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

***Remote exam** of 13rd January 2022, a.y. 2021-22. Time: 2 hours*

Q1: **Before you start**

Please insert starting from top line:

A. position (regular, not Infostud registered, Infostud registered but blocked, etc.)
B. degree course (master in something, or other)
C. number of homeworks (≥ 0) validly (within the proper deadline, or, if on late, explicitly authorized by the prof.) delivered
D. comment (whatever you want to say to prof.)

best wishes now…

Q2: **Data integrity**

Q2.1 [3/30] Describe what we mean by data integrity and discuss the use of keyed HMACs for guaranteeing the integrity of a file being transmitted over the network (no other guarantees requested).

Q2.2 [3/30] Suppose you are requested to ensure the integrity of a file but you are only allowed to use AES (and a symmetric key): what can it be done?

Q3: **Diffie-Hellman**

Q3.1 [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.

Q3.2 [3/30] Generalize Diffie-Hellman so that three parties can establish a shared secret key.

Q3.3 [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 Q3.1 still hold?

Q4: **Leader selection**

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

<table>
<tr><td>$A \rightarrow B$: N_A</td><td>{ A chooses nonce N_A }</td></tr>
<tr><td>$B \rightarrow C$: ($N_{AB} = N_A$ ^ N_B)</td><td>{ B chooses nonce N_B and sends $N_{AB} = N_A$ ^ N_B, where ^ is the ex-or operation}</td></tr>
<tr><td>$C \rightarrow A$: ($N_{ABC} = N_{AB}$ ^ N_C)</td><td>{ C chooses nonce N_C and sends $N_{ABC} = N_{AB}$ ^ N_C }</td></tr>
<tr><td colspan="2">{ Now both A and C know N_{ABC} }</td></tr>
<tr><td>$A \rightarrow B$: N_{ABC}</td><td>{ Now B knows N_{ABC}, too }</td></tr>
<tr><td colspan="2">{ Each of the three parties can now compute p = N_{ABC} mod 3, where p = 0 denotes A, p = 1 denotes B, and p = 2 denotes C }</td></tr>
</table>

Q4.1 [1/30] 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, while the others are not aware of the fraud?

Q4.2 [3/30] Fix the protocol.

Q5: **Shamir**

Q5.1 [3/30] Describe the Shamir scheme (k, n) for sharing a secret.

Q5.2 [3/30] Make a numerical example for the case (2, 4), for sharing the secret number 6. Show how the 4 fragments are computed.

Q6: **Access control**

Q6.1 [2/30] 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.

Q6.2 [2/30] Why is the DAC model vulnerable to Trojans? What type of access control model can prevent them from illegally accessing private data? Discuss.

Q7: **Miscellaneous**

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

Q7.1 [1/30] RSA: if *p* = 13 and *q* = 17, what is the range for exponent *e*?

Q7.2 [1/30] Can iptables block incoming datagrams that are IPSec-tunneled packets going to port 25?

Q7.3 [1/30] What is port forwarding and what protocol implements it?

Cybersecurity/CNS exam

14th July 2022

Syllabus 2021-22

Please write in a large and understandable handwriting, using a pen. Any pencil portions will be skipped. If necessary, use capital or block letters.

1. Write the name of the exam, first name, surname, matriculation and number of homeworks done in the top line of the first page.

2. Define *weak collision resistance*. Is it needed for making a hashing function of cryptographic quality? What is the difference with *second preimage resistance*? [3pt]

3. Why do we want hashing *fingerprints* longer than 160 bits? [3pt]

4. Compare *keyed hashing functions* to *digital signatures*: pros and cons. [3pt]

5. Explain how *authenticity* is a strengthening of *integrity*. [3pt]

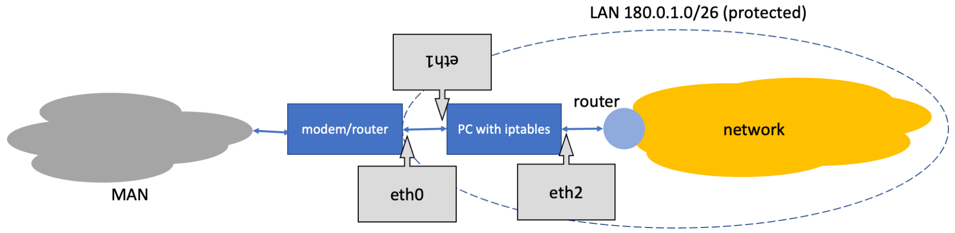
6. What are the differences between *integrity verification* and *digital signature verification*? Discuss in depth. (Superficial approaches will be penalised). [3pt]

7. Define Shamir's secret sharing technique (n, k), where n is the number of participants and $1 < k \leq n$, where k is the threshold. Given three points, will these be sufficient for $k = 3$? Discuss. [3pt]

8. Public keys checking.
   8.1. Define OCSP. How is it better than CRLs? [2pt]
   8.2. Why does OCSP cause privacy issues? [2pt]

9. RSA: What happens if we exchange public and private keys? [2pt]

10. Firewalls
    10.1. What is the difference between packet filtering and session filtering? [2pt]
    10.2. You are a home user with a strong Internet connection, however the modem/router - offering only wired connection - is not providing any firewall/NAT. Carefully check the figure.



Default iptables policy is ALLOW and you are asked to protect ALL the LAN blocking bidirectional http/https traffic to/from site 140.11.201.23. Write the corresponding iptables rules. [4pt]

    10.3. Can a session filtering firewall help confidentiality? (It cannot guarantee it, but some policies may help). Discuss. [2pt]

Cybersecurity/CNS exam

8th September 2022 - Syllabus 2021-22 - 120 minutes

Please write in a large and understandable handwriting, using a pen. Pencil portions will be skipped. If necessary, use capital or block letters.

0. Write the name of the exam, first name, surname, matriculation and number of homeworks done in the top line of the first page. (I will save time).

1. **Collision resistance**
   1.1. Define *strong* and *weak collision resistance*. [2pt]
   1.2. Why does the strong one imply the weak one? [2pt]
   1.3. Consider the mod *s* function (% *s*), where *s* is a large random prime number. Why isn't it cryptographic? Provide **all** reasons. [2pt]

2. **RSA**
   2.1. When is RSA normally used for confidentiality and why? [1pt]
   2.2. What are the keys (private and public) used for RSA and what relationship binds them? [2pt]
   2.3. What is OS2IP? Describe it in detail. [3pt]

3. **Authentication**
   3.1. Define SPEKE and all parameters/options that occur in it. [2.5pt]
   3.2. In a web application, authentication is made by requesting username and password to the user, who connects via https. Design the details of authentication, clarifying how the server checks the user's credentials. [3.5pt]

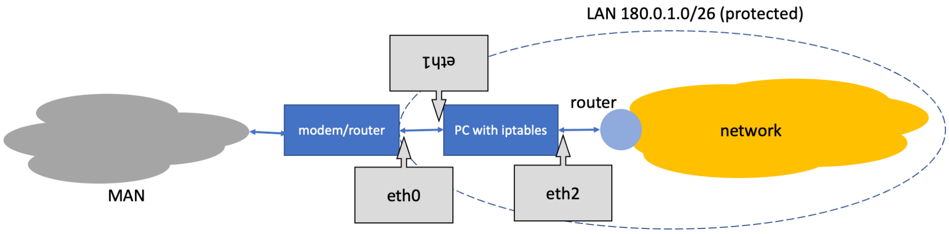
4. Explain the difference between a key and a password. [1pt]

5. A VPN is based on IPSec tunnelling. What partial (meta)information is available to an eavesdropper that intercepts the packets? [2pt]

6. Describe strengths and limits of inserting a timestamp within a message of some cryptographic protocol. [2pt]

7. **Timestamp Authority**
   7.1. What is a Timestamp Authority (TSA) and what function does it perform? [1pt]
   7.2. Illustrate a way of timestamping a digitally signed message. [2pt]
   7.3. Illustrate a way of timestamping a message without digital signature but with integrity. [2pt]

8. **Firewalls**
   8.1. What is the difference between a personal firewall and a perimeter firewall? [1pt]
   8.2. You are a home user with a strong Internet connection, however the modem/router - offering only wired connection - is **not** providing any firewall/NAT. Carefully check the figure.



Default iptables policy is ALLOW and you are asked to block all connections to the pc running iptables (and vice versa) except those initiated inside the LAN. Write the corresponding iptables rules. [3pt]

Computer and network security
Sicurezza nelle reti e nei sistemi informatici
Crittografia e sicurezza delle reti
Cybersecurity (6 of 9 credits)

Exam of 13 January 2022, a.y. 2021-22. Time: 2 hours
Outcomes will be published in web page within three weeks:
https://sites.google.com/diag.uniroma1.it/cybersecurity/exams

FOR NON-ENGLISH: 2 penalty points (applicable only to courses provided in English)

1. Cryptographic hashing functions

1.1. [2/30] State a minimal but sufficient set of conditions why a hashing function be cryptographic.

1.2. [3/30] Can I use a cryptographic hashing function for a hash table? Motivate.

1.3. [3/30] Can I use the hashing function of a hash table as a cryptographic hashing function? Motivate.

2. Authentication

2.1. [3/30] Username/password based authentication: propose a protocol for having this type of authentication in the LAN, resistant to all types of replay attacks. Can you avoid saving user passwords on the server?

2.2. [3/30] How could an authentication process be based on a public key and what are the relevant weaknesses?

2.3. [3/30] Locate the weakness in this bidirectional challenge-response authentication scheme and mitigate it:

A → B: A, Enc(a, X)
B → A: a, Enc(b, X)
A → B: b

where X is a shared secret key, Enc(y, X) denotes symmetric encryption of y by key X, a is a nonce chosen by A and b is a nonce chosen by B.

2.4. [2/30] Bob is a smart guy and knows how to invent 128-bits random passphrases (typeable on keyboard) that are robust against dictionary attacks. Alice tells him that in spite of such robustness a 128-bits random key is more secure. Bob replies that the security is the same, but the passphrase can be more easily remembered. What's your position? Explain.

3. Access control

3.1. [2/30] Is the HRU (Harrison, Ruzzo, Ullman) model secure against *offline dictionary attacks*? Explain.

3.2. [2/30] Give at least two cases where HRU is decidable. Explain.

4. Firewalls

Assume that the iptables software is running on host *H*, having a network interface eth0 (IP: 192.168.0.2) connected to a LAN (IP: 192.168.0.0/24; the LAN is protected by *H*) and a network interface eth1 (IP: 151.100.4.3) connected to the Internet. Assume that the default policy for all built-in chains is DROP.

4.1. [3/30] Since the LAN contains only local hosts with private IP addresses, it is not possible to directly contact local hosts from the Internet (no IP remapping). However, if *H* accepts, local hosts can establish two-ways communications with remote hosts on the Internet, based on TCP. For this purpose, which rules will you have to define on the perimeter firewall?

4.2. [3/30] Define suitable rules for mitigating a distributed DOS attack to *H*, based on ping-flooding. Avoid blocking/slowing down other protocols.

5. Short answer (at most 4 lines)

5.1. [2/30] Make a comparison between HMAC and digital signing for the purpose of non-repudiation.

Number of homeworks validly (within the proper deadline, or, if on late, explicitly authorized by the prof.) delivered?	

To be delivered with the exam notes written in decent handwriting

Cybersecurity/CNS exam

8th September 2022 - Syllabus 2021-22 - 120 minutes

Please write in a large and understandable handwriting, using a pen. Pencil portions will be skipped. If necessary, use capital or block letters.

0. Write the name of the exam, first name, surname, matriculation and number of homeworks done in the top line of the first page. (I will save time).

1. **Collision resistance**
   - 1.1. Define *strong* and *weak collision resistance.* [2pt]
   - 1.2. Why does the strong one imply the weak one? [2pt]
   - 1.3. Consider the mod *s* function (% *s*), where *s* is a large random prime number. Why isn't it cryptographic? Provide **all** reasons. [2pt]

2. **RSA**
   - 2.1. When is RSA normally used for confidentiality and why? [1pt]
   - 2.2. What are the keys (private and public) used for RSA and what relationship binds them? [2pt]
   - 2.3. What is OS2IP? Describe it in detail. [3pt]

3. **Authentication**
   - 3.1. Define SPEKE and all parameters/options that occur in it. [2.5pt]
   - 3.2. In a web application, authentication is made by requesting username and password to the user, who connects via https. Design the details of authentication, clarifying how the server checks the user's credentials. [3.5pt]

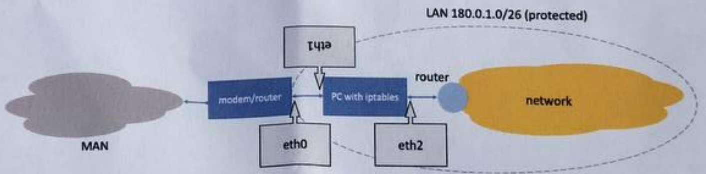
4. Explain the difference between a key and a password. [1pt]

5. A VPN is based on IPSec tunnelling. What partial (meta)information is available to an eavesdropper that intercepts the packets? [2pt]

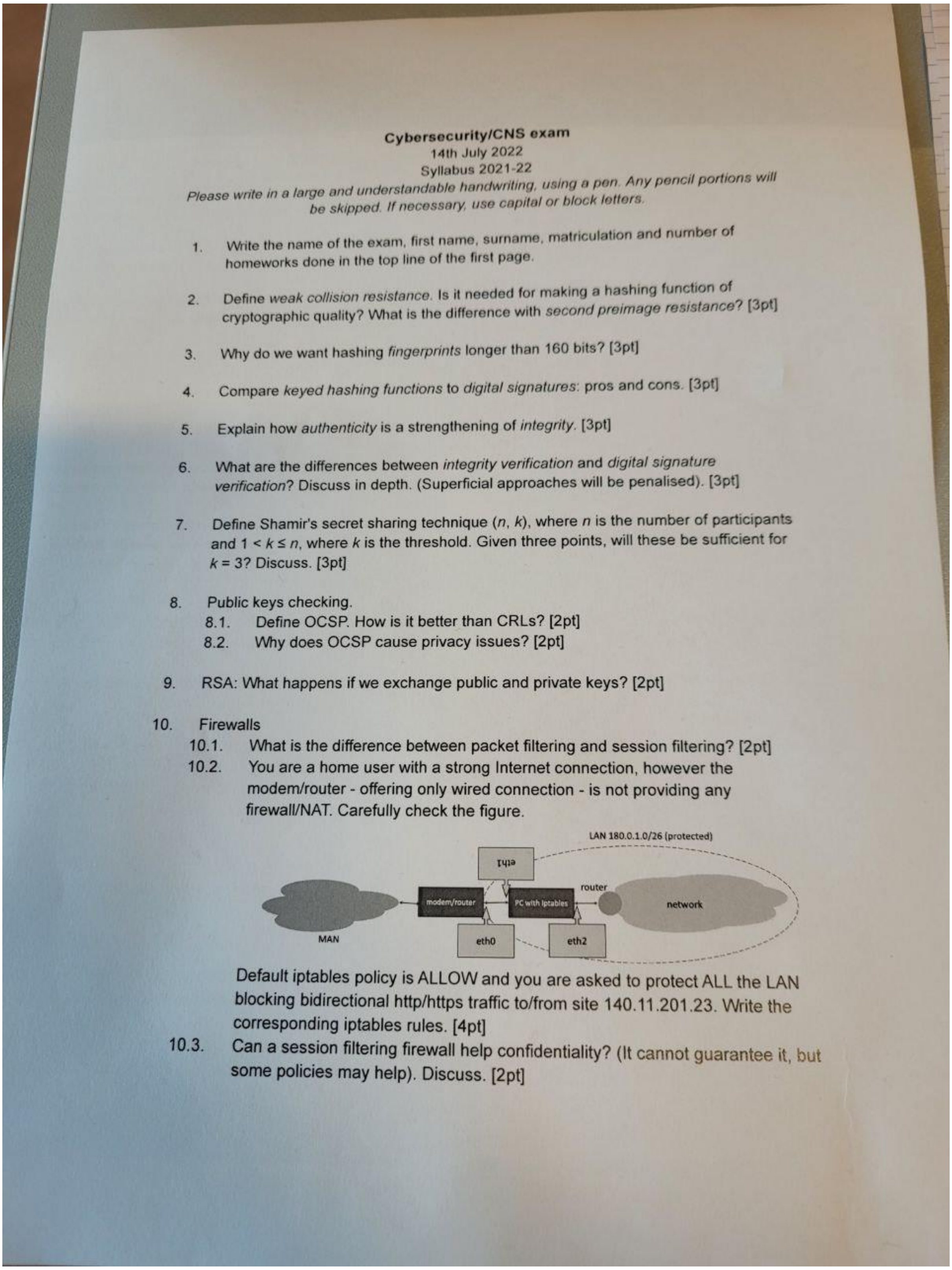
6. Describe strengths and limits of inserting a timestamp within a message of some cryptographic protocol. [2pt]

7. **Timestamp Authority**
   - 7.1. What is a Timestamp Authority (TSA) and what function does it perform? [1pt]
   - 7.2. Illustrate a way of timestamping a digitally signed message. [2pt]
   - 7.3. Illustrate a way of timestamping a message without digital signature but with integrity. [2pt]

8. **Firewalls**
   - 8.1. What is the difference between a personal firewall and a perimeter firewall? [1pt]
   - 8.2. You are a home user with a strong Internet connection, however the modem/router - offering only wired connection - is **not** providing any firewall/NAT. Carefully check the figure.



Default iptables policy is ALLOW and you are asked to block all connections to the pc running iptables (and vice versa) except those initiated inside the LAN. Write the corresponding iptables rules. [3pt]



Cybersecurity/CNS exam
14th July 2022
Syllabus 2021-22

Please write in a large and understandable handwriting, using a pen. Any pencil portions will be skipped. If necessary, use capital or block letters.

1. Write the name of the exam, first name, surname, matriculation and number of homeworks done in the top line of the first page.

2. Define *weak collision resistance*. Is it needed for making a hashing function of cryptographic quality? What is the difference with *second preimage resistance*? [3pt]

3. Why do we want hashing *fingerprints* longer than 160 bits? [3pt]

4. Compare *keyed hashing functions* to *digital signatures*: pros and cons. [3pt]

5. Explain how *authenticity* is a strengthening of *integrity*. [3pt]

6. What are the differences between *integrity verification* and *digital signature verification*? Discuss in depth. (Superficial approaches will be penalised). [3pt]

7. Define Shamir's secret sharing technique (n, k), where n is the number of participants and $1 < k \leq n$, where k is the threshold. Given three points, will these be sufficient for $k = 3$? Discuss. [3pt]

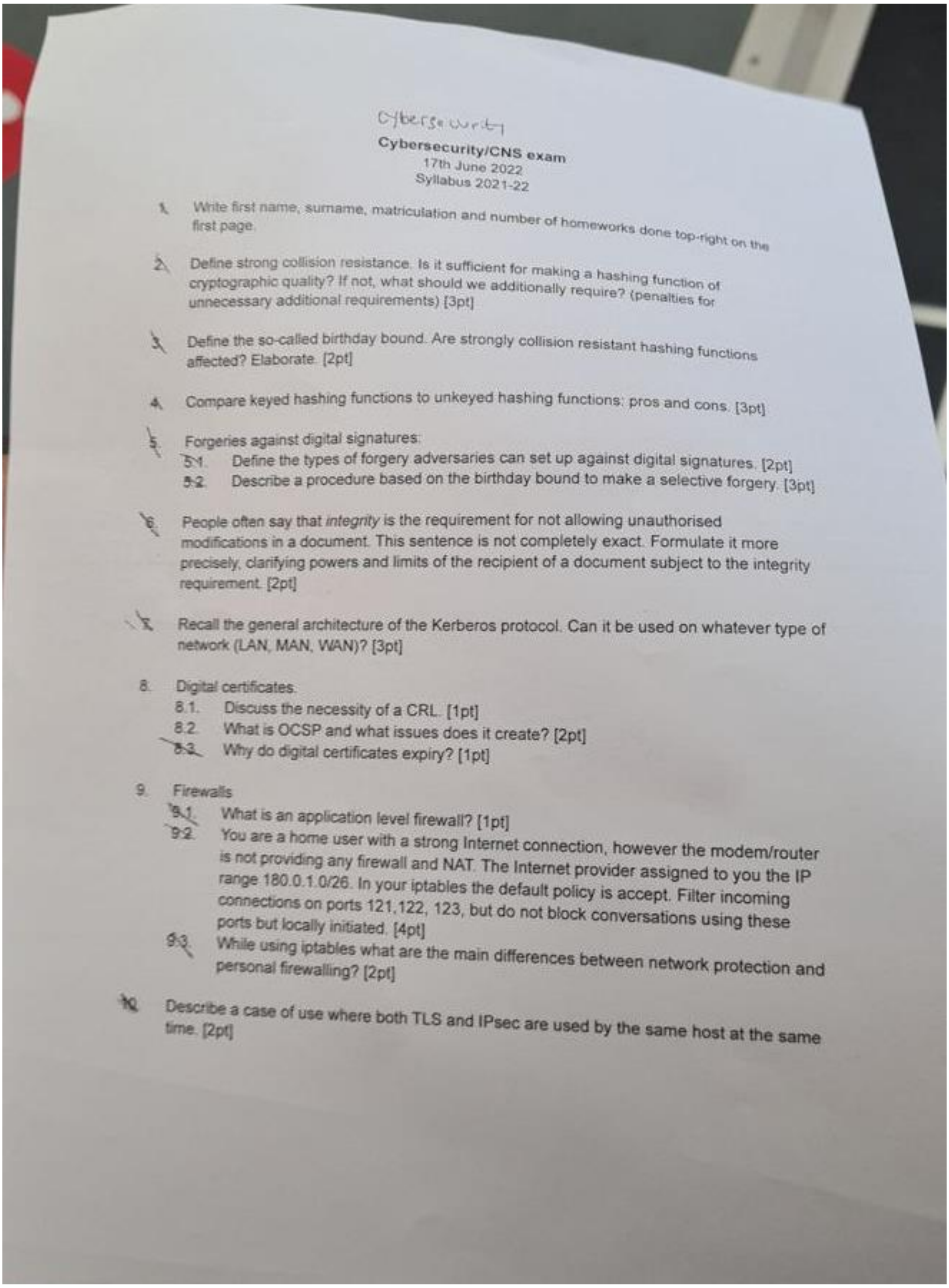
8. Public keys checking.
   8.1. Define OCSP. How is it better than CRLs? [2pt]
   8.2. Why does OCSP cause privacy issues? [2pt]

9. RSA: What happens if we exchange public and private keys? [2pt]

10. Firewalls
    10.1. What is the difference between packet filtering and session filtering? [2pt]
    10.2. You are a home user with a strong Internet connection, however the modem/router - offering only wired connection - is not providing any firewall/NAT. Carefully check the figure.

Default iptables policy is ALLOW and you are asked to protect ALL the LAN blocking bidirectional http/https traffic to/from site 140.11.201.23. Write the corresponding iptables rules. [4pt]

10.3. Can a session filtering firewall help confidentiality? (It cannot guarantee it, but some policies may help). Discuss. [2pt]



Cybersecurity

Cybersecurity/CNS exam
17th June 2022
Syllabus 2021-22

1. Write first name, surname, matriculation and number of homeworks done top-right on the first page.

2. Define strong collision resistance. Is it sufficient for making a hashing function of cryptographic quality? If not, what should we additionally require? (penalties for unnecessary additional requirements) [3pt]

3. Define the so-called birthday bound. Are strongly collision resistant hashing functions affected? Elaborate. [2pt]

4. Compare keyed hashing functions to unkeyed hashing functions: pros and cons. [3pt]

5. Forgeries against digital signatures:
   5.1. Define the types of forgery adversaries can set up against digital signatures. [2pt]
   5.2. Describe a procedure based on the birthday bound to make a selective forgery. [3pt]

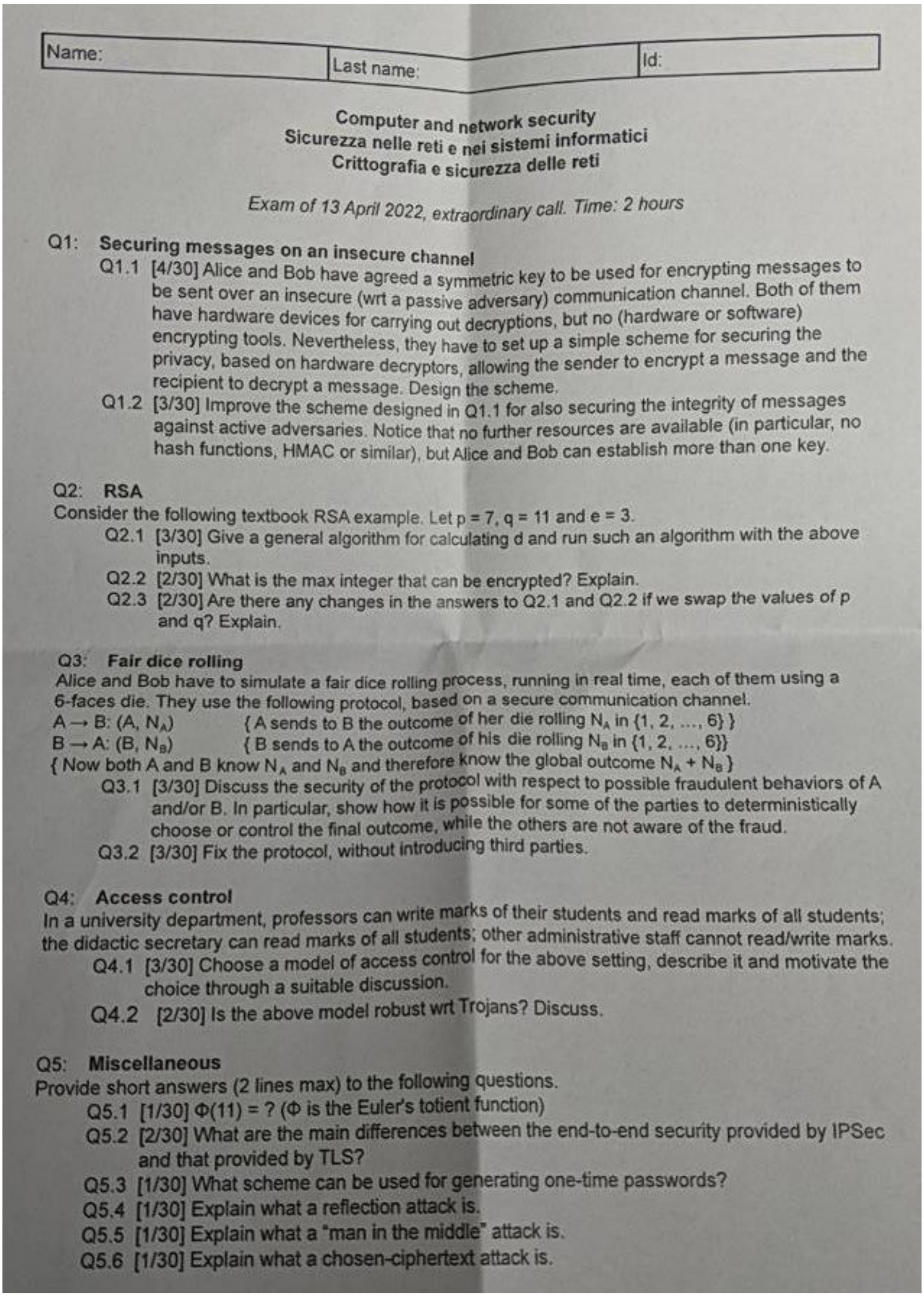
6. People often say that *integrity* is the requirement for not allowing unauthorised modifications in a document. This sentence is not completely exact. Formulate it more precisely, clarifying powers and limits of the recipient of a document subject to the integrity requirement. [2pt]

7. Recall the general architecture of the Kerberos protocol. Can it be used on whatever type of network (LAN, MAN, WAN)? [3pt]

8. Digital certificates.
   8.1. Discuss the necessity of a CRL. [1pt]
   8.2. What is OCSP and what issues does it create? [2pt]
   8.3. Why do digital certificates expiry? [1pt]

9. Firewalls
   9.1. What is an application level firewall? [1pt]
   9.2. You are a home user with a strong Internet connection, however the modem/router is not providing any firewall and NAT. The Internet provider assigned to you the IP range 180.0.1.0/26. In your iptables the default policy is accept. Filter incoming connections on ports 121,122, 123, but do not block conversations using these ports but locally initiated. [4pt]
   9.3. While using iptables what are the main differences between network protection and personal firewalling? [2pt]

10. Describe a case of use where both TLS and IPsec are used by the same host at the same time. [2pt]



Name:	Last name:	Id:

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

Exam of 13 April 2022, extraordinary call. Time: 2 hours

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 decryptions, but no (hardware or software) encrypting tools. Nevertheless, they have to set up a simple scheme for securing the privacy, based on hardware decryptors, 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: RSA

Consider the following textbook RSA example. Let $p = 7$, $q = 11$ and $e = 3$.

Q2.1 [3/30] Give a general algorithm for calculating d and run such an algorithm with the above inputs.

Q2.2 [2/30] What is the max integer that can be encrypted? Explain.

Q2.3 [2/30] Are there any changes in the answers to Q2.1 and Q2.2 if we swap the values of p and q? Explain.

Q3: Fair dice rolling

Alice and Bob have to simulate a fair dice rolling process, running in real time, each of them using a 6-faces die. They use the following protocol, based on a secure communication channel.

$A \rightarrow B$: (A, N_A) { A sends to B the outcome of her die rolling N_A in $\{1, 2, \ldots, 6\}$ }
$B \rightarrow A$: (B, N_B) { B sends to A the outcome of his die rolling N_B in $\{1, 2, \ldots, 6\}$}
{ Now both A and B know N_A and N_B and therefore know the global outcome $N_A + N_B$ }

Q3.1 [3/30] Discuss the security of the protocol with respect to possible fraudulent behaviors of A and/or B. In particular, show how it is possible for some of the parties to deterministically choose or control the final outcome, while the others are not aware of the fraud.

Q3.2 [3/30] Fix the protocol, without introducing third parties.

Q4: Access control

In a university department, professors can write marks of their students and read marks of all students; the didactic secretary can read marks of all students; other administrative staff cannot read/write marks.

Q4.1 [3/30] Choose a model of access control for the above setting, describe it and motivate the choice through a suitable discussion.

Q4.2 [2/30] Is the above model robust wrt Trojans? Discuss.

Q5: Miscellaneous

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

Q5.1 [1/30] $\Phi(11) = ?$ (Φ is the Euler's totient function)

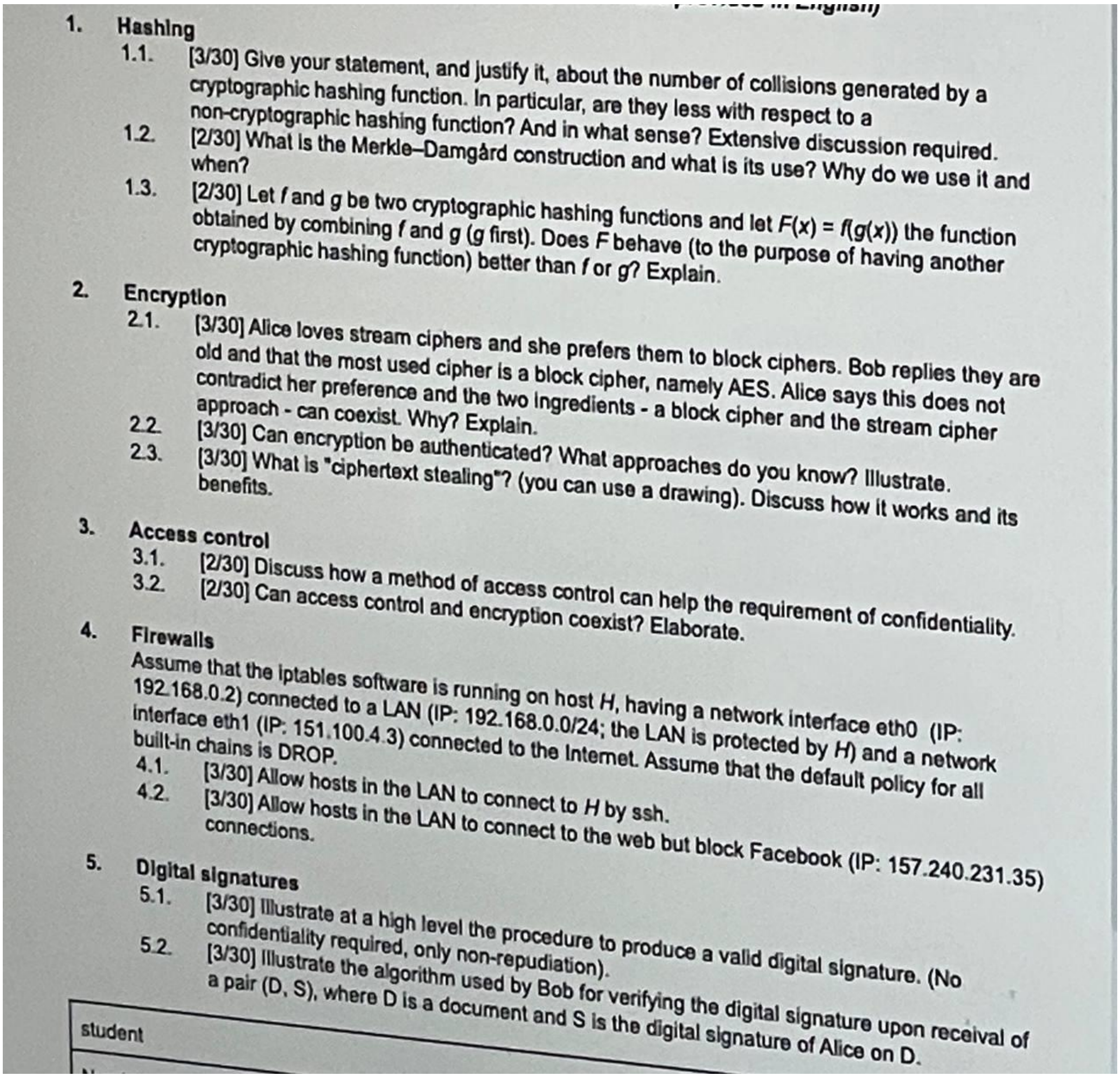
Q5.2 [2/30] What are the main differences between the end-to-end security provided by IPSec and that provided by TLS?

Q5.3 [1/30] What scheme can be used for generating one-time passwords?

Q5.4 [1/30] Explain what a reflection attack is.

Q5.5 [1/30] Explain what a "man in the middle" attack is.

Q5.6 [1/30] Explain what a chosen-ciphertext attack is.



in English)

1. **Hashing**
   - 1.1. [3/30] Give your statement, and justify it, about the number of collisions generated by a cryptographic hashing function. In particular, are they less with respect to a non-cryptographic hashing function? And in what sense? Extensive discussion required.
   - 1.2. [2/30] What is the Merkle–Damgård construction and what is its use? Why do we use it and when?
   - 1.3. [2/30] Let *f* and *g* be two cryptographic hashing functions and let $F(x) = f(g(x))$ the function obtained by combining *f* and *g* (*g* first). Does *F* behave (to the purpose of having another cryptographic hashing function) better than *f* or *g*? Explain.

2. **Encryption**
   - 2.1. [3/30] Alice loves stream ciphers and she prefers them to block ciphers. Bob replies they are old and that the most used cipher is a block cipher, namely AES. Alice says this does not contradict her preference and the two ingredients - a block cipher and the stream cipher approach - can coexist. Why? Explain.
   - 2.2. [3/30] Can encryption be authenticated? What approaches do you know? Illustrate.
   - 2.3. [3/30] What is "ciphertext stealing"? (you can use a drawing). Discuss how it works and its benefits.

3. **Access control**
   - 3.1. [2/30] Discuss how a method of access control can help the requirement of confidentiality.
   - 3.2. [2/30] Can access control and encryption coexist? Elaborate.

4. **Firewalls**

   Assume that the iptables software is running on host *H*, having a network interface eth0 (IP: 192.168.0.2) connected to a LAN (IP: 192.168.0.0/24; the LAN is protected by *H*) and a network interface eth1 (IP: 151.100.4.3) connected to the Internet. Assume that the default policy for all built-in chains is DROP.
   - 4.1. [3/30] Allow hosts in the LAN to connect to *H* by ssh.
   - 4.2. [3/30] Allow hosts in the LAN to connect to the web but block Facebook (IP: 157.240.231.35) connections.

5. **Digital signatures**
   - 5.1. [3/30] Illustrate at a high level the procedure to produce a valid digital signature. (No confidentiality required, only non-repudiation).
   - 5.2. [3/30] Illustrate the algorithm used by Bob for verifying the digital signature upon receival of a pair (D, S), where D is a document and S is the digital signature of Alice on D.

student