**1** **a)** Security threats in a network can be handled by looking at the objectives that you have for the security. One model for this is the CIA model. Additional goals can be **Authentication**, **Non-repudiation** and **Authorization**. Briefly describe these additional goals.

**b)** In the CIA model for security you can further define C as **Data Confidentiality** and **Privacy**. You can also break down I as **Data Integrity** and **System Integrity**. Briefly describe these four areas.

**c)** One model for network security is the Network Access Security Model. One component in this model is a Gatekeeper function. Describe this model and the type of threats it can be applied to.

(4+4+4 p)

**2** **a)** Apply Vigenère Cipher for the encryption first to calculate the cipher and then apply decryption on that cipher to calculate plaintext. Please follow complete procedure and steps of the methods. Given plaintext = DABC and key = ABDA.

**b)** DES (or any block cipher) forms a basic building block, which encrypts/decrypts a fixed-sized block of data. We usually need to handle arbitrary amounts of data in the practice. So, what would be the best way for an arbitrary amount of information to encrypt? Please describe the best possible approach.

(6+6 p)

**3** **a)** Use the public key infrastructure (message encryption) to offer a methodology that offers confidentiality and authentication?

**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 a methodology to advertise the public key in an authorized manner and avoid the MITMA.

(6+6 p)

**4** **a)** TLS is a protocol offering transport security. What does TLS stand for? What different sub protocols are parts of TLS? Describe briefly how TLS works and how the different sub protocols work together.

**b)** Another protocol offering transport security is SSH. What does SSH stand for? What is the basic service SSH offers? Transport security is offered through tunnelling; briefly explain how that works in SSH.

(6+6 p)

**5** **a)** Security for emails requires many different considerations. One aspect of email security is the protection (confidentiality) of email delivery from the sender's email server to the recipient's email server. In the course we have discussed two different standards for this. Shortly describe these two standards and especially what the main difference is between them.

**b)** There are many different security threats concerning email. Shortly describe the types below in terms of what the actual threat is and if there a simple solution to mitigate each threat:

- Spam
- Phishing
- Spoofing

(6+6 p)

**6** **a)** IPsec offer several services (to upper layer protocols). Three of these services are **Access Control**, **Message integrity** and **Limited traffic flow confidentiality**. Shortly describe what each of these services give and how IPsec can offer them.

**b)** When you configure **IPsec** you must also define a **Security Policy Database**. What function has this database?

**c)** One of the protocols in IPsec is **IKE**. What is this protocol used for?

(6+2+2 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 older standard **SET** had a feature called **Dual Signature** that is not part of the newer standard. What was the purpose of the Dual Signature?

**c)** 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?

(6+2+4 p)