AQA Computer Science A-Level

4.5.6 Representing images, sound and other data

Past Paper Mark Schemes

Additional Spec Qs AS Paper 2

04	**1**		**Mark is for AO2 (apply)** COMPUTING VHFINMBGZ ;	1

04	**2**		**Mark is for AO2 (apply)** IRMAHG PYTHON;	1

04	**3**		**Marks are for AO2 (apply)** 01010011 01001111 01010011 10111001 00110101 00011010 11101010 01111010 01001001 1 mark - correctly writing out binary for S O S; 1 mark - laying out the key under/by the correct letters; 1 mark - correctly applying XOR;	3

05	**1**		**Marks are for AO1 (knowledge)** A pixel is a picture element; smallest addressable element of a picture;	MAX 1

05	**2**		**Marks are for AO1 (understanding)** run length encoding//RLE;	1

05	**3**		**Mark is for AO1 (understanding)** lossy compression results in lost data / quality from the original version;	MAX 1

05	**4**		**Marks are for AO2 (analyse)** Date/time information; camera settings; **A.** example of camera setting (exposure/aperture) thumbnail; copyright information; **A.** Any other sensible item of information	MAX 2

Additional Specimen Paper 2

10	**1**	**Mark is for AO2 (apply)** ELEPHANT; **A.** letters in uppercase or lowercase or mixed	1

10	**2**	**Marks are all AO2 (apply)** **1 mark**: "RUN" correctly encoded in ASCII as: 01010010 01010101 01001110 **1 mark**: Student has recognised that bitwise XOR operation should be used by either stating this or demonstrating it by correctly XORing at least one character with the key; **1 mark**: Fully correct encrypted ciphertext: 11101011 00011000 00001111 Award the second and third marks if the student has incorrectly encoded RUN into ASCII, but has performed the XOR operation on this incorrect encoding correctly.	3

10	3	**Marks are all AO1 (understanding)** **Why Caesar cipher insecure (MAX 3):** Each plaintext letter is always converted to the same ciphertext letter // it is a monoalphabetic cipher; Frequencies of usage of letters in writing in English well known; Use of frequency analysis of letters in ciphertext can easily reveal which plaintext letters they correspond to; As this is a shift cipher, only need to map one (or a small number) of letters back from ciphertext to plaintext to correctly deduce the mapping used for all letters; There are only 25 / 26 possible mappings from plaintext to ciphertext; Trivial to use brute force // try out all possible mappings from ciphertext to plaintext; **Why Vernam cipher perfectly secure (MAX 3):** Ciphertext contains no useful information about plaintext; Mapping from plaintext to ciphertext (or vice-versa) is different for each letter position in the plaintext/ciphertext; Brute force // trying every possible key/mapping cannot reveal plaintext // will reveal every possible plaintext // too many possible keys to use brute force; Frequency analysis does not help as different plaintext letters can map onto the same ciphertext letter (depending upon position) // as ciphertext letters have uniform/equal probability; **MAX 4**	4

11	1	**All marks AO1 (recall)** Object type; Fill colour; Edge colour; Line/edge width/thickness; Line/edge pattern/style; Fill pattern/style; **NE** colour, co-ordinates **MAX 2**	2

11	2	**All marks AO1 (understanding)** **Advantages of vector graphics (MAX 2):** (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; **Limitations of vector graphics (MAX 2):** Only appropriate for images made of geometric shapes // where it is known what objects an image is composed of; Unsuitable if colour of each pixel is likely to vary // example of a situation in which this is the case eg a digital photograph; Some drawing tools are unlikely to be/won't be available when using vector graphics (eg spray paint, blurring); Can take longer to render an image (for complex images);	3

June 2012 Comp 3

5	(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**	1

5	(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**	1
	(b)	(ii)	As A's public key is available to anyone; Anybody could decrypt it; **MAX 1**	1

5	(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.	

June 2016 AS Paper 2

06	1	**Marks are for AO2 (apply)** 16 * 16 * 2 / 8 = 64 **Mark as follows:** **1 mark:** working out that there are 256 (16*16) pixels in the image **1 mark:** multiplying by 2 **1 mark:** dividing by 8 so that number of bits needed is converted to number of bytes needed **Max 2** if final answer is not correct. Award all 3 marks if final answer is correct.	3
06	2	**Mark is for AO1 (understanding)** Because metadata will also be stored // other data about the image will be stored; **A**. by example eg width in pixels / height in pixels / (colour) depth of image will also be stored	1
06	3	**Mark is for AO2 (apply)** 1;	1

06	4	**Marks are for AO2 (analyse)** Store the colour of a pixel and a count; **A.** by example the count indicates the number of pixels of that colour there are before a pixel of a different colour is used in the image // the count indicates the total number of pixels of that colour there are in a run // the count indicates the number of consecutive pixels of the same colour;	2

June 2017 AS Paper 2

03	1	**Marks for AO2 (apply)** Identification of length (180 s/ 3 * 60), sample resolution (16 bit) and sample rate (44,000 Hz) in working ; **A**. 44 (kHz) for sample rate but do not allow follow through. Performing the correct calculation (3 * 60 * 16 * 44,000 // 180 * 16 * 44,000) **or** showing correct intermediary value (126,720,000 bits / 1,584,000 Bytes) ; **I.** Conversion Final answer 15.84(MB) ; **A.** to fewer significant places as long as 15.84 can be seen in working.	**3**

03	2	**Marks are for AO1 (understanding)** The ADC takes samples of the (analogue/continuous electrical) signal (at regular intervals); **R.** voltage for signal, soundwave, analogue data, sound, waveform for signal. Samples are quantised // the amplitude/height of each sample is approximated to an integer value // the amplitude/height of samples are measured; **A.** voltage for amplitude **A.** digital, number, value for integer value **A.** explanation of how the signal is quantised Each sample is assigned a binary value/encoded as a binary value; **R.** Digital value for binary value **A.** Stored, converted so long as sample is stated	**3**

03	3	**1 mark for AO1 (knowledge) and 1 mark for AO1 (understanding)** **Mark as follows:** **AO1 (knowledge) – 1 mark:** No/only redundant data is lost during the compression process (if using a lossless format); Data is lost when storing using a lossy format; **Max 1 mark** **AO1 (understanding) – 1 mark:** The song can be reproduced identically to the (recorded) original with no loss of quality (if using a lossless format); If stored in a lossy format the quality may limit later editing possibilities; **Max 1 mark** **A.** Recording will be of higher quality / quality of recording will be maintained. **NE.** music will be of higher quality.	**2**

June 2017 Paper 2

02	**1**	**Mark is for AO2 (apply)** KAITLEN; **I.** Case	**1**

02	2	**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**

02	3	**Mark is for AO1 (knowledge)** Symmetric: The same key is used to encrypt and decrypt; **A.** Sender and receiver use same key Asymmetric: Different (but related) keys are for encryption and decryption; **A.** Sender and receiver use different keys **NE.** Symmetric uses one key // asymmetric uses two keys **MAX 1**	**1**

08	1	**All marks AO2 (apply)** **Method (MAX 1):** A multiplication by 20 000; A multiplication by 16; A multiplication by 30; **Answer:** 1200 **A.** 1171.875 (expressed to at least 4 significant figures) this time **If answer is correct and some working has been shown, award all marks, even if working would not have gained credit on its own.** Accept 30*16*20000/8/1000 for **2 marks** or any other reasonable calculation that would arrive at the correct answer, even if the final answer is not stated.	**2**

08	2	**All marks AO1 (understanding)** **1 mark:** As a result of Nyquist's theorem // the sample rate must be at least twice the frequency of the (highest frequency component in the) original signal; **1 mark for any point in this list:** • 20 000 is less than double of 14 500 • 14 500 is more than half of 20 000 • the sample rate would need to be at least 29 000 Hz • with a sample rate of 20 000 Hz frequency components of over 10 000 Hz will not be reproduced faithfully **MAX 2**	**2**

08	3	**2 marks for AO1 (knowledge) and 2 marks for AO1 (understanding)** **AO1 (knowledge): Representation (MAX 2):** Music represented as sequence of MIDI (event) messages; **A.** Music represented as sequence of instructions **R.** Music represented as sequence of notes One example of data that might be contained in a message: • Channel • Note on / note off • Pitch / frequency / note number • Volume / loudness • Velocity • Key pressure / aftertouch	**4**

		• Duration / length • Timbre • Instrument • Pedal effects • Pitch bend • Note envelope; MIDI messages are usually two or three bytes long; First byte of each MIDI message is a status byte (others are data bytes); Bit rate is 31,250 bits per second; MSB value of 1 indicates status byte, 0 indicates data bytes; Status bytes are divided into a command and a channel number (4 bits for each); Sixteen channels are supported; **AO1 (understanding): Advantages of MIDI (MAX 2):** More compact representation; Easy to modify / edit notes // Easy to change values eg octave for entire score //easy to change instruments; Simple method to compose algorithmically; Musical score can be generated directly from a MIDI file; No data lost about musical notes // through sampling; **A.** "better quality" but only if it there is some explanation of this eg "no error introduced during sampling", "no background noise recorded"	

June 2011 Comp 1

09	The number of pixels/dots; per cm/inch/unit of measurement;	**2**

10	The number of bits used to represent (the colour/greyscale value); **R.** number of (different) colours of a single pixel;	**2**

11	50;;// 10*10;*4÷8;//100; ÷2;//100;*0.5; **MAX 1** if final answer not correct	**2**

12	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**

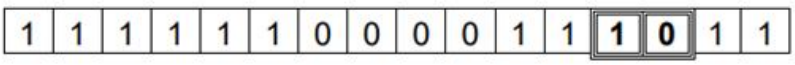
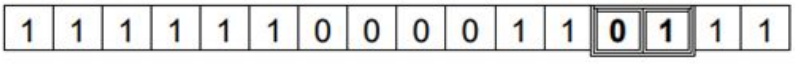
June 2012 Comp 1

05	300; * 2; // 600;; NOTE: award 1 mark for doubling an incorrectly calculated highest frequency	**2**

06	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**

07	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**

08	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**

11	(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**
12	 ;; //  ;; **Mark as follows:** 13th and 14th bits correct; Other bits correct;	**2**
13	8*8 =64; * 2 = 128; ÷ 8 = 16; // 8*8*2÷ 8;;; 16;;; **A.** 128 bits as being worth 2 marks	**3**

14	(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**

15	(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**

June 2013 Comp 1

15	16 (bit); **A.** 2 bytes	**1**

16	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**

17	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**

18	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**

Specimen AS Paper 2

05	**1**		**Marks are for AO1 (knowledge)** Encryption is the encoding of a message; conversion of plaintext into ciphertext; so that other parties cannot read; message can only be decrypted by the authorised receiver; **Max 2 marks**	MAX 2

05	**3**		**Mark is for AO2 (analyse)** (Large) software libraries have many lines of code; Cryptography software is complex; (Open source software) programmers are volunteers; (Open source software) library has limited funding; tracing the effect of one line of code is hard/time consuming; (Heart beat) functionality was not critical to the running of the code // code ran without any noticeable problems so didn't raise concerns. Code review (of OpenSSL) was defective; No-one needed to change this code for two years so they presumed it worked and did not inspect it; **Any 1 from above. Max 1**	MAX 1

05	**4**		**Marks are for AO2 (analyse)** **1 mark:** Reasons for: Max one Detection of illegal activities; Monitoring of other states / countries; Protection of national interests; **1 mark:** Reasons against: Max one Invasion of privacy; Commercial secrecy;	2

08	**2**		**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

08	**3**		**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

Specimen Paper 2

05	**1**	**Mark is for AO2 (apply)** Grey Pixel: 00 White Pixel: 11; **Must have both correct to achieve mark**	1

,

05	**2**	**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

05	**3**	**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

05	**4**	**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

05	**5**	**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;	3
		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);	

10	**1**	**All marks AO1 (understanding)** **1 mark:** A will encrypt the message using **B's public;** key. **1 mark:** The message will be decrypted by B using **B's private;** key.	2

10	**2**	**All marks AO1 (understanding)** **1 mark:** Detect (unauthorised) changes to message; **1 mark:** Authenticate sender's identity // confirm who sent it;	2