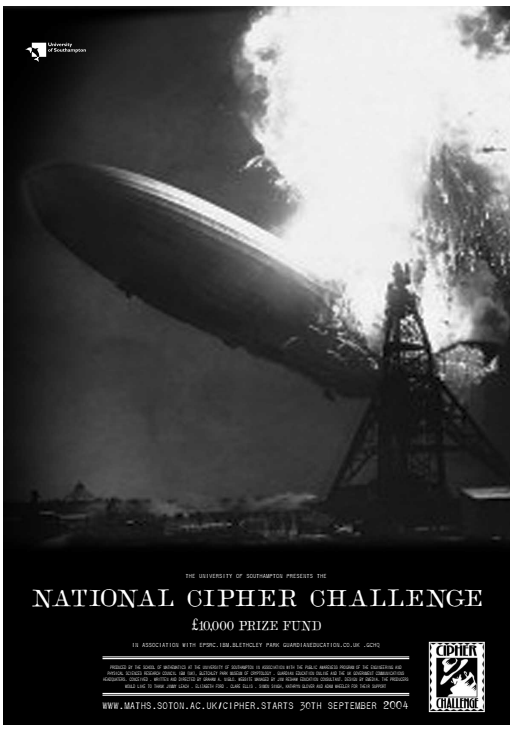
National Cipher Challenge 2020 Edition

Tinker, Tailor, Tourist, Spy

Trainer's Manual v2

Change log:
Initial publication 20/10/20
V2: Published 14:13, 21/10/20 - added section on the Forums, including the new Teachers' Forum

About the Challenge



The first National Cipher Challenge was published in 2002. For this 19th official edition (following an unofficial "special edition" during lockdown) we present an all new story set in 1937.

Over the next 11 weeks we invite you and your charges to join us as we solve the mystery in

Tinker, Tailor, Tourist, Spy

The story

In the lead up to WWII the British intelligence services were flooded with reports of Nazi spies and sympathisers. With war fast approaching and limited resources the task of vetting all these reports was passed to a fledgling security organisation known as BOSS. As a new recruit you are given the job of decoding the secret messages that will expose the enemy agents. Although the Allies don't know it yet, it is a race against time and they need your help ...

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 couple of 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 intimidating, 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

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

Including a beginner's guide to codebreaking

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

How to register and join in

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 by following @Cipher_Master.

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

https://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).

When you register, you will be asked to either create or request to join a team. You need to do this even if you are taking part alone, as it is the team name we use on the leaderboards. If you ask to join an existing team make sure to let the team captain know so they can log in and approve your request. If your request is turned down, don't worry, you can request to join another team, or set up your own team from your account area at

https://www.cipherchallenge.org/my-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.

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.

This year for the first time we are also hosting a Forum for teachers. This is private in the sense that only those with a cipher challenge account will be able to see it, though we are not collecting personal information at registration so anyone with such an account could post there regardless of whether or not they are a teacher. We are assuming that in practice only teachers will want to use it given that we have a more public forum available for everyone else.

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 Boris Johnson; the Foreign Secretary William Hague; the media scientists Adam Hart-Davis and Simon Singh; Newsnight editor Mark Urban, who has a passion for military history; 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.

We have also 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.

Part A and Part B of the Challenge

Each round of the competition will be published in two parts, part A - the mission briefing and part B - the mission intercept. Part A will contain instructions and advice, and since it is classified you will need to decipher it to take advantage of that. The mission intercept is an enemy message that has been caught by our listening posts and we hope it will provide clues to solve the mystery. Each part will get progressively more difficult as the competition proceeds, but part A is intended for you to break it so it will not in general be as difficult as part B which is deliberately a little more difficult. Each part will have its own leaderboard and certificate, and scores for challenges 3-7 will be aggregated to produce an overall leaderboard.

As well as the certificates, this year we are introducing achievement badges that you will see collecting in your user account area.

Competition schedule

Registration will open online for registration at 3pm on Thursday, October 22nd, and you will find the first episode waiting for you there as a training exercise. The next training exercise will be published after the half term break at 3pm on Thursday 5th November. These first two episodes are designed as a warm up, and while we will publish leader boards, the

marks for those challenges won't count towards the final competition standings, so don't worry if you miss one of them. The main competition starts with episode 3 on12th November, with the remaining challenges published weekly until December 10th. The later rounds will be a lot tougher than the first ones and the last one will be hard to break, but you will have four weeks to crack it. Rounds 2-6 will each last one week.

PLEASE NOTE: We have changed the publication time back to 3pm from the 9am start we used in the special edition back in March.

Challenge	Publication date 15:00 on	Final deadline 23:00 on
Practice Challenge 1	22/10/2020	04/11/2020
Practice Challenge 2	05/11/2020	11/11/2020
Practice Challenge 3	12/11/2020	18/11/2020
Competition Challenge 4	19/11/2020	25/11/2020
Competition Challenge 5	26/11/2020	02/12/2020
Competition Challenge 6	03/12/2020	09/12/2020
Competition Challenge 7	10/11/2020	06/01/2021

Registration

This will open on Thursday 22nd October at our registration page:

http://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!)

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.

Age: Again you don't have to tell us this but it will help us enormously in monitoring diversity if you do. We will NOT store this information as part of your personal data either, but will use it in aggregate to help us understand the Cipher Challenge community.

Password: This is for logging on. Choose it carefully, make it strong and keep it secret. 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.

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.

Teams and solo entries

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

http://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.

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 wish to join a different team after you have already registered then you will need to do this by using the "Change Team" form on this page:
   http://www.cipherchallenge.org/my-account/team/
   Your new Team Captain will need to accept the invitation.
4. 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 using the "Search Team" function on the same page:
   http://www.cipherchallenge.org/my-account/team/
5. 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.
6. 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.
7. 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!

8. 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. Think VERY carefully about changing teams!
9. 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.
10. Every member of a team can see the feedback on submissions and can download a copy of any certificates from their account page.

The structure of the competition

There are seven rounds to this edition[1] of the Cipher Challenge, and the first three are for practice only. As we said above, each round of the competition will come in two parts. Think of them as the "easy" and the "hard" challenges (or the "hard" and "much harder" challenges if you prefer). The mission briefings will be fairly lightly encrypted, at least at first, although in the latter stages of the competition, security will be tightened and you will find the Part A ciphers harder to crack. At the start the mission intercept encryption (part B) is not too hard to crack, but as you get deeper into the mystery you will find that the encryption gets much tougher and you may find that learning to use a spreadsheet, or even to programme, will be of particular value in tackling the later challenges. We provide a brief guide to programming, written for us by a Cipher Challenge alumnus, Julian Bhardwaj, and

[1] We would love to have brought you more, but Covid-19 has brought its own challenges and time is precious.

you will find it, together with other helpful materials in the Resources section.

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 you 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.

Participants often get stuck on a challenge but, as in real life, sometimes a good night's rest is all you need. Other times you might need more practical help and can turn to the website for clues, either hidden in earlier rounds of the competition, 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 at

cipher@soton.ac.uk

Scoring

Each of the two challenges 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 challenge. 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 challenge.

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 two rounds are a warm-up so the points will not count for the overall leaderboards but from round 3 we will publish a Championship leaderboard based on your total points from then on, in each of the parts.

Certificates

Everyone who takes part in any part of the Challenge will be able to download a certificate recording their achievements, 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!

How many can enter?

Teams of any size and composition may enter.

Support materials

The Resources section of the website can be found at:

www.cipherchallenge.org/resources-media/

It contains a variety of materials you might find useful in developing your skills. These include 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 it, 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

https://www.cipherchallenge.org/information/rules/

These rules are mostly just to ensure the system works and are described above.

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

cipher@soton.ac.uk

Urgent queries should be directed to the Challenge Director, Prof. Graham Niblo who can be contacted on 023 80593674. He is working from home during the Covid-19 period but if you leave an answerphone message someone will get back to you as soon as we can.