Name:	Last name:	Id:

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

Exam of 24th June 2019, a.y. 2018-19. Time: 2 hours
Outcomes will be published in web page within three weeks

1. ***Please fill & sign this form, to be consigned to the prof.***
2. ***FOR NON-ENGLISH: 2 penalty points (only applicable to Computer and network security)***
3. ***FOR UNREADABLE HAND-WRITING: unreadable parts will be skipped***
4. ***YOU ARE KINDLY REQUESTED NOT TO WRITE BY A PENCIL. BALLPOINT PENS ARE STRONGLY PREFERRED***

Q1: **Authentication**

Q1.1 [2/30] **Describe the goals** of authentication and possible attack models against it.

Q1.2 [3/30] Describe the **technical features** of an authentication based on trusted third-parties and mention a few practical examples where this technology is actually employed.

Q1.3 [3/30] Alice and Bob agreed the special message T = "The cat is on the moon" and on a 256b secret key K. For one-way authentication Alice sends to Bob $Enc_K(T)$: Bob decrypts, recognizes T and authenticates Alice. **Discuss the security of the protocol and possible improvements**.

Q2: **Forgery**

Q2.1 [4/30] **Carefully define** the types of message forgery and how they are related to the power of an attacker. For the **weakest type** of message forgery, discuss the reasons why modern information security still requires full protection against it.

Q2.2 [3/30] **Describe in detail** one method to prevent message forgeries.

Q3: **TLS**

Q3.1 [3/30] You have just published a new library providing full support to the TLS protocol and before starting to write the technical documentation, you want to write an introduction explaining to programmers what services are provided by your library (not the list of API, just a description of the high level services provided by TLS). **Write the introduction (max 1 page). Longer introductions will be penalized.**

Q3.2 [3/30] Even if your library is written without bugs and perfectly follows the last technical specification of TLS (1.3), and assuming that no vulnerabilities are known in TLS 1.3, the security of the services offered by your perfect library can be affected by….. (**complete and discuss**).

Q4: **Firewalls**

Assume that the iptables software is running on host *H*, having a network interface eth0 (IP: 192.168.0.2) connected to a LAN (IP: 192.168.0.0/24) and a network interface eth1 (IP: 151.100.4.3) connected to the Internet. Assume that the default policy for all built-in chains is DROP. There are no DNS within the LAN.

Q4.1 [2330] **Define suitable rules** for allowing the administrator of iptables to connect to *H* (by ssh) only from host 192.168.0.200, for the purpose of **administering iptables**.

Q4.2 [4/30] **Define suitable rules** for allowing standard users of the LAN to **browse the web** only in the case of **https connections** (http not allowed): for example: https://www.icann.org/. *Remind that the default policy for all built-in chains is DROP,*

Q5: **Shamir secret sharing**

Q5.1 [2/30] **Define** what an (*n*, *k*) Shamir secret sharing scheme is, where $1 < k < n$

Name:	Last name:	Id:

Q5.2 [2/30] Suppose that an (n, k) scheme is already in use. In the case we need to change n into n+1 (a new participant arrives), and we want to minimize the impact of that, **what actions can be carried out** for getting an (n+1, k) scheme?

Q5.3 [1/30] What do we mean by "the Shamir scheme is information-theoretically secure"?

HAVE YOU SENT 2018-19 HOMEWORKS TO THE PROF.? YES / NO (circle your answer)

If YES:
I hereby confirm that I sent no. _____ contributions

Signature

_____
(please sign, in the case of both yes and no!)