Cambridge O Level

Cambridge Assessment International Education
Cambridge Ordinary Level

COMPUTER SCIENCE **2210/11**

Paper 1 **May/June 2019**

MARK SCHEME

Maximum Mark: 75

Published

This mark scheme is published as an aid to teachers and candidates, to indicate the requirements of the examination. It shows the basis on which Examiners were instructed to award marks. It does not indicate the details of the discussions that took place at an Examiners' meeting before marking began, which would have considered the acceptability of alternative answers.

Mark schemes should be read in conjunction with the question paper and the Principal Examiner Report for Teachers.

Cambridge International will not enter into discussions about these mark schemes.

Cambridge International is publishing the mark schemes for the May/June 2019 series for most Cambridge IGCSE™, Cambridge International A and AS Level and Cambridge Pre-U components, and some Cambridge O Level components.

© UCLES 2019

PUBLISHED

Generic Marking Principles

These general marking principles must be applied by all examiners when marking candidate answers. They should be applied alongside the specific content of the mark scheme or generic level descriptors for a question. Each question paper and mark scheme will also comply with these marking principles.

GENERIC MARKING PRINCIPLE 1:

Marks must be awarded in line with:

- the specific content of the mark scheme or the generic level descriptors for the question
- the specific skills defined in the mark scheme or in the generic level descriptors for the question
- the standard of response required by a candidate as exemplified by the standardisation scripts.

GENERIC MARKING PRINCIPLE 2:

Marks awarded are always **whole marks** (not half marks, or other fractions).

GENERIC MARKING PRINCIPLE 3:

Marks must be awarded **positively**:

- marks are awarded for correct/valid answers, as defined in the mark scheme. However, credit is given for valid answers which go beyond the scope of the syllabus and mark scheme, referring to your Team Leader as appropriate
- marks are awarded when candidates clearly demonstrate what they know and can do
- marks are not deducted for errors
- marks are not deducted for omissions
- answers should only be judged on the quality of spelling, punctuation and grammar when these features are specifically assessed by the question as indicated by the mark scheme. The meaning, however, should be unambiguous.

GENERIC MARKING PRINCIPLE 4:

Rules must be applied consistently e.g. in situations where candidates have not followed instructions or in the application of generic level descriptors.

© UCLES 2019

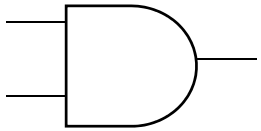
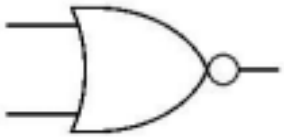
GENERIC MARKING PRINCIPLE 5: Marks should be awarded using the full range of marks defined in the mark scheme for the question (however; the use of the full mark range may be limited according to the quality of the candidate responses seen).
GENERIC MARKING PRINCIPLE 6: Marks awarded are based solely on the requirements as defined in the mark scheme. Marks should not be awarded with grade thresholds or grade descriptors in mind.

© UCLES 2019

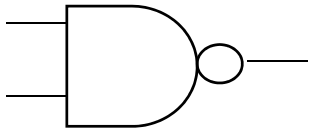
Question	Answer	Marks
1(a)	97  1 mark 1 mark 5C  1 mark 1 mark E1  1 mark 1 mark	**6**
1(b)	**Four** from: • Media Access Control (address) • Used to identify a device • It is a **unique** (address) • It is a static address // It does not change • It is set by the manufacturer • The first part is the manufacturer ID/number/identifies the manufacturer • The second part is the serial number/ID	**4**

© UCLES 2019

Question	Answer	Marks
1(c)	**Two** from e.g.: • Colour **codes** // Colour in **HTML / CSS** • Error messages • Locations in memory • Memory dump // debugging • IP address • ASCII // Unicode • Assembly language • URL	**2**

Question	Answer	Marks
2(a)	1 mark for correct name, 1 mark for correct gate symbol – AND 	**2**
2(b)	1 mark for correct name, 1 mark for correct gate symbol – NOR 	**2**

© UCLES 2019

Question	Answer	Marks
2(c)	1 mark for correct name, 1 mark for correct gate symbol – NAND 	**2**

Question	Answer	Marks
3	1 mark for each correct device	**5**

Description of input or output device	Name of device
This is an input device that works by shining a light onto the surface of a document. The light source is automatically moved across the document and the reflected light is captured by mirrors and lenses.	**2D Scanner**
This is an input device where a laser or a light source is moved across an object. The width, height and depth of the object are measured to allow a model to be created.	**3D scanner**
This is a large input device that is usually fixed to a wall. A user can calibrate the device to make sure the sensors align with a projected image. The user can use either their finger or a special pen to make selections.	**Interactive whiteboard**
This is an output device that uses many small mirrors to reflect light towards a lens. This will display an image.	**Projector**
This is an output device that creates an object by building layer upon layer of material.	**3D printer**

© UCLES 2019

Question	Answer	Marks
4(a)(i)	1 mark for security method, 2 marks for description **Anti-virus (software) // Anti-malware (software)** • Scans the computer system (for viruses) • Has a record of known viruses • Removes/quarantines any viruses that are found • Checks data before it is downloaded • … and stops download if virus found/warns user may contain virus **Firewall // Proxy server** • Monitors traffic coming **into and out of** the computer system • **Checks** that the traffic meets any criteria/rules set • Blocks any traffic that does not meet the criteria/rules set // set blacklist/whitelist	**3**

Question	Answer	Marks
4(a)(ii)	1 mark for security method, 2 marks for description **Firewall // proxy server** • Monitors traffic coming into and out of the computer system • Check that the traffic meets any criteria/rules set • Blocks any traffic that does not meet the criteria/rules set // set blacklist/whitelist **NOTE: Cannot be awarded if already given in 4(a)(i)** **Passwords** • Making a password stronger // by example • Changing it regularly • Lock out after set number of attempts // stops brute force attacks // makes it more difficult to guess **Biometrics** • Data needed to enter is unique to individual • … therefore very difficult to replicate • Lock out after set number of attempts **Two-step verification // Two-factor authentication** • Extra data is sent to device, pre-set by user • … making it more difficult for hacker to obtain it • Data has to be entered into the same system • … so if attempted from a remote location, it will not be accepted	**3**

© UCLES 2019

Question	Answer	Marks
4(a)(iii)	1 mark for security method, 2 marks for description **Anti-spyware software // Anti-malware (software)** • Scans the computer for spyware • Removes/quarantines any spyware that is found • Can prevent spyware being downloaded **NOTE: Anti-malware (software) cannot be awarded if already given in 4(a)(i)** **Drop-down boxes // onscreen/virtual keyboard** • Means key logger cannot collect data // key presses cannot be recorded • … and relay it to third party **Two-step verification // Two-factor authentication** • Extra data is sent to device, pre-set by user • … making it more difficult for hacker to obtain it • Data has to be entered into the same system • … so if attempted from a remote location, it will not be accepted **NOTE: Cannot be awarded if already given in 4(a)(ii)** **Firewall // proxy server** • Monitors traffic coming into and out of the computer system • Check that the traffic meets any criteria/rules set • Blocks any traffic that does not meet the criteria/rules set // set blacklist/whitelist **NOTE: Cannot be awarded if already given in 4(a)(i) or 4(a)(ii)**	**3**
4(b)(i)	**Three** from: • Human error e.g. accidentally deleting a file • Hardware failure • Physical damage e.g. fire/flood • Power failure // power surge • Misplacing a storage device	**3**

© UCLES 2019

Question	Answer	Marks
4(b)(ii)	**Two** from: • Back data up • Use surge protection • Keep data in a fireproof / waterproof / protective case • Use verification methods (for deleting files) • Following correct procedure e.g. ejecting offline devices / regularly saving	**2**

Question	Answer	Marks

5	**Five** from:
	• A (compression) algorithm is used
	• No data is removed in the process // original file can be restored
	• **Repeated** words (are identified) // **Patterns** in the data (are identified)
	• … and are indexed/put into a table // by example
	• … and are replaced with their index // by example
	• … and their positions are stored (in the table) // by example
	• … and the number of times the word/pattern appears is stored (in the table) // by example
	
	NOTE: Other valid methods of lossless compression can be awarded marks
		5

© UCLES 2019

Question	Answer	Marks
6(a)	**Four** from (max 2 marks per improvement): • Make the password require more characters • Makes the password harder to crack/guess • More possible combinations for the password • Make the password require different types of characters • Makes the password harder to crack/guess • More possible combinations for the password • Use a biometric device • Hard to fake a person's biological data // data is **unique** • Two-step verification // Two factor-authentication • Adds an additional level to hack • Have to have the set device for the code to receive it • Drop-down boxes // onscreen keyboard • To prevent passwords being obtained using keylogger • Request random characters • Won't reveal entire password • Set number of password attempts • Will lock account if attempting to guess • Will stop brute-force attacks	**4**

© UCLES 2019

Question	Answer	Marks
6(b)	**Four** from (max 3 marks for benefits only, without an explanation): • More read/write cycles (over its lifetime) // greater longevity … • … likely to be a lot of read/write functions each day • Read/write speed is sufficient … • … even though it is slower than solid-state • Cheaper **per unit of data** stored … • … better value for the company to purchase • … so the law company can afford to buy a server with greater storage capacity • No requirement for portability … • … as a server, it does not need to be moved • Trusted technology … • … it has been traditionally used for many years	**4**
6(c)	• DVD • CD • Blu-ray	**3**

© UCLES 2019

Question	Answer	Marks
7	1 mark for each correct term, in the correct place: • Syntax • High-level language • Translator • Machine code • Assembly • Low-level language	**6**

Question	Answer	Marks
8(a)	**Six** from: • SSL is a (security) protocol • It encrypts any data that is sent • It uses/sends digital certificates … • … which is sent to the (buyer's/user's) browser // requested by (buyer's/user's) browser • … that contains the gallery's public key • … that can be used to authenticate the gallery • Once the certificate is authenticated, the transaction will begin	**6**

© UCLES 2019

<table>
<tr><th>Question</th><th>Answer</th><th>Marks</th></tr>
<tr><td>8(b)</td><td>1 mark for each correct tick.

<table>
<tr><th>Statement</th><th>True (✓)</th><th>False (✓)</th></tr>
<tr><td>Firewalls are only available as hardware devices</td><td></td><td>✓</td></tr>
<tr><td>Firewalls allow a user to set rules for network traffic</td><td>✓</td><td></td></tr>
<tr><td>Firewalls will automatically stop all malicious traffic</td><td></td><td>✓</td></tr>
<tr><td>Firewalls only examine traffic entering a network</td><td></td><td>✓</td></tr>
<tr><td>Firewalls encrypt all data that is transmitted around a network</td><td></td><td>✓</td></tr>
<tr><td>Firewalls can be used to block access to certain websites</td><td>✓</td><td></td></tr>
</table></td><td>6</td></tr>
<tr><td>8(c)</td><td>Four from:
• A set of guidelines
• Rules/laws that govern the use of computers / by example
• Tell people how to behave when using computers // helps keep users safe when using computers // by example
• Art gallery could be subject to plagiarism / intellectual property theft
• Art gallery could copyright their work (to make it illegal to steal it)</td><td>4</td></tr>
</table>

© UCLES 2019