Exam without consultation of documentation (closed-book test) **Normal Period Exam**
Duration: 1.5 hours **10.January.2024**
Maximum grade: 10 x 1 = 10 points - weight in course final grade: 50%

You may answer in English or in Portuguese.

1.

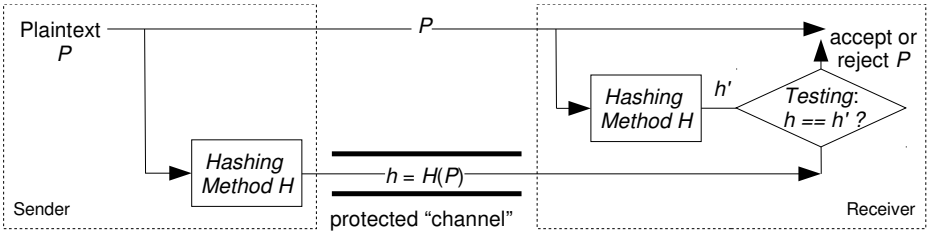
The importance of the human component on the successful protection of a computer system was emphasized in class. For 2 of the main protection objectives presented right in the introductory chapter (Confidentiality, Integrity, Availability and Authenticity), present real (or realistic) situations in which people's actions can compromise a system even if good security mechanisms are in place.

2.

Consider the nearby picture, copied from sheets presented in class.

a) What type of protection for the transmitted document *P* do you want to achieve?

b) What security properties must the protected "channel" have? For example, does it need Confidentiality protection?



c) But, after all, what is the hashing operation needed for?

3.

Consider the following sequences of numbers/letters, labeled A, B and C:

A	B	C

`69:41:33:`
`5f:20:6a:`
`4e:48:4f:`
`49:6f:20:`
`44:5a:53:`
`7a`
	`I0am00John007Doe`	`-----BEGIN RSA PRIVATE KEY-----`
		`MIICXgIBAAKBgQCeN79yFboITNRnxLpUzxO+fnFysK8FqtE176e2CrqjSoyLldw2`
		`QD1LwV/AM3RL/T7/lUZYoxKEhiB4xb4nPrului+Vd336bQw48e6tGlPM9PmUNToc`
		`... 9 more "similar" lines omitted ...`
		`exeutUsDvwYSiPSE8XjxAkEAgVQsoAwqkfSnvs+3tbZDs/GDdigYhJ5r7azOeGTK`
		`bVrmSdIJckU44mkMdQ7b8hLqTDxL4BQkRHagC9Ql7A/4Mw==`
		`-----END RSA PRIVATE KEY-----`

Say which of those sequences (none or one or more of the set {A, B, C}):

a) could be
   i. a cryptographic symmetric key
   ii. a fingerprint of a file
   iii. a password used for login

b) makes sense to be
   i. produced by a normal human
   ii. calculated with a computer
   iii. continually changed after every use

4.

Remember the procedure for obtaining a free digital certificate that you should have done for a practical work.

a) What was all that labor for, that is, what was the purpose of obtaining a digital certificate?

b) Of the elements contained in a digital certificate, present the 4 mandatory ones.

5.

You receive an email message that is enciphered but not digitally signed. Explain:

a) What does an "enciphered message" mean?

b) The sender's address is that of a friend of yours; what level of trust should the message deserve?

6.

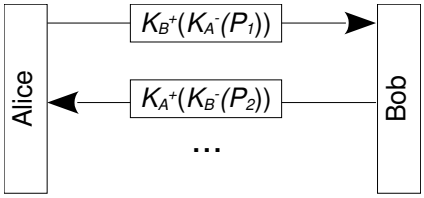
Remember the concept of steganography, that was presented both in theoretical and in practical classes.

a) Why is not a good idea to use a “pure” steganography technique in order to guarantee absolute confidentiality for the transmission of a document?

b) But then, what is the point of using steganography at all?!

7.

The nearby picture (copied from sheets presented in class) outlines a communication between Alice and Bob that is both confidentially and integrity protected.

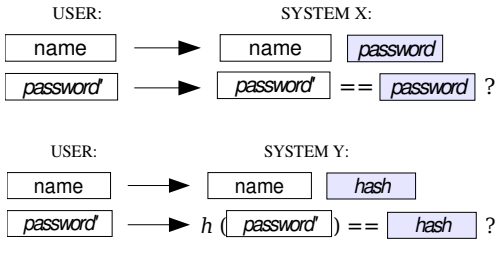


a) Is the protection based on a public key (asymmetric) or shared key (symmetric) system?

b) What keys should Alice and Bob initially have (i.e. before the illustrated message exchange begins)?

8.

Consider two computer systems in which user authentication is carried out using identifiers (login names) and associated passwords. The nearby pictures represent the authentication operation carried out in each system.



a) Which of the systems would you recommend if you were asked for an opinion, as a security consultant.

b) Repeat the previous paragraph, now considering a similar situation, but with user authentication done with a biometric method (e.g. users' fingerprints), instead of using passwords.

9.

In one of the practical classes of the course unit, a specific application (FileZilla) was used to securely transfer files to a remote machine (e.g. `GNOMO`).

a) Explain what does it mean to "transfer securely".

b) The protocol recommended to be used with the FileZilla application was SSH (`sftp://gnomo.fe.up.pt`). Say if this protocol:

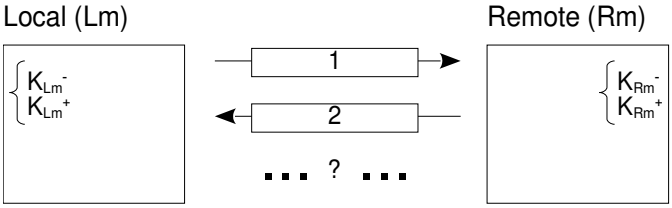
i. guarantees that the user connects to the right remote machine (and not a fraudulent one);

ii. requires the user to have a public key;

iii. requires the user to previously encipher the files to be transferred (to guarantee a secure transfer).

10.

Consider the nearby picture that shows a message exchange used to authenticate the Remote machine to the Local machine.[1]



a) Specify the possible contents of messages 1 and 2 and of other following messages, if needed.

b) Both machines seem to not have the public key of each other at the beginning of the session. Is that a problem for the intended authentication process?

JMMC

1 This exchange is similar to the (First Phase of) SSH protocol used to establish a connection from the Local machine (one of the computers in the practical classroom) to the Remote machine (`gnomo.fe.up.pt`, in our practical work).