The Roots of Modern Cryptography: Leon Battista Alberti's "*De Cifris*"

Stefano Selleri

Department of Information Engineering
University of Florence
Via di S. Marta, 3, 50139, Florence, Italy
E-mail: Stefano.selleri@unifi.it

Abstract

hile cryptography is almost as old as writing, its earliest applications were rather trivial and relatively easily broken via statistical analysis, as Al-Kindi proved in the VIIIth century. Modern ciphers deceive statistical analysis thanks to complex algorithms and ciphering keys. The very first concept of these can be found in a 1466 manuscript by Leon Battista Alberti, the importance of which was for many years overlooked. This paper focuses on the work by Alberti and its impact, within the framework of a brief and necessarily incomplete history of cryptography.

1. Introduction

Cryptography is the practice of enciphering and deciphering of messages in secret code in order to render them unintelligible to all but the intended receiver. While this art is very old, as the second section of this contribution briefly summarizes, ciphers were elementary and hence easy to break. Indeed, it is astonishing for we moderns that the greatest general of antiquity, Julius Caesar, sometimes simply wrote his message in Latin but using the Greek alphabet, since there was no one among his enemies that knew the Greek alphabet [1]:

> ...ibi ex captivis cognoscit, quae apud Ciceronem gerantur quantoque in periculo res sit. Tum cuidam ex equitibus Gallis magnis preamiis persuadet, uti Ciceronem epistulam deferat. Hanc Graecis conscriptam litteris mittit, ne intecepta epistula nostra ab hostibus consilia cognoscantur...
>
> ...there, he [Caesar] learns from the prisoners what is happening near Cicero and what danger he is in. Hence he convinces with great rewards a knight of the Gauls to bring a letter to Cicero. He writes the letter in Greek characters so that if it falls into enemy hands it does not reveal his plans...

Even if Caesar also used a more-refined technique, he, as all ancient and middle-aged people, used what is called *mono-alphabetic* substitution. This is easy to break if the message is long enough and the language in which the clear text is written is known.

It was in the Renaissance that we had a true leap forward in cryptography, when Leon Battista Alberti developed the ideas of a substitution cipher that changes *within* a same message. He thus invented *poly-alphabetic* substitution; *super-enciphering*, which further reduces the chances of statistical analysis; and a ciphering disk able to automate the ciphering-deciphering process.

The concepts of Alberti were sadly not finalized into a truly secure algorithm, and his contributions were overlooked by contemporaries. Some of his ideas were indeed for long credited to Blaise de Vigenere, who, on the other hand, in 1586, gave practical instructions for poly-alphabetic ciphering. Indeed, the ideas of Alberti were behind all mechanical ciphering algorithms, the most complex of which are the crypto machines *Enigma* and *Lorenz*, developed in Germany during World War II.

2. Ancient Cryptography

The oldest way of conveying a ciphered message of which we have historical evidence is the scytale, used by the Spartans and described by Plutarch [2]. This consisted of a rod on which a thin strip of parchment was wound, with letters written along its axis, one per wind of the strip. The receiver, having a rod of the same diameter, was able to immediately reconstruct the message (Figure 1). Plutarch wrote that Lysander [Sparta, Greece, c. 441 B.C.[1]– Haliartos, Greece, 395 B.C.] was reached in 404 B.C. by a wounded messenger, the only one of five that survived the crossing of Persian territory. The messenger handed his belt to Lysander, who wound it along his scytale to read that Farnabazo was planning to attack him. Lysander hence had the time to prepare his army and eventually won the battle.

To remain in Greece, Polybius [Megalopolis, Greece, ca. 200 B.C. – Somewhere in Greece, 118 B.C.] suggested

1 For the sake of simplicity, only before Christ (B.C.) will be indicated in dates; when no specification is given, Anno Domini (A.D.) is implied and suppressed.

Figure 1a. A reconstruction of a scytale.

	1	2	3	4	5
1	A	B	Γ	Δ	E
2	Z	H	Θ	I	K
3	Λ	M	N	Ξ	O
4	Π	P	Σ	T	Y
5	Φ	X	Ψ	Ω	

Figure 1b. Polybius' table.

the usage of a "matrix" of characters named the *Polybius Square* (Figure 1), where the coding of messages was done using the row-column numbers of each letter [3]. Due to the limited number of symbols (the numbers 1 to 5), this was a code that could also be used for optical-torch-based communications.

In ancient bibles, some words were ciphered using one of the oldest examples of a substitution cipher, or ATBSH. This was obtained by substituting the first letter of the Aramaic alphabet (Aleph) with the last (Taw), the second (Beth) with the penultimate (Shin), and so on. In practice, this was a mono-alphabetic substitution with a reversed alphabet.

The first widespread use of a substitution cipher in military applications appeared in the writings of Gaius Julius Caesar [Rome, Italy, 13 July 101 B.C. – Rome, Italy, 15 March 44 B.C.] (Figure 2), where the second alphabet was not reversed as in the ATBASH cipher, but rather shifted by a pre-determined number of letters [4]. This *shift mono-alphabetic substitution* remained the best ciphering method for all antiquity and the Middle Ages. Mono-alphabetic ciphers, even more general than Caesar's – since they exploited *shuffled* alphabets, not just shifted alphabets – were also found, for example, in India. The art of *Mlecchita vikalpa* is a mono-alphabetic ciphering with a shuffled alphabet, and is credited to date back to the IVth century B.C., as it was cited even if not detailed among the 64 arts that should be studied by learned people in the *Kāma Sūtra* [5].

During the Middle Ages, no significant evolution in ciphering techniques took place, but Arabs were working on code breaking. The oldest treatise on this was due to Al-Kindi [Kufa, Iraq, ca. 801 – Baghdad, Iraq, ca. 873] (Figure 2) who proved how code breaking for simple mono-alphabetic substitution was relatively easy if the language of the original message is known, and a statistical analysis is applied to the ciphered message and checked against the letter frequencies in such a language [6].

3. The Renaissance of Cryptography: Leon Battista Alberti

Leon Battista Alberti [Genoa, Italy, 14 February 1404 – Rome, Italy, 25 April 1472], was a polymath as were many Renaissance geniuses: architect, historian, humanist, mathematician (Figure 3).

Figure 2a. Gaius Julius Caesar.

Figure 2b. Abū Yūsuf Yaʿqūb ibn Isḥāq al-Kindī.

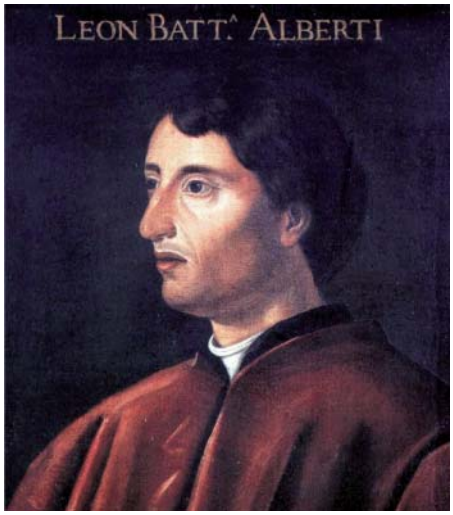


Figure 3a. A painting depicting Leon Battista Alberti (Uffizzi Gallery, Florence), attributed to Cristofano Dell'Altissimo, who never met Alberti, being born in 1525.

Figure 3b. The statue of Leon Battista Alberti in the Uffizzi front porch, were the statues of 28 eminent people of the Florentine Renaissance are on show. The statue is by Giovanni Lusini, sculpted in 1850.

Although born in Genoa, his parents were rich merchants from Florence and banned from the city for political reasons, which was quite common in Italy in the Middle Ages and the Renaissance. He studied in Venice and then in Padua, at the school of the humanist Gasparino Barzizza, where he learned Latin and perhaps also Greek. He then moved to Bologna, where he studied law, simultaneously dedicating himself to music, painting, sculpture, mathematics, and literature.

After the death of his father (1421), Alberti had some hard years because his relatives did not want to recognize his hereditary rights nor favor his studies. Anyway, he actually graduated in law (1428). In his years in Padua and Bologna, he befriended many important intellectuals such as Paolo Dal Pozzo Toscanelli and Tommaso Parentuccelli (future Pope Nicholas V). He was then in Rome (1431-1433) and, after the ban on his family was relieved, in Florence and Ferrara (1434-1443). He was then returned to Rome, but continued working in Florence, Rimini, and Mantua, from 1444 up to his death.

Most celebrated as an architect, he designed the Tempio Malatestiano in Rimini, conceived the main square in Pienza, and the churches of Sant'Andrea and San Sebastiano in Mantua. In Florence, he designed the upper facade of Santa Maria Novella church and of Palazzo Rucellai (Figures 4 and 5). He also designed part of the San Martino a Galgalandi parish, next to Florence. Alberti was actually rector of the parish from 1432 up to his death.

Figure 4. The Palazzo Rucellai.

Figure 5. The Santa Maria Novella: the facades in both Figures 4 and 5 were designed by Leon Battista Alberti in Florence.

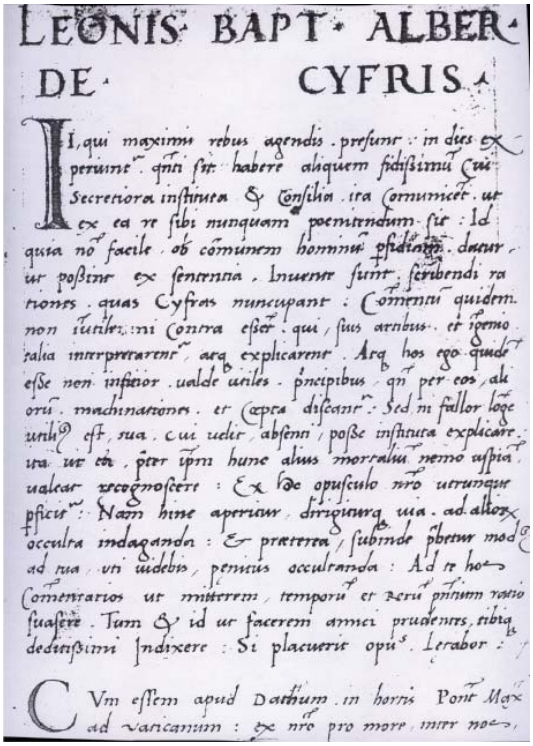

LEONIS BAPT. ALBER-
DE CYFRIS

Figure 6. The first page of one of the existing manuscripts of [10]. Note that in this case, the title was spelled "Cyfris," while the usual spelling is "Cifris."

Agnolo Pandolfini, a close friend of Alberti, was buried there. Alberti actually lived of these prebendary, which were not limited to San Martino a Galgalandi, while he worked for the pope as an *Abbreviator*, a writer of the Papal Chancery who adumbrated and prepared in correct form Papal bulls, briefs, decrees, etc. Leon Battista Alberti was indeed also a writer, among the first in the Renaissance to write on arts. His main literary works were on architecture [7], painting [8], and sculpture [9].

However, among the many other activities, in 1466 or 1467 (the date is uncertain), Alberti composed a text on cryptography [10]. Fifteen manuscript copies of this are still existent, each with slight differences, also in the title, due to copyists. An English translation is available [11]. The relevance of the text was underestimated up to the XXth century. While it was known for the first description of the cipher disk, it also contains a refined analysis of the language, aimed both at deciphering – as it was in the Al-Kindi treatise [6] – and at improving ciphering, by providing important new contributions [12].

The incipit of the text clearly states the aims of Alberti: to provide governors with a way to communicate in a secure way with their most trusted collaborators (Figure 6). In particular, two ideas were notable: the idea of using a *poly-alphabetic* cipher in place of the weak, mono-alphabetic, Caesar's code in use up to Alberti time; and the idea of *super-encipherment*.

Poly-alphabetic ciphering means that when ciphering the text, the ciphering alphabet is *changed* during encoding. If cleverly used, this makes frequency analysis impossible, since a same letter is translated into a different letter by each different ciphering alphabet. Alberti was not very practical, and proposed to change the code at random – which is smart – every two or three words, and to indicate the change in rotation in his disk within the ciphered message – which is less smart, indeed, an unexpected letter in writing that could easily give hints to attackers.

Super-encipherment, in Alberti's concept, is to substitute common phrases with numbers, up to four digits, but containing only the digits from 1 to 4 contained in the disk. This even more messes up the frequency of letters and avoids frequency-based code breaking.

Alberti wrote about the disk description [10]:

Scribendi autem ratio occultissima et commodissima, quam imprimis probemus, haec est. Facio circulos duos duabus tabellulis aeneis, unum maiorem qui stabilis

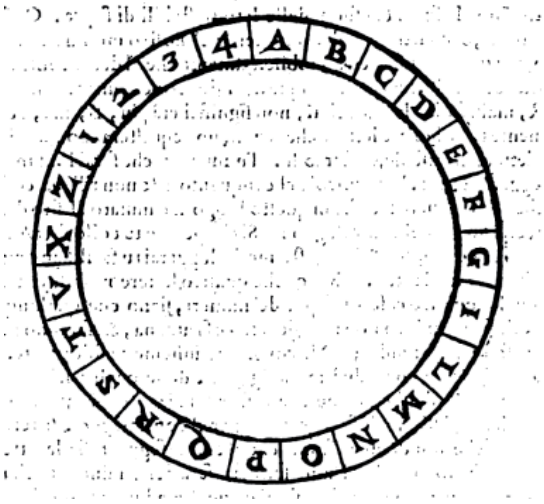


Figure 7a. Alberti's disk from the first printed edition of the *De Cifris*.

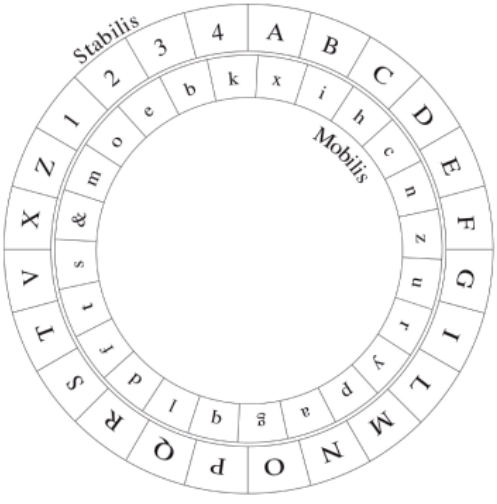


Figure 7b. Alberti's disk from its critical online edition [10].

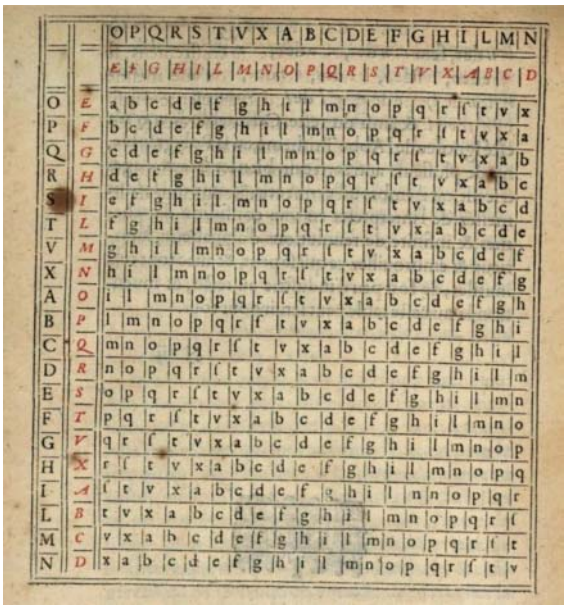


Figure 8. The Vigenère ciphering table, from a XVIIth century edition of [15].

dicitur, alterum minorem quem appellamus mobilem. Excedit autem stabilis mobilem ex suae diametri parte nona. Totas circumferentias amborum circulorum divido in partes coaequales quattuor et viginti. Hae partes domicilia nuncupantur.

The way for writing secret and safely, which we prove, is this. I fabricate two rings from two sheets of brass, one larger, which we call fixed, the other smaller, which we term movable. The fixed diameter is one ninth larger than the movable. I divide the circumferences of them both in twenty-four equal parts. These parties I call homes.

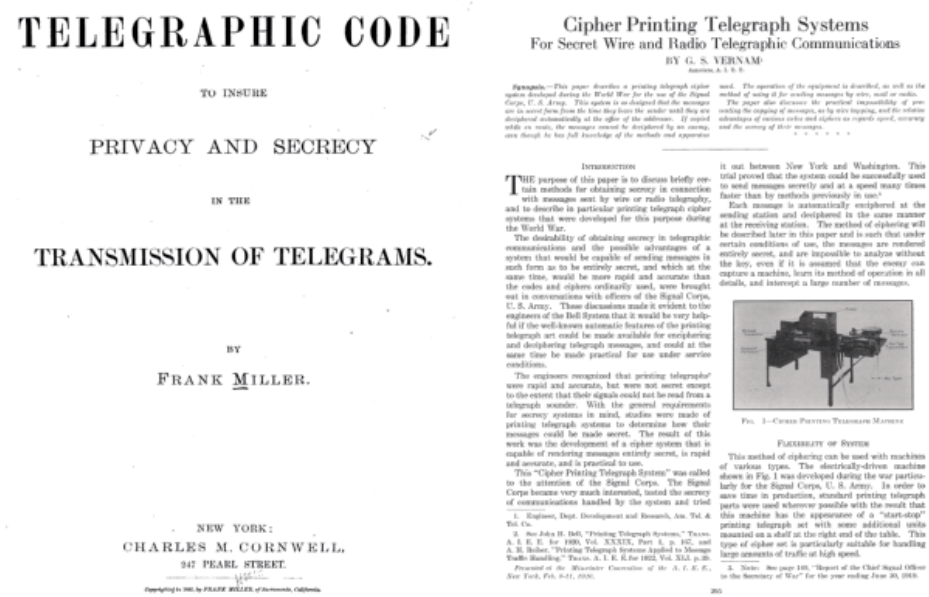
There then followed a rather lengthy description of the utilization of the disk, a reproduction of which is in Figure 7, and of which we give only a couple of citations:

Prius de indice mobili. Sit verbi gratia inter nos constitutus index ex mobili tabella k. Statuam tabellam formulae uti quidem scribenti mihi libuerit, puta ut k ipsa statuta sub maiuscula B et sequens sub sequenti. Ad te igitur scribens primam omnium scribam B maiusculam sub qua indicem k in formula scripturus posuerim; id indicabit ut id quoque tu in provincia volens nostra legere, formulam quae apud te gemella est versionibus aptes usque sub B itidem sit index ipse k. Hinc demum caeterae omnes litterae minores in epistola inventae superiorum stabilium vim et sonos significabunt

The case of the mobile disk. Let there be among us, and shall be established, for example, the index ask of the movable disk. And I have established the formula, for example, that k is under the uppercase B and the following letters follows. So I write you first letter B uppercase, to let you know that index k is under it; so that it will tell you that you, far away, wanting to read my message, having an identical device, set the formula where B corresponds to the index k. Finally, all other literature were found under the letter sounds indicate the upper permanent force

Then, about changing the alphabet:

Cum autem tres quottuorve dictiones exscripsero mutabo nostra in formula situm indicis versione circuli, ut sit index ipse k fortassis sub R. Ergo in epistola inscribam maiusculam R inde igitur k significabit non amplius B sed R et quae sequentur singulae superiorum stabilium


TELEGRAPHIC CODE

TO INSURE

PRIVACY AND SECRECY

IN THE

TRANSMISSION OF TELEGRAMS.

BY

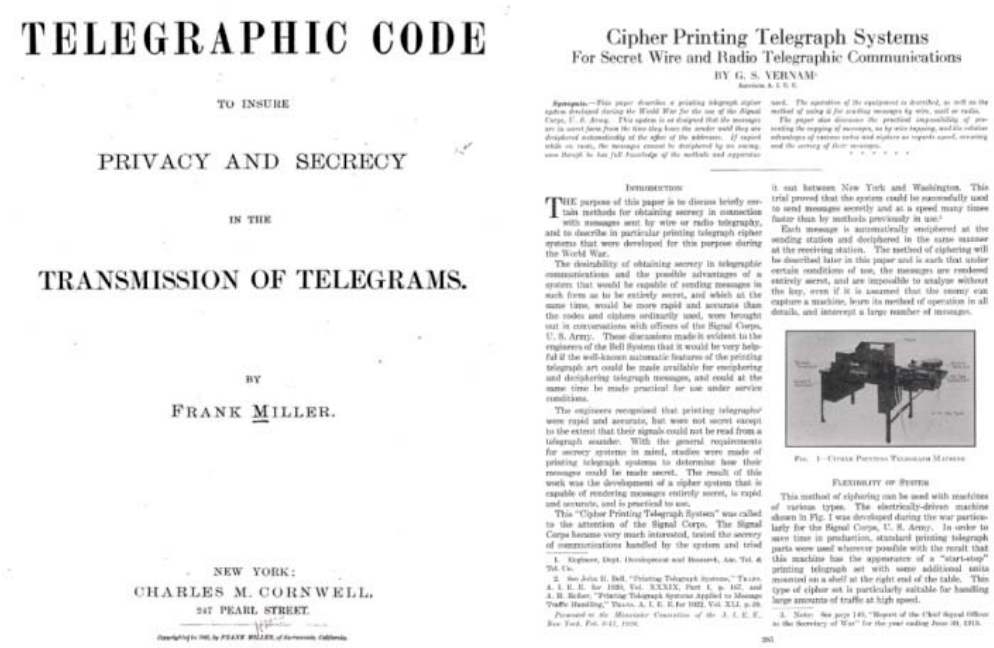
FRANK MILLER.

NEW YORK:
CHARLES M. CORNWELL,
247 PEARL STREET.

Cipher Printing Telegraph Systems
For Secret Wire and Radio Telegraphic Communications

BY G. S. VERNAM

Figure 9. The first pages of Miller's book [18] and the Vernam article [19] introducing perfectly secure coding.



TELEGRAPHIC CODE

TO INSURE

PRIVACY AND SECRECY

IN THE

TRANSMISSION OF TELEGRAMS.

BY

FRANK MILLER.

NEW YORK:
CHARLES M. CORNWELL.
247 PEARL STREET.

Cipher Printing Telegraph Systems
For Secret Wire and Radio Telegraphic Communications

BY G. S. VERNAM

Figure 10. (l) The first pages of the papers by Miller (1882 [18]) and (r) by Vernam (1926 [19]).

novissima suscipient significata.Tu idem in provincia interlegendum admonitus inventa maiuscula eam scies nihil aliud importare ex se nisi ut moneat mobilis circuli situm atque indicis collocationem isthic esse immutatam. Ergo tu quoque sub ea indicem collocabis, eo pacto facillime cuncta perleges et perdisces.

Having written three or four words I will change our formula of the position of the index of the circle, so that the index k is for example under R. Hence I will write an uppercase R. From now on k will mean R and not B any more and letters following will have new meanings. You, far away, will find an uppercase letter with no meaning, except that it is to notify itself and to imply a change of the movable disk. Therefore if you place that letter under the index k, this way it is very easy to read.

Indeed in this case what will be later known as the "key" of the cipher is a single character. The rule for changing the alphabet is random, which is not very strong since whomever had read the treatise could decipher the message with just 26 guesses, at worst, on the first key! A slightly better cipher is given later on, where it is the fixed (uppercase) letter to be fixed and changes are better hidden in the ciphered text. This is the weakest point in a treatise, which, on the other hand presents the brightest idea in cryptography that occurred in the last fifteen centuries [13, 14] and which, sadly, went overlooked.

It was Blaise de Vigenère [Saint-Pourc¸ain-sur-Sioulè, France, 5 April 1523 – Paris, France, 19 February 1596], more than a century later, who had success in promoting poly-alphabetic ciphering [15]. His approach consisted in agreeing on a keyword, and repeating it as much as the string is as long as the message, then for each letter in the message the ciphering alphabet is selected as the row of the table in Figure 8. In this way the same letter is ciphered with a *different* letter, based on its position relative to the keyword.

The weak points here are that the number of alphabets used for coding is small (equal to the number of letters in the keyword), and that the same letter is coded the same way if it occurs in correspondence of the same letter of the keyword. As a result, ironically, even if Vigenere's table-based code gained exceptional notoriety and was considered unbreakable, it was indeed weaker than Alberti's more "random" approach, where the substitution alphabet was not changed on a regular basis. The Vigenere code was indeed used even for many years after Friedrich Wilhelm Kasiski [Schlochau, Poland, 29 November 1805 – Neustettin, Poland, 22 May 1881] published his algorithm for deciphering poly-alphabetic ciphers [16].

4. Modern Times

The Vigenere code, and in general all poly-alphabetic ciphers with a "short" key, can be attacked via the Kasiski approach. This first discovers the length of the key and then applies frequency analysis separately to each alphabet. The Kasiski approach is useless if the key is infinite in length or, as is the same, if it is as long as the message, but never repeating. Such an idea was due to Frank Miller [1842 – 1925][2] [18] (Figure 10), even if it is commonly credited to Gilbert Sandford Vernam [Brooklyn, New York, 4 April 1890 – Hackensack, New Jersey, 7 February 1960] (Figures 10 and 11), who indeed gave a full algorithm [19]

[2] Miller could have been born in Milwaukee, Wisconsin, but indeed this information, as well as full dates, are unknown [17].

Figure 11a. Gilbert Sandford Vernam.

Figure 11b. Arthur Scherbius.

The weak point for these algorithms lies in the necessity of sharing the key, which must be long, truly random, and used only once. However, the strong point, as Claude Elwood Shannon [Petoskey, Michigan, 30 April 1916 – Medford, Massachusetts, 24 February 2001] proved, is that it is absolutely secure [20].

In the meantime, Arthur Scherbius [Frankfurt, Germany, 30 October 1878 – Berlin, Germany, 13 May 1929](Fig. 11) patented on 23 February 1918 a cipher machine based on rotating wired wheels [21] (Figure 12). This was a "rotor machine" that was to put pen and paper back in the drawer of cryptographers. His "model A" was quite large, followed by Model B. Finally, with Model C, the machine was fully portable and letters were indicated by lamps. He called his machine *Enigma*, which is the Greek word for "riddle," and aimed it at the commercial market. The German Navy adopted it in 1926, and the German army and aviation adopted it a few years later.

Scherbius' Enigma provided the German Army with the strongest cryptographic cipher in the world at that time, and the military communications of the Germans were optimally protected during World War II. The disks of the machine (Figure 12) indeed performed a simple mono-alphabetic cipher, but the key idea of Scherbius was to have the disk rotate by one step after each letter. This would call for a poly-alphabetic cipher with a (fixed) key as long as the disk. To improve security, there were three disks (and more in later modified models) so that the second disk would advance one step after a full turn of the first, and the third would do one step after a full step of the second. This, given the 26 letters of the alphabet, leads to a key 17576 characters long. The introduction of a reflector, forcing the letter to go through and back the three disks, added complexity and allowed symmetric utilization. Writing a clear message gave a ciphered one; typing a ciphered message gave back the clear message.

Finally, by selecting the initial position of the rotors on the basis of a three (or more) pre-determined letter keyword, the coding was made stronger, since a different ciphering scheme would be used on a daily basis. Furthermore, a set of plugs allowed the further exchange of some letters (Figure 12).

Deciphering the Enigma is a many-times-told story [21, 22], first done by Polish mathematicians and then by Alan Mathison Turing [London, England, 23 June 1912 - Wilmslow, England, 7 June 1954] at Bletchley

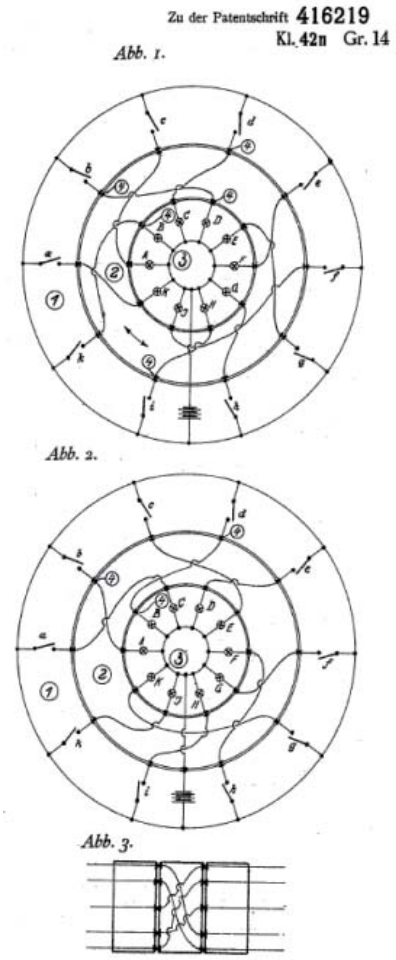


Figure 12a. A schematic of the rotor of the Enigma machine, from the original patent [20].

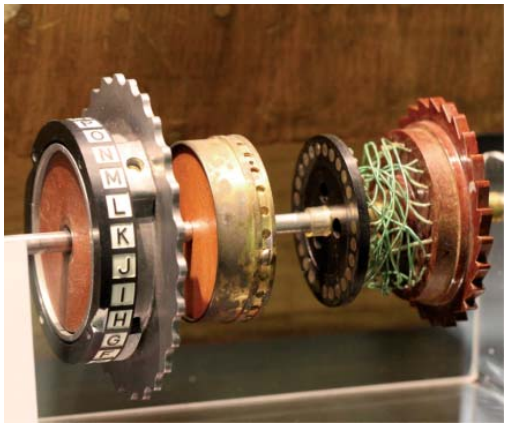


Figure 12b. An exploded view of a rotor of the Enigma machine, showing wires and contacts.

Park in England. This was possible not so much because of a weakness in the Enigma machine, but because of weaknesses in its usage, with repetition in words within the same message and phrases repeated identically in different messages. This allowed the decryption of German Air Force messages, which proved weaker, since 1939 with a limited success, and then, with increasing success in the following years, up to a pace of 4000 messages per day.

The German Navy Enigma was harder to decode, due to more rigid security procedures applied. The capture from U-110 in 1941 and U-599 in 1942 of working Enigma machines with three and then four rotors and relative codebooks for U-boats by the Royal Navy helped a lot [23].

The German Lorenz SZ40/42 also worked on a very similar principle, but with 12 rotors and an alphabet of 32 symbols represented as binary digits. This was stronger than Enigma, and thanks to the binary code, the receiving machine could print the message in clear without assistance. However, it was too cumbersome to replace Enigma on the battlefield or in vehicles. Breaking Lorenz's cipher was also done, but humans needed four days to decipher a message, which made the information too old to be useful. When Colossus, the first programmable computer, came into play (1944), fast decryption of the Lorenz code was possible, and this indeed marked the birth of electronic computing.

Of course, cryptography did not end with World War II. Indeed, it is everyday more important to secure Internet transactions. The weak points of Vernam codes and other codes – that is, the necessity of sharing a key – have been resolved by public-key cryptography, conceived by Martin Hellman [New York, New York, 2 October 1945], Ralph Merkle [Berkley, California, 2 February 1952], and Whitfield Diffie [Washington, DC 5, June 1944], late in the seventies [24, 25]. These are the strongest ciphers currently used.

Figure 12c. A three-rotor Enigma machine (probably 1939).

5. Conclusion

Even if now surpassed, Alberti's work was a leap forward in cryptography. Its importance could be equaled only by public-key coding, since variations over the poly-alphabetic substitution introduced by Alberti, and popularized by Vigenère, were at the basis, with their strengths and weaknesses, of all ciphering techniques up to a few decades ago.

6. References

1. G. J. Caesar, *Commentaries on the Gallic War, Book V*, 48.2-4 – 58-50 B.C., available online https://la.wikisource.org/wiki/Commentarii_de_bello_Gallico/Liber_V#48

2. Plutarch, *Lives of the Noble Greeks and Romans: Lysander*, end I c. - beginning II c., available online http://classics.mit.edu/Plutarch/lysander.html

3. Polybius, *The Histories, Book X*, 45.6, II c. B.C., available online https://penelope.uchicago.edu/Thayer/E/Roman/Texts/Polybius/10*.html#45.6

4. Suetonius, *The Twelve Caesars: Caesar*, 119-122, available online https://penelope.uchicago.edu/Thayer/E/Roman/Texts/Suetonius/12Caesars/Julius*.html

5. Vatsyayana, *Kāma Sūtra*, IV c. B.C., available online https://freeditorial.com/en/books/the-kama-sutra

6. Al-Kindi, *On Extracting Obscured Correspondence*, manuscript, VIII c.

7. L. B. Alberti, *De Re Aedificatoria*, manuscript 1450, first printed ed. 1541, Argentorati (now Strasbourg), France: M. Iacobus Cammer.

8. L. B. Alberti, *De Pictura,* manuscript 1435, first printed ed. 1540, Basel, Switzerland.

9. L. B. Alberti, *De Statua,* manuscript 1464, first printed ed. 1568, Venice, Italy, Francesco Franceschi (within a larger collection of Alberti works).

10. L. B. Alberti, *De Cifris*, manuscript, 1466 or 1467, first printed ed. 1568, Venice, Italy, Francesco Franceschi (within a larger collection of Alberti works), available online http://www.apprendre-en-ligne.net/crypto/alberti/decifris.pdf.

11. L. B. Alberti, *A Treatise on Ciphers, trans. A. Zaccagnini. Foreword by David Kahn*, Torino: Galimberti, 1997.

12. G. Pelosi and S. Selleri "Florence and a Leap in Cryptography: The Leon Battista Alberti Cypher Disk," *IEEE HISTELCON 2021*, Moscow, Russia, 10-12 November 2021.

13. D. Kahn, "On the Origin of Polyalphabetic Substitution," *Isis*, **LXXI**, 1980, pp. 122-127.

14. N. Galimberti, "Il De componendis cyfris di Leon Battista Alberti tracrittologia e tipografia," *Digest of the Conference "Subiaco culla dellastampa,"* Abbazia di Santa Scolastica, Subiaco, Italy, 2006-2007.

15. B. de Vigenère, *Traicté des chiffres ou secrètes manières d'escrire*, Paris, France: Abel L'Angelier, 1586.

16. F. W. Kasiski, *Die Geheimschriften und die Dechiffrir-Kunst*, Berlin, Germany: E. S. Mittler und Sohn, 1863.

17. S. Bellovin, *Frank Miller: Inventor of the One-Time Pad*, Columbia University, *Cryptologia*, **35**, 2011, pp. 203-222.

18. F. Miller, *Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams*, New York, New York, Charles M. Cornwell, 1882.

19. G. S. Vernam, "Cipher Printing Telegraph Systems for Secret Wire and Radiotelegraphic Communications," *J. Amer. Inst. Elect. Eng.*, **XLV**, 1926, pp.109-115.

20. C. Shannon, "Communication Theory of Secrecy Systems," *Bell System Tech. J.*, **28**, 1949, pp. 656-715 [preceded by a classified report in 1945].

21. A. Scherbius, *Reichspatent 416219*, Kl. 42n, Gr. 14, 23 February 1918.

22. D. Turing, *X, Y & Z, The Real Story of How Enigma Was Broken*, Stroud, England, The History Press, 2018.

23. N. Cawthorne, *Alan Turing, The Enigma Man,* London, England, Arcturus, 2014.

24. D. Kahn, *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943*, New York, New York, Barnes & Noble, 1991.

25. W. Diffie and E. M. Hellman, "New Directions in Cryptography," *IEEE Trans. Information Theory*, **22**, 1976, pp. 644-654.

26. R. C. Merkle, "Secure Communications Over Insecure Channels," *Communications of the ACM*, **21**, 1978, pp. 294-299.