

Name:	Last name:	Id:
-------	------------	-----

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

*Exam of 26th March 2015, a.y. 2014-15. Time: 2 hours*  
*1<sup>st</sup> extraordinary call 2014-15*

**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 the encryption, but no (hardware or software) decrypting tools. Nevertheless, they have to setup a simple scheme for securing the privacy, based on hardware encryptors, 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: Diffie-Hellman**

- Q2.1 [3/30] Describe in detail how two parties can establish a secret key by using the Diffie-Hellman scheme and discuss the vulnerability of the approach.
- Q2.2 [2/30] Generalize Diffie-Hellman so that three parties can establish a shared secret key.
- Q2.3 [3/30] Describe a scheme for mutual authentication that is strong with respect to dictionary attack and that uses Diffie-Hellman for defining a session key. Do vulnerabilities discussed in Q2.1 still hold?

**Q3: Leader selection**

A leader should be selected by randomly choosing one of three parties  $A$ ,  $B$  and  $C$ . The parties use the following protocol

$A \rightarrow B: N_A$  {  $A$  chooses nonce  $N_A$  }

$B \rightarrow C: (N_{AB} = N_A \wedge N_B)$  {  $B$  chooses nonce  $N_B$  and sends  $N_{AB} = N_A \wedge N_B$ , where  $\wedge$  is the ex-or operation }

$C \rightarrow A: (N_{ABC} = N_{AB} \wedge N_C)$  {  $C$  chooses nonce  $N_C$  and sends  $N_{ABC} = N_{AB} \wedge N_C$  }

{ Now both  $A$  and  $C$  know  $N_{ABC}$  }

$A \rightarrow B: N_{ABC}$

{ Now  $B$  knows  $N_{ABC}$ , too }

{ Each of the three parties can now compute  $p = N_{ABC} \bmod 3$ , where  $p = 0$  denotes  $A$ ,  $p = 1$  denotes  $B$ , and  $p = 2$  denotes  $C$  }

- Q3.1 [3/30] Discuss the security of the protocol with respect to possible fraudulent behaviors of  $A$ ,  $B$  and/or  $C$ . In particular, is it possible for some of the parties to deterministically choose the leader, being the others not aware of the fraud?
- Q3.2 [3/30] Fix the protocol.

**Q4: (A.Y. 2014-15 only) Shamir**

- Q4.1 [3/30] Describe the Shamir scheme  $(k, n)$  for sharing a secret.
- Q4.2 [3/30] Make a numerical example for the case  $(2, 4)$ , for sharing the secret number 6. Show how the 4 fragments are computed.

**Q5: (A.Y. < 2014-15) Access control**

- Q5.1 [3/30] Illustrate the DAC model (from Harrison-Ruzzo-Ullman, or HRU), define the concept of safety of the protection system and discuss what practical problems arise within the model.
- Q5.2 [3/30] Why such DAC model is vulnerable to Trojans? What type of access control model can prevent them from illegally access private data? Discuss.

**Q6: Miscellaneous**

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

- Q6.1 [1/30]  $\Phi(10) = ?$  ( $\Phi$  is the Euler's totient function)

Name:	Last name:	Id:
-------	------------	-----

Q6.2 [2/30] RSA: if  $p = 13$  and  $q = 17$ , what is the range for exponent  $e$ ?

Q6.3 [2/30] What is the multiplicative group  $Z_{10}^*$ ?

Q6.4 [1/30] Can iptables filter out incoming datagrams that are IPSec-tunneled packets going to port 25?

Q6.5 [2/30] What is port forwarding and what protocol implements it?

*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*

\_\_\_\_\_