Exam-style Questions

1 **a** 1 mark each for any of the following up to a maximum of 4: Confidentiality is about content only being for disclosure to a specified recipient (1), the communication must ensure no interception (1), authenticity is about a receiver knowing that a communication is genuine (1) and from a genuine sender (1), integrity is about the communication received being precisely what was sent (1).

b 1 mark each for any of the following up to a maximum of 6: Encryption converts a plaintext message to ciphertext using a key (1). In symmetric encryption the same key is needed for decryption (1), which converts the ciphertext back to the original plaintext (1), this key must be secret (1). In asymmetric encryption two keys are used (1), one is a public key (1) used for encryption (1) the other is a private key (1) which is used for decryption (1) and is a secret key (1).

c A digital signature is sent at the same time that a message is sent (1) to confirm the identity of the sender (1). It is created by encrypting a digest derived from the message (1) using a private key (1).
A digital certificate is obtained from a certification authority (1) using encryption with the authority's private key (1) to ensure safe delivery of a genuine public key (1) to anyone wishing to receive a communication from the owner of that key (1).

2 **a** More than one protocol (1), each protocol is self-contained (1), can receive input or provide output to other protocols (1).

b 1 mark each for any of the following up to a maximum of 4: A client (1) is accessing a website (1) and needs to communicate with the website (1) without the possibility of the communication being intercepted or scrutinised by an unauthorised party (1) because sensitive data is being transferred (1).

c 1 mark each for any of the following up to a maximum of 3: The client system requests a digital certificate from the website (1) to check it is authentic (1), the website may request similar from the client (1) because the client might be impersonated by someone else (1).

d 1 mark each for any of the following up to a maximum of 5: A session is created for which a session key is to be used (1), the key is used only for one individual session (1), at the start of the session the encryption algorithm and the key to be used have to be agreed (1), the process of agreeing the key begins by the use of a public key to encrypt a message (1), there might be a shared secret protocol used (1), the key agreed to be used for the session is a symmetric key (1), which is used for encryption and decryption (1) by both parties (1).

3 This is Question 2 in 9608 Paper 31 June 2016. At the time of writing the published mark scheme is available on the Cambridge International School Support Hub (requires registration). The Examiners Report for the June 2016 series is also available there and this may contain comments specific to this question.

The following are what the author of this chapter in the Teacher Resource would suggest as reasonable answers with alternatives suggested where appropriate. Where a suggested answer includes bullet points, each bullet point would be worth one mark up to the maximum mark allocation for the question.

a There are several items that could be named, including a serial number and an expiry date. However, the most important are:

- The identity of the owner
- The public key for this owner
- The name of the CA
- The digital signature of the CA

b **i** public

The user with a private key will never send it to anyone. The user sends the public key so that the CA can make an authenticated version available.

ii public

The CA will never make its private key available. The user encrypts with the CA's public key so that only the CA can decrypt with its private key.

iii private

The digital signature uses the CA's private key. Anyone else can decrypt the signature using the CA's public key. Thus establishing that the signature is genuinely from the CA.

c **i** Digital signature

ii There are a number of statements that can be made:

- Beena has received a copy of Alexa's digital certificate
- This certificate contains the public key of Alexa
- Beena uses this public key
- Successful use confirms that Alexa sent the email
- When uses this key to decrypt
- The process begins with Alexa using a private key and a hash function to produce a digest
- Beena uses the public key of Alexa and the same hash function to check that the same digest is produced.

iii This requires two names. An activity could be identified or a type of document being transmitted. Examples should identify sensitive or secret information, such as:

- Online payments for goods received
- Legal documents
- Downloaded software provided for clients only
- Minutes of private committee meetings.

Cambridge International AS & A Level Computer Science 9608 paper 31 Q2 June 2016

4 This is Question 4 in 9608 Paper 32 November 2016. At the time of writing the published mark scheme is available on the Cambridge International School Support Hub (requires registration). The Examiners Report for the November 2016 series is also available there and this may contain comments specific to this question.

The following are what the author of this chapter in the Teacher Resource would suggest as reasonable answers with alternatives suggested where appropriate. Where a suggested answer includes bullet points, each bullet point would be worth one mark up to the maximum mark allocation for the question.

a **i** A set of rules that are followed when transmitting data

ii The answer is either a browser or an email client

iii The answer is either a web server or an email server

iv The answer has to identify two of the three main concerns relating to transmitting data. An answer might give a name from the following list or provide a suitable example:

- Security
- Authentication
- Privacy.

b An example should be named and then briefly described. There are several possibilities:

- Encryption to be used; symmetric or asymmetric; keys to be used
- Authentication method to be used; digital certificate or digital signature
- Compression to be used; method of encryption; lossy or lossless
- Protocol to be used; which version
- Type of session to be used; reusable or not.

c The answer should identify an activity. This could be an application such as:

- A banking transaction
- Online shopping
- A financial transaction

An alternative approach is to name a generic activity but this must be identified as requiring security, so the following examples would be acceptable as answers:

- Secure email
- Secure file transfer.

Cambridge International AS & A Level Computer Science 9608 paper 32 Q4 November 2016