OTS Masterclass Codebreaking and Ciphers

Session Leader Notes

Inspiration:

Cryptography is a fascinating topic and makes today's world possible. The ways we keep our messages secret has improved significantly over millennia, moving from very simple ideas to increasingly complex and computationally difficult techniques as we got better at cracking the codes and ciphers used. Working out how to crack encryption and read secret messages is a skill which has always been in high demand and is a very interesting career for many mathematicians.

This Masterclass explores simple techniques for creating and reading secret messages. Students will focus on ciphers, where each letter is replaced or moved to create an encrypted message. We examine two different types of cipher, the route cipher, where the letters in the message are moved around (this is a transposition cipher), and the Caesar cipher, where letters are replaced (this is a substitution cipher). Students will hear how these types of encryption were used (even relatively recently), will create their own ciphers to try on their friends and will work on cracking some of the ciphers. These activities will teach them the basics of encryption, strategic thinking and how to think logically to solve a problem. They will also give them the tools to write their own secret messages at home or in the classroom.

Overview of Activities:

- Individual/group work – Route cipher encryption: activities to practice encrypting messages using a simple method to swap their order.
- Individual/group work – Route cipher decryption: activities to practice decrypting messages using the same method to work out how to unscramble the cipher text (i.e. the encrypted message).
- Individual/group work – Breaking the route cipher: activities to practice cracking this cipher so that the text can be read without knowing the key information usually needed for encryption and decryption (can be left out for shorter sessions).
- Individual/group work – Caesar cipher: working out how to encrypt and decrypt messages using a shift of 3. Making their own Caesar wheels (with a set shift) to encrypt their own messages and challenge friends.
- Whole class activity – Breaking the Caesar cipher: the whole group puts their collective brains to the test to crack a Caesar cipher, each testing a different shift.
- Discussion (if time) – How can we make ciphers harder to crack? Talk about some of the more involved methods of encryption and how they can be cracked – mention frequency analysis, the Vigenère cipher, the enigma and the way it was cracked, and internet security.

Additional activities are available if there is time, or as take-home activities – see worksheet list below.

General Masterclass resources needed:

- Register of children
- Consent forms and emergency information to hand
- Stickers and markers for name badges
- Adult register
- Ri child protection policy
- Paper and pencils/whiteboards for workings
- 2 different coloured post it note pads
- Settling activity if not included in specific Masterclass
- Drinks and biscuits

Specific resources needed (available on slides or separately in worksheet folder):

- Worksheet printouts:
    1. Route Cipher Encryption – one each
    2. Route Cipher Decryption – one each
    3. Breaking the route cipher – one each [could be left out for a shorter session]
    4. Caesar cipher – one each

- Caesar wheels printouts*:

    1. With a shift of 3, printed on card from the template & cut out – one each
    2. A class set of Caesar wheels, each one with a different shift, printed on card from the template and cut out (repetition will be needed for a group of over 26 – ensure that at least one of the students has a shift of 14, preferably more; you may not wish to use shift 0)
    3. Blank Caesar wheels for students to make their own, enough for at least one each (have spares in case of mistakes)

    *Instead of the above fixed wheels, you could just print copies of the **Rotating Wheel** template onto card (one per student) and use **split-pins** to make the wheels rotate. You will need to make sure they are on the correct setting for each activity, and when you are trying to break the Caesar cipher you will need to give out "shift numbers" to each student to ensure that all are trying a different number. Please bear in mind that with some students this can be more difficult as they often accidentally move the wheel between each letter, giving them the wrong shift. **Paperclips** to secure the wheels for each question and a lot of adult helpers may help to mitigate this problem.

Additional worksheets for extra time or to take home:

- Worksheet 5: Unbreakable route ciphers (this does not have an explanation on the sheet, so only use accompanied by the slides if you have extra time)
- Worksheet 6: Take-home worksheet on the rail-fence cipher

Support resources:

- Templates for the Caesar wheels (called codewheels in the filenames)
- Worksheet solutions

Things to prepare in advance

- Print worksheets and resources as detailed above – cut out the Caesar wheels
- Gather general Masterclass resources

Ask the Ri

Don't forget to collect any questions which arise, and email them to the Masterclass team at the Royal Institution: masterclasses@ri.ac.uk

Feedback

We would very much welcome your feedback on this session. If you have time, please collect feedback from the students at the end of the Masterclass and send it through to us. We would also appreciate feedback on how you have used the session, what you think worked well and what improvements would be useful.

Time plan of Masterclass:

Slides & Time	Overview	Activity
Slide 1	**Can you read it?** Challenge for students to think about as they arrive	Can the students break the 'code' (actually a cipher) and read what is on the screen?
Slide 2	**Off the Shelf: Codebreaking and ciphers** Introduction	Today we will be looking at codes/ciphers, working out how to make coded messages and crack some codes.
Slides 3-8 5 mins (5 mins)	**Introduction to the Ri** *[Only include these slides for the first session in the series – otherwise remember to hide the slides before you start the Masterclass]*	Use these slides to introduce the students to the work of the Ri and other ways they can get involved – see notes on the slides for more detail. In particular: • The Ri is a science communication charity which has been around since 1799. We've got a huge amount of history and lots of famous scientists lived and worked at the Ri. Most importantly, we've always been about communicating science to the general public – and that's something we still do today. We do talks and activities for the public as well as with schools all across the UK. • There are lots of family events at our building in London, including family fun days and holiday workshops just like the Masterclasses. • The CHRISTMAS LECTURES are for young people and are on television at Christmas time, looking at a different topic every year. We've got an archive on our website of all of the recent series plus many of the older ones. The CHRISTMAS LECTURES are what started the Masterclass programme. See slide notes for links. • We have a YouTube channel with lots of videos for people interested in science (and maths engineering, computer science…), especially our ExpeRimental series which is all about doing experiments at home. • Students are part of a big family of Masterclass attendees – we have been running Masterclasses since 1981. • Students at series running within reach of London will be invited to a Celebration Event at the Ri in June/July. • You can become an Ri Member to get more involved with what we do (and enter the ballot to buy tickets to the CHRISTMAS LECTURES filming).
Slides 9-11 5 mins depending on discussion (10 mins)	**Can you read it?** Discussion of introductory work	*Slide 9:* **Who was able to break this code? What does it say?** – write answer on board *Slide 10:* This is called the phonetic alphabet, and it helps you to spell things over the phone. It is a type of cipher because you are replacing letters. A lot of the codes which we talk about aren't technically codes – they are ciphers. A code would be where you are replacing whole words with other words. **Can you think of any similar ciphers which are used?** – Morse code, semaphore, numbers on a phone. *Slide 11:* These ciphers help us to transmit messages. But what about when we want to keep something secret? **What ways could we do that?** **Ideas from the class.**

Slides & Time	Overview	Activity
Slides 12-13 2 minutes (12 minutes)	**Definitions, Transposition ciphers** Discussion of definitions – speaker to lead, input from students *Slide 12 animation: click to reveal definitions* *Slide 13 animation: click for examples of different letter rearrangements – the first example is randomly scrambled, but the second and third have been mixed up in an ordered way and can be decrypted*	*Slide 12:* Today we will be creating secret messages using ciphers and working backwards to read what other messages say. It's useful to be able to use the proper terms to talk about these things. **Does anyone know what 'encryption' means?** This is where you code or cipher a message. **What does 'decryption' mean?** This is where you have a message which is already been encrypted and you need to decode or decipher it so that you can read it. The last term I want to show you is '**Key'. Any ideas what this might mean?** Like the key that you use to unlock a door, the cipher key is the information you need to be able to unlock or decipher an encrypted message – that is to turn the message back into the original one that you can read and understand. *Slide 13:* The first thing we are going to do today is look at a type of cipher called a **transposition cipher**. These types of ciphers work by swapping the order of the letters around – but we can't just do it randomly. I can write these letters in any order I like, and no-one would be able to crack the cipher – but the person I am sending it to wouldn't be able to read it either. I could swap the order of the letters in specific ways though, using special rules; there is a set order for the second and third ciphers on the board, even if it doesn't look like it at first glance. This method of encrypting messages has been used for a long time and was still used in the world wars as it was quick and easy, as long as you had something to write on and knew the type of cipher being used. It was used mainly on the battlefields as the soldiers didn't have time to try and decipher even simple messages that they might have intercepted, and it wasn't used for really important information. The important messages from the leaders of each side had much stronger encryption.

Slides & Time	Overview	Activity
Slide 14 3 mins – slide 5-10 mins worksheet (25 mins)	**Route cipher** (encryption) How to encrypt a message using a route cipher Speaker to demonstrate method; during activity, speaker and helpers to circulate *Slide animation: Click to show steps of encryption – could write a separate example on the board. If doing this, ensure message has a square number of letters*	***Resources:*** *Worksheet 1, one each (route cipher encryption worksheet)* We are going to look at a transposition cipher called the 'route cipher'. We write the letters in a grid in one direction, and then encrypt the message by reading them in another direction. You just have to know which directions to use. To make it easier, we will also write actual messages in lowercase and encrypted messages in capitals. We call our original message 'plain text' and our encrypted message 'cipher text'. Today, we are going to write our actual message going across and read off our enciphered text going down. So, to encrypt 'send cakes' we will write the letters along the rows in a grid; To get our enciphered text we read down the columns and write each letter down in that order. **Using this rule, have a go at worksheet 1.**
Slide 15 Slide & worksheet 10 mins (35 mins)	**Route cipher** (decryption) How to decrypt a message where a route cipher has been used to encrypt it Speaker to demonstrate method; during activity, speaker and helpers to circulate *Slide animation: Click to show steps of decryption*	***Resources:*** *Worksheet 2, one each (route cipher decryption worksheet)* **How do we decrypt these messages?** We need to go backwards. We write the encrypted letters down the columns of a grid, then read the actual message sideways along the rows. *You could write a separate example on the board. If doing this, ensure message has a square number of letters.* **Using this rule, have a go at worksheet 2.**
Slide 16 5 minutes, depending on discussion (40 mins)	**Route cipher decryption** More in-depth discussion of how to decrypt the route cipher. Ideas from students *Slide animation to reveal each point*	In all the questions you have done so far, you know the size of the grids. What happens if we don't? If we have the wrong grid-size, we won't be able to read the message. **Can we figure out the grid size – any ideas?** *NOTE: For shorter Masterclasses, you may choose not to explore this section – leave it as a discussion and do not include slides 17-18 or the activity on the worksheets (saves 25 mins).*

Slides & Time	Overview	Activity
Slide 17 Slides 17-19: 20 mins (60 mins)	**What size grids?** Exploration of cracking the route cipher. Speaker to go through slides, asking students questions as they go through. *Slide animation: Click to go through questions/answers and to reveal grids*	***Resources:*** *Worksheet 3, one each (breaking the route cipher worksheet)* *Slide 17:* We might know that we need to use a square grid. This makes things easier. **Does anyone know what a 'square number' is?** It is when a number has been multiplied by itself. If we are using square grids, the number of spaces will always be square numbers. This helps us work out what size to use. **What are the first few square numbers?** *(Write on board)* – 1x1=1; 2x2=4; 3x3=9; 4x4=16; 5x5=25. So, we need to fit our messages into grids of this size. First, we need to count the letters. 'Send cakes' has 9, so would fit into a 3x3 square. 'Ham sandwich' has more than 9 letters, but less than 16 – **can we fit it into a square?**
Slide 18, 19 Slides 17-19: 20 mins (60 mins)	**What size grids?** Exploration of cracking the route cipher. Speaker to go through slides, asking students questions as they go through. During activity, speaker & helpers to circulate *Slide animation to reveal each point*	***Resources for slide 19:*** *Worksheet 3, one each (breaking the route cipher worksheet)* *Slide 18:* When we don't know whether the grid is square it is a little trickier – we have to try all of the different possibilities. **How can we work out what size grids to try?** First we need to count the number of letters; let's say that in our message we have 12 letters. Now we need to work out what size grids we can get. We need to know what numbers go into 12 – these are called its factors. 12 can be 1x12, 2x6, 3x4, 4x3, 6x2 or 12x1. These are the size grids we could use. To work out our message we would need to try it in all of the grids and see whether it made sense. *Slide 19:* **Try the questions on worksheet 3.** (Extension activity – use if workshop length is over 1.5 hours)
10 mins (70 mins)	BREAK: Drinks, snack and comfort break	Students can carry on with the worksheet if they wish – could put break earlier, during the worksheet section
Stay on slide 19 5 mins (75 mins)	**Discussion of worksheet 3**	*Do not include if have not done worksheet 3:* *Go through the answer to one of the questions on the board - pick one that the students found difficult or which caused discussion*

Slides & Time	Overview	Activity
Slide 20 Slides 20-25: 5 mins	**Substitution ciphers** Introduction to next part of Masterclass, substitution ciphers. Speaker to lead, input from students. *Slide animation: click for description and example*	We are now going to look at another type of cipher, a substitution cipher. **What do you think a substitution cipher is?** This is where you replace each letter with something else, instead of just rearranging them. Again, you need to stick to a special rule – you can't just do it randomly or no-one will be able to decrypt your message to read it. You need to have a rule in place which covers all of the letters, numbers or other symbols you want to encrypt, otherwise they will stay as plain text and won't be able to be encrypted. **What type of cipher is the phonetic alphabet we saw at the beginning? Why?** Substitution – replacing each letter with a word. The person you are sending the message to needs to know the rule you have used to encrypt your message, or they won't be able to read it. This is called the 'key' for the cipher.
Slide 21 Slides 20-25: 5 mins	**Caesar cipher 1** - Introduction. Speaker to lead, ask students for input *Slide animation: click to work through each step in example*	**Has anyone heard of Julias Caesar?** He famously used a substitution cipher to communicate with his generals. It was cutting edge at the time – very few people could read and write, let along crack a simple cipher. He used what is known as a 'shift cipher', meaning he shifted the alphabet along a few places. It is very easy to use, as long as you can read, write and count. A very simple one is putting the next letter along each time, so 'B' instead of 'a', 'C' instead of 'b' and so on. Caesar used a shift of three, which means he counted along 3 letters. From 'a' you count along once to get to 'B', twice to get to 'C' and three times to get to 'D'. So you replace 'a' with 'D', and so on for the other letters. **What would 'b' be replaced with?** E **What would 'c' be replaced with?** F **How about 'w'?** Z **What happens when you get to 'x'?** You start again at the beginning; it becomes 'A'. You have to think about the alphabet as if it was a circle; when you get to the end, start again at the beginning. **So what is 'y'?** B **And 'z'?** C You get the whole alphabet like this. You can fill in a table to help you encrypt and decrypt a message. Our table has been filled in for a shift of 3, so the letter on the bottom row is 3 places along in the alphabet from the letter on the top row. Notice we have used all little lowercase letters for our actual message, and capitals for our encrypted message. If you remember to do this it is a lot easier! Remember from your definitions that you always need to know the rule for the cipher you are using, and that it is called a 'key'. Because we know we are using a Caesar shift, so our key just tells us how many places we are shifting by. In this case, our key is '3'.

Slides & Time	Overview	Activity
Slide 22 Slides 20-25: 5 mins	**Caesar cipher 2** -Encryption/decryption Demonstration of encryption & decryption using the Caesar cipher. Speaker to lead, input from students. *Slide animation: click to work through each step*	We have talked about how to encrypt the letters – you move along 3 places, and you can put this in a table to help you. So, if I wanted to encrypt the phrase 'attack at dawn' I would look at my table and see which letter I need to use each time. I would replace 'a' with 'D', 't' with 'W', and so on (*do on board if possible).* It would become: DWWDFN DW GDZQ **How about decryption – what would I do for that?** Instead of counting forward 3 places for each letter of my message, I take the encrypted text and count <u>back</u> 3 places for each letter. **So, D becomes…?** 'a'. If you look at the table, it is just going up instead of down; you look for your cipher letter on the bottom, and your actual letter is on the top. **What would E become?** b **What would Z become?** w **What would A become?** x – remember we are thinking about the alphabet like it was a circle, so 'a' is after 'z'. **What would B become?** Y
Slide 23 Slides 20-25: 5 mins	**How to use a Caesar Wheel** – encrypting a message. Speaker to lead, input from students. *Slide animation: Click for each step*	You can make it easier to do the table by using something called a 'Caesar wheel'. You put your table into a circle, so that 'z' is next to 'a'. You can position the inside wheel in the right place to give the correct 'shift'; for a shift of 3, you would put the inside alphabet 3 places along from the outside alphabet, so 'D' is below 'a', just like in the table we were using before. Remember that we were using capitals for the encrypted text and lowercase for the actual message? If you remember this the Caesar wheel will be very easy to use. The lowercase alphabet, for the actual message, is on the outside, and the uppercase alphabet, for the cipher text, is on the inside. So to <u>encrypt</u> a message, you are going <u>from the outside alphabet to the inside alphabet</u>, and 'a' would become 'D'.
Slide 24 Slides 20-25: 5 mins	**How to use a Caesar Wheel** – decrypting a message. Speaker to lead, input from students. *Slide animation: Click for each step*	To <u>decrypt</u> a message, you are going <u>from the inside alphabet to the outside alphabet</u> – capitals to lowercase; so E would become b.

Slides & Time	Overview	Activity
Slide 25 Slides 20-25: 5 mins (80 mins) Activity – 15 mins (95 mins)	**How to use a Caesar Wheel** - Key. Speaker to lead, input from students. Activity – speaker and helpers to circulate. Students might need a lot of help. Check students are understanding the activity & go through some solutions with them – will need to understand to be able to do the next bit. *Slide animation: Click for each step*	***Resources:*** 1. *Worksheet 4 (Caesar cipher worksheet)* 2. *Caesar wheels with shift 3 (if using moveable wheels, you will need to leave extra time to manage this (see Specific Resourced Needed section above))* You need to know the 'key', or rule for your cipher, to make sure your Caesar wheel is in the right place. The key for this Caesar cipher is 3, because that is the shift we are using. You each have a Caesar wheels with a '3' shift on them. **Use this to do page 1 of worksheet 4.** You might have time to write your own ciphers at the end of the worksheet – if you do, put your hand up and we will give you a blank Caesar wheel to create your own shift. Follow the instructions on **page 2 of worksheet 4** to make your own wheel.

Slides & Time	Overview	Activity
Slides 26-28 10 mins (105 mins)	**Breaking the cipher** Breaking the Caesar cipher. Speaker to lead, students to use Caesar wheels to solve problem – will indicate when have an answer ***Resources:*** 1. *Scrap paper* 2. *Caesar wheels with a variety of shifts (see Specific Resourced Needed section above for extra info – ensure at least one student who is quicker at decrypting the Caesar cipher has a shift of 14)*	*Slide 26:* Now, what if we don't know the key but still want to read the messages? Can we crack the cipher? **Any ideas?** *[gather input from students]* You could try all of the shifts to see which one works. You could also try to guess letters based on how often they come up. *Slide 27:* You have another Caesar wheel. Each of you has a different shift. I am about to put up an encrypted message; try to work out what it says using your Caesar wheel. Remember, the inside alphabet in capitals is the encrypted letters and the outside alphabet in lowercase will give you the letters from the actual message. **How will you know that your Caesar wheel is the one which works?** You will be able to read the message. *[Remind students that they don't have to work out the whole message to find the key – as soon as it starts making sense they know they have the correct one]* **Try to crack the cipher using your Caesar wheel** *[Students to attempt to decrypt the message]* *Slide 28:* *[Keep an eye on who has found the correct shift – time is tight, so you may not want to wait for them to decrypt the whole thing]* **Who thinks they have found out what the right key is?** **What was the key?** Shift = 14 **Did you have time to work out what the message said?** cracking simple ciphers is easy when you try hard **Was that difficult to crack? Would we use it these days?** No – far too easy to crack, computers could solve this very quickly. *[Include if not covering slide 29]* The Enigma machine was used around the second world war, and even afterwards – it used a substitution cipher just like this, but scrambled the letters in a more complicated way so that no two letter was encrypted to the same letter of cipher text. The Cipher also changed every day, so there was a limited time to crack each combination. British and Polish mathematicians managed to crack the code by building the first computers and using clever logic to help them narrow down the possible solutions.

Slides & Time	Overview	Activity
IF TIME: Slides 29 – 31 (10 mins) Activity (10 mins) **OR give as take-home activity**	**Unbreakable ciphers?** ***These slides are currently hidden*** *in the presentation – un-hide them during student activities if you will have enough time to cover this section. If only some students have finished quickly, give out the rail fence cipher take-home worksheet for them to try.* Ideas on how to make these ciphers more secure. Can include if the earlier activities/discussion took less time than allocated. Speaker to lead, gather lots of ideas from students as well as showing ideas on slides. *Slide 29 animation: Click for next idea/demo of idea*	*Slide 29:* **What do you think we could do to make substitution ciphers, like the Caesar shift cipher, harder to crack?** - Changing the shift after each letter - Using several shifts, one after the other, for each letter, changing the shifts each time. - Other ideas? Of course, these can be broken in other ways, especially using computers. The Enigma machine was used around the second world war, and even afterwards – it used a harder substitution cipher just like this: there were several cipher wheels (like Caesar wheels) for each letter, all with the cipher text shifts in non-alphabetical order, and they rotated each time a letter was typed. This scrambled the letters in a more complicated way so that no two letter of plan text was encrypted to the same letter of cipher text. The Cipher wheel arrangements also changed every day, so there was a limited time to crack each combination. British and Polish mathematicians managed to crack the code by building the first computers and using clever logic to help them narrow down the possible solutions. *Slide 30:* **How can we make transposition ciphers more unbreakable?** One idea is to change the direction of how we read off the encrypted text; this would make it harder to work out. However, we then need to describe what we have done to the person we are sending the message to. *Slide 31:* Another, slightly simpler solution is to change the order we write down the columns of text. Instead of doing column one, column two, column three and then column four, we could do 1, 3, 4 2. Then we just need to send the column order, which we will call the 'key'. ***If time:*** *worksheet (Unbreakable route cipher worksheet) on creating own messages and keys (10 mins) – do not give as a take-home worksheet unless they have seen these slides in the workshop.*
Slide 32	**Challenge** for students to try at home with friends	It is time to finish now, but I have one final challenge for you to try at home or in school: try to come up with a cipher which is nearly unbreakable.
Slide 33 5-10 mins (120 mins)	**Thank you!** Tidy up, feedback and question time Ask the Ri *[Ensure you collect any Caesar wheels you are not giving the students, and hand out any take-home worksheets]*	*Don't forget to collect any questions which arise, and email them to the Masterclass team at the Royal Institution: masterclasses@ri.ac.uk. We will send you answers as soon as possible. Then these can be reported back to the children at their next Masterclass session. In this way you cannot be "caught out" by a question. It also demonstrates the point that not everything in maths is known, but some questions need time and research to find answers sometimes, and sometimes the answer has not been found by anyone yet, of course! Maybe our Masterclass students will be the ones who solve the problem when they are older?*

Slides & Time	Overview	Activity
Slide 34	**What else could you do to explore cryptography?** Further activities, including possible NRICH problems related to cryptography – use as extension activities, activities for them to try in school or additional activities for them to do at home	*Give out the take-home worksheet.* *Students can also try the following NRICH challenges to further develop their code breaking and reasoning skills:* • *Code Breaker: https://nrich.maths.org/1172* • *Ancient Runes: https://nrich.maths.org/2186* • *Coded Hundred Square: https://nrich.maths.org/6554*