3.5.2 Digital Signatures and Digital Certificates

Computer Science (9608)

May/June 2015.P31/P32

2 (d) A user downloads software from the Internet.

(i) State what should be part of the download to provide proof that the software is authentic. **[1]**

(ii) Describe the process for ensuring that the software is both authentic and has not been altered. **[4]**

May/June 2016.P31/P32

2 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:

1 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.

2 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.

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

4 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]**