5.6 Representing images, sound and more part 1
Mark Scheme

Q1.

Marks are for AO1 (understanding)

Level of response question

Level	Description	Mark Range
3	At least five points have been made that shows a very good understanding of both how an image is captured and how run-length encoding is applied.	5-6
2	At least three points have been made that show a good understanding of at least one of how an image is captured and how run-length encoding is applied.	3-4
1	At least one point has been made that shows some understanding of either image-capture or run-length encoding.	1-2

Guidance: Indicative Response

Image Capture

- Light enters through / is focussed by the lens; on to (an array of sensors on) the sensor chip **A.** light sensors capture / record light (intensity) **A.** CCD as sensor;
- Each sensor produces an electrical current / signal;
- The signal represents a pixel;
- An (ADC) converts measurement of light intensity into binary / digital data;
- (Colour) filter is applied to generate separate data values for red, green and blue colour components;
- The pixels are recorded as a group / array;

Run-Length Encoding

- The image is analysed to identify runs / sequences of the same colour / value **N.E.** patterns;
- The colours / values and counts of pixels / values / run-lengths are represented / identified / stored **A.** example;

[6]

Q2.

(a) **2 marks for AO1 (knowledge) and 1 mark for AO1 (understanding)**

2 marks AO1 (knowledge):

Image is represented as / composed of objects;
Properties (of objects) are stored //objects have properties;
A. "shapes" or "instructions" for "objects" (this time only)
N.E. "formulae" for objects
A. "attributes" for "properties"

1 mark AO1 (understanding):
A property of the black rectangle is given; e.g.

- fill colour
- outline / edge colour
- x coordinate of a specific point e.g. top right-hand corner
- y coordinate of a specific point e.g. top right-hand corner
- outline / edge width
- width
- height

A. if a property is given without it being directly related to the black rectangle.
A. coordinates of a specific point eg top right-hand corner for one mark only if x and y not referenced
R. properties that are too vague eg position, colour, coordinates (without further explanation), points (without reference to coordinates)
Marks should be awarded if student has asserted that rectangle drawn as a wide line.

3

(b) **All marks AO2 (apply)**

50 × 50 × 2 / 8 = 625 (bytes)

2 marks for the correct answer with some working shown
OR
1 mark for one of:

- multiplying 50 by 50 in the working // 2500 in the working
- multiplying by 2 in the working
- giving the correct solution of 625 (bytes) with no working shown

2

(c) **All marks AO1 (knowledge)**

A run is a sequence / series of pixels of the same colour // the number of consecutive pixels of the same colour would need to be counted;
(Pairs of values would be stored), which would consist of a run length and the colour of the pixels in the run;
Example of how the specific row of pixels would be compressed eg 7 Yellow, 4 Blue, 9 Yellow; **A.** assignment of numeric values to colours
A. "row" for "run" as **BOD**

Max 2

2

(d) **All marks AO1 (understanding)**

Runs will be of shorter length // the image (in the second figure) contains a lot more different colours; **A.** colour depth is higher in the second image.
(For short runs) the additional run length data may (largely) cancel out (or even outweigh) the reduction in storage of pixel colour data;

A. responses given in reverse ie why first figure was compressed more effectively

2

[9]

Q3.

(a) **4 marks for AO3 (design) and 8 marks for AO3 (programming)**

Mark scheme

Level	Description	Mark Range
4	A line of reasoning has been followed to arrive at a logically structured working or almost fully working programmed solution that meets most of the requirements of **Task 1**. All of the appropriate design decisions have been taken. To award 12 marks, all of the requirements must be met.	10-12
3	There is evidence that a line of reasoning has been followed to produce a logically structured program. The program displays a prompt, inputs the string value and includes a loop. An attempt has been made to count the number of consecutive instances of a character and to output a character followed by the count of that character, although some of this may not work. The solution demonstrates good design work as most of the correct design decisions have been taken.	7-9
2	A program has been written and some appropriate, syntactically correct programming language statements have been written. There is evidence that a line of reasoning has been partially followed as although the program may not have the required functionality, it can be seen that the response contains some of the statements that would be needed in a working solution. There is evidence of some appropriate design work as the response recognises at least one appropriate technique that could be used by a working solution, regardless of whether this has been implemented correctly.	4-6
1	A program has been written and a few appropriate programming language statements have been written but there is no evidence that a line of reasoning has been followed to arrive at a working solution. The statements written may or may not be syntactically correct. It is unlikely that any of the key design elements of the task have been recognised.	1-3

Guidance

Evidence of AO3 (design) – 4 points:

Evidence of design to look for in responses:

1. Identifying that a method that looks at each character in text entered is needed
2. Identifying that a comparison is needed to check if the current character

is the same as the previous character or not

3. Mechanism that "remembers" value of previous character in the string // mechanism that "remembers" character at start of the run
4. Identifying that the first character in the string can't be compared to a previous character // the last character in the string can't be compared to the next character **NOTE:** award mark based on method attempted in answer provided

Note that AO3 (design) points are for selecting appropriate techniques to use to solve the problem, so should be credited whether the syntax of programming language statements is correct or not and regardless of whether the solution works.

Evidence for AO3 (programming) – 8 points:

Evidence of programming to look for in response:

5. Suitable prompt displayed before any loop structures
6. Text input by user and stored into a variable with a suitable name, after prompt is displayed and before any loop structures
7. Loop structure coded with correct termination condition
8. Selection structure coded with correct condition, selection structure must be inside loop **A**. second loop structure with correct condition that is nested in first loop structure
9. One added to count of character under the correct circumstances
10. Count of character reset to one under the correct circumstances
11. Character and correct count of character displayed for some characters from beginning of text input by user
12. Character and correct count of character displayed for all characters of any text entered by the user

Note that AO3 (programming) points are for programming and so should only be awarded for syntactically correct code.

Information for examiner: Refer answers that use alternative methods to produce the RLE to team leader.

12

VB.NET

Example Solution

```
Sub Main()
  Dim Text As String
  Dim LastChar As String
  Dim CountOfLastChar As Integer
  Console.Write("Enter the text to compress: ")
  Text = Console.ReadLine()
  LastChar = ""
  CountOfLastChar = 0
  For Count = 0 To Len(Text) - 1
    If Text(Count) = LastChar Then
      CountOfLastChar += 1
    Else
      If LastChar <> "" Then
        Console.Write(LastChar & " " & CountOfLastChar & " ")
      End If
      LastChar = Text(Count)
      CountOfLastChar = 1
    End If
```

```
  Next
  Console.Write(LastChar & " " & CountOfLastChar & " ")
  Console.ReadLine()
End Sub
```

PYTHON 2

```
text = raw_input("Enter the text to compress: ")
print "The compressed text is:",
LastChar = ""
CountOfLastChar = 0
for Count in range(0, len(text)):
  if text[Count] == LastChar:
      CountOfLastChar += 1
  else:
      if LastChar != "":
        print LastChar, CountOfLastChar,
      LastChar = text[Count]
      CountOfLastChar = 1
print LastChar,CountOfLastChar
```

PYTHON 3

Example Solution

```
text = input("Enter the text to compress: ")
print ("The compressed text is: ", end="")
LastChar = ""
CountOfLastChar = 0
for Count in range(0, len(text)):
  if text[Count] == LastChar:
      CountOfLastChar += 1
  else:
      if LastChar != "":
        print (LastChar, " " , CountOfLastChar, " ",end="")
  LastChar = text[Count]
  CountOfLastChar = 1
print (LastChar, " " , CountOfLastChar, " ")
```


C#

```
string Text = "";
string LastChar = "";
int CountOfLastChar = 0;
Console.Write("Enter the text to compress: ");
Text = Console.ReadLine();
Console.Write("The compressed text is: ");
for (int Count = 0; Count < Text.Length ; Count++)
{
  if (Text[Count].ToString() == LastChar )
  {
    CountOfLastChar++;
  }
  else
  {
    if (LastChar != "")
    {
      Console.Write(LastChar + " " + CountOfLastChar + " ");
    }
    LastChar = Text[Count].ToString();
    CountOfLastChar = 1;
  }
}
Console.Write(LastChar + " " + CountOfLastChar + " ");
Console.ReadLine();
```

PASCAL

Example Solution

```
var
  Text : string;
  LastChar : string;
  CountOfLastChar : integer;
  Count : integer;
begin
  write('Enter the text to compress: ');
  readln(Text);
  write('The compressed text is: ');
  LastChar := '';
  CountOfLastChar := 0;
  for Count := 1 to Length(Text) do
    begin
      if Text[Count] = LastChar then
        inc(CountOfLastChar)
      else
        begin
          if LastChar <> '' then
            write(LastChar, ' ', CountOfLastChar, ' ');
          LastChar := Text[Count];
          CountOfLastChar := 1;
        end;
    end;
  write(LastChar, ' ', CountOfLastChar, ' ');
  readln;
end.
```

JAVA

```
public static void main(String[] args)
{
  String Text;
  char LastChar;
  int CountOfLastChar;
  Console.print("Enter the text to compress: ");
  Text = Console.readLine();
  Console.print("The compressed text is: ");
  LastChar = ' ';
  CountOfLastChar = 0;
  for (int Count = 0; Count < Text.length(); Count++)
  {
    char CurrentChar = Text.charAt(Count);
    if(CurrentChar == LastChar)
    {
      CountOfLastChar += 1;
    }
    else
    {
      if (LastChar !=' ')
      {
        Console.print(LastChar + " " + CountOfLastChar + " ");
      }
      LastChar = CurrentChar;
      CountOfLastChar = 1;
    }
  }
  Console.print(LastChar + " " + CountOfLastChar + " ");
  Console.readLine();
}
```

(b) **Mark is for AO3 (evaluate)**

*****SCREEN CAPTURE(S)*****
Info for examiner: Must match code from part (a), including prompts on screen capture matching those in code. Code for part (a) must be sensible.
Display of suitable prompt and user input of `AAARRRRGGGHH` followed by output of `A 3 R 4 G 3 H 2;`

A. Each output on its own line, no spaces, other delimiter used instead of space

1

(c) **Mark is for AO3 (evaluate)**

*****SCREEN CAPTURE(S)*****
Info for examiner: Must match code from part (a), including prompts on screen capture matching those in code. Code for part (a) must be sensible.
Display of suitable prompt and user input of `A` followed by output of `A 1;`

A. no space between `A` and `1,` other delimiter used instead of space

1

[14]

Q4.

All marks AO1 (knowledge)

The key must be (at least) as long as the data to be encrypted/plaintext;
The key must not be reused // key must only be used once;
The key must be (truly) random;
The key must be kept securely / not revealed / only known by user(s);

Max 2

[2]

Q5.

(a) (Using an algorithm) to convert a message into a form that is not understandable (without the key to decrypt it);
(Using an algorithm) to convert a message into a form that is only understandable by the intended parties // can only be read with the correct key;
(Using an algorithm) to convert a message into cipher text;
NE. Scrambling unless further explanation is provided
NE. Coding
A. "Unreadable" for "understandable"
A. "Data" for "a message"
R. Responses that do not make clear that encryption is a process

Max 1

(b) **1 mark** for two or three keys correctly named.
2 marks for all four keys correctly named.

Label	Key Name
❶	A's Private Key
❷	B's Public Key

❸	B's Private Key
❹	A's Public Key

A. "Sender" for "A" and "Recipient" for "B" (or similar role descriptions)
Allow use of same key name more than once and mark correct in the position it is correct (if any).

2

(c) Two (message) digests are compared // received and recalculated digests compared;
A. "They" for the two message digests
A. "Hash" for "digest"
R. Two messages are compared

1

(d) To authenticate/confirm identity of sender // to confirm that message was sent by A;
A. Ensures sender is who they say they are
NE. Identify the sender (must be clear that the signature confirms this identity), know who the sender is

To detect if message has been tampered with/altered/changed;
NE. Prevent/stop the message being tampered with

Award marks in part (d) for valid responses to part (d) that are made in part (c).

2

[6]

Q6.

Marks are for AO2 (apply)

Mark Scheme

Level	Description	Mark Range
3	A line of reasoning has been followed to produce a coherent, relevant, substantiated and logically structured response. The response covers both the comparison of car control and painting (see Guidance Table 1) and the use of data for car control (see Guidance Table 2). At least two points from each column of Table 1 have been made and substantiated and at least three sources of input, its processing, the derived information and why it is needed must have been addressed successfully.	7-9
2	There is some evidence that a line of reasoning has been followed. The response	4-6

	is relevant and most but not all points made are substantiated. The response covers both the comparison of car control and painting (see Guidance Table 1) and the use of data for car control (see Guidance Table 2) but one of these two may be covered at a fairly superficial level. EITHER: At least two points from each column of Table 1 have been made and substantiated and at least one source of input, its processing, the derived information and why it is needed must have been addressed successfully OR: At least one point from each column of Table 1 has been made and substantiated and at least two sources of input, its processing, the derived information and why it is needed must have been addressed successfully	
1	There is little or no evidence that a line of reasoning has been followed. Some relevant points have been made but these may only cover one of the comparison of car control and painting (see Guidance Table 1) or the use of data for car control (see Guidance Table 2). If both have been covered, the coverage is superficial and the points made are not successfully substantiated.	1-3

Guidance

Guidance Table 1: Automated car control vs programmed control of a robot for spraying car bodies	
Robot for spraying car bodies	**Automated car control**
Exactly same operation performed over and over again by programmed robot sprayer Position of car bodies predetermined / / car bodies in known precise positions all the time / / Robot sprayer does not need to deviate from pre-programmed position at any time / / a strictly controlled environment Actions to be performed known in advance for programmed robot sprayer.	The environment in which the car operates is not predictable / / is more complex / / has greater uncertainty Car system needs to know at all times exactly where it is Car system needs to recognise what it sees Car system will need a range of sensors Car system has to analyse / react to an input very quickly

Programmed robot sprayer requires only limited sensing of environment if any / / fewer inputs to monitor Robot sprayer does limited processing. Robot sprayer has a relatively simple program which is numerically controlled	(and then adjust one or more of the three given outputs to alter car motion) Car system has to continuously monitor many external variables Car system has to perform very complex processing Car system will need very powerful processors

Guidance Table 2: Processing, why, sources of input data, derived information

Source of data: Radar:

Processing:
(long range) radar returns / signals
- Processed to obtain location information of every object over a 360 degree view
- Plotted on a two dimensional map (for further processing)
- Changes in position processed
- Trajectories of moving objects calculated

(long range) radar returns / signals
- Processed to obtain speed of moving objects
- Speed of the car subtracted from the speed of object

Derived information:
- Precise fix on the location of every object
- Distance from objects
- Speed information from changes in position and time
- Speed information from (speed) radar
- Direction information from changes in position
- Trajectories of moving objects

Why?
- To keep car at safe distance from other objects / / to steer car safely
- To negotiate roundabouts / junctions

Processing:
- Radar return / signal processed to obtain speed information of objects
- Speed of the car subtracted from the speed of object.

Derived information:
- A zero result indicates a stationary object, a non-zero result indicates a moving object

Why?
- The car must be able to distinguish moving objects from stationary objects, e.g. pedestrian from fence post

Processing:
(short-range) radar returns / signals
- Separation distance between car and object
- Closing speed on object

Why?

To avoid collision by applying brakes automatically
To maintain safe separation distance from objects at sides
of car

Source of data: Stereoscopic Camera (at front of car):

Processing:

Separate images processed to construct view of surrounding area in 3D
Machine intelligence processing used to extract important features

Derived information:

Depth information
Road edge
Road centre
Lane edges

Why?

To predict car's trajectory
Keep car within its lane
Keep car on safe overtaking course

Source of data: High resolution video camera (at front of car):

Processing:

Video frames processed and matched by comparison with a database of road signs

Derived information:

Particular road sign

Why?

Needed to observe highway code
Needed to be aware of junctions, etc.

Source of data: Global Positioning Satellite receiver:

Processing:

Satellite signals processed to obtain location and time information
Comparison made with a stored representation of road system

Derived information:

Position of car relative to junctions, etc
Speed of car

Why?

Needed to observe highway code
Needed to be aware of junctions, etc

[9]

Q7.

(a) **Marks are for AO1 (understanding)**

Solid-state memory chips are more robust;
No reliance on mechanical parts that could fail;

No corruption of data due to magnetic fields;
Faster write speed so more data could be recorded;
Max 2

MAX 2

(b) **Marks are for AO2 (apply)**

1 mark: 8000 * 2 * 360 ;
1 mark: / 1000 ;
1 mark: Final answer: 5760 (KB) ;

OR

Alternative method:

1 mark: 8000 * 16 * 360 ;
1 mark: / 8
1 mark: / 1000;

3

(c) **Marks are for AO1 (understanding)**

1 mark: Nyquist's theorem / / sample rate should be twice the highest frequency to be stored;
1 mark: With a sample rate of 8000 Hz any audio frequency over 4000 Hz would not be properly measured;

2

[7]

Q8.

(a) **Mark is for AO2 (apply)**

Grey Pixel: 00
White Pixel: 11;
Must have both correct to achieve mark

1

(b) **Mark is for AO2 (apply)**

1 mark for either:

1	1	1	1	0	0	1	0	0	1	0	1	1	0	1	0	0	0	1	1

or:

1	1	1	1	0	0	0	1	1	0	1	0	0	1	0	1	0	0	1	1

1

(c) **All marks AO2 (apply)**

Working 1 mark:
20*10 / / 2*10*10 / / 200;
Division of a number of bits by 8 to convert to bytes (even if number is not 200);

1 mark:
25 (bytes);

2

(d) **Mark is for AO1 (understanding)**

1 mark (Max) for any of the items in this list, or a description of any of them:

- image width
- image height
- colour (bit) depth / / bits per pixel
- number of colour planes
- colour table / palette
- number of colours in palette
- number of important colours
- colour channel bitmasks
- colour channel gamma correction
- file size
- image size
- type of compression used
- pixel density / / pixels per metre (**A** any other measurement unit)
- offset to pixel data within file.

A Any other valid answer (there are many possibilities)

1

(e) **2 marks for AO1 (knowledge) and 1 mark for AO1 (understanding)**

AO1 (Knowledge): How it works (2 marks):
1 mark: Identifies sequences of identical data values / colour pixels;
1 mark: Represents these as one data value / pixel colour together with a count of how many such values are in the sequence;

AO1 (Understanding): Why suitable for icons (Max 1 mark):
Images / icons often contain sequences of pixels that are the same colour;
RLE is a lossless compression method, so the quality of the image will not be affected (which is important for icons);

3

[8]

Q9.

(a) (Type of) shape // circle;
Coordinates of centre / midpoint;
Identifier;
(Length of) radius / diameter;
Line colour // outer colour;
Line width;
Fill colour // inner colour;

NE Position / coordinates
NE Colour
NE Size
NE Centre / midpoint

MAX 3

(b) The image is divided into pixels;
Each possible colour is represented using a bit pattern // each pixel is

represented using the same number of bits;
Information is stored about the colour of each pixel;
The position of the pixel in memory determines its location in the image;
A metadata will be stored about the image

MAX 3

(c) (For geometric images) less storage space / memory likely to be needed;
NE less space
(For geometric images) will load faster (from secondary storage);
(For geometric images) will download faster;
Can be scaled / resized without distortion;
A zoom
Image can be (more easily) searched for particular objects;
Can (more easily) manipulate individual objects in an image;
Can preserve the background so that it can be recreated if an object is deleted;

MAX 3

[9]

Q10.

(a) (Using an algorithm) to convert a message into a form that is not understandable (without the key to decrypt it);
(Using an algorithm) to convert a message into a form that is only understandable by the intended parties // can only be read with the correct key;
(Using an algorithm) to convert a message into cipher text;
NE Scrambling unless further explanation is provided
NE Coding
A "Unreadable" for "understandable"
A "Data" for "a message"
R Responses that do not make clear that encryption is a process
MAX 1

1

(b) **1 mark** for two or three keys correctly named.
2 marks for all four keys correctly named.

Label	Key Name
❶	A's Private Key
❷	B's Public Key
❸	B's Private Key
❹	A's Public Key

A "Sender" for "A" and "Recipient" for "B" (or similar role descriptions)
Allow use of same key name more than once and mark correct in the position it is correct (if any).

2

(c) Two (message) digests are compared // received and recalculated digests compared;
A "They" for the two message digests

A "Hash" for "digest"
R Two messages are compared

1

(d) To authenticate / confirm identity of sender // to confirm that message was sent by A;
A Ensures person is who they say they are
NE Identify the sender (must be clear that the signature confirms this identity), know who the sender is

To detect if message has been tampered with / changed;
NE Prevent the message being tampered with

Award marks in part (d) for valid responses to part (d) that are made in part (c).

2

[6]

Q11.

(a) 16 (bit);
A 2 bytes

1

(b) 8,800,000 // 100 * 2 * 44,000;;;
//
100;
2; **A** 16 ÷ 8; **A** different value for the sampling resolution (16) being used in the calculation but only if matches answer to part 15 44,000;
Max 2 if final answer incorrect

3

(c) Because of Nyquist's theorem // Because we should sample at least double the highest frequency in the original sound;
Some people can hear higher frequencies than the average (so more than double has been chosen);
There is no need to sample at a higher rate as humans won't notice any difference in quality above this level // sampling at a lower rate would mean that some people would notice the lower quality of the recording // sampling at a lower rate would mean that some meaningful changes in the analogue signal could be missed;
higher rate would require more, unnecessary, storage space;

Max 2

(d) Compression has been used;
A Explanation of a particular compression method that could have been used on the recording e.g. lower sampling frequency used // lower sampling resolution used;

1

[7]

Q12.

(a) 300; * 2;
//
600;;

Note: award 1 mark for doubling an incorrectly calculated highest frequency

2

(b) Regular samples are taken (of the analogue signal);
Samples are quantised // the height of each sample is approximated to an integer value // height of samples measured // amplitude/volume measured;
Each integer value is encoded as a binary value // measurements are coded in a fixed number of bits;
output the binary numbers as digital signals / voltage levels;

Max 3

(c) Can (easily) synthesise musical notation from it;
Can be played on different instruments;
Can be (easily) transposed to a different key/pitch;
Produces (relatively) small files;
Easy to manipulate (the data);
Allows for easy interface with electronic musical instruments;
No data lost about a musical note;

Max 1

(d) Length/duration (of note) // Note-on and Note–off;
Instrument;
Velocity//Speed;
Volume//Amplitude;
Timbre;
Pedal effects;
Channel;
Instructions about how to recreate a sound;
Aftertouch;
Pitch bend;
Note envelope;
R Note/key/pitch/frequency;
A Other sensible answers;

Max 1

[7]

Q13.

(a) (Each pixel) can be one of $4/2^2$ possible colours/values // Two bits are needed to represent the 4 possible bit patterns / colours / values // because there are 4/more than 2 colours in the image

1

(b)

1	1	1	1	1	1	0	0	0	0	1	1	**1**	**0**	1	1	;;

//

1	1	1	1	1	1	0	0	0	0	1	1	**0**	**1**	1	1	;;

Mark as follows:
13th and 14th bits correct;
Other bits correct

2

(c) 8*8 =64; * 2 = 128; ÷ 8 = 16; //
8*8*2÷ 8;;;
16;;;

A 128 bits as being worth 2 marks

3

(d) (Type of) shape // rectangle // square;
Coordinates of corner/corners // position of a corner // top left coordinates;
Identifier;
Length of side(s) // width // height // coordinates of an opposing corner;
Line colour // outer colour;
Line width;
Fill colour // inner colour;
Angle of rotation;
A coordinates of midpoint/centre;
A radius/diameter
A circle/oval
NE Position/coordinates
NE Colour

Max 3

(d) (For geometric images) less storage space / memory likely to be needed;
NE less space
(For geometric images) will load faster from secondary storage;
(For geometric images) will download faster;
Can be scaled / resized without distortion;
A zoom
Image can be (more easily) searched for particular objects;
Can (more easily) manipulate individual objects in an image;

Max 2

[11]

Q14.

(a) (Using an algorithm) to convert a message into a form that is not understandable
(without the key to decrypt it);
(Using an algorithm) to convert a message into a form that is only understandable
by the intended parties // can only be read with the correct key;
Converting a message into cipher text;
NE scrambling unless further explanation is provided
A "unreadable" for "understandable"
A "data" for "a message"

Max 1

(b) (i) B will not be able to decrypt it // A's private key would be needed to decrypt it // only A could decrypt it; (as ...)
Only A has access to A's private key // B cannot access A.s private key;

Max 1

(ii) As A's public key is available to anyone;
Anybody could decrypt it;

Max 1

(c) **Subject-related points:**

Purpose:
To authenticate/confirm identity of sender // that message was sent by A // To detect if message has been tampered with/changed;

How used:

*[1] Hash / digest produced/calculated from message // (shortened) value calculated from message;
A message is hashed
A message digest created
*[1]Hash encrypted with A's private key;
*[1]Encrypted hash is known as the (digital) signature;
*[2](Digital) signature is appended to message;
A transmitted with message
A even if stated or implied that this is done after the encryption of the message using B's public key
A hash or digest
A encrypts message and signature with B's public key;
A without reference to signature but **TO** if clear from order of statements or what candidate has written that the signature is not encrypted with B's public key
B decrypts message and signature with B's private key;
A without reference to signature
B decrypts (digital) signature using A's public key (to reveal hash);
B reproduces/recalculates hash from received message;
A re-hashed
A creates new digest
*[3]If received hash matches reproduced hash then message has not been tampered with // identity of sender is authenticated;
A Data for message
A Digest, checksum for hash
A Encrypted hash / Encrypted digest for signature
A Example of hashing method e.g. MD2/4/5/6, SH0/1/224/256/384/512

*[1] = as an alternative to these three points, allow one mark for the idea that the digital signature is calculated from/hashed from/a digest of the message
*[2] = only award this mark if there is previously the concept of the hash or signature being produced.
*[3] = can only be awarded if there is clear concept that the comparison is to a recalculated hash

Only one mark should be awarded for the purpose. Other marks must come from how the digital signature is used.
The purpose mark could be implicit in the how used mark and should be awarded if it is.
It is acceptable for steps to be missed out.
Accept responses with message sent from B to A if it is clear that this is what the candidate has done.

How to award marks:

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and all 5 of the quality of language criteria (QWCX).

SUB	Candidate has covered both the purpose and the use of digital signatures, and has ma at least five subject-related points including both creation and use. **To get 6 marks, the answer must include reference to the encryption of the message digest/hash usi A's private key.**
QWC1	Text is legibl
QWC2	There are few, if any, errors of spelling, punctuation and grammar. Meaning is clear
QWC3	The candidate has selected and used a form and style of writing appropriate to the purpose and has expressed ideas clearly and fluently.
QWC4	Sentences and (paragraphs) follow on from one another clearly and coherently.

QWC5 Appropriate specialist vocabulary has been used.

5–6

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 4 of the 5 quality of language criteria (QWCx)./span>

SUB Candidate has provided a description of some parts of the process and has made at least three subject-related points.
QWC1 Text is legible.
QWC2 There may be occasional errors of spelling, punctuation and grammar. Meaning is clear.
QWC3 The candidate has, in the main, used a form and style of writing appropriate to the purpose, with occasional lapses. The candidate has expressed ideas clearly and reasonably fluently.
QWC4 The candidate has used well–linked sentences (and paragraphs).
QWC5 Appropriate specialist vocabulary has been used.

3–4

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 4 of the 5 quality of language criteria (QWCx).

SUB Only one or two relevant points have been made.
QWC1 Most of the text is legible.
QWC2 There may be some errors of spelling, punctuation and grammar but it should still be possible to understand most of the response.
QWC3 The candidate has used a form and style of writing which has many deficiencies. Ideas are not always clearly expressed.
QWC4 Sentences (and paragraphs) may not always be well– connected.
QWC5 Specialist vocabulary has been used inappropriately or not at all.

1–2

Candidate has made no relevant points.

0

Note: Even if English is perfect, candidates can only get marks for the points made at the top of the mark scheme for this question.

If a candidate meets the subject criterion in a band but does not meet the quality of language criteria then drop mark by one band, providing that at least 4 of the quality of language criteria are met in the lower band. If 4 criteria are not met then drop by two bands.

[6]

Q15.

(a) The number of pixels / dots; per cm / inch / unit of measurement;

2

(b) The number of bits used to represent (the colour / greyscale value);
R number of (different) colours of a single pixel;

2

(c) 50;;// 10*10;*4÷8;//100; ÷2;//100;*0.5;

Max 1 if final answer not correct

2

(d) Does not deteriorate (**A** Concept of deteriorating by implication)

when enlarged/magnified //
(usually) faster to transmit //
(usually) faster to load //
(usually) uses less memory / storage space //
Easier to edit/manipulate objects in the image (**A** Alternative word to object);
NE Easier to edit / manipulate

1

[7]

Q16.

(a) Copyright Design and Patents Act (1988) // Copyright and Related Regulations (2003) // Digital Economy Act (2010);
NE Copyright, Copyright Act

1

(a) Encrypt the music file;
A (decrypt) key is needed for playback; **R** code, PIN, password for key
Download server keeps records of authorised clients (hardware devices) allowed to decrypt music; R tied to IP address
Playback tied to a particular (set of) hardware device(s);
A Using a digital watermark in the music file a form of steganography;
R cannot be transferred to other devices
NE "player" for "device"

Max 2

[3]

Q17.

(a) 6/100; //600;;

2

(b) 8 (bits);
A 1 byte;

1

(c) Sample at a frequency (at least) twice the rate; of the highest frequency (that can be present in the original signal);

2

[5]

Q18.

Arguments for DRM:
Protects *copyright* // makes it harder to breach copyright/pirate works / restricts sharing the music;
Ensures creators/suppliers receive payment for work;
Preserves incentive for people to develop new works / promotes continuation of business;
Facilitates online rental service;

Arguments against DRM:
Restricts the potential audience;
Content difficult to access as encrypted;
Makes it difficult for purchasers to make legitimate copies / backups;
Prevents use on multiple devices // tied to one or a small number of (hardware) devices;
Ineffective at preventing copying / example of why ineffective;
Can restrict playback of music to particular software packages / competing systems

incompatible;
May be unable to listen to music if company ceases to exist / relies on company continuing to exist / unable to listen if can not authenticate copy // unable to listen if NO Internet connection;
Does not deal with expiry of copyright period;
Limits creativity / limits collaboration in creating content;

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 4 of the 5 quality of language criteria (QLx).

SUB Candidate has provided a balanced argument for and against DRM (**at least two points on either side**) , making at least 5 distinct points.

QL1 Text is legible
QL2 There are few, if any, errors of spelling, punctuation and grammar. Meaning is clear.
QL3 The candidate has selected and used a form and style of writing appropriate to the purpose and has expressed ideas clearly and fluently.
QL4 Sentences and paragraphs follow on from one another clearly and coherently.
QL5 Appropriate specialist vocabulary has been used.

5–6

To achieve a mark in this band, candidates must meet the subject criterion (SUB) and 4 of the 5 quality of language criteria (QLx).

SUB Candidate has made at least three points. Additionally, to get four marks, **there must be at least one point on each side** of the argument.
QL1 Text is legible
QL2 There may be occasional errors of spelling, punctuation and grammar. Meaning is clear.
QL3 The candidate has, in the main, used a form and style of writing appropriate to the purpose, with occasional lapses. The candidate has expressed ideas clearly and reasonably fluently.
QL4 The candidate has used well-linked sentences and paragraphs.
QL5 Appropriate specialist vocabulary has been used.

3–4

To achieve a mark in this band, candidates must meet the subject criterion (SUB). The quality of language should be typified by the QLx statements.

SUB Candidate has made one or two relevant points.
The answer may be one-sided.
QL1 Most of the text is legible.
QL2 There may be some errors of spelling, punctuation and grammar but it should still be possible to understand most of the response.
QL3 The candidate has used a form and style of writing which has many deficiencies. Ideas are not always clearly expressed.
QL4 Sentences and paragraphs may not always be well-connected or bullet points may have been used.
QL5 Specialist vocabulary has been used inappropriately or not at all.

1–2

Candidate has not made reference to any of the points listed above.

0

Note: Even if English is perfect, candidates can only get marks for the points made at the top of the mark scheme for this question.

If a candidate meets the subject criterion in a band but does not meet the quality of language criteria then drop mark by one band, providing that at least 3 of the quality of language criteria are met in the lower band. If 3 criteria re not met then drop by two bands.

[6]

Q19.

(a) Smallest ;
picture element // unit which can be drawn on screen //
addressable / resolvable part / unit of a picture ;

2

(b) (i) 0010 1010 ;

1

(ii) 184 ;

1

(c) (i) pixels are stored as numbers // bit patterns / binary code // RGB bits ;

1

(ii) 8 ; **A** 1 byte

1

(d) (i) drawing is made up of drawing objects // or by example e.g. drawing is made up of circle / rectangle / straight line / etc. (must give at least two example objects) ;
different objects(**A** shapes) have a defined set of properties // or by example;

objects are stored as drawing commands / drawing list ;
some properties use mathematical equations / formulae ;

Max 2

(ii) object type ; co-ordinates / location of the centre **R** centre (only) ; radius / diameter ; fill colour ; fill style ; line thickness ; line colour ; line style ; anything reasonable ;
R colour (only) Position (only)

Max 3

[11]

Q20.

(a) **What**:
Access management system for digital media;
Method of encrypting digital media;
Media can only be read/used/accessed with correct key;

Why:
To enforce copyright law // Protect intellectual property;
A Prevent criminal offence
R Just illegal
To stop people copying music (without permission)/prevent piracy/prevent illegal sharing/prevent illegal downloads;
R stop reselling
To ensure company/artist receives income from sales of music // does not lose money;

Max 2 for what, max 2 for why, max 3 overall

3

(b) Music/files are encrypted;
R Encoded/Scrambled for encrypted
User obtains key when purchases track/file;
Music/files must be decrypted with key;
R Password, Code
Key may only work on computer file downloaded onto;
A Playback tied to particular hardware device/group of devices
R Files cannot be copied
Key may need to be authenticated with server over Internet whenever file used // Company may have licence/key server;
Time lock so music will not play after certain date // only play a fixed number of times;
Use of a specific/proprietary program to play music;
Usage rights may be expressed in a Rights Expression Language;
R Streaming;

Max 2

[5]

Q21.

(a) (i) Picture element // smallest resolvable/rectangular area/unit (**A** smallest dot) which can be drawn on screen // smallest addressable part/unit of a picture;
smallest unit which is mapped to memory;

1

(ii) Pixels are stored as numbers/bit patterns (**A** values) which represent different colours;
A or by example;

1

(b) 1;

1

(c) (picture / image) width;
(picture / image) height;
A (picture / image) dimensions
R size
image resolution / colour depth / No. of bits per pixel;
colour palette / No. of colours in image;
offset to the start of image data;
compression type;

Max 2

(d) (i) loop counter / (loop) control variable // array subscript/index;
array of Byte;
A array of Integer

2

(ii) 1101;
I. any additional leading 0's

1

(e) (i) ThisWidth;
X;

2

(ii) 2-dimensional array (of Byte);

1

(f)

ThisWidth	ThisHeight	Counter	X	Y	ThisByte		Final
8	5	0	1	1	255	[0]	25
				2	255	[1]	96
				3	255	[2]	96
				4	255	[3]	24
				5	255	[4]	24
				6	255	[5]	113
				7	255	[6]	
				8	255	[7]	
			2	1	255	[8]	
				2	25	[9]	
		1		3	25	[10]	
		2		4	96	[11]	
		3		5	96	[12]	
		4		6	24	[13]	
		5		7	24	[14]	
		6		8	113	[15]	

Mark as follows:
Counter has incremented from 0 to 6 (only);
X variable has incremented 1 and 2 (only);
Y variable has incremented 1 – 8 (only) at least once;
ThisByte contains first ten correct values;
Final[0] contains 25;
Final[1] to Final[5] are correct and with no other array subscripts used;

A correct six values (only) in Final array (in consecutive but wrong positions)

Max 6

(g) (i) program / constant / module / unit / user defined type / label /object / component / control / class;

A 'control' by example e.g. text box, drop down list
A any elements which are SQL specific

1

(ii) Maximum number of characters;
No punctuation characters;
No use of reserved words;
Must not start with a digit character;
case critical e.g. must start with lower case character;

A any answer which describes 'general' programming language restrictions.
identifier names must be unique;free-format not allowed for certain constructs, e.g. statement must not spread over two lines;
restrictions on identifiers used for labels;
loop control variable must be ordinal/integer;
array index range is restricted;
all variables must be pre-declared;

Max 2

[20]

Q22.

(a) **Symmetric key encryption:** the same key/process/algorithm is used for encrypting and decrypting;
A sending/receiving instead of encrypting/decrypting public key encryption:
Public Key enscryption: a public key and a private key // a pair of keys are used in combination; one to encrypt, the other to decrypt;

3

(b) (i) **When:** the symmetric key is sent (from B to A)
// when establishing the initial connection;
How: B must encrypt the symmetric key; with A's public key;
so A can decrypt (the symmetric key) with A's private key;
A A must encrypt the symmetric key; with B's public key;
so B can decrypt (the symmetric key) with B's private key;

Max 3

(ii) Anyone could intercept the message with the symmetric key (and then decrypt the personal data);
distributing the symmetric key securely is not possible (unless it is encrypted);
R unspecific answers such as 'easily hacked'

1

[7]

Q23.

(a) (Sound/voice) recording/er // sampling/er (software) // audio capture software;
Operating system **A** OS;
Driver;
Codec;
R Microphone software
R Analogue to digital converter

Max 2

(b) (i) Number of samples/measurements taken per second/unit time;
Frequency/how often samples are recorded/taken;
R Rate of …"
R "Intervals at which …"

Max 1

(ii) 1000 samples/measurements per second;
1 sample/measurement per millisecond (ms);
1000 Hz /1 KHz;
R 1000 (only)

Max 1

(c) 8 (bits);

1

(d) (i) (Sound) quality will be improved/clearer **R** Smoother // better/higher resolution //more accurate // higher fidelity;
the height of the wave will be measured more precisely/accurately;
R larger range of frequencies is possible

Max 1

(ii) The size of the sound file will increase // file uses more memory /disk space;
R 'uses more space'

1

(e) 0110 1100;

1

(f) *All correct answers must fit the context of how the byte(s) are interpreted by the application program (not by the user of the application).*

Program instruction(s) // machine code;
Integer (number);
Real (number) / Floating point;
Exponent;
Mantissa;
(BUT Real/Floating Point + Exponent + Mantissa scores Max 2)
BCD (number);
R Number / denary / binary

ASCII (code);
Unicode;
EBCDIC;
Character (BUT not in addition to specific codes above) **R** Keystroke;

Address / pointer /memory reference **R** Location;
String **R** Word;
Format code // system setting / device status/signal;

A any 'data type' descriptor (e.g. Boolean) – any three data types gets but excluding any answers above;
A Colour;

Max 3

[11]

Q24.

(a) (i) (x, y) coordinates; **R** Position
Length / Width;
Line width/thickness; line colour; line style;
Fill colour; fill style;
(Text) Label / Caption;
Object/identifier name;

Object type;
A any property considered reasonable
R Colour

Max 2

(ii) Vector graphics store properties/description/coordinates for each object;

Mathematical equations/formulae generate each object;
Properties (**A** by example) can be re-calculated / re-scaled;
The drawing is re-rendered/re-drawn when properties are changed;
I. Any reference to bitmaps/pixels

Max 2

(iii) Allows for future editing of the graphic (without loss of quality/distortion);
Potential for graphics libraries;

Max 1

(b) (i) 1 (byte);

1

(ii) 960 KB // 1280 x 768 / 1024;

1

(iii) 480 KB // **ft** answer given for (ii) /2;

1

[8]

Q25.

(a) If you send the key with the message, anyone can decrypt the message.

Key would need to be sent by means other than email, otherwise anyone could intercept the key and use it do decrypt the message;

1

(b) (i) Jill's public key;

1

(ii) Jill's private key;

1

(c) (i) The message data is hashed into a message digest;
The message digest is encrypted; with the sender's private key;

3

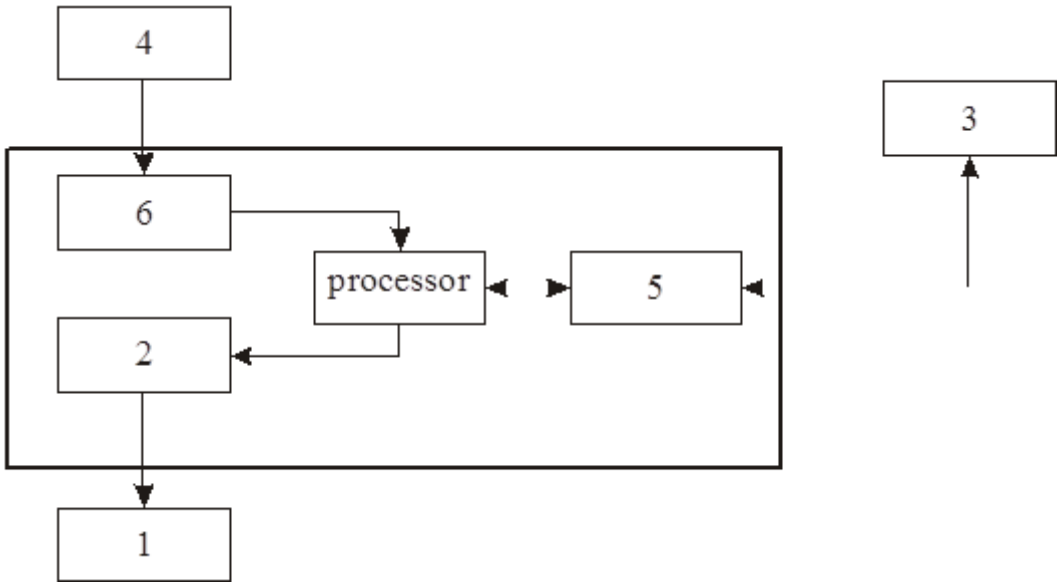
(ii) Jill's software decrypts the signature;
Using Jack's public key; contained in digital certificate sent with message;
To verify Jack's public key;
Decrypt digital certificate using Certificate Authority's (trusted third party's) public key;
Jill's software then hashes the document data into a message digest;
If recalculated message digest is the same as the original message digest (decrypted signature);
Then Jill knows that the signed data has not been changed;
I decryption of message

4

[10]

Q26.

(a)



A text labelling of the diagram

6

(b) (i) Sound which has been produced using the computer/from software;
Sound which has been digitally produced;
R 'electronically' produced

Max 1

(ii) Any plausible example where sound is not naturally produced e.g. keyboard synthesiser /computer generated voice response / mobile phone ring-tone;
R anything 'geographically'
R edited sound files

1

[8]

Q27.

(a) (i) (line) thickness / style;
(line) colour;
Label (text);
(object) name;
co-ordinates;
A length;
R start-end points / position / location

Max 2

(ii) Label (text) / co-ordinates / etc - if not used for (a)(i);
Fill colour / style;
Width;
Height;

Max 1

(iii) Vector graphics stored properties for objects // vector graphics use mathematical equations/formulae;
Bitmaps show a staircase effect / size of each pixel is enlarged // vector graphics will re-calculate the equations/formulae;

2

(b) (i) 4;

1

(ii) Each byte can represent 256 different numbers/bit patterns/combinations; Each number represents a different colour; 2^8=256 and 8 bits = 1 byte;

Max 1

(iii) 1024 x 768 div 1024 KB // 768 (KB);

1

(iv) Header data will be stored about the file e.g. file type; width value / height value; resolution; palette data;

Max 1

[9]

Q28.

E-mails
Encrypt the message:(1)
//keep password(s) for accessing account(s) / system private;
//log off from the computer at the end of the session;

[1]

Q29.

(a) **Serial transmission**
Bits are sent along a single wire/line // bits are sent one after the other / 'bit by bit';

1

(b) (i) 1;

1

(ii) (5 * 768 * 1024 / 1024) // 3840 Kbytes; **F/T** from (i);

1

(c) **Advantage**
The sound quality is higher/better;(1)

Disadvantage:
The files will be larger / files take up more disc space;(1)
R anything which suggests 'data transfer'

2

[5]

Q30.

Any 2 reasons × 1 mark each
to prevent unauthorised users understanding any intercepted data;
to prevent the message being altered; to identify authentic users;

2

[2]

Q31.

(a) So the resulting password will not be easy to guess
/Harder to hack;
R general security – TV

1

(b) 1 Convert each character to a numeric equivalent; **A** password
2 Perform some arithmetic on the number string;
A concat, algorithm, example of arithmetic,
R Process number, Translate
3 Reduce/Map arithmetic result onto two-byte integer range//example of mapping; *NB must be two bytes*
R To give a byte no.

3

[4]

Q32.

(a) Converting/transforming from plain text into ciphertext/secret code;
A scrambled;
A transposition / conversion / coding
The sender processes the message prior to transmission so that if it is accidentally or deliberately intercepted while it is being transferred it will be incomprehensible to the intercepting party;
Data coded so that unauthorised users can't read or access the data;

Max 1

(b) (i) B's public key;

1

(ii) B's private key;

1

(c) (i) A hashing function is applied to the text of the message; the result/message digest is encrypted; using B's private key;
A the data generated is added to the end of the message;
A message/date stamp is used to produce digital signature;

Max 3

(ii) A uses Certificate Authority's public key; to verify B's public key;
Digital signature is decrypted;
Using B's public key;
The hashing function is applied to the text of the message;
The result of the hashing function is compared with the digital signature;
If they are the same the message is authentic;

Max 4

[10]

Q33.

(a) (i) Analogue to Digital Converter;
A sound card
A A-D Converter
A ADC
R MIDI

1

(ii) Microphone generates analogue signals;
Computer/System requires digital/binary/discrete signals//

Computer/System stores/processes sound in digital/binary form;

2

(b) 2 – Digital to Analogue Converter;
A D-A Converter
A DAC
A Sound card (but not if given in (a) (i))
3 – Speaker/ headphones;

2

(c) Sound wave is recorded/sampled at regular intervals;
Height/Amplitude/Height/Value of sound wave is represented by a number/binary code/binary pattern;

2

(d) Number of bits used to store each value// range of values/numbers/binary codes/binary patterns;
Sampling rate// frequency of sampling // time between samples/values;
R Quality of equipment

2

[9]

Q34.

(a) (i) 52;

1

(b) (i) '4' // 4 ;

1

(ii) UNICODE // EBCDIC // EBCD // extended binary coded decimal // extended binary coded decimal interchange code;
A minor misspelling of EBCDIC

1

(c) (i) Each pixel stored in several bits/one byte/one word;
Each colour represented by a different value;

2

(ii) Endpoints // a pair of / two (x,y) co-ordinates // start point, direction and length;
Type of object / shape;
Thickness of shape / line;
Colour of shape/line;
A Properties of shape/line on its own;

3

[8]

Q35.

(a) (i) Analogue to Digital Converter;
A Sound Card

1

(ii) Stored as a sequence of numeric values;
Each value represents amplitude/height/volume of a signal at that moment;
Sound sampled regularly;

2

(b) (i) Each pixel represented by a value // image is divided into pixels;
R screen

1

(ii) Each graphic / drawn element / shape stored individually;

1

(c) Uses less memory // faster to load / transmit;

2

(d) (i) Each character stored as a unique code;
Or by example

1

(ii) ASCII/UNICODE/EBCDIC/BCDIC;

1

[9]

Q1.

The workings of a digital camera were generally well known, with many students receiving 3 or 4 marks. Run length encoding is also well understood, but frequently a lack of clarity is demonstrated with students referring to patterns of data or the same data in a row. Neither of these was specific enough to be awarded a mark.

Q2.

(a) Just under half of the students achieved two of the three marks on this question part but only around 10% achieved all three. Students needed to explain that a vector graphic system represents an image as a set of objects and that properties of these objects would be stored. It was not considered creditworthy to say that vector graphics were represented by equations. When stating properties of the black rectangle students had to be specific. For example, “coordinates” was not accepted as it would be the x and y coordinates of a specific point eg the top left corner of the rectangle that would be stored.

(b) Almost all students achieved at least one mark for this question but only just over half achieved both marks. The mark given to most candidates who only scored one mark was for calculating the number of pixels in the image by multiplying 50 by 50. The two most common mistakes were to multiply the number of pixels by the number of colours in the image (4) instead of the colour depth (2) or to express the answer in bits instead of bytes.

(c) Just under half of the students achieved full marks for this question. Many students chose to state how the particular row of pixels might be encoded using RLE but the associated descriptions of how RLE worked were often less good. For example, a student might state that the run lengths needed to be stored and not mention that the pixels colours also needed to be stored. Students needed to make clear that the pixel counts refer to adjacent pixels of the same colour and are not, for example, simply a count of yellow pixels.

(d) Approximately 90% of students achieved a mark by recognising that the second image could not be compressed very effectively because it contained many more colours and so very short runs of the same colour. Only a small minority went on to develop this response by discussing the fact that adding the run lengths into the image representation might counter any memory savings as a result of representing some runs.

Q3.

A wide variety of approaches were used to successfully answer this question showing with students often coming up with creative and unexpected approaches to the task set. Some of the more common errors from students who had made a good but not completely accurate attempt at answering the question were to count all instances of a character in the string (rather than all consecutive instances) and to fail to stop the program from checking a position outside the bounds of the string entered by the user.

It was disappointing that more than 10% of students either did not attempt to answer the question or obtained fewer than two marks when it was possible to obtain this mark by simply displaying an appropriate message on the screen and storing the string entered by the user in an appropriately-named variable.

Q4.

This question was well answered, with three quarters of students achieving some marks. Students who lost marks generally did so because their answers were too vague or unclear rather than because they were fundamentally wrong. For example, a response might state that “only the sender knows the key” when clearly the recipient would need to know it as well even if it was kept securely, or did not make clear that a point that was being made related to the key by, for example, writing that “it must be totally random”.

Q9.

Most students could state some data items that would be stored about a circle object and could give a description of how bitmapped images would be represented that was worth some marks. They could also state advantages of vector graphics over bitmaps but only a few students were able to state three creditworthy reasons.

Q10.

This question was about encryption and the use of a digital signature.

Almost three quarters of students were able to define encryption for part (a). Encryption is the conversion of plaintext into ciphertext using a key so that the message cannot be understood except by the intended parties. Some students missed out on achieving the mark by giving responses that were too vague or by offering a definition that sounded more like steganography than encryption.

For question part (b) over half of students achieved both marks. This indicates a pleasing improvement in students’ understanding of public and private key encryption. However, for part (c) just under half of students were able to achieve the mark, with many incorrectly believing that one of the hashes would be compared to the message. Good responses recognised that the two hashes would be compared.

For part (d) students had to explain the purpose of the digital signature. Three quarters of students achieved at least one mark. Good responses explained that the signature would allow the verification of the sender’s identity and that it enabled the identification of any tampering that had taken place with the message contents. It was not enough to state that the signature would allow the user to be identified; responses needed to make clear that it was the verification of this identity that would be achieved.

Q11.

Students found this question about sound representation harder than the other two Section A questions. Many students got confused between sampling resolution and sampling rate, giving answers measured in hertz for part (a). For part (b) a significant proportion of students did not include their working out, meaning that they would get zero marks if their answer was wrong. Students should be encouraged to include working out for any calculation question worth more than one mark as this could mean they get marks for correct working, even if their final answer is incorrect.

Q12.

There was a higher proportion of students this year who included their working for the calculation question in the EAD – meaning that they could get a mark for correct working, even if their final answer was incorrect. There is still a significant number of students who are not including their working – this means that if they get the answer wrong they can’t get any marks. Answers for part (b) were often vague and many students provided only a rephrase of the question as their answer. Parts (c) and (d) were the first COMP1

questions about MIDI and this topic was not well understood. More students were able to give an advantage of MIDI than could state an item of data that would be stored about a note. Quite a few students thought that MIDI was used to store samples taken from an analogue sound.

Q13.

Image representation questions have appeared in several previous COMP1 exams and this year's paper contained a mixture of questions similar to those on previous papers and questions that assessed different aspects of this topic.

The explanation of why more than one bit was needed part (a) was answered well by many students and the majority were able to work out the correct bit pattern for part (b). For part (c), students who did not provide any working for the file size calculation were unable to get any marks if their final answer was incorrect. Most students were able to give some of the data that would be stored about a vector graphic object, but few got all 3 marks available for this question. Similarly, most students could give one advantage of vector graphics, but few gave two correct advantages. The most common correct answer was that vector graphics do not lose quality when enlarged; it was not enough to say that vector graphics do not pixelate – the concept of "when enlarged" was needed for the mark for this advantage to be credited.

Q14.

Part (a): This question part asked for a definition of encryption (using an algorithm and a key to convert message data into a form that is not understandable without the key to decrypt it). Approximately three quarters of students were able to provide a suitable definition.

Part (b)(i): This question part was well answered, with most students recognising that B would not have A's private key so could not decrypt the message. Some students did not understand the asymmetric nature of the process and so wrote responses that assumed that if A's public key was used to encrypt the data, the same key would need to be used to decrypt it.

Part (b)(ii): This question part was far less well answered than part (b)(i). The correct answer was that this would be insecure as A's public key, which would be used for decryption, is available to anyone. As in the previous part, some students lost marks because they did not recognise the asymmetric nature of the encryption. The response that, "anyone with A's public key could decrypt the message" was not considered to be enough for the mark as it did not make clear that everyone could get this key.

Part (c): This question part required students to explain the purpose of a digital signature and how digital signatures are used. Approximately three quarters of students were able to explain the purpose. More disappointingly, less than half were able to describe how digital signatures were used. Nevertheless, students who knew the topic provided excellent, detailed explanations. The most commonly made mistakes were: to be confused between the hash and the digital signature; to believe that the digital signature was attached to the end of the original message after the original message was encrypted rather than before; and to provide an unclear description of how the hash would be regenerated at the receiver and compared to the transmitted hash. Some students confused a digital signature with a digital certificate. The quality of written communication of almost all responses was satisfactory.

Q15.

Many candidates could give the correct definition of the resolution of an image for part (a).

The most common mistake was to give a definition for the resolution of a VDU instead of the resolution of an image. Fewer candidates were able to define colour depth. The most common wrong answer was to state that the colour depth was the number of colours, rather than the number of bits used to represent the colour of a pixel. Most candidates were unable to calculate the file size for part (c). Candidates should be encouraged to show their working out as this may allow them to get some marks even if their final answer is incorrect. Most candidates were able to give an advantage of vector graphics, although some answers were too vague to be creditworthy. Good answers made it clear that the quality of a bitmapped image deteriorates as it is enlarged whereas a vector graphic does not.

Q16.

The answer for part (a) has been asked before and candidates should be aware that we are after the full name of the law. Many candidates stated only 'copyright' and did not secure the mark. The actual law is the Copyright, Design and Patents Act.

Digital Rights Management has also been asked about before, but many candidates did not secure any marks for part (b). Many candidates answered by stating that DRM prevents one from copying the file, rather than preventing playback if a file has been copied. Discussion about limiting the number of times a file could be played or placing a time restriction onto the file did not secure any marks as this would not stop the sharing of downloaded files which was the point of the question. Candidates need to make sure that they answer within the context of the question. Some candidates answered by stating that it was illegal to share copyrighted files or that, terms and conditions would have to be agreed. Both of these points might be true, but it does not stop the sharing of downloaded files. The usual correct answers were the 'file being encrypted□ and 'playback being limited to one device□.
Candidates sometimes wrote about passwords, codes or PINs to playback the file, rather than the correct answer of a decryption key.

Q17.

While the majority of candidates were able to answer this question well, a significant number had little understanding of this topic and were unsure what was meant by sampling resolution and sampling rate. The definition of Nyquist' s theorem was often vague. Candidates often seemed to have read something about it but couldn' t quite remember what it was; answers often indicated that there was little understanding of the sampling process and sound waves in general.

Q18.

This is the question that also concerns quality of English and was asked around DRM (Digital Rights Management). The ideas about protecting copyright / preventing copying and ensuring artists get paid for their work were well known as were the opposite ideas of problems making legal backups, and not being able to play the items on a range of hardware / software platforms.

Many answered a different question i.e. how DRM works. There were many references to the fact that DRM infringes human rights! This was another example of some candidates not reading the question as many answered with reference to software rather than music / video DRM.

There were many answers arguing that using DRM puts up the cost of the purchased media but this was usually stated in a vague manner. There was also much philosophising about theft and 'right and wrong', but candidates often stated that if you could not afford it (the music or video) then you should get it for free.

Q19.

For question (a) the explanation of what is meant by a pixel was generally not well answered with very few candidates gaining the full 2 marks. The 'smallest picture element' was required for 2 marks to be awarded.

In question (b)(i) most candidates appreciated how the memory contents shown were arrived at from the grid of pixels given in the question. Some candidates did not read the rubric and gave the answer for question (b)(ii) in binary.

For question (c)(i) all that was required was a statement which described each colour being represented by a different number. Some candidates gave detail about numbers mapping to the various amounts of red, green and blue for each colour which was not expected, but was creditworthy.

In the final part of the question (d) despite being popular on the legacy CPT1 paper, answers describing vector graphics were disappointingly poor. Candidates failed to describe the two key points that any drawing is built up as a series of drawing objects and these drawing object types each have their own set of defined properties. Candidates were often unable to give a clear explanation for question (d), but were then able to name typical properties for a circle object.

Q20.

Most candidates understood that the purpose of DRM was to control access to digital media, so as to prevent piracy. Fewer went on to explain that this was done to enforce copyright legislation and to ensure that artists received the income from music sales. Some errantly believed that DRM was a law or a company.

Many candidates were able to explain at least one method of applying DRM, the most common descriptions being of encryption or limiting playback to a particular hardware device or piece of proprietary software. A common, but incorrect response was that DRM could stop the music files being copied, whereas DRM is unlikely to be able to do this. Rather, if the files are copied they could not be played. Some candidates mistakenly continued with their descriptions of why DRM was used or gave advantages and disadvantages of it, rather than explaining how DRM would work. Encryption and encoding are not the same things, nor are a key and a code or password.

Q21.

(a) See earlier comment in the General section of this Report.

(b) All that was required in this question was the association between a number value and a colour, and hence that different numbers are used to represent different colours. The suspicion was that the candidates were not clear of the meaning of the word 'encoding' in the question stem. Some candidates described the idea that the picture was formed by putting together many pixels. A common misconception was that the pixel value stored its location.

(c) A common wrong answer – as seen in a previous examination – described 'data which is stored in the file directory' (not the file header).

(d) (i) Very poorly answered, despite a very similar question on a recent January series question paper.

(e) (i) Well answered.

(ii) Often candidates latched on to the term 'data structure' and then chose from

the stack, queue options, failing to appreciate that an array is referred to as a data structure.

(f) On the one previous question paper on which the algorithm trace used a nested loop, the quality of answers seen was encouraging and the Report commented on this. Alas, the impetus was not maintained, and the number of candidates who were able to score 5 or 6 marks was small. The common error on the better scripts was not to make the final increment of the Counter variable value 6.

(g) (i) Most candidates came up with a valid answer from the large range deemed acceptable.

(ii) Many candidates were able to come up with two restrictions on the choice of identifier names. Some scored 1 mark only by quoting two near identical reasons e.g. cannot contain a 'comma' character followed by 'cannot contain a question mark' character. Some candidates answered their own question e.g. 'cannot store a text character in a integer data type variable'. Other candidates read the question as 'general restrictions' of the programming language and so gave answers such as 'variables must be declared before they can be used,' Answers of this nature were given credit.

Q22.

The topic of this question seemed to be understood very poorly. Many answers were seen where rote-learning was only partially successful and the part-remembered answers made little sense. Real understanding is required to be able to answer these questions successfully.

For part (a) symmetric encryption uses the same key for encryption and decryption, whereas public key encryption uses a public key – private key pair in combination, one to encrypt the other to decrypt.

In part (b), since few candidates understood the difference between symmetric and public-key encryption, the point of this question evaded many candidates. The symmetric key needs to be communicated securely to the other party. Therefore, it must be encrypted with the Public key of the recipient. The recipient can then decrypt it with their own private key. Encrypting with the private key and decrypting with the public key is not appropriate here, as anyone intercepting the message could decrypt the encrypted symmetric key.

Q23.

This question framework was different to that seen on previous papers but candidates generally answered well and were able to relate the diagram given to their basic definitions.

(a) The most popular answers were 'sound recording software' and 'the operating system'.

(b) (i) Many answers simply rearranged the word in the question stem e.g. 'rate and which samples are taken' and so failed to score.

(ii) This was poorly answered, often when the candidate had been unable to write a worthy answer for (i).

(c) Well answered.

(d) (i) Generally candidates scored the one mark. Any answer which suggested that a more 'faithful' recording was obtained was given credit. However 'smoother' sound suggested more samples would be required and so did not score.

(ii) Again, generally well answered. Wrong answers included that it would slow down the processing time or (worst) take more time to sample.

(f) There is a statement at the start of the mark scheme for this question which is indicative of what was expected. Some candidates carried forward answers from a previous similar question which, because of their different context, were deemed unacceptable and included 'part of a word processed file, etc'. The key discriminator was how the bytes(s) would be interpreted by the processor or application software – not by the user sat in front of the application. The computer scientist who wrote typically, 'binary integer, memory address, ASCII character code,' pocketed three very accessible marks, and quickly moved on.

Q24.

Despite being asked on previous papers, the level of candidates' knowledge, possible lack of any skills based work with vector based software, or simple poor expression, all too often meant answers seen were poor.

(a) (i) It is likely that any candidate who had used a vector package for 2 minutes, dragged a rectangle object onto the canvas and changed its line thickness, fill colour and fill pattern style could not fail to score two easy marks .

(ii) Most frequent answers gave only a hint of some understanding, mentioning 'mathematical equations' or similar. Many candidates often talked themselves out of the mark by suggesting that 'the formula is re-calculated or altered'.

(iii) Again a question where, if the experience had included some practical work, the answer would have been forthcoming.

(b) Despite similar questions on previous examination papers, the standard of answers seen for all three parts was poor.

Q25.

(a) Very few candidates appreciated that the issue with encryption of e-mails using symmetric keys is how to get the key from the sender to the recipient. Some wrongly thought that the key would have to be made public, or that all e-mails would have to use the same key.

(b) Most candidates stated correctly that Jack would need to encrypt the message with Jill's public key and then Jill could decrypt it with her private key. Some candidates did not state whose public/private key was required to be used, and so did not gain the marks available.

(c) There seems to be a lot of uncertainty about what a digital signature is or how it might be produced. It is not a signature in the conventional sense. Candidates who gained full marks could explain that the message (before encryption) was hashed into a message digest, which was then encrypted using the sender's private key.

(d) The lack of understanding of digital signatures was further highlighted by the responses to this part of the question. Verifying Jack's digital signature means, to ensure that the message really was sent by Jack, Jack will need to have sent a digital certificate with the message, containing his public key. The digital certificate

needs to be decrypted using the Certificate Authority's public key, ensuring that the digital certificate is genuine. Now the signature sent with the message can be decrypted using Jack's public key. The received (and decrypted) message is hashed and the result is compared to the decrypted signature. If both are the same the message has not been tampered with and is genuine.

Q26.

(a) For the majority of candidates this scored the maximum six marks.

(b) Poorly answered.

(i) Many candidates seemed to think that any electronically produced sound or copied/edited sound files were synthesised sound.

(ii) There were few answers seen which gained credit. Some candidates drew on their own experience and correctly suggested that most mobile phone ring-tones are synthesised. No credit was given for geographic answers such as "at a pop concert" or "in the recording studio".

Q27.

From the January 2006 CPT1 paper there was a clear conclusion that where candidates are able to draw on their own experiences in answering a question, they will generally score marks. This was the rationale for this change to the style of question set on the 'graphics' section of the specification. However, it was the question which generally generated the lowest mark and hence was a disappointing outcome as surely all students will have had some experience at this stage in their learning of the use of both a graphics and vector based drawing software?

(a) (i)(ii) Most candidates were able to state two properties. However they must be encouraged to be precise. An answer of 'colour' is significantly different from 'line colour'. The most common answers were 'colour' and '*x*, *y* coordinates'.

(iii) Candidates with a good understanding were able to describe that a bitmapped graphic when enlarged becomes pixellated and hence distorted; very few candidates were able to express themselves to explain that a vectored drawing simply re-calculates all the drawing list properties for each object.

(b) (i) Most candidates answered four, making the connection that four bits will make possible sixteen different bit patterns, which can then each be used to represent a different colour.

(ii) The better candidates were then able to carry this thinking through to (ii) and complete the 'joined up thinking' that 256 different bit patterns will make possible 256 different colours.

This was a good example of a question where good exam technique pays dividends. The most common answer seen was "Each pixel uses one byte, so 256 colours can be used". All this does is re-word what is given in the stem of the question and more was required to score the mark; typically that "one byte is eight bits, and eight bits have 256 different binary numbers, each of which can represent a different colour".

(iii) An alarmingly large number of candidates (over (50%) assumed that 1KB was 1000 bytes. Candidates need to be familiar with these simple calculations for

bitmapped graphics, as a file's size can be a factor in determining the choice of file type selected when saving a file.

(iv) Very few correct answers were seen. Any bitmapped file contains header data indicating the width, height and resolution of the file.

Q28.

If candidates suggested using password protection for their e-mails in this question, they needed to explain that they were either passwording their system or their user accounts. Encrypting the e-mails was the other obvious answer here.

Q29.

(a) This has been repeatedly examined on previous papers and despite the comments in previous examiners' reports, candidates are still describing "bits of data" or "data sent byte by byte". Others think it is one-way data communication or describe asynchronous data transfer.

(b) This should have been an easy mark. Candidates should have practical experience of saving a bitmap image where there are a number of different colour resolutions possible. This is an excellent example where the use of binary numbers can be given a practical dimension. The understanding required is to make the connections that a 256-colour image will require 256 different numbers to represent each possible colour, and consequently 256 different numbers can be achieved with a single byte to represent each pixel.

Part (ii) was no more than a simple calculation requiring the fact that a kilobyte is 1024 bytes.

Candidates should appreciate the full range of bitmap types; monochrome, 16-colour, 256-colour and 24-bit colour and the subsequent implications for the representation of each pixel.

(c) Well answered, again probably with candidates able to draw on practical experience of music downloads, etc. The most common misconception was the suggestion that the advantage was that you could download faster at the higher encoding rate. The disadvantage would then be poorer sound quality or lost bits/chunks of the sound due to interference.

Q30.

Data transmitted over a network is encrypted to prevent unauthorised users understanding it if intercepted, to prevent the message being altered if intercepted and to identify authentic users. It would not prevent the data from being intercepted; it would just be incomprehensible to any interceptor. A number of candidates gave the same reason in two different ways. 'So that if it is intercepted it can't be understood.' 'So that only authorised people will be able to decode it.'

Q31.

Most candidates appreciated that organisations set rules for acceptable passwords so that they will not be easy to guess or work out. Fewer candidates scored full marks for part (b). The better candidates realised that the characters in the alphanumeric string had to be converted into an equivalent numeric form (they were already in binary). These numbers then needed to be combined in some arithmetical way. Finally the numeric result needed to be mapped onto a two-byte integer, perhaps by using integer remainder division.

Q32.

This question was either very well done, by those candidates who had a clear understanding of the principles involved, or very poorly done by those who only had a vague notion of how this important aspect of security on the Internet works.

(a) Many candidates found it difficult to express clearly what encryption was. A creditworthy response was converting plain text into cyphertext.

(b) Many candidates failed to realise that both A and B had a private and a public key. The answer therefore needed to include whose public/private key should be used.

Sending a message that only B can understand must be encrypted using B's public key, so that only B's private key can decrypt the message.

(c) There seems to be much confusion as to what a digital signature is and the role of a digital certificate. Here is an explanation:

So that the digital signature will show up any tampering of the original message, the digital signature is based on the (date-stamped) message: a hashing algorithm is applied to the text of the message. This produces what is known as a message digest. So that this cannot be substituted when the message is tampered with, it is encrypted with the sender's private key and attached to the message.

The recipient can decrypt the signature with the sender's public key.

To check that the message has not been tampered with: The same hashing function has to be applied to the received message and the resulting message digest compared with the decrypted signature (which was the message digest of the original message). If the two are the same the message is taken as being authentic.

However, how can we be sure that the sender's public key is genuine? This is where the digital certificate comes into play: The digital certificate will be sent with the original message. It includes the sender's public key, encrypted with the Certificate Authority (the trusted party)'s private key. So the recipient first has to decrypt the encrypted sender's public key using the Certificate Authority's public key.

Q33.

Candidates showed some knowledge of the way sound is processed by the computer. Unfortunately, many answers either failed to answer the question or were very superficial.

(a) Most candidates were able to state that Device1 is an analogue to digital converter. Although sound card was accepted this year there is no guarantee that it will be in future questions of this type. In part (ii) many candidates answered the question "How does it convert analogue to digital" rather than "Why is this device necessary". Many of the answers were very superficial.
Credit will not be given for an answer that states: "The analogue to digital converter converts analogue signals to digital signals".

(b) Many candidates scored well here. Speakers were almost universally given as the answer to Device 3.

(c) The answers to this part were very disappointing. Few candidates seemed to understand the way that sound is encoded. There was evidence that the majority of candidates have some idea that it is stored in some binary system but few were able to give a satisfactory explanation.

(d) The answers to this part were even more disappointing. Many candidates failed to answer the question by giving answers relating to the quality of the speakers or the quality of the original sound. Neither answer is relevant to the coding system.

Q34.

(a) Many candidates were able to work out the correct answer to this part showing that they have an understanding of data encoding.

(b) Candidates who answered part (i) generally gave the correct result. ASCII was sometimes given for part (ii) showing that the candidate had not read the question. There continues to be a problem with the spelling of EBCDIC. This is a technical term that should be understood by the candidates and there is no guarantee that misspellings will be given credit in the future.

(c) It was disappointing to see how many candidates were unable to answer this part satisfactorily.

(i) Candidates should be aware that each pixel is stored separately in bit-mapped graphics. Although many candidates stated that the colour would have to be stored, few were able to explain how. A common misconception was that one bit could store a range of numbers.

(ii) There was even less understanding shown of vector graphics. Candidates should appreciate what needs to be stored. Stating that the line would be stored as an equation is insufficient.

Q35.

(a) The analogue to digital converter was well known but the way that sound is coded in a computer system was not. Many answers were trivial or just simply incorrect.

(b) Bit mapped graphics are better understood than vector graphics. There were a number of candidates who confused the display of graphics on the screen with the storage of graphics in the computer system.

(c) The ability to resize without deterioration of the image was fairly well known as was the reduction in file size.

(d) The storage of characters is well understood. A number of candidates failed to obtain full credit by poor explanations but most were able to provide a character coding system correctly.