The Evolution of Communications Security Devices

A look at ancient locks and cipher devices in the evolution of US Army cryptographic systems

by Louis Kruh

Author's Note: This article owes much to helpful people in various libraries and archives, both in this country and abroad. I also want to express my gratitude to David Kahn, author of the landmark book, The Codebreakers, for his encouragement, advice and assistance. My thanks also to Dr. Brian J. Winkel of Albion College for calling my attention to an obscure letter written by Charles Babbage. I would be pleased to hear from readers with further ideas or thoughts of this subject. (TAC readers can contact Mr. Kruh through the magazine office.)

Communications security is essential for any nation seeking to keep its military and diplomatic messages from being read by its enemies. Aside from basic measures of physical and transmission security, cryptographic security, which usually involves the use of ciphering devices to encrypt information, is one of the most important elements in communications security.

Cryptography is an ancient science with a fascinating history that touches on the lives of many famous people. In the United States, two of its long-used cryptosystems, the cylindrical and later the flat strip cipher devices, evolved through the ingenuity of several individuals.

M-94 and M-138-A

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 a widely used system in American cryptography. The two devices use the identical cryptographic principle: the simultaneous use of a number of different, sliding, mixed alphabets. Both played an important role in secret communications prior to and during World War II.

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

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.

The M-138-A works in a similar fashion. The device consists of a hinged aluminum board with 30 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.

The strips, inserted in the channels in a particular order designated by a key, slide from side to side. The encipherer aligns the plain text 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. The

Figure 1. US Army Cipher Device M-94.

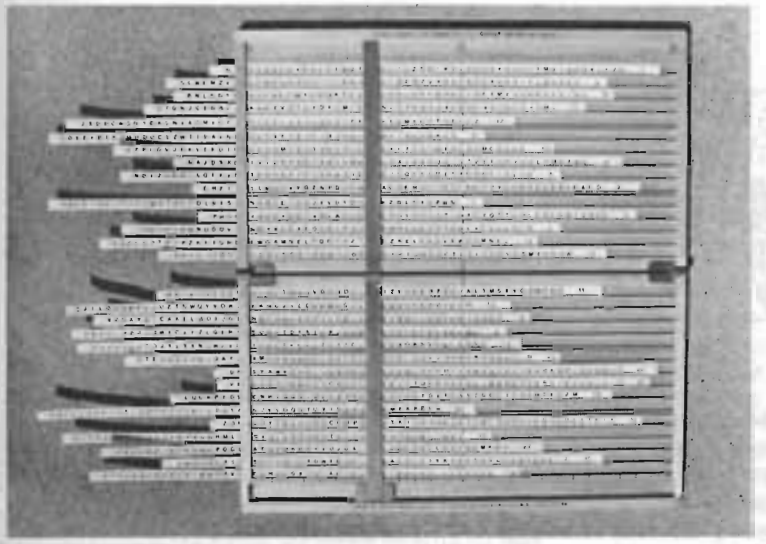


Figure 2. Cipher Device M-138A (Simulated Strips)

decipherer simply reverses the process after assembling the strips according to the key.

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 cylindrical version was officially adopted as a United States cryptosystem by the Army in 1921. 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 1919, naval attaches in 1930, and in 1939 it went to the Coast Guard under the title CSP 493.

The cipher device M-94 was used extensively between World Wars I and 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 Aug 9, 1943, when sufficient M-209s were available for replacement purposes, Cipher Device M-94 was declared obsolete.

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. 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.

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.

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. 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. All together, 17,872 flat strip cipher devices in all versions were ordered from 1935 through 1943.

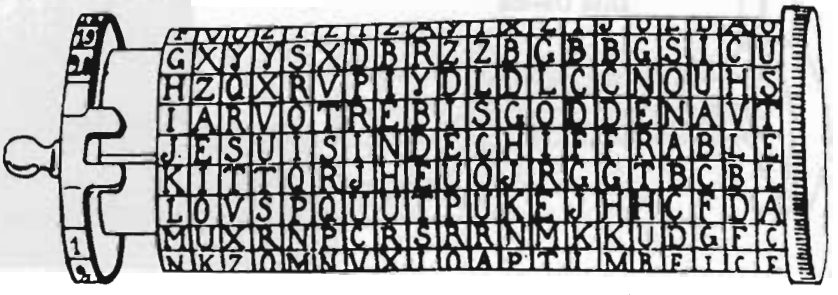
In addition to the Army and the Navy, strip cipher devices were used by almost a dozen different government agencies during the war. Strip cipher systems were also distributed to at least six foreign governments, including France, Italy and Russia, to maintain secure communications with US Army personnel.

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

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 . . . ." Another author, in 1967, wrote that the Navy also was using the strip cipher system at that time.

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

Figure 3. Bazeries' Drawing of his "Cylindrical Cryptograph"



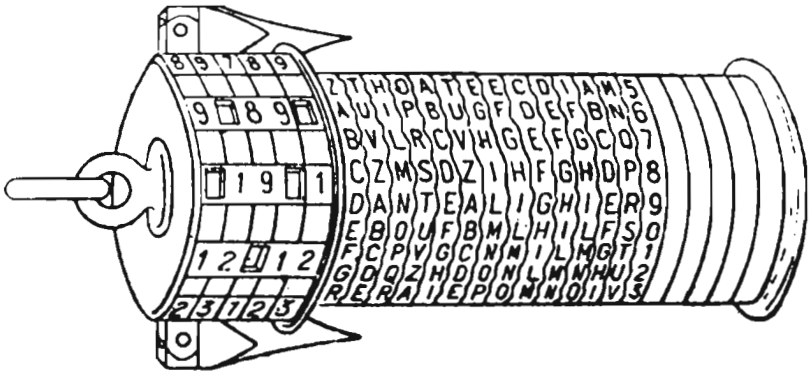


Figure 4. Ducros' Scotograph

Jefferson, Bazeries and Other Inventors

The device was invented, or apparently so, a number of times. Charles Babbage, the eminent mathematician, scientist and harbinger of the modern computer, hinted in the *Journal of the Society of Arts* in 1854 at a cylindrical-type device. He commented that a cipher system proposed by a reader in a previous issue was not new and that Babbage had made "the same thing in a series of pasteboard circles moveable around a common centre, each circle having on its circumference the twenty-six letters of the alphabet." He then wrote, "The best form is, perhaps, rings of box-wood placed side by side on a cylinder, and having the twenty-six letters on the circumference of each." But this reference, precise and early as it was, faded into obscurity.

Apparently independently, for he never mentions Babbage, whose work seems not to have been known to cryptographers of the time, MAJ Etienne Bazeries, a French cryptologist, developed a 20-disk mechanism (Figure 3). On Sep 19, 1891, he described it in Marseilles at the convention of the French Association for the Advancement of Science. And after it was rejected by the French army, he pictured and wrote about it in his book, *Les Chiffres Secret Devoiles.* 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 Sep 2, 1893, issue of *Revue Scientifique.*

In 1900, an article in *Rivista Militare Italiana* by Gioppi di Turkheim, a writer on cryptology, described the Ducros Scotograph, invented that year by COL Oliver Ducros of the Italian army. 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, CPT Parker Hitt, an instructor at the US Army Signal School, Fort Leavenworth, KS, created a 10-disk device. He acknowledged that his work was influenced by the ideas of Bazeries.

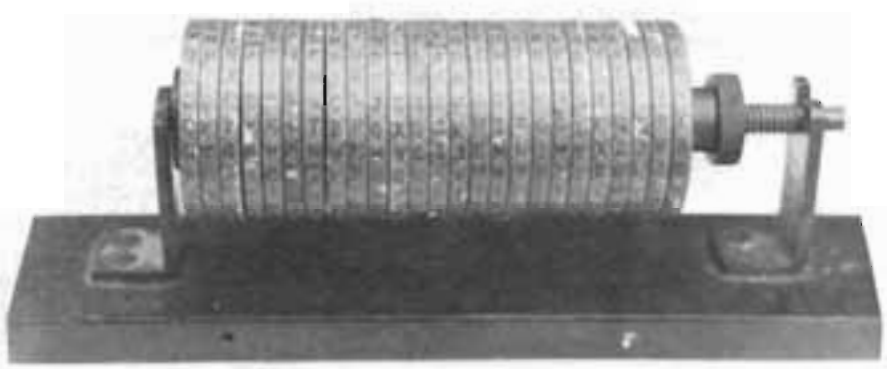
He then reinvented the strip cipher — he gives no evidence of having read Hermann's article. Since Hitt preferred the flat form because of its "compactness, simplicity of operation, and ease with which alphabet strips could be reproduced if lost," he abandoned his work on the cylindrical device. His first flat device had 20 alphabet strips, possibly because Bazeries' cylinder had 20 disks. But by 1916, it had expanded to 25 (Figure 5).

MAJ 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. He then had two 25-disk devices using these alphabets made in the Army Signal School shop in early 1917 (Figure 6). Mauborgne's work led directly to the M-94, Hitt's ultimately 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 revealed that before Babbage and Bazeries, Jefferson had invented a cipher device based on the same principle but using 36 disks, which he called his "wheel cypher." Despite its precocity, however, it seems never to have been used and so was lost to the world of cryptography.

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 alphabet 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.

Figure 6. One of Mauborgne's Original Models of his 25 Disk Device



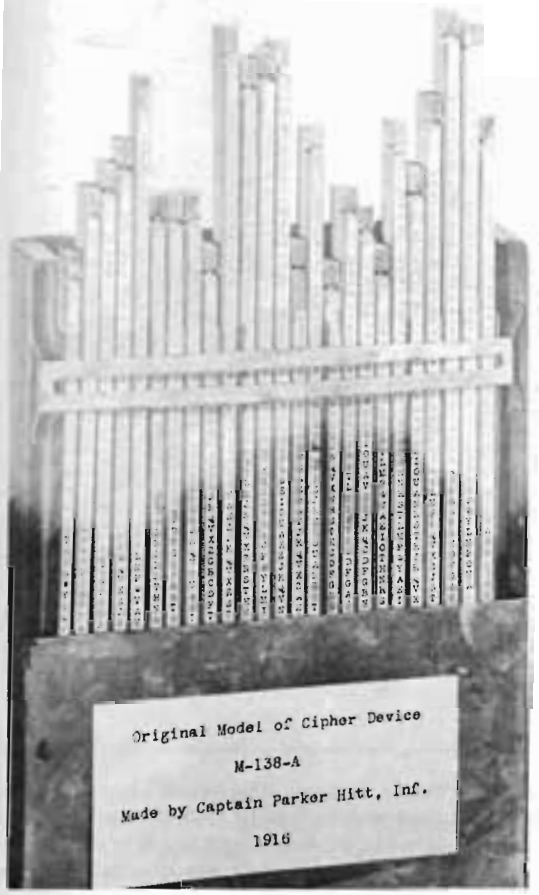


Figure 5. Hitt's Strip Cipher Device.

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?

Letter 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.

As I began to investigate this possiblity, I reread GEN Luigi Sacco's *Manual of Cryptography*, and the following sentence, not noted in previous readings, almost leaped out of the page: "The Bazeries device resembles very much one of those word padlocks which are used for locking some secret box." 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 padlocks."

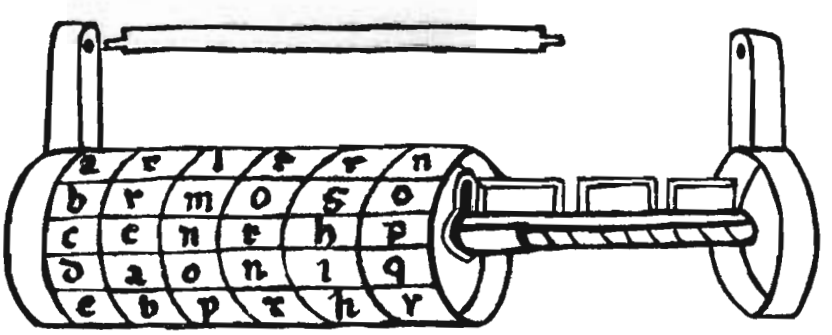
Gioppi, too, said the similar Ducros device "has no little analogy with the so-called word padlock (combination lock based on a word instead of numbers)." Obviously, cryptologists other than myself have seen the relationship between the wheel cipher and the letter lock. But how was the connection made?

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.

In the West, the letter lock dates back to at least the early 1400's (Figure 7). Knowledge of it seems never to have been lost. In the mid-1500's, Girolamo Cardano, a 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. Silvestro Pietrasantra's *De Symbolis Heroicis*, published in Antwerp in 1643, depicts two letter locks. 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."

The letter lock seems to have become well enough known for other writers in the 17th Century to allude to it. The poet, Thomas Carew, referred to it in his poem, "To my honoured Friend, Master Thomas May, upon his comedy, The Heir." And in their play, *Noble Gentlemen*, Beaumont and Fletcher wrote, "A cap-case for your linens and your plate,/With a strange lock that opens with AMEN."

Figure 7. Letter Lock Circa 1420



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

The device increased greatly in popularity during the last decade of the 18th Century and the first part of the 19th, 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 letter lock when necessary. Previously, the combination of a lock was fixed and, if it became known to others, it had to be discarded.

The Frenchman was Edme Regnier (1751-1825). With more than 70 inventions to his credit, he planned, organized and became the first director of the Artillery Museum in Paris. In 1777, he won first prize from the Societe libre d'Emulation de Paris for his invention of a

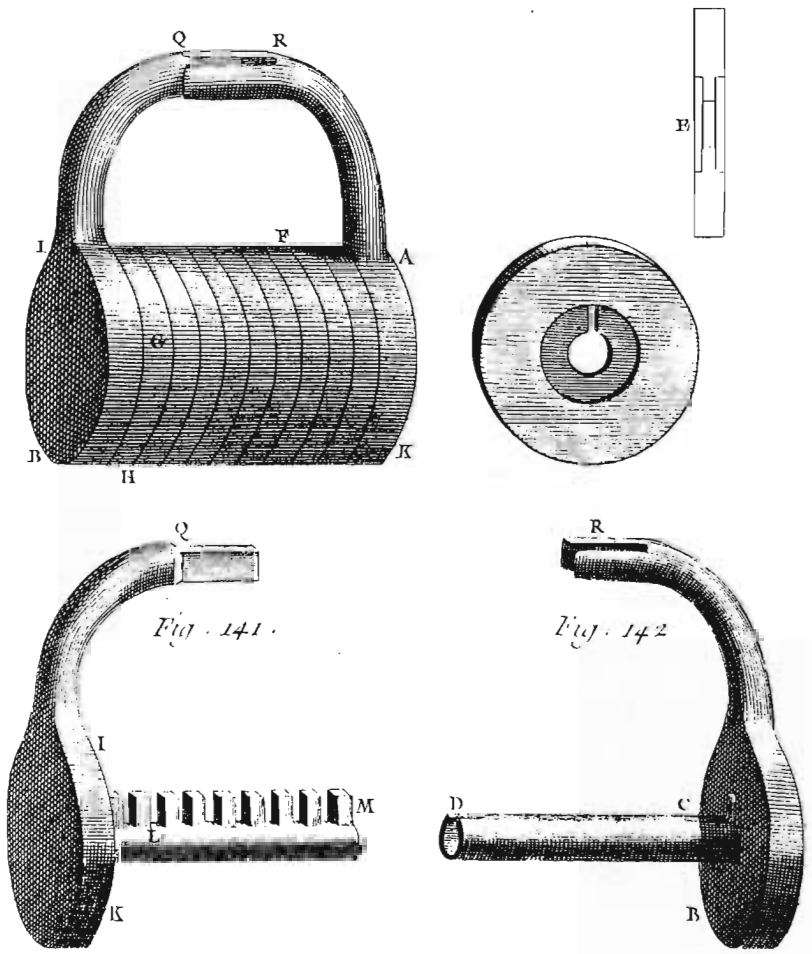
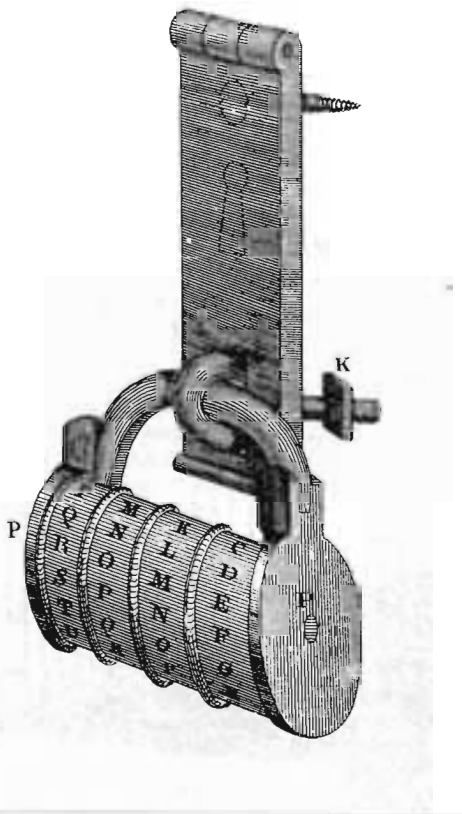


Figure 8. Combination Lock in the Encyclopedie Methodique

combination lock. Some years later he developed the letter lock or word padlock, possibly because a combination in the form of a word is easier to memorize than a string of numbers.

A description of his lock appeared in 1790 in Volume VII, *Arts et Metiers Mecaniques*, of *L'Encyclopedie Methodique*. The article pointed out that a picture was unavailable but, instead, furnished a thorough description of Regnier's invention: the lock had nine disks, each divided into 11 parts, containing the numbers 0 through 9 and a star. The article also described the 11-



disk combination lock that Regnier had improved upon, which was illustrated in Volume IV of the encyclopedia's plates series, published in 1785. Although its description indicates that figures and characters distributed on the circumference of the disks must be properly aligned for the lock to open, 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). One Regnier lock, similar to those in his pamphlet, is today in the Musee National des Techniques in Paris (Figure 10).

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," 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 another. 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 finding the right one.

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

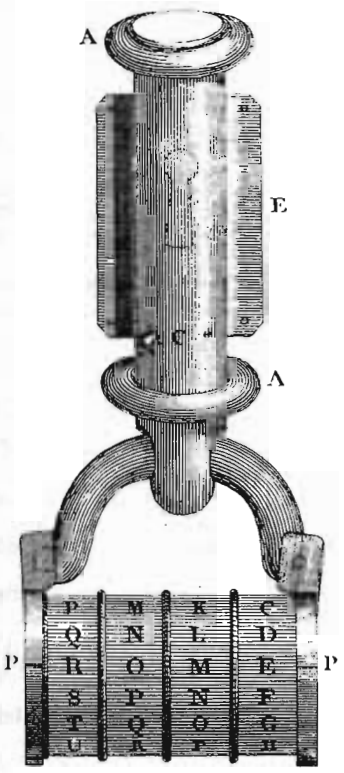


Figure 9. Illustration from Regnier's Pamphlet

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." When he became Secretary of State in 1789, he was in effect the country's first Superintendent of Patents and "he scrupulously . . . investigated every claim to satisfy the statutory test of originality."

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

Connections

Could Jefferson have known of Regnier's lock?

Chronology, first of all, permits it. Regnier arrived in Paris in 1778 and apparently spent the remainder of his life there. Jefferson went to France in 1784 and stayed for five years. According to Dr. Julius Boyd, editor of *The Jefferson Papers*, Jefferson wrote the description of his wheel cypher in the period of 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" of the *Encyclopedie Methodique*, which had first published a description of Regnier's lock. Jefferson's library included most of the encyclopedia volumes. 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.

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. 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. Volume II, published in 1751, carried a description of a "secret padlock"; and its picture in Volume IX, published in 1771, 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.

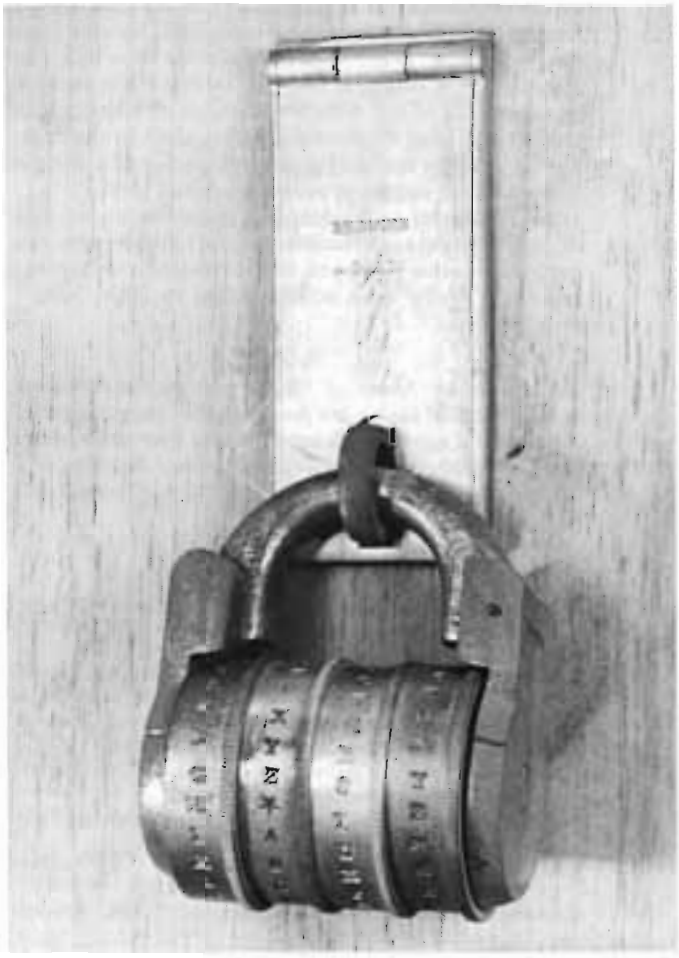


Figure 10. A Regnier Letter Lock in the Musee National Des Techniques

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, only 12 years after a biographical sketch of Regnier said his locks were in wide use. 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."

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 concepts: 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.

Editor's Note: Many of the sources in the following bibliographical listing are foreign publications; some of these should appear with accent marks over some letters for correct spelling and pronunciation. Because of a limitation in typesetting equipment, the staff was unable to print these accent marks.

BIBLIOGRAPHY

Babbage, Charles. *Passages from the Life of a Philosopher.* London: Longman, Green, Longman, Roberts & Green, 1864.

Bazeries, Etienne. "Cryptographe A 20 Rondelles-Alphabets (25 Lettres Par Alphabet)." *Compte rendu de la 20e session de l'Association Francaise pour l'Avancement des Sciences.* Paris: Au Secretariat de l'Association, 1892.

Bazeries, Etienne. *Les Chiffres Secrets Devoiles.* Paris: Libraire Charpentier et Fasquelle, 1901.

Biographie Universelle et Portative des Contemporaines. Paris: Chez F.G. Levrault, 1834. Tome Quatrieme.

Candela, Rosario. *The Military Cipher of Commandant Bazeries.* New York: Cardanus Press, 1938.

Cardano, Girolamo. *De Substilitate libri XXI.* Basiliae: Petreium, 1560.

Catalogue of the Library of Thomas Jefferson. Compiled by E. Millicent Sowerby. Washington,: GPO, 1959.

Dictionary of American Biography. Edited by Dumas Malone. New York: Charles Scribner

Dictionary of American Biography. Edited by Dumas Malone. New York: Charles Scribner's Sons, 1961. Vol V, Part 2.

di Turkheim, L. Gioppi. "La Crittografia." *Rivista Militaire Italiana.* December 16, 1900. Vol. 45, No. 12.

Dyce, Alexander. *The Works of Beaumont and Fletcher.* London: Edward Moxon, 1846. Vol. 1.

Encyclopedie Ancienne. Paris: M. Diderot, 1751 (Vol. II), 1771 (Vol. IX).

Encyclopedie Methodique. Paris: Chez Panckoucke, 1782-1832. 136 volumes.

Feldhaus, F. M. *Die Technik der Vorzeit, de geschichtlichen zeit und der Naturvolker.* Leipzig: Engleman, 1914.

Fontanon, Claudine. Chef de Documentation d'Histoire des Techniques. Letter to author, January 20, 1976.

Hermann, Arthur J. "Nouveau Cryptographe Construit d'apres le System Bazeries." *Revue Scientifique.* September 2, 1893. Tome LIII, No. 10.

Hitt, Parker, Cipher Papers. Letters from the David Kahn Collection.

Home Correspondence. *Journal of the Society of Arts.* September 1, 1854. Vol. II, No. 93.

Jomard, M. "Notice sur la vie et les traveaux de feu M. Regnier, membre de Conseil d'administration de la Societe d'Encouragement." *Bulletin de la Societe d'Encouragement pour l'Industrie Nationale.* July 1826. CCLXV.

Kahn, David. *The Codebreakers.* New York: Macmillan Co., 1967.

Knight, Linton. Rincon Key Company, Letter to the author, February 5, 1975.

Larousse, Pierre. *Grand Dictionnaire Universel Du XIX Siecle.* Paris: Libraire Classique Larousse et Boyer, 1873. Vol. 13.

"Lock & Key." *MD.* October 1964. Vol. 8, No. 10.

Malone, Dumas. *Jefferson and His Time.* Boston: Little, Brown and Company, 1951. Vol. 2.

Martel, Colonel. Conservateur, Musee de l'Armee. Letter to the author, January 20, 1975.

Peterson, Merrill D. *Thomas jefferson and the New Nation.* New York: Oxford University Press, 1970.

Pietrasanta, Silvestro. *De Symbolis Heroicis.* Antwerp: Ex Officina Plantiniana Balthasaris Moreti, 1634.

The Poems of Thomas Carew. Edited by Arthur Vincent. New York: Charles Scribner's Sons, 1889.

"Rapport sur le cadenas a combinaisons de C. Regnier, garde des archives de l'artilleriex." *Bulletin de la Societe d'Encouragement pour l'Industrie Nationale.* Premiere Annee. VII (Ventose AN XI).

Regnier, Edme. *Descriptions et Usage du Cadenas de Surete a Combinaisons.* Paris: De l'Imprimerie de Madame Huzard. No date.

Sacco, Luigi. *Manuel de Cryptographie.* Translated by J. Bres. Paris: Payot, 1951. Also translated by Howell C. Brown, US War Department, Office of the Chief Signal Officer. Washington: GPO, 1941.

US, War Department, Army Security Agency. *The History of Army Strip Cipher Devices.* 1948.

US, War Department, Office of the Chief Signal Officer. *Instructions for Using the Cipher Device M-94.* Washington: GPO, 1922.

US, War Department, Office of the Chief Signal Officer. "Edgar Allan Poe, Cryptographer (Addendum)," William F. Friedman. *Articles on Cryptography and Cryptoanalysis Reprinted from the Signal Corps Bulletin.* Washington: GPO, 1942.

Valdour, C. Conservateur-Adjoint, Musees de Rouen. Letter to the author, February 17, 1976.

von Ense, Vanhagen. *Sketches of German Life.* Translated by Sir Alexander Duff Gordon. London: John Murray, 1847.

Mr. Louis Kruh, a founding editor of CRYPTOLOGIA Magazine, is president of the New York Cipher Society. Interested in cryptology for more than 35 years, he is the book review editor of THE CRYPTOGRAM, the official publication of the American Cryptogram Association. Mr. Kruh holds a bachelor's degree from the City College of New York and a master's degree from Pace University. He is a public relations executive with New York Telephone.