Fachbereich Mathematik
Elena Klimenko

WS 2017/18
Homework 7

NUMBER THEORY AND CRYPTOGRAPHY

Due in class on Friday, December 8th, at 12:05 pm.

Use each of the following methods to solve the same discrete logarithm problem

$$5^x \equiv 76 \pmod{97}.$$

(Show all work including all intermediate steps.)

1. The Pohlig–Hellman algorithm.

2. The index calculus method.

3. Shanks' babystep–giantstep algorithm.

4. Pollard's ρ algorithm.