On the Origin of Polyalphabetic Substitution
Author(s): David Kahn
Source: *Isis*, Vol. 71, No. 1 (Mar., 1980), pp. 122-127
Published by: University of Chicago Press on behalf of History of Science Society
Stable URL: http://www.jstor.org/stable/230316
Accessed: 07-03-2016 03:42 UTC

NOTES & CORRESPONDENCE

ON THE ORIGIN OF POLYALPHABETIC SUBSTITUTION

*By David Kahn**

In an article forty years ago, Charles J. Mendelsohn first described the evolution of the most widely used cipher system in the world, polyalphabetic substitution.[1] In its various forms, this system serves today in the computerized electronic cipher machines of the U.S. Government, in the mechanically marvelous Hagelin cipher machine that almost one hundred nations employ to keep their official communications secret, and in the postage-stamp-sized one-time pads of spies. During World War II, the Japanese PURPLE and the German Enigma machines, which the Allies cracked to contribute so much to their war efforts, both embodied forms of polyalphabetic substitution.[2]

Mendelsohn traced the cipher from its first appearance in a small treatise of about 1466 by Leon Battista Alberti (1404–1472),[3] one of the world's true polymaths, through its refinement by later theoreticians. But neither he nor any other scholars have looked into Alberti's source of the idea for his invention, one of the most important in the known history of cryptography.

Polyalphabetic substitution is a form of substitution cipher, one of the two great classes of ciphers, the other being transposition cipher. Transposition ciphers jumble the letters of the original message, or plaintext: *attack* may become TTAKCA. Substitution ciphers replace the letters of the original message with other letters or numbers of symbols: *attack* may become ZGGZXP. The two may be combined.

All substitution ciphers employ a listing of paired plain and cipher equivalents that is called a cipher alphabet. In the example above, the cipher alphabet was a = Z, b = Y, c = X, . . . , z = A. Usually the cipher alphabet is written out with the plain letters above and the cipher letters below:

plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
cipher	O	A	H	M	T	Z	X	B	I	N	U	F	C	J	P	V	R	E	K	Q	W	D	G	L	S	Y

This juxtaposition maps the plain letters to the cipher letters and vice versa. Thus *go* = XP; HPCT = *come.*

Because only a single cipher alphabet is used, this system is called monoalphabetic substitution. Its chief weakness is the fixity of its replacements. It permits solution by matching the frequency of the ciphertext letters with the known frequency of letters in the language of the plaintext. The obvious way of correcting this weakness is to

*120 Wooleys Lane, Great Neck, New York 11023.

I thank Professor Cecil Grayson, Serena Professor of Italian Studies in the University of Oxford, and Robert D. F. Pring-Mill, Lecturer in Spanish in the University of Oxford, for their comments on the thesis set forth here.

[1]Charles J. Mendelsohn, "Blaise de Vigenère and the 'Chiffre Carré,'" *Proceedings of the American Philosophical Society,* 1940, *82*:103–129.

[2]David Kahn, *The Codebreakers: The Story of Secret Writing* (New York: Macmillan, 1967), pp. 18–24, 427–433, 398–400, 606, 655; F. W. Winterbotham, *The Ultra Secret* (New York: Harper & Row, 1974); Ronald Lewin, *Ultra Goes to War* (New York: McGraw-Hill, 1978).

[3]Jacob Burckhardt, *The Civilization of the Renaissance in Italy,* trans. S. G. C. Middlemore, Pt. II, Ch. 2 (1929, reprinted New York: Harper Torchbooks, 1958), pp. 148–150; Joan Gadol, *Leon Battista Alberti: Universal Man of the Early Renaissance* (Chicago: University of Chicago Press, 1969).

give each plaintext letter more than one cipher equivalent. In the West, this technique started in the late 1300s and rapidly came into general use.[4] Though it delays cryptanalysis, it does not defeat it,[5] and because its plain-to-cipher equivalents are still fixed, the system remains monoalphabetic substitution.

The weaknesses of the monoalphabetic system disappear when the cryptographer provides additional cipher alphabets as a source of substitutes. For then not only will a given plaintext letter have several substitutes, but each ciphertext letter will stand for different plaintext letters depending upon its position in the text. The apparently capricious behavior of a cipher letter will greatly confuse the cryptanalyst. This idea first appears in Alberti's little manuscript of about twenty-six pages generally called "De cifris."[6]

How did Alberti create multiple cipher alphabets? Taking two copper disks of different sizes, he inscribed the plain alphabet, including numbers for a special use, around the circumference of the larger bottom disk and wrote the cipher alphabet around the smaller, upper disk. (See Fig. 1.) Moving the inner disk from one position to another places different ciphertext letters against the plaintext letters. Each new position therefore creates a new cipher alphabet—hence "polyalphabetic" substitution.

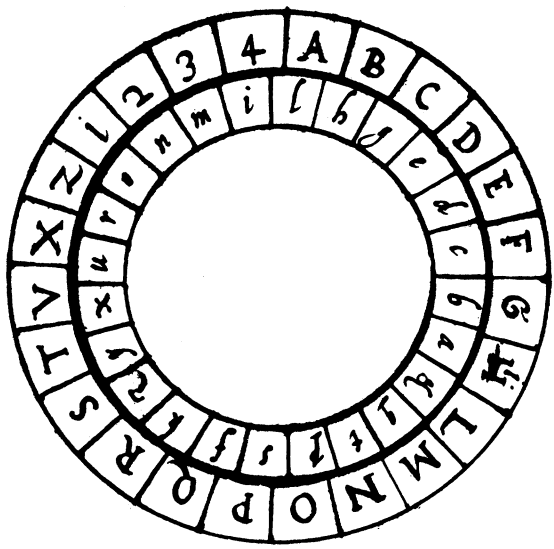

Figure 1. Alberti's cipher disk (from Biblioteca Apostolica Vaticana MS Chigi M II 49, vol. 35).

Obviously, the two persons who want to use the system for secret correspondence must have identical disks. They must also know what successive positions are being

[4] Aloys Meister, *Die Anfänge der modernen diplomatischen Geheimschrift: Beiträge zur Geschichte der italienischen Kryptographie des XV. Jahrhunderts* (Paderborn: Schöningh, 1902), p. 41 and passim.

[5] J. P. Devos and H. Seligman, eds., *L'art de deschiffrer: traité de déchiffrement du XVII siêcle de la Secrétairerie d'État et de guerre espagnole* (Louvain: Bibliothèque de l'Université, 1967), esp. pp. 43–89.

[6] An early copy (no holographs seem to exist) is reprinted in Aloys Meister, *Die Geheimschrift im Dienste der päpstlichen Kurie: von ihren Anfängen bis zum Ende des XVI. Jahrhunderts* (Paderborn: Schöningh, 1906), pp. 125–141. Portions in English, with discussion, appear in Kahn, *Codebreakers,* pp. 125–129. For a list of the known manuscripts with their locations see Charles J. Mendelsohn, "Bibliographical Note on the 'De Cifris' of Leone Battista Alberti," *Isis,* 1947, *32*:48–51. For discussion of the origins of its linguistic analysis, see Cecil Grayson, "Leon Battista Alberti and the Beginnings of Italian Grammar," *Proceedings of the British Academy, 1963,* 1964, *49*:291–311, on pp. 302–303.

used, or they will be as confused as a would-be cryptanalyst. So before they part they agree on a key. A simple example is to set the disks at a prearranged position and then turn the inner one one space clockwise after enciphering each plaintext letter. The system's flexibility and strength commended it, and eventually polyalphabetic substitution in far more complex forms came to dominate cryptography.[7]

Alberti himself never said where he got the idea for his epoch-making invention. Scholars seem to have simply assumed that it evolved from his "horizon," an astrolabe he adapted for surveying, which consisted of a circle whose circumference was graduated, over which swung a pointer.[8] It is true that both the horizon and the cipher disk are circular, have circumferences divided into sections, and have an element that rotates. But the significant feature of the cipher disk—the juxtaposition of two sequences—is lacking in the horizon. I therefore find this derivation unconvincing.

I propose another source: the mechanism devised by the medieval Catalan mystic Ramon Lull (c. 1232–1315) to combine letters, which stand for philosophical concepts, in groups of three.[9] Although it cannot be proved that Lull's device inspired Alberti, there are grounds for suspecting that it did.

The device was created for purposes very different from Alberti's. Lull, at thirty-one converted by a series of visions to a religious way of life, determined to become a missionary to the Moslems and the Jews. To prepare for this, he spent from about 1265 to 1273 improving his Latin, learning Arabic, and reading widely. Convinced that the ultimate truth would support the Christian faith and that such truth, by comprehending all knowledge, would be acceptable to Moslems and Jews as well, he devised his *Ars inventiva veritatis,* the "art of finding truth." This took nine attributes of God, such as goodness, greatness, and power, which participated in all aspects of creation, and joined them in all possible ways to encompass all forms of existence.[10]

To facilitate the combining process, Lull employed two techniques, in which scholars tend to see the germ of later scientific achievements. First, anticipating modern symbolic notation, he replaced the words for God's attributes by arbitrary letters, much as symbolic logic employs letters for sentences or elements of sentences; thus "goodness" was represented by B, "knowledge" by F, "truth" by I.[11] Lynn Thorndike has characterized this use of "brief handy designations" as the "chief contribution of Raymond Lull to modern science, or at least his chief step in the direction of scientific method."[12]

The second technique, foreshadowing the mechanisms for logic of electronic computers, automated the combining of one idea with another.[13] Working at first with pairs of concepts, Lull distributed the letters in a diagram, usually around the circumference of a circle, and drew lines from each letter to every other to show

[7]Kahn, *Codebreakers,* pp. 150–151, 153–154, 191.

[8]Gadol, *Alberti,* pp. 171–174, 208.

[9]The device is reproduced widely, e.g., in Frances Yates, *The Art of Memory* (London: Routledge and Kegan Paul, 1966), p. 183, where I first saw it. See also Robert D. F. Pring-Mill, "Ramon Lull," *Dictionary of Scientific Biography,* Vol. VII (New York: Scribner's, 1973), p. 549.

[10]Pring-Mill, "Lull," pp. 547–551. See also R. D. F. Pring-Mill, "The Analogical Structure of the Lullian Art," in *Islamic Philosophy and the Classical Tradition. Festschrift for Richard Walzer* (Oxford: Cassirer, 1972), pp. 315–326, on p. 315.

[11]Pring-Mill, "Lull," p. 549; J. N. Hillgarth, *Ramon Lull and Lullism in Fourteenth-Century France* (Oxford: Clarendon Press, 1971), pp. 8, 315; see also Erhard Wolfram Platzeck, *Raimund Lull: sein Leben—seine Werke—die Grundlagen seines Denkens (Prinzipienlehre)* (Düsseldorf: Schwann, 1962–1964), Vol. I, pp. 265–266.

[12]Lynn Thorndike, *A History of Magic and Experimental Science* (New York: Columbia University Press, 1923–1958), Vol. IV, p. 27.

[13]Pring-Mill, "Lull," p. 549; Martin Gardner, *Logic Machines and Diagrams* (New York: McGraw-Hill, 1958), pp. 9–14, 19.

graphically all possible two-letter connections.[14] In 1289 he developed a device to combine all possible ideas in threes. It consisted of three concentric rotatable disks of graduated size with letters inscribed on the circumferences. As the disks turn, all possible groupings of three letters are juxtaposed.[15] The resemblance of this device to Alberti's disk is striking. (See Fig. 2.)

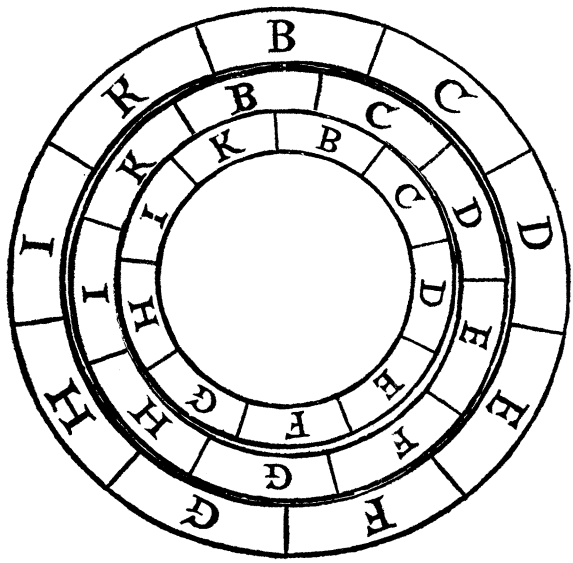

Figure 2. Combinatory disk. Ramon Lull, *Ars magna generalis et ultima* (Leyden, 1517), folio 4v. (Countway Library of Medicine, Boston.)

Lull's art had great appeal. Its mechanical exhaustion of all combinations of elements seemed to make its investigations more complete than other philosophical techniques, such as scholasticism, and thus better able to attain the final all-embracing truth. The many references to Lull in the letters and literature of Renaissance Italy, the many manuscripts of his work there, and the many Italian commentaries on him attest to his wide influence before, during, and after Alberti's lifetime.[16] Apparently no document states that Alberti knew of Lull.[17] Alberti's own

[14] Pring-Mill, "Lull," p. 548; Platzeck, *Raimund Lull,* Vol. I, p. 321.

[15] Pring-Mill, "The Analogical Structure of the Lullian Art," p. 318; Pring-Mill, "Lull," p. 549; and Platzeck, *Raimund Lull,* Vol. I, pp. 332 and 321, in which the first I should be an F.

[16] M. Batllori, "Le Lullisme de la Renaissance et du Baroque: Padoue et Rome," *XIème Congrès International de Philosophie, Actes* (Amsterdam: North-Holland, 1953), Vol. XIII, pp. 7–12 on pp. 10–11; Miguel Batllori, "Relíques manuscrites del Lul-lisme Italià," *Analecta Sacra Tarraconensia,* 1935, *11*:129–141; Hillgarth, *Ramon Lull,* pp. 137–138, 281; Paul Oskar Kristeller, *Iter Italicum: A Finding List of Uncatalogued or Incompletely Catalogued Humanistic Manuscripts of the Renaissance in Italian and Other Libraries* (London: Warburg Institute, 1965–1967), Vol. I, pp. 165, 278, 292, 302, 303, 307, 308, 312, 317, 345, 370, 427; Vol. II, pp. 19, 107, 140, 141.

[17] Discussions of Alberti's sources do not mention Lull, e.g., Gadol, *Alberti*; L. Zoubov, "Léon Battista Alberti et les auteurs du Moyen Age," *Medieval and Renaissance Studies,* 1958, *4*:245–266; Paul-Henri Michel, *La pensée de L. B. Alberti* (Paris: Société d'Editions "Les Belles Lettres," 1930); Franco Borsi, *Leon Battista Alberti,* trans. Rudolf G. Carpini (New York: Harper & Row, 1977); George Sarton, *The Appreciation of Ancient and Medieval Science during the Renaissance (1450–1600)* (Philadelphia: University of Pennsylvania Press, 1955).

wide-ranging curiosity, eclecticism, and energy make it highly probable, however, that he read an author who so permeated the intellectual climate of the time. The close resemblance between Alberti's and Lull's disks and the small difference between the two processes—juxtaposing letters to combine them and juxtaposing them to substitute one for another—further increase the probability that Lull's disk inspired Alberti's.[18]

As to where Lull got the idea for his disk, scholars have suggested three different possibilities. Robert Pring-Mill suspects that the volvelles of certain Arabic treatises on humoral medicine suggested the disks to Lull, who wrote on the subject. The volvelles were astrological wheels that could be revolved to show the different positions of the signs of the zodiac.[19] J. N. Hillgarth has suggested as a possible source the rotae or wheels found in the work of the encyclopedist and educator Isidore, Bishop of Seville (c. 570–636), especially those in the *De natura rerum.*[20]

Most convincing is the statement by Father Erhard Wolfram Platzeck in his comprehensive study of Lull that Lull owes the rotating disk of 1289 to the *Sefer Yezirah* (The Book of Creation), one of the pillars of the cabala, written between the third and sixth centuries.[21] Platzeck discusses the disk in the context of a full discussion of the possible relation between cabalism and Lull's work. Two correspondences between Lull's art and the *Sefer Yezirah,* which describes how the cosmos was created out of the twenty-two letters of the Hebrew alphabet, are relevant to the disk: the use of letters to represent elements of reality, such as air, wisdom, and wealth, and the combining of the letters to form all creation. The passage on combination is particularly suggestive: "Twenty-two basal letters: they are placed together in a ring, as a wall with 231 gates. The ring may be put in rotation forwards or backwards . . . ."[22] Pring-Mill has also discerned a connection between the cabala and Lull, apparently through oral diffusion from cabalistic schools existing in Catalonia during his lifetime,[23] while the existence of a translation of the *Sefer Yezirah* into Arabic,[24] which Lull could read, increases the probability that he knew of it. In addition, Blaise de Vigenère (1523–1596), a writer on cryptology, traces polyalphabetics to the *Sefer Yezirah,* though he does not mention Lull, Alberti, or disks in making the connection, whose basis he never states.[25] Mendelsohn criticizes this derivation, citing the section of the *Sefer Yezirah* quoted above. But his use of a translation that renders "ring" as "sphere" vitiates his criticism.[26]

Given the similarity in spirit between the *Sefer Yezirah* and Lull, in that both seek to seize and know the whole universe, and given the principle of combination

[18] A difference between Lull's disk and Alberti's lies in the sequence of letters. Lull's is alphabetical (though with gaps). Alberti, however, specified that his disk's letters be "not in regular order, . . . but scattered at random." This greatly improves the cipher. Alberti may well have got the idea for mixing the sequence, not from current cryptographic practice, which rarely did it, but, as Gadol also thinks (p. 207), from the movable type of the printing press, which Alberti mentions at the beginning of his treatise.

[19] Pring-Mill, "Lull," p. 548, and letter, May 5, 1972.

[20] Hillgarth, *Ramon Lull,* p. 19. The *rotae* are illustrated in Isidore de Seville, *Traité de la nature,* ed. Jacques Fontaine (Bordeaux: Féret, 1960), pp. 190 and 190-bis, 212 and 212-bis, and Harry Bober, "An Illustrated Medieval School-Book of Bede's 'De Natura Rerum,'" *The Journal of the Walters Art Gallery,* 1956–1957, *19–20*:65–97, on p. 91.

[21] Platzeck, *Raimund Lull,* Vol. I, pp. 327–332. On the *Sefer Yezirah,* see Gershom G. Scholem, *On the Kabbalah and Its Symbolism,* trans. Ralph Manheim (New York: Schocken, 1969), pp. 166–169.

[22] *The Book of Formation (Sepher Yezirah) by Rabbi Akiba ben Joseph,* trans. Knut Stenring (1923, reprinted New York: Ktav, 1970), Ch. II, Sec. 4. See Platzeck, *Raimund Lull,* Vol. I, pp. 330, 332.

[23] Pring-Mill, "Lull," p. 547.

[24] Lazarus Goldschmidt, trans. and ed., *Das Buch der Schöpfung* (Frankfurt: J. Kauffmann, 1894), p. 30.

[25] Blaise de Vigenère, *Traicté des chiffres* (Paris: Abel L'Angelier, 1587), fols. 23r and 36r.

[26] Mendelsohn, "Vigenère," pp. 122–123.

common to both, Platzeck's derivation of the rotating disk from the Hebrew work is especially persuasive.

Whatever the inspiration for Lull's disk, it seems an excellent candidate as the source of the Alberti device that created polyalphabetic substitution. If so, Alberti's disk provides yet another example of the fate of Lull's techniques. Devised to convert the heathen to the ultimate truth, they ended by being themselves converted to secular ends.

THE STARS AND HUMAN SEXUALITY: SOME MEDIEVAL SCIENTIFIC VIEWS

*By Helen Lemay**

Astrology was an integral part of the Arabic scientific corpus which was so decisive in transforming Western intellectual life in the twelfth and thirteenth centuries. Along with purely Aristotelian writings, astrological works expanded considerably the sources of scientific information available to the Latin West. Astrology was referred to by the Arabs as the "science of the stars," and this science had as its object the examination of all aspects of man in his social context, including the study of the human reproductive system. Sexual behavior is given extensive consideration in Arabic astrological treatises.

Western scientists did not merely receive Arab astrology as part of the baggage that contained Aristotelian science: they eagerly embraced the study of the stars and their effects on man. Arabic astrological works were widely translated and copied; Latin authors composed their own summaries of astrology; and astrologers played an important part in the cultural life of the West. For example, Michael Scot served as court astrologer for Frederick II, and Giovanni Pontano, the renowned Italian humanist, composed a major astrological treatise. Both of these men treat human sexuality in detail in their writings.

Astrology played a particularly significant role in the field of medicine. Astrological works were formally incorporated in the curricula of medieval medical faculties from at least the fourteenth century, and even from the moment of their reception in the West they were studied avidly by doctors. The pseudo-Ptolemaic *Centiloquium,* for example, an astrological handbook designed primarily for the use of physicians, was translated into Latin six times during the twelfth century by many of the central figures of this period, and over 150 manuscripts have been identified so far.[1] Physicians wrote treatises on

*Department of History, State University of New York, Stony Brook, N.Y. 11794.

[1]The *Centiloquium* (*Kitāb al-Tamara* or *Liber fructus*) was composed by pseudo-Haly (Abū Ja'far Aḥmad ibn Yūsuf ibn Ibrāhīm al-Kātib al-Tūlūni) in the late 9th or early 10th century in Cairo. It was used in Paris (1348), Bologna (1405), and Cracow (mid 1400s). See Heinrich Denifle and Emile Châtelain, *Chartularium Universitatis Parisiensis, Auctarium* (Paris: Delalain, 1889), Vol. I, p. 235; Carlo Malagola, *Statuti delle Università e dei Collegi dello Studio Bolognese* (Bologna: Zanichelli, 1888), pp. 276 and 214; Aleksander Birkenmajer, *Études d'histoire des sciences en Pologne, Studia Copernicana,* 1972, *4*:469–495. The *Centiloquium* is being studied at present by a research group at the CUNY Graduate Center under the direction of Richard Lemay. See Lemay, "Origin and Success of the Kitāb Tamara of Abū Ja'far Aḥmad ibn Yūsuf ibn Ibrāhīm from the Tenth to the Seventeenth Century in the World of Islam and the Latin West," *Aleppo University, Proceedings of the First International Symposium for the History of Arabic Science, 5–12 April 1976* (Aleppo: University of Aleppo Institute for the History of Arabic Science, 1978), pp. 91–107. The author of the *Centiloquium* will henceforth be referred to as Ahmad ibn Yūsuf.