Assignment 1: Due 12 March 2024 (23:59)
Bruteforcing

Security

Universiteit Leiden
The Netherlands

Motivation

This is an easy and fun assignment to start you on the security path. It focuses on a fundamental attack technique (bruteforcing) and will allow you to appreciate the cryptography lectures later in the course.

Task

You are provided two files: a zip archive and a txt file. The goal is to find a *flag* hidden inside the two files. Your solution should be automated (implement it as a script) and we will test it on another set of files that will have similar properties. You may assume you are provided with *a* zip archive (.zip) and *a* txt file (.txt).

We don't tell you what the flag is. But you will recognize it when you find it.

This is an individual assignment.

Submission

You need to submit a Python script and a short report that describes how you have solved the assignment.

Requirements for your assignment submission package (use it as a checklist):

- ☐ Submission is a zip file titled with your student ID number (e.g., `s12345678.zip`).
- ☐ Report (in pdf and in English) is included. It includes your name and your student ID.
- ☐ Your script is called `assignment1.py` and it does **not** expect any arguments. For testing, you can assume that the files will be in the same folder as your script.
- ☐ Your script returns the flag value (i.e., prints the entire flag).

Evaluation criteria

This project will be evaluated on the following components:

- Handling of flag finding on a different (similar but not identical) test set-up. The flag format can be different in the test environment.
- Computer lab machines will be used as a reference: your solution should work there out of the box (no additional installations).
- Our grading will be automated: if you do not follow the submission instructions your solution will not work correctly.
- Correct error handling.
- Concise, typo-free and clear report. Recommended report length: 1 page.