Cybersecurity/CNS exam

9 January 2023

- Don't use pencils
- Have a good (and big) handwriting
- Use English
- Answers without a motivation will be not considered

0. Write name, surname, matriculation and number of delivered homeworks in the top right corner of first page

1. **Hashing** [9 points]
   1.1. What are pros and cons of keyed and unkeyed hashing? No definition needed. [2 points] ✓
   1.2. Do cryptographic hash functions have less collision than non-cryptographic hashing functions? Elaborate (no definition needed) [2 points] ✓
   1.3. Why are strongly collision-resistant functions also weakly collision-resistant? [3 points] ~
   1.4. Is the traditional binary representation of integers a cryptographic hash function? Explain [2 points] ✓

2. **Key exchange**. Describe at least two methods used for letting two parties exchange a secret key. [3 points] ✓

3. **Authentication** [10 points]
   3.1. Why do servers that authenticate users with Lamport hashing prefer that the user always use the same device? [3 points]
   3.2. With reference to password-based authentication, describe a (any) protocol to make client and server talk so that the client supplies the password but prevents replay and reflection attacks. [4 points] ✓
   3.3. Can digital signature (whatever it is) authenticate a user of a web application? Discuss [3 points] ✓

4. **Shamir secret sharing** [5 points]
   4.1. In a Shamir scheme (2, 5) users got the points A=(1, 5), B=(2, 0), C=(3, 2), D=(4, 4) and E=(5, 6). Assume to work on GF(7). Reconstruct and return the secret starting from the points A and B. [3 points]
   4.2. Reconstruct again the secret starting from D and E, and verify that the secret is the same. [2 points]

5. **Firewalls** [5 points]
   5.1. When iptables is used as a personal firewall is there any case where the routing chain needs to be configured with rules? [1 point] ✓ FORWARD
   5.2. Suppose iptables is running on host H which is protecting a LAN, from which it can be reached with the IP 192.168.1.254/24. Write appropriate rules so that the only network connection allowed to H is via ssh (two-way talk) to the LAN host 192.168.1.2/24 to allow firewall configuration. All other network connections to and from H are prohibited. [4 points] ✓