CNS/Cybersecurity exam
October 25, 2022

- *Please write with good handwriting, big letters (small characters will be ignored) and ensure you are using a pen (and not a pencil)*
- *Write (on each independent sheet) top-right name, surname, matricola, name of your exam*

1. **Data integrity**
   - 1.1. Define the concept of data integrity [1pt]
   - 1.2. Illustrate the difference between data integrity and authenticity [1pt]
   - 1.3. Can you see any use case where the integrity requirement is not requested? [1pt]
   - 1.4. Show that using the CBC technique for providing a Message Authentication Code is failing for variable-lengths messages. [3pt]
2. **Digital sign**. Alice is sending to Bob a digitally signed file.
   - 2.1. How does Bob verify the signature? [2pt]
   - 2.2. What checks are necessary on the digital certificate? [1pt]
   - 2.3. Is the digital signature still valid after the expiration of Alice's certificate? Explain. [1.5pt]
3. **Hashing functions**
   - 3.1. What is a password based key derivation function? [2pt]
   - 3.2. What is a "rainbow table"? [2pt]
   - 3.3. Given a hash function, is the property of being cryptographic retained forever? [2pt]
   - 3.4. Describe the case where the keyed hashing h(m||k) - where is the message and k is the secret key - is insecure. [2pt]
4. **Symmetric encryption**
   - 4.1. What is a perfect cipher? Give the mathematical definition. [2pt]
   - 4.2. Under what conditions is OTP perfect? [1.5pt]
   - 4.3. Why is it dangerous reusing the same keystream in OTP? [2pt]
   - 4.4. Carefully describe the Meet-in-the-Middle attack. [3pt]
   - 4.5. What is "key whitening"? Why and how is it made? [2pt]
5. **Firewalls**
   - 5.1. Can a packet filtering firewall detect malware? Discuss. [2pt]
   - 5.2. Provide the iptables rules for the following scenario: [3pt]
     - 5.2.1. Default policy is allow for all chains
     - 5.2.2. Packets are delivered to the LAN through the ethernet adapter eth0
     - 5.2.3. TCP segments are delivered to the LAN with a maximum speed of 3 per second (other segments will be dropped)

Honours for points not less than 32 (without approximation)