ECE4750J

Introduction to Cryptography

Rust Warmup and GMP

Instructor: Manuel Charlemagne

Binhao Qin — UM-JI (Summer 2024)

Goals:

- Get familiar with programming in Rust
- Get familiar with Rust build system, `cargo`
- Implement extended Euclidean algorithm using GNU Multi-Precision (GMP) arithmetic library

1 Rust Warmup

1. Read chapters 1-4, 6.1-2, 8.1-2, 9-11, and 13 of the Rust book.
2. Complete the Rust warmup exercise.

2 Extended Euclidean Algorithm

1. Get an environment with GMP installed:
   - Install the GNU Multi Precision Arithmetic Library (GMP) from https://gmplib.org/ or its fork MPIR available at https://mpir.org/. Note that MPIR has a better support for Windows, although no binaries are officially provided. GMP is available on any modern Linux distribution.
   - Or, use the `Dockerfile` provided. It has all of the software needed for this course.
2. Create a new Rust package of type library, implement the extended Euclidean algorithm. (Hint: Check out `rug`, a Rust package for calling GMP functions)
3. Write a test that generates 2 random integer, and compares the result of the extended Euclidean algorithm you just implemented to the result of the library function.
4. Run `cargo test` to demonstrate that your implementation passes the test.