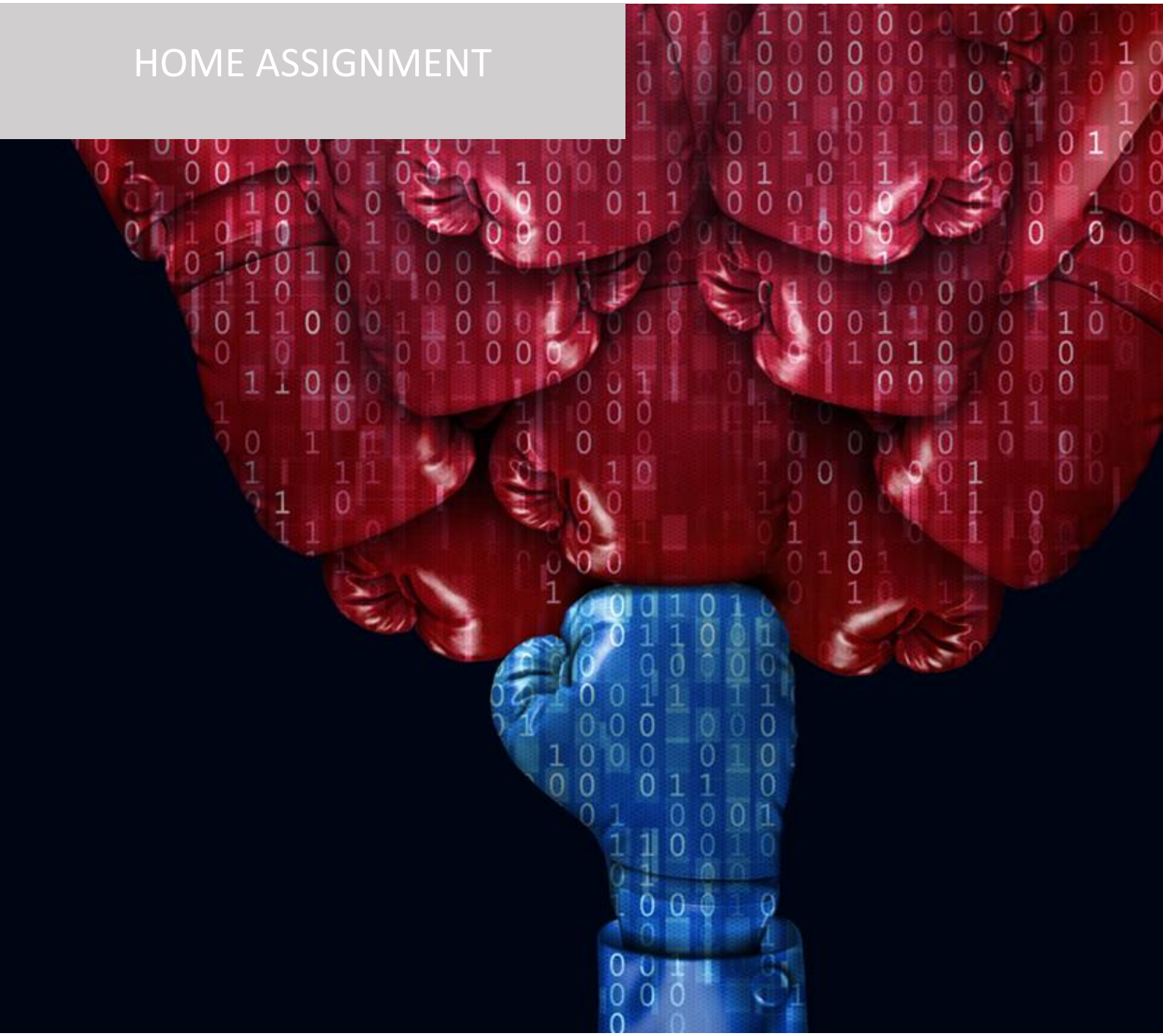
Password Cracker

HOME ASSIGNMENT



PCYSYS
Cyber Resilience

In this exercise, you will create a password cracking service.

You will receive a file containing hashes and will need to write an output of the cracked password.

How a password is cracked:

Password hashes are created through a one-way calculation. This means you cannot calculate the password from the hash.

The way passwords are cracked is to simply try to recreate the same hash with different passwords (Basically, guessing the right password).

In our exercise, the hashes will be simple MD5, and the passwords will always be phone numbers (05X-XXXXXXX). So, to crack a given hash, you'll need to go over all possible phone numbers, calculate their MD5 hash, and check which is equal to the given hash.

Instructions:

The cracking of even a single hash may be resource-intensive, so we wish to separate it between several machines. To achieve this, you'll need to implement a master server that handles the input processing and manages several minion servers, each of which will try to crack the hash in parallel:

Minion:

The minion is a server that receives a hash and a range of potential passwords.

It should go over the range, calculating the hash of each password and compare it to the given hash.

Master:

The master is a server that reads the input file and manages the minions, dividing the cracking workload between them.

Additional notes:

- The communication between the master and the minions should be RESTful.
- Your solution should include crash handling (What happens if any of the minions, or the master, stops in mid-run).
- The workload division should exist even if only one hash is given.
- You are free to implement it in whichever language you feel most comfortable with. We wish to see you coding skills, rather than your familiarity with any specific language.
- Your solution should include the source code, and either a link to a working solution, or instructions on how to deploy and run your code.
- Feel free to ask any questions or clarifications