Name:	Last name:	Id:

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

Exam of 4th November 2015, a.y. 2014-15. Time: 2 hours
Supplementary exams session

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

Q1: **Digital signatures and time-stamping**

Q1.1 [3/30] Describe the basic characteristics of the DSS approach to digital signing. What is the advantage of using two pairs of keys for each signature?

Q1.2 [3/30] Alice, Bob and Charlie have made a written agreement and now need to digitally sign it, and to attach a secure time-stamp to each signature. Describe what type of infrastructure they need and a sequence of steps for accomplishing their task.

Q2: **Cryptographic hashing functions**

Q2.1 [2/30] Describe the requirements to be met by a cryptographic hashing functions.

Q2.2 [2/30] Describe the Merkle–Damgård construction for hashing a message longer than just one block.

Q2.3 [2/30] Compare keyed to non-keyed hashing and discuss the security of hashing $k|m$, $m|k$, $k|m|k$, where m is a message, k is a secret key and | a symbol denoting concatenation.

Q3: **Rock-paper-scissors game**

Alice and Bob play a Rock-paper-scissors match. In a single match the two party simultaneously form one of the shapes and the winner is established by the simple chain of circular rules *rock beats scissors*, *scissor beats paper* and *paper beats rocks*. The two players use the following protocol:

[Alice and Bob choose their shapes a and b, where h is a known cryptographic hash function]

A→B: $h(a)$

B→A: b

A→B: a

[Bob checks $h(a)$; then both Alice and Bob know the winner of the game]

Q3.1 [3/30] Discuss possible weaknesses of the protocol, with respect to possible fraudulent behaviors from Alice and/or Bob, both ready to cheat in order to win the game.

Q3.2 [3/30] Fix the weaknesses (small changes!), without introducing third parties or public-key cryptography.

Q4: **Firewall**

Q4.1 [2/30] Illustrate the most relevant characteristics of `iptables`, employed as a firewall.

Q4.2 [2/30] What rules you would set for a mail server accepting connections for EMSTP (port 465) and IMAP (port 993) having a network interface `eth1` exposed to the Internet and another network interface `eth2` exposed to the corporate network?

Q5: **Miscellaneous**

Provide *short* answers to the following questions.

Q5.1 [1/30] What is the existential forgery attack?

Q5.2 [2/30] What is the Optimal Asymmetric Encryption Padding (OAEP) and why it provides "all-or-nothing" security ?

Q5.3 [3/30] Determine the multiplicative inverse of 47 mod 64.

Q5.4 [3/30] Given the two primes 23 and 11 find integer α such that $\alpha^{11} = 1 \bmod 23$

Q5.5 [2/30] Describe what *mandatory access control* 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

____