## MEIC Segurança em Sistemas Informáticos (Computer Systems Security) – 2025/26 FEUP

**Test without consultation of documentation (closed-book test)** **Diagnostic Test**
**Duration: 0.5 hours** **February.2026**
**Maximum (dummy) grade: 10 x 1 = 10 points**

**You may answer in English or in Portuguese.**

---

### 1.

When a user begins using an institution-owned workstation (for example, when a student logs in to a classroom computer during a practical session), the user typically types a password via the attached keyboard to authenticate to the system.
Make two brief remarks about the security of this proces.

### 2.

In the Basic Cryptography chapter of a Security Computer course, an operation *H* was presented - *hashing* or *fingerprinting* - that must have two main properties:

1. unidirectionality («*it is impractical to invert the function H:* $P \neq H^{-1}(C)$»)
2. uniqueness («*it is impractical to find two texts P1 and P2 such that H(P1) = H(P2)*»)

Knowing that for each of the following situations the mentioned systems rely on hashing, give an example of a problem that would arise if:

*a)* property 1 was missing in an authentication system based on passwords;

*b)* property 2 was missing in a system used for the integrity protection of documents.

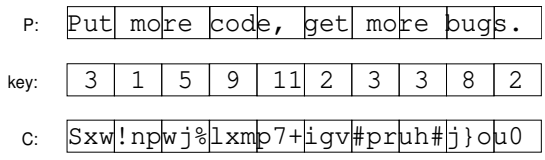
### 3.

The *stream cipher* method is schematically represented in the nearby picture.
Present:

*a)* an advantage of the method over the *block cipher* method;

*b)* a disadvantage of the method over the *block cipher* method;

*c)* a new picture similar to the shown nearby, that illustrates the essence of the *block cipher* method.
(For the *C:* line, fill out just two or three rectangles.)




### 4.

In one of the practical classes of a Security Computer course, each student obtained a free, personal, email digital certificate from a Certificate Authority packed in a `.P12` (or `.PFX`) file which was (most probably) protected by a password.

*a)* What was the other content of the `.P12` file and why was it (most probably) password-protected?

*b)* What is fundamentally flawed on that procedure for getting a digital certificate from a Certificate Authority?

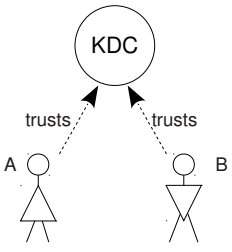
*c)* By the way, what are the 4 absolutely necessary items (pieces of information) of a digital certificate?

### 5.

In the nearby picture (taken from sheets presented in a class of a Security Computer course), KDC means (public) *Key Distribution Centre*.

*a)* What does "trust" mean in the phrase: *A(lice) trusts the KDC*?

*b)* Suppose the KDC is a Certification Authority, from which Alice got a Digital Certificate. She then sends a copy of the digital certificate to B(ob).
In order for Bob to safely "use" the digital certificate is it necessary that he also "trusts" the KDC, as shown in the picture?




### 6.

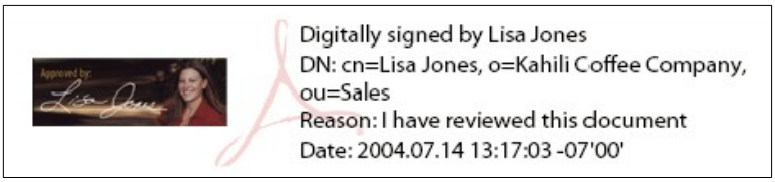
The concept of steganography, was presented in a class of a Security Computer course.

*a)* What can be achieved with the technique: protection of confidentiality, of integrity, of availability or what?

*b)* Explain the essence of the technique.

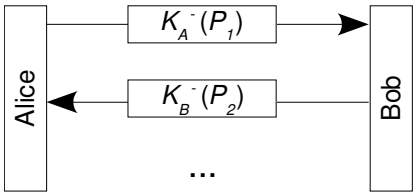
## 7.

The nearby picture is a snapshot of the bottom of the last page of an (electronic) PDF document you have just received.
Are you sure the document was reviewed and sent by Lisa Jones?




## 8.

The nearby picture (taken from sheets presented in a class of a Security Computer course) outlines a digitally signed communication between Alice and Bob. (Remember that $K_X^-$ denotes the private key of $X$.)




*a)* What type of protection covers the communication?

*b)* Sketch a new picture, showing a variant of the same public key protection technique, but this time using *hashing*. The new picture should be as similar as possible to the one shown here.

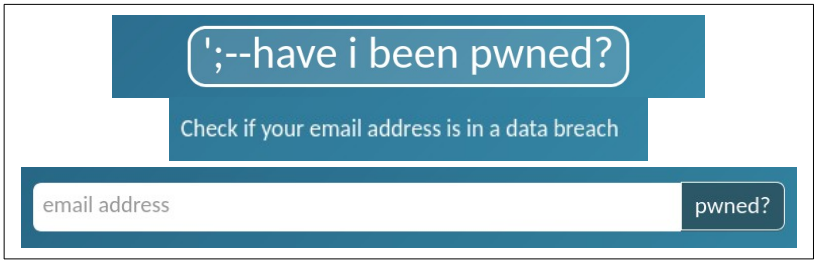
*c)* Name one advantage of the scheme you have just sketched over the original one.

## 9.

There are several websites on the Net that try to assist people on protecting themselves and become informed about safe Internet usage. For each of the following examples, present a critical security view of the anticipated use of those online tools.

*a)* `https://howsecureismypassword.net/`


*b)* `https://haveibeenpwned.com/`




## 10.

In one of the practical exercises of a Security Computer course, the SSH protocol was used to securely transfer files to a remote machine (`gnomo.fe.up.pt`).
Explain if the protocol:

*a)* in the step "machine authentication" (with public-key), guarantees that an user connects to the right remote machine (and not to a fraudulent one);

*b)* in the step "user authentication",

*i.* requires public-key authentication;

*ii.* allows public-key authentication;

*iii.* does not support public-key authentication.

**JMMC**