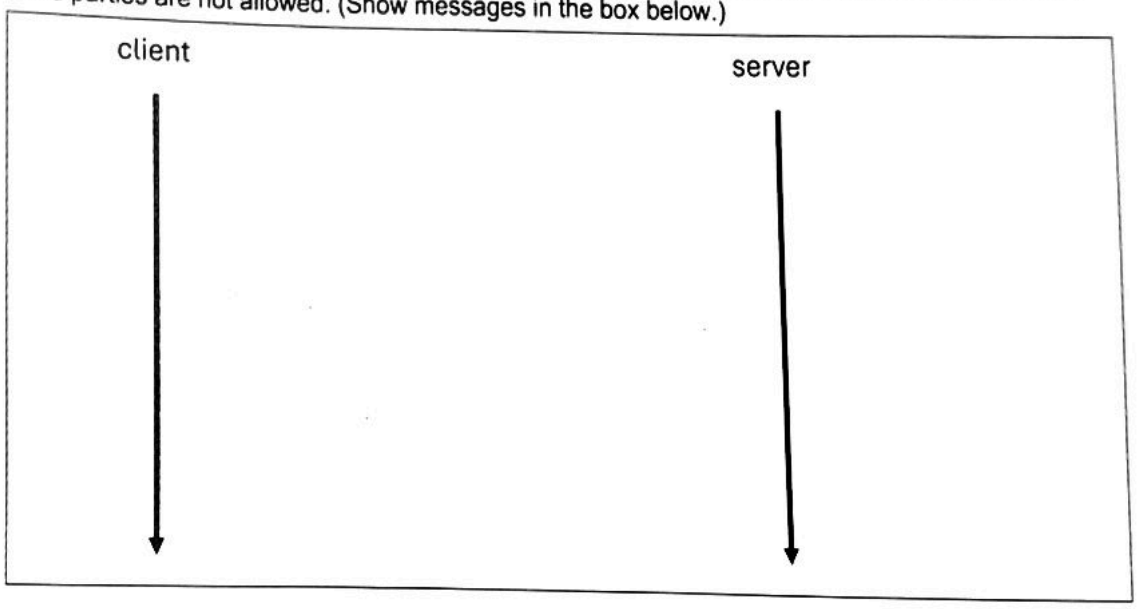
SURNAME	FIRST NAME	MATRICOLA	# of HWs

complete the assignment by using this sheet – don't write in small letters and in case of bad handwriting use block letters

1. [0–3] Determine whether the function $f(x) = (ax + b) \bmod p$, where p is a prime number and a, b are positive integers, qualifies as a cryptographic hash function. Justify your reasoning. (Definitions not expressly requested are taken for granted.)

2. [0–7] Design a detailed authentication protocol for a client-server application in which the server securely stores information derived from user passwords to facilitate login. The protocol should meet the following criteria:
   a. It must reliably distinguish between legitimate and illegitimate users.
   b. It must be robust against replay and reflection attacks.
   c. The protocol should operate over an unsecured plain connection between the client and the server, without relying on secure protocols such as TLS, IPsec, or similar.

   Provide a step-by-step description of each message exchanged during the authentication process. Third parties are not allowed. (Show messages in the box below.)



3. [0–4] What is the exact meaning of the following OpenSSL command line? Explain each option in it.

```
openssl rsa -in privatekey.pem -outform PEM -pubout -out publickey.pem
```

4. [0–3] What is the meaning of the following line? Explain each part:

```
age -p -output x test.txt
```


students who have been granted a reduction in the assignment may OMIT questions 3 and 6

5. [0–5] Provide a set of iptables rules to allow firewall access only via ssh from LAN IP 1.2.3.4. The stricter the rule, the better. Default is blacklisting; firewall-LAN network adapter is eth1.

6. [0–5] Describe the sequence of messages in Kerberos (from the initial login) to allow Alice (in Wonderland realm) to use the services of Bob that is in the Oz realm.

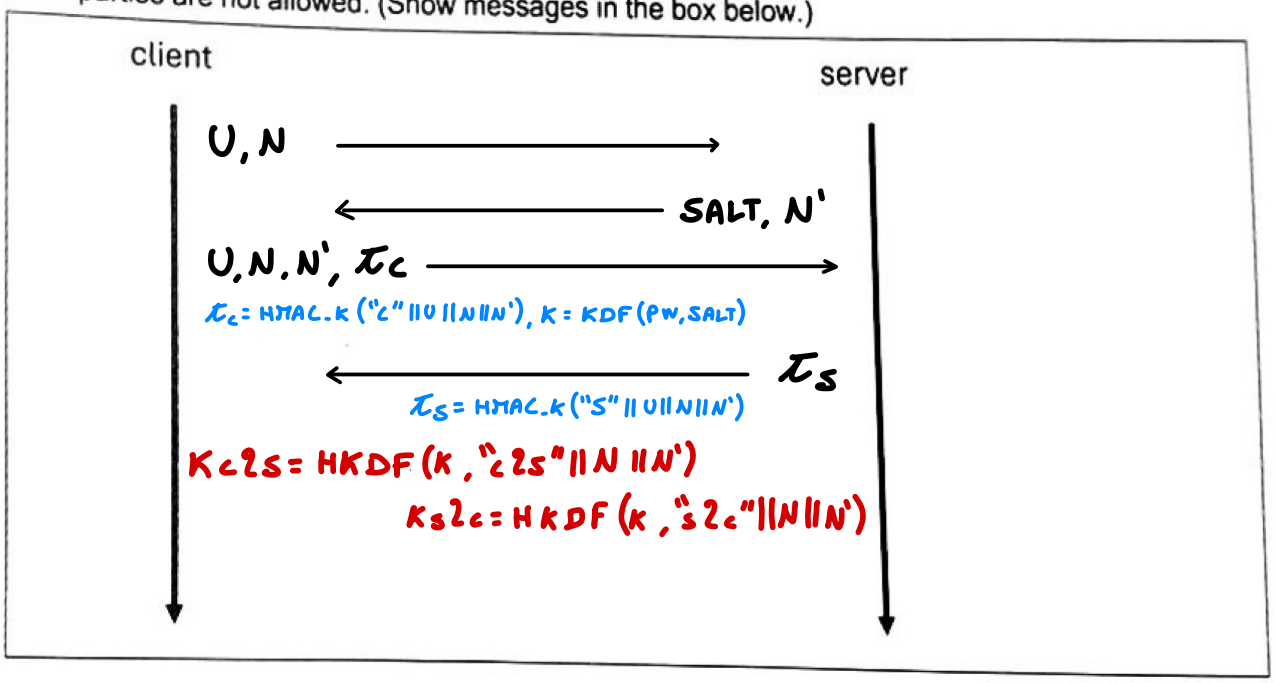
7. [0–5] Provide a complete list of steps to perform a digital signature verification

1. [0–3] Determine whether the function $f(x) = (ax + b) \bmod p$, where p is a prime number and a, b are positive integers, qualifies as a cryptographic hash function. Justify your reasoning. (Definitions not expressly requested are taken for granted.)

?

2. [0–7] Design a detailed authentication protocol for a client-server application in which the server securely stores information derived from user passwords to facilitate login. The protocol should meet the following criteria:
   a. It must reliably distinguish between legitimate and illegitimate users.
   b. It must be robust against replay and reflection attacks.
   c. The protocol should operate over an unsecured plain connection between the client and the server, without relying on secure protocols such as TLS, IPsec, or similar.

Provide a step-by-step description of each message exchanged during the authentication process. Third parties are not allowed. (Show messages in the box below.)



3. [0–4] What is the exact meaning of the following OpenSSL command line? Explain each option in it.

```
openssl rsa -in privatekey.pem -outform PEM -pubout -out publickey.pem
```

THIS COMMAND EXTRACTS THE PUBLIC KEY FROM AN RSA PRIVATE KEY.

- -IN PRIVATEKEY.PEM SPECIFIES THE PRIVATE KEY IN INPUT
- -OUTFORM PEM SETS THE OUTPUT FORMAT TO PEM
- -PUBOUT TELLS OPENSSL TO OUTPUT THE CORRESPONDING PUBLIC KEY RATHER THAN THE PRIVATE KEY
- -OUT PUBLICKEY.PEM DEFINES THE OUTPUT FILE WHERE THE PUBLIC KEY WILL BE WRITTEN

4. [0–3] What is the meaning of the following line? Explain each part:
   `age -p -output x test.txt`

THIS COMMAND ENCRYPTS THE FILE TEST.TXT WITH A PASSPHRASE.
-P ENABLES PASSWORD-BASED ENCRYPTION
-OUTPUT X SPECIFIES THAT THE ENCRYPTED RESULT SHOULD BE WRITTEN TO THE FILE X

5. [0–5] Provide a set of iptables rules to allow firewall access only via ssh from LAN IP 1.2.3.4. The stricter the rule, the better. Default is blacklisting; firewall-LAN network adapter is eth1.

TO RESTRICT SSH ACCESS ONLY TO THE HOST 1.2.3.4 ON INTERFACE ETH1, WE ADD IPTABLES RULES THAT ACCEPT NEW AND ESTABLISHED TCP CONNECTIONS TO PORT 22 FROM THAT ADDRESS, ALLOW CORRESPONDING REPLIES, AND DROP ALL OTHER SSH ATTEMPTS. THIS ENSURES ONLY 1.2.3.4 CAN REACH THE FIREWALL VIA SSH, WHILE ALL OTHER TRAFFIC ON PORT 22 IS DENIED.

```
IPTABLES -A INPUT -i ETH1 -P TCP -S 1.2.3.4 --DPORT 22
-m CONNTRACK --CTSTATE NEW,ESTABLISHED -J ACCEPT

IPTABLES -A OUTPUT -O ETH1 -P TCP -D 1.2.3.4 --SPORT 22
-m CONNTRACK --CTSTATE ESTABLISHED -J ACCEPT

IPTABLES -A INPUT -I ETH1 -P TCP --DPORT 22 -J DROP
```

6. [0–5] Describe the sequence of messages in Kerberos (from the initial login) to allow Alice (in Wonderland realm) to use the services of Bob that is in the Oz realm.

ALICE FIRST AUTHENTICATES IN HER REALM WONDERLAND AND OBTAINS A TGT FROM THE LOCAL AS FOR THE LOCAL TGS. SHE THEN ASKS THE LOCAL TGS FOR A CROSS REALM TICKET TO THE TGS OF OZ. WITH THIS TICKET, SHE CONTACTS THE TGS OF OZ AND OBTAINS A SERVICE TICKET FOR BOB. FINALLY SHE PRESENTS THIS TICKET TO THE SERVER.

7. [0–5] Provide a complete list of steps to perform a digital signature verification

TO VERIFY A DIGITAL SIGNATURE, THE VERIFIER COMPUTES THE HASH OF THE RECEIVED MESSAGE, USES THE SIGNER'S PUBLIC KEY TO PROCESS THE SIGNATURE AND RECOVER THE EXPECTED HASH, AND THEN COMPARES THE TWO VALUES. IF THEY MATCH, THE SIGNATURE IS VALID, PROVING BOTH AUTHENTICITY AND INTEGRITY.