Worksheet 21.1: for testing basic understanding

1 Classify each of the following statements as true or false. Some relate to encryption in general, others relate specifically to asymmetric key encryption:

A Encryption converts plain text into cipher text.

B Encryption requires an encryption algorithm that must be secret.

C The same key used to encrypt must be used to decrypt.

D Asymmetric encryption begins with a receiver having a public key and a private key.

E An individual can have many public keys.

2 Consider a scenario where an individual intends to encrypt messages before sending them to a number of associates. The encryption will be carried out using a private key.

a If the individual intends to send a public key to each associate, define the type of encryption that is going to be used.

b State what each associate would wish to be confident about when a message is received.

c To ensure that associates can be confident, explain what the individual should do before sending the public key.

d Name the type of organisation involved in this.

3 Each word identifies a concern regarding the transmission of encrypted data between two parties. Match each word with the correct explanation.

Authenticity	Nothing should happen to prevent the receiver from receiving the transmission.
Availability	Only the intended recipient should be able to decrypt the ciphertext.
Confidentiality	The receiver must be certain who sent the ciphertext.
Integrity	Neither sender nor receiver should be able to deny involvement in the transmission.
Non-repudiation	The ciphertext must not be modified during transmission

4 Consider a scenario where A is sending a message to B and wishes to confirm B's identity. A has a public key and a private key plus B's public key. B has a public key and a private key plus A's public key. Choose the correct word or phrase from the list, A–E, to complete the blank spaces in the following paragraph describing the steps involved in the process. Each word or phrase may be used more than once.

To begin the process, A uses a public _____ to create a _____ from the message. The _____ is encrypted with A's _____ to produce a _____ which is sent to B. A also uses B's _____ to encrypt the message which is also sent to B.

At the receiving end B decrypts the _____ using A's _____ to recreate the _____. Then B decrypts the message using B's _____. Finally, B uses the public _____ to create a _____ from the message which should be the same as the other _____.

A digest

B digital signature

C one-way hash function

D private key

E public key

5 This question refers to the process of obtaining a digital certificate so that a receiver of a transmission can be confident of the identity of its sender. Sort the activities into the correct sequential order by labelling them with a sequence number:

A The individual sends their public key to the Certification Authority.

B The Certification Authority confirms the identity of the individual.

C The Certification Authority uses encryption with their private key to add a digital signature to the digital certificate.

D An individual who is a would-be receiver and has a public–private key pair contacts a local Certification Authority.

E The Certification Authority creates a digital certificate and writes the individual's public key into this document.

F The individual posts the digital certificate on a website.

G The digital certificate is given to the individual.

H Any other individual can download the signed digital certificate and use the Certification Authority's public key to extract the first individual's public key from the digital certificate.

6 **a** Secure Socket Layer is the name of a protocol. Explain the likely reasons for why this particular name was chosen.

b Explain how this protocol interacts with the TCP protocol.

7 Sort the following steps in the order that would be followed in establishing and using a secure connection for transmitting sensitive data from a client to a server. Label each step with its number in the sequence.

A Browser asks for identification.

B Browser creates, encrypts, and sends back a symmetric session key using the server's public key.

C Browser supplies URL.

D Data encrypted by browser using session key is transmitted to server.

E Server decrypts the symmetric session key using its private key and sends back an acknowledgement encrypted with the session key to start the encrypted session.

F Server sends a digital certificate plus a public key.

G Session closed.

H TCP sends acknowledgement.

I TCP sends request to establish connection.