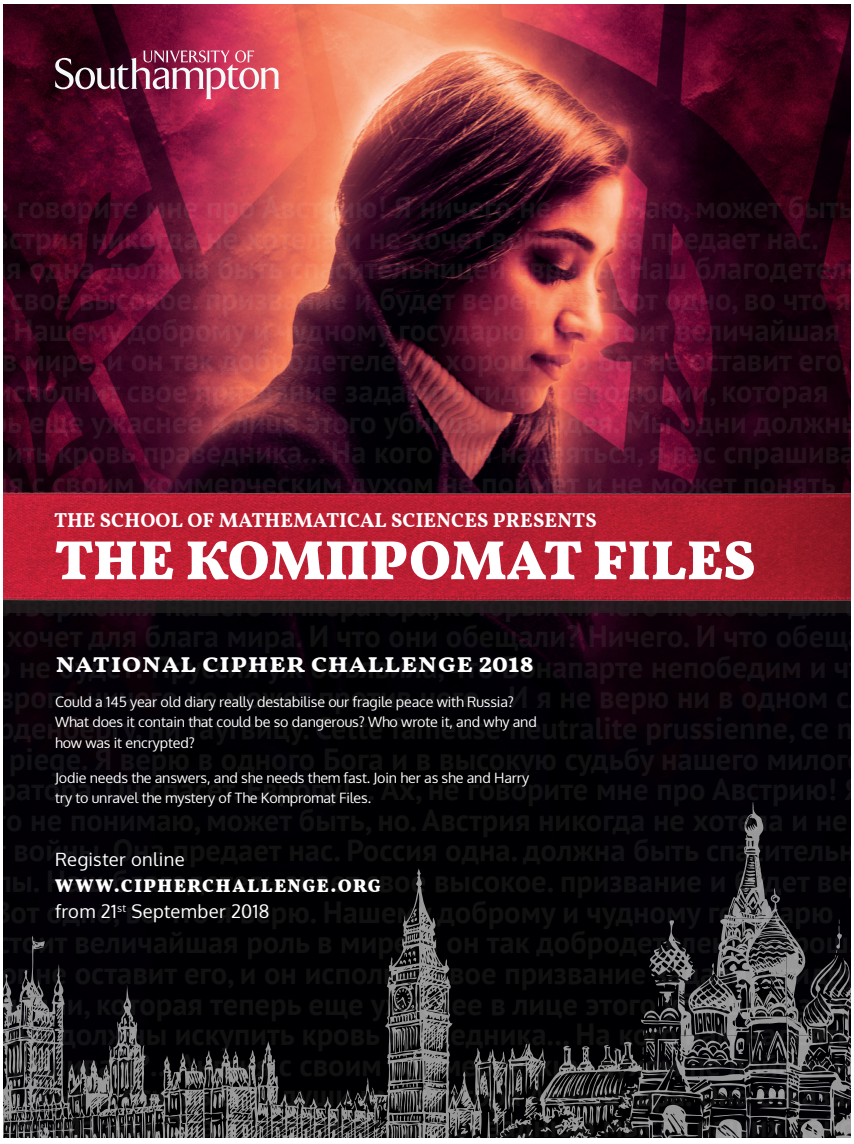
National Cipher Challenge 2018 Teacher's Pack v1.4



IBM bcs TrinityCollegeCambridge Southampton GCHQ NETCRAFT

About the Challenge

Welcome to the National Cipher Challenge, a nationwide, online codebreaking competition, which will run again from October 4th 2018 to January 9th 2019. If you have any questions please contact Harry at cipher@soton.ac.uk. The competition is structured as a series of encrypted messages which tell a story. This year we rejoin our hero Jodie, who is recovering from her adventures in last year's competition, The Lost Legion, by taking a quiet job cataloguing Victorian government secrets for the British Library. Unfortunately (or, just maybe, fortunately?) the dark world of espionage is lurking, ready to

draw her back in, and she will need your help, and all your skill and cunning, to survive and to solve the mystery of The Kompromat Files.

Who is the competition for?

The competition is aimed at school and sixth form students of mathematics and computer science, and is a great extension activity (or a fantastic maths club project) that can be tackled by them in teams or on their own.

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 us on Twitter.

Entrants can take part alone or in teams of any size. To take part you will need to register for an account on the website, and we will ask you for a Code Name (which we will use to identify you on the forum, where you can discuss a whole range of things connected to the competition, and quite a few that are totally unrelated). You will then be asked to create or join a team which you will use to submit your entires. 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.

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. The names of everyone on a team will be on the certificate and we will publish the team name on the leaderboards so you can see how everyone is getting on.

When setting up the team we ask you to say whether or not you are eligible for a prize. The rules are below. If you are eligible we will ask you for some information about your school, including the name and email

address of a teacher contact. We need this in case you win a prize, but please do ask them first. If you are home educated then state that in the School name box and give the name and email address of an adult we can contact if we need to. We will not publish your name or the contact information of your teacher without your (or their) permission, but of course if you win a prize we will want to tell the world about your success!

Resources

You can download lessons and notes on codebreaking from the resources page on the competition website. 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 Mathematics department at the University of Southampton since 2002. It regularly attracts entries from teams at over 700 UK schools and colleges. Long time competitor, Julian Bhardwaj, said of the Challenge

> "*If I were to name one thing which has undoubtedly influenced my academic drive, interests and overall career to date, it would be the National Cipher Challenge. Since being introduced to cryptography and the challenge in Year 8, it has been my one passion and driving force in pursuing further education in maths.*"

Julian went on to study Discrete Mathematics and made it to the Grand Final of the UK National Cyber Security Championship in 2013, following in the footsteps of the 2008 National Cipher Challenge winner, Jonathan

Millican, who was crowned winner of the UK National Cyber Security Championship the previous year.

Our competition has attracted support from a number of people over the years, who have encouraged us by giving up their time to launch the competition, to meet with competitors and to attend the annual prize giving at Bletchley Park. These include 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. Two Foreign Secretaries, Boris Johnson and William Hague have supported the competition (though Boris was London Mayor at the time), and we are also grateful to our sponsors who give time as well as money to support the competition. It is not unknown for our winners to meet members of the secret world of GCHQ at the awards dinner despite their busy schedules.

Competition schedule

Registration will open online on 21st September and the first episode will be published at 3pm on Thursday October 4th. 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. There will be a break for half term from and the main competition starts with episode 4 on 1st November, with the remaining challenges published weekly until December 13th:

Challenge	Publication date 15:00 on	Solution deadline 23:59 on
Practice Challenge 1	4/10/2018	10/10/2018
Practice Challenge 2	11/10/2018	17/10/2018
Practice Challenge 3	18/10/2018	31/10/2018
Competition Challenge 4	01/11/2018	07/11/2018
Competition Challenge 5	08/11/2018	14/11/2018
Competition Challenge 6	15/11/2018	21/11/201
Competition Challenge 7	22/11/2018	28/11/2018
Competition Challenge 8	29/11/2018	05/12/2018
Competition Challenge 9	06/12/2018	12/12/2018
Competition Challenge 10	13/12/2018	09/01/2019

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, but the main prizes are reserved for the more difficult Part B challenge.

Registration

To take part you will need to register for the competition on our registration page:

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

This will be open from September 15th, and you will need to provide the following information. Owing to the GDPR competitors under the age of 13 will be asked for a restricted set of information and we will ask for them to provide an adult contact email address. If you have any questions about this please do get in touch:

Nickname: This will be the name we use to identify you in public. Choose something memorable. It will appear whenever you post something in the forum so don't include anything in your username that identifies you. You are, after all, working with an undercover organisation.

Name: We will keep this private, but need it for our records. We will only publish it if you win and accept a prize.

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.

Email address: This will be used to confirm your registration so it must be an active account you can check to authorise the account. If we need to contact you this is how we will do it, so add the account cipher@soton.ac.uk to your email account address book to avoid sending our emails to your junk mail bin. Make sure the account is not too full, and check it regularly.

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.

Teacher contact: Give the name and email address of a teacher (or parent/guardian) we can write to if we need to check anything. You should get their permission first! We don't usually do this unless you win a prize. If you are home educated give us a parent or carer's name here and write home educated in the school name field.

School: Tell us which school you are at so we can include that on your certificate and the leaderboard. We have tied this into a Google Search to simplify the data entry, so do try that by typing in your school name and selecting from the list. If you really can't find your school there then enter the details of your city/town/village etc, as you would be surprised how many schools share a name across the UK.

The "Ineligible for a prize" box on the registration form

If you are a teacher who is registering in order to keep an eye on the forum, or a Cipher Challenge alumnus who is now too old to take part but just can't keep away, or ineligible for some other reason (like living overseas), then please tick this box so that the computer doesn't award you a prize by mistake! It is embarrassing for us to have to ask for it back. Thanks.

Teams and solo entries

If you are taking part on your own you need to register and create a team that will have just you in it. The team name can be set on this page:

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

If you want to enter as a group the Team Captain should register first and create a new team. The Team Captain can then send the team members a link to their team from the same page:

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

Team members can then register for accounts and use the link to request to join the 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 editing the name on the Team page under your account.

Please note the following important information:

1. 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.
2. If you wish to join a team after you have already registered then you will need to change your team. 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.
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 a team using the "Search Team" function on the same page:

   http://www.cipherchallenge.org/my-account/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.
6. 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!
7. 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.
8. For the purpose of awarding prizes an individual entry means an entry by a team consisting of one individual, and a team entry refers to a team with at least two members.
9. Team membership will be frozen at the start of Challenge 10 so that no further requests will be issued or can be accepted after that point.
10. You do not have to all be at the same school to form a team, we will use the Captain's school and email address for any communications with the team. The names of all the members of the team will appear on the certificates. You can also all read the feedback and download individual certificates from your account page.

The structure of the competition

There are ten rounds to the National 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 consist of Jodie’s notes to herself and her friends, and you can expect them to 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. Part B consists of the mysterious texts that reveal the story behind The Kompromat Files. At the start of the challenge the 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 on the form. 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. Don’t try to correct any errors

you think we have made, always type in an exact decryption of the text. 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. 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

Getting help

We offer online feedback on submissions during each round to help you if you make mistakes. The feedback is delayed so you will 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 speed doesn't matter for Part A challenges which are only scored for accuracy). The feedback consists of a score for accuracy, together with a copy of your submission with the first error highlighted. The feedback also contains a link to your certificate for the round. 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 Jodie in Part A, or posted (by us) as comments on the forum. We ask you not to post hints of your own without checking them with us first as this will spoil the Challenge for others. Anyone posting solutions or links to solutions on our site or elsewhere may be barred from the site and disqualified from the competition – we do search for them and do find them!

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. The more similar they are the higher the score you will get, 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, according to 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 leader board for each round. The first three rounds are a warm-up so the points will not count for the overall leader boards but from round 4 we will publish a Championship leader board based on your total points from then on in each of the competitions.

Rewards and Prizes

Everyone who takes part in any part of the competition 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!

In addition, courtesy of our wonderful sponsors, we have a number of major prizes for our top codebreakersand these will be announced on the website when the competition begins. Winners will be asked to provide information about how they cracked Challenge 10 in order to verify that their solution is their own work.

The Prize-giving

We will be hosting a prize giving ceremony in the Spring. Date and location will be announced as soon as possible and we anticipate that alongside winners and their families we will be able to offer some tickets to schools and individual competitors. These tickets will be available by lottery and you will be able apply for them online at a later date at:

www.cipherchallenge.org/tickets/

How many can enter?

Teams of any size and composition may enter, and a school can enter as many teams as it wishes. Inter-school teams are also allowed, indeed, encouraged. We have even had trans-national teams taking part, though prizes are strictly limited to teams entirely composed of eligible competitors.

Classroom materials

The Resources section of the website can be found at:

www.cipherchallenge.org/resources/

It contains a variety of materials you might find useful in the classroom or for a codebreaking or mathematics club. These include 6 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.

For those of you who like to decorate a noticeboard for the competition we also provide some graphics you might find useful for display work, alongside the usual pdf of the poster for download, and a list of movies with a cipher theme.

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

Rules, regulations and policies

These can be found online at:

www.cipherchallenge.org/information/rules/

If you have any questions or concerns about these or any other aspects 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.