Name:	Last name:	Id:

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

Exam of 13 January 2016, a.y. 2015-16. Time: 2 hours

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

Q1: **Perfect ciphers**

Q1.1 [1/30] Define what a *perfect cipher* is.
[If definition is wrong subsequent questions cannot be correctly answered]

Q1.2 [2/30] Prove that the property that defines what a perfect cipher is also holds if we exchange the roles of ciphertext and plaintext.

Q1.3 [2/30] Prove that a cipher cannot be perfect is the size of its key space is less than the size of its message space.

Q1.4 [2/30] *Describe* the Vernam Cipher (a.k.a. One Time Pad) and *clearly state* the property that must hold for it being a perfect cipher.

Q2: **Meet in the middle**

With reference to a *symmetric-key block-ciphering* algorithm, answer the following:

Q2.1 [2/30] Describe the so called *Meet-In-The-Middle* attack (*not to be confused with Man-In-The-Middle*) as well as a possible scenario where Meet-In-The-Middle can be used by an attacker.

Q2.2 [2/30] Give a rough estimation of the max key-length that can be successful attacked by Meet-In-The-Middle, assuming an adversary using 2 hours computation time of a 64GB RAM machine (and negligible external storage), capable of encrypting/decrypting a block in 20ns (for any key of reasonable length) and of accessing a RAM word in 4ns. *Ignore CPU time that you can assume involving simple arithmetics on cache; also assume that block size is 128b.*

Q3: **The birthday attack**

Q3.1 [3/30] Illustrate the so-called *birthday paradox* and describe what type of attack (*birthday attack*) can be prepared by exploiting this property.

Q3.2 [2/30] Is the birthday bound affected by the quality of the hash function (cryptographic or non-cryptographic). Elaborate.

Q3.3 [2/30] Is keyed hashing making the birthday attack harder? Elaborate.

Q4: **The HRU model**

Q4.1 [3/30] With reference to the Harrison-Ruzzo-Ullman model illustrate the concepts of *subject*, *object*, *primitive operation*, *command*, *protection system*, *leakage* of a right and *safety* of a protection system. State *decidable* and *undecidable* questions about safety.

Q4.2 [2/30] Explain why the HRU model is unable to protect against Trojan horses.

Q4.3 [2/30] Is the HRU model a DAC or a MAC model? Elaborate.

Q5: **Digital signatures**

Q5.1 [2/30] Illustrate the (generic) processes for generating/verifying *digital signatures.*

Q5.2 [2/30] Define the *existential forgery* attack and point out the steps whose bad implementation

Name:	Last name:	Id:

can easier an existential forgery.

Q6: **Miscellaneous**

Provide *short* answers to the following questions.

Q6.1 [1/30] Explain the difference between *packet filtering* and *session filtering.*

Q6.2 [2/30] Is TLS is said to give *end-to-end* security. Carefully *explain* what end-to-end means in this case.

Q6.3 [2/30] Given primes 11 and 5 find $\alpha > 1$ such that $\alpha^5 = 1 \bmod 11$. (No calculators allowed)

Q6.4 [1/30] Describe what *port forwarding* is within the SSH protocol.

HAVE YOU SENT 2015-16 HOMEWORKS? YES/NO (<u>circle your answer</u>)

If YES:
I hereby confirm that I sent the following contributions (state HW and Q numbers):

_____

_____

_____

_____

_____

_____

_____

_____

Signature

_____