Trithemius, Bellaso, Vigenère
Origins of the Polyalphabetic Ciphers

Paolo Bonavoglia
Mathesis Venezia c/o Convitto-Liceo Marco Foscarini 4942 Venezia, Italy
paolo.bonavoglia@mathesisvenezia.it

Abstract

The purpose of this paper is to show how polyalphabetic ciphers developed, using primary sources, from Trithemius and Bellaso to Vigenère, including the recent discovery of the Bellaso 1552 zero cipher.

1 Primary Sources

Doing research using only primary sources is of course impossible, except for a few limited cases. A great number of mistakes, small or big, arise from using secondary sources; errors of transcription, translation, interpretation accumulate, migrate from book to book, even of the most authoritative authors, and are very hard to die.

I will try to use this method about the origin of poly-alphabetic ciphers. Nowadays Google Books, great libraries and others publish more and more digitized original books, making possible the use of primary sources without the burden of visiting remote libraries.

The first polyalphabetic cipher published in print (1518) is the one of abbot Trithemius, the *Recta Tabula* present in the *Libri Polygraphiae VI.* [1]

The second well known polyalphabetic cipher is the one of G.B. Bellaso published in Venice in 1553, which for the first time introduces what today is called a password or pass-phrase as the key. Bellaso writes in the preface this cipher was a remake of a 1552 cipher printed on leaflets; and it was one of these leaflets the one I found in November 2018 in the State Archives of Venice.[2] See figure 1.

The best known polyalphabetic cipher remains the one of Blaise de Vigenère, published in 1586. Vigenère in his work mentions both Trithemius and Bellaso, and merges their ideas into his square table.

These ciphers are all basically square tables, as shown in the figure at the end of this paper (7).

2 Johannes Trithemius

Johannes Trithemius[3] in his book *Libri Polygraphiae VI*[4] introduced the *Recta Tabula*, Latin for square table, shown in figure 2. It uses a 24 letters alphabet, the ancient Latin alphabet extended with the three Greek letters **K, Y, Z** and the new letter **W**.[5]

One should use the first alphabet to encrypt the first letter, the second alphabet to encrypt the second letter and so on. So the same plaintext letter may be encrypted using different ciphertext letters, thus confusing frequency analysis.

[1] As a matter of fact Leon Battista Alberti had written a treatise on ciphers before 1470, proposing an encrypting disk and a few ways to use it, but the book was kept secret for about a century and published in Venice only in 1568. This is a common problem with many ciphers, kept secret for years or even centuries.

[2] See (Bonavoglia-2018)

[3] Johann Heidenberg or Johannes Zeller (1462-1516) was born in Trittenheim, a village that gave him the surname Trithemius.

[4] (Trithemius, 1518) The book was written between 1506 and 1508 and published in 1518, after his death.

[5] It may be appropriate to remark that the letter **W**, as a consonant variant of the Latin vowel **V**, (lowercase **u**) was introduced before the splitting of **V** in the vowel **U** and the consonant **V**. In English it is still known as *double u*.

Figure 1: Bellaso's cipher zero of 1552, discovered in December 2018 in Venice. No instructions were found. *Archivio di Stato di Venezia, Cifre, chiavi e scontri di cifra ... busta 3.* Any commercial use of this image forbidden.

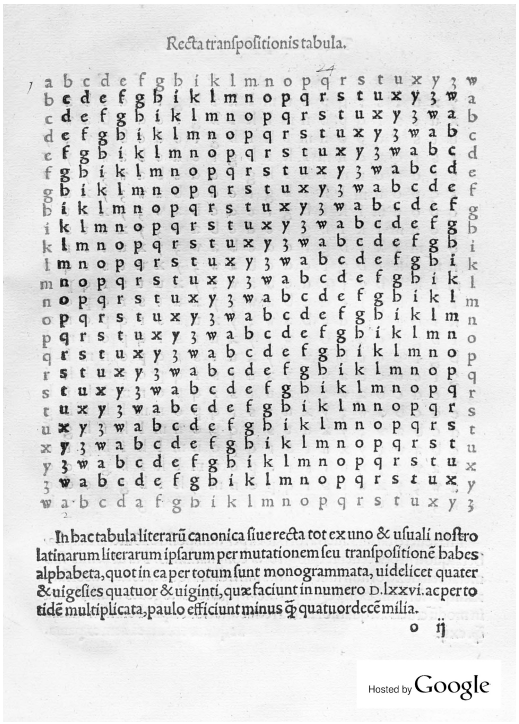

Figure 2: Trithemius *Recta Tabula*.

3 Giovan Battista Bellaso, 1552

This cipher had been printed in 1552, and was given to friends and other people. See figure 1. Basically his table uses 22 reciprocal alphabets, one for each letter, listed in a "vowels first" order. If one removes the superfluous first line of each list, a 22x22 square table, like the ones of Trithemius or Vigenère, remains, (see figure 7 at the end of this paper).

There were no instructions for using it, as confirmed by Bellaso himself in the preface to his 1553 paper, see next section.

4 Bellaso's Cipher of 1553

Indeed in the preface of his 1553 booklet Bellaso wrote[6]:

> La onde à prieghi et consegli di molti, & per mio minor fastidio, mi sono risoluto di farla ristampare per commune sodisfattione, & seruigio de Principi Cristiani. & holla oltre à cio ridotta alla quarta parte di quello che era prima, & à tanta breuità & ageuolezza, che una sola riuolta d'occhio la comprende tutta, & potrebbesi ancora in breuissimo spatio di tempo imparare à mente, [...]

[6] English: Therefore [answering] to prayers and advice of many people, and for my minor trouble, I resolved to have it reprinted for common satisfaction, and to the service of Christian Princes. And in addition to this I reduced it to the fourth part of what it was before, and to such brevity and ease, that a single glance includes it all, and they could also be memorized in the shortest period of time, [...]

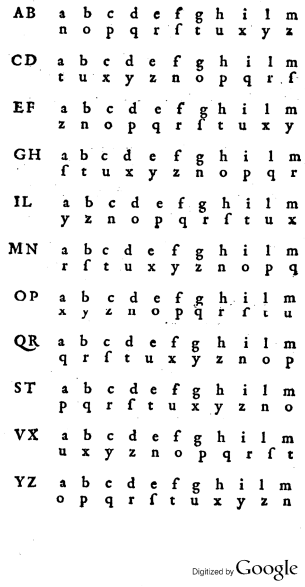

Figure 3: Bellaso 1553 cipher.

This cipher is clearly a remake of the 1552 cipher with letters coupled and ordered in the normal alphabetical order. This cipher has been known for centuries as *Porta's table*, a typical example of the mistakes arising from the use of secondary sources.[7]

5 Vigenère

Blaise de Vigenère in his famous 1586 *Traicté des chiffres* presented, at page 46r, a table using only the original 20 Latin alphabet (without the Greek**Y** and **Z**), honestly mentioning "*un certain Belasio*" as the inventor of this cipher. Really it is Bellaso's 1553 table, reduced to the 20 letters classical Latin alphabet, excluding **Y** and **Z**, Greek letters added at the end of the Latin alphabet. See figure 4.

After a few examples of use he writes[8]:

[7] See (Buonafalce, 2006)

[8] English: But all this can be done as well, even better, by the following table, in a way in which everything is reduced to one, taking the traverse capital letters which are at the front up, for the meaning we

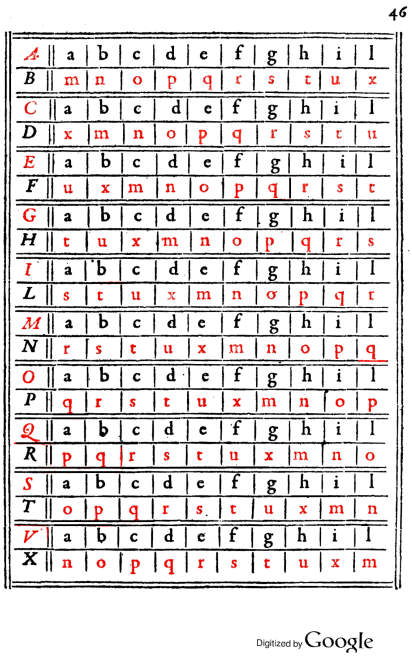

Figure 4: Bellaso's table adapted by Vigenère. *Traicté des chiffres*, p. 46r.

> Mais tout cecy se peut practiquer aussi bien, voire trop mieux, par la table encore suiuante, combien que tout reuienne presqu'à vn, prenant les capitales trauersantes qui sont au front d'enhaut, pour le sens qu'on veut exprimer: & les perpendiculaires au costé gauche descendant en bas, au lieu de clefs. I'en ay mis icy deux rengees: l'vne de noir, l'autre de rouge, pour monstrer que les alphabets tant de l'escritur, que des clefs, se peuuent transposer & changer en tante de sortes qu'on voudra [...][9].

So Vigenère converts Bellaso's cipher into a Trithemius like square, using a key word; it is simpler to use than Bellaso's and safer than Trithemius's. You look for the letter of the plaintext (p) among the column labels and the letter of the key (k) among the row labels or viceversa, the operation is commutative. The cipher (c) is anyway at the crossing of column and row.

want to express: and the perpendiculars to the left side descending downward, for the keys. I have put here two rows: one in black, the other in red, to show that the alphabets of the text, as well as those of the keys, can be shifted and changed in as many sorts as one wants [...]

[9] (Vigenere, 1587) p. 49v.

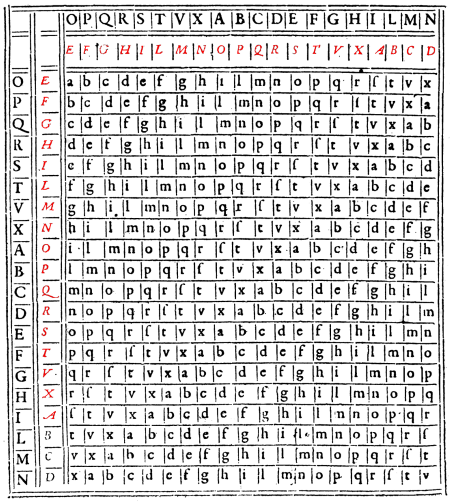

Figure 5: Vigenère's original table from his treatise. *Traicté des chiffres*, p. 51v.

The table has red headings and black headings. One can shift the alphabets of s steps; starting with the letter **E** the shift is of 4 steps.

Indeed it is a simplification, without the shifting, of the table in figure 6, the one that became popular as Vigenère's table:

Mathematically, assigning to every letter his ordinal number in the alphabet, stating from 0, the encoding procedure is a simple arithmetic addition modulo 20 (for a 20 letters alphabet).

$$c = p + k + s \mod 20$$

The introduction of the shifting improved the security only a bit, mathematically it just removes the constant s from the addition:

$$c = p + k \mod 20$$

Security depends mainly on the length of the key. The longer the key, the safer the cipher.

6 Conclusion

Figure 7 is the best summary of this paper, showing at a glance the evolution of these ciphers, here written in square table form for better comparison. The classic Vigenère table is a Trithemius like cipher, using a Bellaso's like keyword.

Figure 6: Vigenère's table as it is known today, adapted to the modern 26 letters alphabet.

7 Acknowledgments

A special thank to Giovanni Caniato and the other archivists of the *Archivio di Stato di Venezia* for assistance and help, to Augusto Buonafalce for advice and to Antonio Giovanni Colombo for reviewing the English text.

References

Paolo Bonavoglia. 2019. Cryptologia *Bellaso's 1552 Cipher recovered in Venice*. Philadelphia, PA. DOI 10.1080/01611194.2019.1596181

Augusto Buonafalce. 2006. Cryptologia *Bellaso's Reciprocal Ciphers*. Philadelphia, PA. DOI 10.1080/01611190500383581

G. B. Bellaso. 1553. *La cifra del sig. Giouan Battista Bellaso* .... Venezia.

Joannes Trithemius. 1508. *Libri Polygraphiae VI*. Ioannis Haselbergi de Aia, 1518. Argentorati (Strasbourg), 1613.

Blaise de Vigenère. 1587. *Traicté des chiffres, ou Secrètes manières d'escrire*. Abel L'Angelier, Paris 1586 1587

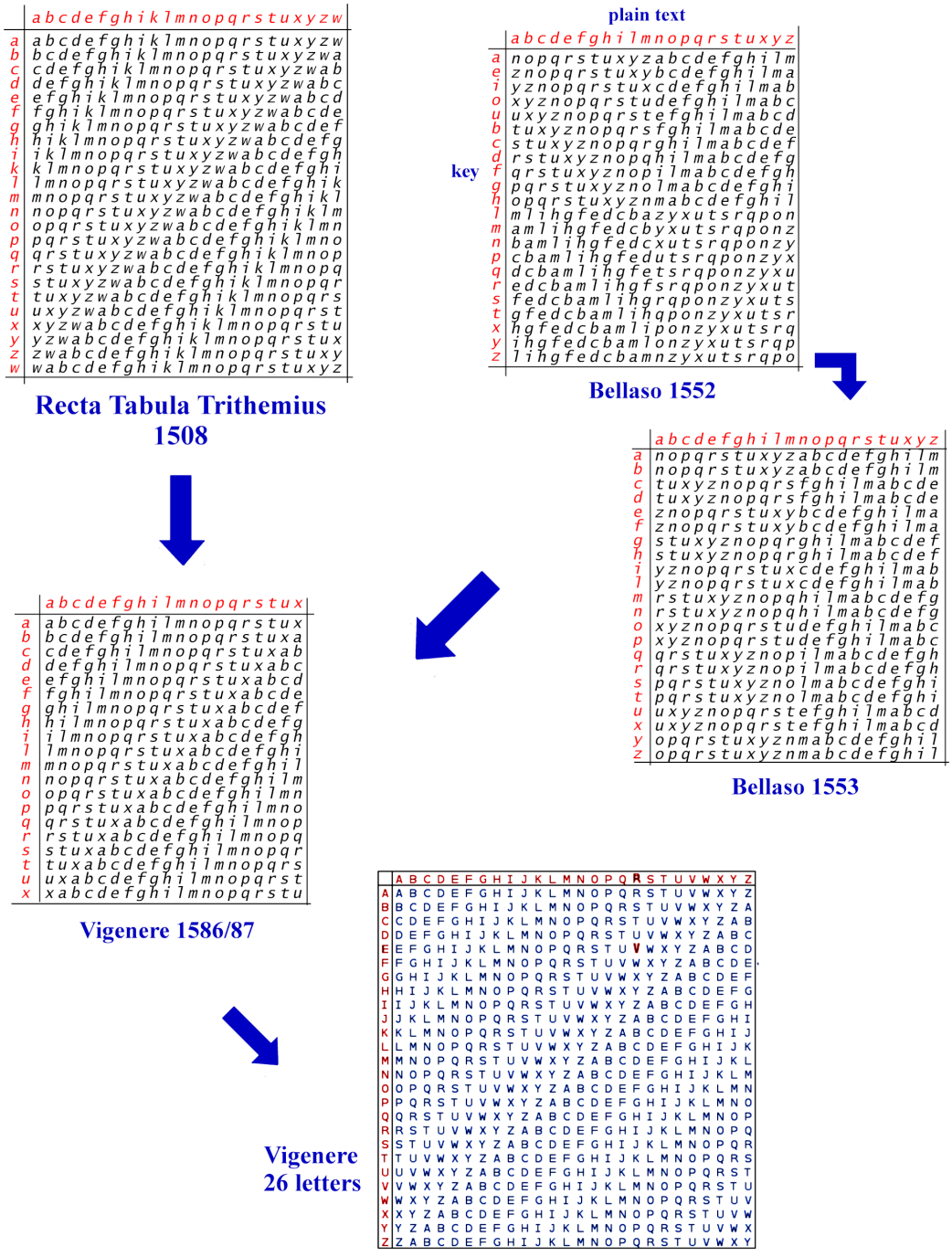

Figure 7: Comparison of all ciphers written in square table form.