PUBLIC KEY CRYPTOGRAPHY

Lab 3 (Weeks 5-8)

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

Topics: modern primality and factorization.

- Implement one of the following algorithms, which will be assigned to you during the labs:

  1. Miller-Rabin algorithm. It will work for numbers of arbitrary size.

  2. Pollard's ρ algorithm. The implicit function will be $f(x) = x^2 + 1$, but it will also allow the use of a function f given by the user.

  3. Generalized Fermat's algorithm. It will first consider $k = 1$. If not successful, then it will consider $k = 2, 3, \ldots$ until getting a factor.

  4. Pollard's $p - 1$ algorithm. It will have an implicit bound B, but it will also allow the use of a bound B given by the user.

Points

- **1 point** if handed in by Weak 9 (odd week groups) or Weak 10 (even week groups).
- **0.5 points** if handed in by Weak 11 (odd week groups) or Weak 12 (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.*