When Algorithm Meets Reality

Homework Assignment 1 - Temporal Side-Channel

Description

A password-checking website has been set up at the address: http://aoi-assignment1.oy.ne.ro:8080

You access the website with your username (your ID number) and with a password. It returns 1 if the password is correct. In addition, there is a difficulty parameter which makes the assignment progressively harder, for example:

http://aoi-assignment1.oy.ne.ro:8080/?user=albert&password=perot&difficulty=1

The design of the password checking code is similar to slide 8 of lecture 2. Your mission is to find the password corresponding to your id number within the shortest amount of time and at the highest difficulty.

Submission Guidelines

1. Submission is through the Moodle site.

   NOTE: Late submissions are always allowed, with the price of 1 point deducted per day. Please notify the grader of any late submission.

2. The execution time of all submissions will be measured on the grader's computer. The team whose code runs fastest on this computer, and finds the password with the highest difficulty, will get special recognition.

3. Submission is allowed in groups of up to two students. Grading will take into account group size, i.e., larger groups are expected to submit higher quality submissions.

4. For the first milestone, you do not need to submit a pdf report, for the second milestone you do.

5. The quality of the code will affect the grade - proper layout, meaningful function and variable names, comments and documentation for functions and major code blocks, no hard-coded constants inside code, etc.

6. Submission is only in **Python** (version 3+).

7. For questions, please use the Moodle Homework Q&A.

8. For problems regarding submission, contact the grader Anna Kolkovsky at **annakul@post.bgu.ac.il**

Hints and Tips

- You can use the first milestone as part of your solution to the second milestone, so write it well!
- The password's character set is a-z. The maximum password length is 32 characters.
- Start with difficulty 1 and only after you crack it progress to difficulty 2.
- It might be difficult to determine the running time based on a single run of the program. **Try running it multiple times per input and calculating the average**.
- This command line program accesses a website and returns how long it took. It works on Mac and Linux. It might also work on Windows after installing cURL for Windows (not tested):

```
curl -s -w '\nTime:\t%{time_total}\n' -o -
http://132.72.81.37\?user=123\&password=NaNaKaNaNa\&difficulty=1
```

- The web server is accessible from anywhere using VPN.
- Do not attempt to "hack" the web server or any other services that are running on the host. This will be considered as an ethics violation and will result in disciplinary action.
- Teamwork is important, make sure that each team member's contribution is clearly described.

Running the Assignment:

- To offload the server and make sure the running time is not affected by other users, you are provided with a docker image to run the assignment locally.
  when you are finished you can test yourselves on the course official server.
- Through the image you can access the server's source code (look online how).
  According to Kerckhoffs's principle an attacker has knowledge about the entire system except the secret key.
  The only difference between the code you run locally and the code that runs on the server is the password salt:

```
10    const DIFFICULT_PASSWORD_SALT = "no_secrets";
```

- Install Docker engine on your PC - link
- To run the docker run the following commands in your terminal:

```
docker pull amarmic/attacks_on_implementations:Assignment1_x86_64
docker run -p 80:8080 amarmic/attacks_on_implementations:Assignment1_x86_64
```

- For mac M1 users:

```
docker pull amarmic/attacks_on_implementations:Assignment1_amd_arm
docker run -p 80:8080 amarmic/attacks_on_implementations:Assignment1_amd_arm
```

- You should be able to query your local server like so:

  http://127.0.0.1/?user=albert&password=perot&difficulty=1

Example:


Desktop — -zsh — 123×24
~/Desktop % curl -s -w '\nTime:\t%{time_total}\n' -o - http://127.0.0.1\?user=123\&password=NaNaKaNaNa\&difficulty=1
0
Time:	0.014899
~/Desktop %

Submission Milestones

Milestone 1 (two weeks from now):

a. **Submission date: 22/04/2025**

b. This milestone does not take the time under consideration, your only mission is to crack your password with difficulty=1.

c. Input: username

d. Output: password.

e. Functionality: nothing except the password should be printed to stdout.

f. The submission should include:

   a. A link to Google Colab with the name "ex01_M1_ID1_ID2" with the complete source code where ID1, ID2 is replaced with the students' ID.

   b. The grader is going to change the username and run the code on the Google Colab.

a. **Submission date: 13/05/2023**

b. Input: username and difficulty.

c. Output: password.

d. **Functionality:** Nothing except the password and the execution time should be printed to stdout. You have 10 minutes to receive your highest difficulty (minimum difficulty = 5).

e. The submission should include:

   a. A link to Google Colab with the name "ex01_M2_[#DIFFICULTY]_ ID1_ID2", where [#DIFFICULTY] is replaced with the highest difficulty level that you solved in under a minute, and ID1, ID2 is replaced with the students' ID. The zip should include the complete source code and a pdf report.

   b. The grader is going to change the username and run the code on the Google Colab.

c. A PDF report with the name: "ex01_M2_[#DIFFICULTY]_ID1_ID2.pdf", inside the submitted zip. Should include:

    1. Output of a sample execution of the program, showing how it recovers the passwords for each member of the team.
    2. Analysis: how many password attempts were theoretically needed with the brute force approach? How many password attempts did your program make?
    3. Optimizations: What did you do to your program so that it would run as fast as possible? How did you deal with the differences between your home network and the University network?
    4. NOTE: you can submit the report only in English.

Good luck!