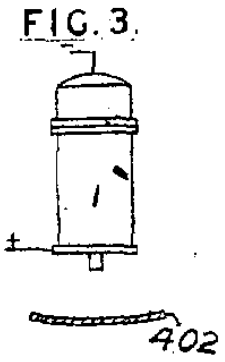
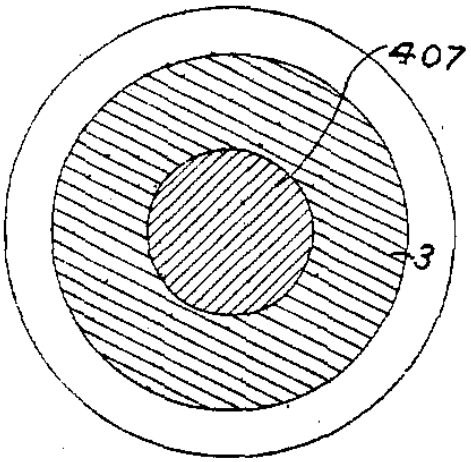
NATIONAL CIPHER CHALLENGE 2020 SPECIAL EDITION

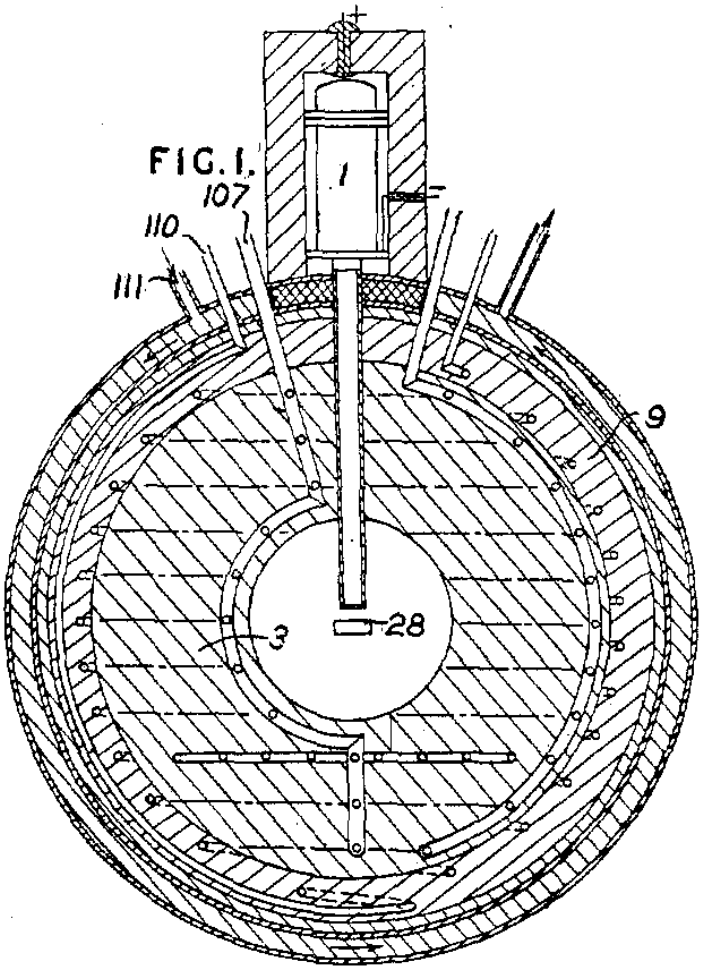
TOP SECRET

BOSS TRAINING DIVISION

DIE ALCHEMISTEN, 2ND EDITION TRAINER'S MANUAL V1.3







ABOUT THE CHALLENGE

The third National Cipher Challenge was published in 2004 and was the first one to feature Harry.

Here BOSS presents a revised edition of that Challenge, with a slightly updated story, an extra episode and some new challenges to train the next generation of its operatives.

There are no prizes, (almost) no rules, and it is open to everyone. Enjoy ...

THE STORY

In March 1937, in the wreckage of the Hindenburg the FBI discovered a small packet of documents. They carried a swastika and the legend “Die Alchemisten”.
The papers, although partly encrypted, appeared to be nonsense and were ignored until 1939, when a young intelligence officer called Philomena Black was tasked with analysing them.
With the cipher department fully engaged on cracking signals intelligence from Europe she had no resources to crack the code herself and called her friend Harry from the newly formed Bureau of Security and Signals Intelligence. Short staffed and in a race against time, they need your help to break the ciphers ...

WHO IS THE COMPETITION FOR?

The competition was originally written for secondary school and sixth form students of mathematics and computer science, but it has gained a wide following among teachers and parents and across a range of age groups. 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 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 at www.cipherchallenge.org, and you can also keep up to date with competition news by following @Cipher_Master on Twitter.

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 then we will email your request to the team captain and let you know the outcome. If your request is turned down, don't worry, you can request to join another team, or set up your own from your account pages.

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/

This is the competition library and 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. You can even build your own cipher machines, including the simple cipher wheel and the more complicated Pringle Can Enigma Machine.

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. You can read more about it at https://www.cipherchallenge.org/boss-trainers-manual-v1-2/

PART A AND PART B OF THE CHALLENGE

Each round of the competition will be published in two parts, part A and part B. Each part will get progressively more difficult as the competition proceeds, but part A is intended for newcomers and will not in general be as difficult as part B. Each part will have its own leaderboard and certificate, and scores for challenges 4-9 will be aggregated to produce an overall leaderboard.

COMPETITION SCHEDULE

Registration will open online on Monday March 30th, and the first episode will be published at 9am on Thursday April 2nd. The first three 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 4 on April 23rd, with the remaining challenges published weekly until May 28th.

PLEASE NOTE: We have changed the publication time from the usual 3pm (designed for the school day) to 9am so you can get started earlier.

Challenge	Publication date 09:00 on	Solution deadline 23:00 on
Practice Challenge 1	02/04/2020	08/04/2020
Practice Challenge 2	09/04/2020	15/04/2020
Practice Challenge 3	16/04/2020	22/04/2020
Competition Challenge 4	23/04/2020	29/04/2020
Competition Challenge 5	30/04/2020	06/05/2020
Competition Challenge 6	07/05/2020	13/05/2020
Competition Challenge 7	14/05/2020	20/05/2020
Competition Challenge 8	21/05/2020	27/05/2020
Competition Challenge 9	28/05/2020	10/06/2020

REGISTRATION

This will be open after Monday March 30th at our registration page:

http://www.cipherchallenge.org/account-login/

If you already registered for the competition last autumn, then you will be able to use that account for this one too. Otherwise you will need to provide the following information:

A user name: You will use this to log in to the site and it will appear on any Forum posts, 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.

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 receive an email on each request 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. 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, and keep your personal accounts 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. 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 forming a team for the first time during the competition will be sharing any points they have gained up to that stage with the team. Think VERY carefully about changing teams!
8. While you can choose to leave a team, once you have requested and been accepted to join one you cannot be thrown out by 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.

THE STRUCTURE OF THE COMPETITION

There are nine rounds to this special edition 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, Part A and Part B. Think of them as the "easy" and the "hard" challenges (or the "hard" and "much harder" challenges if you prefer). Part A challenges 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 Part B encryption 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 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 page. 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 (though given the speed with which we have thrown this together, I wouldn't count on it!). 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 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, 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 those with the highest mark. We then take the first one of those that you submitted 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 the feedback section of the site, 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 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 and if you have any suggestions of your own please let us know in the Forum or via Twitter so we can improve the resources available to you all.

RULES, REGULATIONS AND POLICIES

The annual cipher challenge has a well established set of rules, but most of them don't apply to this competition, which is purely for fun. Those rules that still apply are 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 Prof. Graham Niblo who can be contacted on 023 80593674. Please leave an answerphone message and we will get back to you as soon as we can.