Topics in Algebra: Cryptography - Blatt 3

11.30-12:15, Seminarraum 9, Oskar-Morgenstern-Platz 1, 2.Stock

http://www.mat.univie.ac.at/~gagt/crypto2018

Goulnara Arzhantseva
goulnara.arzhantseva@univie.ac.at

Martin Finn-Sell
martin.finn-sell@univie.ac.at

1 Test questions from the lecture to refresh:

Question 1. Give a proof of Theorem 2 from the Annex notes for Chapter 2.

2 Exercises

Question 2. Suppose that $p > 3$ is an odd prime, and $a, b \in \mathbb{Z}_p$. Further, suppose that the equation $x^3 + ax + b = 0 (\mathrm{mod} p)$ has three distinct solutions in $\mathbb{Z}_p$. Prove that the corresponding elliptic curve group $(E, +)$ is not a cyclic group. (Hint: Consider the subgroup of elements of order 2.)

Question 3. Suppose that E is an elliptic curve defined over $\mathbb{Z}_p$, where $p > 3$ is prime. Suppose also that $|E|$ is a prime, $P \in E$ and $P \neq \mathcal{O}$.

i) Prove that the discrete logarithm $\log_P(-P) = |E| - 1$;

ii) Describe how to compute $|E|$ in $O(p^{\frac{1}{4}})$ time using Hasse's bound on $|E|$ together with a modification of Shank's algorithm.