Name:	Last name:	Id:

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

Exam of 26th January 2018, a.y. 2017-18. Time: 2 hours
Outcomes will be published in web page within two weeks

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 be skipped***
4. ***YOU ARE KINDLY REQUESTED NOT TO WRITE BY A PENCIL. BALLPOINT PENS ARE STRONGLY PREFERRED***

Q1: About block cipher modes of operation
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
ECB is insecure for encrypting one single block of plaintext		
ECB is parallelizable		
CBC-encryption is parallelizable		
CBC-decryption is parallelizable		
In CBC decryption: a bit flip in the ciphertext corrupts only the current block		
Ciphertext stealing is a technique for reducing the size of the ciphertext by a constant factor		
CFB makes a block cipher into a self-synchronizing stream cipher		
OFB: knowledge of the initialization vector is not sufficient for breaking its security		
OFB: can preprocessing speed-up the encryption/decryption process?		
CTR: reusing the initialization vector does not introduce a vulnerability		

Q2: Odd/even game
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, 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.

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

Q2.1 [4/30] Show that Alice can cheat so that she can manage to win all the games.
Q2.2 [4/30] Show how to fix the protocol (by adding/changing messages) so that it is made more secure wrt possible Alice misbehaviors. (Do not introduce 3rd parties)

Name:	Last name:	Id:

Q3: Authentication

Q3.1 [3/30] Describe a scheme of authentication based on Needham-Schroeder that makes use of a trusted third party. Discuss the type of authentication (one/two way) and its robustness against *replay* attacks.

Q3.2 [4/30] Inspired to the scheme above, design a scheme of mutual authentication between three parties, that makes use of a trusted fourth party.

Q4: Iptables

Describe at your best each the following iptables commands, clarifying whether they are meant to protect a network or a single host (explain why). In what follows eth0 is a network interface exposed to the extern, eth1 is a network interface to the LAN.

Q4.1 [2/30] `iptables -A FORWARD -p udp -i eth0 -o eth1 --dport 53 --sport 1024:65535 -j ACCEPT`

Q4.2 [2/30] `iptables -A INPUT -p tcp -i eth1 --dport 22 --sport 1024:65535 -m state --state NEW -j ACCEPT`

Q4.3 [2/30] `iptables -A OUTPUT -p tcp -i eth0 --dport 22 --sport 1024:65535 -m state --state NEW -j ACCEPT`

Q5: Short questions on BLP (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] Does BLP protect against Trojan horses? (Few lines)

Q5.2 [2/30] Does BLP protect against covert channels? (Few lines)

Q5.3 [2/30] Does BLP help in preserving the data integrity? (Few lines)

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)