


How to know that you haven't solved the Zodiac-340 cipher

Ryan Garlick

garlick@unt.edu


March 2014

You want to solve the Zodiac-340 cipher. I do too. No one has done it yet.

This is a symbol in the cipher: . It may translate into an English letter, a concept, an Arabic letter, a word from a book, punctuation, nothing at all, directions such as 'go up in the cipher', or something else entirely. Your 'key' is your translation of these symbols into letters, words, concepts, etc. This paper will assume that a symbol stands for an English letter, but most of the concepts as to why existing solutions are wrong should apply in most cases.

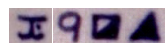
The two main **indicators of an incorrect solution are multiple translations (English letters) that can be represented by each symbol, and anagramming (rearranging letters)**, neither with a pattern. Basically, **a lack of patterns is bad**. A lot of existing attempts try to hide the fact that they have no pattern to their solution by introducing a fake pattern (not maliciously in most cases) such as switching keys frequently, which results in the same lack of coherent steps to a solution.

WARNING SIGN #1: If your solution has symbols representing multiple letters. I've seen solutions where some symbols represented more than 10 letters. Even with less than 10 possible letters for each symbol, I can make the cipher say that your grandmother was the Zodiac (and spell her name correctly). Having any symbol stand for any letter at any time can produce any solution, so some solutions mask this with a fake pattern, such as switching the key frequently for no reason. If I switch the key (the translation of symbol to letter) after every symbol, I have the same algorithm (or method of decoding the cipher) as one that allows any symbol to stand for any letter anywhere, it just looks more complex and thus more 'correct' (but isn't).

If  represents 'A' the first time it appears in the cipher, 'B' the second time, 'C' the third time, and so on, that's a pattern (and a polyalphabetic cipher). If that symbol represents five random letters because that's the best fit for what you think Zodiac wrote, that is not a pattern.

Zodiac may have been drunk and encoded it your way, but we'll never know. You're making up a solution. If you switch keys based on some pattern of the first letter of each subsequent sentence in the Declaration of Independence (and it works throughout the cipher), then we have something. If you just decide when we switch keys because it fits what you thought Zodiac wrote, we don't.

If you switch keys so often that you only have a few symbols before the key changes, then your sample is too short for analysis. For example, I made a cipher:



Can you break it? Well, any 4 letter word with all distinct letters will work. If multiple letters are represented by each symbol, then *any* 4 letter word will fit.

(The answer was actually 'dog' since in my cipher triangle symbols are meaningless.)

If your solution starts out really strong and then turns to gibberish, that's a very large warning sign. You can make the symbols mean anything that you want at the start. I want the cipher to start with "HI MY NAME IS GRANDMA". Now continue the translation using the same letters I did for these symbols and notice how not much makes sense afterward? That's because the key is wrong. Don't start allowing symbols to mean multiple letters – that's making up a solution. If you are using a transposition cipher where instead of just going left to right line after line through the cipher, you spiral clockwise from the outer edges toward the center, now that is a coherent pattern.


WARNING SIGN #2: Any form of anagramming. Anagramming is rearranging letters to make a word. Anagramming is OK if for every word, the first and second letters are swapped. That's a pattern. If in the first half of the cipher the first letter is at the end and the last letter is at the start of each word, and in the second half, every first and second letter is swapped, that is a pattern. If you can arbitrarily rearrange letters, I can make the cipher give all sorts of nasty details on your gram-gram's killing spree. If you convert symbols to letters, and then anagram and have letters left over at the end of each sentence, you are allowing symbols to mean nothing arbitrarily and you almost certainly have an incorrect solution. Anagrammers usually suffer from pareidolia.

WARNING SIGN #3: Other fake patterns

If your pattern is really not a pattern (particularly if it is something based on numerology), that's not good. For example, Zodiac killed Darlene Ferrin in July, which is the 7th month, so skip 7 characters. Paul Stine was in Cab number 912. $9+1+2$ is 12, so use the next 12 characters, etc. I can find any number of ways to do that with the facts of the case, and there is no pattern to how you chose the action of skipping, adding, or deciphering symbols. You tried to introduce an artificial pattern through numerology, and 10 out of 10 mathematicians agree that numerology is bullshit. (Numerology even has 10 letters, to 'prove' the thing about the 10 out of 10 mathematicians). However, if the first quadrant uses a key based on the number of claimed victims in Zodiac's first letter, the second quadrant uses a key based on the number of claimed victims in his second letter, (and you don't introduce a bunch of anagramming), that is a pattern. If every time you come across the plus symbol, you remove the next two symbols, that is a pattern.

There are a lot of solutions that just ignore portions of the cipher and pick and choose words in a 'solution'. Sometimes these words are left to right, sometimes they are diagonal or backward. Sometimes the leftover letters are anagrammed. With rules as arbitrary as this, I can make your granny's name appear up and down in the middle of the cipher and ignore everything around it. This is extreme 'lack of pattern'.

A lack of pattern before or after the translation is the same thing. I have recently seen 'solutions' where each symbol only represents one or two letters, but the lack of pattern then presents itself in the English 'translation'. In other words, having a consistent key but then trying to fudge the English to make "ITTKEM" mean "I TOOK THEM" is the same problem. If you are getting short, choppy, forced sentences that don't really sound like something Zodiac would bother to encode, you're probably mistaken.

If you are a visual person, and see the  as a mountain, and mountains can also be called peaks, and PEEK is then reversed into KEEP. Well, I interpret the up arrow as "TOP", and TOP reversed is POT, which

often calls the kettle BLACK, so BLACK is the word represented by this symbol. I don't think either of us is correct.

Don't make up words. **B K Φ O** does not spell 'BOOK'. "SLAVESS" in your translation might spell 'slaves' though. AUNCE doesn't spell 'once' any more than it does 'a(n) unc(l)e'.

Can I generate other solutions using your method or a slight variation of your method? If so, why is your solution the right one? The SFPD will not hesitate to perp-walk your sweet grandmother.

One other warning sign is people who emphatically claim that they have solved it. A real scientist publishes his or her work as a potential solution to have others look over and verify. It's not entirely certain that the 408 solution is accurate (I think it is), but in reality we will never know to certainty. If someone says "this is my solution", read on. When someone says "this is THE solution" and reacts harshly to peer review, beware.

Other people say they are close... this is also a warning. You are close when the entire solution presents coherent text (with a lot of patterns in the decoding steps!), but you realize that you need to switch the half-filled circle from a 'P' to a 'W'. Otherwise, you're probably just guessing that you are close. It's like saying you were close to finding Atlantis. You either found it or you didn't.

If someone will not detail how they solved the cipher or tries to sell a solution, it should be dismissed.

Responses

Hey, the solved Zodiac-408 had multiple letters for each symbol. It is believed to be a fat-tipped felt pen that Zodiac used that caused a triangle and a filled in triangle to be interchangeable, etc. but it did not appear to be an integral part of the encoding.

Hey, Zodiac made mistakes and misspellings. Yes, he did. If you have a few symbols that can represent 2 letters, and a few spelling mistakes, you're on the right track. If each symbol can represent 7 letters or your solution has 5 of the letter 'T' in a row, granny is going to jail. Don't disparage her memory.

I don't care what you say... I solved it! The message boards will not be kind and the FBI will probably be polite but think you are a nut.

So I can break pattern half way through the cipher, but not every 5 symbols? Why is one OK but not the other? How many patterns do I get to break? Any break in a pattern lessens the likelihood that your solution is correct. Anagramming with multiple translations for each symbol is really no pattern at all.

If you do most of the things in this paper, please don't send your submission to the FBI / San Francisco Chronicle / SFPD / Universities, etc. But please do keep working on it.

I don't mean to dampen any enthusiasm for this project or hurt anyone's feelings. A lot of effort has gone into solving this cipher, and it will probably be solved by someone like you. Actually, if there is a solution it will probably be discovered by Kevin Knight at USC - he's really good at these things. But please keep it

up – I just hate to see the time of so many hard working people wasted on creating and evaluating solutions that violate most of the principles above.

It is my opinion that this is not a straight homophonic substitution cipher like the 408. I believe that some manipulation of the cipher has to occur first, such as dividing the cipher into quadrants. The cipher may also be meaningless.

Happy hunting and best of luck!