Past-paper walk-through

Encryption ▪ 2.3

eXercise

Questions in this set

- 0478/11 J25 Q6 ▪ 9 marks
- 0478/11 J24 Q7 ▪ 4 marks
- 0478/12 M24 Q7 ▪ 8 marks
- 0478/12 N23 Q8 ▪ 6 marks

Reading the mark scheme

- **B1** a mark that stands on its own – the point is either made or not.
- **M1** a *method* mark: the right approach, even if the number is wrong.
- **A1** an *answer* mark, and it usually needs its M mark first.
- **C1** a working mark on the way to the answer.
- // separates answers the examiner accepts equally.
- **ecf** = error carried forward: a later part is marked on your own earlier answer.
- **owtte** = "or words to that effect" – the wording need not match.

Question 6

0478/11 J25 ▪ Q6 ▪ 9 marks

Data can be encrypted using asymmetric encryption.

(a) Complete the paragraph about asymmetric encryption.

Use the terms from the list.

Some of the terms in the list will not be used. You may use a term more than once.

- algorithm
- binary
- cipher text
- compression
- error
- hardware

Question 6

- hexadecimal
- meaningless
- plain text
- private
- public
- readable
- transmission
- unreadable

Data is encrypted using an encryption key. This is a type of ___ that scrambles the ___ and turns it into ___. This makes the data ___.

A ___ key is used to encrypt the data. This key cannot be used to decrypt the data. A ___ key is used to decrypt the data. Any device is able to request the ___ key, but only your device knows the ___ key. **[8]**

Question 6

0478/11 J25 ▪ Q6 ▪ 9 marks

Data can be encrypted using asymmetric encryption.

(b) Data can also be encrypted using symmetric encryption.

Give **one** reason why a person would use asymmetric encryption instead of symmetric encryption. **[1]**

Solution 6

(a) Mark scheme

- One mark for each correct term in the correct position
- ▪ algorithm
- ▪ plain text
- ▪ cipher text
- ▪ meaningless
- ▪ public/private
- ▪ private/public (must be opposite of MP5)
- ▪ public

Solution 6

- ▪ private
- Data is encrypted using an encryption key. This is a type of algorithm that scrambles the plain text and turns it into cipher text. This makes the data meaningless.
- A public/private key is used to encrypt the data. This key cannot be used to decrypt the data. A private/public key is used to decrypt the data. Any device is able to request the public key, but only your device knows the private key.

Solution 6

(b)

Mark scheme

- Any one from:
- ▪ The process is more secure.
- ▪ Do not need to worry about key exchange.

Question 7

0478/11 J24 ▪ Q7 ▪ 4 marks

Data is encrypted to keep it safe during transmission.
Complete the paragraph about asymmetric encryption.
Use the terms from the list.
Some of the terms in the list will **not** be used. You should only use a term once.

- asymmetric
- certificate
- cipher text
- decrypted
- encrypted
- parallel key

Question 7

- plain text
- private key
- protected
- public key
- serial key
- symmetric

___ is encrypted into ___ using a ___. The encrypted data is then transmitted from the sender to the receiver. The encrypted data is then decrypted using a ___. **[4]**

Solution 7

Mark scheme

- One mark for each correct term in the correct place.
- ▪ plain text
- ▪ cipher text
- ▪ public key
- ▪ private key

Question 7

0478/12 M24 ▪ Q7 ▪ 8 marks

Data is transmitted using the internet.

(a)(i) State the purpose of encrypting data. **[1]**

(a)(ii) Describe the differences between symmetric and asymmetric encryption. **[4]**

(b)(i) Identify **two** items of data contained in a packet header.

1. 2. **[2]**

(b)(ii) Give the purpose of a router in the packet-switching process. **[1]**

Solution 7

(a)(i)

Mark scheme

- If the data is intercepted, it cannot be understood

Solution 7

(a)(ii) Mark scheme

- Four from:
- ▪ Symmetric has a shared key...
- ▪ ... to encrypt and decrypt
- ▪ Both the sender and receiver know the key
- ▪ Asymmetric has different keys // a public key and a private key
- ▪ ...public to encrypt the data and private to decrypt
- ▪ ...anyone can know the public key but only those intended know the private key

Solution 7

(b)(i)

Mark scheme

- Any two from:
- e.g.
- ▪ Destination address/IP
- ▪ Sender address/IP
- ▪ Packet number

Solution 7

(b)(ii)

Mark scheme

- Any one from:
- ▪ Control the route the packet takes
- ▪ Send each packet towards its destination
- ▪ Choose more efficient route

Question 8

0478/12 N23 ▪ Q8 ▪ 6 marks

8 **(a)** Draw and annotate a diagram that demonstrates the cyber security threat of data interception.

Question 8

[4]

(b) Identify **one** security solution that will help keep data safe from data interception and state why it will help keep the data safe.

Solution 8

(a) Mark scheme

- The diagram demonstrates (One mark for each part of the diagram):
- –
- Data is being sent from one device to another
- –
- The data is being examined during transmission
- –
- Packet sniffer is used
- –

Solution 8

- Intercepted data is reported to a third-party during transmission ...
- —
- ... and analysed for anything useful
- —
- Connection hacked to spoof destination address
- e.g.
- 4

Solution 8

(b) Mark scheme

- –
- Encryption ...
- –
- ... if the data is intercepted it will be meaningless (because they do not
- have the decryption key)
- 2
- 0478/12
- October/November

Solution 8

- 2023