Name:	Last name:	Id:

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

Exam of 21st February 2018, a.y. 2017-18. Time: 2 hours

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. ***UNREADABLE HAND-WRITING will not be considered by the prof***
4. ***YOU ARE KINDLY REQUESTED NOT TO WRITE BY A PENCIL***

Q1: About digital signatures
Evaluate the truth of the following assertions (please mark by **X** the T or F column, for true or false). [correct: +0.5; wrong: -0.25; no answer: 0]

Assertion	T	F
A digital signature is obtained by encrypting a message digest by the public key of the signer		
ElGamal signature uses a temporary pair of public/private keys		
DSS signature uses a temporary pair of public/private keys		
RSA is the standard signing algorithm chosen by NIST		
The encryption effort requested by RSA is quickly growing with the size of the document to be RSA-signed		
All modern standards for digital signatures require a cryptographically secure hashing function		
RSA is slower than DSS in signature verification		
If the hashing function is replaced by h(x) = x then the RSA signature is subjected to existential forgery attacks		
The security of a digital signature relies on the non-modifiability of the signed document		
Alice sends a digitally signed message to Bob: the verification of the signature relies on the certification of the public key of Bob		

Q2: An odd/even game, again
Alice and Bob want to play the odd/even game by exchanging messages on the net. In the classic odd/even game the players choose two non-negative integers Z_A and Z_B (assume both numbers < 128 and represented by 7 bits), after having betted on the parity (even or odd) of $Z = Z_A + Z_B$; at time of betting the players have not yet chosen their numbers. The players play in the net by the following protocol. In what follows h(.) is a cryptographic hashing function, and || denotes concatenation.

A → B: n_B [Bob chooses nonce n_B and sends it to Alice]
A → B: $(p, h(Z_A||n_B))$ [Alice chooses parity $p \in$ {even, odd} and Z_A, then sends p and $h(Z_A||n_B)$]
B → A: Z_B [Bob chooses Z_B and sends it to Alice; now Alice can compute Z_A+Z_B]
A → B: Z_A [Alice reveals her data, then Bob can check hash and compute Z_A+Z_B too]

Q2.1 [4/30] Show that one party can cheat and manage to win all the games.

Question 1

Digital signatures

Focus on the process of signing a document by a valid digital signature and discuss the following points:

Q1.1 [2/30] What is the role of the hashing function? What happens if we choose to hash by the function $f(x) = x$?

Q1.2 [2/30] Describe a signing algorithm that is using a pair of temporary public/private keys. What is the advantage of temporary keys?

Q1.3 [1/30] On what relies the information security of a valid digital signature?

Name:	Last name:	Id:

Q2.2 [4/30] Show how to fix the protocol (by adding/changing messages) so that it is made more secure wrt possible misbehaviors. (Do not introduce 3rd parties)

Q3: Secret sharing

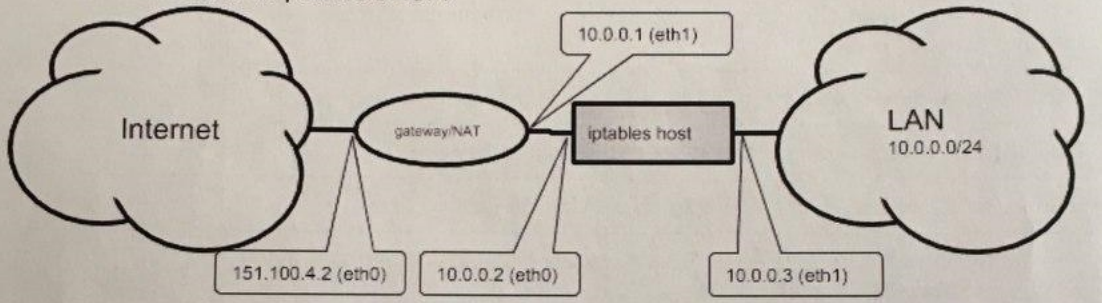
Consider the problem of sharing a secret $S < 53_{10}$ among 5 parties. (Ignore problems related to the small size of S)

Q3.1 [3/30] Consider the basic problem (all shares needed for reconstructing the secret) and show how to generate the shares for $S = 100011_2$. Provide details.

Q3.2 [5/30] Consider the Shamir secret sharing case with threshold 3 and show an example of generation of the shares for $S = 100011_2$. Arbitrarily (but correctly) choose the parameters you need for the generation. Provide details.

Q4: **Iptables**

Consider the scenario summarized by the following drawing and focus the host where iptables is running. Assume that the FORWARD chain has as policy ACCEPT, and that both INPUT and OUTPUT chains have as policies DROP.



Q4.1 [3/30] Define an iptables rules allowing ssh connections from the LAN to the iptables host

Q4.2 [3/30] Define an iptables emergency rule preventing LAN packets from going to the Internet

Q4.3 [3/30] Define an iptables emergency rule preventing Internet packets from entering the LAN

Q5: **Short questions (You have to show your ability to be ability to be concise)**

Provide short answers to the following questions. (Answers must be short! Using many lines reduces the quality of the answers)

Q5.1 [2/30] Port to port security is needed. How to choose between TLS and IPSec?

Q5.2 [2/30] Does HRU protect against covert channels? Explain.

Q5.3 [2/30] Compute 2^{280} mod 251. (No calculators allowed; 251 is prime)

If you haven't registered to the exam through the Google form provided by the prof., please answer:

HAVE YOU SENT 2017-18 HOMEWORKS TO THE PROF.? YES / NO (circle your answer)

If YES: I hereby confirm that I sent no. _____ *contributions*

Signature

_____

(please sign, in ANY case)