M.EIC Segurança em Sistemas Informáticos (Computer Systems Security) – 2025/26 FEUP

Exam without consultation of documentation (*closed-book* exam) **Normal Exam**
Duration: 1,5 hours **16.June.2026**
Weight in course final grade: 50%

You may answer in English or in Portuguese.

---

1. [1 pt]

The following quote was taken from the documentation of one of the case studies of vulnerabilities mentioned in the "Motivation" section of the course's Introductory chapter slides.

> «*EMV, named after its founders Europay, Mastercard, and Visa, is the international protocol standard for in-store smartcard payment. (…) Despite the standard's advertised security, various issues have been previously uncovered, deriving from logical flaws that are hard to spot in EMV's lengthy and complex specification, running over 2,000 pages. (…) Using our model, we identified several authentication flaws that lead to two critical attacks: one affecting Visa cards and another affecting Mastercard cards*.»[1]

a) What fundamental Information Technology (IT) security requirement was left out that hints at the probable root cause of the vulnerabilities mentioned in the quote?

b) As an IT security expert, comment on the usefulness of cryptography in addressing this type of security problem.

2. [1 pt]

In the review of basic aspects of Cryptography, the nearby table was presented as part of a general classification table of cryptographic systems.

a) State one *pro* and one *con* for each of the methods: stream, block and block *mixed*.

b) In the practical (lab) assignment «*Padding Oracle Attack Lab*», the Cipher Block Chaining (CBC) mode of operation was seen. What classification does CBC fits in: stream, block or block *mixed*?

Perspective	***Variant***	***Sub-variant***	***Comments***
on the method	stream		• each piece is (de)ciphered with a different key, $K = K_1 K_2$ ... • e.g. $C = K(P) = K_1(P_1)\ K_2(P_2)$ ...
	block	(pure)	• each piece is (de)ciphered with the same key, K • e.g. $C = K(P) = K(P_1)\ K(P_2)$ ...
		mixed	• each piece is (de)ciphered with a "virtual" different key, based on the same key

3. [1 pt]

The second practical (lab) assignment of the course unit was entitled «*Getting free Digital Certificate for email usage: the right way!*» and students were expected to obtain such personal digital certificates.

a) Why was "the right way" specified, in opposition to the *supposedly* "most common way" of getting such digital certificates?

b) Were you able to get your digital certificate? In what "*way*"? From which Certificate Authority?

4. [1 pt]

Regarding the cryptographic digital signature of documents, the message digest technique is the most commonly used.

a) Explain what is the alternative technique for providing a cryptographic digital signature of a document *P*.

b) Present two advantages for using the message digest technique over the alternative one you described in a).

5. [1 pt]

The basic idea of a *chain of blocks* as presented in Nakamoto's "*Bitcoin: A Peer-to-Peer Electronic Cash System*", and in class, was to allow people to make financial transactions under two conditions:

i. without the arbitration of a trusted third party (like a bank);
ii. without being able to spend the same money more than once[2].

Explain how the mentioned conditions could be implemented in Nakamoto's view.

1 D. Basin et al., *The EMV Standard: Break, Fix, Verify*, https://emvrace.github.io/, 2021
2 Meaning: money spent by someone cannot be respent by the same person unless it is re-earned!

6. [1 pt]

The Bell-LaPadula's security policy model is characterized by the usage of "security labels" for both subjects (users) and objects (resources), each label being composed of an ordered *level* and an unordered *category* (or *compartment*)[1].

a) What is the main type of protection Bell-LaPadula's model tries to establish?

b) In the nearby concrete situation, say which users should be allowed to

i. read Document A;

ii. add information to it.

Entity/Object	*level (*)*	*compartment*
User A	3	{marketing}
User B	4	{marketing, maintenance}
User C	1	{marketing}
Document A	3	{marketing}

(*) the higher, the more (security) important

7. [1 pt]

Regarding our very soft introduction to Quantum Cryptography, explain:

a) What is the deliverable of the BB84 protocol and what is the security benefit of using the protocol?

b) The E91 protocol could be used, instead, with exactly the same result and benefit. So, why should we prefer one over the other?

8. [1 pt]

IT Security has several facets; one, deals with Authentication, Authorization and Access Control.

a) Distinguish Authentication, Authorization and Access Control.

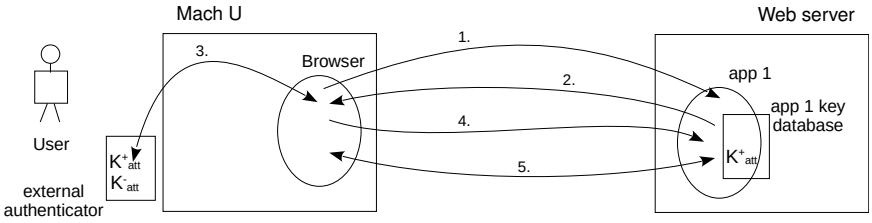
b) Regarding Authentication (of subjects, not objects!), why must we consider two phases: setup (or registration) and (normal) usage?

9. [1 pt]

Passkeys are being advertised as the modern authentication replacement for passwords. Its use is represented in the nearby picture, that can be applied to both phases of authentication (setup and normal usage).

a) Complete the picture by giving a succinct legend for the numbers shown in the phase of your choosing.

b) Can you say if there are cryptographic techniques in use? If so, where?



c) Some *passkey* systems might also use PIN[2] authentication. Where? After all, it was said that *passkeys* were a replacement for passwords!...

10. [1 pt]

Remember what was presented in class on OpenID Connect and OAuth 2.0 and consider the given example of OAuth 2.0 usage: «*Alice can grant a Printing service access to her protected photos stored at Bob's Photo-sharing service, without sharing her username and password with the Printing service.*»

a) Sketch that use case using a diagram similar to the ones shown in class, illustrating the entities interacting in the correct workflow. Take care in showing the mapping of the example's actors and OAuth's entities[3] (Resource Owner, Resource Server, Client, Authorization Server).

b) With the same framework, would you be able to deal with a similar situation, in where Alice is away on holiday and asks Clare to use the same Printing service for printing Alice's protected photos (stored at Bob's Photo-sharing service)? If so, how?

JMMC

1 many times with the form of a set of elements, e.g. {army, navy}
2 Personal Identification Number
3 roles, in its parlance