UNIVERSITY OF PADOVA
DEPARTMENT OF INFORMATION ENGINEERING

Biomedical Wearable Technologies
for Healthcare and Wellbeing

The theory exam

A.Y. 2023-2024
Giacomo Cappon

DEPARTMENT OF INFORMATION ENGINEERING
UNIVERSITY OF PADOVA

Exam structure

Written test of 90-minute duration:

- 10 multiple-option questions (only one correct answer)
- 5 true/false questions
- 3 open questions

Notes:

- The exam is in English, answers to be provided in English (English errors not penalized). Dictionary is not allowed.
- At the exam, the students cannot use any course material (slides, books, articles, etc.), nor any electronic device (e.g., smartphone, notebook, etc.). Only the pen is allowed.
- The theory exam will cover all the theory program.

Mark of the theory exam

- Multiple-option questions:
  - 1 point for each correct answer
  - -0.33 points for each incorrect answer
  - 0 points for each not given answer
- True/false questions:
  - 1 point for each correct answer
  - -0.33 points for each incorrect answer
  - 0 points for each not given answer
- Open questions:
  - 0 to 5 points each
- Total score: up to 30 points

Final mark

- The written exam is passed if the student gets at least 18/30 points.

- To get the final mark, students must pass both the written exam and the project discussion.

- The mark of the project is up to 12/30 (based on Q&A project discussion, different students in the same group can get different marks for the project).

- The vote of the theory exam accounts for 2/3 of the final mark.

$$final\ mark = \frac{2}{3} \cdot mark\ of\ the\ theory\ exam + mark\ of\ the\ project$$

Examples of multiple-option questions

Q1. A diffuse-reflective optical sensor:

a. is made of two separate components, a light emitter and a light detector, and the sensing object is interposed between these two components.

b. is made of two separate components, a light emitter and a light retroreflector, and the sensing object is interposed between these two components.

c. is made of a single component integrating both a light emitter and a light detector.

d. none of the previous options.

Examples of multiple-option questions

Q1. A diffuse-reflective optical sensor:

a. is made of two separate components, a light emitter and a light detector, and the sensing object is interposed between these two components.

b. is made of two separate components, a light emitter and a light retroreflector, and the sensing object is interposed between these two components.

c. is made of a single component integrating both a light emitter and a light detector.

d. none of the previous options.

Examples of multiple-option questions

Q2. The following HTTP request:

```
POST /library HTTP/1.1
Host: www.example.com

{
  “Author”: “Stephen Hawking”
  “Title”: “A Brief History of Time”
}
```

a. Delete the book with author “Stephen Hawking” and title “A Brief History of Time” from the book list at the URL www.example.com/library

b. Add to the book list at the URL www.example.com/library a new book with title “A Brief History of Time” and author “Stephen Hawking”

c. Replace the book list at the URL www.example.com/library with the book list containing the book “A Brief History of Time” by “Stephen Hawking”

d. None of the previous answers

Examples of multiple-option questions

Q2. What is the most appropriate use of the following HTTP request?

```
POST /library HTTP/1.1
Host: www.example.com


{
  “Author”: “Stephen Hawking”
  “Title”: “A Brief History of Time”
}
```

a. Delete the book with author “Stephen Hawking” and title “A Brief History of Time” from the book list at the URL www.example.com/library

b. Add to the book list at the URL www.example.com/library a new book with title “A Brief History of Time” and author “Stephen Hawking”

c. Replace the book list at the URL www.example.com/library with the book list containing the book “A Brief History of Time” by “Stephen Hawking”

d. None of the previous answers

Examples of multiple-option questions

Q3. The Diffie-Hellman protocol can be used to:

a. Generate a shared secret key, without the need to exchange the key through a communication channel.

b. Authenticate two communicating parties.

c. Perform the digital signature of a message.

d. None of the previous answers.

Examples of multiple-option questions

Q3. The Diffie-Hellman protocol can be used to:

a. **Generate a shared secret key, without the need to exchange the key through a communication channel.**

b. Authenticate two communicating parties.

c. Perform the digital signature of a message.

d. None of the previous answers.

Examples of multiple-option questions

Q4. In the O-Auth 2 protocol, the authorization server is responsible for:

a. Checking access tokens and providing access to protected resources

b. Checking access tokens and providing authorization codes

c. Checking authorization codes and providing access tokens

d. None of the previous answers.

Examples of multiple-option questions

Q4. In the O-Auth 2 protocol, the authorization server is responsible for:

a. Checking access tokens and providing access to protected resources

b. Checking access tokens and providing authorization codes

c. Checking authorization codes and providing access tokens

d. None of the previous answers.

Examples of true-false questions

Q6. Amperometric electrochemical sensors measure the current between the working electrode and the counter electrode, while the potential of the working electrode is fixed.

TRUE

Examples of true-false questions

Q7. TCP (Transport Communication Protocol) is an unreliable connectionless protocol of the transport layer.

FALSE

Examples of open questions

Q9. Provide a brief description of the following HTTP methods: GET, HEAD, POST, PUT, DELETE.

<u>Possible answer:</u>

- GET: Method used to request the server to send a page or an object. It only retrieves data.
- HEAD: Method used to ask for the response message header, without requesting the actual page content.
- POST: Method used to ask to upload data to a server. With POST the client asks to the server to accept the entity enclosed in the request as a new subordinate of the resource identified by the request URL.
- PUT: Method used to ask to write a content in the server to the specified URL. If the request URL refers to an already existing resource, the server replaces the existing entity with the new enclosed entity.
- DELETE: Method used to ask to delete the content in the server at the specified URL.

Examples of open questions

Q10. Describe the general idea of symmetric cryptography and asymmetric cryptography. Comment the main advantages and disadvantages of both approaches.

Possible answer:

In symmetric cryptography a shared secret key, K, must be established between the two communicating entities. The sender encrypts the message with K and sends it to the recipient. Then, the recipient decrypts the message with K in order to retrieve the plain message. Advantages: encryption and decryption are fast. Disadvantages: the sender and the recipient need to exchange the key K through a safe communication channel; a new key must be generated for each pair of communicating entities.

In asymmetric cryptography, each user is provided a private key, which is secret, and a public key, which is public and can be shared through unsafe communication channels. The sender encrypts the message with the public key of the recipient. Then, the recipient can decrypt the message by its own private key. Advantages: strong security level; there is a pair of keys for each user. Disadvantages: Encryption and decryption are slow.

Examples of open questions

Q11. List and briefly describe at least 5 of the 7 main principles of the GDPR.

Possible answer:

1. Lawfulness, fairness and transparency: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
2. Purpose limitation: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Data minimisation: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accuracy: personal data must be accurate and, where necessary, kept up to date.
5. Storage limitation: personal data shall be stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed.