3.5.1 Asymmetric Keys and Encryption Methods

Computer Science (9608)

May/June 2015.P31/P32

2 (c) Explain the following terms:

Encryption

Public key **[2]**

May/June 2015.P33

3 (c) Explain the following terms:

Cipher

Private key **[2]**

(d) Bill, a manager of a company, sent an email with very sensitive information to a work colleague, Alison. However, Bill also accidentally sent it to everybody in the company.

Describe the method used that ensured only Alison was able to read the original contents of the email. **[4]**

May/June 2016.P31/P32

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

(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]**