General Guidelines on Browsing the Source Code

Ajeesh T Vijayan
MSc Cryptography
London Metropolitan University

January 12, 2024

Notes

This document describes how to browse the code developed as part of the Number Theory assignment.

1. Assignment answer sheets are named as:
   - ajeesh_msc_crypto_ass1.pdf,
   - ajeesh_msc_crypto_ass2.pdf,
   - ajeesh_msc_crypto_ass2.pdf
2. "src" directory contains the source code. "main.rs" is where the all the control flow starts
   - primality.rs contains all primality related code,
   - groups_modulo.rs has all the primitive roots related code,
   - quadratic_sieve.rs contains the method to print the matrix for linear dependency calc.
   - prime_factors.rs contains code for prime factoring. It import methods from primality.rs
   - logarithms.rs contains the code for Pollards Rho method
   - presets.rs is a wrapper module for many of the methods in the above file. For example, when we need factorisation for a range of numbers, we write a wrapper in presets.rs which calls methods from primality.rs and prime_factors.rs in loop
   - utils.rs contains code for modular exponentiation, gcd calc, etc.
   - cli_ops defines the command line options
3. "notes" directory contains all the "latex" files.
4. "results" directory has some sample json files from code execution.
5. nt-assignments.exe is the executable file