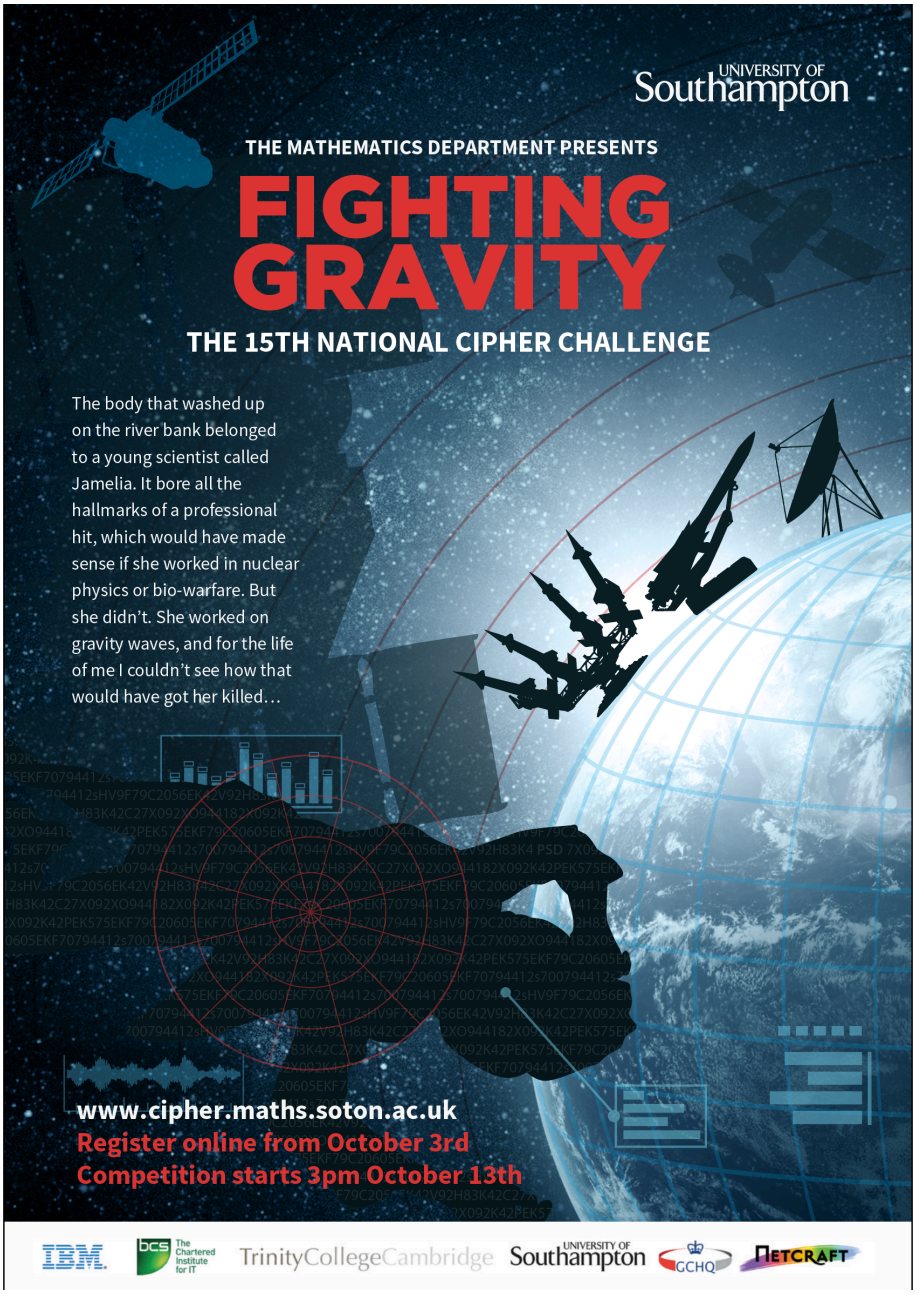
National Cipher Challenge 2016 Teacher's Pack v1.2



About the Challenge

Welcome to the National Cipher Challenge, a nationwide, online codebreaking competition, which will run from October 13th 2016 to January 4th 2017. We will open for online registration on October 3rd.

The competition is a great extension activity (or a fantastic maths club project) that can be tackled by students in teams or on their own. There is no charge to register or take part, and all you need to get involved is a reasonably modern web browser.

The competition has been running since 2002, and 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.
While the public image of the spy is as a lone wolf agent, team work can be critical in code breaking and a number of teachers have told us that the most valuable aspect of the competition is the way it encourages the competitors to work together. We have prizes for individuals and for teams. Claire West, a Mathematics teacher at Peter Symonds College commented on this:

> "As a teacher, I see the students form themselves into successful teams; with self-elected leaders who are responsible for organising their group after identifying their member's individual strengths. In our college, the challenges are worked on entirely by the groups alone as they use our library to work past the usual college close time. I am so proud of them."

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 to meet with competitors and to attend the annual prize giving at Bletchley Park. These include the media scientists Adam Hart-Davis, Hannah Fry 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 Hut 33, Robert Bathurst whose aunt worked at Bletchley in the war; two Foreign Secretaries, Boris Johnson and William Hague (though Boris was London Mayor at the time). We are also grateful to our sponsors

give time as well as money to support the competition, and it is not unknown for our winners to meet members of the secret world of GCHQ at the awards dinner. All of these people are really busy and they all see the value of the National Cipher Challenge, we hope you will too.
The competition is structured as a series of encrypted messages which tell a story. This year the competitors will be trying to unravel the mysterious death of Jamelia, a young scientist working in the hottest topic in mathematical physics, gravity waves. The police are certain it was suicide, but Harry is not so sure, and he needs your help to find out what really happened.
Entrants can take part alone or in teams of any size. To take part you will need to register on the website, and your account also gives you access to the forum where you can discuss a whole range of things connected to the competition, and quite a few that are totally unrelated.
Everyone involved in the challenge can have their own account to allow them access to the forum, but only the Team Captain can post entries for a team with multiple members. If you want to allow other members of the team to edit and submit entries then you will need to share the login for the Team Captain account with them. The Team Captain can also invite others to join their team using the link in the Team tab under their account details. If the person you want to invite already has an account then just send them the team “unique id” (which you will find under the team tab) and they can use the change team option in their account details to enter that code and join the team.

Competition schedule

Registration will open online on 3rd October 2016 and the first challenge will be published at 3pm on October 13th. Challenges will be set periodically on the web-site in the Challenges section, following this schedule:

Challenge	Publication date 15:00 on	Solution deadline 23:59 on
1	13/10/2016	19/10/2016
2	20/10/2016	02/11/2016
3	03/11/2016	09/11/2016
4	10/11/2016	16/11/2016
5	17/11/2016	23/11/2016
6	24/11/2016	30/11/2016
7	01/12/2016	14/12/2016
8	15/12/2016	04/01/2017

Points are awarded for speed and accuracy (with accuracy more important) but you do not have to rush to download the first challenges immediately as you have a day or two in which you can still get top marks. In later challenges speed will become important, and the full schedule of marks will be published so you can see how quickly you need to get started in each round.

The first two challenges should be thought of as a “warm-up” exercise and will not count in the final leader board rankings or for the award of main prizes, however it is still worth tackling rounds one and two as they give excellent practice and they do develop the storyline. There will also be a range of smaller prizes for those challenges and you will be able to download certificates recording your team’s performance at each stage.

As usual we apologise in advance if your school holidays clash with the schedule. It is impossible to set the schedule to avoid them all, but there is nothing to stop you doing the challenge during the break, you only need a web browser and your brain!

Registration

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

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

This will be open from October 3rd, and you will need to provide the following information:

Username: This will be the name you use to log on to the site to post comments, and also to submit your entries, check feedback and to print your certificate. 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.

Password: Again 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.

Teacher contact: Give the name of a teacher 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 schooled give us a parent or carer's name here and write home schooled in the school name field. You will still need to give us contact details in the address fields below.

School: Tell us which school you are at so we can include that on your certificate and the leaderboard. Do add your city/town/village (as in King Edwards School, Southampton for example) 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, 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 only need to register - and this will create a team of 1 with you as Captain. The team name can be set on this page: https://www.cipherchallenge.org/my-account/details/
If you want to enter as a group the Team Captain should sign up for an account. The Team Captain can then invite team members from this page: https://www.cipherchallenge.org/my-account/team/. Team members will then register for accounts using the team invite link they receive by email. The team name can be set by the team Captain editing your Profile on the “Details” page.

Please note the following important information:

A. Only Team Captains can submit solutions for the team. If someone else needs to do that then the Captain will need to share their log in information. Please be careful if choosing this option as once someone has your log-in information they can post as you on the Forum! 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. Then issue the invite from the shared account.
B. If you receive a team invite from a Captain after you have already registered then you will need to change your team. Do this by using the “Change Team” form on this page: https://www.cipherchallenge.org/my-account/team/. You will need to ask your Team Captain for your team’s "unique ID"
C. If you create your account using the instructions in a team invite received by email, you will automatically start in that team.
D. If you create another account having already joined a team, that new account will not be linked to the team unless you change your team using the “Change Team” form on this page: https://www.cipherchallenge.org/my-account/team/.
E. 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.

F. 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 ensure your team members join other teams. The whole team will lose any points accrued to that stage.

G. If you join a team after you have gained points you will lose those points and the team will not gain them. 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, and Team Captains joining another team will lose any points for themselves and their original team. Think VERY carefully about changing teams!

H. While you can choose to leave a team, once you have been invited and joined one you cannot be thrown out by the Team.

I. 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.

J. Team membership will be frozen at the start of Challenge 8 so that no further invitations will be issued or can be accepted after that point.

K. 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

You will find the Challenges on the Challenge page. 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 communications between Harry and his friends and you can expect these messages 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

texts that Harry is trying to decrypt in order to solve the mystery. 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 do 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 Harry 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 two rounds are a warm-up so the points will not count for the overall leader boards but from round 3 we will publish a Championship leader board based on your total points from then in each of the competitions.

Prizes

The GCHQ prize of £1,000 will be awarded to the top individual entry this year as measured by performance in the part B competition, and the IBM prize of £1,000 will be awarded to the best team entry. The Trinity College prize of £800 is awarded to the runner up in the individual category, and the University of Southampton will award £800 to the runner up in the team category. Winners will be asked to provide information about how they cracked Challenge 8 in order to verify that their solution is their own work.

The Prizegiving

We will be hosting a prize giving ceremony in the Spring. Date and location will be announded 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 from November 1st you will be able apply for them online 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. Teams can be run from one or several individual accounts (see above) and inter-school teams are also allowed, indeed, encouraged. We have even had trans-national teams taking part, though prizes are strictly limited to UK competitors.

Classroom materials

This year we have an all new site which has a new resources section.

www.cipherchallenge.org/resources/

This 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.

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.