ECE4750J

Introduction to Cryptography

Rust Warmup and GMP

Instructor: Manuel Charlemagne
Binhao Qin — UM-JI (Summer 2024)

Goals:

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

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. 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.