LELEC2770

Project part 1: voting

1 Goal

Write code that is able to take part to and verify all the steps of the voting protocol explained in the class. The format of the bulletin board is specified in the exercise 5 of the "voting" exercise session.

2 Organization

The project has to be done by group of 1 or 2 students (use the moodle forum to find a project partner if needed). Discussion with other students about the project is welcome (including through the moodle forum), but sharing of code is not allowed. We will check for plagiarism.

3 Deadline

October 26th.

4 Deliverable

A zip file containing (at its root) the following files:

- `verify_bb.py`: a script that, when called as "`python3 verify_bb.py board.json`" (where `board.json` is an existing bulletin board file), print a single line, either "`OK` *n*" if the election is valid (and *n* is replaced by the number of "1" votes), or a line that starts with "`FAIL`" if there is something invalid in the bulletin board.

- `generate_election.py`: a script that, when called as "`python3 generate_election.py` *nt* *nv*" (with *nt* and *nv* being integers), generates randomly an election bulletin board with *nt* trustees and *nv* voters and prints it.

- board_random.json: a valid board generated by running "python3 generate_election.py 3 5 > board_random.json".
- Any other files needed for your scripts to run.
- README.txt containing
  - your name(s),
  - a short overview of the organization of your code and
  - any other information of interest.

Make you code as readable as possible (see https://www.python.org/dev/peps/pep-0008/ for guidance). Excellent tools for this are docstrings and comments.

5 Hints

- The following functions may be helpful: json.dumps, json.loads, json.load (see https://docs.python.org/3.9/library/json.html)
- Your generate_election.py script may start in this way:

```
import sys
nt = int(sys.argv[1])
nv = int(sys.argv[2])
...
```

- We advise you to use the files provided for the exercise sessions:
  - MPC session: elgamal.py (don't forget to complete it!) and number.py
  - Voting session: vote_dproof.py and canonicaljson.py
- Test your tally/verification code on the bulletin boards provided to you (they are with the code for the Voting exercise session).
- Do not hesitate to ask any question on the moodle forum.