|  |  |
| --- | --- |
| 1 | Please do read what you are told about Challenge 1B in Challenge 1A. The hint is right at the beginning of the message and tells you how 1B has been encrypted. Take the hint at face value. If that is how it has been encrypted, which one of the possible encryptions has been used? Look for three letter words like “the” and “and” and use them as cribs. |
| 2 | 2b: Is it a bit like 1b where it is backwards and bottom to top ignoring the spaces  I figured out 2B in literally 10minutes. Just use substitution. I found substitution very easy. (Of course it may not apply to all challenged)  All monoalphabetics are fairly easy with frequency analysis – I usually don’t try to figure out the cipher, just work it out – it works well for the part A and early part B  On the Challenge page there is a “tips” button, this week it states “As usual Challenge 2B is more obscure than Challenge 2A, and you have less information to go on than you did for Challenge 1. On the other hand Jamelia has not been quite so devious in putting you off the scent this week. She must have thought her hiding place was secure enough. Frequency analysis is still your friend, but you will probably need to use it to help you find more than just the letter e this week. You can find out how to use cribs to help you, and discover more about some of the elementary ciphers in our Beginner’s Guide to Codebreaking which you can download. Best of luck, Harry” I’d suggest following these hints, also you can look at words with only 1 letter. This should help as there are only a few choices for 1 letter words in the English language (then see how they appear in other words to try and guess which is which).  Now is “A fine” time to give a hint for 2B. Jamelia had a lot of Questions for Martin. |
| 3 |  |
| 4 | For those of you struggling with 4b, hope this helps. Use frequency analysis, this should tell you something about the type of cipher used (check on the beginner’s guide to code breaking if you need a hint). Next, look for cribs. A really good one is a word from the story which contains the letter x as this letter doesn’t occur in many other words in the English language.  Once you have done a frequency analysis compare it to a frequency analysis for the English language, you should notice something very, very important here. Then look at the beginners guide to code breaking, and see if you can figure out what kind of cipher it is (it is different to all the ones in this challenge so far). You should then easily be able to find the letter x & hopefully that whole word.  I solved 4B without a keyword too so I was also curious…  Joan posted that the keyword was ‘dupin'(https://www.cipherchallenge.org/forums/topic/official-clues-for-4b/page/2/#post-18708)  Dupin is the name of the protagonist of a detective novel called The Purloined Letter, which Trinity hinted at in 4A. Strangely, I remember trying this keyword and not getting a result. |
| 5 | 5a: There is a keyword, but you don’t need it to crack the cipher.  If you have already cracked it, then order your plaintext alphabet [abc..xyz] and the corresponding cipher text letters will reveal the keyword.  5A is a mono-alphabetic cipher (i.e. each letter has been substituted with another letter). Do a frequency analysis, and this should help.  Use cribs (likely words especially at the start and end, loook back at previous messages). Think what could be at the start. |
| 6 | 6a: Some of the solutions may have spelling errors put in deliberately, it was mentioned at the start of this year’s challenge.  6b: Read question 5B for hints for the question, I doubt there will be many hints for 6B.  Read Challenge 5B for the type of cipher. (for 6A). read challenge 5 very carefully, it tells you the type of cipher & key length for 6A.  6B: First Clue: Use the beginners guide to codebreaking. Do a frequency analysis, this should tell you if you are looking at a mono-alphabetic, transposition or poly-alphabetic cipher. More official clues will be posted following each points deadline.  Second Clue: The analysis shows that the frequencies are fairly flat compared to standard English so it is neither a transposition cipher nor a monoalphabetic cipher and so, most likely it is a polyalphabetic and the classic example is a Vigenere cipher. Now your task is to try to work out if that is possible by hunting for the likely length of a keyword. Look up how to do this using the index of coincidence in the Beginner’s Guide to Codebreaking.  Third clue: Calculate the ioc’s for lengths of 2,3,4 etc. until it is close to that of the English language (see page 15, 27 and 28 of the beginners guide to codebreaking).  Note: if you are struggling with this cipher, don’t worry it is harder than the previous ones and a big clue will be given tomorrow.  Fourth clue: You should have worked out from the ioc’s that the length of the keyword is 7. So, now write out the cipher text in 7 columns. You know each column has been coded with a Caesar shift. So on each column perform a frequency analysis and try to figure out the shift. You may end up with a couple of possible shifts, so note them both down and then check with the other columns to make sure it decodes to make proper words! After you have worked out a few of the shifts you may be able to guess the others by looking for cribs too.  Fifth clue: This is a note from Martin to Jamelia. Cribs for this kind of cipher are only helpful if you know where in the message the word occurs. |
| 7 | 7a: The frequency analysis shows that the frequencies are fairly flat compared to standard English so it is neither a transposition cipher nor a monoalphabetic cipher and so, most likely it is a polyalphabetic and the classic example is a Vigenere cipher. Now your task is to try to work out if that is possible by hunting for the likely length of a keyword. Look up how to do this using the index of coincidence in the Beginner’s Guide to Codebreaking.  Yes, this is a vigenere cipher, but with a twist. Calculate the ioc’s for lengths of 2,3,4 etc. until it is close to that of the English language (see page 15, 27 and 28 of the beginners guide to codebreaking).  Have you looked in the beginner’s guide to codebreaking on the resources page? Specifically at pages 15, 27 and 28?  OFFICIAL CLUE: From the ioc’s you should have noticed that the keyword is 7 letters long. Write out the cipher text in 7 columns. You know each column has been coded with a caesar shift. So on each column perform a frequency analysis and try to figure out the shift. You may end up with a couple of possible shifts, so note them both down and then check with the other columns to make sure it decodes to make proper words! After you have worked out a few of the shifts you may be able to guess the others by looking for cribs too. Remember, there is a twist too. So if at first you don’t succeed look back at previous challenges for a hint.  OFFICIAL CLUE: If you are still struggling with 7a hope this helps … This challenge is titled “The interview”, you have been told to look back in previous challenges for clues. It is more than just a vigenere cipher. I suggest you look through challenge 4 for ideas.  OFFICIAL CLUE: The message has been encoded twice, as well as a vigenere, it has been reversed.  7b: As you can tell from the frequency analysis the distribution is too flat for a mono-alphabetic cipher, but that doesn’t mean it has to be a vigenere. Further clues to follow on Sunday.  You may also notice something else crucial about the frequency of the letters, or lack thereof. This hint will be expanded on later on Sunday.  The fact there is no letter J, suggests that maybe I and J have been identified as 1 letter. Look up options for ciphers which use only 25 letters instead of 26.  OFFICIAL CLUE: There is more than one option for a 25 letter cipher. What has been used here is a Bifid cipher. There is some useful information at <http://cmup.fc.up.pt/cmup/v2/include/filedb.php?id=120&table=publicacoes&field=file>  OFFICIAL CLUE: On http://cmup.fc.up.pt/cmup/v2/include/filedb.php?id=120&table=publicacoes&field=file look at the end of page 2, section 2 for how to work out the period.  OFFICIAL CLUE: The period is 4. You now have a couple of days before any information about the keyword length and the keyword is released. Hope this clue gives you something to work with.  If you check out the other bifid forum pages, e.g. https://www.cipherchallenge.org/forums/topic/find-period-biffed-cipher/  there are some good explanations on how to work out the period. Or following the link earlier in this forum it explains it (but in more complex maths terms).  More clues will be coming out this weekend. No the keyword is not just a random word, it is related to the storyline. For ideas about how to encrypt (and therefore ideas about how to decrypt) a bifid cipher check out the example on the forum https://www.cipherchallenge.org/forums/topic/bifid-cipher/. You know the period so this should help out to work out the position in the table of the letters. The table is a 5×5 grid of all the letters in the alphabet (excluding J), but with a keyword at the start, e.g.if the keyword is cipher, it would look like:  –1 2 3 4 5 (ignore the — they are just there to try and put the column numbers in the right place)  1 c i p h e  2 r a b d f  3 g k l m n  4 o q s t u  5 v w x y z  If I wanted to write the message HELLO YOU with the above table and with period 4 (note challenge 7B has period 4), this is what I would do:  ——H E L L O Y O U  row: 1 1 3 3 4 5 4 4  col: 4 5 3 3 1 4 1 5  First split into blocks of 4 (the period), then write out the row & column numbers of each letter in the message from the grid. The read off row and then column, block by block, giving:  1133 4533 4544 1415, and use these as the row and column numbers for the cipher text  ——c l u l u t h e  row: 1 3 4 3 4 4 1 1  col: 1 3 5 3 5 4 4 5  Hope this helps, and look out this weekend for more info on the keyword length. You could also be thinking of possible starting words for challenge 7b, and maybe even come up with part of the grid this way.  Yes, challenge 7b is hard, it is supposed to be! Well done if you are 10 and have got this far. Keep a check on the forum, you will be able to break it before the deadline.  OFFICIAL CLUE: The keyword is 4 letters long. No it is not just a random word. Use this and the previous clues and descriptions to have a go at breaking this. Also think about what you may expect the start of this challenge to be.  OFFICIAL CLUE: The keyword is related to gravitational waves and is 4 letters long.  OFFICIAL CLUE: The keyword is LIGO. Hope this helps you to solve 7B – remember to look back through this forum for other hints and tips about how to solve it, e.g. use the example from earlier to set up your matrix etc. |
| 8 | First OFFICIAL CLUE: Watch <https://m.youtube.com/watch?v=ueZ6tvqhk8U> Remember you have 4 weeks to complete this challenge, so don’t expect too much too soon.  OFFICIAL CLUE: This challenge is more like water than sulfuric acid, more like nitric oxide than sodium nitrate.   * The first clue is not as cryptic as this one. For the first clue listen carefully to what is said. There is 1 key phrase which is helpful.   The second clue, the 4 compounds do not have anything in common. But 2 of them are different from the other 2 in a significant way.  OFFICIAL CLUE: Yes, this is harder than previous challenges, but not as hard as some of you think. I would say it is maybe, twice as hard, but not three times.  OFFICIAL CLUE: The previous clues were hinting at this. This is not ternary, it is in fact binary. You need to think what the extra characters could be there for.  Just a quick note for anyone who is working in excel at all, if you copy 8b it is more that 32767 characters, so not all of it will go in a cell when you paste it. You have to remove the spaces beforehand to prevent this (as after removing spaces it is under the character limit).  OFFICIAL CLUE: How long a map is needed to get from A to 26?  OFFICIAL CLUE: Happy Christmas everyone. You have all the digits you need for the alphabet on one hand.  OFFICIAL CLUE: Binary needs just 0 and 1. Work out how many digits you need to hold the number 26 in binary. Now look back at the 2’s and see if you can figure out how they are used.  OFFICIAL CLUE: If something is worth doing it is worth doing twice. Double or quits.  OFFICIAL CLUE: As you have probably guessed by now, this has been double encrypted, it is not just simple binary. We have not been too mean, but have used a cipher you are already familiar with. There is a keyword, and yes, it is related to the story.  CLUE: For binary you just need 0 and 1, the 2s have been used as a spacer. Use the other clues about how many digits you need to figure out how the 2s are spacers.  I have some mistakes in getting the letters as some of the spacers are variable distance apart eg 7 digits or 13 digits so dont know if that is a combination of 2 letters or just one I had previously used all the way up to 52 in decimal to identify the digits.  There are 26 letters in the alphabet and so you should need 5 binary digits to encode for each letter of the alphabet. What do you do with the other 6 letters? (There are 32 possible combinations of 5 digit binary numbers)  You don’t need to fill all 32 possible combinations of 5 binary digits, the last 6 can be left out. So if they only encoded letters then the largest number you can find would be 25 (in binary), so if you find a number larger than 25 you may have gone wrong, or they have added symbols to fill the last 6 numbers (comma could be 26 and full stop/period could be 27, but this is unlikely). And (edited…).  when the twos are made into spaces , you are left with chunks no larger than 5 digits. as 26 is made of 5 digits in binary form, this makes sense. however, i am still left with 5 digit chunks like 11111 which are more than 26. I must be missing something. i am also left with chunks that are simply 00000 or 0000 etc. if i make 0 = a, 1 = b etc., then i am left with even more chunks above 25 in binary. when i swapped 0s for 1s and 1s for 0s, the same problems arose. i tried using 25 as the maximum and using a modulo method to make numbers>25 = numbers<26 and then make the new numbers letters, but the frequency analysis was so out for the cipher type. HELP! what do i do???  OFFICIAL CLUE: Happy New year. The keyword is Dynamix, and there is one final twist …  OFFICIAL CLUE: This has been double encoded, I will not reveal the twist just yet, by you have seen something similar before. The general idea behind it is… Write out the binary for each letter in columns (5digits), write out a column of 5 2s at the end of each word. Read off by rows.  I have worked out what all of the clues mean but I still have no idea about what to do with values greater than 11001 – e.g. 11111  Normally “a” would be 00001 in binary, but … things are not always as straight forward as they seem.  ZXQ3N: The keyword will fast track you to the second layer of decryption. Sure you can work without it, but that just means more work. With the 99.99% correct answer – well done for getting so far. I had a similar message initially and I found that I had truncated the longest word by one letter. Proof read your plaintext carefully and see if a word (or two) has been clipped, then check your decoding in that place. Good luck.  What I don’t get is how the columns and rows bit works because if I split the message into 5, write them down in rows and read down the columns then the 2s still don’t line up as I thought they should do!   * OFFICIAL CLUE: Keyword is used to shuffle the letters of the alphabet, like in a mono alphabetic keyword cipher. Then use the binary to write out each letter, but in columns. So the word “and” would be: A n d 0 0 0 2 0 1 0 2 0 1 1 2 0 1 0 2 1 1 0 2   Then it would be read off in rows as 00020102011201021102.  But just to complicate things, the binary was written in reverse, bottom to top, and a keyword of dynamix was used to shuffle the letters.  In the example above you can see there are 3 digits between each number 2, and the are 5 groups of digits. This tells you the word is 3 letters long.   * The two encryption steps are:   1. Use a keyword to shuffle the alphabet (like in a keyword substitution) then write each letter as a binary number using its place in the list. Just to complicate things the binary numbers are written right to left rather than as left to right so whatever letter is first in the shuffled list gets encrypted as 10000. Use 22222 as a spacer between words.  2. Now write each block of of digits vertically under its character and read off horizontally by row for each word,  Foes that help?  Harry New Year!   * As the challenge is now closed:   Using the beginning of 8b ciphertext, remove the spaces and use the “2”s as the new line delimiter. Separate into blocks of 5 lines. The first part of 8b the looks like:  102 002 002 012 002  1112 0002 1002 0102 1012  1002 1102 0112 0112 0002  00101112 10100112 11000112 11000002 00000012  Within each block read the binary from bottom to top. Discard the 2s. This gives decimal equivalents of  1,8 (00001, 01000) 21,9,17 (10101, 01001, 10001) 3,14,12 14,12,3,0,1,7,23  Convert to alpha characters. A=0, B=1, C=2… and you get  BI VJR DOM OMDABHX  Now for the second level of decryption. Use a substitution cipher, keyword DYNAMIX and the plaintext becomes  IF YOU ARE READING  I used the pattern A = 00000, B = 00001, etc. reading up the columns (as numbers larger than 25 showed up reading down), giving me a text with an english-like IOC and then solved the rest as a normal monoalphabetic. |

can someone please help me with vigenere ciphers please because I am having some trouble understanding her

First, find the key length. Once you know that, the rest is easy.  
To find the length look for repeating patterns in the cipher text (my program looks for 3 letter long repeating patterns) and measure the distances between them, more specifically the distance between start of the 1st pattern and the start of the 2nd pattern (eg in “qqabcdqqqqabcdqq” there would be a distance of 8 between patterns). Then, factorise the distance and take a note of the factors. Do this for any other repeating patterns. Once you’re finnished, count up how many of each factor you have written down. The number appearing most often should be your key length.  
You can now use frequency analysis to work out the keyword. For example, if the length of the keyword is 8, preform frequency analysis on every 8th letter starting with the 1st letter, then another on every 8th starting with the 2nd, then every 8th starting with the 3rd and so on. Each time the frequencies should look like the letter frequency of plain english, but shifted. Work out the shift as if it was a cesar cipher.

Can someone please explain how to decrypt a playfair cipher without a keyword as I am very confused

* First you want to check if the text is encrypted with playfair, here are some of the checks you can do:

Ciphertext must have an even number of letters  
Ciphertext would probably have at most 25 different letters (due to one of the letters being removed to create a polybius square)  
Looking at each pair of two characters throughout the ciphertext, the two letters can’t be the same.

Then, look at section II in this guide (page 13):  
<https://fas.org/irp/doddir/army/fm34-40-2/ch7.pdf>

How To Work Out The Keyword of A Hill Cipher?

I mean, I’ve never actually done this, but, assuming a 2 by 2 matrix, you could try frequency analysis to find the most common digraphs and match them up to English, then use that information to find the matrix (though that may be hard due to the moduluses involved)

* This link explains a method, called “crib dragging”:  
  <http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-hill-cipher/>

Using this method requires knowing about modular multiplicative inverses, determinants of matrices and adjugate matrices. All three of these have Wikipedia articles, check them out.

I’ve written a program to use this method of finding a solution, and it usually solves a 2×2 hill-ciphered text in less than 3 seconds. It is quite complicated, but it works. My old method was just to brute force through every possible 2×2 matrix that gives a decryption, checking if it was correct, if it wasn’t it discards it and moves on to the next matrix. That usually took 30 mins to try all the possible 2×2 matrices.

How do you solve a Bifid cipher without knowing the key?

By hand, I would guess keywords and block lengths until a solution that works is found.

If you are experienced at programming, then I would suggest creating a program that runs through a simulated annealing algorithm, until it finds a solution.

I won’t tell you how to write this algorithm, but the idea is as follows:

You have a function that decrypts a Bifid-enciphered ciphertext given a key and a block length. Then you make it decipher the text given the alphabet (excluding J, Q, X or Z as it is Polybius-based) for a given block length. With that you can swap two letters at random in the key, and decrypt it again. If the solution you get is more english-like you can keep the key you used to get the new decryption, else discard the new key and swap another two letters in the last best key. Then carry on this process of having a key, swapping two letters and checking if it is closer to English, until it decrypts returning the correct decryption (or it gets stuck or isn’t the correct block length). You will have to try this algorithm on multiple block lengths, as it only improves the Polybius square used.

Simulated annealing can also be used to attack other, one-key, Polybius square-based ciphers e.g. Playfair. For two-key Polybius square based ciphers, I would use a dictionary attack on one square and run this algorithm each time to find the other square.

My python program that does this doesn’t swap random letters, but tries every swap possible on each iteration, and then chooses the best swap and modifies the key based off of that. If it can’t find a swap that improves it, it has either: found the correct decryption, got stuck in a local maximum, or the ciphertext isn’t Bifid with the given block length.

Simulated annealing: <https://en.wikipedia.org/wiki/Simulated_annealing>

Checking how english-like a text is: <http://practicalcryptography.com/cryptanalysis/text-characterisation/quadgrams/>

to decipher the code, you need to know how it was ciphered first: basically, you have a key which is a 5×5 grid with all the letters of eng alphabet in alphabetical order and i and j are combined so all j’s show as i’s in the text. then, each letter has a row no. and a column no. e.g letter a is row 1 coloumn 1. and b is row 1 and column 2. then, you take the plaintext and translate each letter into its row no. and column no. so a becomes 1 1 and b is 1 2. you write all the row no’s above the column no’s and then, you read all the numbers of the rows of the plaintext in twos, and the new two numbers next to each other become the rows and columns of the cipher text number. so if your plaintext was just ab, you would get  
a c b plaintext then you would read 111132 and take 11 to get a, 11 to get another a, and 32 to get m, reading cipher text as  
1 1 1 row aam. now, that is with the standard 5×5 grid. but with a cipher, it uses a keyword. the key word is then put  
1 3 2 column into the table starting in the top left corner with no repeating letters. now the key grid is changed about  
a little, the values will mean different things. that is why it is impossible to crack without key word.  
hope that helps

To find the period of a BIFID cipher:

* I didn’t know how to do this earlier, but I’ve tried a method and the results are quite consistent, so here we go.  
  This is also quite time-consuming to be done by hand, sorry but it’s the only method I’ve found to work so far. You’ll also need a calculator.

Firstly, we need to find the variance of bigrams/digraphs for different periods. I’ll take the first 20 letters of a ciphertext to demonstrate how this works, though you may have to take a larger sample (say the first 50 or 70 letters) to get accurate results.  
“HTPEGWEEHWAOHCPNIRXE”  
Count the digraphs skipping no characters between them: “HT”,”TP”,”PE”,”EG”,”GW”,”WE”, and so on.  
With the digraphs written down and the amount of that digraph in the text written next to each digraph, you need to work out the variance. This link shows you how to do it (ignore the things on standard deviation, it doesn’t help here):  
<http://www.mathsisfun.com/data/standard-deviation.html>  
Steps found on that page:  
Work out the Mean (the simple average of the numbers). Then for each number: subtract the Mean and square the result (the squared difference). Then work out the average of those squared differences.  
This process gives you the “variance”.

Then count the digraphs skipping 1 letters between them, “HP” (note the T has been skipped), “TE” (P skipped),”PG”,”EW”,”GE”, and so on. With these, calculate the variance of this new set of frequencies.  
Then count the digraphs skipping 2 letters between them: “HE” (skipping the “TP”), “TG”,”PW”, and so on, and calculate the variance of these.

Try and put the variances on a bar chart, there should be a peak on the graph. The number below the peak bar (the amount of skips between each digraph you counted to get the highest variance), plus 1, should be half the period.  
Say if you found the variances to be:  
Skipping 0 between digraphs: 0.05, skipping 1: 0.06, skipping 2: 0.35  
then you can see there is a peak at 2, so add one and double it, telling you the period is 6 (these numbers were made up, don’t use these, they are only for example).  
If the block length is odd then the peak will be split over two bars, much more difficult to see and may need even more ciphertext to analyse. If there is no peak, or a the peak is not significantly more than the other two (often one bar is double the size or more on an even period) then you may need to check skipping three or four digraphs and add their variances to the graph.

Please note: you need to analyse a decent chunk of ciphertext for this to work. I’ve also checked what would happen analysing certain amounts of text, and for some reason analysing the first 50 characters gives one clear peak, but analysing the first 60 gives two separate peaks between no skips and 3 skips, and analysing the first 70 letters gives one clear peak – so be careful.

An odd note: I also found that Kasiski examination also gave me the correct block length. Unsure if this works in every case though.

* UPDATE ON KASISKI EXAMINATION: (please read my first post before this, in that post is a much better-tested way to find out the period than this)  
  For those who are unfamiliar with this, check this out: <https://en.wikipedia.org/wiki/Kasiski_examination>  
  This method was designed for Vigenere and also works on similar polyalphabetic ciphers. It wasn’t designed for the Bifid cipher at all.

I’ve found that it works sometimes, and doesn’t work other times – it is somewhat inconsistent. I encrypted the solution to 3A with the bifid cipher at various periods / block lengths. As long as you check for repeated strings of 4 letters in a row or longer, Kasiski examination seems to work when a block length of less than 6/7 has been used.

I created a program to test various situations. This program encrypted the solution of challenge 3A with a bifid cipher with the keyword “SOLVED”, then it did Kasiski examination on the ciphertext. Each iteration of the loop did this with different periods, this is the console output:

Period: 2 – Result from Kasiski examination: 2  
Period: 3 – Result from Kasiski examination: 3  
Period: 4 – Result from Kasiski examination: 4  
Period: 5 – Result from Kasiski examination: 5  
Period: 6 – Result from Kasiski examination: 2  
Period: 7 – Result from Kasiski examination: 7  
Period: 8 – Result from Kasiski examination: 2  
Period: 9 – Result from Kasiski examination: 59

After testing a few other ciphertexts and different keys, it almost always finds the period if what was used is less than 6. And with a slight edit to my Kasiski examination functions (to allow it to accept more anomalies before it discards each number as a possible key length), it can quite often find periods of six too, but not higher.

If you were wondering, the Kasiski examination function in my Vigenere cipher file is well tested and accurate, it only checks repeated sequences of 4+ length as I found that using 3 letter sequences as well makes it fail to find the correct keyword length about 30% more. On a text the size of 3A (1355 letters) encrypted with Vigenere, it can almost always find the keyword length up to 23. On longer keys (23-27 letters) it finds the correct keyword length about 50% of the time. I told you this just to show that it is an accurate Kasiski examination, and not a badly written one that gives out bad answers lots of the time. This is also to try to verify the results I found are not a result of luck.

This is an alternate way to find the period, but as shown it can fail to find longer periods – using the method in my first post is more accurate, given you have enough ciphertext. I suppose it could be used after the method described in my first post, if no peak could be found.

* This page tells you how to use python to find the digraph frequency as well as trigraphs

[Help using code/script for ciphers](https://www.cipherchallenge.org/forums/topic/help-using-codescript-ciphers/)

Please note that the link above gives code for finding frequencies of digraphs/trigraphs/quadgraphs etc. but it doesn’t give you the code to get digraphs when skipping n letters between them.

This is a list of ciphers that could be used, but it doesn’t list some ciphers.  
<http://www.cryptogram.org/resources/cipher-types/>  
It lists many types of ciphers but it doesn’t show you how to decrypt them without a key.

I saw something on the resources page about a solitaire cipher which technically has 2.3×10^71 possible keys

* The National Cipher Challenge Wikipedia page is a great for ciphers used in the previous competitions, there is a chance that these could pop up again so I would do a little research if you want to be well prepared:  
  (Pasted from Wikipedia page)

The part A challenge consists of a relatively simple cryptogram that is intended for beginning cryptographers. In later challenges the cryptograms become harder to break. In the past, part A cryptograms have been encrypted with the Caesar cipher, the Affine cipher, the Keyword cipher, the Transposition cipher and the Vigenère cipher.

The part B challenges are intended to be harder. These begin with relatively simple substitution ciphers, including the Bacon cipher and Polybius square, before moving on to transposition ciphers, Playfair ciphers and polyalphabetic ciphers such as the Vigenère cipher, the Autokey cipher and the Alberti cipher. In the later stages of the competition, the ADFGVX cipher, the Solitaire cipher, the Double Playfair cipher, the Hill cipher, the Book cipher and versions of the Enigma and Fialka cipher machines have all been used. The 2009 challenge ended with a Jefferson Disk cipher, the 2012 challenge ended with the ADFGVX Cipher, the 2014 with the Playfair Cipher, and the most recent challenge ended with a sectioned Cadenus transposition.

* Being my fourth year now, I’ve been through a fair few different ciphers. I’ve found that Bifids are good to know. Vigineres are also useful as 7 and 8 A is almost always one. Others like playfair can be useful. The main problem is that 1-6 are fairly predictable, but 7 and 8 is when the guys making the ciphers have a bit of fun so there isn’t really much of a pattern for B other than that they will be a type that you didn’t know about (:P) and you will waste lots of time trying to crack them with the wrong type of cipher.

P.S. if you think that 7 and 8 are hard, be prepared for 9… (It is released to the winners then to the public a while later.)

* From the last 4 years of doing the cipher challenge I believe this is a comprehensive list of all ciphers used to date.

Caesar Shift  
Affine  
Keyword  
Columnar Transposition  
Porta  
Vigenere  
ADFGVX  
Beaufort  
Hill  
Solitaire  
Playfair  
Rail Fence Transposition  
AMSCO Transposition  
Cadenus Transposition

Just remember they still may use new ciphers

* Lots of the ciphers that have been used around this stage have already been mentioned.  
  Refer to Bottersnike’s and dompeel’s posts, mentioned in their posts are: Autokey, Alberti, ADFGVX, Bifid, Vigenere, Solitaire, Hill and Playfair – these have most likely been used before, though I can’t confirm.

Some other ciphers that haven’t been mentioned yet that I’d expect could come up around this stage (and probably have in one of the previous years) would be: ADFGX, AMSCO, Beaufort, Checkerboard, CM Bifid, Four-square, Gronsfeld, Myszkowski, Nhilist, Railfence, Trifid, Tri-square, Two-square and Variant.  
These are a selection of ciphers from my earlier post that are around the same strength of the ciphers already mentioned for this stage. There are others, but too many to list here.

As there are absolutely loads of ciphers, you need to find out which cipher has been used. When you don’t know what type of cipher it is, you have to look at certain properties of the ciphertext. Some examples of this are:  
Ciphers that encode 2 characters at a time (Playfair, Four-square, 2×2 Hill, etc.) must have an even amount of characters in the ciphertext.  
If the ciphertext is fairly long and doesn’t have a certain letter (usually J), it could be the omitted character in a Polybius-square based cipher.  
If the letter frequencies of the ciphertext is similar to English, it is usually a transposition cipher.  
If the text has an index of coincidence significantly lower than English, it is usually a polyalphabetic or polygraphic cipher.

For 8B, mentioned in the Wikipedia article: Playfair, Cadenus, ADFGVX, Jefferson Disk and Enigma.  
However, they probably won’t repeat a rarely-used cipher that has been previously used in 8B. I’d expect something that is extremely difficult to solve by hand. They’ve used machine ciphers before, so they could use something like TypeX or Lorenz. They could use really difficult ciphers that can be done by hand that incorporates multiple keys, like the Quagmire ciphers or the VIC cipher. They could also use difficult versions (or just use a really long key) of any of the ciphers mentioned above. In reality, there are too many ciphers to prepare for, unless you put some serious effort into researching as many ciphers as possible and devising ways to beat them.

I found Bottersnike’s earlier post really useful and quite accurate, use his/her advice. I spent loads of time trying to solve 1B and 7B with the wrong type of cipher.

I had never deciphered an encrypted text before 1A of this year’s challenge, but I hoped this helped.