Name:	Last name:	Id:

Computer and network security
Sicurezza nelle reti e nei sistemi informatici
Crittografia e sicurezza delle reti

Exam of 10th September 2015, a.y. 2014-15. Time: 2 hours

*FOR NON-ENGLISH: 2 penalty points (only applicable to **Computer and network security**)*
FOR UNREADABLE WRITING: arbitrary penalty points

Q1: **Authentication**

[6/30] Alice, Bob and Charlie need to authenticate themselves in such a way that each of them is certain about the identities of the other two parties. The process is successful if and only if all pairs are mutually authenticated, otherwise it fails.
Present and discuss two possible message-based solutions, respectively using (a) *symmetric-key cryptography* and (b) *public-key cryptography*.

Q2: **Data integrity**

- Q2.1 [2/30] Define the concept of *data integrity* and motivate its relevance.
- Q2.2 [3/30] Discuss at a high level at least *two* approaches for enforcing the data integrity, pointing out their respective strengths.
- Q2.3 [2/30] If Alice has to publish a file on a public web server, what measures she can adopt for reassuring web users about the integrity of the file? (She is a contents editor).

Q3: **TLS vs. IPSec**

- Q3.1 [2/30] Describe at a high level the main security goals of TLS
- Q3.2 [2/30] Describe at a high level the main security goals of IPSec.
- Q3.3 [1/30] Describe an application/infrastructure scenario where TLS looks more useful than IPSec.
- Q3.4 [1/30] Describe an application/infrastructure scenario where IPSec looks more useful than TLS.

Q4: **Bell-LaPadula model**

- Q4.1 [3/30] Describe the goal of the model and present its main ideas (*access classes*, *clearance*, *axioms*, etc.).
- Q4.2 [2/30] Discuss the main limits of the model.

Q5: **Miscellaneous**

Provide *short* answers to the following questions.

- Q5.1 [2/30] What is the difference between weak and strong collision resistance?
- Q5.2 [1/30] What is a man-in-the-middle (MITM) attack?
- Q5.3 [1/30] What it can be the sense of digitally signing a digital signature?
- Q5.4 [1/30] What is a reflection attack?
- Q5.5 [2/30] Define packet filtering, session filtering, proxy gateway (both circuit and application level)
- Q5.6 [1/30] Explain what a *chosen-plaintext attack (CPA)* is.

Name:	Last name:	Id:

HAVE YOU SENT HOMEWORKS TO THE PROF.? YES/NO (circle your answer)

If YES
I hereby confirm that I sent n. ___ contributions:
_____ *in cooperation with* _____
_____ *in cooperation with* _____
_____ *in cooperation with* _____
_____ *in cooperation with* _____

Signature

_____