Name: ANDREA	Last name: PUCCIATI	Id: 1665823

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

Exam of 24th July 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 of messages (emails, files) (type: AoM) vs. authentication of entities (people, processes, devices) (type: AoE)**

Q1.1 [2/30] **Compare** the two types of authentication and **discuss** the information security requirements.

Q1.2 [3/30] **How**, **to what extent**, and with **what limitations** cryptographic hashing could be employed to enforce some authentication, **clarifying** whether AoM or AoE.

Q1.3 [3/30] **Describe** a technique guaranteeing at the same time AoM and AoE (detailedly describe every single step).

Q1.4 [2/30] Alice and Bob share a 256-bits secret key K, and Alice sends to Bob $Enc_K(M)$. **Discuss** if this allows authentication of the sender and/or of the message M (M is arbitrary), or no authentication at all.

Q2: **Confidentiality and RSA**

Q2.1 [3/30] **Carefully describe** how RSA could allow confidentiality through data encryption, illustrating each single step at the two ends of the communication. **Also discuss** the characteristics of an even small PKI supporting the functioning of RSA.

Q2.2 [3/30] If N = pq = 37769 **what is the maximum size** of a single message that RSA can encrypt and how to let RSA encrypt **bigger messages**?

Q2.3 [2/30] Discuss the efficiency of the solution at Q2.1, and **propose an alternative** and more effective approach still benefiting from a PKI.

Q2.4 [3/30] You are the consultant of the IT department of a small hospital. They need to strongly protect the confidentiality of their patients' health data and have heard of strong symmetric encryption (AES based) that can act at different levels: self-encrypting disks, encrypted file-systems, encrypted DBMSs, user level encryption, etc. Can you help them to avoid confusion by **writing a short summary** (max: half a page) illustrating the pros and cons of encrypting at such different logical levels?

Q3: **Access control**

Q3.1 [3/30] Modern operating systems provide users/administrators with commands like `chown` (change owner) and `chmod` (change mode) for changing ownership of and permissions to access some given resource in the file system. Is this an access control DAC or MAC based? **Carefully explain** and **motivate**.

Q3.2 [2/30] Do `chown`/`chmod` allow protection from **Trojans**? **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 ACCEPT. Host *H* is also a DNS.

Q4.1 [3/30] **Define suitable rules** allowing the administrator of iptables to connect to *H* (by ssh) from any host of the LAN, for the purpose of **administering `iptables`**, and

Name:	Last name:	Id:

blocking all attempts to administer `iptables` coming from the Internet. (Among correct rules, **shorter ones** will get an award; in particular do not add useless rules)

Q4.2 [4/30] The **LAN is under attack** and many hosts have been **compromised**, except host **B** (whose IP is 192.168.0.111) and host ***H*** that **are massively protected**. Define emergency rules **blocking all traffic** LAN-to-Internet and Internet-to-LAN, **but still allowing** (as an exception) traffic B-to-Internet and **the related responses.**