1 **a)** The “X.800 Security Architecture for OSI” defines attacks, services, and mechanism for network security. Briefly describe this standard.

b) You can apply security in different ways to any of the levels in the protocol stack. Why do you choose to implement something either high up or low down in the stack? You can give some examples to prove your point.

c) Describe the concepts Attack Surface. Give some examples on how the attack surface for an IoT device like a surveillance camera can look like.

(4+6+4 p)

2 **a)** To encipher the large messages, which one would be more suitable out of symmetric-key, or asymmetric-key cryptography? Also please justify the answer with reasoning.

b) Please apply Playfair cipher for the encryption and decryption of plaintext = WORLD and key = SECURE. Please solve with all the necessary steps.

c) What is the main issue with the double DES? Please suggest the possible solution used to address it with motivation.

(4+4+4 p)

3 **a)** Please explain Message Authentication Code where authentication is tied with ciphertext with a block diagram.

b) The most common attack in the Public Key Distribution under asymmetric-key cryptography is the man in the middle attack (MITMA). So, please suggest the most appropriate methodology to broadcast the public key in an authorized manner and avoid the MITMA.

c) Please explain KERBEROS in detail concerning secured key distribution among parties with a block diagram.

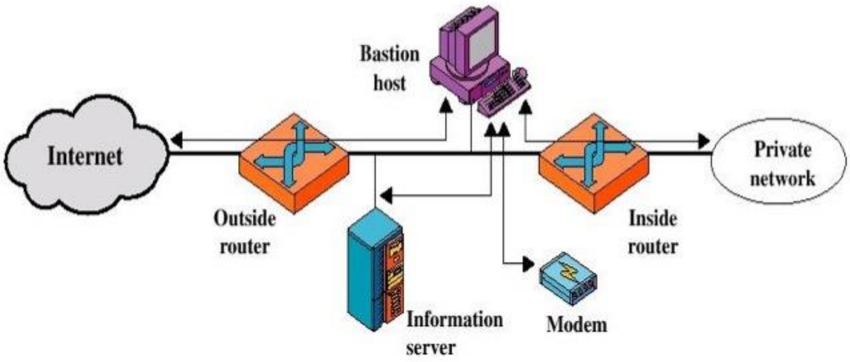
(4+4+4 p)

4 **a)** S/MIME is an alternative to PGP for email security. What are the most important differences between S/MIME and PGP?

b) S/MIME and PGP offer end-to-end security. If you don’t use either of them, you are potentially vulnerable to attacks targeting your emails in transit between users. What standards can help to improve the security in this situation and how do they do it?

(4+6 p)

5 **a)** In the figure below you can see a typical firewall configuration, the Screened-subnet firewall system. Describe the different parts in the figure and in what way they help to secure the system.



b) Firewall testing is a complex task with many areas to consider. Describe some of the tasks you should do during firewall testing and the tools to use for it.

(6+6 p)

6 **a)** IT Security threats are constantly changing. Some of the recent threats we have seen are:

- Ransomware attacks
- Supply Chain Attacks (e.g. the Solarwinds attack)
- Social engineering attacks

Give a short description of each of these threats and what the purpose of them are.

b) One way to deal with some of these types of attacks is via an **intrusion detection system**. Give a short description of such a system and the different parts that it can have.

c) What purpose has audit logs in such systems?

(6+4+4 p)

7 **a) 3D Secure** is a security standard that might be used by a web shop. Describe the main architecture of 3D Secure and the problems it is meant to solve.

b) The concept **Electronic money** can be defined in a narrow or a broad view. What is the broad definition? Where does crypto currencies like **Bitcoin** fit into this area?

c) Describe briefly how mobile payments (e.g. Apple Pay) are secured.

(6+4+4 p)