

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

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

Exam of 21 June 2023, a.y. 2022-23. Time: 2 hours

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

FOR UNREADABLE WRITING: arbitrary penalty points

Q1: Symmetric ciphers

- Q1.1 [1/30] Describe the scenario of symmetric ciphers and define the concepts of: synchronous/asynchronous stream ciphers, block ciphers and modes of operations.
 [If definition is wrong subsequent questions cannot be correctly answered]
- Q1.2 [3/30] Describe the RC4 cipher (both the key generation and the encryption process). What type of cipher is it?
- Q1.3 [4/30] Describe and compare OFB and CTR. Can you suggest possible design criteria for their adoption?

Q2: Man in the middle

- Q2.1 [2/30] Describe the attack *Man-In-The-Middle*, as well as a possible scenario where it could be run.
- Q2.2 [2/30] Alice suspects she is currently being the target of a *Man-In-The-Middle* attack, and she decides to hire you as a personal adviser. Is it still possible to carry out safe actions? Discuss.

Q3: Hashing

- Q3.1 [2/30] Define the properties that qualify a hashing function as cryptographic (the more formal, the better).
- Q3.2 [2/30] Describe the Merkle-Damgård construction. If the underlying hash function maps 256b blocks into 128b blocks, how many rounds are required for hashing a 140KB file?
- Q3.3 [2/30] Discuss and compare possible schemes for keying a hash function.

Q4: RSA verification

- Q4.1 [2/30] Describe how to verify an RSA digital signature.
- Q4.2 [2/30] Explicitly describe the possible causes of a verification failure.
- Q4.3 [2/30] For having non-repudiation is the verification needed? [2/30].

Q5: Authentication

- Q5.1 [2/30] Discuss the security of the following challenge-based scheme for mutual authentication, where Alice (A) and Bob (B) share a secret key K: (information below is transmitted as clear text)
- A -> B: (A, NA, B) { NA is a nonce chosen by A }
- B -> A: (B, NB, K(NA), A) { NB is a nonce chosen by B }
- A -> B: (A, K(NB), B)
- Q5.2 [2/30] How would you improve the above schema?

Name:

Last name:

Id:

Q6: Miscellaneous

Provide short answers to the following questions.

Q6.1 [2/30] Compute $5^{12241} \bmod 13$.

Q6.2 [2/30] Describe as best as you can the meaning of the following command `iptables -A INPUT -p tcp -s 0/0 -d 195.55.55.78 --sport 513:65535 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT`

Q6.3 [2/30] Describe as best as you can the meaning of the following command `ssh -L 44044:192.168.1.221:22 user@host.example.com`

HAVE YOU SENT 2022-23 HOMEWORKS? YES/NO (circle your answer)

If YES:

I hereby confirm that I sent the following contributions:

Signature
