THE EMPTY VAULT

Presented by The School of Mathematical Sciences at The University of Southampton

The box was found lying abandoned on the floor of the vault, empty...
except for a small slip of paper carrying nine mysterious characters.
There is only one team in the world that can crack this mystery. Will you join it?

Trainer's manual 2022 v6

20 YEARS NATIONAL CIPHER CHALLENGE

University of Southampton

Registration opens **15th September**

Competition starts **6th October**

cipherchallenge.org

IBM ten° BLUESPARK FOUNDATION TRINITY COLLEGE CAMBRIDGE UKRI Engineering and Physical Sciences Research Council GCHQ NETCRAFT Institute of mathematics & its applications Mathematics Teacher Training Scholarships

About the Challenge

The National Cipher Challenge launched in 2002 and we have seen a host of competitors and protagonists come and go over that time. This year we will follow the adventures of Harry and Jodie as they wrestle with loyalties and ambitions while trying to solve the mystery of The Empty Vault. They need your help and invite you to join them.

Mission Briefing

In the depths of GCHQ there is a cold case division nicknamed "the Archaeologists". They spend their time deciphering unbroken but obsolete wartime despatches and diplomatic communications in the hope of finding something still significant. Until recently it was run by Jodie, one of Harry's top agents, on secondment from the Bureau of Security and Signals Intelligence (BOSS). Now she is missing, apparently on the run and involved with the Lighthouse Conspiracy, a renegade group of spies independent of any government or corporation.

Whatever her motivation, a rogue agent is always dangerous and Harry now has a decision to make. Should he report Jodie or try to track her down and bring her back in from the cold? And if the latter, then how can he find her?

You are invited to join the puzzle solvers, linguists, mathematicians, and computer scientists in The Archaeologists to assist Harry in his mission at

www.cipherchallenge.org

Good luck!

Who is the competition for?

The competition is written for UK secondary school and sixth form students of mathematics and computer science, but it has always had a wide following among teachers and parents and across a range of age groups. It also attracts a small number of international competitors. The first three rounds are accessible to everyone, and we hope you enjoy it enough to try and crack the harder messages in the later rounds. The challenges can be tackled by teams or individuals, and there is a forum where you can exchange ideas.

How do I get started?

If you have never tried codebreaking before it can be a little daunting at first, but we will do our best to make it easy to get started. You can download a whole collection of information from our training page

www.cipherchallenge.org/resources-media/

Including a beginner's guide to codebreaking

www.cipherchallenge.org/boss-cryptanalyst-handbook/

What do I need to take part?

There is no charge to register or take part, and all you need to get involved is a reasonably modern web browser. We publish news about the competition on Twitter so you should sign up to follow Harry @Cipher_Master.

To join in you will need to register for an account on the website at

www.cipherchallenge.org/account-login/

which will also allow you to take part in our Forum, where you can discuss a whole range of things connected to the competition (and quite a few that are totally unrelated).

You can find out more about this in the Registration section below.

If you are a teacher and want to register several teams at once then you should sign up using the link at the bottom of the page

www.cipherchallenge.org/teacher-registration/

Once you have done that you can use the bulk registration tool to register multiple teams at once. You will need to name each team and nominate a captain for each one. You will be asked to enter the team captain's email address, which we will use to send them an email telling them they are registered and giving them some initial instructions. We will not store the team captain's name or email so if there are problems with the registration (like an email going astray) you will need to email us at cipher@soton.ac.uk for help. (We are trying to store as little info about participants as we can for GDPR reasons.)

Pupils can also set up their own teams, and registering as a teacher will give you a pin number that they can use to associate their account with yours so you can follow their progress more easily. You can read more about this on our How to... web pages on the site.

Resources

You can download lessons and notes on codebreaking from the resources page on the competition website

https://www.cipherchallenge.org/resources-media/

Alongside the materials we have produced you will find links to books, online videos and help guides that contain everything you need to be a successful code-breaker in our other resource pages. You can even build your own cipher machines, including the simple cipher wheel and the more complicated Pringle Can Enigma Machine. Our cipher tools page also has a few simple programs to help you get started, including a Caesar wheel, an affine shift encryption machine and a frequency analyser to help you break down patterns in a text.

Forums

As usual we will be running a moderated discussion board as part of the competition to encourage a community spirit. We have a basic set of rules for this which are intended to support a warm and friendly atmosphere and to make sure no-one spoils the competition for anyone else. We encourage you to make full use of it. The forum is open for anyone to read, but posting is reserved for those with a cipher challenge account.

The history of the competition

The National Cipher Challenge has been run by the University of Southampton Mathematics Department since 2002 and has attracted a wide following. Fans and supporters include Anthony Horowitz, who has kindly suggested some books that cipher fans might enjoy; Simon Singh, whose book on codes and ciphers inspired the original competition; comedy writer James Cary who wrote Bluestone 42 and the Radio 4 comedy Hut 33; and the star of that show (and many others), Robert Bathurst, whose aunt worked at Bletchley in the war.
Boris Johnson, the ex Foreign Secretary William Hague and Newsnight editor Mark Urban, who has a passion for military history, have all taken part in our prize-giving ceremonies at Bletchley Park, and we had the pleasure of introducing the Cipher Challenge team from Saint Anne's School in Southampton to the Duke of Edinburgh who, remembering his work in the second world war immediately fell in love with the competition and gave Harry a reading list for the summer. The real fans though are the competitors who take part every year until they are too old, by which time it is too late and they are hooked. Many of them go on to careers in cyber security and others follow other paths using the mathematics and computing skills they learned tackling our fiendish challenges. You can read some of their stories on our new page:

cipherchallenge.org/boss-your-cipher-challenge/

The structure of the competition

Part A and Part B of the Challenge

Each round of the competition will be published in two parts, part A - Harry's journal and part B - the mission intercept. Harry's journal will record his thoughts on the adventure and may contain instructions and advice. Since he is trying to protect Jodie and himself it is encrypted and you will need to decipher it to take advantage of that.

The mission intercepts are messages that will help us in our hunt for Jodie. As we get closer to her the security is likely to get tougher so each part will get progressively more difficult as the competition proceeds. On the other hand Harry wants you to be able to break his journal while Jodie almost certainly doesn't want you to do so well with the intercepts, so it will not in general be as difficult
Each part will have its own leaderboard and certificates, and scores for challenges 4-10 will be aggregated to produce an overall leaderboard.
As well as the certificates, there are a range of achievement awards that you will collect in your user account area.

Competition schedule

Registration will open online at 12pm on Thursday September 15th, and you will find the introduction on the Challenge pages. The first training exercise will be published at 3pm on Thursday 6th October, with two more in the weeks leading up to half term. While we will publish leader boards for those challenges, the marks for them won't count towards the final competition standings, so don't worry if you miss one of them.

The main competition starts with Challenge 4 on 3rd November, with the remaining challenges published weekly until December 15th. The idea is to see how far you can get. Even if you get stuck you can follow the story and see how others are getting on.
The later rounds will be a harder than the early ones and the last one will be very tough to break, but you will have four weeks to crack it.

Challenge	Publication date 15:00 on	Final deadline 23:00 on
Introduction	15/09/2022	N/A
Practice Mission 1	06/10/2022	12/10/2022
Practice Mission 2	13/10/2022	19/10/2022
Practice Mission 3	20/10/2022	02/11/2022
Mission 4	03/11/2022	09/11/2022
Mission 5	10/11/2022	16/11/2022
Mission 6	17/11/2022	23/11/2022
Mission 7	24/11/2022	30/11/2022
Mission 8	01/12/2022	07/12/2022
Mission 9	08/12/2022	14/12/2022
Mission 10	15/12/2022	05/01/2023

Registration

This will open on Thursday 15th September at our registration page:

www.cipherchallenge.org/account-login/

If you already registered for the competition last autumn, then you will still need to register as we delete accounts for privacy reasons.
You will need to provide the following information:
A user name: You will use this to log in but it will not appear on the website
A display name: This will be published on the leaderboard and on any posts you make to the forum, so please do not use a username that you also use elsewhere, OR that contains any personal information. Be creative (and polite)!
Your age and gender: You don't have to tell us this (there are options for neither or prefer not to say) but it will help us enormously in monitoring diversity if you do. We will NOT store this information as part of your personal data, but will use it in aggregate to help us understand the Cipher Challenge community.
Your School: Again You don't have to tell us this but we can include it on your certificates if you do. You should enter the first few letters of your school name then select it from the drop down list. If you can't find your school then you can email us with the details and we will look into it. You can skip this step now and add the school later from your account page.
Parent/Teacher PIN: Again you don't have to enter this here, but if your parent, carer or teacher has set up a teacher account and you want them to be able to follow your progress then you can get them to give you a special PIN number that is shown on the Student Accounts tab in their user account page. If you enter it here, or later on your team page, then they will be able to see your submissions and your scores.
A team name: Either create one on the form, or apply to join an existing team. Take care not to give any personal information in the team name as this will be published on the leaderboard.

Password: This is for logging on. Choose it carefully, make it strong and keep it secret. It should have at least 8 characters and must contain an upper case letter, a lower case letter and a digit. The system will

discourage you from using a password that is too easy to crack. MAKE A NOTE OF IT IN CASE YOU LOSE IT!
Three security question answers: You will use these if you need to reset your password. Please don't forget the password AND the security question answers as we can't reset your password for you!

Teams and solo entries

TEAMS OF ANY SIZE CAN TAKE PART, BUT PRIZES WILL HAVE TO BE SHARED!
If you want to enter as a group the Team Captain should register first and create a new team. The other team members can then request to join that team when registering for their own accounts . Alternatively, if they have already registered then they can make the request from

www.cipherchallenge.org/my-account/team/

The Team Captain will see each request in their user area and they can then accept or decline invitations. The team name can be set by the Team Captain on the Team page under their account.

If you want others to join your team let them know and they can submit a request through their team page which is linked under their user name at the top right of every page.

Please note the following important information:

1. If you are entering on your own then you are your Team Captain. You still need to make a team.
2. Only Team Captains can submit solutions for the team. If someone else needs to do that then the Captain will need to delegate their captaincy by going to the team page in their account and selecting another member to become the Captain. Please be careful if choosing this option as once someone has been delegated they are in control of the team (there is no 'undo'). If a Team Captain can't delegate then they can share their login details. Beware that once those login details are shared with someone, they can post on the forum as you or even change your password and lock you out of your own account! You can

always change your password if you have had to temporarily share it. It would be better to create a "Captain's account" for all the team to share if you want to all be able to post entries for the team. That way you can keep your personal account private for the forums.

3. If you create another account having already joined a team, that new account will not be linked to the team unless you request to join it when setting up the team.

4. Team members who are not Team Captains will not see the answer submission form when logged in as themselves, but will see a message on the Challenge page reminding them that the Team Captain has to submit answers.
5. You can leave a team at any point, but you cannot keep the score the team has gained. If you are a Team Captain and wish to leave a team with other members in it, you will need to delegate your captaincy to another team member first.
6. Team Captains can delete the team, but it should be obvious that you would have to be very sure that everyone in the team is OK with that. There is no undo!
7. Points are recorded against Teams only (not individual team members). If you join a team after you have gained points those points will stay with the team that you were on at the time. Team Captains accepting a new team member during the competition will be sharing any points the team has gained up to that stage.
8. While you can choose to leave a team, once you have requested and been accepted to join one you cannot be thrown out of the Team.
9. Every member of a team can see the feedback on submissions and can download a copy of any certificates from their account page.

Submitting your solutions

The Team Captain (or anyone in the team using the Team Captain account) can submit solutions to either Part A or Part B at any time during a round by typing them into the submissions box at the bottom of the challenge page. Be careful to paste the correct solution in the box (part A and part B each have their own). If you don't see a submission box that is

either because you have submitted a correct solution already, or because you are not a team captain. Make sure to remind your captain to submit before the deadline!

If you need to resubmit (because you found a mistake, or because we pointed one out to you) you can use the same form. Just paste your entry as text in the appropriate box. It doesn't matter how you format your answer, with or without punctuation and spaces and whether or not you use capital letters, however you must only type or paste in the exact text of a decrypt of the message.

It is a good idea to use a simple text editor to type up your solution (rather than something like Word) as the spell checker sometimes tries to change what you are typing and any "mistake" in the text might be deliberate.

The rules are simple:

1. Don't try to correct any errors you think we have made, always type in an exact decryption of the text as given.
2. Don't try to tell us what cipher we used, or to ask us a question, or to say how you solved the cipher in the entry form, we don't read it and it will be marked as an error in the solution.

Getting help

We offer online feedback on submissions during each round to help you if you make mistakes. The feedback can be delayed so you might lose points if you rely on it rather than trying to correct your own errors quickly, but it can be useful if you are on the right track and just need a hint on where you went wrong.

At the end of each round we will publish the official decrypts of Part A and Part B on the challenge page, but we won't say how it was encrypted. You can try to work that out for yourself if you haven't already, or you can discuss it with others in the Forum, BUT ONLY AFTER WE HAVE PUBLISHED THE SOLUTION!

Participants often get stuck on a mission but, as in real life, sometimes a good night's rest is all you need (which is why our points bands finish at 23:00!) Other times you might need more practical help and can turn to the website for clues, either hidden in earlier rounds of the competition, in the Case Files, revealed by Harry's team in the briefing notes (Part A), or posted (by Harry and the Elves) as comments on the Forum.
We ask you not to post hints of your own there without checking them with us first as this will spoil the Challenge for others.

If you need to get hold of us you can post a message on the forum or send us an email to

cipher@soton.ac.uk

Scoring

Each of the two missions in a round (Part A and Part B) are scored for accuracy in the same way. We strip out all the non-ascii characters, spaces and punctuation from your solution. We then convert it to lower case and compare that string of letters with our solution, which we have treated the same way. We use the Damerau-Levenshtein distance to determine how similar they are. The closer the match, the higher the score and if they are identical you will score 100% for that mission. If you make enough errors then we automatically give a score of zero for that submission (not necessarily that round!) This is to discourage fishing for hints or brute force attacks on the cipher.

If you spot a mistake in your answer you can submit again. We only ever take your most accurate answer into account and accuracy beats speed in every case, though speed is also important in the Part B competition.

In Part B we look at all your submissions for the round and find the ones with the highest mark. We then take the first one of those and award you points depending on how quickly you submitted it. The available points are given in a schedule that is published with each mission. For part B accuracy and speed both count and accuracy is always more important! It is better to get the solution more accurate and submit later than to submit a

slightly worse solution sooner. Of course it is best to submit a completely correct solution as fast as you can!

There are no speed points for Part A, only for Part B.
You can find your scores for each round in your user area, and we will publish a leaderboard for each round. The first three rounds are a warm-up so the points will not count for the overall leaderboards but from round 4 we will publish an overall Championship leaderboard for each part (A and B) as well, based on your total points from then on.

Certificates

Everyone who takes part in any part of the Challenge will be able to download a certificate, both for the individual rounds and for the overall competition. We will also publish your ranking in the leaderboard so you can boast about your codebreaking skills! The top teams in each round will be awarded Gold, Silver or Bronze Certificates, and your overall certificate will also show your standings in each round.

Prizes

We have been fortunate in having some amazing sponsors for the competition and as usual they are providing fantastic prizes for the top code breakers in the competition. Winners will be selected from among the top competitors by the prize committee who will ask for an account of the strategy used to break the challenge and will take that into consideration in the award of the prize. There are prizes for individual competitors and for teams and details will be published on the competition website.

Prize-giving

rom the beginning the National Cipher Challenge has had a close relationship with the historic home of UK codebreaking at Bletchley Park. For many years we were able to run an annual event to celebrate the achievements of our competitors, with special guests, lunch for our main prizewinners in the Mansion, and an afternoon of lectures and tours of the museum.

In recent years changes at Bletchley meant that we had to scale back our ambitions and were unable to invite more of you to the event, however we are very pleased to announce that this year we are able to return to our roots and will be holding a more traditional National Cipher Challenge Prize Giving event at the Park. The event will start with a private lunch for our main prizewinners and sponsors and will continue with an afternoon of lectures and tours of the Park and museum. We will have around 80 tickets in total and will announce more details about the event nearer the time.

Support materials

The Resources section of the website can be found at:

www.cipherchallenge.org/resources-media/

This page contains a variety of materials you might find useful in developing your skills including six powerpoint presentations on topics covering frequency analysis, the use of cribs and the basic ciphers.

You will also find links to a set of notes on codebreaking, a short introduction to using python to automate your attacks, and, in the library sections, some youtube videos on relevant topics and links to books we recommend.

We welcome comments on these resources and if you have any suggestions of your own please let us know in the Forum or via Twitter so we can improve the support available to you all.

Rules, regulations and policies

The annual cipher challenge has a well established set of rules, that you can find online at

www.cipherchallenge.org/information/rules/

These rules are mostly just to ensure the system works, but they are important so please take a look and ask if anything is unclear.

If you have any questions or concerns about any aspects of the competition please don't hesitate to contact us at

cipher@soton.ac.uk

Urgent queries should be directed to the Cipher Challenge Director, Prof. Graham Niblo who can be contacted at

G.A.Niblo@soton.ac.uk