Available online at www.sciencedirect.com
SCIENCE DIRECT®
Stud. Hist. Phil. Sci. 37 (2006) 269–289
Studies in History and Philosophy of Science
www.elsevier.com/locate/shpsa

François Viète: between analysis and cryptanalysis

Marco Panza

CNRS, Équipe REHSEIS, UMR 7596, CNRS–Université Paris 7, France

Received 16 January 2005; received in revised form 12 June 2005

Abstract

François Viète is considered the father both of modern algebra and of modern cryptanalysis. The paper outlines Viète's major contributions in these two mathematical fields and argues that, despite an obvious parallel between them, there is an essential difference. Viète's 'new algebra' relies on his reform of the classical method of analysis and synthesis, in particular on a new conception of analysis and the introduction of a new formalism. The procedures he suggests to decrypt coded messages are particular forms of analysis based on the use of formal methods. However, Viète's algebraic analysis is not an analysis in the same sense as his cryptanalysis is. In Aristotelian terms, the first is a form of '*ἀνάλυσις*', while the second is a form of *διαίρεσις*. While the first is a top-down argument from the point of view of the human subject, since it is an argument going from what is not actual to what is actual for such a subject, the second one is a bottom-up argument from this same point of view, since it starts from what is first for us and proceed towards what is first by nature.

Keywords: Analysis; Cryptanalysis; Algebra; Aristotle; Viète

1.

François Viète (1540–1603) was certainly one of the figures who mainly inspired the emergence of a new way to do mathematics in the early modern period. He was also a statesman and an adviser of the French King Henry IV, who employed him, during his confrontation with the Holy League, to decrypt the coded messages of the Spaniards and the Italians and appointed him to the title of *déchiffreur du roi*. He has been often

E-mail address: marco.panza@paris7.jussieu.fr (M. Panza).

0039-3681/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.shpsa.2005.06.013

considered the 'father of modern algebra' and, more recently, P. Pesic called him 'the father of modern cryptanalysis'.[1]

The first judgement could be based on the consideration of different parts of Viète's *oeuvre*, according to the different senses that could be attributed to the term "algebra",[2] but is usually justified by relying on the symbolic formalism that Viète used both in the *In artem analyticem isagoge* and in the *Zeteticorum libri*,[3] where capital consonants and vowels are employed to denote known and unknown quantities, respectively.

The second judgement has been justified, instead, by relying on the consideration of two short memoirs that remained unpublished for a long time.[4] The first of them was written by Viète himself on his deathbed and addressed to the duke of Sully, in order to expose his techniques for codebreaking. The second, probably written sometimes after Viète's death, is a more general description of the same techniques.[5] Pesic has translated them into English and published them.[6]

In another paper of his, Pesic argued for the existence of a 'close rapport' between Viète's methods in cryptanalysis and 'the innovations he introduced in the conceptual foundations of mathematics', by maintaining that 'the basic concepts of his "new algebra" parallel those employed in his art of decryption'.[7] This is the thesis I would like to discuss here and partially question.

2.

Pesic begins[8] by mentioning the 'disclosure of secrets' as being 'a central theme in the development of modern science' and contrasting Aristotle's rational optimism, according to which 'nature is fundamentally open to common human understanding', and esoteric mysticism, according to which only few elects, who have been initiated to it, have access—and yet, a very partial access—to these secrets. Provided that Viète's decryption of coded messages is understood as a disclosure of secrets, his attitude with respect to these secrets was certainly closer to Aristotle's rational optimism than to cabalistic or Hermetic habits, and it contrasts under this respect with the attitude of other codebreakers, such as

[1] Pesic (1997a), p. 1. This judgement has been repeated in Delahaye (2003).

[2] I have discussed some of these senses in Panza (Forthcoming).

[3] Viete 1591a, 1591b.

[4] Both memoirs are mentioned in Ritters's classic biography: Ritter (1895), pp. 257–258.

[5] Two transcriptions of these memoirs by F. Ritter are included in a large manuscript intellectual biography of Viète, composed by Ritter himself and forming four manuscript volumes preserved at the Bibliothèque de l'Institut de France (MS 2009–2012 respectively: *François Viète, inventeur de l'Algèbre moderne. Sa vie. Son temps. Son œuvre*; the transcriptions of the two memoirs I refer to occurs in MS 2009, ff. 187–194 and 185–187, respectively; five other volumes—namely MS 2004–2008—contain a French translation of Viète's mathematical works). Ritter says there that he has Viète's autograph of the first memoirs 'sous les yeux' but gives no other indication about his sources, which are presently lost. No other copy of the first memoirs has been localised up to now, while an older copy of the second is preserved at the Bibliothèque National de France, in Paris (see MS Dupuy 661, ff. 219r–220r).

[6] Pesic (1997a), pp. 22–27 and 27–29, respectively. Pesic's paper also contains a large amount of information concerned with the context in which these memoirs were probably written and the transmission of their manuscript copies.

[7] Pesic (1997b), p. 675. Cf. also p. 677: 'my argument points toward parallels between developments in algebra and in decryption rather than unequivocal influences'.

[8] Ibid., p. 674.