The Role of Base 10 in the Beale Papers

Viktor Wase
Stockholm, Sweden
viktorwase@gmail.com

Abstract

The *Beale Papers* is an 1885 pamphlet claiming to contain the location of a huge hidden treasure. The only snag is that the message is encrypted and, as of writing this, unsolved. This study investigates the authenticity of the ciphers by comparing the distribution of the numbers in the ciphers to each other, in different bases. Humans are generally ill-suited to the task of generating random numbers. As such, one might suspect that the behaviour of the distributions in base 10 would be widely different from the other bases if the ciphers were faked. The results of this study strongly indicate that this is the case.

1 Background

The *Beale Papers* is a pamphlet from 1885 in which the unnamed writer claims to have come into possession of three ciphers, which are contained in the publication (Ward, 1885). The ciphers are said to be written by a man called Thomas J. Beale - hence the name. The writer goes on to explain how he manages to break cipher number 2. It was a book cipher that could only be read using the correct book as key. The correct key in this case being nothing other than the *Declaration of Independence*. The cracked cipher claims that cipher 1 describes the location of the most valuable treasure of precious metals and gems ever to be found, and cipher 3 lists the name and place of all next-of-kin that have a rightful claim to the riches. The pamphlet costs 50 cents, which is roughly equivalent to 13 dollars today.

One could, at this point, disregard this as a simple ploy to sell a few pamphlets of false hope to the more gullible parts of the population. However before the idea is dismissed out of hand, there are some things that need be told. One of the characters in the pamphlet is named Robert Morriss. He is an in-keeper who knew Beale from before, and promised to keep these ciphers until Beale returned. If Beale was unable to return in ten years, then an unnamed friend of his would send a letter allowing Morriss to read the ciphers. This letter would arrive no earlier than June 1832. But no letter ever arrived, and neither did Beale. The interesting thing is that the local newspaper *the St. Louis Beacon* has a section where they listed mail couldn't be delivered and was being held at the post office. One of the newspapers from August of 1832, which would fit the time line of the pamphlet's story, such a letter is held for Robert Morriss (Chan, 2008)! It should be noted how unusual the spelling of his last name is, as there were no Morriss listed in the 1840 census of St. Louis, at all.

Another piece of information supporting the credibility of the Beale Papers appeared on Boxing Day 2001. A classified study for an NSA conference in 1970 was released to the public under the Freedom of Information act (Hammer, 1970). It was written by Dr. Carl Hammer, director of computer science at Univac Federal Government Marketing. His doctorate was in mathematical statistics and probability theory. The study investigated some *signatures* of the ciphers as well as of other similar ciphers, and found that they where both data and process dependent. Meaning that one can gain insights about the plain-text as well as the process of enciphering by studying these signatures. This line of inquiry gave such strong evidence for the credibility of the Beale Papers that the last line of the abstract is: "[the signatures] indicate also very strongly that Mr. Beale's cyphers are for real and that it is merely a matter of time before someone finds the correct source document and locates the right vault in the Commonwealth of Virginia." One could easily become rather conspiratorial by thinking too long and hard about why the US government kept this report secret for over three decades.

It should be noted that there is plenty of evidence against their authenticity as well. The most concise comes from 1927 when an author named Kendell F. Crossen asked how the next of kin can possibly be listed in cipher 3 (Kruh, 1982). In the pamphlet it says that there were 30 men in Beale's company, and the cipher is only 618 signs long. That does not leave many letters per person.

Another common argument against it is that it would actually be surprisingly hard to decipher the second text with the Declaration of Independence. First of all, there are several versions of the declaration and unless you have the correct one it will be hard to decipher it. However, even if you do have the correct version it will be hard to decipher it for there are a few peculiarities in the cipher (Mateer, 2013):

- a word was miscounted around position 630, as well as 670.
- 480 was used to represent two different words.
- "self-evident" was counted as one word, instead of two.
- For some reason ten words were skipped around position 480.

The first three might have been mistakes you could realise and fix as you were deciphering, but the last one is harder to explain away.

2 Related Work

The Beale Papers have been studied from a statistical perspective before. Partly by Hammer in 1970 (Hammer, 1970), as mentioned above, who concluded that the ciphers might just be real.

A contrary position was taken by L. Kruh, who considered the possibility that author of the pamphlet also wrote the letters from Beale that are included in the pamphlet (Kruh, 1988). The language use of these texts were compared. Statistics such as the distribution of words per sentence, the distribution of verb tenses, as well as the distribution of word classes were considered. These comparisons show that the texts are very similar, and might be written by the same author.

3 The Importance of Base Ten

Humans are really rather terrible at being random. In a meta-study on the subject from 1972 only one out of the 15 studies were positive towards human's ability to create random sequences (Wagenaar, 1972). In that study the participants were asked to create a sequence of O's and X's using two stamps. Usually, humans will switch symbol more often than what would happen in a true 50/50 random sequence. The author of the meta-study argued that it might in fact be the boredom and laziness of the participants that made them use the same stamp repeatedly - they simply wanted it done with.

On a not entirely different note: if a person was to write a long list of random numbers, then they would probably do so in base 10. This might not seem relevant, but number might be perceived to have certain properties depending on which base they are written in. For example, the numbers 101010_2 and 42 are not obliviously identical, and one of them might even be perceived as having a *symmetry* the other does not. Or how about 12345 and 17836_9 - the first one does seem less random and more ordered than the second one. Which is utter nonsense, of course - they are the same number. But it goes to show some of the limitations of the human perception of numbers.

This would mean that three ciphers, all encoded with the same method, should give similar results under statistical investigation. If two of the ciphers were faked, on the other hand, then such statistical investigations might give similar results in base 10, where humans have intuition, but probably not in other bases.

3.1 The Last Digit

Let's start at the end, with the last digit in each number. The numbers used in the Beale ciphers span a rather large range: from 1 to 2906. With such a large range, one can imagine that the last number is evenly distributed over all digits - that it is simply noise compared to the larger magnitudes.

This hypothesis can be tested using a discrete Kolmogorov-Smirnov (KS) test. This test is used to estimate the likelihood of two sets of samples being drawn from different distribution. The KS statistic is defined as the maximum difference of the cumulative distribution functions of the sets of samples. That is

$$\max_x |f_1(x) - f_2(x)|$$

where f_1 and f_2 are the cumulative distribution functions, and x is a real number. The test is applied to the given distribution (uniform) and the

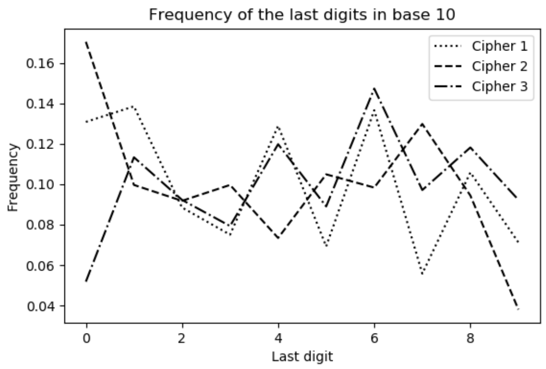

Figure 1: Frequencies of the the last digit of each number, for all ciphers.

given cipher. One starts by generating n random points from the distribution, where n is the number of data points in the cipher. If the KS statistic of the new points and the uniform distribution is larger than the original statistic, then one makes a note of it. This step is repeated multiple times, and the p-value is the portion of iterations with a larger KS difference than the original KS difference.

Using 1,000,000 iterations per cipher one can conclude that the hypothesis is wrong. The distribution of the last numbers are not uniform, for any of the ciphers. The p-values for the three ciphers are: 0.4%, 0.02% and 0.4%. The distributions can be seen in figure 1. The first and third ciphers oscillate a bit, in a way which means that the numbers are more likely to be even than odd.

This is where things are starting to get interesting. The same experiment is repeated but in different bases. Only bases that are relatively prime to 10 are considered, to avoid that the effects of base 10 spill over. For example, the even-odd disparity will show up in all even-numbered bases. See figure 2 for the result.

The p-values of cipher 2 are consistently small, meaning that the numbers are not uniformly distributed and there is nothing inherently specific about base 10. This cannot be said for ciphers 1 and 3. Their p-values are really rather large for all bases except 10, and its neighbours. This strongly indicates that the digits are uniformly distributed, with the exception of when they are given in base 10.

3.2 Benford's Law

Another hypothesis one might consider is that perhaps the leading digit follows Benford's Law (Benford, 1938). It's not a *law* in any sense of the word, nor was it created by Benford. Nomenclature issues aside, the law states that if a distribution spans several multitudes, then the distribution of the first digit might follow the distribution: $\log 1 + \frac{1}{d}$ where d is the leading digit (1-9). It is often used for fraud detection (Nigrini, 1999).

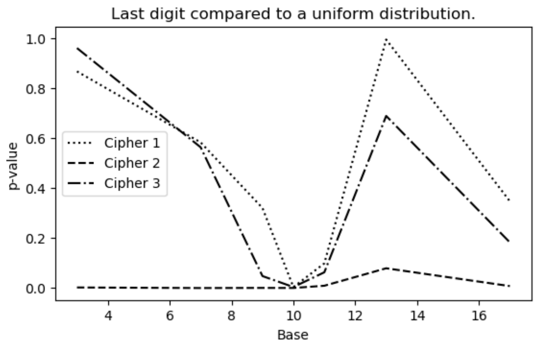

Figure 2: Results of the discrete Kolmogorov-Smirnov test, comparing the distribution of the last digit of all numbers to a uniform distribution.

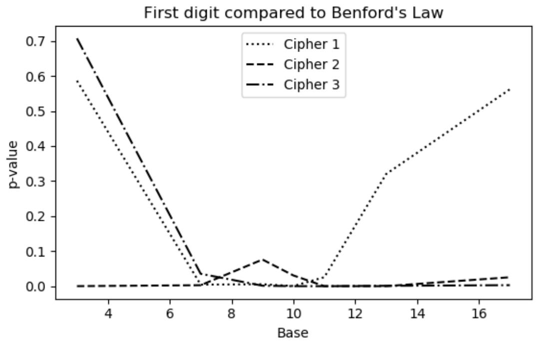

Figure 3: Results of the discrete Kolmogorov-Smirnov test, comparing the distribution of the first digit of all numbers to Benford's Law.

This hypothesis was tested using the KS test described above, with 100,000 iterations. However, it turned out to be false this time too. The p-values are 0.043%, 3.1% and 0.004% for the three ciphers. But, once again, what holds true in base 10 might not hold true in other bases. A KS test was performed, same as last, but looking at the leading digit as compared with Benford's Law. The results can be seen in figure 3.

Cipher 1 takes a clear dive at base 7, and doesn't start growing again until after base 10. Cipher 3 never starts growing again. The valley around 10 is wider than when looking at the final digit, but that is to be expected since the last digit is more sensitive to a small base change than the first digit. As of why the third cipher never grows, I

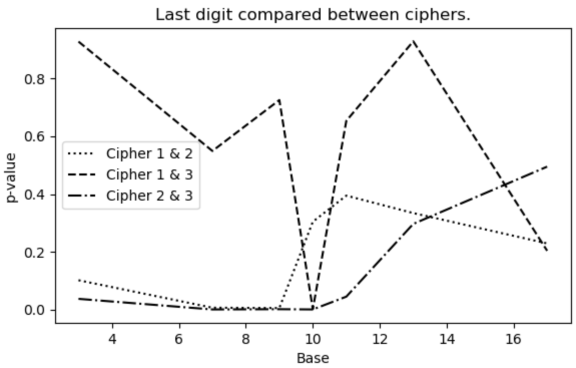

Figure 4: Results of the discrete two-sample Kolmogorov-Smirnov test, based on the last digit in each number.

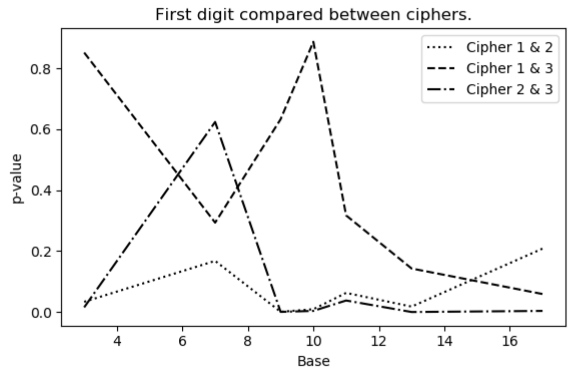

Figure 5: Results of the discrete two-sample Kolmogorov-Smirnov test, based on the first digit in each number.

find the most likely explanation to be that it spans the range [1, 975] and cipher 1 spans the range [1, 2906] and Benford's Law works better when several orders of magnitudes are spanned.

3.3 Non-assumptive Comparisons

Instead of comparing the ciphers against analytical distribution one can compare the ciphers against each other. Using a discrete two-sample KS test each pair of ciphers was tested to see if they were drawn from different distributions - for the first and the last digits, separately. The general idea of the test is simple, one calculates the KS difference between the ciphers. Then the samples are randomly shuffled between the ciphers, and a new KS difference is calculated using the shuffled samples. The shuffling is repeated 100,000 times, and each time the shuffled KS value is larger than the original value, one makes a note. The idea is that if the ciphers are different, then shuffling the samples between them should decrease the difference, but if they are created from the same distribution then the difference between them shouldn't change by shuffling the samples.

The last digits are compared in figure 4. Base 10 shines like a beacon, but not in the expected way. The comparison of cipher 1 and 3 has consistently large p-values, with the exception of a large valley at base 10. The values of comparison of 2 and 3 are low for all bases at 10 or lower. However, contrary to the expectations, the comparison of 1 and 2 does not show a valley around 10. Figure 5 shows the comparison of the first digits, and it shows a distinct valley at base 10, although not nearly as pronounced as in the earlier experiments.

4 Conclusion

One can, with a greater certainty than before, declare the Beale Papers to be frauds. The statistical tests strongly indicate that cipher 1 and 3 are inherently different when viewed through the lens of base 10 as compared with the other bases. I would consider this, in and of itself, to be damning evidence. But the fact that we have access to a real cipher, supposedly written by the same author, which does not show the same behaviour in the slightest, makes the argument even stronger.

There might possibly be different explanations for this behaviour. Perhaps the key to the book cipher has ten words on every line, or a multiple of ten lines per page. Perhaps the creator of the ciphers predicted this line of attack and deliberately made sure that we would get this result to throw us off their scent. Or perhaps they were just human with all our faults and limitations and learned to count, write and talk numbers in base 10.

5 Acknowledgements

I would like to express my very great appreciation to Johannes Wennberg for many and long fruitful discussions, as well as novel and interesting ideas. Thank you!

References

Frank Benford. 1938. The law of anomalous number. *Proceedings of the American Philosophical Society*, 78(4):551–572.

Wayne S. Chan. 2008. Key enclosed: Examining the evidence for the missing key letter of the beale cipher. *Cryptologia*, 32(1):33–36.

Carl Hammer. 1970. Signature simulation and certain cryptographic codes. *Third Annual Simulation Symposium*.

Louis Kruh. 1982. A basic probe of the beale cipher as a bamboozlement. *Cryptologia*, 6(4):378–382.

Louis Kruh. 1988. The beale cipher as a bamboozlement - part ii. *Cryptologia*, 12(4):241–246.

Todd D. Mateer. 2013. Cryptanalysis of beale cipher number two. *Cryptologia*, 37(3):215–232.

Mark J. Nigrini. 1999. I've got your number. *Journal of Accountancy*, 187(5):79 – 84.

W. A. Wagenaar. 1972. Generation of random sequences by human subject: A critical survey of literature. *Psychological Bulletin*, 77(1):65–72.

James B. Ward. 1885. *The Beale Papers Containing Authentic Statements Regarding the Treasure Buried in 1819 and 1821 near Bufords in Bedford County, Virginia.*