THE HISTORY OF BOOK CIPHERS

Albert C. Leighton[1] and Stephen M. Matyas[2]

[1]Department of History
State University of New York
Oswego, New York 13126, U.S.A.

[2]Cryptography Competency Center
IBM Corporation 69K/988
Neighborhood Road
Kingston, New York 12401, U.S.A.

INTRODUCTION

You can do a lot with a book, besides read it! In fact, we know that by 1526--some 70 years after Gutenberg printed his first Bible--at least one of our forebears, Jacobus Silvestri, was thinking of how a book might be used for cryptographic purposes. Silvestri wrote of a sort of code book, or dictionary, which he recommended as a means to encipher written communications. From Silvestri, we can trace the development of book ciphers over a period of at least 400 years.

Book ciphers can be defined as any means of concealment in which a book, or existing text, is used as a basis for a cipher, from the simple and ridiculous to the complex and secure. They may include such oddities as Centos, in which words taken from the text are rearranged to form a different story; acrostics, which are built into a text and are extracted according to various rules to form a hidden meaning, and anagrams, in which the letters of a text are rearranged to form another text. The chief object of this paper is to demonstrate some ways in which book ciphers have been used for secure communications.

The simplest, and least secure method, is to take a dictionary and use the numbers of the page, column and line on which the desired word is found. This is equivalent to a one-part code in which both the numbers and the words run in their usual order. With such a simple method the approximate length of the dictionary and the location of particular initial letters in the dictionary can soon be ascertained.

Words may be cut from a text such as a newspaper or magazine and rearranged in Cento fashion to form a desired message. Handwriting and

G.R. Blakley and D. Chaum (Eds.): Advances in Cryptology - CRYPTO '84, LNCS 196, pp. 101-113, 1985.

other clues as to the origin of the message are concealed.[1] One of the oldest methods, used even by the ancient Greeks, makes use of tiny dots or pinpricks placed under the words or letters of a book to spell out a desired message.[2] The text is then sent to the recipient. The most effective of the book ciphers is the running key cipher where the cipher key is formed by the text of the book itself, which never repeats. As long as the key is used only once, the system is quite effective and reaches perfect security when the text used is random.

Centos are not practical for secret communication but are more likely to represent the recreational activities of medieval monks, with such productions as the Life of Christ made up from lines extracted from the Homeric poems or Virgil.[3]

Another use of texts which is more recreational than cryptographic is the formation of acrostics, where the secret information is concealed, frequently by the use of initial letters in a specially prepared text. The Hypnerotomachia Poliphili, where a Dominican monk confesses his love for one Polia,[4] and certain of the poems of Edgar Allan Poe are good examples.[5]

Anagrams, which use the letters of one text to form a secret message were frequently used by 17th century scientists to conceal and establish priority of discoveries. Unfortunately, it is often possible to anagram several perfectly good plain texts from a particular collection of letters, as witness the several thousand anagrams made up from the angelic salutation "Ave Maria...."[6] An anagram can be considered as an unkeyed transposition cipher and is worthless for the purposes to which it was put by Galileo, Huygens, and others.[7] Oddly, anagramming is often used as a last resort, especially by the unskilled, to unscramble impossible cryptograms even when there is no logical basis whatsoever for doing so.

THE SIXTEENTH CENTURY

A rather impractical method of book cipher was suggested by Blaise de Vigenere in 1586, which consists of placing a transparent sheet over the pages of a book and underlining the words you wish to use on the transparency. When a copy is sent to the receiver, he can place it over his copy of the book and see which words have been marked.[8] (This is really the equivalent of making a simple grill by cutting holes in a sheet of paper and sending it to the receiver to fit over a page.[9]) But the chances of finding the desired words for a message in a page or so of print is very slim.

Vigenere also describes the book cipher method which is probably the one most commonly used--that in which a letter is indicated by using numbers to show page, line, and location of the letter within the line.[10] This obviously takes a good many figures to encipher a single letter. He feels that such a cipher would be impossible to break without the key, but that, nevertheless, it is slow and tiresome to use and subject to error. He ascribes the method to Leone Battista Alberti of Florence (d. 1472) and quotes Alberti as saying that the method was "worthy of an emperor or a king." However, this is apparently based on a mistranslation. In actuality Alberti was referring to his own invention of the disk cipher and a more correct translation of the passage in Vigenere would be "It is sufficient to have mentioned it (the book cipher) in passing, because I have seen some who prize it very highly, just as a certain Leone Alberti of Florence prizes his own cipher (the disk cipher), 'worthy,' he says, 'of an emperor or king.'"[11]

The first actual description of a true book cipher that the authors were able to discover is that of Jacobus Silvestri in 1526.[12] Silvestri writes of a sort of code book, or dictionary, with root words in multiple columns. A unique symbol is associated with each column and row, and additional symbols are available for grammatical inflections. This is really an early form of an artificial language. Some current investigators are of the opinion that the famous Voynich manuscript may be composed in a form of artificial language.[13] [14] The Voynich Manuscript is often referred to as the "most mysterious manuscript in the world." Even its authorship is a puzzle. It has been attributed by some to Roger Bacon in the 13th century and has been thought to contain early records of scientific discoveries. In actuality, not even its date of origin or the language it is written in has ever been satisfactorily established.

Another early practitioner of the book cipher was the famous mathematician Girolamo Cardano, writing in the 1550's, whose impractical method was to find the words he wanted in a text and then write and send the words before or after the desired ones, altering them to make connected sense and adding, if necessary, extra words in parentheses. It is easy to imagine the recipient of such a cipher searching through his copy of the book which was used looking for the words before and after those in the cipher. Charles J. Mendelsohn charitably says "Other ways of communicating with the aid of two copies of the same book have been devised, but this one has never come into favor."[15]

A similar method of using a book was proposed by Giovanni Battista Porta in 1563,[16] but by 1586 Vigenere was proposing several ways of using a book such as the oiled-paper transparency already referred to and the commonly used method of using numbers for page, line, and location of the letter within the line, but also of disguising the cipher as an astronomical table. The signs of the zodiac were used to indicate the page, the numbers in the degree column to indicate the line, and the numbers in the minute column to indicate the individual letter. As he says, a mathematician would be suspicious if he checked the numbers closely.[17]

An aberration in the story of book ciphers is the famous biliteral cipher of Francis Bacon[18], which has caused so much error and confusion in the Bacon-Shakespeare authorship question. With a biliteral cipher, the text of a book is printed in two fonts, an A-font and a B-font, and the secret message is encoded in 5-letter groups such that aaaaa=A, aaaab=B, aaaba=C, etc. Bacon may indeed be the first to have employed a binary numbering system. It is a perfectly legitimate cipher, but depending as it does on often questionable differences in type fonts, has frequently been misused or misunderstood. The Great Cryptogram of Ignatius Donnelly[19], intended to expose Francis Bacon's Cipher in the Shakespeare plays, was nothing more than an elaborate cipher unwittingly constructed in reverse by Donnelly that allowed him to recover a desired plain text. The vivid imaginings of Elizabeth Wells Gallup come to mind also.[20]

THE SEVENTEENTH CENTURY

The 17th century is marked by the often naive efforts of scientists to protect their claims to priority in discoveries by concealing them in anagrams. Huygens and Galileo furnish good examples. They didn't realize that an anagram is nothing more than an unkeyed transposition cipher containing many legitimate solutions. Galileo's discovery of the phases of the planet Venus "Cynthiae figuras aemulatur mater amorum" (The mother of love (Venus) imitates the phases of Cynthia (the moon)) was concealed in the anagram "Haec immatura a me jam frustra leguntur o.y."(These unripe things are now read by me in vain o.y.).[21]

THE EIGHTEENTH CENTURY

By the 18th century Christian Breithaupt writes of using numbers for the page and line in which the desired letter occurs first. But he felt the method was not secure, since a clever investigator might find out what key book had been used.[22] Moreover, a great deal of searching might have to be done to find the desired letter as the initial letter of a line. Nevertheless, he says the method has become very common and is known to wanderers and beggars.

Later in the century Philip Thicknesse writes of a method of numbering the pages, lines, and words of a text.[23] He says that it is "scarce possible to be disclosed without the key." But searching through many pages to find a desired word would make this a very slow system for practical use.

With the coming of the American Revolution a number of different and improved book ciphers made their appearance. Numbering schemes were adopted that permitted the enciphering of individual letters. This made them somewhat easier to use and more precise. An early example of this sort was sent to Benjamin Franklin in Paris on 10 June 1776 by Barbeu-Dubourg, the translator of Franklin's works.[24]

Barbeu-Dubourg proposed numbering each letter of a key text, whose source has recently been found. With the assistance of Dr. Eric Gans, Chairman of the French Department, University of California at Los Angeles, Dr. Leighton was able to extend the Barbeu-Dubourg key somewhat. As printed in the Franklin Papers (Vol. 22, p. 470) the short example of plain and cipher text was:

```
3 2   19 5 23 16 12   44 53   10 51 4 61   36 17 6 24 71 1
M A   F  E M  M  E    E  T    D  E  U X    F  I  L L  E  S

42 28 37 33   82 54 11 9 8 47 59 88 13 69 31 92 72 34 56 73
V  O  U  S

6 94 4 20 40 100 68 48
```

from which the fragmentary key:

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 ....
S A M U E L       D     E              M  I     F
```

was derived. Dr. Gans suggested completing the plain text phrase "Ma femme et deux filles" with the words "embrassent de tout leur etre" to form the greeting "My wife and two daughters embrace you with all their being." This extends the key to:

```
S A M U E L _ A R D B E N _ _ M I _ F R _ _ M L _ _
```

plus other scattered letters and indicates that the key begins with the names Samuel Ward and Benjamin Franklin (with an M mistakenly used for K) and suggests that the key was made up of names taken from the membership of the Secret Committee of the Continental Congress, which was obviously in touch with Barbeu-Dubourg. (The Secret Committee was the predecessor of the present day State Department.)

Another of Franklin's correspondents was C.W.F. Dumas, who used a similar method of cipher.[25] By carefully following clues in Dumas' letters, Dr. Matyas determined that the book Droit des Gens was used as the key.[26] The key was mentioned subsequently in the Franklin Papers, indicating that it was found by at least one other person as well.[27]

One of the leading British generals in the Revolution, Frederick Haldimand, Governor of Canada, used a book cipher whose key was discovered some years ago "by an officer to whom Wm. F. Friedman (head of the U.S. Army cryptanalytic effort before and during WWII) was indebted."[28] It turned out to be the title page of a British Army List, a small book sure to be in the hands of every officer.[29] Further analyzing the problem, Dr. Leighton was recently able to extend this solution by finding the system which governed the associated code list. In his enciphered correspondence Haldimand was using numbers of the form 10-19 to stand for complete words. By studying the numbers and associated words found in some examples of Haldimand's deciphered messages,[30] Dr. Leighton was able to determine that the second part of the number stood for the letter which began the word and the first part indicated its position in the code list under that letter. Thus the word "there", represented by number 10-19, is the 10th word in the 19th sublist (of words all beginning with the letter "T"). Enough numbers and words have been analyzed to suggest that the code list had forty to fifty words per sublist.

Benedict Arnold tried to use Blackstone's Commentaries as a key book, but found it so slow and cumbersome that he and Major Andre soon switched to Bailey's Dictionary, 21st edition, 1770, using a system based on page, column, and line numbers with a plus one displacement. Thus, "Zoroaster" became 928.2.2 not 927.1.1. If they had switched key books earlier, West Point might have been lost to the British. Two other famous British generals, Cornwallis and Clinton, in 1781, based a code on the 1777 edition of Entick's Dictionary, while Aaron Burr, in 1805, used a similar method based on the 1800 edition of the same book.[31]

THE NINETEENTH CENTURY

The first commercial venture to bring cryptography to the fingertips of most Americans occurred in 1805 with the publication of a small dictionary "to enable any two persons to maintain a correspondence, with a secrecy, which is impossible for any other person to discover."[32] A short list of directions for using the dictionary and numbering the words in a pair of books was provided. But there is nothing to show that this dictionary code was well-received, perhaps indicating that it was published more as a marketing ploy, since two books were required to make it work.

Kluber's Kryptographik, published in 1809, is the most complete, useful, and possibly most influential of the early how-to books on cryptology.[33] He gives his highest recommendation to book ciphers as being extremely secure. Provided also are instructions showing how words, syllables, and individual letters can be enciphered differently each time they occur. For example, with a key text where figures 3 and 61 stand for "also" and "sich", the cipher 3.61.... denotes the plain text "ach", that is, the first letter of "also" and the third and fourth letters of "sich."[34] (Even in this simple example the letter "s" could be enciphered in two ways using 61. or 3...)

A cipher from about 1810 found in the Thurn und Taxis archives in Germany, by Dr. Erich Huttenhain, uses page, line, and letter numbers.[35] He was able to recover a few words of the key, but has not yet found the key book.

The most sought after solution to a book cipher is that of the Beale ciphers, alleged to contain instructions to the Beale Treasure, supposedly buried in Virgina about the 1820s.[36] Of the three ciphers, the solution to one has been known about 100 years. It is based on numbering each word in the Declaration of Independence (When 1 in 2 the 3 course 4 ....) and then using only the initial letters of the words: 1=W, 2=I, 3=T, 4=C, etc. Despite the best efforts of many, including the Beale Cypher Society, no key document or book breaking the other two ciphers has been found.

Better luck has been achieved with the book ciphers of Nicholas Trist, whose unauthorized negotiations with Mexico ended the Mexican War in 1847 and greatly expanded U.S. territory. While in Mexico, he found it necessary to devise two ciphers to permit secure communication with his superiors in Washington. One was based on numbering each letter of a passage; the other on a triple coordinate system in which individual letters were designated by numbers corresponding to the page, line, and position of the letter within the line. He described the key book circuitously in letters to James Buchanan, the Secretary of State, later to become President. In a model of scientific and literary detections, described in a recent issue of Cryptologia, Dr.

Matyas, by carefully delimiting the field of investigation and then checking methodically hundreds of books, identified the key book, thereby unlocking additional enciphered Trist material.[37]

For anyone who wishes to undertake a similar quest, here is a good opportunity. Jefferson Davis, President of the Confederacy, proposed using a dictionary as a code book.[38] All that is necessary is to find a three column dictionary in which the 20th word in the left column of page 146 is "Junction."

The use of a dictionary as a key book was particularly common in Victorian times and was frequently proposed in popular magazines.[39] This really results, as previously said, in a one-part code with page numbers increasing from A to Z. Without super-encipherment of the numbers it is soon possible to estimate the size of the dictionary, number of columns, and average number of words per column.

Perhaps the most curious use of a dictionary is in an international astronomical cipher code published at Harvard College Observatory in 1881.[40] Here we have a reverse dictionary code in which words from a particular edition of a dictionary are used to represent numbers. As an example, in this astromonical cipher, the first word always represents the day of the year and the time of day; the second word indicates the "distance of perihelion from node" and the third word stands for the "longitude of node." The message "Customably digitated butternut" is deciphered in this way: On page 136 the 73rd word "customably" = the 136th day of the year (16th of May), 73 is the time of day expressed decimally. "Digitated" the 8th word on page 150 = 150°8', the distance of perihelion from node, and "butternut" the 28th word on page 91 represents 91°28", the longitude of node.

Sherlock Holmes, never unaware of current trends, used a book cipher based on a non-existent edition of Whitaker's Almanac in The Valley of Fear.[41] His creator, Sir Arthur Conan Doyle, sent messages to British POWs in Germany in World War I by inconspicuous pinpricks under desired letters, a method already described.[42]

THE TWENTIETH CENTURY

The outstanding achievement in solving a book cipher must go to William F. Friedman, who cryptanalyzed a Hindu book cipher in World War I. He did so without knowledge of the key book, although the book was later identified.[43]

Herbert O. Yardley, author of The American Black Chamber, worked in China shortly before our entry into World War II. Some of his achievements are told in his recently published The Chinese Black

Chamber, including the use of a book as a key to encipher messages in the Chinese Telegraph Code (Ming Code).[44] After receiving a message, which began with the 5-letter group EHEER, he theorized that the letters might indicate message numbers and date. Thus, he equated EHEER = 10112 = message 101 of the 12th. A similar equivalency was made on successive days, which allowed him, after putting the letters in normal order, to recover parts of three words:

0	1	2	3	4
H	E	R		
L	I	G	H	
G	R		I	N

Investigation revealed that the words came from pages 17, 18, and 19 of Pearl Buck's The Good Earth.

Many of the systems using books result in cipher messages which are much longer than the original plain text. A way to avoid this is the running key, where a text from a book is combined in one of many possible ways with the desired plain text to produce a cipher text of the same length. Robert Graves, in his I, Claudius (a fictional work), describes a running key cipher in which the key is the first hundred lines of Homer's Iliad.[45] Each letter in the cipher is represented by the number of letters in the alphabet (ABC...Z) between it and the corresponding letter in Homer. Suppose the Iliad began with the word "Achilles," then the recipient of the cipher 10 6 4 3 would count 10 letters from A, 6 from C, 4 from H and 3 from I and would find the plain text KILL:

```
    A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
10  A - - - - - - - - - K
6       C - - - - - I
4                 H - - - L
3                   I - - L
```

Another common way of using a running key is illustrated:

```
P | W H E N I N T
K | T A K E O F F
C | X T G R G S M
```

where P = plain text, K = Key, and C = Cipher text. When two standard alphabets are slid against each other with the "T" of the second alphabet aligned under the "W" of the first alphabet, in this way

```
ABCDEFGHIKLMNOPQRSTUV|W|XYZABCDEFGHIJ....
   ABCDEFGHIKLMNOPQRS|T|UVWXYZ
```

then the cipher "X" is the letter in the second alphabet aligned under the letter "A" of the first alphabet, assuming that the first alphabet is continuous.

William F. Friedman, who broke the Japanese diplomatic cipher used in World War II, was the first person known to the authors to systematically solve running key ciphers.[46] His basic approach was to assume that both the key and the plain text were intelligible sequences. Once started, an extension of the key automatically extends the plain text and vice versa. The example above can illustrate the principle. If the first two words "When" (plaintext) and "Take" (key) are known, the assumption of the word "in" (plain text) would automatically give "of" for the key. Completion of the word to "off" would give "t" as the beginning of the next word in the plain text suggesting "the". Thus the key and plain text can be worked against each other to extend both.

If the key is not intelligible, but random (e.g. using a book of random numbers or letters), then one has a completely unbreakable one-time system. But no part of the key can be used more than once, so that the amount of keying material needed must be equal to the anticipated amount of plain text to be communicated, which could be substantial. A code book of random numbers or letters is not easily hidden among the books of an ordinary library, so that it may be difficult to maintain the secrecy of the keying material without drawing undue attention to it. An example of a one-time system is found in one of Che Guevara's worksheets, which was discovered after his death in 1967. The worksheet is in the following form:

```
P   72  8  32  34  8

K   34  6  51  42  1
    ------------
C   06  4  83  76  9
```

The plain line (P) represents a simple numerical substitution of the plain text LECHE (i.e. Fidel Castro). The key (K) is a stream of random numbers. The cipher text (C) is produced by non-carrying addition.[47]

CONCLUSION

We have traced the origin and development of book ciphers over a period of at least 400 years and seen a few of the ways in which a book may be used for secure communications. The Beale ciphers are excellent proof that sometimes book ciphers are very secure indeed!

ACKNOWLEDGEMENT

Dr. Leighton would like to thank the Center for Medieval and Renaissance Studies at the University of California, Los Angeles, for making some of his research possible.

FOOTNOTES

1. See example in Sir Arthur Conan Doyle "The Hound of the Baskervilles", *The Complete Sherlock Holmes*, Garden City, N.Y., n.d., p. 801.

2. Aeneas Tacticus. 31.1-3. Albert C. Leighton, "Secret Communication among the Greeks and Romans," *Technology and Culture*, Vol. 10, No. 2, April 1969, p. 149.

3. Article "Cento," *Encyclopaedia Britannica*, 11th ed., New York, 1910, p. 674.

4. David Kahn, *The Codebreakers*, New York, 1967, pp. 873-4.

5. William F. and Elizebeth S. Friedman, *The Shakespearean Ciphers Examined*, Cambridge, 1957, p. 97.

6. Kahn, *Codebreakers*, p. 869.

7. Kahn, *Codebreakers*, p. 773.

8. Blaise de Vigenere, *Traicte des Chiffres ou Secretes Manieres d'Escrire*, Paris, 1586, pp. 208-9.

9. The grill cipher had already been invented by Girolamo Cardano in the 1550s. See Charles J. Mendelsohn, "Cardano on Cryptography," *Scripta Mathematica*, Vol. 6, 1939, pp. 164-5.

10. Vigenere, *Traicte*, pp. 208-9.

11. Charles J. Mendelsohn, "Blaise de Vigenere and the 'Chiffre Carre'," *Proceedings of the American Philosophical Society*, Vol. 82, No. 2, March 1940, pp. 117-8.

12. Jacobus Silvestri, *Opus Novum*, *praefectis arcium*, Rome, 1526.

13. Philip M. Arnold, "An Apology for Jacopo Silvestri," *Cryptologia*, Vol. 4, No. 2, April 1980, pp. 96-103.

14. Mary E. D'Imperio, *The Voynich Manuscript*, National Security Agency, Ft. Meade, Maryland, 1978, pp. 67-8, 118.

15. Mendelsohn, "Cardano on Cryptography," pp. 161-2.

16. Giovanni Battista Porta, *De Furtivis Literarum Notis, vulgo de Ziferis libri IV*, Naples, 1563, pp. 106-7.

17. Vigenere, *Traicte*, pp. 208-9.

18. Francis Bacon, *Tvvoo bookes of Francis Bacon of the Proficience and Advancement of Learning, Divine and Humane*, London, 1605, p. 61.

19. Ignatius Donnelly, *The Great Cryptogram*, Chicago, 1888.

20. On this and other pseudo-ciphers see Friedman and Friedman, *Shakespearean Ciphers*.

21. Kahn, *Codebreakers*, p. 773.

22. Christian Breithaupt, *Ars decifratoria sive scientia occultas scripturas solvendi et legendi*, Helmstadt, 1737, p. 20-21.

23. Philip Thicknesse, *A treatise on the art of decyphering and of writing in cypher*, London, 1772, pp. 111-12

24. *Franklin Papers*, Philadelphia, 1982, Vol. 22, p. 470.

25. National Archives Microfilm Publications, Microcopy no. 247, Papers of the Continental Congress, 1774-1789, Roll 121, Item no. 93, Letters Received from Charles W. F. Dumas. Washington, 1959.

26. *Le Droit des Gens par M. de Vattel*, Amsterdam, 1775, pp. iii-v.

27. *Franklin Papers*, Vol. 22, p. 464.

28. William F. Friedman, *Six Lectures on Cryptology*, National Security Agency, Ft. Meade, Maryland, 1963, pp. 41-3.

29. *A List of the General and Field Officers as they rank in the Army*, London, 1778.

30. Public Archives Canada, Haldimand Papers MG 21, Additional Manuscripts 21807 and 21808, Microfilm Roll A-741, Correspondence with Sir Henry Clinton and others at New York, 1777-1783.

31. Carl van Doren, *Secret History of the American Revolution*, New York, 1969, pp. 200, 204. Kahn, *Codebreakers*, pp. 177-8, 183, 186.

32. *A Dictionary, to enable any two persons to maintain a correspondence, with a secrecy, which is impossible for any other person to discover*, Hartford, 1805.

33. Johann Ludwig Kluber, *Kryptographik*, Tubingen, 1809.

34. Kluber, *Kryptographik*, p. 349.

35. Albert C. Leighton, "Ciphers in Bavarian Archives," *Proceedings of the Second Beale Cypher Symposium*, Washington, 1979, p. 79.

36. James B. Ward, *The Beale Papers*, Lynchburg, 1885.

37. Albert C. Leighton and Stephen M. Matyas, "The Search for the key book to Nicholas Trist's book ciphers," Cryptologia, Vol. 7, No. 4, October 1983, pp. 297-314.

38. Friedman Lectures, p. 75.

39. Examples of dictionary codes are found in G.P.B. (George Parker Bidder), "Ciphers and Cipher-Writing," Macmillan's Magazine, Vol. 23, 1871, p. 330; (Anonymous) "Missives in Masquerade," Cornhill Magazine, Vol. 29, 1873, p. 179; (Anonymous) "The Art of Secret Writing," The Practical Magazine, Vol. I, 1873, p. 318; (Anonymous) "Writing to Conceal One's Thoughts," All the Year Round (conducted by Charles Dickens), Vol. 35, 1875, p. 510; T.J.A. Freeman, "Cipher," American Catholic Quarterly Review, Vol. 18, 1893, pp. 863-4; George Wilkes, "Cryptography," Cosmopolitan, Vol. 36, 1903, p. 716.

40. William W. Payne, "Astronomical Cipher Messages," The Sidereal Messenger, Vol. 4, No. 6, pp. 161-3.

41. Arthur Conan Doyle, "The Valley of Fear," Complete Sherlock Holmes, p. 904.

42. Arthur Conan Doyle, Complete Sherlock Holmes, Preface, p. x.

43. Kahn, Codebreakers, p. 371-3.

44. Herbert O. Yardley, The Chinese Black Chamber, Boston, 1983, pp. 114-24, 129.

45. Robert Graves, I, Claudius, New York, 1934, Chapter 17, pp. 232-33.

46. Kahn, Codebreakers, p. 375. William F. Friedman, Methods for the Solution of Running-Key Ciphers, Riverbank Publication, No. 16, Geneva, Illinois, 1918.

47. David Kahn, Kahn on Codes, New York, 1983, pp. 139-44. Barbara Harris of new York solved the simple numerical substitution for the plain text with the following result:

	8	2	0	6	4	9	1
	e	s	t	a	d	o	y
3	b	c	f	g	h	i	j
7	k	l	m	n	n	p	q
5	r	u	v	w	x	z	

Note that it was not the one-time system that was cryptanalyzed but only the simple substitution of the worksheet.