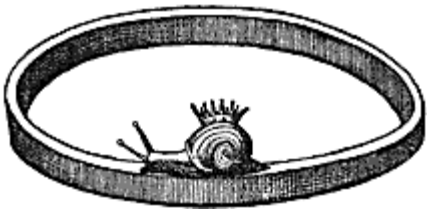


# Early Cryptology

AN accurate assessment of a proposed cryptogram in the work of "Shake-speare" can only take place when the evidence is judged in the light of both the history and techniques of cryptology. Just as the correctness of a solution to a mathematical problem must be determined by one who is cognizant of relevant fields of mathematics, so it is necessary to cast a question of cryptologic validity into appropriate contextual relief. While a complete treatment of the history and methods of cryptology is to be preferred to the brief outline given here, it is hoped that a short review of pertinent information will help provide a sufficient basis for appraising the *Sonnets* cryptogram solution demonstrated elsewhere.

Cryptography has been in practical use for a very long time. While it may well have been used previously, extant records indicate that the Spartans

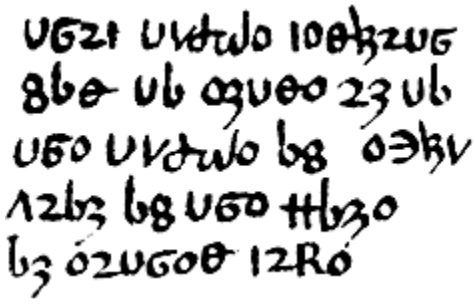
> established the first system of military cryptography. As early as the fifth century B.C., they employed a device called the 'skytale' [which] consists of a staff of wood around which a strip of papyrus or leather or parchment is wrapped close-packed. The secret message is written on the parchment down the length of the staff; the parchment is then unwound and sent on its way (@ Kahn 82).

Not content with what Francis Bacon called the "cypher'd staffe" method, Julius Caesar invented the first substitution cipher, which bears his name to this day. The substitution key is formed by cyclically displacing an alphabet with respect to itself. A message, called "plaintext", is enciphered by substituting for each letter the corresponding letter from the shifted alphabet. The substitution produces a new string of letters called "ciphertext". A cryptogram enciphered in this way can be deciphered by reversing the process and translating each ciphertext letter into its plaintext equivalent. An example of a 21 letter alphabet key for a 4 letter shift Caesar cipher is shown below. This is the key used to solve the acrostic cryptogram found in the *Sonnets* frontmatter.

| A | B | C | D | E | F | G | H | I | K | L | M | N | O | P | Q | R | S | T | V | Y |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| s | t | v | y | a | b | c | d | e | f | g | h | i | k | l | m | n | o | p | q | r |

Throughout the Middle Ages, ciphers were used by monks "for scribal amusement, and the Renaissance knew from its study of such classic texts as Suetonius that the ancient world had used ciphers for political purposes" (@ Kahn 106). Around the middle of the 13th century, the English monk Roger Bacon wrote "Concerning the Marvelous Power of Art and of Nature and Concerning the Nullity of Magic". He listed seven cipher methods and asserted that "a man is crazy who writes a secret in any other way than one which will conceal it from the vulgar" (@ Davis).

Geoffrey Chaucer is considered "the outstanding English poet before Shakespeare and 'the first finder of our language' " (@ *Britannica* 3: 141). In *The Equatorie of the Planetis,* a supplement to his 1391 *Treatise on the Astrolabe,* Chaucer included six passages written in cipher. The cipher system consists of a substitution alphabet of symbols. The solution to the cryptogram shown below is: "This table servith for to entre in to the table of equacion of the mone on either side."

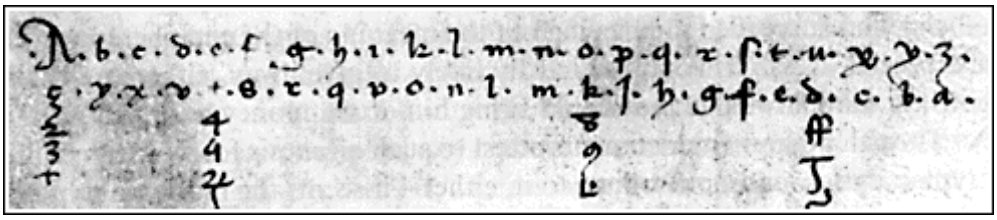


The first European manual on cryptography, a collection of Gabriele de Lavinde's ciphers, was produced in 1379. The nomenclator system described therein "was to hold sway over all Europe and America for the next 450 years.... [It] united the cipher substitution alphabet of letters and the code list of word, syllable, and name equivalents" (@ Kahn 107).

Simeone de Crema's work at Mantua in 1401 used a key in which

> each of the plaintext vowels [had] several possible equivalents. This testifies silently that, by this time, the West knew cryptanalysis. There can be no other explanation for the appearance of these multiple substitutes, or homophones. ... That the homophones were applied to vowels, and not just indiscriminately, indicates a knowledge of at least the outlines of frequency analysis (@ Kahn 107).

This type of cryptanalysis, which compares the relative frequency of letters in ciphertext to that generally found in regular text, allows the cryptanalist to make good guesses about letter substitution. Using frequency analysis can quickly lead to the solution of simple monoalphabetic substitution ciphers. De Crema's homophonetic substitution key is show below:



In 1474, Sicco Simonetta published *Regulae ad extrahendum litteras zifferatas sine exemplo,* a short work which stressed "methods of decipherment and afford[ed] considerable statistical data" (@ Galland 171). In the context of the present discussion, "the date of Simonetta's little essay on ciphers is important, for it was the period when cryptography became the universal practice, when simple ciphers developed into complicated cryptograms" (@ Thompson, qtd. in Galland 171). By the end of the 15th century, "cryptology had become important enough for most states to keep full-time cipher secretaries occupied in making up new keys, enciphering and deciphering messages, and solving intercepted dispatches" (@ Kahn 108-9).

The popularity of cryptology was not limited to those who used it for military and diplomatic intelligence. The increasing popularity of cryptology in the 16th and 17th centuries is clearly attested to by the proliferation of books on the subject. So much was published that Duke August of Brunswick, author of the encyclopedic *Cryptomenytices et Cryptographiae Libri IX,* "had managed by 1622 to accumulate and analyze almost two hundred books on the subject of cryptology" (@ Strasser 51). In the preface of *Cryptomenytices,* he listed 187 authors of cryptographic works (45).

The claim of a steganographically concealed cryptogram in the *Sonnets* frontmatter must be viewed and judged in the context of the popularity and availability of cryptographic information prior to the publication of the *Sonnets*. **Many books on cryptography were published prior to the 1609**

**first edition of *Shake-speares Sonnets.*** A few of the more popular and important cryptographic works are listed below (indicating only dates prior to 1609):

**1470** Leone Battista Alberti's *Trattati in cifra* was published in Rome. Alberti dealt "especially with theories and processes of cipherment, methods of decipherment, and statistical data" (@ Galland 3).

**1518** Johannis Trithemius wrote (but did not publish) his *Steganographia,* which "circulated in manuscript for a hundred years, being copied by many persons eager to suck out the secrets that it was thought to hold" (@ Kahn 132).

**1518** Trithemius' *Polygraphiae libri sex*, which included his *tabula recta* Caesar substitution tableau, was published (though there is some disagreement on the first edition date [Galland 183]). It was reprinted in 1550, '64, '71, and 1600; a French translation appeared in 1561 and '64.

**1526** Jacopo Silvestri's *Opus novum ... principibus maxime vtilissimum pro cipharis* was published. The work discussed six cipher methods, including the Caesar cipher, for which he recommended the use of a cipher disc. *Opus novum* was written as a practical manual and "was clearly intended to reach a wide circle of readers" (@ Arnold 102).

**1540** Giovanni Battista Palatino published his *Libro nvova d'imparare a scrivere ... Con vn breue et vtile trattato de le cifere*. It was reprinted in 1545, '47, '48, '50, '53, '56, '61, '66, '78, and 1588. A revised version was printed in 1566, '78, and '88.

**1550** Girolamo Cardano's *De subtilitate libri XXI* was published. "This famous work of a noted mathematician, physicist and philosopher contain[ed] ... a considerable amount of information concerning processes of cipherment" (@ Galland 34). It was reprinted in 1551, '54 {x2}, '59, '60 {x2}, '80, and '82; a French translation was printed in 1556.

**1553** Giovanni Battista Bellaso's *La cifra del* was published. It "stress[ed] especially processes of cipherment" (21) and was corrected and reprinted in 1557 and 1564.

**1556** Cardano published *De rerum varietate libri XVII,* which contained cryptographic information and was a follow-up to his popular *De Subtilitate*. Both books were "translated and pirated by printers throughout Europe" (@ Kahn 144). *De rerum* was reprinted in 1557, '58, '80, and '81.

**1558** Ioan Baptista Porta's *Magiae natvralis libri XX,* in which Book XVI treats deciphering, was published. It was reprinted in 1560, '61 {x2}, '62, '64, '67, '76, '85, '91, '97, and 1607. An anonymous French translation was printed in 1565, '67, '70, '71, and '84.

**1563** Ioan Baptista Porta's *De fvrtivis literarvm notis, vvlgo de ziferis Libri IIII* was published; it appeared in the same year translated into English under the title *On secret notations for letters, commonly called ciphers*. "Its four books, dealing respectively with ancient ciphers, modern ciphers, cryptanalysis, and a list of linguistic peculiarities that will help in solution, encompassed the cryptologic knowledge of the time" (138). A working set of rococo cipher discs was packaged with it. The work was reprinted in 1591, '93, 1602 {x2}, '03, and '06.

**1586** Blaise de Vigenère's 600 page *Traicté des chiffres* was published. In it he discussed many ciphers, including the "running autokey" system (used in some modern cipher machines) and the so-called "Vigenere tableau" method. He was "scrupulous in assigning credit for material from other authors, and he quoted them accurately and with comprehension" (146).

**1591** Porta's *De fvrtivis* was reprinted by John Wolfe in London who "counterfeited the original 1563 edition almost to perfection" (142).

**1592** Julius Caesar Scaliger published his 1220 page *Exotericarvm exercitationvm liber XV*. "This philosophical treatise on Cardano's *De subtilitate* ... was a popular text-book until the final fall of Aristotle's physics" (@ Galland 161). It was reprinted in 1557, '60, and '76.

**1593** Porta's *De fvrtivis* was reissued (without permission) as *De occvltis literarvm notis* and included the first set of cryptological synoptic tables ever published. It was reprinted in 1603 and 1606.

**1594** Sir Hugh Platt published *The Jewell House of Art and Nature, conteining divers rare and profitable Inventions*.... The fifth tract included a description of a steganographic method: "How to write a letter secretlie that cannot easilie be discovered, or suspected" (144).

**1605** Francis Bacon published *Proficience and Advancement of Learning Divine and Humane*. In book VI, he gave a single paragraph description of cryptography and explained that preference should be given to those ciphers whose "vertues" include that they "bee without suspition" (60-1). That is, he recommended using a steganographic method which produces ciphertext that does not appear to be an enciphered message. Bacon concluded his brief treatment by noting that "in regarde of the rawnesse and Vnskilfulnesse of the handes, through which they passe, the greatest Matters, are many times carryed in the weakest *CYPHARS*."

**1606** Johannes Trithemius' *Steganographia...Ars per occvltam scriptvram animi svi volvntatem absentibvs aperiendi certa* was printed for the first time (however there is "considerable disagreement concerning the early editions of this work", including some indication it was published in a very limited edition in 1531 at Lyon [181-3]). The work dealt explicitly with methods of hiding the very existence of cryptograms in "normal" appearing text. Book IV treated acrostic steganograms and listed words which could be used "to construct a cover text in which only the second letters of each word would carry the secret message" (@ Kahn 135).

---

Clearly, there was sufficient discussion of cryptology prior to the publication of the *Sonnets* to make it possible for an author to use steganographic cryptography in a book. Furthermore, Bacon was familiar with steganography and recommended its use. As he later wrote in *Advancement of Learning*, it is advisable to use ciphers which "*may be managed without suspition*" because if

> Letters Missive fall into their hands, that have some command and authority over those that write; or over those to whom they were written; though the Cypher it selfe bee sure and impossible to be *decypher'd,* yet the matter is liable to examination and question;

> unless the *Cypher* be such, as may be voide of all suspition, or may elude all examination.

It is thus reasonable to conclude, along with David Kahn, author of the encyclopedic *Codebreakers,* that attempts to discover cryptograms demonstrating Bacon wrote the Works are "not entirely without cryptologic warrant." Indeed, it was "perfectly possible for Francis Bacon to have used steganography to simultaneously conceal and reveal his authorship of the Shakespeare works" (873-4). That this in fact occurred has been proven using the standard mathematical analysis techniques of modern cryptology.

Contents