Question 1 **[Access Control]** You want to book a room in the BC building but find that it is already booked. You contact EPFL maintenance from a corridor phone to report a water leak in the room. To be on the safe side, the maintenance team cancels all bookings in the room and puts it in maintenance status. After discovering that there was actually no leak, the maintenance team reopens the room for bookings. Quickly, you manage to book the room before anyone else.
Which of the following is true? Question cancelled. both B anc D could be right

- ☐ There is no confused deputy because everyone has an equal opportunity to book the room once the booking reopens.
- ☐ There is a confused deputy problem because the maintenance team wrongly believes there is a leak.
- ☐ There is no confused deputy problem because the maintenance team has the right to cancel all bookings.
- ☐ There is a confused deputy problem because the maintenance team cancels all bookings.

Question 2 **[Applied Cryptography]** You download a sketchy version of Microsoft Office from an untrusted website. To check that the download corresponds to the true software, you look at the checksum (hash) of the Microsoft Office program from the official Microsoft website. Then you compute the hash of the software you downloaded and compare it to the official checksum.
What property must the hash function have for you to be sure that you just downloaded the correct version of Office and not a modified version that could contain malware?

- ☐ The hash function used to compute the checksum of the Office program must be preimage resistant.
- ☐ The hash function used to compute the checksum of the Office program must be slow to compute.
- ☐ The hash function used to compute the checksum of the Office program must be collision resistant.
- ☒ The hash function used to compute the checksum of the Office program must have second preimage resistance.

Question 3 **[Authentication]** Which of the following statements is correct?

- ☐ In password-based authentication, storing salts in the clear leads to offline brute-force attacks.
- ☐ For password storage, a fast hash function is more secure against offline brute-force attacks than a slow hash function.
- ☐ For a 6-digit password that only contains numbers (1 000 000 eligible passwords), the probability of a user manually choosing "000000" as their password is $p = \frac{1}{1\,000\,000}$.
- ☒ Having the server sign the challenge used to prevent replay attacks in password-based authentication would not increase security against these attacks.

Question 4 **[Security Principles]** After listening to the COM-301 lecture on Security Principles, you are enthusiastic about analysing the security of systems you use every day and to what extent they fulfil the eight main principles. You start by analysing the PubliBike system in which a registered user can rent a bike at a fixed hourly rate through a mobile application.
Which of the following statements is correct?

- ☐ The fact that I have to pay for every bike rental after I have returned it to a docking station satisfies the complete mediation principle.
- ☒ The fact that bikes are locked unless a user enters a valid code to unlock a bike satisfies the fail-safe defaults principle.
- ☐ The fact that anyone can download the mobile application from the app store satisfies the open design principle.
- ☐ The fact that payment occurs after a bike rental satisfies the economy of mechanism principle.

Question 5 **[Access Control]** A group of psychology `researchers` plan to study group dynamics. They set up an experiment where `volunteers` need to solve a puzzle together and write their progress in a file `puzzle/updates.log`. `Researchers` hire "`spies`" to hide among the `volunteers` to cause tension in the group and disrupt their progress. To avoid being discovered, `spies` do the same activities as the `volunteers`. To keep the experiment unbiased, `researchers` should not communicate with `volunteers` nor `spies`.
At the end of the experiment, the `spies` write their observations regarding group dynamics to a separate file `dynamics/observations.log`. These observations must be kept secret from `volunteers`. In the end, `researchers` analyse `puzzle/updates.log` and `dynamics/observations.log` to generate their `report.txt` that must not be shared with `spies` nor `volunteers`.

Assuming that
(1) for Bell-LaPadula model the ordering of classes is (TOP SECRET > SECRET > CONFIDENTIAL > UNCLASSIFIED),
(2) for BIBA, the ordering is (HIGH INTEGRITY > LOW INTEGRITY),
(3) "Puzzle" and "Dynamics" are categories;
which of the following options is a good choice to ensure that all accesses happen according to the rules?

- ☐ **BIBA**
  Subjects: `researchers`: HIGH INTEGRITY, `spies`: HIGH INTEGRITY, `volunteers`: LOW INTEGRITY
  Objects: `report.txt`: HIGH INTEGRITY, `dynamics/observations.log`: LOW INTEGRITY, `puzzle/updates.log`: LOW INTEGRITY
- ☒ **Bell-LaPadula**
  Subjects: `researchers`: (TOP SECRET, {Puzzle, Dynamics}), `spies`: (UNCLASSIFIED, {Puzzle, Dynamics}), `volunteers`: (UNCLASSIFIED, {Puzzle})
  Objects: `report.txt`: (TOP SECRET, {Puzzle, Dynamics}), `dynamics/observations.log`: (SECRET, {Dynamics}), `puzzle/updates.log`: (UNCLASSIFIED, {Puzzle})
- ☐ **Bell-LaPadula**
  Subjects: `researchers`: (SECRET, {Puzzle, Dynamics}), `spies`: (SECRET , {Puzzle, Dynamics}), `volunteers` (UNCLASSIFIED, {Puzzle, Dynamics})
  Objects: `report.txt` (TOP SECRET, {Puzzle, Dynamics}), `dynamics/observations.log` (SECRET, {Dynamics}), `puzzle/updates.log` (SECRET, {Puzzle})
- ☐ **Bell-LaPadula**
  Subjects: `researchers`: (TOP SECRET, { }), `spies`: (SECRET, {Dynamics}), `volunteers`: (UNCLASSIFIED, {Puzzle})
  Objects: `report.txt` (TOP SECRET, { }), `dynamics/observations.log` (SECRET, {Dynamics}), `puzzle/updates.log` (SECRET, {Puzzle})

Question 6 **[Applied Cryptography]** Assuming that:
`m` is a message,
`Enc` denotes a symmetric encryption scheme,
`MAC` a message authentication scheme,
`K1` and `K2` are two symmetric keys,
and that Roberta and Gustave have securely pre-shared the keys `K1` and `K2` before.

Which of the options below would allow Roberta to send messages to Gustave while ensuring the confidentiality and integrity of the exchange?

- ☐ `Enc(K1, m), MAC(K1, m)`
- ☐ `Enc(K1, m), MAC(K2, m)`
- ☐ `MAC(K2, Enc(K1, m))`
- ☒ `Enc(K1, m), MAC(K2, Enc(K1, m))`

Question 7 **[Authentication]** Which of the following statements is correct?

- ☐ A token-based authentication system is only secure if the seed is kept secret.
- ☐ Biometric templates cannot be compromised.
- ☐ AES-128 cannot be used in a token-based authentication mechanism.
- ☒ A signature on a credit card is an example of biometrics.