Worksheet 21.1: for testing basic understanding

1 A True, B False, C False, D True, E True

The principles need to be understood: plain text is converted to cipher text by using an encryption algorithm with an encryption key; only the key must be a secret, not the algorithm; in symmetric encryption, there is just one key used to encrypt and then to decrypt, so this key is a secret known to both sender and receiver; in asymmetric encryption there are two different keys; an individual can have their own public key but also several public keys received from other individuals who wish to receive encrypted messages.

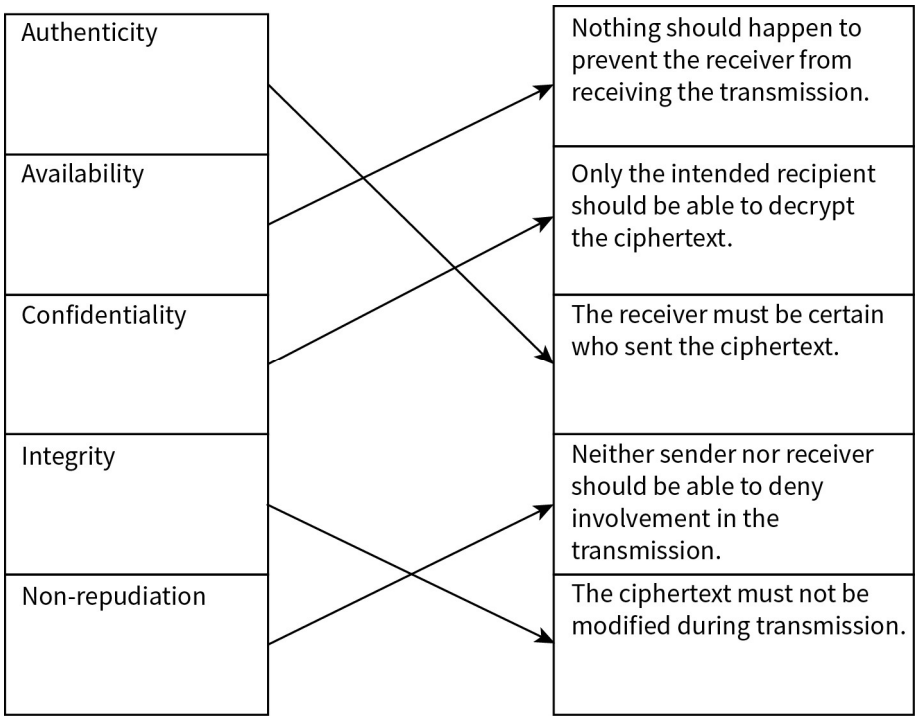
2 **a** Asymmetric

b
- That the message has been received exactly as it was sent.
- That no person could intercept and read the message during its transmission.
- That the message when sent is received by the associate.
- That the sender is the person who is claiming to be sending the message.

c The individual needs to ensure that the private key is kept secret and that the public key is made available only to those for whom it is intended. The secure method of providing the public key is to obtain a digital certificate that contains the public key.

d A Certification Authority (CA).

3



Most of these are concerns that the receiver will have. The receiver wants to be sure who sent the communication and that the communication has not been interfered with during transmission. Both sender

and receiver have a concern that the transmission will happen and both may have a concern that the transmission only reaches the appropriate receiver. The interesting one is non-repudiation. There are many cases where someone denies having information because they never received an email. The sender may wish to take steps to try to ensure that an email has been received and opened.

4 ANSWER1–one-way hash function

ANSWER2–digest

ANSWER3–private key

ANSWER4–digital signature

ANSWER5–public key

5 A 4, B 2, C 1, D 5, E 3, F 7, G 6, H 8

6 **a** In the interface between the application layer and the transport layer in the TCP/IP protocol stack, a port number is used. When a message is initially sent from the application layer, the port number to be used for any returning message has to be known. The combination of an IP address and a port number is called a socket. Because the Secure Socket Layer (SSL) protocol works between the application layer and the transport layer, in effect as a sublayer, the name seems appropriate.

b As with all application layer protocols at the initial stage, TCP sends a message to the server to establish that the server is ready to receive a communication. TCP repeats this process if necessary and proceeds to the next stage only when an acknowledgement has been received. At the next stage the SSL protocol uses its Handshake Protocol to establish a session. Every single communication is handled as usual by TCP and, in particular, TCP ensures that all packets sent are received for both directions of the communication.

7 A 3, B 9, C 8, D 1, E 6, F 2, G 5, H 4, I 7

Note that this is only an abbreviation of what is a complex process. Also note that when a client wishes to interact with a server the first step is to use TCP to establish a connection. Only after this connection has been established can a secure transmission session be established by communication between browser and server.