PUBLIC KEY CRYPTOGRAPHY

Lab 1 (Weeks 1-2)

All programs will be written in versions of C or Python with commented code.

Topic: greatest common divisor.

- Implement 3 different algorithms for computing the greatest common divisor of 2 natural numbers. One of the algorithms should work for numbers of arbitrary size!

  Perform a comparative running-time analysis of these algorithms for a set of at least 10 inputs (use appropriate time units in order to differentiate the algorithms).

Points

- **1 point** if handed in by Week 3 (odd week groups) or Week 4 (even week groups).
- **0.5 points** if handed in by Week 5 (odd week groups) or Week 6 (even week groups).

Note: *Each student will keep her/his semigroup for the lab throughout the semester! Taking and presenting labs in weeks with a changed parity may only be done in exceptional cases, if the teaching assistant agrees with it and if time allows.*