Name:	Last name:	Id:

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

Exam of 20th July 2015, a.y. 2014-15. Time: 2 hours

FOR NON-ENGLISH: 2 penalty points
FOR UNREADABLE WRITING: arbitrary penalty points

Q1: **Securing communications in an open wifi**

[4/30] Upon her arrival to hotel Hotel Alice forgot to ask at the check-in desk for information on possibly available wifi networks. Nevertheless, once entered her room, Alice turns her notebook on and finds out an open and unencrypted wifi named FreeHotelWiFi.
Alice is happy but also concerned about her privacy and possible man-in-the-middle attacks.
Discuss the concerns of Alice and suggest proper behaviors that can secure her communications.

Q2: **Diffie-Hellman**

Q2.1 [3/30] Describe in detail the Diffie-Hellman exchange of keys.

Q2.2 [3/30] Explain in detail how an attacker can carry out a man-in-the-middle attack and what results it can provide.

Q2.3 [2/30] Suggest a mechanism for securing Diffie-Hellman with respect to man-in-the-middle attacks.

Q3: **Time-stamping service**

Alice is commissioned to design a time-stamping service within a corporate network, aiming at associating a secure time-stamp to files and to digital signatures. To this purpose, the network administrator has set up a time-server using the following protocol. When receiving a request (<id>, *n*), where <id> is the sender and *n* is an integer, the time-server replies by sending to <id> a message (<id>, *t*, H(*t*, *n*)), where *t* is the current time and H is a known hash function of cryptographic quality; when receiving from <id> a request (<id>, *t*, *n*, *h*) the time-server replies by sending to <id> the message (<id>, true) if $h = \mathrm{H}(t, n)$, (<id>, false) if $h \neq \mathrm{H}(t, n)$.

Q3.1 [3/30] Design a scheme of using the time-server resource for associating a time-stamp to a file and to a digital signature (upon request of the legitimate user).

Q3.2 [3/30] Discuss the security of the scheme with respect to possible fraudulent behaviors by the users of the service. If necessary, improve the protocol used by the time-server, *without digitally signing the time-stamps*.

Q4: **Reflection attacks**

Q4.1 [2/30] Describe what a *reflection attack* is (no examples here).

Q4.2 [2/30] Give an (any) example of a reflection attack.

Q5: **Miscellaneous**

Provide short answers (2 lines max) to the following questions.

Q5.1 [2/30] What is the birthday attack?

Q5.2 [2/30] Give a suitable security association for a home user needing to securely connect to a corporate network for read-accessing its corporate shared files,

Q5.3 [2/30] Describe a general technique for contrasting replay attacks.

Q5.4 [2/30] Define what a perfect cipher is.

Q5.5 [1/30] Explain what an *adaptive chosen-plaintext attack* is.

Q5.6 [2/30] Briefly describe the main differences between MAC and DAC access control models.

Name:	Last name:	Id:

HAVE YOU SENT HOMEWORKS TO THE PROF.? YES/NO

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

Signature

____