Final Eighteen Letters of the Zodiac Killer's 408 Cipher Solved … and his Identity Revealed

Tony Polito, Ph.D.

August 9, 2014[1]

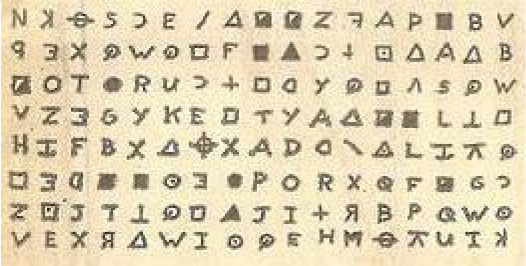
For 45 years, the decoding of the 18 alphanumeric characters from Zodiac's first 408-symbol cipher—which Zodiac stated twice would reveal his identity—has eluded a solution by any and all cryptographers, professional or otherwise. I present here my decoding of those 18 characters—which indeed plainly reveal Zodiac's true identity.

Introduction

Just so you won't initially write off my solution as that of a *total* crackpot, let me first say that I have been a member of MENSA for 35 years, I hold a double undergraduate degree in Mathematics & Statistics (two skills closely associated with successful cryptographers) … and I hold a masters degree and a doctoral degree from top-tier universities as well. So I am not a dumb guy! To be fair, I must state that I do NOT have any special expertise or experience in the field of cryptography, only a general and basic knowledge of it … and neither am I an expert or especially accomplished mathematician and/or statistician.

Background/Prefacing Discussion

On July 31, 1969, The Zodiac Killer—his puzzling infamy reignited by the 2007 film *Zodiac* starring Jake Gyllenhaal—sent his first three letters to San Francisco area newspapers claiming responsibility for several murders. One letter was sent to the *Vallejo Times-Herald*, one to the *San Francisco Chronicle* and one to the *San Francisco Examiner*. The 7/31/69 letters were the first of many Zodiac letters sent to the media over the years following.



Each of the three 7/31/69 letters contained one-third of a cryptogram, each containing 136 symbols, totaling to 408 symbols. The third sent to the *San Francisco Chronicle* is pictured at right as an exemplar. Accordingly, taken together, they have come to be referred to as "the 408 Cipher."

Zodiac demanded his materials be printed in the newspapers … and the papers ultimately complied.

The professional cryptographic community—CIA, FBI, DIA, NSA (ie, "CryptoCity") and Naval Intelligence/NCIS—were apparently unsuccessful in cracking the 408 Cipher. However, a week later, a local high school teacher, Donald Harden, and his wife had successfully decoded the symbols within the 408 Cipher as follows:

[1] 2014-08-17, substituted *Chronicle* cipher as exemplar on page 1. 2014-08-19, credits 2 as a prime number. 2017-11-12, update at page 10.

> I LIKE KILLING PEOPLE BECAUSE IT IS SO MUCH FUN IT IS MORE FUN THAN KILLING WILD GAME IN THE FORREST BECAUSE MAN IS THE MOST DANGEROUE ANAMAL OF ALL TO KILL SOMETHING GIVES ME THE MOST THRILLING EXPERENCE IT IS EVEN BETTER THAN GETTING YOUR ROCKS OFF WITH A GIRL THE BEST PART OF IT IS THAE WHEN I DIE I WILL BE REBORN IN PARADICE AND THEI HAVE KILLED WILL BECOME MY SLAVES I WILL NOT GIVE YOU MY NAME BECAUSE YOU WILL TRY TO SLOI DOWN OR ATOP MY COLLECTIOG OF SLAVES FOR MY AFTERLIFE
> **EBEORIETEMETHHPITI**

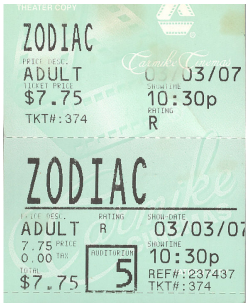
Experts today concur that this is the correct decoding of the 408 symbols; the Hardins received a single telephone call from the FBI acknowledging their success.

The misspellings are generally believed to be intentional, in that Zodiac viewed them as sort of Socratically satirical—making him sound stupid, when he was actually proving to himself and others to be rather clever and elusive. Clumsy misspelling of words that were phonetically correct (ie, paradice, anamal, forrest, Christmass) was a consistent behavior throughout The Zodiac correspondences. And it was just one of the many behaviors Zodiac used to self-satisfy his intellectual superiority complex, a complex that required him to constantly prove to himself and others that he was more clever than "lesser minds."

The final eighteen alphabetic characters of the 408 Cipher have, up to now, never been successfully decoded. In the next section, I explain how I decoded those 18 characters … and how they decode to reveal Zodiac's identity.

Decoding of the 18 Alphabetical Characters (2007)

On March 3, 2007, I saw *Zodiac* in theatre on release, then I rented it to watch again on August 9, 2007. Prior to that, my only interest in this topic was the reading of an interesting article about the Zodiac 'radian theory' in a magazine sometime in the early 1980s, which I *think* I recall to have been published in *Esquire.*



After watching the movie several times, I spent another afternoon further educating myself about The Zodiac case from information available on the Web. I thought it might be interesting to attempt to crack the final 18 characters of the cipher. I did not consult any cryptographic texts or materials, but simply relied upon what I recalled from readings in my youth about cryptography, pen & paper and a few Excel spreadsheets.

There really was no evidence that Zodiac was any kind of accomplished and/or expert cryptographer. Accordingly, the use of complex algorithms and/or techniques to try to decrypt the cipher really didn't make much sense. It made more sense to look for very simple techniques that he could have easily understood. And the encoding techniques used were indeed very basic.

Zodiac used two basic techniques to encrypt this 18-character message. First, he used a simple **substitution scheme** … where one letter of the alphabet is simply substituted for another:

> B occurs once in the cipher. It replaced the one instance of G in the uncoded message.
>
> M occurs once in the cipher. It replaced the one instance of N in the uncoded message.
>
> O occurs once in the cipher. It replaced the one instance of T in the uncoded message.
>
> P occurs once in the cipher. It replaced the one instance of U in the uncoded message.
>
> R occurs once in the cipher. It replaced the one instance of I in the uncoded message.
>
> H occurs twice in the cipher. They replaced the two instances of E in the uncoded message.
>
> I occurs three times in the cipher. They replaced the three instances of L in the uncoded message.
>
> T occurs three times in the cipher. They replaced the one instance of M … as well as the two instances of A … in the uncoded message.
>
> E occurs five times in the cipher. They replaced the three instances of R … as well as the two instances of H … in the uncoded message.

As an aside, Zodiac had purpose in using E & T—and *only* E & T—more than once. E & T are, respectively, the most frequently used letters in English. All decoders know this well … and will investigate the possibility that the most frequent letters in the cipher … might be E or T in the uncoded message. Zodiac intentionally created some modicum of confusion in decoding by making E & T the two most frequently used letters *in the cipher*. Decoders might (erroneously) believe the two letters "map" to themselves (and be led astray in their efforts at solution) … or would have difficulty figuring out what they map to, since other letters appear less frequently in normal usage (than E and T appear in the encoded message). In fact, Zodiac used this same "double-mapping" technique in the decrypted section of the 408 Cipher, where a specific symbol (a triangle with a dot in the middle) was used as substitute for both A & S. Again, Zodiac is using a very simple-to-understand, but reasonably effective, coding technique. Simple, in order to prove (to himself) how unintelligent his pursuers were.

Reversing these substitutions into the 18-letter cipher yields:

E B E O R I E T E M E T H H P I T I

R/E G/B R/E T/O I/R L/I R/E M/T H/E N/M H/E A/T E/H E/H U/P L/I A/T L/I

R G R T I L R M H N H A E E U L A L

The second, underlying, coding technique was also basic. The result from above is actually no more than an **anagram**; meaning that the letters are scrambled/mixed up just as they are in the "Jumble" puzzle seen on the comics page of most American newspapers. Common letter patterns (such as the double-L, which did occur in this message) yield clues to crackers when they are exactly duplicated in the coded cipher; anagramming disguises such patterns. Simply unscrambling the letters in the correct manner yields the original, uncoded Zodiac message:

R G R T I L R M H N H A E E U L A L

M R A R T H U R L E I G H A L L E N

And there you have it. The 408 Cipher was "signed" by "Mister" Arthur Leigh Allen. Allen is indeed the major Zodiac suspect as portrayed in the 2007 *Zodiac* movie, in turn based on Zodiac expert Robert Graysmith's books *Zodiac* and *Zodiac Unmasked*. I suspect the addition of the prefix "MR" was added by Allen merely to effect some incremental complexity in the decoding. QED.

Further down in this document, I explain the deduction of Zodiac's offset key … that data-evidences that this is indeed the intended and unique solution.

Solution as Circumstantially Correct

To me, it was plain enough to strongly suspect the 18 characters to contain Zodiac's identity:

> First, in the *San Francisco Chronicle* version of the 7/31/69 letter delivering the 408 Cipher, Zodiac plainly stated that "in this cipher is my identity." Recall that the 408 Cipher was delivered in thirds—one-third of 136 characters each to the *Chronicle*, the *Vallejo Times-Herald* and the *San Francisco Examiner*—each with its own handwritten letter. Each handwritten letter is almost identical in content … but ONLY the *Chronicle*'s letter's states that "in this cipher is my identity." And, indeed, it is the *Chronicle*'s third of the 408 Cipher that contains the 18 characters in question.
>
> Second, on 8/4/69 another letter from Zodiac arrived at the *San Francisco Examiner*; in it Zodiac said about the 7/31/69 408 Cipher, "when they do crack it, they will have me."
>
> Third, the 18 characters are positioned at the end of the cipher, exactly where we would ordinarily expect to find the signature to a correspondence.
>
> Fourth, when you think about it, there's really no way Zodiac's intellectual superiority complex was going to allow him to NOT leave some way to definitively claim and mark "his work" as his own .. right under the noses of investigators and the media.

However, instead of taking the above facts to suspect the 18 characters to reveal Zodiac's identity, investigators took Zodiac "at his word" when he says earlier in the 408 Cipher "I will not give you my name." To some extent, the 18 characters had been "written off" as meaningless "filler characters" to make each third of the 408 characters to be of equal (136 character) length. To be fair, that is not an uncommon cryptographic practice. However that rationale, to me, seems odd given Zodiac could have slightly reworded the bulk of the message slightly so as to accomplish the same effect. No, the 18 characters have meaning. And given they require additional decrypting, likely a more important meaning.

As mentioned above, Zodiac established a consistent pattern of "proving" his own superior intellect over others. And that is what he has done here. He's plainly stated both beforehand and afterward that the cipher contains his identity, and yet he's tricked "inferior minds" into concluding it does NOT contain his identity by the statement he made in the decoded section of the cipher "I will not *give* you my name." But there Zodiac chose his words carefully, intending to mislead "lesser minds." Zodiac is saying that he is not "giving" his identity *away so easily* … as easily as he had the rest of the cipher. And indeed his identity requires an additional degree of decrypting. He is privately reveling in the notion that, though he's made it plain enough that the 18 characters must be his identity and signature, investigators could not see through to it.

Zodiac often used such confounding statements to self-satisfy his intellectual superiority complex on other occasions, such as:

- Writing in one letter "I think I shall wipe out a school bus one morning." Then, in a later letter, stating "If you cops think I'm going to take on a bus the way I stated I was, you deserve to have holes in your head."

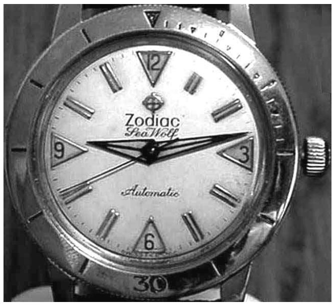
- In the Lake Berryessa incident, he fabricates a detailed story (about being an escaped convict from Montana who needs their car and money to get to Mexico) toward convincing his victims that he had no need/intention to harm them. The roping/tying of the victims may have been intended to extend this ruse. He then "proves" to them that they were foolish to have ever believed him at all by assaulting them anyway.

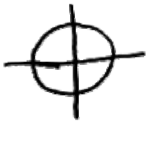
- In the Kathleen Johns incident, when the tire falls off and she then trusts him and gets in the car with him anyway, he's proving to himself that he's the more intelligent … in that "the plain evidence" is that he had loosened the lug nuts rather than tightened them.

Taken in total, then, there's excellent circumstantial cause to believe the eighteen characters were a coding of Zodiac's identity … and given they decode to the name of the major suspect … good cause to believe that the decoding as above is correct.

Circumstantial Evidence against Allen

There is a tremendous amount of circumstantial evidence against Allen. The most persuasive item amongst them, in my opinion, being the fact that Allen wore a Swiss "Zodiac Sea Wolf" watch bearing both the brand name Zodiac, as well as the killer's trademark "cross-haired circle" icon, on its face. The watches were a popular choice among Navy divers at the time and there is much evidence that Zodiac had been in military service; Allen was less-than-honorably discharged from the Navy in December, 1958. It was gifted to Allen at Christmas, 1967 by his mother. These watches were the only place that investigators were ever able to discover where the word Zodiac and the cross-hair symbol occur together … other than within Zodiac's own correspondences. Surely Allen took great pride in his own intelligence in that he "wore" this damning evidence in plain sight every day, yet went unsuspected.





It was almost exactly one year after the gifting of this watch, 12/20/68, that the first fully-confirmed Zodiac murder took place—perhaps to "celebrate" Allen's own birthday (12/18) as well as the first "birthday" of his Zodiac identity. (On 12/18/69, Zodiac called the home of attorney Melvin Belli. Zodiac told the maid who answered the phone that he had to kill since it was his birthday. Two days later, on the first anniversary of the first confirmed Zodiac murder, a fully-confirmed Zodiac letter was mailed by Zodiac to the Belli residence.)

While investigators have never been able to uncover any "hard" scientific evidence—DNA, prints, blood—that would conclusively prove Arthur Leigh Allen to be Zodiac, there is an undeniably enormous amount of circumstantial evidence identifying him as prime suspect. Quick references for the reader on this topic include:

http://www.zodiackillerfacts.com/allen.htm

http://www.zodiackiller.com/Cheney.html

http://www.zodiackiller.com/MulanaxReport4.html

http://www.crimelibrary.com/serial_killers/notorious/zodiac/34.html

Zodiac (2007) at 1:16:24 (reenactment of 7/21/71 Don Cheney interview about his 1/1/68 conversation with Allen)

Zodiac (2007) at 1:20:14 (reenactment of 8/4/71 Arthur Leigh Allen interview by investigators)

Zodiac (2007) at 2:23:00 (Tochi & Graysmith characters summarize circumstantial evidence against Arthur Leigh Allen)

https://www.youtube.com/watch?v=KBBHl0l1pcc (beginning at 25:10)

Solution as Data-Evidenced Correct (2014)

What is stated above as solution, is that I obtained on August 14, 2007 after about five hours of filling my trash can with crumpled paper many times over … and using several crafted Excel worksheets that could quickly iterate the various possibilities. Then I wrote the solution up neatly, essentially as it is presented above. After that, I stopped working on the task, in order to prepare to begin my Fall, 2007 courses at my University. I set the matter aside, folded up the scratch notes, sealed them into an envelope and put it into one of my in-baskets … then became preoccupied with a thousand other matters. I did not to return to the project for another seven years.

On Tuesday, July 22, 2014, I had a drink and a conversation with an acquaintance who is an aficionado of cinema, and the topic of the 2007 *Zodiac* film arose. He claimed he believed that the balance of the Zodiac ciphers had recently been solved. And that conversation provoked me to renew my interest in the work that I had accomplished. I could not find any significant evidence that corroborated what my acquaintance had said. So I retrieved and reexamined the solution, document, scratch notes and Excel worksheets I had developed in 2007.

The major reason I had set the solution aside was I did not believe the work was *entirely* accomplished. While I had discovered the decoding … and a decoding that fit extraordinary well with the facts surrounding the cipher and the case ***circumstantially*** … argument could still be made against it. Other substitution schemes and other descramblings of any resultant anagram could result in other words, names or phrases, some even sounding relevant. What *data-based* evidence was there to support my solution was above all those other possibilities?

After several more hours of examination of those materials on July 28 & 29, 2014, I was able to quickly deduce pretty conclusive evidence to that effect. To explain that evidence first requires a little more discussion about substitution ciphers.

The simplest substitution scheme known is called a "Caesar cipher." The coder picks an "offset" number. Let's say 4 is picked. Then the coder simply substitutes the fourth letter "away from" the original letter…. E substitutes for A, F substitutes for B, and so on. When you "reach" the end of the alphabet, you just "wrap around" … A substitutes for W, and so on. Such ciphers, as they should sound, are incredibly easy to crack. For one thing, there are only 25 possible encryptions. Such a straightforward Caesar cipher is easily cracked by "brute force" (ie, by simply generating all of the 25 possible solutions). And if you look at the frequency of the cipher characters (Again, E is, by far, the most common letter used in the English language, followed by T), you can probably crack it without even generating all the 25 possibilities. So Caesar ciphering is basically useless as an effective encoding scheme.

Accordingly, many substitution ciphers possess some type of scheme to make the "offset" more complex. For instance, the number *pi*—3.14159265358979323846264433…—could be used as the "offset key." In that case, 3 is used as the offset for the first letter of the message, 1 is used as the offset for the second letter, 4 is used as the offset for the third letter of the message, and so on. Someone trying to crack the cipher would find this offset pattern difficult to discover … but the intended receiver of the message can decode it very easily so long as he/she knows in advance that the offset key is *pi*. The possibilities for such offset keys is endless. Any commonly available sequence of numbers could be used, or one can be created by using a random number generator and giving the result in advance to the message receiver. The Enigma Machine, the cryptography device used by Nazi Germany, essentially was a device capable of developing a vast number of highly complex (but replicable) offset patterns/keys through a complicated gear-set mechanism. The sender turned and set the gears according to a certain previously agreed-upon setting, typed in the uncoded message, and the machine typed out the coded message; the receiver set the gears in the same previously agreed-upon setting, typed in the coded message, and the machine typed out the uncoded message. There was an enormous number of possible settings for the Enigma devices.

Knowing all this meant that if I could reconstruct the "offset key" that was used for substitution, that fact would essentially prove my decoding was unquestionably the correct one. So I looked at the offsets … and almost immediately an incredibly simple but undeniably "man-made" pattern readily emerged:

M in the cipher replaced N in the uncoded message. The offset is + 1.

E in the cipher replaced H in the uncoded message. The offset is +3.

I in the cipher replaced L in the uncoded message. The offset is + 3.

B in the cipher replaced G in the uncoded message. The offset is + 5.

O in the cipher replaced T in the uncoded message. The offset is + 5.

P in the cipher replaced U in the uncoded message. The offset is + 5.

T in the cipher replaced A in the uncoded message. The offset is + 7.

E in the cipher replaced R in the uncoded message. The offset is +13.

R in the cipher replaced I in the uncoded message. The offset is + 17.

T in the cipher replaced M in the uncoded message. The offset is + 19.

H in the cipher replaced E in the uncoded message. The offset is + 23.

All these offsets are prime numbers! A prime number is a number that is evenly divisible only by 1 and itself. [2] In fact, Zodiac has used almost *every* prime number between 1 and 25 (inclusive). Only 2 and 11 are not used. Prime numbers are an unusual artifact and area of study within the discipline of mathematics. They quickly become more rare as numbers become larger; there are only 169 prime numbers less than 1000.

The use of prime numbers here can hardly be attributable to chance. Let's look at the odds. The possibility that one offset would be prime, just by chance, would be 10 (the number of primes between 1 and 25, inclusive) divided by 25 (all the possible offsets). That's 40%. Now what are the odds of *all* of the eleven offsets being *any* prime number, just by chance?

$(0.40)^{11}$ … or 0.00004194304 … or approximately 0.0042% … or approximately 4.2 chances out of 100,000 … or about 1 chance in 25,000.

And they are not all just *any* prime number, they are almost **ALL** of the prime numbers available to use. The odds that almost ALL of them would be used, by chance, must be incredibly lower. (I'll leave it to a professional statistician to calculate *those* odds.)

Let me paint an analogy for those whom cannot easily visualize the significance of such odds. Suppose you happened upon a family with eleven children, all boys. Now *that* would seem pretty rare, wouldn't it? Of course, because most large families end up with some kind of mix of boys and girls. The chances of a family having just two children, both boys, is just $(0.50)^2$ or 25%. But *eleven* boys out of eleven children, just by chance, that would be

$(0.50)^{11}$ or 0.000488281 or 0.0488281% … or about 5 chances out of 10,000 … or about 1 chance out of every 2,000 families with eleven children. (And that's about 12 times *more* likely than the probability calculated just above for the prime number usage.)

Now imagine that those eleven boys have their birthdays spread over ten different months, that all of the months have been used up for birthdays except two. That would be *very, very* rare, wouldn't it? (Again, I'll leave it to a professional statistician to calculate those odds.) So very rare indeed that we might start to suspect, not chance, but parental planning … that the parents timed conception so that each child would have a birthday in a different month, that the parents timed conception so that a boy was more likely, and so forth.

[2] The number 1 is often excluded as a prime number for various theoretical reasons, however most people not deeply familiar with the theory of primes would almost certainly include it in a list of primes.

Yet it is many, many times more likely that parents, by chance, would have all eleven children as boys *and* use up all but two of the birthday months … than it is that, by chance, these offset keys would all be prime numbers *and* would use up all but two of the prime numbers. It's virtually impossible that these offsets occurred by chance. **"Prime numbers" is the offset key … the key chosen by Zodiac.**

Prime numbers make for a very simple offset key to understand, yet amazingly elusive to discover. Even if a decoder knew for certain that the offset key was "prime numbers," the message would still be impossible to fully decrypt. There would not be a unique solution, but rather endless possibilities of combinations of prime numbers. Using brute force would eventually result in the "unreadable" (but correct) anagram looking as gibberish … as one among a massive number other possible solutions that also decrypt to look as gibberish. Most encrypted message are intended for decrypting, but Zodiac's message was not intended for "a recipient" to readily decrypt, hence he did not have to select an offset key that would make decryption easy and/or result in a unique solution. The choice of prime numbers as key only made it more difficult for crackers to discover, since they would be prone to look for keys that derive a unique solution, as is typical practice.

I cannot definitively speak to why Zodiac excluded 2 & 11 as part of his prime number offset key choices, but here are a few of the possibilities I considered:

- There are exactly eleven letters used as substitutions into the uncoded message. Yet another unlikely coincidence, statistically speaking.
- It could be an attempt to throw off decoders investigating prime numbers as an offset key, as 11 would appear to be useless.
- Eleven "splits exactly in half" those prime numbers used; there are four primes used below it and four primes used above it.
- Zodiac exhibited a pattern of selecting numbers for his purposes to have underlying personal relevance, including the commemoration of dates. One possibility in that vein is that Allen was tributing his successful escape from what many suspect to be the first true Zodiac murder, that of Cheri Jo Bates late on 10/30/66 in Riverside, California. That puts Allen driving back to Northern California (to where he worked in Valley Springs, California) on 10/31/66 and/or 11/1/66. Allen was unusually absent from work on 11/1/66, perhaps a personal holiday taken in "celebration of his accomplishment."
- Zodiac might have skipped over 2 since it was the odd duck, the only even prime number.

The possibilities of why the prime numbers 2 and 11 was excluded from use … and/or why it might be significant to Zodiac … are truly endless. I searched for a "meta-key" that could explain why 2 and 11 went unused, why certain primes were used more frequently, and so forth … however I was unsuccessful in that effort. Indeed, such a meta-key may well not even exist.

Investigators have never been able to uncover any "hard" scientific evidence—DNA, prints, blood—that would conclusively prove Allan to be The Zodiac. ***Now they have that hard evidence* … in the form of *statistical* evidence**. Though I left the final statistical calculations to the experts, I feel certain they will find that there is virtually no statistical possibility whatsoever that this 18-character message could be decoded into the major suspect's exact name … and also into offsets of this nearly-complete set of prime numbers … by pure chance.

Update [2017-11-12]:

In the three-plus years since this document was made public, there have certainly been some armchair-expert nay-sayers posting on blogs, claiming that substitutions-plus-anagramming could "produce anything." I did acknowledge that possibility, at the top of page 7. However, combined with the introductory set of positive prime numbers as offset key, deriving a solution that as at least as relevant, while true to the methodology, is virtually impossible. That is the core of the argument being made at pages 7 through 9.

While such nay-sayers simply state 'oh yeah, you could get anything out of this approach' and then dismiss this solution out-of-hand**, the fact is that no one has actually DONE IT … produced & posted a solution that is anywhere near as relevant, while remaining true to the methodology at its level of efficiency**.

As example, one poster claims to have used this methodology to produce the solution MR RICHARD GAIKOWSKI. Since Gaikowski is considered by more than a few to be a suspect, that solution certainly IS as relevant. However, that solution is NOT as efficient and/or true to the methodology:

> The offset key used in this 'Arthur Leigh Allen' solution is basically the set of all positive prime numbers between 1 & 23, with only two of them missing, and it only employed two of them more than once. The posted 'Gaikowski' solution employs 7 positive prime numbers *and three negative* prime numbers, using four of them twice, one of them three times. Technically, *there's no such thing as a negative prime number* (since all negative numbers are divisible by -1). Further, the number zero is used three times … *also not a prime number* … because it has more than two divisors. If the crypter was using prime numbers, he surely knew that zero was not one of them.
>
> In the 'Arthur Leigh Allen' solution I've given here, there are nine letters of the alphabet being substituted. Seven of them are a direct replacement (such as 'B replaces G'). The other two letters each replace two letters … and there's argument presented as to why that those two specific letters might have been picked to be used in that way. The posted 'Gaikowski' solution is similar with regard to seven direct substitutions, however one of the letters is used to replace *three* letters. And there's no argument presented as to why it was done.

Again, anagramming just by itself could provide other solutions … some even sounding relevant. But with the introduction of most of this set of positive prime numbers between 1 & 23 as the offset key, obtaining a equally relevant solution, true to that method, is going to be virtually impossible.

Nay-sayers should either (1) actually produce an alternate relevant solution true to the entire methodology to back-up their 'anything' claim and/or at least (2) produce a credible opinion from a professional statistician that supports their position.

Questions & Answers

I suspect my solution will generate all sorts of inquiries from all sorts of people. In the interest of parsimony and/or economy, I will below attempt to answer what I suspect some of those questions would be.

I have a whole lot of questions about The Zodiac? Can you answer them?

I am not a Zodiac researcher or a Zodiac expert. There's an amazing about of detailed information about the Zodiac case on the Web authored by such individuals where you can find answers to most of your questions. Please don't fill my email in-box with those kind of questions, thank you. Try ZodiacKiller.Com for starters.

You mean, after over four decades, no one in the worldwide professional cryptographic community ever came up with a good solution for this?

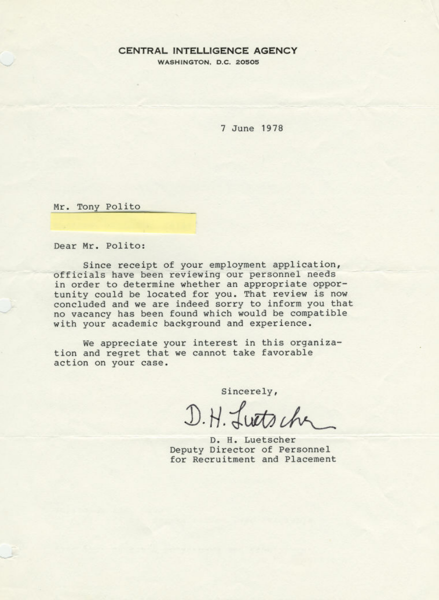
If someone did, he/she did not make it public … and that fact probably says something about the state of 'professional' cryptography today. An unfortunate trend these last few decades is that professionals everywhere try to turn everything they touch into an exact mathematical science/sport, when, in fact, the social "sciences" are not anywhere near exact. Success within the world in which we live still quite usually requires human skill, intuition, experience; solution—of anything—it really still "part art." I am reasonably sure that decades of preening of cryptographic techniques have led to this same sort of posture … analysis done solely by tremendously overwrought mathematical techniques that "torture" the data without any human insight whatsoever. So I believe it is this "pure quant" perspective that is the root cause as to why "professional" cryptographers were unable to solve it. The only known (and somewhat) reasonable solution offered came from the Hardins, who believed it solved to "Robert Emmet The Hippie." (And this solution required the Hardins to add characters.) It turns out that Arthur Leigh Allen did once tangentially know someone by this name, but there is no known motivation as to why Zodiac (or Allen) would have mentioned him, and investigators have no reason to believe the man was in any way actually involved in the case. Googling as I write this returns claims to some other lesser-known solutions that do not seem very meaningful (eg, Time I hit the beer Poe). The solution herein is obviously much more "on point" than all of that.

Oh, come on dude, you must be ***some*** kind of professional cryptographer.

No. As a high school student and as a mathematics and statistics undergraduate major (1970 through 1978), I took a very healthy reading interest in many unusual mathematical/statistical/logical/puzzle topics. I had a sharp mind, I was basically a speed reader with a fairly photographic memory and I was very interested in learning, well, what seemed interesting. I could have cared less about doing homework or studying for tests at high school or university. Those topics that captured by interest included not only cryptography but topology, the nature of the fourth dimension, Escher & tessellations, game theory, Möbius strips & Klein bottles, transfinite numbers & Hilbert's Hotel, Gödel's Incompleteness Theorem and a lot of other similar discipline oddities. Also during that time I also developed a fascination with *solving* puzzles, and so reading a great deal in that area, such as books authored by the late Martin Gardner, formerly of *Scientific American* magazine. I still have a few of his books on my bookshelf today.

From all that I developed, what was at the time, a somewhat decent skill for out-of-the-box puzzle-solving. I recall the first day of my undergraduate "Introduction to Logic" class very well. The professor presented, at the end of class, a logic puzzle of a form many people have seen at one time or another—three men on a train, each with a different hat, a different destination, a different color tie, and so on … certain facts are given such as "the man with the red tie is going to Chicago, the man with the black suitcase is wearing a green tie, and so on … and then a question is posed such as "What kind of hat is the man going to Tulsa wearing?" These types of problems are difficult for neophytes not informed as to the logical processes used to derive the solutions. He told us to turn in our solutions and then we could leave. I had just finished working about six of these kinds of problems for fun the week prior (out of a puzzle book) and so I was "on my game" in that area, so to speak. It took me two minutes to work it, and I was the first to turn something in. When I put the solution on the professor's desk he didn't look at it; no doubt he thought I was clueless and just wanted to leave class. I insisted he check it. When he did, he looked pretty astonished. (I earned a final letter grade of B).

Ironically, I suppose, in 1978, as college senior finally thinking about finding a job, I thought work as a cryptographer would be fascinating and I applied for such work with the CIA, NSA and DIA … and I was turned down. Below are copies of a couple of the rejection letters.



CENTRAL INTELLIGENCE AGENCY
WASHINGTON, D.C. 20505

7 June 1978

Mr. Tony Polito
[redacted]

Dear Mr. Polito:

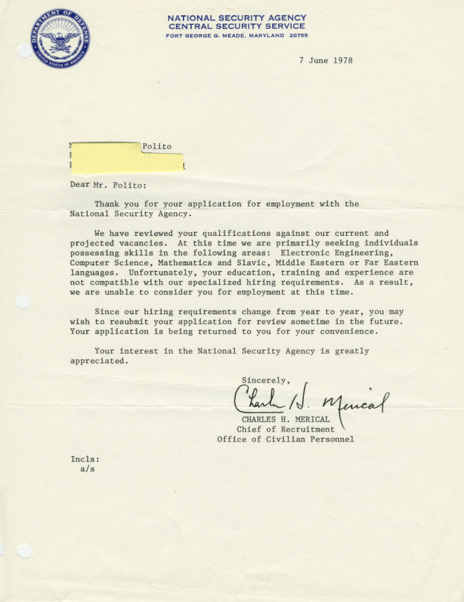
Since receipt of your employment application, officials have been reviewing our personnel needs in order to determine whether an appropriate opportunity could be located for you. That review is now concluded and we are indeed sorry to inform you that no vacancy has been found which would be compatible with your academic background and experience.

We appreciate your interest in this organization and regret that we cannot take favorable action on your case.

Sincerely,

D. H. Luetscher

D. H. Luetscher
Deputy Director of Personnel
for Recruitment and Placement



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755

7 June 1978

[redacted] Polito

Dear Mr. Polito:

Thank you for your application for employment with the National Security Agency.

We have reviewed your qualifications against our current and projected vacancies. At this time we are primarily seeking individuals possessing skills in the following areas: Electronic Engineering, Computer Science, Mathematics and Slavic, Middle Eastern or Far Eastern languages. Unfortunately, your education, training and experience are not compatible with our specialized hiring requirements. As a result, we are unable to consider you for employment at this time.

Since our hiring requirements change from year to year, you may wish to resubmit your application for review sometime in the future. Your application is being returned to you for your convenience.

Your interest in the National Security Agency is greatly appreciated.

Sincerely,

Charles H. Merical

CHARLES H. MERICAL
Chief of Recruitment
Office of Civilian Personnel

Incls:
a/s

In solving this cipher, again, I did not do any prior consulting of any cryptography source materials or information, rather I relied just upon what I remembered about it all from my youthful readings. As I prepared this document, I *did* look at and/or double-check my facts (eg, Was the DIA still in business? Was 'Caesar Cipher' for sure the correct name for that stuff, What comes first again E or T, etc.). I also Googled the phrase "EBEORIETEMETHHPITI" just to make sure no one else had offered this solution. That's it.

What about all that other stuff in the bulk of the 408-character cipher?

I suspect that the much of what was contained in bulk of the cipher, such as Allen thinking he was making "paradice slaves," was just nonsense on his part, intended by Allen to prove himself smarter (to himself), in that investigators would foolishly conclude Zodiac was psychotic and/or delusional, when in fact Allen was simply enjoying the knowledge that he had concocted such odd statements in order to fool/confuse them. I don't believe Allen intended the bulk of the cipher to communicate any meaningful/useful information about who he was or "why he did it." I think, so far as the cipher was concerned, he was far more interested in the self-satisfaction he could derive from having his identity "right under the noses" of investigators who did not recognize it as such. Again, a major part of Zodiac's overall pattern was to prove to himself that he was smarter than others … and to do so at their expense. The bulk of the cipher served to distract investigators from focusing upon the far more important final 18 characters, just as Allen intended.

Ok, I have a lot of experience with cryptography and this method doesn't follow the most standard crypto practices and so this solution of yours strikes me as sort of phony.

There's no reason for us to expect Zodiac to follow the most rigorous, official standard techniques of the profession. He employed basic, easy-to-understand techniques, as seen in the bulk of the 408 Cipher. He chose his offsets/substitutions to suit his purpose, not to use absolute recognized "best practice" in the professional cryptographic community, who crypts to defeat other professional crypters … all that was probably far too complicated for him to actually understand anyway. By using a variety of offsets, it's plenty difficult to crack the code unless you at least have the offset key. Allen may not have intended it, but by NOT following the most generally accepted "high-powered" practices of *encoding* messages, he probably prevented the success of the most generally accepted practices of *decoding* messages. The fact the bulk of the 408 Cipher was cracked by a husband/wife amateur team … instead of the various government agency professionals assigned to such tasks … is evidence to that point.

The "litmus test," though, is really found in the pattern of the offset key. A cracker just substituting at will *could* come up with a number of possible messages (albeit not as 'to the point' and so closing following the letter frequency as this one). But the offset key pattern demonstrates that the substitution scheme used in this solution is in no way random.

Having a statistical perspective on matters, it seems to me that the probability that all these facts—the strong relevance of the message (ie, the name of the major suspect), the match between the type of message expected (ie, a signature/identity) and that actually found, the comparative "neatness" of the solution (ie, Occam's Razor), the prime number offset key, the attempt to disguise letter frequency just as done in the bulk of the cipher, etc.—well, the chances that ***all that*** is actually due to coincidence/chance must be very, very close to zero, indeed.

I thought handwriting analysis cleared Allen?

Yea, like he was going use his actual handwriting. Give me a break. Handwriting analysis, in the long run, has proved out to be far less than a science and a pretty unreliable methodology. Few scientists today will defend the notion that there are inviolate handwriting traits. These days, you see a myriad of scientific methods used all the time in courtrooms; handwriting analysis is not among them. I suppose it sounded like good science forty-five years ago, though. And, to be fair, investigators of the day had few other choices; mostly all they had were the letters, so they had to default to handwriting analysis as a major investigative process.

What about the April 20, 1970 "my name is" 13-symbol cipher?

I don't know and I haven't given it much thought. My first guess/intuition would be to say that this was another "reverse taunt" by Allen, that it IS NOT a coded message at all, just a string of meaningless symbols. Given he stated so plainly it was his name in this "fill-in-the-blank" style, he could expect investigators to spend a lot of time to assume it WAS his name … and so Allen would have delighted in the thought that he had tricked investigators into wasting a ton of time trying to decode a random list of meaningless symbols.

What about the 22-symbol "bomb-map" cipher?

Again, I don't know and I haven't given it much thought. My first guess/intuition is that it IS a coded message of some kind. I doubt it actually reveals the location of an actual bomb. I believe Allen intended the "bomb scare" to be an extensive "wild goose chase" for investigators from which he could derive even more self-satisfaction. When he thought they weren't taking the bait, he tried to "egg them on" to it several times; that says to me he wanted satisfaction out of it … and no bomb plus lots of looking would for Zodiac equal a lot of satisfaction. Small bombs and bomb-making equipment were found on Allen's property; perhaps he tinkered in it, but never quite figured out how to "pull it all off big-time." Thank goodness he didn't think of filling up a rental truck like Timothy McVeigh did; Zodiac's diagram indicated use of the same explosive materials. The decoding of the cipher, had it been accomplished, might have indeed sent police chasing a lot of geese, much to Allen's pleasure.

What about the November 9, 1970 340-symbol cipher?

> Again, I don't know and I haven't given it much thought. I expect it would take a lot more work to decode such a large message … and perhaps a lot more talent than I have in the area of cryptography. My first guess/intuition is that it IS a coded message of some kind … and that it is not a total ruse of random symbols.

Who was Jack the Ripper?

> OK, I give up. Who was it?

Can you explain *Mulholland Drive* and *Lost Highway* to me? What really happened in *The Magus*? Who killed Kennedy? What does "666" mean? Was Arnold dreaming the whole thing in *Total Recall*? Where is Malaysian Airlines Flight 370? Did the top stop spinning in *Inception*? What did they do with Jimmy Hoffa's body?

> Actually those are all among many "puzzles" I have enjoyed intellectually wrestling with a good bit in the past and I do have reasonably strong opinions about them. Perhaps I will write them up and post them someday. But I am not going to spend weeks composing a response to such questions … just to give them up to you.

If you are so smart, you must be rich.

> No, but I am currently very interested in finding a new job that pays better. I'm *that* smart. Can you hook me up?

# # #