2WF90 Algebra for Security

Software Assignments Overview and Guideline

2023 – 2024

Andreas Hülsing
Responsible Lecturer
`a.t.huelsing@tue.nl`

Benne de Weger
Lecturer
`b.m.m.d.weger@tue.nl`

Matthias Meijers
Teaching Assistant
`m.c.f.h.p.meijers@tue.nl`

October 5, 2023

Table of Contents

1 Introduction

On top of the weekly homework exercises, this course comprises two software assignments. In these assignments, you are asked to construct software that implements some of the material covered in the course. On a high level, the first assignment concerns implementing a certain set of operations on "arbitrarily" large integer values;[1] the second assignment concerns implementing a certain set of operations on polynomials with integer coefficients.

The first assignment starts at the very beginning of the course and runs up until and including 25/09/2023; this assignment counts for 7.5% of your final grade. The second assignment starts on the day after the deadline of the first (i.e, 26/09/2023) and runs up until and including 27/10/2023; this assignment counts for 12.5% of your final grade. Table 1 provides an overview of the deadlines and weights of the software assignments.

Software Assignment	**Deadline**	**Weight**
1 (Integer and Modular Arithmetic)	25/09/2023 23:59 (CEST)	7.5%
2 (Polynomial and Finite Field Arithmetic)	27/10/2023 23:59 (CEST)	12.5%

Table 1: Overview of Deadlines and Weights of Software Assignments

Although each assignment has its own description (that becomes available when the assignment starts), a general guideline applies to both assignments; this guideline is described in Section 2. You are expected to follow this guideline in both assignments; failure to do so may result in a loss of points.

Following the description of the guideline, Section 3 details the grading process for both assignments. Finally, Section 4 provides information regarding whom to contact for what kinds of questions in what manner at which time.

[1] The values are not actually arbitrarily large, but can have values corresponding to several hundred decimal digits.

2 Guideline

As above-mentioned, this section describes a general guideline that is applicable to both software assignments of the course. You are expected to follow this guideline in both assignments; failure to do so may result in a loss of points.

The guideline essentially consists of a list of points that you should take into consideration when carrying out the assignments. For clarity, this list is divided into two different categories: process and deliverables. Each of the ensuing subsections goes over one of these categories.

2.1 Process

- The assignment is carried out/submitted in groups; these groups are the same as the groups that are used for doing/submitting homework.
- The work you submit should be entirely your own. However, if you provide proper references, you may use results from the lecture material and/or literature.
- Every group member should contribute a fair share of work.
- Ensure you submit your work before the relevant deadline. Deadlines are strictly enforced; that is, any work submitted after the relevant deadline will not be taken into consideration (and graded with a 0).

2.2 Deliverables

For both software assignments, the deliverables comprise two parts: software and documentation. The guidelines for these deliverables are presented below.

2.2.1 Software

- The software deliverables consist of source code written in Python 3, preferably one of the stable versions of 3.9 or 3.10.[2] Refer to https://realpython.com/installing-python for a tutorial on the installation and setup of Python 3 on most popular operating systems (including Windows, Linux, and macOS).
- The submitted software should run under the interpreter corresponding to the version of Python 3 in which the source code is (claimed to be) written.
- The submitted source code may only use libraries that are explicitly permitted in the relevant assignment description. In case you really want to use other libraries, ask permission to do so by sending an e-mail to m.c.f.h.p.meijers@tue.nl; in this e-mail, clearly state the reason(s) for using the libraries. Naturally, any libraries that make the assignment significantly easier will immediately be rejected.

[2] See https://www.python.org/downloads/source for a list of stable versions.

- The submitted source code should adhere to the rules and restrictions imposed by the relevant assignment description.
- The submitted source code should be commented in such a way that a reviewer with some (i.e., not much) Python knowledge can understand the source code and navigate through it with relative ease.

2.2.2 Documentation

- The documentation of each assignment must be submitted in a single PDF file.
- The use of LaTeX in the construction of the documentation is encouraged.
- The submitted documentation should be written in proper English. It does not matter whether you use American English or British English, as long as you are consistent in the use of one of the two.
- The submitted documentation should be well-structured and well-formatted. For example, the documentation should be logically divided into sections and subsections, tables and listings should be properly formatted and positioned, et cetera.
- The submitted documentation should satisfy the requirements defined in the relevant assignment description.
- The submitted documentation of each assignment should, at the very least, contain the following.
  - A title page with an appropriate title (e.g., "2WF90 Software Assignment 1" for the first assignment), the group number, as well as the names and student IDs of the group members.
  - Table of contents.
  - A clear statement specifying the version of Python 3 in which the submitted software is written.
  - In case you have been given the permission to use additional libraries (in addition to the explicitly permitted libraries in the relevant assignment description), a clear statement specifying the additional libraries that are used in the submitted software. Moreover, if necessary, provide clear installation and setup instructions for each of these libraries.
  - A concise explanation of the purpose of your software; that is, a short problem description.
  - A comprehensive explanation of the approach your software takes to serve its purpose/solve the considered problem. This includes a mathematical description of what your software is capable of doing and how it does so.
  - An explanation of the limitations of your software.

- Illustrative examples demonstrating the correctness of your software (both in regular cases and in edge cases).
- A description of each group member's contribution to the submitted work.
- Where relevant, proper references to lecture material and/or literature.
- In case any references are used throughout the document, a proper list of references at the end of the document.

3 Grading

For both software assignments, the deliverables are graded as follows.

- **Software** (50%)
  Valid (under the relevant interpreter) Python 3 source code that is capable of properly handling input/output and performing the required computations while adhering to the rules and restrictions imposed by the relevant assignment description. Moreover, the source code is commented in such a way that allows a reviewer with some Python 3 knowledge to easily understand and navigate through the code.

- **Documentation** (50%)
  - *Aspects, Structure and Format* (10%)
    Well-structured and well-formatted document that adheres to the guideline described in Section 2.2.2.
  - *Content Quality* (40%)
    Proper description and explanation of the submitted source code, including a discussion on its capabilities and limitations, using well-written English and sound mathematics. Finally, illustrative examples are provided and discussed.

4 Asking Questions

The person responsible for the software assignments is Matthias Meijers. In case you have any questions regarding the software assignments, you are encouraged to proceed in one of the following ways.

- Come to Matthias's office (MetaForum 6.142) and ask your question(s) during one of the office (one-and-a-half) hours. Each week, there will be such an office (one-and-a-half) hour right before the lecture on Thursday, from 12:00 to 13:30 (CEST).
- Send an e-mail with your question(s) to `m.c.f.h.p.meijers@tue.nl`.
- Send an e-mail with a request to schedule a call (in which you can then ask your question(s)) to `m.c.f.h.p.meijers@tue.nl`.