Accredited

Computing

GCSE

COMPUTING – J275

Sample Material B2

A452

www.ocr.org.uk/computing

OCR
Oxford Cambridge and RSA

Disclaimer on use of Sample Material

Confidentiality

These tasks are taken from legacy Controlled Assessment tasks, undertaken and submitted by candidates. Where possible, we have removed all identifying information from these assessments. Should any data remain, you are requested to treat this confidentially and inform OCR as soon as possible highlighting the data concerned.

Use of URS Sheets and Sample Material

These tasks have all been moderated as part of the relevant exam series in which they were submitted and the marks submitted have all been allowed to stand. However, schools should bear in mind that this only indicates that the **overall assessment** of the Controlled Assessment is within tolerance and not necessarily each individual mark band. There may be instances where the mark scheme has been applied too generously, or similarly too harshly. This would have been identified in the reports to the centre – but will not be evident from URS alone. The spirit of the release of these samples is to give teachers better understanding of what High, Medium and Low graded coursework would feel like as an entity, rather than exact definitions of requirements for mark bands independently.

The provision of high graded does **not infer** that this is the only, or best way of writing up a Controlled Assessment Task. Candidates are encouraged to map their personal journey through the tasks. Writing frames, or 'guides' for documentation are against the spirit of the coursework and constitute malpractice.

Each set of materials released contains a High, Middle and Low grade band. This should allow teachers to gain good understanding of the general standard of work quality required for each mark band, and as a whole – especially when comparing each set side by side.

Teachers are encouraged to seek further support when they feel clarification is needed in applying the mark scheme. We would also recommend regular CPD in respect of Controlled Assessment delivery and marking.

Accuracy

All work has, where possible, remained unaltered from the original submission. There may well be grammatical errors and poor layout in diagrams. This is to allow better matching of mark band criteria, where specific bullet points refer to quality of Spelling, Punctuation and Grammar, and also ease of navigation etc. Any significant changes are clearly marked. Some data that is perceived sensitive may be blocked out in black.

GCSE Computing Controlled Assessment

Unit A452 Practical investigation

Unit Recording Sheet

Please read the instructions printed on the other side of this form. **One** of these Unit Recording Sheets, suitably completed, should be attached to the assessed work of **each** candidate.

Unit	A452		Year	
Centre Name			**Centre Number**	
Candidate Name			**Candidate Number**	

	Guidance			Teacher Comment	Mark
Practical investigation	There may be limited evidence of any practical investigation. The evidence supplied is minimal with limited relevance to the set task. The practical evidence may be largely the result of group or teacher led activity with limited input from the student. 0 = no response or responses not worthy of credit **[0 - 5]**	There is evidence of a practical investigation. The evidence supplied is documented clearly and is relevant to the set task. There is evidence of individual research beyond the group activity and any teacher led activity. The practical investigations show signs of planning but there may be omissions made in assessing the consequences. **[6 - 10]**	There is evidence of a well-structured practical investigation. The evidence supplied is well organised and clearly relevant to the set task. There is extensive evidence of individual practical investigation beyond the group activity and any teacher led activity. The practical investigation shows clear signs of planning and a structured approach, providing a complete investigation of the set topic area. The practical investigation has been carried out with skill and due regard to safety issues. **[11 - 15]**	The student has successfully completed the practical investigation and this is evidenced in their write-up. The write-up is easy to follow but it lacks detail, it is not detailed enough for more than mark band two. There is some evidence of planning and some evidence of research (web link) but this could be more extensive.	7 **Max 15**

Effective and efficient use of techniques	The techniques used will produce partially working solutions to a small part of the problem. 0 = no response or responses not worthy of credit **[0 - 3]**	The techniques will be used appropriately giving working solutions to most of the parts of the problem. Some parts of the solution may be executed in a partial or inefficient manner. **[4 - 7]**	The techniques are used appropriately in all cases giving an efficient, working solution for all parts of the problem. **[8 - 10]**	They have successfully completed all the tasks in the practical investigation. They have evidenced working solutions for all tasks that show technical ability and understanding.	8 **Max 10**
Technical understanding	The candidate demonstrates a limited understanding of the technical issues related to the scenario. Little detail is presented. There is limited indication of any evidence provided being analysed. There is limited use of technical terminology. 0 = no response or responses not worthy of credit **[0 - 3]**	The candidate demonstrates a reasonable understanding of the technical issues related to the scenario. The amount of detail presented is adequate to support the arguments. There is some analysis carried out on the evidence collected. Technical terminology is for the most part used appropriately. **[4 - 7]**	The candidate demonstrates a thorough and secure understanding of the technical issues related to the scenario. A wide range of relevant and detailed information is presented. The evidence which has been collected is fully analysed. Technical terminology is used correctly. At the top end of the band, this will be extensive and confidently used. **[8 - 10]**	The learner's written report is generally well presented. It is easy enough to follow and gives a good sense of the investigation undertaken. They have explained some of their formulae but this could have been more detailed. There is enough detail to warrant mark band two, but not enough for mark band three.	6 **Max 10**

Conclusions and evaluation	Conclusions are limited with little justification. The solution is presented with limited evidence of testing. Information may be ambiguous or unclear. There is limited reference to evidence. The evidence of written communication is limited with little or no use of specialist terms. There are many errors in spelling, punctuation and grammar. The evaluation may be simplistic with little or no relevance. 0 = no response or responses not worthy of credit **[0 - 3]**	The material has structure and coherence with justifiable conclusions being reached although there may be some omissions. There is evidence that the solutions have been tested for basic functionality. Candidates have produced a sound evaluation which reviews some aspects of the task. There is evidence of good written communication using some specialist terms. There are few errors in spelling, grammar and punctuation. Specialist terms are used appropriately and for the most part correctly. **[4 – 7]**	Thorough and convincing conclusions have been reached, which are borne out by the research carried out by the candidate. The solutions are fully tested and there is little doubt that the solutions presented are fully functional. This material has been presented in a clear and relevant way which is simple to navigate. A high level of written communication is obvious throughout the task and specialist terms/technology with accurate use of spelling is used. Grammar and punctuation are consistently correct. The evaluation is relevant, clear, organised and presented in a structured and coherent format. **[8- 10]**	The candidate shows screenshots of aspects of the solutions working, and they state that they have tested it and that it works - but they have not produced the evidence to support this. There are brief conclusions are provided at the end of each task but these are not sufficient for more than mark band one. They have given a good response to the final question but this could have been aided with evidence of researching further afield.	5 **Max 10**
				Total/45	**26**

Guidance on Completion of this Form

1 **One** sheet should be used for each candidate.
2 Please ensure that the appropriate boxes at the top of the form are completed.
3 Using the guidance identify the most appropriate mark range for the work and enter the mark awarded for each element in the mark column.
4 Add appropriate comments to assist the moderator in the 'Teacher Comment' column.
5 Add the marks for the strands together to give a total out of 45. Enter this total in the relevant box.

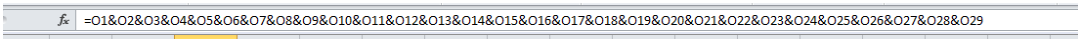
A452 Encryption

1. (i) Set up spreadsheet and add to it to decrypt message.

Evidence

	A	B	C	D	E	F	G	H	I
1	c	n	o	*					
2	o	g	o	y					
3	m	*	d	o					
4	p	i	*	u					
5	u	s	f	*					
6	t	*	o	*					
7	i	g	r	*					
8									
9	encrypted message					decrypted message			
10	cno*ogoym*dopi*uusf*t*o*igr*					computing*is*good*for*you***			
11									

Formula



I used a simple formula to decrypt the message into its plain text. I did this by transferring each individual letter of the encrypted message to a separate cell marked 'encrypted message' using a concatenate function, then selecting every fourth letter and placing them together using another concatenate function. I repeated this starting from 1, 2, 3 and 4 until I had the original message. I then placed the letters together in the cell titled 'decrypted message'. This works because the grid to enter the message that you want to be decrypted is a 4x4 grid, which selects its letters along the X-axis while you enter the message on the Y-axis. This means that every fourth letter in the encrypted message is the next letter in the decrypted message. Upon attempting task (ii) I found that I could not find any way to produce the same results as task (i) in a more simple way without using a Microsoft Visual Basic Macro.

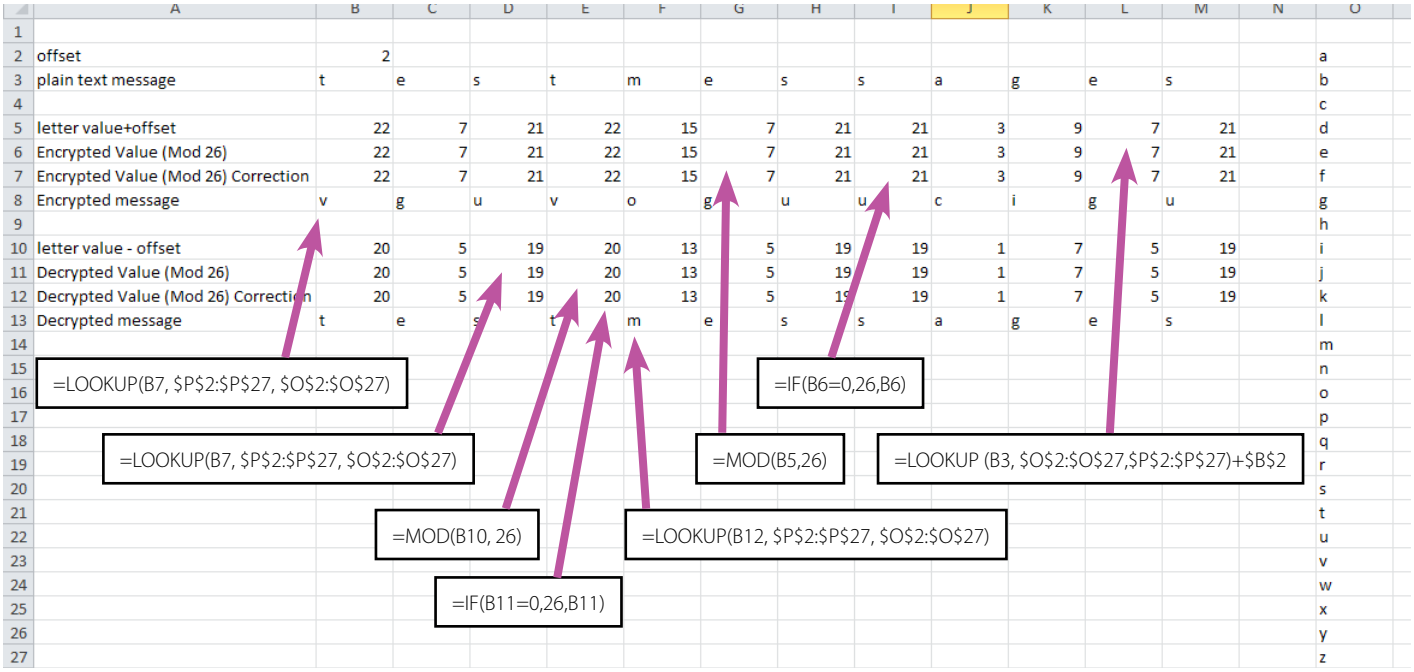
Testing

I know this works because the test phrase 'computing*is*good*for*you***' encrypts into 'cno*ogoym*dopi*uusf*t*o*igr*' and then back into 'computing*is*good*for*you***'.

(ii) Upon attempting task (ii) I found that I could not find any way to produce the same results as task (i) in a more simple way without using a Microsoft Visual Basic Macro.

2. Set up spreadsheet and add to it to decrypt message.

Evidence



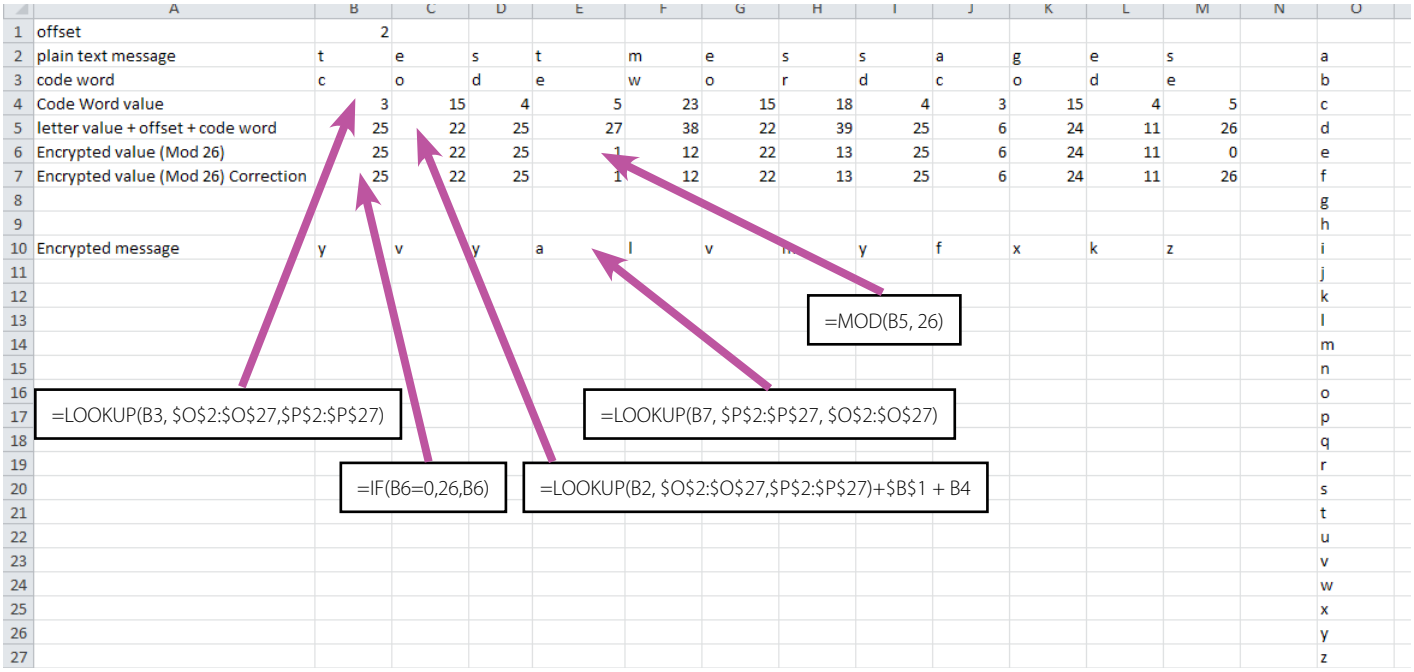
In this task I was making a cyclic substitution cipher. A cyclic substitution cipher works by taking an offset and applying it to a message. For example, if the offset was 2, A would become C, D would become F, G would become I, ECT. I did this by using a LOOKUP function to obtain the value of each letter in the message from the O and P columns and then adding an offset variable (shown in the 'offset' cell). I would then use the resulting number as a new value for the letters of the encrypted message. However, if the offset was larger than the difference between the letter value and 26, it would cause an error. I then researched MOD functions and fixed this by adding a MOD function that divides the answer by 26, thus creating the effect of cycling. I then changed the encrypted message to take the value from that row instead. In order to decrypt the message I created a function to subtract the offset from the letter value of the encrypted message; upon doing this, I received some negative values. I fixed this by creating another MOD function. A weakness of the way I implemented this cipher into Excel is that the MOD statement used would cause any 26s entering the formula to come out as 0, and thus be unusable. I fixed this by using an IF statement to change any 0s in the result row back into 26s.

Testing

I know this works because an offset of 2 and the message 'testmessages' would produce an encrypted message of 'vguvoguucigu' which then decrypted into 'testmessages'.

3. set up a spreadsheet to implement a double key encryption method.

Evidence



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	offset	2													
2	plain text message	t	e	s	t	m	e	s	s	a	g	e	s		a
3	code word	c	o	d	e	w	o	r	d	c	o	d	e		b
4	Code Word value	3	15	4	5	23	15	18	4	3	15	4	5		c
5	letter value + offset + code word	25	22	25	27	38	22	39	25	6	24	11	26		d
6	Encrypted value (Mod 26)	25	22	25	1	12	22	13	25	6	24	11	0		e
7	Encrypted value (Mod 26) Correction	25	22	25	1	12	22	13	25	6	24	11	26		f
8															g
9															h
10	Encrypted message	y	v	y	a	l	v	m	y	f	x	k	z		i
11															j
12															k
13															l
14															m
15															n
16															o
17															p
18															q
19															r
20															s
21															t
22															u
23															v
24															w
25															x
26															y
27															z

In this task I was improving my spreadsheet by adding an algorithm that decrypts a message created by the cypher in task 3. This works by taking the value of each letter in the code word and applying it like an offset to its adjacent letter in the message. I created this by taking the previous substitution cipher, added new rows for the code word and its letter values and modified the "Letter value + offset" and the "letter value – offset" into "letter value + offset + code word" and "Letter value – offset – code word". A weakness of the way I implemented this cipher into Excel is that the MOD statement used would cause any 26s entering the formula to come out as 0, and thus be unusable. I fixed this by using an IF statement to change any 0s in the result row back into 26s.

Testing

I used the previous test message, 'testmessages', with a code word of 'codewordcode' to produce the encrypted message of 'yvyalvmyfxkz'.

4. Develop your spreadsheet to decrypt a message encrypted using the double key method described above.

offset		2													
plain text message	t	e	s	t	m	e	s	s	a	g	e	s			
code word	c	o	d	e	w	o	r	d	c	o	d	e			
Code Word value	3	15	4	5	23	15	18	4	3	15	4	5			
letter value + offset + code word	25	22	25	27	38	22	39	25	6	24	11	26			
Encrypted value (Mod 26)	25	22	25	1	12	22	13	25	6	24	11	0			
Encrypted value (Mod 26) Correction	25	22	25	1	12	22	13	25	6	24	11	26			
Encrypted message	y	v	y	a	l	v	m	y	f	x	k	z			
letter value - offset - code word	20	5	19	-6	-13	5	-7	19	1	7	5	19			
Decrypted value (Mod 26)	20	5	19	20	13	5	19	19	1	7	5	19			
Decrypted value (Mod 26) Correction	20	5	19	20	13	5	19	19	1	7	5	19			
Decrypted message	t	e	s	t	m	e	s	s	a	g	e	s			

In this task I was improving my spreadsheet by adding an algorithm that decrypts a message created by the cypher in task 3. I did this by subtracting the offset and code word values from the encrypted message values instead of adding them to the plain text values. A weakness of the way I implemented this cipher into Excel is that the MOD statement used would cause any 26s entering the formula to come out as 0, and thus be unusable. I fixed this by using an IF statement to change any 0s in the result row back into 26s.

Testing

I used the previous test message, 'testmessages', with a code word of 'codewordcode' to produce the encrypted message of 'yvyalvmyfxkz'. It then successfully decrypts back into 'testmessages'.

5. Devise and implement a more secure method of encryption than that shown in tasks 2, 3 and 4.

Evidence

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	offset	2													
2	plain text message	t	e	s	t	m	e	s	s	a	g	e	s		a
3	code word	c	o	d	e	w	o	r	d	c	o	d	e		b
4	Code Word value	3	15	4	5	23	15	18	4	3	15	4	5		c
5	letter value + offset + code word	25	22	25	27	38	22	39	25	6	24	11	26		d
6	Encrypted Value (Mod 26)	25	22	25	1	12	22	13	25	6	24	11	0		e
7	Encrypted Value (Mod 26) correction	25	22	25	1	12	22	13	25	6	24	11	26		
8	Encryption result 1	y	v	y	a	l	v	m	y	e	x	k	z		g

In this task I was making my previous cyclic substitution cipher more secure by implementing some more security features.

10	Encryption 2	y	l	e
11		v	v	x
12		y	m	k
13		a	y	z
14				
15	Encryption result 2	ylevvxymkayz		

I originally tried an idea involving a collection of different offsets and code words that each affected the message result in different ways. I decided against this because, once I tried it, I realised that it was creating errors in the 'value correction' row.

Instead, I decided to implement the cipher that I used in task 1, which, upon research (http://www.princeton .edu/~achaney/tmve/wiki100k/docs/ Transposition_cipher.html), I found out is called a route transposition cipher. I did this by using code similar (if not identical) to the code I used in task 1 to create a 3x4 grid which the encrypted message is placed into from top to bottom; the text is then concatenated from left to right in the cell marked 'encryption result 2'. This would further encrypt it, making the message further away from the original text, thus making it harder to decrypt.

17	Decryption 1	y													p
18		l													q
19		e													r
20		v													s
21		v													t
22		x													u
23		y													v
24		m													w
25		k													x
26		a													y
27		y													z
28		z													
29															
30	Decryption result 1	yvyalvmyexkz													
31															
32	Character Division	y	v	y	a	l	v	m	y	e	x	k	z		
33															
34	Decryption 2	20	5	19	-6	-13	5	-7	19	0	7	5	19		
35	Decrypted Value (Mod 26)	20	5	19	20	13	5	19	19	0	7	5	19		
36	Decrypted Value (Mod 26) Correction	20	5	19	20	13	5	19	19	26	7	5	19		
37	Decryption result 2 (Original message)	t	e	s	t	m	e	s	s	z	g	e	s		
38															

I decrypted this by separating the characters and taking every third character; I concatenated the result into the cell marked 'Decryption result 1'. From then on, the characters are decrypted and placed through the same decryption process as in tasks 2, 3 and 4. A weakness of the way I implemented this cipher into Excel is that the IF statement used can only subtract or add 26 once, this means that only a small offset can be used otherwise the number that enters the value correction cell is over 52 or the number that enters the additional value correction cell is under -52, resulting in a value over 26 or under zero entering the encryption result 1/decryption result 2 cells.

Testing

The plain text I used was 'testmessages'. I placed it into the 'plain text message' cell and the values from each character were added to an offset of 2 and the values of each letter from the code word (codewordcode). I then put the result through a MOD formula to simulate cycling through the alphabet; this produced the message 'yvyalvmyfxkz'; this was then turned back into letters and placed into the row 'Encryption result 1'. The grid cipher then automatically takes the characters in 'Encryption result 1' and places them into a grid, reading top-to-bottom. A concatenate formula than reads the grid left-to-right and concatenates what it reads into the cell marked 'encryption result 2', producing the message 'ylfvvxymkayz'. To decrypt, a MID formula separates the characters; a concatenate formula takes every third character and concatenates the result into the cell marked 'Decryption result 1', resulting with the same result as in 'Encryption result 1'. From then on, the characters are placed through the same decryption process as in tasks 2, 3 and 4. In the end, the text was successfully decrypted back into 'testmessages'.

6. Write a conclusion about the effectiveness of the encryption methods described in this assignment

The cipher used in task 1 is called a route transposition cipher. This cipher is fairly secure since it encrypts the cipher-text into an unrecognisable form and does not require the transfer of multiple keys between the sender and receiver of the message. However, the cipher-text has the same characters as the encrypted message, meaning it can be decrypted without the key more easily than other encryptions can.

The cipher used in task 2 is called a Caesar cipher. This cipher is very secure since it scrambles the cipher-text into an unrecognisable form, like any good cipher should. It also only requires the transfer of a single key between the sender and the receiver: the offset. However, through frequency analysis, the message can be deciphered without the key more easily than other encryptions.

The cipher used in task 3 is an extension of the Caesar cipher used in task 2. This extension is the addition of a code word to act as a shift key. This is more secure than the Caesar cipher in task 2 because the code word affects different characters in the original message differently from each other, meaning that each character in the encrypted message could be a different distance from its original character than another character from the same encrypted message. However, it does require that two keys are shared with the receiver.

The cipher used in task 4 is the same cipher used in task 3, but with a decryption algorithm added. This is not more or less secure than the cipher used in task 3 because it is the exact same cipher, and would produce the same encrypted result. The cipher used in task 5 is a combination of the cyclic substitution cypher used in task 4 and the route transposition cipher used in task 1. This is more secure than the cipher used in task 4 because it scrambles the characters as well as changes them, this protects the information against frequency analysis and the reassembly of the message according to the characters. However, it does require that 3 keys are shared with the receiver of the message instead of 2.

All of the methods described above rely on private, pre-shared information (the sharing of keys) and are thus not useful on the internet. Public-key encryption does not rely on private, pre-shared information and thus is useful on the internet. This is because it uses two keys; a public key and a private key. The private key is not given out to anyone while the public key is freely distributed. The public key cannot decrypt the information but the private key can. This makes public-key encryption useful on the internet because the public key, which is the only key that is transferred across the internet and thus usable by hackers, cannot decrypt data, only encrypt it.

The small print

We'd like to know your view on the resources we produce. By clicking on the 'Like' or 'Dislike' button you can help us to ensure that our resources work for you. When the email template pops up please add additional comments if you wish and then just click 'Send'. Thank you.

If you do not currently offer this OCR qualification but would like to do so, please complete the Expression of Interest Form which can be found here: www.ocr.org.uk/expression-of-interest

OCR Resources: *the small print*

OCR's resources are provided to support the teaching of OCR specifications, but in no way constitute an endorsed teaching method that is required by the Board and the decision to use them lies with the individual teacher. Whilst every effort is made to ensure the accuracy of the content, OCR cannot be held responsible for any errors or omissions within these resources. We update our resources on a regular basis, so please check the OCR website to ensure you have the most up to date version.

OCR acknowledges the use of the following content:

Square down and Square up: alexwhite/Shutterstock.com

Please get in touch if you want to discuss the accessibility of resources we offer to support delivery of our qualifications: resources.feedback@ocr.org.uk

We will inform centres about any changes to the specification. We will also publish changes on our website. The latest version of our specification will always be the one on our website (www.ocr.org.uk) and this may differ from printed versions.

ocr.org.uk/alevelreform
OCR customer contact centre

General qualifications
Telephone 01223 553998
Facsimile 01223 552627
Email general.qualifications@ocr.org.uk