THE GENESIS OF THE JEFFERSON/BAZERIES CIPHER DEVICE

Louis Kruh

THE GENESIS OF THE JEFFERSON/BAZERIES CIPHER DEVICE

Louis Kruh

ABSTRACT

Cipher Device M-94 was adopted by the United States Army in 1922, the same year papers found in the Library of Congress revealed that Thomas Jefferson had invented the same device about 125 years earlier.

Almost 100 years after Jefferson, Commandant Etienne Bazeries, a French army cryptologist, independently developed a similar device.

Both inventions, which ultimately formed the basis for the most widely used cryptosystems in the 20th century, apparently had a common antecedent in the letter lock, which was popularized in France by Edme Regnier during the late 18th and early 19th centuries.
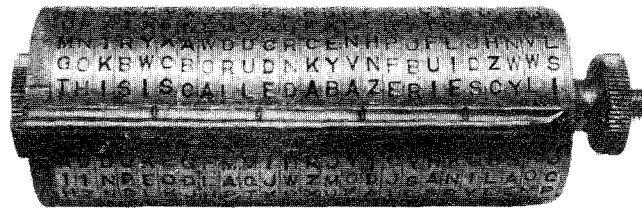
Figure 1. U.S. Army Cipher Device M-94.

DESCRIPTION AND BACKGROUND

The concept behind the cylindrical cipher device adopted by the United States Army under the designation M-94, (Figure 1) and the subsequent flat strip cipher board, M-138-A, (Figure 2) which evolved from it, became "one of the most widely used systems in the history of American cryptography."[1] The two devices utilized the identical cryptographic principle; the simultaneous use of a number of different, sliding, mixed alphabets.[2]

The M-94, made of aluminum alloy, consists of a central shaft on which is mounted a set of 25 rotatable alphabet disks. On the rim of each disk is

[A version of this article appeared in The Army Communicator, Winter 1980, 48-54.]

stamped a different, completely disarranged alphabet. Lugs and slots on each side of the disks enable them to be held together side by side in any desired position by tightening the knurled thumb nut at the end of the shaft. Both sender and receiver must have a device.

Each disk has its own identifying symbols, a letter and number on its side. The numbers run from 1-25 and the letters from B-Z. These symbols are used to designate the sequence in which the disks are to be assembled on the shaft. This order constitutes the key which both the encipherer and decipherer must know.

After the encipherer places the disks on the shaft in the prearranged order, he revolves one disk after another to align the first 25 letters of the message in a horizontal row. Then he selects at random any one of the other rows, which will form 25 letters of gibberish, as the ciphertext. He repeats this process in groups of 25 letters to the end of the message.[3]

The decipherer begins the same way. He assembles the disks on the shaft in the order given by the key and then rotates each disk individually until the first 25 letters of ciphertext stand in a row. Then he scans the other rows for the one which will read intelligibly.[4]
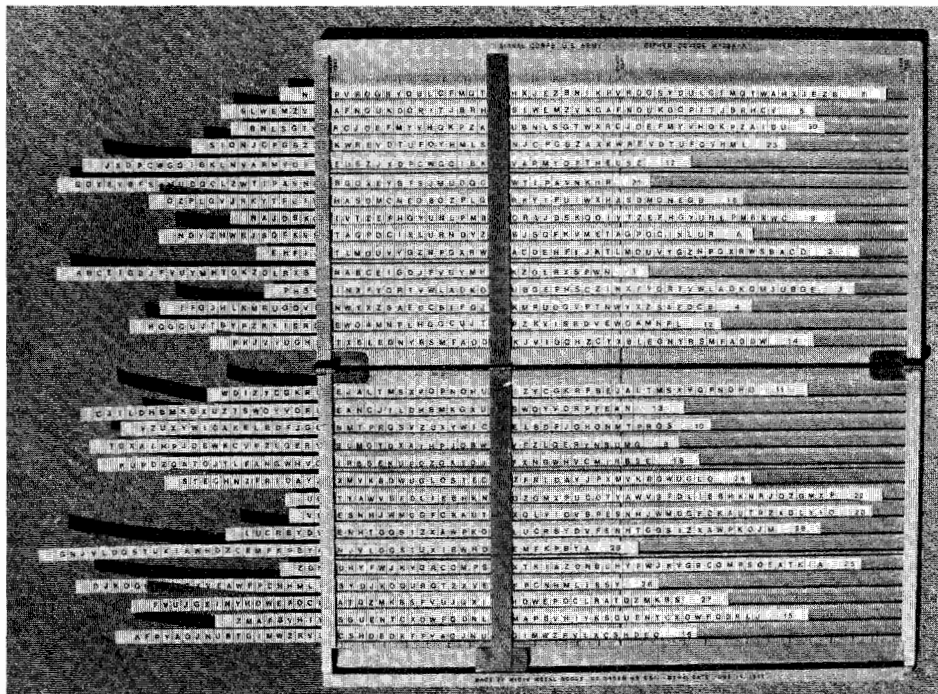

Figure 2. Cipher Device M-138-A (simulated strips).

The M-138-A works in a similar fashion. The device consists of a hinged aluminum board into which are milled thirty grooved channels. These channels are designed to hold removable paper strips containing randomly mixed alphabets. Each strip has its own mixed alphabet repeated twice and printed in a horizontal row.[5]

The strips, inserted in the channels in a particular order designated by a key, slide from side to side. The encipherer aligns the plaintext letters to read vertically alongside a guide rule which is part of the device. Then he chooses a ciphertext column at random and slides the guide rule adjacent to it for easier copying. This procedure is repeated for the entire message.[6]

The decipherer simply reverses the process after assembling the strips according to the key.[7]

Because the system underlying these devices employs several cipher alphabets, it is a polyalphabetic one. But because they are employed simultaneously and not serially, as in most polyalphabetics, the system is usually termed a "multiplex" one.

The system played an important role in secret communications both prior to and during World War II.

The cylindrical version was first officially adopted as a United States cryptosystem by the Army in 1921.[8] In 1927, it was issued to the Navy under the designation CSP 488 for joint communications with the Army. Military attaches began using it in 1929, naval attaches in 1930, and in 1939, it went to the Coast Guard under the title CSP 493.[9]

The cipher device M-94 was used extensively between World War I and World War II and a total of 9,432 were eventually produced. When tests were started on the use of converter M-209, a more complicated mechanical printing device, plans were made for the discontinuance of the M-94. On August 9, 1943, when sufficient M-209's were available for replacement purposes, Cipher Device M-94 was declared obsolete.[10]

In 1933, the Army turned to the flat version. It wanted to provide an easy method for changing the random alphabets while still using the basic principle of the M-94.[11] Several experimental models were built and evaluated before one was officially adopted in 1934 as the M-138. In 1938, an improved model, the M-138-A, was adopted. Included in the improvements was an increase, from 25 to 30, in the number of mixed alphabets that could be used.[12]

The Navy had participated in the development of this strip device, designating it CSP 845. When a shortage of aluminum forced both services to seek substitute material the Navy developed the CSP 845 (Plastic). The Army ordered 5,000 of the plastic versions from the Navy in October, 1942, and distributed them widely around the world. The plastic strip boards, however, did not prove satisfactory, particularly in tropical climates where the hot, moist weather caused them to warp.[13]

The Army had developed a wooden board made of Honduras mahogany, Cipher

Device M-138-A (Wood) or SIGWOWO. Two thousand were ordered in February, 1943, but they also proved unsatisfactory in the field due to the friction of the paper strips on the wood and warping of the board.[14]   In September, 1943, aluminum became available again and the Army ordered 8,000 aluminum cipher devices CSP 845 from the Navy because it was more expedient than renegotiating with the manufacturer for the aluminum M-138-A.[15]

All together, 17,872 flat strip cipher devices in all versions were ordered from 1935 through 1943.[15]   In addition to the Army and the Navy, strip cipher devices were used by almost a dozen different government agencies during the war.[17]   Strip cipher systems were also distributed to at least six foreign governments including France, Italy, and Russia so they would maintain secure communications with United States Army personnel.[18]

Even after cipher machines were introduced during World War II, strip cipher systems continued in use by individuals such as military attaches, or units not authorized to use cipher machines, and as standby equipment for machine users.[19]

They were also used after the war. A 1948 Army document said, "Strip systems. . . at the present time are a very important means of communication . . ."[20]   Another author, in 1967, wrote that the Navy was using it at that time.[21]

This is an amazing longevity for a cryptosystem in a technological era that obsoletes complex mechanisms almost overnight.

JEFFERSON, BAZERIES AND OTHER INVENTORS

The device was invented, or apparently so, a number of times. Charles Babbage, the eminent mathematician, scientist and precursor of the modern computer, hinted in the Journal of the Society of Arts in 1854 at a cylindrical type cipher device. His letter said that a cipher system proposed by a reader in a previous issue was not new and that Babbage had made, " . common centre, each circle having on its circumference the twenty-six letters of the alphabet."[22]   He then wrote, "The best form is, perhaps, ring of box-wood placed side by side on a cylinder, and having the twenty-six letters on the circumference of each."[23]   But this reference, precise and early as it was, faded into obscurity.
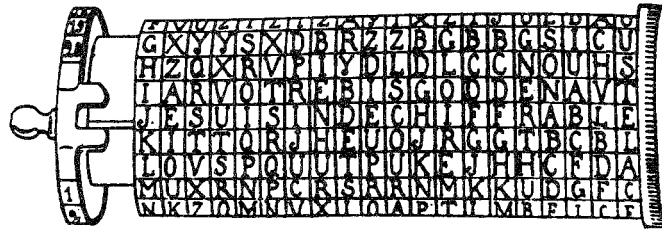

Figure 3. Bazeries' drawing of his ''cylindrical cryptograph.''

Apparently independently, for he never mentions Babbage, whose work seems not to have been known to cryptographers of the time, Major Etienne Bazeries, a French cryptologist, developed a 20-disk mechanism (Figure 3). On September 19, 1891, he described it in Marseilles at the convention of the French Association for the Advancement of Science.[24] And after it was rejected by the French army he pictured and wrote about it in his book, Les Chiffres Secrets Devoiles.[25] Probably because this work stood in the mainstream of cryptologic literature, Bazeries' invention influenced cryptography more than all the similar inventions.

A contemporary, one Arthur J. Hermann, a member of the French Mathematical Society, proposed, apparently for the first time, a flat strip format of Bazeries' cylinder with 18 wooden or cardboard strips in his article, "Nouveau Cryptographe Construit d'apres le Systeme Bazeries," in the September 2, 1893 issue of Revue Scientifique.[26]
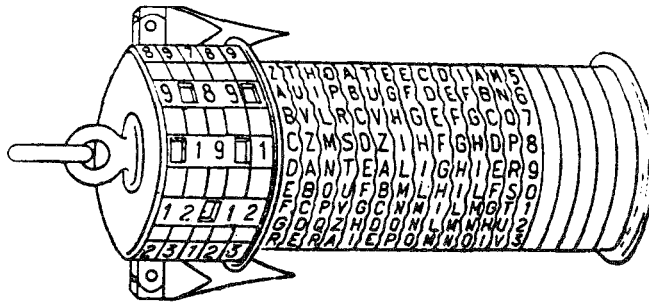

Figure 4. Ducros' Scotograph.

In 1900, an article in Rivista Militare Italiana by Gioppi di Turkheim, a writer on cryptology [27] described the Durcos Scotograph, invented that year by Colonel Oliver Ducros of the Italian army.[28] It was a 13-disk device similar to the Bazeries cylinder which had possibly inspired it, but with some added embellishments (Figure 4).

During the summer of 1913, Captain Parker Hitt, an instructor at the United States Army Signal School, Fort Leavenworth, Kansas, created a 10-disk device.[29] He acknowledged that this work was influenced by the ideas of Bazeries.[30]

He then reinvented the strip cipher -- he gives no evidence of having read Hermann's article. Since Hitt preferred the flat form because of its "compactness, simplicity of operation, and ease with which alphabet strips could be reproduced if lost,"[32] he abandoned his work on the cylindrical device.[33] His first flat device had twenty alphabet strips, possibly because Bazeries' cylinder had twenty disks. But by 1916, it had expanded to twenty-five.[34] (Figure 5)
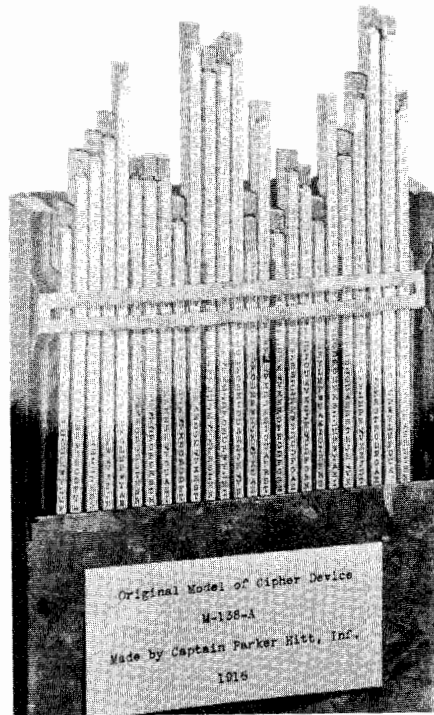
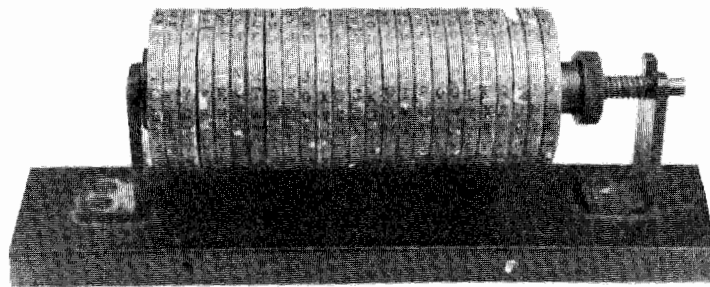Figure 5. Hitt's Strip Cipher Device.

Figure 6. One of Mauborgne's original models of his 25 disk device.

His friend, Major Joseph O. Mauborgne, Assistant Commandant of the Signal
School at Fort Leavenworth, examined Hitt's alphabets and decided that they
were not scrambled enough to assure sufficient cryptosecurity. So he
constructed mixed alphabets that would repeat as few pairs of letters among
them as possible.[35] He then had two 25-disk devices using these alpha-
bets made in the Army Signal School shop in early 1917.[36] (Figure 6)
Mauborgne's work led directly to the M-94, Hitt's led to the M-138-A.

But the most remarkable inventor, discovered by chance in 1922 from his
papers in the Library of Congress, was Thomas Jefferson. The discovery, by
Dr. John M. Manly, a Chaucer scholar and cryptanalyst in World War I,
revealed that before Babbage and Bazeries, Jefferson had invented a cipher
device based on the same principle but using 36 disks [37] which he called
his "wheel cypher."[38] Despite its precocity, however, it seems never
to have been used and so was lost to the world of cryptography until Manly
found it.

But where did Bazeries and Jefferson get the ideas for their systems? One
was a professional cryptologist and the other a mere dilettante in an
esoteric art. Did one evolve the concept from a deep-seated knowledge of
the science, and did the other get a flash of inspiration? Or was there
some mechanism that triggered their thinking along similar paths?

LETTERS LOCKS AND EDME REGNIER

Up to now no one has suggested a source for these virtually identical but
almost certainly independently conceived ideas.

I believe I have found it.

One summer day I visited a lock museum and suddenly found myself in front
of a letter lock. It contained six disks or wheels with a complete alpha-
bet engraved on each one. When six particular letters -- and only those
six -- are lined up with notched benchmarks at the edges of the lock, the
lock opens. As an amateur cryptologist with a particular interest in
cipher devices, I recognized at once that the lock resembled a six-disk M-
94. It struck me that the letter lock might well be the forerunner of the
Jefferson/Bazeries cylinder.

As I began to investigate this possibility, I reread General Luigi Sacco's
Manual of Cryptography[39] and the following sentence, not noted in pre-
vious readings, almost leaped out of the page, "The Bazeries device resem-
bles very much one of those word padlocks which are used for locking some
secret box."[40] In the next paragraph, Sacco described the operation of
the Bazeries device this way, " . . . to encipher we simply rotate the
successive disks . . . in the same way we form the word in the word pad-
locks.''[41]

Gioppi, too, said the similar Ducros device, " . . .has no little analogy
with the so-called word padlock (combination lock based on a word instead
of numbers)."[42] Obviously, cryptologists other than just myself have
seen the relationship between the wheel cipher and the letter lock. But
how was the connection made?

Letter locks, the ancestors of modern combination locks, appeared about 1,000 years ago in China. They consisted of a group of rings engraved with symbols, letters or numbers revolving around their bolt, opening only when the rings were moved to spell out a prearranged set of letters or symbols.[43]

In the West, the letter lock dates back to at least the early 1400's.[44] (Figure 7) Knowledge of it seems never to have been lost. In the mid-1500's, Girolamo Cardano, famed Milanese physician, mathematician and scholar who touched on cryptology in his writings, suggested a cipher lock with alphabet wheels that would open only when the wheels were correctly aligned to form a particular word.[45] Silvestro Pietrasantra's De Symbolis Heroicis, published in Antwerp, in 1643, depicts letter locks on pages 3 and 254. The motto above the first lock says, "It opens to a word" and above the second lock the motto is, "By luck or hard work."[46]
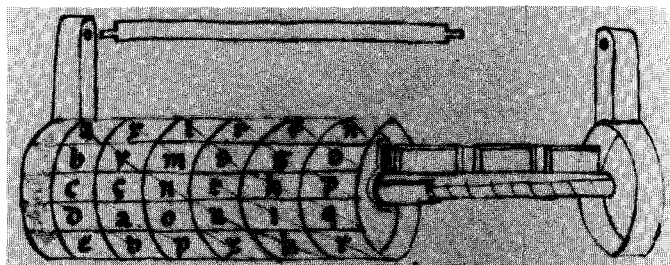

Figure 7. Letter lock ca. 1420.

Later, the letter lock seems to have become well enough known for writers of the 17th century to allude to it. The poet, Thomas Carew, used this verse in his poem, To my honoured Friend, Master Thomas May, upon his comedy, The Heir.

> The whole plot doth alike itself disclose
> Through the five acts, as doth the lock that goes
> With letters, for, till every one be known,
> The lock's as fast as if you had found none.[47]

In their play, Noble Gentlemen, Beaumont and Fletcher have a character say:

> A cap-case for your linens and your plate,
> With a strange lock that opens with AMEN.[48]

The Museum le Secq des Tournelles in Rouen has letter locks in its collection that predate the French Revolution.[49]

The device increased greatly in popularity during the last decade of the 18th century and the first part of the 19th century, due largely to the efforts of a Frenchman who claimed to have invented it but, in fact, merely improved it. This improvement made it possible to change the combination of a lock when necessary. Previously, the combination of a lock was

fixed and if it became known to others the lock had to be discarded.

The Frenchman was Edme Regnier (1751-1825), a prolific inventor with over 70 inventions to his credit.[50] He planned and organized the Artillery Museum in Paris and became its first director in 1796.[51] In 1777, he won first prize from the Societe libre d'Emulation de Paris for his invention of a combination lock.[52] Some years later he developed the letter lock or word padlock[53] possibly because a combination in the form of a word is easier to memorize than a string of numbers.
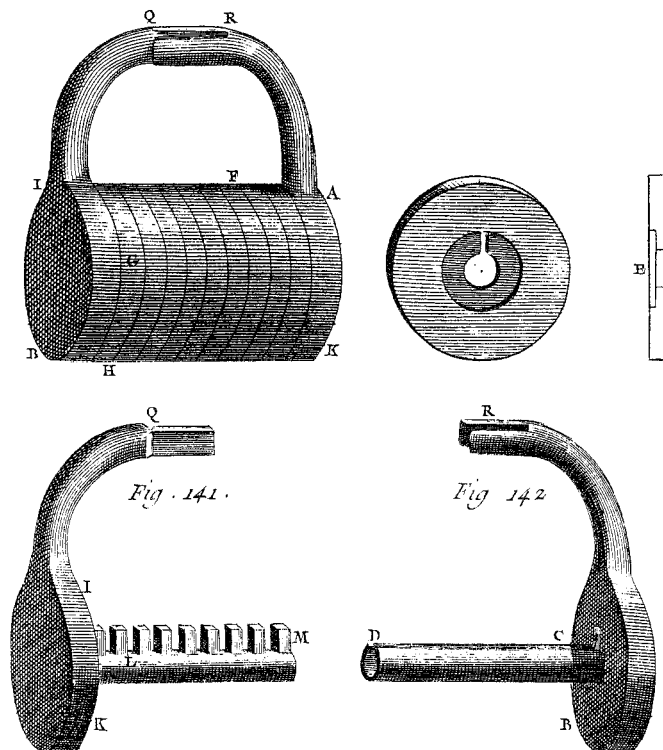
Figure 8. Combination lock in the Encyclopedie Methodique.

A description of his lock, important for this paper, appeared in 1790 in Volume VII, Arts et Metiers Mecaniques, of L'Encyclopedie Methodique,[54] whose 194 volumes were published between 1782 and 1832. The encyclopedia's article pointed out that a picture was unavailable and, instead, furnished a thorough description of Regnier's invention. It said the lock had nine disks, each divided into eleven parts, containing the numbers 0 through 9 and a star.[55] It also described the combination lock that Regnier had

improved upon. That one is illustrated in Volume IV of the encyclopedia's
plates series, published in 1785, and is an 11-disk combination lock.[56]
Although its description says that figures and characters distributed on
the circumference of the disks must be properly aligned for the lock to
open,[57] the drawing shows blank disks (Figure 8). Still, if the shackle
or U shaped section is omitted, it clearly resembles a letterless version
of Jefferson's wheel cypher.

Other papers and articles about Regnier's lock inventions also appeared
around the turn of the century. Regnier himself prepared a three-page
pamphlet which described and pictured his letter locks (Figure 9).[58]
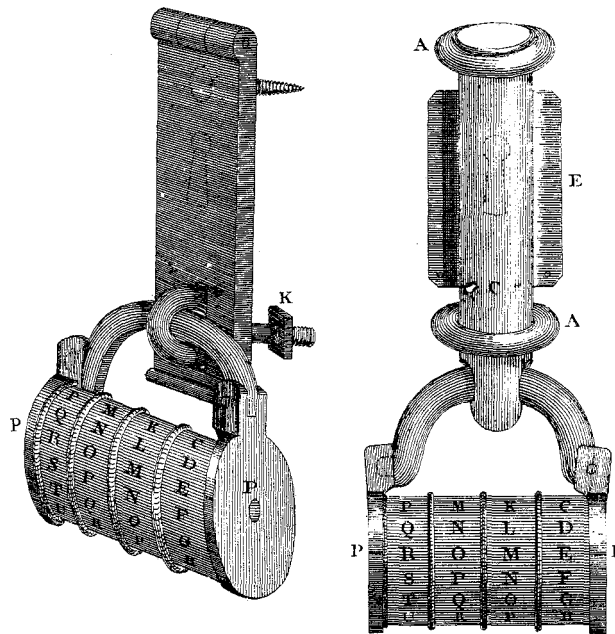
Figure 9. Illustration from Regnier's pamphlet.

One Regnier lock, similar to those in his pamphlet, is today in the Musee
National des Techniques in Paris (Figure 10).[59]

Vanhagen von Ense, a German writer who spent some time in Paris around
1810, wrote in his memoirs that "Regnier was a man of some invention and
had taken out a patent for a sort of lock,"[60] which he described:

> These consisted of broad steel rings, four, five or eight deep,
> upon each of which the alphabet was engraved; these turned round
> on a cylinder of steel, and only separated where the letters,

forming a particular word, were in a straight line with one an-
other. The word was selected from among a thousand and the choice
was the secret of the purchaser. Anyone not knowing the word
might turn the rings around for years without succeeding in find-
ing the right one.[61]
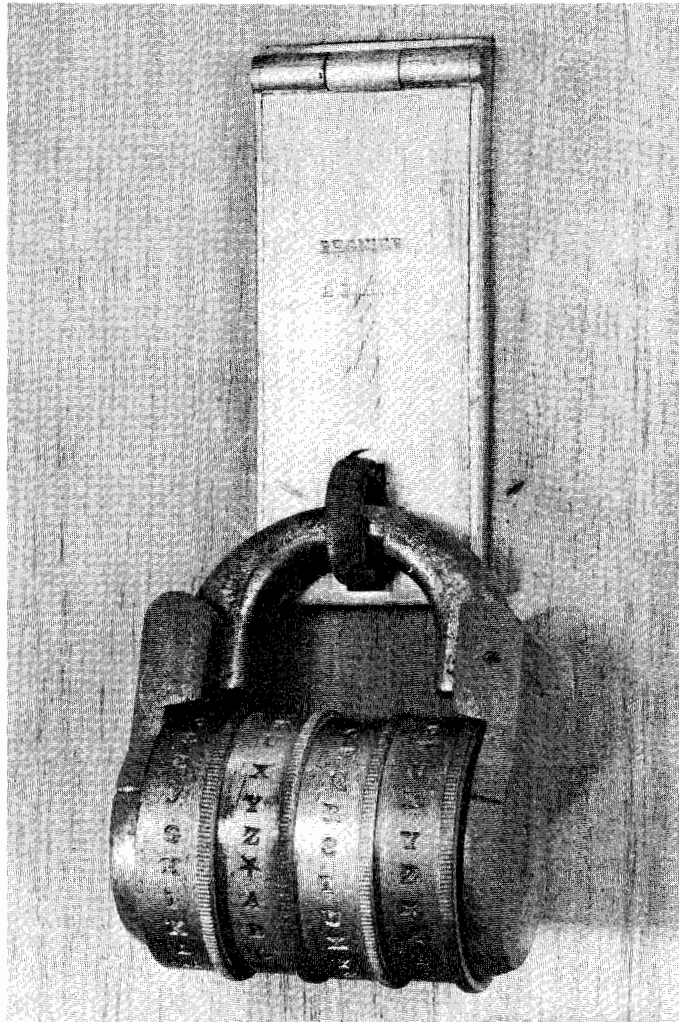

Figure 10. A Regnier letterlock in the Musee National Des Techniques,
           Paris France.

Ense further said that the lock,"made some noise at the time everybody praised his invention and bought his locks."[62] A lock collector specializing in letter locks confirms that they "were rather popular from 1750 to early 1900's."[63]

Could Jefferson have known of Regnier's lock?

CONNECTIONS

Chronology, first of all, permits it. Regnier arrived in Paris in 1778[64] and apparently spent the remainder of his life there. Jefferson went to France in 1784 and stayed for five years.[65] According to Dr. Julius Boyd, editor of The Jefferson Papers, Jefferson wrote the description of his wheel cypher in the period, 1790-1793 or 1797-1800 -- or after he returned from France.

Circumstances further make the connection likely. Jefferson considered himself " . . . one of the original subscribers . . . "[67] of the Encyclopedie Methodique, which had first published a description of Regnier's lock. His library included 136 of its volumes.[68] He thought so highly of it that in 1786 he began taking subscriptions for many of his friends back in the United States, including Benjamin Franklin and James Monroe.[69]

He corresponded with authors of articles, contributed his own material for use in at least one of the volumes, and mentioned the encyclopedia frequently in his correspondence.[70] Jefferson's intense and lengthy interest in the Encyclopedie Methodique is most important because it suggests with high probability that he was familiar with the secret combination locks described and pictured in its volumes.

Furthermore, an earlier edition of the Encyclopedie Methodique, the 39-volume Encyclopedie Ancienne, was also in Jefferson's library.[71] Volume II, published in 1751, carried a description of a "secret padlock"[72] and its picture in Volume IX, published in 1771,[73] shows that it is the same combination lock illustrated in the Encyclopedie Methodique (Figure 8). The publishers used the same drawings and virtually identical descriptions in both encyclopedias, doubling the possibility of Jefferson being exposed to it.

Finally, Jefferson's personality further makes his knowledge of Regnier likely. He was mechanically inclined and had "himself invented or adapted to personal uses numerous ingenious devices, the best known of which is his polygraph."[74] When he became Secretary of State in 1789 he was in effect the country's first Superintendent of Patents[75] and " . . . he scrupulously . . . investigated every claim to satisfy the statutory test of originality."[76]

A knowledgeable cryptologist, Rosario Candela, questioning in Bazeries' defense whether Jefferson was the originator of the wheel cypher, pointed out that " . . . Jefferson was a prolific writer who had the excellent habit of jotting down almost everything that struck him as being unusual. An insatiably curious man, he travelled widely."[77] Therefore, asks

Candela, "Is it not possible that in his European peregrinations he had come across the device . . . ?"[78] Though in a narrow sense this seems improbable, in the broad sense of a general stimulus it appears not unlikely.

It thus seems highly probable that Jefferson knew of Regnier's letter locks which perhaps inspired his wheel cypher. But how about Bazeries?

He was born in 1846,[79] only 12 years after a biographical sketch of Regnier said his locks were in wide use.[80] Therefore, Bazeries may well have had many opportunities to become familiar with Regnier's combination locks. Their mutual association with the French Army may have also contributed to this possibility. The evidence, although circumstantial, makes it likely that Bazeries too got the idea for his cylindrical cipher device from the type of letter locks developed by Edme Regnier.

It is perhaps significant that Charles Babbage included a chapter in his autobiography on "Picking Locks and Deciphering," in which he said, "These two subjects are in truth more allied than might appear upon a superficial view of them."[81]

CONCLUSIONS

A careful review of the information available to Jefferson leads one to conclude that he almost certainly knew about Regnier's locks, or other combination locks, or perhaps both, and that his wheel cypher was consciously or unconsciously derived from one of those sources. The same apparently was true of Bazeries.

It therefore seems likely that the independent inventions of Bazeries and Jefferson had a common antecedent, the letter locks of Edme Regnier. And others, like Babbage, may have also gotten the ideas for their similar devices from the letter lock. This does not detract from the inventiveness of these individuals because their devices were not a simple adaptation of the letter lock, but required the addition of two new conceptsµ the variable arrangements of the disks and the idea of a key, which enables any user to place them on a shaft in the order agreed upon by themselves and by someone else. But the letter lock, of course, provided the initial idea.

So, to Regnier, to the unknown ancient technician who devised the first such mechanism, and to those ingenious individuals who borrowed that technology, cryptology owes one of the most widespread of its 20th century cryptosystems.

FOOTNOTES AND REFERENCES

1. David Kahn, The Codebreakers (New York: Macmillan Co., 1967), p. 325.
2. U.S., War Department, Army Security Agency, The History of Army Strip Cipher Devices (n. p.: n.n., 1948), p.2.

3. U. S., War Department, Office of the Chief Signal Officer, Instructions for Using the Cipher Device Type M-49 (Washington: Government Printing Office, 1922), pp. 9-10.

4. Ibid., p. 10.
5. The History of Army Strip Cipher Devices, op. cit., Tab 26.
6. Ibid.
7. Ibid.
8. Ibid., p. 19.
9. Ibid., pp. 22-23.
10. Ibid., pp. 22-26.
11. Ibid., p.30.
12. Ibid., Chapters IV, V and VI passim.
13. Ibid., pp. 44, 56, 58-59.
14. Ibid., pp. 61-62.
15. Ibid., pp. 6, 62.
16. Ibid., Tab 33.
17. Ibid., p. 111.
18. Ibid., pp. 112-121.
19. Ibid., p. 70.
20. Ibid., p. 72.
21. Kahn. op. cit., p. 195.
22. Home Correspondence, Journal of the Society of Arts, Vol. II, No. 93 (September 1, 1854) 707.
23. Ibid., pp. 707-708.
24. Etienne Bazeries (Capitaine), "Cryptographe A 20 Rondelles-Alphabets (25 Lettres Par Alphabet)," Compte rendu de la 20 e session de l'Association Francaise pour l'Avancement des Sciences (Paris: Au Secretariat de l'Association, 1892), 160.
25. Etienne Bazeries (Commandant), Les Chiffres Secrets Devoiles (Paris: Libraire Charpentier et Fasquelle, 1901).
26. Arthur J. Hermann, "Nouveau Cryptographe Construit d'apres le Systeme Bazeries," Revue Scientifique, Tome LIII, No. 10 (September 2, 1893) 306-307.
27. L. Gioppi di Turkheim, "La Crittografia," Rivista Militare Italiana, Vol, 45, No. 12 (December 16, 1900) 2202-2235.
28. J. Bres (trans.), Manuel de Cryptographie by Luigi Sacco, (Paris: Payot, 1951), p. 58.
29. The History of Army Strip Cipher Devices, op. cit., p. 14.
30. Kahn. op. cit., p. 325.
31. The History of Army Strip Cipher Devices, op. cit., p. 15.
32. Parker Hitt Cipher Papers, David Kahn Collection, Letter December 19, 1914.
33. The History of Army Strip Cipher Devices, loc. cit.
34. Parker Hitt Cipher Papers, Letters, December 19, 1914, September 10, 1943.
35. The History of Army Strip Cipher Devices, op. cit., p. 16.
36. Ibid., p. 17.
37. William F. Friedman, "Edgar Allan Poe, Cryptographer (Addendum)," Articles on Cryptography and Cryptanalysis Reprinted from the Signal Corps Bulletin, U. S., War Department, Office of the Chief Signal Officer (Washington: Government Printing Office, 1942), pp. 181-182.
38. Kahn, op. cit., p. 192.
39. Howell C. Brown (trans.), Manual of Cryptography by Luigie Sacco. U. S. War Department, Office of the Chief Signal Officer (Washington: Government Printing Office, 1941).
40. Ibid., p. 34.
41. Ibid.

42. Gioppi, op. cit., p. 2220.
43. ''Lock and Key,'' <u>MD</u>, Vol. 8, No. 10 (October 1964) 248.
44. F. M. Feldhaus, <u>Die Technik der Vorzeit, der geschichtlichen zeit und der Naturvolker</u> (Leipzig: Verlag von Wilheim Engelman, 1914), pp. 969–970.
45. Girolamo Cardano, <u>De Subtilitate libri XXI</u> (Basiliae: apud J. Petreium, 1560), pp. 1074–1076.
46. Silvestro Pietrasanta, <u>De Symbolis Heroicis</u> (Antwerp: Ex Officina Plantiniana Balthasaris Moreti, 1634), pp. 3, 254.
47. Arthur Vincent (ed.), <u>The Poems of Thomas Care</u> (New York: Charles Scribner's Sons, 1889), p. 128.
48. Alexander Dyce (Rev.), <u>The Works of Beaumont and Fletcher</u>, Vol. 1, (London: Edward Moxon, 1846), p. 183.
49. C. Vaudour, Conservateur-Adjoint, Musees De Rouen, Letter to author, February 17, 1976.
50. Pierre Larousse, <u>Grand Dictionnaire Universel Du XIX Siecle</u>, Vol. 13, (Paris: Libraire Classique Larousse et Boyer, 1873), p. 864.
51. Colonel Martel, Conservateur, Musee de l'Armee, Letter to author, January 20, 1975.
52. ''Rapport sur le cadenas a combinaisons du C. Regnier, garde des archives de l'artillerie,'' <u>Bulletin de la Societe d'Encouragement pour l'industrie Nationale</u> Premiere Annee, VII (Ventose An XI) 127.
53. Ibid., pp. 125–127.
54. <u>Encyclopedie Methodique</u>, Tome Septieme, Arts et Metiers Mecaniques (Paris: Chez Panckoucke, 1790), pp. 471–473.
55. Ibid., p. 472.
56. <u>Encyclopedie Methodique</u>, Tome Quatrieme, Recueil de Planches de L'Encyclopedie, Par ordre de Matieres (Paris: Chez Panckouke, 1785), p. 99.
57. <u>Encyclopedie Methodique</u>, Tome Septieme, op. cit., pp. 496–497.
58. Edme Regnier, <u>Description et Usage Du Cadenas De Surete a Combinaisons</u> (Paris: De l'Imprimerie de Madame Huzard, n. d.).
59. Claudine Fontanon, Chef de travaus, Centre De Documentation D'Histoire Des Techniques, Letter to author, January 20, 1976.
60. Sir Alexander Duff Gordon (trans.), <u>Sketches of German Life</u> by Vanhagen von Ense (London: John Murray, 1847), pp. 141–142.
61. Ibid.
62. Ibid.
63. Linton Knight, Rincon Key Company, Letter to author, February 5, 1975.
64. M. Jomard, ''Notice sur la vie et les Traveaux de feu M. Regnier, membre de Conseil d'administration de la Societe d'Encouragement,'' <u>Bulletin de la Societe d'Encouragement pour l'industrie Nationale</u>, CCLXV (July, 1826) 237.
65. Dumas Malone, <u>Jefferson and His Time</u>, Vol. Two (Boston: Little, Brown and Co., 1951), pp. 1, 243.
66. Kahn, op. cit., p. 192.
67. E. Millicent Sowerby (comp.), <u>Catalogue of the Library of Thomas Jefferson</u>, Vol. V (Washington: Government Printing Office, 1959), p. 149.
68. Ibid., p. 143.
69. Ibid., p. 147.
70. Ibid., pp. 143–147, 150.
71. Ibid., p. 150.
72. <u>Encyclopedie Ancienne</u>, Vol. II (Paris: M. Diderot, 1751), p. 512.

73. *Encyclopedie Ancienne*, Vol. IX, Recueil De Planches (Paris: M. Diderot, 1771), plate XXX.

74. Dumas Malone (ed.), *Dictionary of American Biography*, Vol. V, Part 2 (New York: Charles Scribner's Sons, 1961), p. 33.

75. Ibid.

76. Merrill D. Peterson, *Thomas Jefferson and The New Nation* (New York: Oxford University Press, 1970), p. 450.

77. Rosario Candela, *The Military Cipher of Commandant Bazeries* (New York: Cardanus Press, 1938), p. 69.

78. Ibid., p. 70.

79. Kahn, op. cit., p. 244.

80. *Biographie Universelle et Portative Des Contemporaines*, Tome Quatrieme (Paris: Chez F. G. Levrault, 1834), p. 1072.

81. Charles Babbage, *Passages from the Life of a Philosopher* (London: Longman, Green, Longman, Roberts and Green, 1864), p. 233.

A USER'S GUIDE IN VOICE AND DATA COMMUNICATIONS PROTECTION: BOOK REVIEW

Louis Kruh

Who, What and Where in Communications Security, Marketing Consultants International, Inc., 100 W. Washington St., Hagerstown, MD   21740, 1981, 124 pp.

This guide provides an in-depth look at the problem of electronic interception along with a discussion of the variety of techniques currently available for protecting facsimile, data, and voice communications utilizing the total range of transmission paths available. It contains a tutorial on the vulnerabilities of present day communications systems with details on scrambling and cryptographic fundamentals.

The non-technical reader is given information on the key issues involved in designing a communications security system with specific information about available products and their vendors. The real heart of the book is the product matrix section which lists a total of 35 national and international vendors offering 173 different products. The matrix is divided into sections for various types of protection needed, voice scrambler analog, voice encryption wideband, voice encryption narrowband, and data encryption.

The detailed product/feature matrix permits comparisons of competing products in relation to cost and interoperability issues. Specific information is given on product capabilities, sales outlets, manufacturing facilities and telephone numbers.

Also included is a listing of more than 500 terms with definitions and 200 acronyms commonly used in the communications security industry along with a comprehensive bibliography for additional readings.