A Brief Guide to the Authentication of Cryptanalytic Claims

Richard B. Shapiro
Independent scholar
Massachusetts, USA
Rick@Rickshapiro.com

Abstract

Information theory provides powerful tools for the analysis of cryptographic systems. These tools may be used to discredit pseudo-cryptographic claims, validate legitimate claims, and assess whether a ciphertext is likely to be decipherable. Although information theory can be found in most cryptology textbooks, what is often lacking is practical guidance that addresses different types of classical cipher systems. This article presents information theory with a minimum of technical details, focusing on a few powerful concepts and several basic formulae. It demonstrates how to test various types of cryptographic systems. Of special concern is the difficulty of authenticating short ciphertexts. It proposes further work that would aid in the authentication of historical ciphers.

1 Introduction

How does one know that a cryptanalytic solution is valid? Might another key have produced a different message? This uncertainty most frequently arises when the ciphertext is relatively short. Fortunately, quantitative tests are available that can authenticate cryptanalytic solutions. They also provide an effective means to discredit pseudo-cryptographic claims.

This article has two principal arguments. The first is that pseudo-cryptography can be most persuasively discredited using quantitative methods rather than qualitative arguments. Typically, pseudo-cryptographic claims are repudiated by pointing to the overly free rules used in the deciphering process. While this may suffice, qualitative arguments may strike claimants as subjective and unfair. A more effective attack against such claims is achieved by demanding that claimants meet an objective standard based on quantitative measurement. Claims that do not meet this standard could then be treated as lacking authentication. However, as explained in Section 10, there are some mitigating factors. But for those claims that employ overly free methods (pseudo-cryptography), failed authentication should be treated as invalidating the claim.

Is pseudo-cryptography really a serious problem? Unfortunately, pseudo-cryptographic claims frequently arise in the popular press (Schmeh, 2012), and on some occasions have appeared in peer-reviewed publications (see Section 2). The danger posed by unchallenged pseudo-cryptography is that non-cryptologists might come to believe that the field lacks rigor, leading to legitimate cryptographic claims being questioned.

My second argument is that the quantitative analysis of legitimate cryptanalytic claims on a routine basis would be beneficial. True, the validity of many cryptanalytic solutions is abundantly clear and therefore formal validation may be unnecessary. But the validity of the decryption of shorter ciphertexts is often uncertain. As James Reeds (1977) explains, there may be "several completely different meaningful plaintexts which, when enciphered by completely different keys, result in the same cipher text." Examples of short ciphertexts include encrypted marginalia, alchemical formulae, and shorter messages such as the Zodiac Killer's Z340 ciphertext. A further benefit of quantitative analysis is that it can be used to estimate whether an unbroken ciphertext can be deciphered.

This article builds upon Benedek Láng's (2025) typology of pseudo-cryptology. He observes that some cryptographic methods are more susceptible

to pseudo-cryptographic claims, and he therefore examines claims based on the type of cryptographic system. This article extends his conceptual framework by demonstrating how quantitative authentication methods can be applied to several types of cryptographic systems. Further work is required to extend this conceptual framework to other types of cryptographic systems (for example, transposition ciphers).

Section 2 examines the most common form of pseudo-cryptography, para-steganography, which typically employs excessively free methods. Section 3 provides a brief introduction to information theory. Section 4 describes how cryptographic solutions are authenticated, and how that process can often be reduced to relatively simple arithmetic formulae. Sections 5, 6, 7, and 8 discuss the authentication of several types of cryptographic systems: "ad hoc steganography," simple monoalphabetic ciphers, polyalphabetic ciphers, and homophonic ciphers, respectively. Section 9 argues that the authentication process appropriately follows Bayesian probability principles, eschewing the frequentist probability approach. Section 10 identifies opportunities for further work and argues for a wider use of information theory.

2 Para-steganography

Cryptologists have on many occasions disputed pseudo-cryptographic claims. William and Elizebeth Friedman (1958) demonstrated that many so-called "Shakespearean ciphers" are without merit. More recently, Klaus Schmeh (2012) produced a broad survey of dubious cryptographic claims. Benedek Láng (2025) characterizes various types of pseudo-cryptographic claims. In their critiques, these cryptologists most frequently encounter a loosely regulated form of steganography. Schmeh coined the term "para-steganography" to describe the unsystematic, or barely systematic, use of steganography. For example, letters may be arbitrarily extracted from a text and rearranged to produce a "deciphered" message. The practitioners often misleadingly refer to this as "anagramming." Anagrams are more properly defined as rearrangements of short sequences of characters. In para-steganography, far greater liberties are often taken.

In a book on Shakespeare's *Sonnets*, Harvard professor Elaine Scarry (2016) asserts that Shakespeare and another sonneteer, Henry Constable, were lovers and that they embedded each other's name in their sonnet sequences. Her three-step procedure begins with her (mostly) arbitrary selection of one line of poetry from among many. In one case, she selects the line, "MY L**OV**E M**Y** T**R**UET**H** A**N**D **BL**A**C**K DISDAI**N**D **ESTA**TE." She then arbitrarily chooses certain letters in the line, shown in bold. Finally, she "anagrams" (i.e., rearranges) the letters to spell "HENRY CONSTABLE."

Of course, this practice allows far too many degrees of freedom; indeed, almost any plaintext can be extracted. Although deeply flawed, such practices have nonetheless appeared in the work of some fine scholars. A good example is a claim made by R. L. Winnick (2009), published by one of the world's leading academic presses. He argues that the name WRIOTHESLEY (Henry Wriothesley, the third Earl of Southampton) is steganographically embedded in Shakespeare's *Sonnets*. Wriothesley was the dedicatee of two of Shakespeare's poetry books and some scholars believe that he may be the young man to whom Shakespeare dedicated his *Sonnets*.

Winnick claims that it is significant that each of the letters needed to form WRIOTHESLEY appears twice in three of work's lines: a "double WRIOTHESLEY." However, the *Sonnets* has over 2100 lines, and if one calculates the probability of this occurring by chance, the calculated incidence is close to the actual incidence of three lines.[1] An alternative quantitative test is to determine the incidence of a double WRIOTHESLEY in an independent sample set of sonnet poetry not written by Shakespeare. Indeed, Winnick performed this test and found that the incidence of double WRIOTHESLEY lines was about the same as that found in Shakespeare's *Sonnets*. Thus, ironically, Winnick offers conclusive evidence against his own thesis. Indeed, this raises an essential point: when evaluating a para-steganographic claim, if one cannot show statistical significance, it is very likely inauthentic. Indeed, another plaintext may be extracted with an equal claim to validity.

Nevertheless, Winnick, undeterred, persists in his claim. He admits that it "cannot be proven by statistical means" but then offers two defenses.

[1]This can be calculated by determining the probability that any given poetry line contains two sets of WRIOTHESLEY letters out of the approximately 45 letters in each line.

First, he asserts that cryptographic claims should be understood as similar to qualitative literary judgments, such as recognizing symbols or discerning the meaning of polysemous words. This reveals the problem at the core of pseudo-cryptography: the failure to recognize cryptology as a scientific discipline.

In his second defense against the negative results of his own statistical analysis, Winnick offers what I would characterize as "special pleadings." He argues that in those lines in which WRIOTHESLEY appears, the letters are bunched closely together within the poetic lines. He also argues that the three lines that contain a double WRIOTHESLEY are of special poetic significance. In my view, these arguments, made ex post facto of his "discovery," must be seen as rationalizations. Such explanations are almost always available because some detail or artifact can always be judged to be significant.

Winnick is not the only literary critic to engage in anagrammatic speculations. Martin Dodsworth (2017) notes that eminent scholars Alastair Fowler, Helen Vendler, and Christopher Ricks have published similar claims with respect to Shakespeare's *Sonnets*. What motivates these specious claims? The *Sonnets* promises that its subject, an unnamed young man, will enjoy renown in the future, and this suggests to some that the text might by some means hide his identity. Of course, this is no excuse to practice pseudo-cryptography. Indeed, early modern English poets were wary of pseudo-cryptographic practices because they understood the limitations of anagrams. According to Dodsworth, the English only used anagrams as a parlor game.

I have considered Winnick's claim at length because its methods and logic are representative of pseudo-cryptographic claims. Indeed, his example can guide us in formulating a set of rules for evaluating and discrediting such claims. First, all claims must be subjected to quantitative testing. This may be accomplished by either (1) comparison to incidence rates in other texts, (2) a probability calculation, or (3) information theory tests as described in Section 4. Second, failed quantitative analysis cannot be justified by special pleadings because it is almost always possible to find some rationale for a desired result.

3 Information as entropy

This section provides a brief overview of some essential concepts in information theory, and a few basic arithmetic formulae needed for authenticating cryptographic solutions. Claude Shannon developed a revolutionary theory of information in the 1940s and applied it to cryptology. His theory is frequently employed by computer scientists, especially in the field of data compression. Yet it is less frequently employed by practitioners of historical cryptography.

Shannon's (1948) revolutionary insight was to use entropy to measure the amount of information in a text. Entropy is a measure of the order (or disorder) of a system. Shannon's measurement of information uses the same statistical mathematics as the measurement of thermodynamic entropy in physical systems (as described by Boltzmann). As is practiced in thermodynamics, Shannon measures information logarithmically.

Shannon also recognized that natural languages contain redundant information. For example, if every other letter of a text is missing, one can often guess the value of the missing letters. Redundancy is also apparent when we make use of the type-ahead feature while texting. Of course, this is fundamental to cryptanalysis, for without redundancy, cryptanalysis is impossible. Also, redundancy is what makes natural languages compressible. If a language is reduced to its most theoretically compressed state (a practical impossibility), we have what might be called "pure information," but is properly referred to as entropy. The difference between this pure information and the language's normal appearance is called "redundancy."

One of Shannon's (1951) contributions was to measure the redundancy of the English language. Figure 1 provides a schematic view of Shannon's conception of the order (or entropy) found in the English language. He envisioned a series of steps by which a sequence of letters that exhibits no apparent order progressively approaches a grammatically correct English sentence. The labels inside the trapezoid figure describe the level to which an English text is approximated; the messages to the right of the trapezoid are sample texts for each level of approximation.

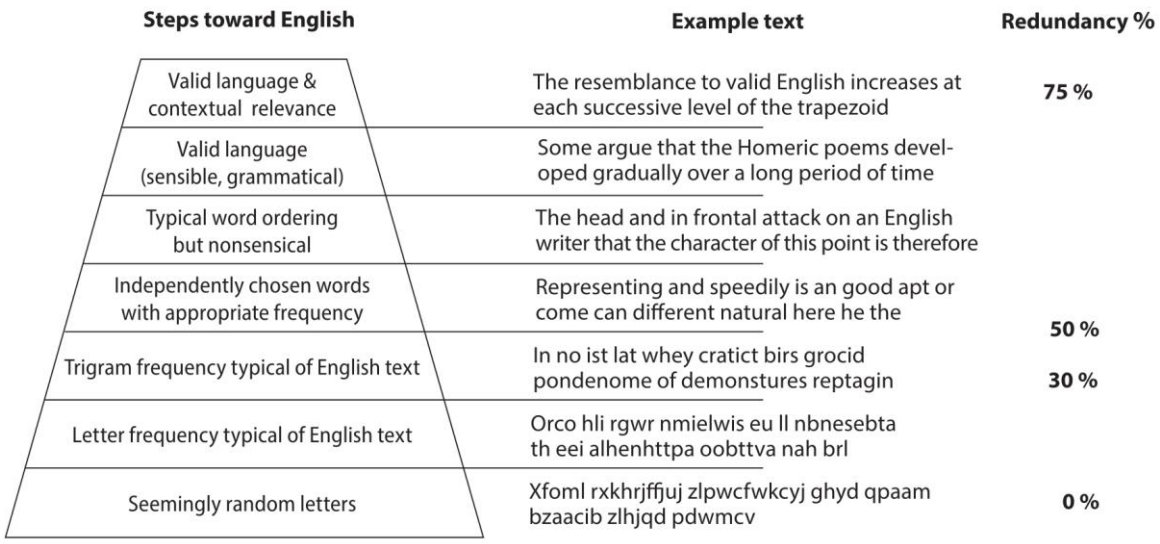

Fig. 1 Shannon Information: Successive approximations to English

At the lowest level of the trapezoid, the sequence of letters shows no apparent pattern. Such a sequence, seemingly random, cannot be significantly compressed—it approaches perfect concision and thus consists of 100% information with no redundancy. At the next level up, Shannon's first step toward English, the letters have no meaningful order but duplicate the individual letter frequencies of English.

At the third level, Shannon increased his approximation to English by duplicating trigram frequencies. The redundancy for trigrams in English is about 30%. Shannon then extrapolated from trigrams to 8-grams and reports a redundancy of about 50%.[2] This is marked at just above the trapezoid's third level.

At the fourth level, only sequences of letters that are valid English words are included, but the words lack any meaningful order. The fifth level improves the resemblance to English by mimicking English word order, but the text is still nonsensical. Not until the sixth level do we have a meaningful and grammatical English sentence. In climbing up each level of the trapezoid, the number of qualifying texts is diminished exponentially. At the sixth level, only an extremely small number of the sequences of unordered letters from the lowest level qualify as valid English.

The seventh and top level of trapezoid adds a further important qualification: contextual relevance. The sample text at the sixth level is grammatical and sensible English but it concerns the origin of the Homeric poems, a matter irrelevant to cryptology. In contrast, the sample text at the seventh level is descriptive of Figure 1 itself. This is an important distinction because when a cryptogram is deciphered, one expects the deciphered text to have some contextual relevance. Indeed, the cryptanalytic process often involves a crib which is guessed based on context.

To quantify information, we first ask how many bits are required to specify each English character. Five bits can specify a 32-letter alphabet ($2^5 = 32$); for a 26-letter alphabet we calculate $\log_2 26 \approx 4.7$ bits. This is known as "the absolute rate of language."

Shannon conducted a set of experiments in which people guessed at the letters of a text. He estimated the redundancy of English to be between 1.3 and 0.6 bits per character, out of the 4.7 bits, the absolute rate of language. This corresponds to a redundancy of 72% and 87%, respectively.[3] Others have measured it between 77% and 86% (Levitin, 721). Throughout this article, a value of 75% is applied, which falls at the conservative end of the range. Most other European languages have similar redundancy levels.

4 The authentication of cryptanalysis

We now have an estimate that English is 75% redundant and that the remaining 25% is a theoretical compression of English to its ultimate level of concision. This allows us to answer the following useful question: for an English text of n characters, how many valid and contextually

[2]See Shannon (1949, page 700).

[3]Shannon (1951, page 64).

relevant texts are there? This will allow us to calculate the probability that a plaintext arises by chance when attempting to guess at a key.

If English is 75% redundant, then for each character in English, the redundant amount is 75% of 4.7 or 3.53 bits per character. The remaining part, the information in its most concise form, is 1.17 bits per character. We now have an estimate of the number of valid and relevant English texts for a plaintext that is n characters long: $2^{1.17n}$ (exponentiation inverts the log function).[4] For a 25-letter plaintext, this is equal to approximately 760 million possible texts.

We now ask the following question: for what length message are we most likely to find that a single spurious solution arises by chance? This is known as the "unicity distance." Calculating the unicity distance provides a means to authenticate a cryptanalytic claim. If the length of the cryptogram is significantly greater than the unicity distance, then the chance of a spurious solution is slight. Shannon (1949) was the first to calculate unicity distances. The unicity distance (U) is defined by the following formula:[5]

$$U = H(K) / R \qquad \text{Formula 1}$$

"H" denotes entropy and H(K) is the entropy of the key, known as "key equivocation" or "key space." A spurious decryption could arise from any key value, and key equivocation is a measure of all possible keys that could be applied. "R" is the plaintext redundancy measured in bits per character. For English, this is the estimate of 3.53 bits per character given above. The result, U, is the number of characters in the unicity distance.

Formula 1, in effect, finds the entropy balance point between the redundant component of the message ($R \cdot U$) and the key equivocation, H(K). Unless the message redundancy is larger than the key equivocation, a spurious key may decipher to what appears to be a valid plaintext.

To demonstrate the use of Formula 1, we take as an example a simple substitution cipher. In this cipher, the key is ideally a random mapping of each of the 26 letters in the English alphabet to another one of those 26 letters. We begin by calculating the entropy of the key space or key equivocation. Assuming the key is a random sequence of the 26 letters of the alphabet, with each letter appearing just once, the number of permutations is 26 factorial.[6] The information content or entropy of the number of the keys is calculated using base 2 logarithms:

$$H(K) = \log_2 26! \approx 88.4$$

Using Formula 1, we now calculate the unicity distance:

$$U = H(K) / R$$
$$\approx 88.4 / 3.53 \approx 25$$

A simple substitution cipher of 25 characters is most likely to have a single spurious solution. To validate a cryptanalytic solution, the number of characters must be greater than 25 characters. How much greater? Reeds (1977) provides a formula which promises that there will be no spurious solution, at a 99.8% confidence rate.[7] Formula 2, which Reeds derived, is used along with the values discussed above, to calculate what I call the "authentication distance" (AD) for a simple substitution cipher:

$$AD = H(K) / R + 20/R \qquad \text{Formula 2}$$
$$\approx 25 + 20 / 3.53$$
$$\approx 30.7$$

The approximately 31 characters represent an increase of about 25% above the unicity distance. Yet is Formula 2 conservative enough—one that would be appropriate to use as a standard for authentication among cryptologists? One might argue for a higher threshold, say, 50% above the unicity distance, rather than 25%. This additional length is intended to account for inaccuracies in estimating the redundancy of language and some biases found in language that our model cannot fully capture.[8] An appropriate threshold to use for authentication purposes is worthy of further investigation.

The concept of unicity distance was extended by both Reeds and Deavours to aid in the determination of whether a cipher is likely to be breakable. Suppose a cryptanalyst intends to crack a cipher using bigram or trigram frequencies, then

[4]See Deavours (1977, page 47), who presents a similar value using base 10 logarithms and exponentiation.

[5]For further explanation, see: Lasry (2018, page 35); Reeds (1977, page 235); or Deavours (1977, page 46).

[6]If the key is randomly selected, then all elements of the key are equiprobable. If the key is not randomly selected, then one must calculate key entropy on a weighted basis.

[7]That is, three standard deviations. Reeds (1977, page 238).

[8]Reeds models variations in language redundancy using a Poisson distribution. But actual redundancy, if measured empirically, might vary somewhat from his model.

one can use a different value for language redundancy based solely on bigram and trigram frequencies. Figure 1 shows that the redundancy is approximately 30% for trigrams. The redundancy per bit is then 30% of 4.7 or 1.41 bits per character. Using Formula 1 with this new value of R (instead of 3.53), we now calculate a "breakable distance" of 63 characters.[9]

The calculations of unicity and breakable distances are not hard limits—one may sometimes be able to crack a cipher that falls below the unicity distance. For example, suppose one has a strong reason to believe that a crib is present such as the name of an encrypted message's addressee. This might significantly reduce the effective key equivocation, allowing the cipher to be broken.

Unicity distance is not the only way to authenticate a cryptanalytic solution. Deavours (1977) asserts that Shannon's "unicity point formula is couched in information theoretic terms but a simpler approach is possible." He then employs standard probability calculations in conjunction with his estimate for the redundancy of English. The basic principle remains the same whether one uses Shannon's formula or probability calculations. The basic parameters are key equivocation, the number of potentially valid plaintexts, and the number of all possible plaintexts, valid or not. These three values determine the probability that a spurious decryption will arise. In the examples presented below, the authentication method chosen is the one most appropriate to the circumstances.

5 Ad hoc steganography

Section 2 discussed para-steganography, the loosely regulated selection of letters to form a plaintext. An effective way to discredit these bogus claims is to demand that the claimant provide a calculation of the key equivocation. In the case of Winnick's claim, equivocation occurs at three levels: selection of lines, selection of letters within lines, and the "anagrammatic" rearrangement of those letters. The key equivocation is so large that authentication convincingly fails.[10]

Nevertheless, some unorthodox steganographic practices may be valid—what might be called "ad hoc steganography." Rather than a steganographic system such as a Cardan grille, a short message may be opportunistically embedded. For example, poets have occasionally placed their names in the acrostic of a poem. An interesting case is that of a late sixteenth-century dialogue on love, *Contramours*, published under the pseudonym Battista Fregoso. The acrostic in a fourteen-line prefatory poem spells out THOMAS SEBILLET. It is only through this use of steganography that scholars have been able to identify the author. We can authenticate this by calculating what is essentially the key equivocation of the steganographic claim. If the volume has five prefatory poems (the likely place for a poet's hidden name), and either an acrostic or telestich is acceptable, then the key equivocation is 5 times 2 or 10, an extremely low value. Obviously, the probability of a spurious appearance of the name of a potential poet in one of these 10 locations is very remote.

Suppose we were to expand our steganographic search to include a fixed character count inward, say, from 1 to 10 characters from the poem's acrostic on each poetic line. In that case, the key space would still be relatively small. But if we were to allow the inward character count to be arbitrary and independent for each line, the key space would expand to 10^{14} (10 possible positions for each of 14 lines). This high value for key equivocation would discredit any claim that a putative plaintext is valid.

My goal here is to avoid the categorical rejection of every ad hoc or para-steganographic claim. This would likely strike claimants as arbitrary and unfair. Instead, the cryptologist critiquing such claims should demand that the claimant provide a quantitative analysis. The claimant's most essential task is to calculate what is effectively the key equivocation. This calculation must carefully consider every arbitrary path taken to produce the putative plaintext, which in the vast majority of cases will lead to an authentication failure.

Under this standard, might it sometimes be possible to validate an anagram that hides an author's name? François Rabelais published *Pantagruel* under the pseudonym Alcofribas Nasier, which is an anagram of his name (ignoring the cedilla). Rabelais' authorship is certain from historical evidence, but what if it were not?

We will attempt to validate the anagram using a probability calculation. We must calculate key equivocation, the number of all possible plaintexts, valid or not, and the number of

[9]This is close to Deavours' (1977) estimate of 55. The difference is due to different redundancy estimates.

[10]This lengthy calculation cannot be included here.

potentially valid plaintexts. First, we calculate the key equivocation of an anagram, which is the number of permutations of its letters, that is, all possible transformations. We must be careful to account for duplicate letters in the anagram (A, I, R, and S). The number of permutations is 16! / (3! $\cdot$ 2 $\cdot$ 2 $\cdot$ 2) $\approx 4.4 \cdot 10^9$.

Next, we calculate the number of meaningless (or not) plaintext messages. This is similar to the absolute rate of language; however, we must account for the fact that an anagram's letters are not random but adhere to the frequencies of letters in the 23-letter Middle French alphabet. This consideration is often missed by pseudo-cryptographers when they provide probability calculations. This reduces the effective alphabet size to perhaps 15 from 23 letters (i.e., the alphabet could theoretically be encoded using 15 equiprobable letters). Then the number of possible plaintexts, sensible or not, is 15^{16}, equal to approximately $6.6 \cdot 10^{18}$.

Next, we calculate the number of meaningful plaintexts. Suppose that scholars judged that only 10 writers in France potentially had the skill to write this brilliant novel. Then 10 is arguably the number of valid plaintext messages.

What is the probability of hitting upon one of these 10 valid plaintexts for any given key? It is 10 out of $6.6 \cdot 10^{18}$, or 1 out of $6.6 \cdot 10^{17}$. But we have $4.4 \cdot 10^9$ chances (the number of keys) to hit on one of these 10 valid plaintexts. The probability of a spurious anagrammatic deciphering is then the division of these two numbers, which is 1 out of $1.5 \cdot 10^8$. As a result, we can be relatively certain that the anagram is intended to be deciphered to François Rabelais.

However, there is unobvious error in my logic. Perhaps Alcofribas Nasier is merely a pseudonym and not an anagram of anyone's name. This possibility should be factored in. But even if we estimate that there is merely a 1 out of 100 chance that the author decided to anagram his true name, the authentication probability is still strong: 1 in $1.5 \cdot 10^6$. It is essential when calculating probabilities to carefully factor in all assumptions (see Section 9 on Bayesian priors).

This example illustrates that in rare cases ad hoc steganography can be valid. But this is only true if one places a restriction—a special case assumption—on what constitutes a valid plaintext. Alternatively, a severely restricted key space might allow authentication. Any claimant must carefully state all assumptions and then perform a valid probability calculation.

Dodsworth (2017) finds some evidence of the practice of hiding information in anagrams among the French (in contrast to the English).

6 Simple monoalphabetic ciphers

Is it possible to authenticate a monoalphabetic cipher of only 8 characters? If the key is short enough, then it may be, though with some uncertainty.

An enciphered marginal note appears in an early edition of Edmund Spenser's *Faerie Queene*. The note, likely written in 1597, is of interest because scholars would like to understand how a poet's contemporaries read and interpreted the poet's work (Hough, 1964). Some modern scholars believe that various characters in Spenser's fictional poem are intended to allegorically represent historical individuals. They wish to know whether Spenser's contemporaries also read in an allegorical manner.

The ciphertext of the marginal note is given below (it employs the 24-letter Elizabethan alphabet). If a Caesar shift of 12 is applied to the ciphertext (either up or down), the following plaintext is produced:

Ciphertext: YB: YRFGRE
Plaintext: LO: LESTER (Lord: Lester)

LO is an abbreviation for "Lord" and LESTER is an alternative spelling of Leicester (spelling was not standardized). Lord Leicester, Robert Dudley, was an intimate friend of Queen Elizabeth and an influential statesman. The marginal note appears next to the third line of Spenser's epic poem, which introduces the Redcross knight. Modern scholars do not necessarily identify the Redcross knight with Leicester, but apparently this early modern reader did.

Should we trust this decryption? If this were a substitution cipher, the key equivocation would be too large to allow any cryptanalysis. But as the key equivocation of a Caesar shift is extremely small (24 possibilities), a good case can be made for this decryption's authenticity. We can test that none of the other 23 Caesar shifts produce anything intelligible, but can the plaintext be quantitively authenticated? Formula 1 gives a unicity distance of about 1.3, but our measurement of the redundancy of English is not necessarily reliable for such an extremely short text.

First, we calculate key equivocation, which is simply 24, the number of Caesar shifts. Next, we calculate the absolute rate of language, which is

the number of all possible sequences of 8 letters in a 24-letter alphabet, which is equal to $24^8 \approx 110$ billion. Now we must estimate the number of valid and relevant plaintexts. Due to the extreme shortness of the message, we cannot rely on language redundancy calculations. We might choose a conservative number based on the number of 8-letter words in English, which is perhaps 10,000. This is conservative because the plaintext is a gloss on a poetic line, which sharply restricts the range of potential plaintexts.

Our probability calculation is straightforward. The chance that any given key produces a plaintext is 10,000 out of 110 billion or 1 out of 11 million. For any of the 24 keys, the chance of a spurious decryption is 24 times greater, which is 1 out of 458,000. We can be almost certain that our decryption is not spurious, even though the plaintext is only 8 characters in length.

7 Polyalphabetic ciphers

In polyalphabetic ciphers, a key is chosen and then applied successively to each letter in the plaintext to encipher it. The key is a fixed length and then used repetitively until the message is fully enciphered. Suppose the key length is 16 and each element of the key is a number from 1 to 26, chosen randomly and applied as an arithmetic shift. Suppose that we apply it to a short message of only 16 characters. This is called perfect secrecy (or a one-time pad), and no cryptanalysis is possible because the redundancy of language is entirely hidden.

We now consider a message of 21 characters, which makes a second use of the first 5 characters of the key. Can a cryptanalytic solution be authenticated?

We first calculate the entropy of the key, each element of which is a number from 1 to 26:

$$H(K) = \log_2 26^{16} \approx 75.2.$$

We next use Formula 1 to calculate the unicity distance:

$$U = H(K) / R \approx 75.2 / 3.53 \approx 21.3$$

The ciphertext length (21) is almost the same as the unicity distance (21.3) and thus authentication fails.

We next consider the case of a Vigenère polyalphabetic cipher, which employs an easy-to-remember key phrase instead of a key with randomly selected numbers. Suppose our plaintext message is HE DISCOVERED LOGARITHMS (length: 22) and our key is NAPIER WAS CUNNING (length: 16). Now we must recalculate the entropy of the key differently because it is no longer a random sequence of numbers. Further, it is contextually relevant to the plaintext: John Napier discovered logarithms.

How do we estimate the entropy of a memorable phrase key? That is, how many possible memorable phrases might be specified by the 16-character key? In Section 4, we posed the same question for plaintext possibilities, and our answer was given by calculating the pure information content of the plaintext: $2^{1.17n}$, where n is the number of characters. For n = 16, the value is $2^{18.7}$ (approximately 426,000). The entropy of the key, H(K), is $\log_2 2^{18.7} = 18.7$. Now that we have the key entropy, we can calculate the unicity distance:

$$U = H(K) / R \approx 18.7 / 3.53 \approx 5.3$$

In the case of the memorable phrase, the unicity distance drops from 21.3 to 5.3. Our ciphertext length of 22 is about four times larger than the unicity distance and thus the cryptanalytic result is easily past the authentication threshold. This demonstrates that polyalphabetic ciphers have a weakness. If a crib is successfully guessed, and crib sliding is attempted, the memorable phrase key may appear. If instead the key had consisted of randomly selected numbers, the cipher would have been far better protected.

It should be noted that the calculation of the entropy of the 16-character key is somewhat uncertain as the redundancy of English may be overstated at short lengths. According to Deavours (1977), the redundancy level of 75% for English is only reached at 20 characters or more. However, as the key includes NAPIER, it is strongly linked to the plaintext, and this compensates for the key being slightly shorter than 20 characters.

8 Homophonic ciphers

Homophonic ciphers improve security by assigning multiple cipher symbols to the same plaintext letter to defend against frequency counting attacks. We consider a system with n symbols and a 26-letter plaintext alphabet. If each plaintext letter is assigned to at least one ciphertext symbol (key space = 26!) and the

remaining symbols (n minus 26) are assigned to any plaintext letter (key space = 26^{n-26}), then the key equivocation is given by:[11]

$$H(K) = \log_2 (26! \cdot 26^{n-26}) \qquad \text{Formula 3}$$

However, this greatly overstates key equivocation because it includes many extremely unlikely key possibilities. For example, if each of 26 symbols is assigned to a single plaintext letter, it is extremely unlikely that every remaining symbol is assigned to a letter that seldom appears such "Z." This obviously makes no sense because symbols are assigned for the purpose of smoothing the frequency counts of cipher symbols. Thus Formula 3 overestimates the key space. An open question is whether it is possible to estimate, in a straightforward manner, the entropy of a homophonic cipher more precisely. To obtain a more realistic estimate of the key space, one must assume that the additional ciphertext symbols are primarily assigned to higher frequency letters.

I was unable to find any survey of homophonic ciphers that estimates the likely range of ciphertext symbol allocation. It appears that there is considerable variation in how symbols are allocated: in some homophonic ciphers, only vowels have additional symbols; in others, a greater range of plaintext letters is assigned to multiple symbols. A survey that examines the characteristics of the key spaces of solved historical homophonic ciphers might prove valuable. It would allow one to estimate the key space of unsolved homophonic ciphers more accurately. This would provide a better estimation of the unicity distance, and by extension, the chances that a cipher might be broken.

When authenticating a solved homophonic cipher, the key equivocation could be estimated based on the distribution of cipher symbols. Yet is it valid to assume a specific distribution given that that is the result that one is attempting to evaluate? In any case, although the unicity distance of homophonic ciphers has been addressed in some articles, additional work is required to more accurately assess key equivocation. The present alternative is to use Formula 3, even though it overestimates key equivocation.

The Z-340 (Zodiac Killer) cryptogram is a short homophonic cipher that demonstrates the potential difficulties in calculating unicity distance. It has 63 ciphertext symbols and is 340 characters long. Competing solutions to this cipher raised concerns about authentication, and particularly the challenges encountered in authenticating homophonic ciphers. Von zur Gathen (2023) begins by calculating an even higher estimate of unicity distance than that provided in Formula 3.[12] Significantly, he recognizes another set of problems in calculating unicity distance: the Z340 solution contains various anomalies, including spelling errors and poor grammar. He puts considerable effort into accounting for these anomalies, which have the effect of increasing the unicity distance. Von zur Gathen's analysis of the Z340 cipher serves as a valuable reminder that redundancy estimates assume (possibly inaccurately) that a clean plaintext is under test.

9 A Bayesian perspective

In reviewing pseudo-cryptanalytic claims, I sometimes found that the claimants offered probability calculations as part of their argument. Without exception, these probability calculations only considered the probability of the putative plaintext message (i.e., the message they hoped to find) spuriously appearing. This follows what is known as a "frequentist" probability model, rather than a Bayesian model. In Bayesian probability calculations, one considers "the priors," that is, all potential hypotheses. Rather than calculate the probability of any single hypothesis H, one must calculate the probability of all possible hypotheses, $H_1 \ldots H_n$. In the context of crypt-analytic validation, $H_1 \ldots H_n$ are all potential cryptanalytic solutions.

In authenticating a cryptanalytic solution, one should consider not only the plaintext message being tested but all valid plaintext messages. Shannon's authentication process is inherently Bayesian because his calculations factor in all potential plaintexts (see the second paragraph of Section 4). These potentially valid plaintexts are essentially Bayesian priors, hypotheses $H_1 \ldots H_n$.

Pseudo-cryptographers invariably calculate based on a frequentist model of probability, which poisons the calculation with circular reasoning. Instead, any authentication method must consider a full range of potential plaintext solutions. This is illustrated by the claims that discover that WRIOTHESLEY is enciphered somewhere in Shakespeare's *Sonnets* (see Section 2). These claims adopt a single hypothesis to the exclusion

[11] See Dhavare et. al. (2013, page 254).

[12] His formula is $H(K) = \log_2 26^{63}$.

of all other possible encrypted names. Shakespeare could have enciphered any one of a hundred other names into his *Sonnets* (or no name at all). When performing quantitative authentication tests, one must either use Shannon's methods, which are inherently Bayesian, or if calculating probabilities, factor in all valid potential plaintexts in one's calculation.

10 Conclusions and future work

Shannon information is a powerful tool that could be applied more widely in the study of historical cryptography. Many fields set a numerical standard for the validity of results. For example, medical research sets "$p < .05$" as the threshold for statistical significance. Might cryptologists set a standard threshold for authentication distance at, say, 50% above the unicity distance? Probability calculations could also be assigned an authentication threshold.

These standards might serve to deter or repudiate pseudo-cryptographic claims. Even if some pseudo-cryptographers are not deterred, their claims could then be challenged for failing to authenticate against the standard.

Standards would also aid in the appraisal of legitimate claims in which the ciphertext is short. If a cryptographic claim meets the standard, it may then be presented as "authenticated." True, some cryptanalysts will not feel comfortable calculating unicity distance, but they might be encouraged to seek the help of an applied mathematician or computational linguist.

Claims that fail authentication are uncertain rather than necessarily false. This is especially true when historical or literary context is present, as this cannot be captured in a mathematical model.

The calculation of the unicity distance of homophonic ciphers would benefit from further research. Knowing the most common mapping patterns of ciphertext symbols to plaintext letters might prove valuable for cryptanalysts.

A generally available tool for the calculation of unicity, authentication, and breakable distances might aid in the evaluation of unsolved ciphers. It would provide some indication of the cipher's difficulty. Perhaps these functions could be integrated into CrypTool (a widely used deciphering tool), or an independent tool could be built reasonably quickly using AI.

Shannon's extraordinary contribution to the field continues to pay dividends eighty years on.

References

Cipher A. Deavours. 1977. Unicity points in cryptanalysis. *Cryptologia*, 1(1):46–68.

A. Dhavare, R. M. Low, and M. Stamp. 2013. Efficient cryptanalysis of homophonic substitution ciphers. *Cryptologia*, 37(3):250–281.

Martin Dodsworth. 2017. The Elizabethan anagram and Shakespeare's sonnets. *The Review of English Studies*, 68(286):666–688.

William F. Friedman & Elizebeth Friedman. 1958. *The Shakespearean ciphers examined: An analysis of cryptographic systems used as evidence that some author other than William Shakespeare wrote the plays commonly attributed to him*. Cambridge University Press, New York.

Graham Hough. 1964. *The First Commentary on the Faerie Queene.* Privately published. Pages 1–2.

Benedek Láng. 2025. A Typology of Pseudo-Cryptology. In *Proceedings of the 8th International Conference on Historical Cryptology, HistoCrypt 2025*, pages 90–100. Linköping University Electronic Press.

George Lasry. 2018. *A methodology for the cryptanalysis of classical ciphers with search metaheuristics*. Kassel University Press, Kassel, Germany. Pages 35, 37–38.

L. B. Levitin and Z. Reingold. 1994. Entropy of natural languages: Theory and experiment. *Chaos, Solitons & Fractals*, 4(5):709–743. Page 721.

James Reeds. 1977. Entropy Calculations and Particular Methods of Cryptanalysis, *Cryptologia*, 1(3):235–254. Page 235.

Elaine Scarry. 2016. *Naming thy name: Cross talk in Shakespeare's sonnets*. Farrar, Straus, and Giroux, New York. Page 20.

Klaus Schmeh. 2012. The Pathology of Cryptology — A Current Survey. *Cryptologia*, 36(1):14–45.

Claude Shannon. 1948. A Mathematical Theory of Communication. *Bell system technical journal* 27(3):379–423.

Claude Shannon. 1949. Communication Theory of Secrecy Systems. *Bell system technical journal*, 28(4):656–715.

Claude Shannon. 1951. Prediction and Entropy of Printed English. *Bell system technical journal*, 30(1):50–64.

J. von zur Gathen. 2023. Unicity distance of the Zodiac-340 cipher. *Cryptologia*, 47(5):474-488.

R. H. Winnick. 2009. "Loe, here in one line is his name twice writ": Anagrams, Shakespeare's Sonnets, and

the Identity of the Fair Friend. *Literary Imagination*, 11(3):254–277. Page 257.