11. (a) Assume that Alice sends a message to Bob and the public key encryption algorithm is used to encrypt the message. Explain which key Alice uses to encrypt the message and how Alice authenticates Bob. [6]

(b) There are two general mechanisms to achieve authentication: Certificate Authority (CA) and Web of Trust. Discuss the differences between these two mechanisms. [8]

(c) What is a replay attack? Give two solutions to prevent replay attacks and explain how these two solutions work. [6]