1 **a)** There are many standards meant to raise Internet Security; “OWASP Top Ten” and “X.800 Security Architecture for OSI” are two of them. Briefly describe the content and purpose of each of them.

b) Internet Security is strongly associated with the TCP/IP model for data communication. Give one example on each of the five levels in that model of some security feature (technique/standard) that is appropriate to implement on that level.

c) Describe the concepts Attack Surface. Give some examples on how the attack surface for a USB flash drive can look like.

(4+6+4 p)

2 **a)** One of the main complications of symmetric key encryption is that it entails a secure and reliable channel for the shared key exchange. So please suggest and explain how a public channel can be used to create a confidential shared key.

b) Apply Playfair cipher for the encryption and decryption of plaintext = HEMANT and key = TEACHER.

(6+6 p)

3 **a)** During Simple Authentication Dialogue, how does plaintext transmission of password affect the operation? What is the best alternative to address it? Please explain?

b) Explain the hash function-based authentication process (method), which covers the message authentication and introduces confidentiality. Also, must have added features in terms of secret key?

(6+6 p)

4 **a)** In a system for Network access you can define three important components. These are an **Access requester**, a **Policy Server** and a **Network access server**. Describe what tasks each of these components have.

b) One important protocol for Network access is EAP. EAP together with 802.1X and EAPOL form a layer between the physical network and the devices. Briefly describe these three protocols.

(6+6 p)

5 **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)

6 **a)** Malware is a term used for many different types of malicious software. What do they have in common? How can we classify different types of Malware?

b) There are many different types of Malware. Shortly describe the types below:

- Virus
- Worm
- Keylogger
- Trojan horse

(4+4 p)

7 **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) Such a system can be complemented with a **Honey Pot** system. What is that and what is its purpose?

(6+4+2 p)