Name:	Last name:	Id:

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

Exam of 18th June 2015, a.y. 2014-15. Time: 2 hours

Q1: **Securing messages on an insecure channel**

Q1.1 [4/30] Alice and Bob have agreed a symmetric key to be used for encrypting messages to be sent over an insecure (wrt a passive adversary) communication channel. Both of them have hardware devices for carrying out decryptions, but no (hardware or software) encrypting tools. Nevertheless, they have to setup a simple scheme for securing the privacy, based on hardware decryptors, allowing the sender to encrypt a message and the recipient to decrypt a message. Design the scheme.

Q1.2 [3/30] Improve the scheme designed in Q1.1 for also securing the integrity of messages against active adversaries. Notice that no further resources are available (in particular, no hash functions, HMAC or similar), but Alice and Bob can establish more than one key.

Q2: **RSA**

Consider the following textbook RSA example. Let be p = 7, q = 11 and e = 3.

Q2.1 [3/30] Give a general algorithm for calculating d and run such algorithm with the above inputs.

Q2.2 [1/30] What is the max integer that can be encrypted? Explain.

Q2.3 [2/30] Is there any changes in the answers to Q2.1 and Q2.2 if we swap the values of p and q? Explain.

Q3: **Fair dice rolling**

Alice and Bob have to simulate a fair dice rolling process, running in real time, each of them using a 6-faces die. They use the following protocol, based on a secure communication channel.

$A \rightarrow B$: (A, N_A) { A sends to B the outcome of her die rolling N_A in {1, 2, …, 6} }

$B \rightarrow A$: (B, N_B) { B sends to A the outcome of his die rolling N_B in {1, 2, …, 6}}

{ Now both A and B know N_A and N_B and therefore know the global outcome $N_A + N_B$ }

Q3.1 [3/30] Discuss the security of the protocol with respect to possible fraudulent behaviors of A and/or B. In particular, show how it is possible for some of the parties to deterministically choose or control the final outcome, being the other not aware of the fraud.

Q3.2 [3/30] Fix the protocol, without introducing third parties.

Q4: **Access control**

In a university department, professors can write marks of their students and read marks of all students; the didactic secretary can read marks of all students; other administrative staff cannot read/write marks.

Q4.1 [3/30] Choose a model of access control for the above setting, describe it and motivate the choice through a suitable discussion.

Q4.2 [2/30] Is the above model robust wrt Trojans? Discuss.

Q5: **Miscellaneous**

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

Q5.1 [1/30] $\Phi(11) = ?$ (Φ is the Euler's totient function)

Q5.2 [2/30] What are the main differences between the end-to-end security provided by IPSec and that provided by TLS?

Q5.3 [2/30] State the Theorem of Galois on Galois Fields.

Q5.4 [1/30] What scheme can be used for generating one-time passwords?

Q5.5 [1/30] Explain what a reflection attack is.

Q5.6 [1/30] Explain what a “man in the middle” attack is.

Q5.7 [1/30] Explain what a chosen-ciphertext attack is.

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

_____