easily break the discrete logarithm problem over such groups. ○

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 $\mathbb{Z}_{13}^\times$.

Solution. $2^4 = 16 \equiv 3 \pmod{13}$, hence $\log_2(3) = 4$. ○

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

Solution. $2^8 = 256 \equiv 3 \pmod{23}$, hence $\log_2(3) = 8$. ○

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

Solution. We are looking for an x such that $2^x \equiv 3 \pmod{299}$. Equivalently, we want $2^x \equiv 3 \pmod{13}$ and $2^x \equiv 3 \pmod{23}$. So $x \equiv 4 \pmod{12}$ and $x \equiv 8 \pmod{22}$, which gives $x = 52$.

We can check that $x^{52} \equiv 3 \pmod{299}$.