Name: Carmela	Last name: Salandria	Id: 1527725	B

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

Exam of February 21st 2019, a.y. 2018-19. Time: 2 hours
Outcomes will be published in web page within three 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. ***FOR UNREADABLE HAND-WRITING: unreadable parts will be skipped***
4. ***USE BALLPOINT PENS AND ENSURE NOT TO WRITE MICROSCOPIC CHARACTERS***

Q1: **Authentication**

Q1.1 [3/30] Consider the following challenge-response protocol for mutual authentication between Alice and Bob, where the parties share a secret X

A → B: (A, *a*)
{ *a* is a nonce chosen by Alice, that challenges Bob }
B → A: (B, *b*, HMAC(X, *a*))
{ *b* is a nonce chosen by Bob, that challenges on his turn Alice, in addition Bob answers the challenge }
{ now Alice recognizes Bob }
A → B: (A, HMAC(X, *b*))
{ Alice responds to the challenge and Bob recognizes her }

Analyze the protocol and determine its vulnerabilities, describing how an adversary can succeed in being illegitimately authenticated (show the protocol messages).

Q1.2 [3/30] Propose a review of the protocol in Q1.2 (you can emend the protocol, but you are not allowed to completely change its nature)

Q2: **Symmetric encryption**

Q2.1 [2/30] Define what block and stream (symmetric) ciphers are. Mention at least one example of stream cipher and one of block cipher.

Q2.2 [3/30] Define the concept of perfect cipher and describe the conditions under which a stream cipher is perfect (you may consider a practical case).

Q2.3 [2/30] Illustrate how a symmetric block cipher, under certain operation modes, becomes a stream cipher.

Q3: **Cryptographic hashing**

Q3.1 [3/30] Define the properties that makes "cryptographic" a hashing function.

Q3.2 [3/30] Describe and justify the so-called birthday-attack and discuss how it affects hashing functions. Are cryptographic hashing functions affected?

Q3.3 [2/30] Is the function $h(x) = x \bmod 2^{256}$ a cryptographic hashing function? (Answers without a proper motivation will be discarded).

Q4: **Firewalls**

Assume that the iptables software is running on host *H*, having a network interface eth1 (IP: 192.168.0.10) connected to a LAN (IP: 192.168.0.0/25: the LAN is protected by *H*) and a network interface eth2 (IP: 151.100.4.4) connected to Internet. Assume that the default policy for all built-in chains is ACCEPT.

Q4.1 [4/30] Both *H* and the whole LAN are under attack: define proper "panic" rules blocking all the traffic towards/from the LAN and towards/from *H*. After enforcing the requested rules how can the network administrator administer *H*?

Q4.2 [3/30] Define suitable rules for preventing hosts of the subnet 151.100.0.0/16 to communicate with the LAN subnet 192.168.0.16/28 (and vice versa).

Q4.3 [2/30] Describe at your best the effect of the following two commands (please don't limit yourself to give a syntactic reading of the lines below, but provide also a high-level interpretation):

```
iptables -A OUTPUT -p tcp --sport 0:1023 -j DROP
```

Name: Carmela	Last name: Salandria	Id: 1527725	B

```
iptables -A OUTPUT -p udp --sport 0:1023 -j DROP
```

Q5: **TLS vs IPSec (short answer, at most 4 lines)**

[3/30] As an application architect, describe some general guidelines for choosing between TLS and IPSec to the purpose of allowing secure communication between two distinct parties.