Summary

- Encryption converts plaintext to ciphertext; decryption reverses the process.
- The five main security concerns when transmitting messages are: confidentiality, authenticity, integrity, non-repudiation and availability.
- Alternatives for encryption are symmetric, using one key, or asymmetric, using two different keys.
- Authentication can be achieved using a digital signature and a digital certificate.
- A digital certificate is provided by a certification authority within a public key infrastructure.
- DES and AES are examples of symmetric key encryption.
- RAS is an important asymmetric key method.
- Secure Socket Layer (SSL) which became Transport Layer Security (TLS) provides security when accessing a website.
- Quantum Key Distribution systems use polarised photons.

Exam-style Questions

1 **a** When transmitting data across a network three concerns relate to: confidentiality, authenticity and integrity.

Explain each of these terms. [4]

b Encryption and decryption can be carried out using a symmetric or an asymmetric key method.

Explain how keys are used in each of these methods. You are not required to describe the algorithms used. Your account must include reference to a public key, a private key and a secret key. [6]

c Digital signatures and digital certificates are used in message transmission.

Give an explanation of their use. [5]

2 Secure socket layer (SSL) and its upgraded version named Transport Layer Security (TLS) is described as a protocol suite.

a Explain the meaning of the description ‘protocol suite’. [3]

b Describe the type of activity where SSL or TLS would be used. [4]

c Explain how digital certificates are used in the protocol suite. [3]

d Explain how encryption keys are used in the protocol suite. [5]

3 Digital certificates are used in Internet communications. A Certificate Authority (CA) is responsible for issuing digital certificates.

a Name **three** data items present in a digital certificate. [3]

b The method of issuing a digital certificate is as follows.

i A user starts an application for a digital certificate using their computer. On this computer a key pair is generated. This key pair consists of a public key and an associated private key.

ii The user submits the application to the CA. The generated .... (i) .... key and other application data are sent. The key and data are encrypted using the CA’s .... (ii) .... key.

iii The CA creates a digital document containing all necessary data items and signs it using the CA’s .... (iii) .... key.

iv The CA sends the digital certificate to the individual.

In the above method there are three missing words. Each missing word is either 'public' or 'private'.

State the correct word. Justify your choice. [6]

c Alexa sends an email to Beena.

Alexa's email program:

- produces a message digest (hash)
- uses Alexa's private key to encrypt the message digest
- adds the encrypted message digest to the plain text of her message
- encrypts the whole message with Beena's public key
- sends the encrypted message with a copy of Alexa's digital certificate.

Beena's email program decrypts the encrypted message using her private key.

i State the name given to the encrypted message digest. [1]

ii Explain how Beena can be sure that she has received a message that is authentic (not corrupted or tampered with) and that it came from Alexa. [2]

iii Name **two** uses where encrypted message digests are advisable. [2]

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

4 Both clients and servers use the Secure Socket Layer (SSL) protocol and its successor, the Transport Layer Security (TLS) protocol.

a **i** What is a protocol? [2]

ii Name the client application used in this context. [1]

iii Name the server used in this context. [1]

iv Identify **two** problems that the SSL and TLS protocols can help to overcome. [2]

b Before any application data is transferred between the client and the server, a handshake process takes place. Part of this process is to agree the security parameters to be used.

Describe **two** of these security parameters. [4]

c Name **two** applications of computer systems where it would be appropriate to use the SSL of TLS protocol. These applications should be different from the ones you named in **part (a)(ii)** and **part (a)(iii)**. [2]

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