

# FRANÇOIS VIÈTE, FATHER OF MODERN CRYPTANALYSIS – TWO NEW MANUSCRIPTS

Peter Pesic

ADDRESS: St. John's College, Santa Fe NM 87501-4599 USA.

**ABSTRACT:** Two recently discovered manuscripts of François Viète clarify his methods of cryptanalysis. He claimed to have an “infallible rule” which could be extended to solve any nomenclator. His technique extends the analysis of frequencies to include digraphs and trigraphs in a systematic way. This yields information distinguishing vowels from consonants and delineates a limited set of alternative hypotheses at each step. In contrast with earlier writers, his methods rely on mathematical and logical approaches rather than on probable words and unsystematic guesswork. Thus he is the originator of modern methodical cryptanalysis. Leibniz and Wallis were aware of his achievements, if not of his exact methods. With Viète in mind they corresponded concerning the nature and scope of cryptanalysis.

**KEYWORDS:** François Viète, cryptanalysis.

François Viète (1540-1603), the father of modern algebra,<sup>1</sup> may now also be called the father of modern cryptanalysis. In two newly recovered manuscripts, he describes his methods of cryptanalysis, which are much more general in scope than any others known previously. Viète goes so far as to assert that he has an “infallible rule” for cryptanalysis, a claim none of his contemporaries dared to make.

This rule has been lost for many years. Writing in 1921, Ernst Dröscher noted that Viète had composed instructions for cryptanalysis, but that these had not been passed on.<sup>2</sup> In the course of his researches David Kahn noted references

<sup>1</sup>The main published source for the life of Viète is Frédéric Ritter, “François Viète, Inventeur de l'Algèbre Moderne, 1540-1603. Essai sur sa Vie et son Œuvre,” *Revue Occidentale*, 10 (1895), 234-274, 354-415. There is also useful material in B. Fillon and F. Ritter, *Notice sur la vie et les ouvrages de François Viète* (Nantes: Ch. Gallimard, 1849). A helpful overview of Viète's cryptanalytic activities can be found in the classic general history of cryptography, David Kahn, *The Codebreakers* (New York: Macmillan Co., 1967), 116-118, and in Ritter, 257-258.

<sup>2</sup>Ernst Dröscher, *Die Methoden der Geheimschriften* (Leipzig: K. F. Koeler, 1921), 24 n. 2. Devos examined some of Viète's solutions in 1935 but remarked that he could learn nothing of Viète's methods; see J. P. Devos, *Les Chiffres de Philippe II (1555-1598) et du Despacho Universel durant le XVIIe siècle* (Bruxelles: Académie Royale de Belgique, 1950), 59 n. 3.

by Frédéric Ritter to a memoir of 1603 concerning cryptanalysis which Viète had addressed to Henry IV's chief minister, the duke of Sully, but was unable to locate this memoir.<sup>3</sup> I have found Ritter's copy of this memoir which, along with another manuscript account of Viète's methods not elsewhere discussed, brings to light for the first time the nature of Viète's cryptanalytic methods. These documents fill an important lacuna in the history of cryptanalysis in France and show why Viète may be said to have founded modern cryptanalysis.

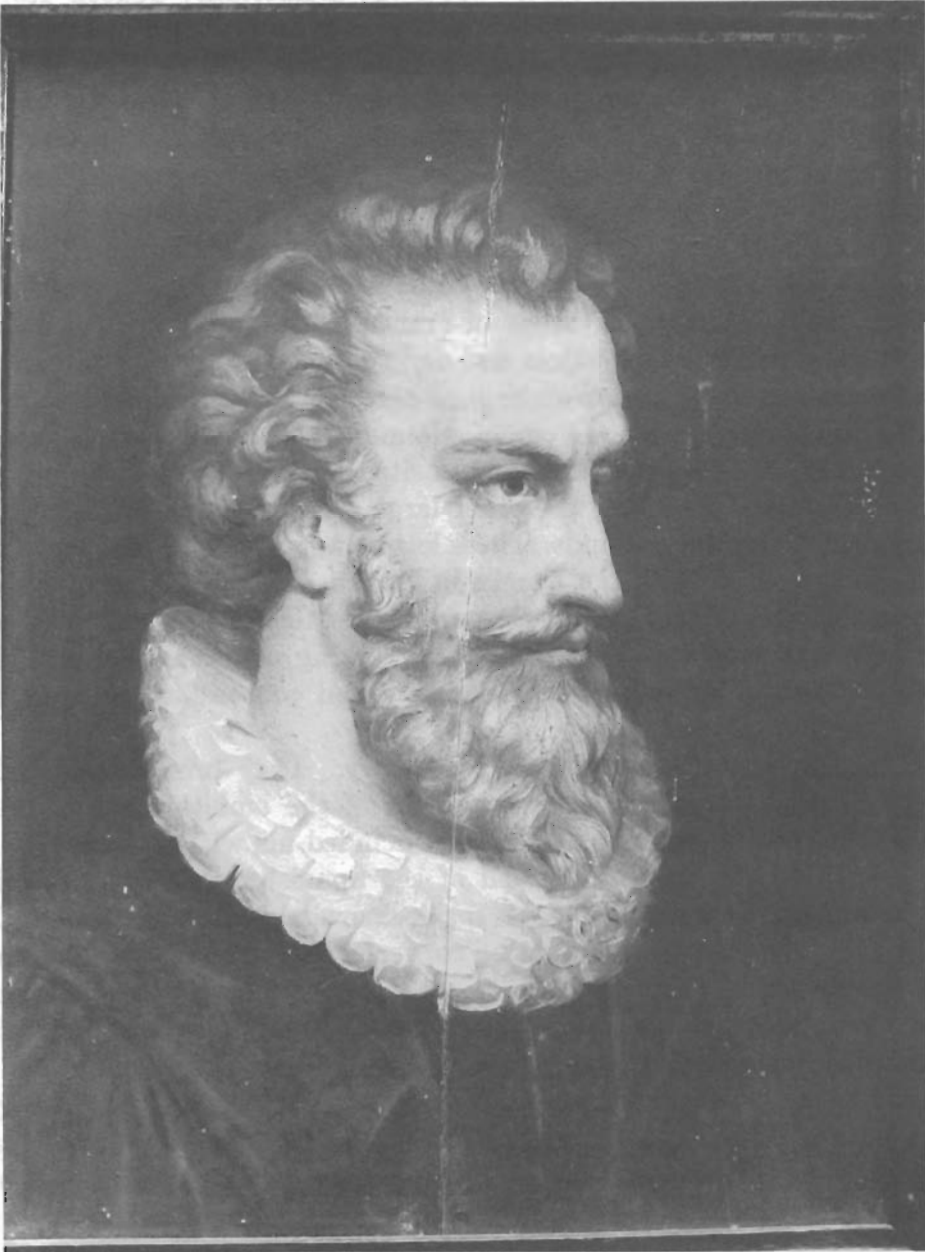
## VIÈTE'S ACTIVITIES IN CRYPTOLOGY

Viète was born in 1540 in Fontenay-le-Comte, near France's southwestern Atlantic coast. There he was raised and completed his secondary education. After training from 1558 to 1559 as a lawyer at the University of Poitiers, he returned to Fontenay to practice law, where he also assumed the title of seigneur de la Bigotière (lord of la Bigotière), the modest manor he inherited from his father. In 1564 Viète became attached to the de Parthenay household, an important Protestant family, for whom he wrote treatises on family history and advised on legal matters. He also tutored Catherine de Parthenay, for whom he wrote his earliest scientific works.<sup>4</sup> After Catherine's marriage to Charles de Quellenec in 1568, Viète came into contact with the principal Calvinist leaders, among them the teenaged King Henry III of Navarre, who developed confidence in him. His services no longer needed as a tutor, Viète left and became a member of the *parlements*, or courts of justice, of Paris (from 1572) and of Bretagne (from 1574). Henry continued to show him favor and entrust to him confidential missions. In 1579, after Viète had succeeded in delicate negotiations concerning the legitimacy of the marriage of the duke of Nemours to Françoise de Rohan, he was given the title of counselor to the king by France's monarch, also called Henry III. The following year Viète was appointed *Maître des requêtes de l'Hôtel*, a high legal office which gave him judicial authority over officials of the royal household and the provincial judiciary. Though Viète's intelligence and diplomatic ability probably recommended him for these positions, the few surviving anecdotes about him emphasize rather his absorption in mathematical matters. Sometimes he worked in his room for three days at a time without sleeping or eating.<sup>5</sup> "Never was

<sup>3</sup> Kahn, 995. Ritter, as well as Viète himself, always used *déchiffrement* for what I am calling "cryptanalysis," a term that was not invented until 1920. *Déchiffrement* was used in these early texts to indicate reading by either authorized or unauthorized readers.

<sup>4</sup> These are listed in Ritter, 242, and include Viète's ambitious work on cosmology, the *Harmonicum coeleste*; see Noel M. Swerdlow, "The Planetary Theory of François Viète 1. The Fundamental Planetary Models," *Journal for the History of Astronomy* 6(1975), 185-208.

<sup>5</sup> Jacques-Auguste de Thou, *Histoire universelle*, tr. from 1604 Latin original (London: 1734), 14:164-166.



Portrait of François Viète (1540-1603)

Oil on wood; Anonymous; undated. Musée Vendéen, Fontenay-le-Comte (Vendée, France). Reproduced with the permission of Conservation Départementale des Musées de Vendée.

a man more born for mathematics,” wrote the memorialist Gédéon Tallemant des Réaux, who also noted that “Viète died young, for he killed himself through excessive studying.”<sup>6</sup> But Viète also possessed a rare and valuable skill which singled him out among other worthy advisors: he was able to solve the cryptograms of the Spanish and Italian courts, which were constantly attempting to intervene in the struggle in France between the Catholic League and the Protestant parties. In 1588, for example, he read a dispatch of Alessandro Farnese, duke of Parma and head of the Spanish forces of the League, perhaps gaining some insight into Farnese’s activities. Perhaps owing to this ability, Henry III of Navarre, who ascended the throne of France in 1589 as Henry IV, confirmed Viète’s position in these high offices and named him as well to his privy council.

As a Protestant Henry had to make good his claim to the throne through battle as well as diplomacy against the counterclaim of the League that no Protestant could be a legitimate king of France. His situation was precarious, for in 1589 the League held Paris and all the other large cities of France. Then ciphered correspondence fell into his hands. These letters were to Philip II, king of Spain, from his liaison officer with the League in France, Commander Juan de Moreo, and his ambassador in France, Don Bernardino de Mendoza. The correspondence was turned over to Viète. While he was working on them, however, Henry defeated the League’s superior forces at Ivry and consolidated himself on the throne.<sup>7</sup>

Nevertheless, Viète’s solutions helped Henry. They revealed not only the details of Spanish plans but also the extent of the ambitions of the duke of Mayenne, the head of the League. These included his wish to become king of France—much to the surprise as well of the Spanish, who were scheming to put an infanta on the throne. Such inside knowledge was valuable as Henry worked out a compromise in which he converted to Catholicism and Mayenne in turn submitted to Henry’s authority. In fact, the struggle to implement this plan involved the public disclosure of these secret communications, like Britain’s exposure of Germany’s Zimmermann telegram of 1917.

In 1590, probably with Henry’s approval, Viète published his cryptanalysis of Moreo’s letter. Dated October 1589, it revealed Mayenne’s avowal of plans to usurp the French throne, encompassing (in Viète’s words) “the desolation and dissipation of France.”<sup>8</sup> Surely Viète was aware of the dangers of revealing that

<sup>6</sup>Tallemant des Réaux, *Les Historiettes* (Paris: Librairie Gallimard, 1960), 1:191-192; notes at 872-873.

<sup>7</sup>Devos, 59; there are helpful biographical notes on Moreo at 44 and on Mendoza (whom Viète gallicizes to “Mendosse”) at 38-39. The ciphers assigned to them respectively are given at 328-334 (1589-1597; noted by Devos as “decrypted by Viète”) and 296-299 (1587).

<sup>8</sup>The pamphlet is entitled *Deschiffrement d’une lettre écrite par le commandeur Moreo au Roy d’Espagne son maître, du 28 octobre 1589 – où se voit que le duc de Mayne s’est déclaré à Moreo vouloir estre Roy et des*

he could read enemy dispatches, including the obvious consequence that enemy codes and ciphers would be changed. What seems paramount in his published presentation is his unmasking of the designs of Mayenne working in concert with Philip and his agents to unseat Henry. Clearly, Henry was willing to sacrifice the strategic advantage of his secret knowledge if it would expose Mayenne's plans. Viète avowed exactly that aim in a letter he wrote to Henry and published with his solution. In view of Mayenne's design to turn the cities of Picardy in northern France over to the Spanish and in general to interpose Spanish control in French affairs as a prelude to gaining the throne, Viète wrote to Henry that "it does not seem to me at all untimely that these cities and governors, and generally all your people, who still are deceived by the League, should know this truth."<sup>9</sup> To this end Viète reminded the king that he is keeping the originals of the letters along with the "alphabets and dictionaries" he used to solve them, so that they might irrefutably prove Mayenne's designs.

The recently discovered 1603 memoir to Sully adds several interesting details to the story made public in 1590. In that memoir Viète reveals that the solutions were used not only to open the eyes of the nobles and the people (as the 1590 publication had announced), but to alert Mayenne in particular to the treachery of his Spanish patrons and even of "his followers themselves."<sup>10</sup> Viète mentions unspecified conspiracies of Mayenne's followers, perhaps with their Spanish allies, as well as the plans of the duke of Parma to make war on both Mayenne and Henry, and the duke of Feria's wish for "the ruin of the duke of Mayenne." These documents revealed manifold Spanish "feints and abuses towards the French," even towards their ally, Mayenne. Unlike the 1590 letter, however, these documents were not published. If the treachery of Mayenne's followers had been communicated privately to Mayenne, that disturbing information might have more effectively persuaded him to accommodate himself to Henry with dignity.

Viète evidenced a supreme confidence in his cryptanalytic powers. He reassured his king not to "get anxious that this will be an occasion for your enemies to change their ciphers and to remain more covert. They have changed and rechanged them, and nevertheless have been and always will be discovered in

---

*moyens qu'il veut suivre pour y parvenir à la désolation et dissipation de la France* (Tours: Jamet Mettayer, 1590) [Decipherment of a letter by Commander Moreo to his master the king of Spain dated 28 October 1589 – where it is seen that the duke of Mayenne declared to Moreo that he wished to be king and the means which he wished to follow to attain to the desolation and dissipation of France]. A copy survives in Paris's Bibliothèque Nationale collection Les 500 de Colbert, No. 33, ff. 198-209, with corrections in Viète's hand. Viète's letter and his solution are reprinted in Étienne Bazerries, *Les chiffres secrets dévoilés* (Paris: Librairie Charpentier et Fasquelle, 1901), 220-232.

<sup>9</sup> Bazerries, 220-222.

<sup>10</sup> Bibliothèque de l'Institut de France Ms. 2009, f. 183.

their tricks.”<sup>11</sup> Nor was Viète’s confidence misplaced, for he continued to read Spanish and other dispatches right up to 1594, when Mayenne finally accepted Henry as rightful king.<sup>12</sup>

Despite Viète’s revelations, the Spanish did not change their ciphers. When Philip realized that the French had been able to read the Spanish ciphers, he complained to the pope that they must have been using black magic to accomplish this feat.<sup>13</sup> The pope ignored his accusation, doubtless cognizant that the papal cryptographers had been able to solve Spanish ciphers for 30 years without any diabolical aid. The contemporary chronicler Jaque-Auguste de Thou noted that Philip’s accusation only earned him the “contempt and indignation” of those who heard it. Spain seems not to have had cryptanalysts, which might explain Philip’s attitude.<sup>14</sup> And indeed, the mystery of how Viète achieved his solutions has only now been revealed.

## VIÈTE’S MEMOIR TO SULLY AND ITS POLITICAL CONTEXT

This mystery has been solved through the finding of two manuscripts that specify Viète’s methods. The first is a copy of Viète’s memoir of 1603 to the duke of Sully; the second is a manuscript entitled “*Règles de Viète pour le déchiffrement des écritures secrètes*” (“Rules of Viète for the decipherment of secret writings”). In response to an inquiry of mine about the lost memoir, Dr. H. L. L. Busard, the noted Dutch historian of mathematics, generously gave me a list of works by and about Viète compiled by his descendant E. Viette de la Rivagerie.<sup>15</sup> This list mentions the missing memoir as well as Ritter’s unpublished notes and drafts of his full-length biography of Viète, which he obviously used in the preparation of his published memoir of 1893. Whether because Ritter died shortly thereafter or for other reasons, this biography remained unpublished and was described by

---

<sup>11</sup> Bazeris, 220-222.

<sup>12</sup> Bibliothèque Nationale, Les 500 de Colbert, No. 33, ff. 178-197. Though no inventory has yet been made of these dispatches, they should prove valuable for historians of the period. Ritter also includes in his unpublished materials (Bibliothèque de l’Institut de France, Ms. 2009) many other letters decrypted by Viète.

<sup>13</sup> De Thou, 14:166; cited in Kahn, 118, 995.


<sup>14</sup> Devos notes at 72 that he found no treatises on cryptanalysis in the Spanish archives at Simancas; the earliest Spanish work that he mentions dates from the late seventeenth century (see note 51). He remarks, though, that the Spanish archives lost a considerable number of documents during their removal to Paris during the Napoleonic period.

<sup>15</sup> Despite my best efforts I have been unable to contact M. Viette de la Rivagerie (the variant spelling is found even in much earlier documents); Dr. Busard received the list from him in 1961 and suspects, as I do, that M. Viette de la Rivagerie is deceased at this writing. Because of the separate mention of the memoir in his list, the original might perhaps be in the hands of one of Viète’s descendants.

188

avoir proposé et conseillé au Roy son illustre legat  
 et en conséquence <sup>continuant</sup> de continuer cette foi de Caribay,  
 l'assurant que luy servir ayse y renuicer ay  
 après toutes autres ~~parties~~ plus aduantageuses factions,  
 Je puis encor représenter les arguments de Six lettres  
 qui en font foi.

Composition du chiffre ? Italie.  
 Les Italiens n'usent guere que des six Caracteres  
 1. 2. 3. 4. 5. 6. 7. 8. 9. 0. Mais ils les occupent aduantage  
 pour représenter les lettres et les Syllabes et les sons  
 propres et mots plus frequents, Encore y a il deux  
 Caracteres ordinairement qui ne leur seruent que  
 de renouer les mots et les phrases. Leur les  
 deschiffrer se fault suivre la methode egressive  
 generallement ouente singulierement ou la remarque  
 de deux ou trois ou quatre Caracteres qui précèdent  
 chaque figure et de trois ou quatre qui la suivent.  
 Et par la comparaison des ordres et suites semblables  
 de voyelles et de consonnes les finales, et par  
 hypothese on parviendra a la lettre.

Regle infallible quand   
 chiffres sont simples.

Quand les chiffres sont simples seront choisis  
 cinq ou six triades de Caracteres divers et voides  
 seulement d'après la conclusion sera donc Syllabotique  
 que les triades estues sont les cinq voyelles au six,  
 l' (y) comprise. par quoy si l se trouve une autre  
 triade des Caracteres tous divers des cinq autres triades  
 pour cinq lettres sera voyelle infalliblement. Et ainsi se  
 discernent les voyelles des consonnes et puis par la  
 marque des finales et hypothese se distingueront  
 les voyelles d'une les voyelles et les consonnes d'une  
 les consonnes et par leur rareté et frequence par individus.

Extension de la Regle quand les chiffres  
 seront composés.

En mesme Regle se peut entendre aux chiffres doubles

Frédéric Ritter's transcription of Viète's memoir, showing Viète's "infallible rule" (discussed on pp. 12-14 below).

Bibliothèque de l'Institut de France, Paris,  
 Ms. 2009, f. 188. Reproduced with permission.

the historian of mathematics T. Richard Witmer in 1983 as “lost.”<sup>16</sup> In fact, Ritter’s papers are preserved in the Bibliothèque de l’Institut de France in Paris and should prove to be a valuable resource for scholars of Viète, as they have been for me.<sup>17</sup> After completing my work I learned of the unpublished doctoral thesis of Jean Grisard in which this same Ritter copy of the 1603 memoir is transcribed, along with other useful materials.<sup>18</sup>

Ritter describes the “precious manuscript” which he has “before his eyes” as itself a copy of a lost original.<sup>19</sup> He says that the copy from which he worked was among papers bequeathed to the city of Fontenay-le-Comte by Benjamin Fillon, an archaeologist and friend of Ritter’s who also collected materials on Viète, though the municipal archivist of Fontenay-le-Comte says the archives have no record of such a memoir.<sup>20</sup> However, it seems to me that Ritter’s transcription can be regarded as quite accurate; the evidence comes from his transcription of

<sup>16</sup> François Viète, *The Analytic Art: Nine Studies in Algebra, Geometry, and Trigonometry* from the *Opus restituta mathematicae analyseos, seu Algebrâ Novâ*, tr. T. Richard Witmer (Kent, Ohio: Kent State University Press, 1983), 1; a very necessary corrective to Witmer’s editorial methods is given in the review by Richard Ferrier, “The Analytic Art of Viète: A Review Essay,” *St. John’s Review*, 38 (1988/89), 67-74.

<sup>17</sup> Bibliothèque de l’Institut de France Mss. 2004-2012, Manuscrits de Frédéric Ritter relatifs à François Viète. In this collection Mss. 2004-2008 consist of Ritter’s translations of Viète’s mathematical works; Mss. 2009-2012 contain the unpublished version of Ritter’s “François Viète, inventeur de l’Algèbre moderne; sa vie, son temps, son œuvre.” The memoir of 1603 can be found in Ms. 2009, ff. 182-189, and will be cited hereafter as BIF Ms.:2009. I am grateful to Madame Annie Chassagne, Conservateur en Chef de la Bibliothèque de l’Institut de France, for her unfailing and kind help in using these collections. I am especially grateful to Mrs. Margo Chávez Charles for her invaluable assistance in copying and arranging for reproduction of these documents, as well as for much generous help in other inquiries without which I could not have completed these researches. I acknowledge the gracious permission to quote from these manuscripts granted by the Bibliothèque; all translations are my own.

<sup>18</sup> Jean Grisard, “François Viète, mathématicien de la fin du seizième siècle,” unpublished Thèse de troisième cycle, École Pratique des Hautes Études, VI-ème section, (1968), listed in Warren Van Egmond, “A Catalog of François Viète’s Printed and Manuscript Works” in *Mathemata: Festschrift für Helmuth Gericke*, ed. Menso Folkerts and Uta Lindgren (Stuttgart: Franz Steiner Verlag, 1985), 359-396 at 393. Grisard transcribes Ritter’s copy of the 1603 memoir at 123-128. Grisard also briefly discusses the bibliography of Viète’s activities in cryptanalysis (25-26), transcribes Henry’s letters of 1585 regarding Viète’s resuming his official post (150-151) as well as Viète’s letters of 1590 to Henry (129-133), and gives Tessier’s translation of de Thou’s life of Viète (166-169). After completing my work I also found a brief popular account of Viète’s memoir based on Grisard by Jean-Paul Guichard and Jean-Pierre Sicre, “François Viète: Un juriste mathématicien” in *Aventures Scientifiques: Savants en Poitou-Charentes du XVI<sup>e</sup> au XX<sup>e</sup> siècle*, ed. Jean Dhombres (Poitou-Charentes: Les éditions de l’Actualité Poitou-Charentes, 1995), 222-235 at 231-234. I thank Madame Virginie Dupuy-Garric, of the Bibliothèque Municipale de Fontenay-le-Comte, for drawing my attention to these works and for her devoted and knowledgeable help.

<sup>19</sup> Ritter says that he deduces this from the erasures in the text. Though somewhat unclear, his presumption seems to be that the original presented to the duke of Sully would have been left without erasures while copies might have been allowed to have them. On the other hand, Ritter notes that his copy bears the superscription “Mons<sup>r</sup> Viète pour les chiffres” in the hand of Sully himself. It should also be noted that the memoir is addressed to “M de Rosny,” Sully’s other style as Marquis de Rosny.

<sup>20</sup> The municipal library and archives of Fontenay-le-Comte have no record of such a memoir, nor any further record of the descendants of the family Viète (or Viette) (letter from Madame Dupuy, August 7, 1995). Grisard writes at 123 that he also searched for the original memoir in the municipal and departmental archives without success; he judges that the original is “presently unfindable.”



the “Règles de Viète,” to be discussed later.

Ritter attaches special importance to this memoir, dated “at the beginning of the year 1603,” a few weeks before Viète died on February 23, 1603, because it is, he feels, “without doubt the last work of a great citizen thinking in his last moments of the interests of his king and of his country.” Thus Viète, near death, is concerned with recording his techniques of cryptanalysis so that his secrets might not die with him. It is not clear from the memoir whether the impetus for this disclosure came from Viète himself or from Sully; clearly the techniques were then uncommon. Although Viète avers that he never has “at all hidden the way which I have taken but I have always shown the light to those who asked me on behalf of the king,” nevertheless he is aware that among those who might have been instructed in such matters “some did not understand and others lacked enough discretion and fidelity to commit to them the secrets of the state.”<sup>21</sup> Besides illustrating the problem of finding sufficiently trustworthy cryptanalysts, Viète’s remark shows that his techniques were difficult to understand and unfamiliar, at least to the extent that he felt moved to disclose them so unambiguously that these obstacles might be decisively overcome.

Early in the memoir Viète avers that he “will not last long,” that he is near death and moreover that “those who were more competent in this work [than himself] are no longer alive.”<sup>22</sup> This sense of urgency makes understandable the disjointed character of the memoir, often hurried and cryptic. Viète said on his deathbed he wanted nothing to do with either a priest or a physician.<sup>23</sup> What roused him to his final statement was his pressing sense of political danger, seemingly not less acute even though many of the “recent troubles” with which he begins his memoir were years in the past as he wrote. However, his mention in the memoir of specifics of the latest ciphers of Spain and Italy that he had seen also indicates that he continued to solve ciphers in 1603.

As he begins his disclosures, Viète is notably concerned with certain political matters that press in on him, underlining the importance and delicacy which cryptanalysis has come to involve in his experience. He reveals more fully than in his 1590 publication the intricacies of Mayenne’s situation. Later in the memoir Viète digresses from technical matters to warn of the prepotent danger he discerns

<sup>21</sup> BIF Ms. 2009, f. 183.

<sup>22</sup> *Ibid.*

<sup>23</sup> This story is told by his contemporary Hugues de Salin in his *Mémoires*, a work which Ritter examined but which was sold in 1887 from the collection of the Bibliothèque de M. Feuillet de Conches and thereafter disappeared from sight; see Grisard, 26. Salin noted that Viète in the end did relent and confess so that his daughter would not be disinherited as the offspring of an atheist; Viète wanted as a physician only Duret, who could discuss mathematics with him. These quotes are preserved in Fillon and Ritter, 19; Ritter comments on Viète’s apparent lack of religiosity in “Viète,” 241.

in Jehan Baptiste de Tassis, one of the Spanish leaders.<sup>24</sup> Tassis had, in fact, been a crucial figure in French affairs from 1580 to 1585, when he was charged with establishing relations with the League. He returned to France in 1589, in the wake of Henry's victory at Ivry, and served as the ambassador to the French court from 1599 to 1604. Viète clearly judges Tassis not only a past enemy but also a present threat. His discourse breaks away into these political directions, transfixed by the great dangers only narrowly surmounted, and even more preoccupied by the revelation of yet greater menaces to come, whose existence and magnitudes have likewise been unveiled by decryption. Ambassadors are essentially "honorable spies" who report through ciphered communications, and among them Tassis is especially dangerous.

Besides these immediate political threats Viète may also have intended to have defended cryptanalysis against misunderstanding and neglect. In his *Traicté des chiffres* (1586), one of the first printed books in France on cryptology, Viète's contemporary Blaise de Vigenère described cryptanalysis as an "*exercice certes d'un inestimable rompement de cerueau, & en fin un travail tout inglorieux*" ("certainly an exercise of an indescribable cracking of the brain, and finally quite an inglorious labor") and devotes his own treatise in large part to the construction of more secure ciphers, rather than the elaboration of techniques for solution.<sup>25</sup> Vigenère here advanced a disparagement of cryptanalysis that continued to have important advocates in France during the following century, including Voltaire, who in 1771 derided cryptanalysts as "as great charlatans as those who boast of understanding a language which they have not even studied."<sup>26</sup> But Viète, who knew better, wrote to preserve a technique of value in state affairs. He does not recommend merely cultivating codebreakers of great native talent but even more the implementation of "infallible rules" that will remedy the lack of understanding that he says he had encountered in his earlier attempts to teach his methods to others.

Turning from his political preamble to the body of his memoir, Viète seeks to

---

<sup>24</sup> Devos, 47-48, gives a brief biography of "Jean-Baptiste de Tassis ou Taxis" and gives the ciphers he used at 300-303 (1580-1584, 1589-1590), 318-327 (no date), 335-350 (1595), 539-547 (1604).

<sup>25</sup> Blaise de Vigenère, *Traicté des Chiffres* (Paris: Abel l'Angelier, 1586), f. 12r; see also Kahn, 145-150. The earliest French book published on cryptography is Gabriel de Collange, *Polygraphie et Vniuerselle escriture Cabalistique de M. I. Trithème Abbé* (Paris: Jacques Kerver, 1561), a heavily edited translation of Trithemius' *Polygraphiae libri sex* (1518).

<sup>26</sup> Voltaire's attack on cryptanalysis is found in his article "Poste" in his *Questions sur l'Encyclopédie* (1771), included in the *Dictionnaire philosophique, Œuvres complètes de Voltaire*, ed. Louis Moland (Paris: Garnier Frères, 1879 [Nendeln/Lichtenstein: Kraus Reprint Ltd, 1967]), 20:257-258. In 1716 the diplomat François de Callières asserted that the reputation of cryptanalysts "rests largely upon the ineptitude of poor ciphers rather than upon their discovery of a good cipher" since "a well-made and well-guarded cipher is practically undiscoverable except by some betrayal"; *On the Manner of Negotiating with Princes*, tr. A. F. Whyte (Notre Dame: University of Notre Dame Press, 1963), 142-143. See also Kahn, 174.

persuade his reader that “once the composition [of Spanish and Italian ciphers] has been understood in one instance, the resolution is not difficult.”<sup>27</sup> He makes this encouraging assertion after having observed that both Spanish and Italian ciphers are “subtle in their composition” even though the Spanish are “crude in using them.” The Italians, on the other hand, are “very subtle in their usage” as well as in their composition. Though he will point out crudities of usage that can lead to solution if rightly exploited, Viète’s exposition does not depend only on such exploitation. His presentation leads up to his “infallible rule” whose efficacy will prove greater than the occasional lucky guess or the mistakes of cipher clerks.

### VIÈTE’S CRYPTANALYTIC TECHNIQUES

Most of the memoir is devoted to the analysis of Spanish ciphers—nomenclators all. Viète’s exposition seeks general empirical principles that go beyond particular solutions, so that the cryptanalyst might understand the characteristic features of the variations on the “one general cipher,” by which he seems to mean the *cifra general* used by the king of Spain “for all his viceroys and ambassadors.” Beginning in *medias res*, as if his reader were already familiar with the simplest forms of ciphers, he first discusses refinements. He outlines the way the Spaniards use three or four symbols for each letter of the alphabet, and one or two for each syllable, besides the use of jargon or codewords, one set for frequent words and another for proper names. Further, they disguise telltale double letters, writing “v” or “s” or “l’C” after a vowel that is doubled. They indicate mutes by accents over the figures; they encipher by syllables of two or three letters, instead of by individual letters. He points out that they break up long words in different ways to avoid repetitions.

Though Viète does not specify it, all these techniques show awareness of the vulnerability of ciphers to analysis by the frequency of occurrence of each symbol or group of symbols; his analysis will gradually unfold the ways he has developed to pierce through the Spanish stratagems and bring frequency analysis to bear. He sets forth a number of what he calls practical “observations.” In his first, he notes that each letter from an ambassador to his king is generally sent in two to four copies; if all are intercepted, they can be compared to reveal the variations the different clerks have employed for the same words. This can reveal equivalent symbols.

Of particular interest is Viète’s second observation, in which he notes that “in ciphers there are always some essential numbers [*chiffres essentiels*],” by which

---

<sup>27</sup> BIF Ms. 2009, f. 184.

he means symbols that stand for numbers, rather than alphabetic characters.<sup>28</sup> That is, the Spanish seem to use “some kind of accent or other mark of the essential number” so that the number 13 can be read as such and not mistaken as a code symbol for some letter. If one can locate these numerical “essential ciphers,” one may have a powerful tool for cryptanalyzing the nearby symbols. In his examples, if one sees “4000” and nearby “500” a likely guess is that the text is speaking of 4000 infantry and 500 horse, which would yield a probable identification of the words following those numbers as “infantry” and “cavalry.” In contrast “100,000” would precede numbers not of men but of ducats. The numbers in dates are similarly revealing, as are locutions like “12 m 38 13,” where the essential ciphers 12 and 13 (marked by underlining) are deduced to be joined by *ou* (“or”, enciphered letter by letter as “m 38”).

In his third observation Viète points out that Spanish dispatches contain a number of stereotypical phrases almost inevitable in each type of document. For instance, documents written in numbered articles will usually begin with “memorial y instruction.” No less helpful are such phrases as “que que” (equivalent to the Latin “Item item” or English “moreover”) or “copia de,” which are often encountered.

Viète notes in his “fourth and general observation” that, when there is no occasion for his preceding techniques, disclosure will be more difficult. Yet there is still a “general method for success,” namely frequency analysis. “One must note all the sorts of figures, whether ciphers or jargon, and count how many times they occur, then note all the sorts of figures which precede or which follow and compare the most frequent in order to discover the same words, and the same meanings. Don’t spare either labor or paper.”<sup>29</sup> Here he has either rediscovered or restated the principle which Italian cryptologists such as Alberti, the Argentis, Soro, or Porta had been using for more than a century and which had been known to the Arabs even earlier.

This method comprises also the formation of “hypotheses” based on the tentative identifications yielded by the frequencies of symbols and groups of symbols. First and foremost is the identification of vowels, characteristically fewer in number than consonants but frequent in quantity because of their involvement in the formation of syllables. This is the heart of Viète’s “infallible rule when the ciphers are simple” (i.e., when each symbol represents only one letter). He also relies on it in his “extension of the rule when the ciphers are composite.” In either case, a sufficiently penetrating analysis will always reveal the underlying linguistic structure of vowels and consonants.

---

<sup>28</sup> *Ibid.*, ff. 185-186.

<sup>29</sup> *Ibid.*, ff. 186-187.

Viète accomplishes this analysis in general by observing the frequency of dyads and triads of symbols. Here his exposition is particularly terse and cryptic. I will illustrate my interpretation of his method by using an example of a monoalphabetic cipher given by Kahn.<sup>30</sup> After making a simple frequency tally of single symbols, Viète enumerates how many triads there are which do not contain the same symbols. In Kahn's example these may be listed as GJX, ZNU, COT, QHY, and EAF, by starting from the beginning of the ciphertext and noting the successive triads that consist of three different letters. Viète asserts that "it follows syllogistically that in these chosen triplets are the five vowels (or six, if 'y' is counted as a vowel)." The reason is that, in French, Spanish, and Italian, there are no common triads without a vowel.<sup>31</sup> Thus in these chosen triads we expect to find all the vowels, one or two each per triad. If we had begun at some other point in the ciphertext we might compile a different list, but it always contains just 5 or 6 members—the number of vowels in English.

Viète extends this result by making a similar list of dyads, taking them without overlapping. In Kahn's example these are: GJ, XX, TZ, NU, CO, HY, AM, VQ, and FK. Several of these do not contain vowels, since there are several common dyads in English composed only of consonants, like "th," "nd," and "st." Interestingly, in Spanish all common dyads contain at least one vowel, so in a Spanish cryptogram there would again only be 5 or 6 such dyads.<sup>32</sup> At this point Viète tersely advises us to "compare [*voir*] the dyads," which I interpret to mean that we compare the list of triads with the list of dyads to see where they overlap. In our example we note that GJX overlaps with GJ, ZNU with NU, COT with CO, and QHY with HY; EAF overlaps only in one symbol with AM and FK. The single symbol frequency count has already revealed that N probably is the most frequent letter, *e*. Then Z should be a consonant, and U either a consonant or *a*, the vowel most frequently found after *e*. Likewise, either G or J is a vowel (unless XX is the less frequent *oo*), either C or O is likely to be a vowel, and either Q is a vowel and neither H or Y are, or one of H or Y is a vowel and Q is not. In our example, it turns out that in the end his rule is obeyed by our triads: GJX (*suc*), ZNU (*dea*), COT (*lin*), EAF (*for*), and QHY (*yth*). At this point we have gained quite a bit of information about one-third of the symbols and have narrowed down several alternative hypotheses which can

---

<sup>30</sup> Kahn, 99-105.

<sup>31</sup> More precisely, this statement holds for the 25 most common trigraphs in these languages; in English the 24th most common trigraph is "sth" so Viète's rule is slightly less valid there. See Laurence Dwight Smith, *Cryptography* (New York: Dover, 1955), 153-155.

<sup>32</sup> Viète goes on at f. 189 to equate "the number of triads of different characters" to that of "dyads themselves (particularly in Italian and Spanish)," which confirms my interpretation of his technique since only in those languages do the common dyads almost always include a vowel (the exception is the dyad "nt" in Italian).

each be followed. Here Viète directs us to try out these hypotheses successively, noting particularly the final letters of words, assuming the word divisions have been left intact.

He can extend this method when there are homophonic substitutions. “For the number of triads of different characters or of dyads themselves (particularly in Italian and Spanish idiom) reveals that there are the same number of different characters to represent the vowels or syllables or entire words.” For instance, if two symbols are used for each vowel, Viète expects to find 10 or 12 independent triads, rather than the 5 or 6 for a purely monoalphabetic cipher.

Viète’s “infallible rule” goes beyond simple frequency counts and leads to a marked simplification of the cryptanalytic problem. It relies not on probable words but only on a few invariant features of the language. Thus by “infallible” Viète means a methodical marshalling of alternatives, whose mathematical character he prefers to fallible guesswork. I argue that this represents a fundamental advance over the methods of cryptanalysis set forth by Viète’s predecessors.

### THE DUPUY MANUSCRIPT OF THE “RÈGLES DE VIÈTE”

Besides this newly recovered account of Viète’s methods, another description of them exists in the Dupuy collection of manuscripts in the Bibliothèque Nationale, which has received scarcely any attention, as far as I am aware. This brief manuscript is undated and unsigned, though it has been given the title “*Règles de Viète pour le déchiffrement des écritures secrètes*” in the listing of the manuscripts collected by Pierre Dupuy, librarian to Louis XIV.<sup>33</sup> Since it refers to the Moreo decryption published by Mettayer in 1590, an earliest possible date is thus established; the tone and tense suggest that it may have been written after Viète’s death in 1603, as if it were a brief résumé of his methods. It could have been written no later than 1648, the date of the whole collection in which it is found.

Ritter refers to this document as the “*Memoire de Peiresc sur la façon de déchiffrer de Sieur Viète*” and refers to them briefly in his published essay; in his draft biography he copies them out in full.<sup>34</sup> His transcription is in excellent agreement with the extant source, with the exception of minute details of orthog-

<sup>33</sup>Bibliothèque Nationale, Ms. Dupuy 661, ff. 219r-220r; this is not included in Grisard or in Van Egmond’s bibliography. The general title of this group of manuscripts is “*Memoirs fort singuliers servans à l’Histoire de France depuis le Roi Charles IX*” and bears the date 1648. I would like to express my particular thanks to Madame Marie-Pierre Laffitte, Conservateur en Chef, Département des Manuscrits, for drawing my attention to this manuscript and for her help in ascertaining its provenance; I also thank the Bibliothèque Nationale for permission to cite the text of this manuscript.

<sup>34</sup>Ritter, “Viète,” p. 257; BIF Ms. 2009 ff. 180-182. He states that the original is in the Bibliothèque de Carpentras; Grisard, 25, notes that it is no longer listed in the catalogue of manuscripts of that library.

raphy that might well have differed in different copies or which are genuinely hard to read and thus subject to differing interpretations. Even when Ritter silently emends the text to regularize its orthography he follows his original closely. This supports the reliability of his transcription of the 1603 memoir.

The mention of Peiresc may clarify the exact date and source of these “Règles.” Nicolas-Claude Fabri de Peiresc (1580-1637), the remarkable polymath and collector, could well have been interested in cryptology, though I have found no direct discussion of it in his voluminous correspondence. Occupied especially in 1631-1633 with collecting Egyptian antiquities, he conferred with Athanasius Kircher – author of a book on cryptology – about the problem of hieroglyphs.<sup>35</sup> His interest in deciphering ancient Egyptian writings might well have drawn his attention to Viète’s “infallible rule.” Peiresc was acquainted with Viète’s astronomical works and, on the death of Viète’s secretary Jacques Alleaume in 1627, worked with Jacques Dupuy to see that Alleaume’s books and scientific instruments were placed in the royal library.<sup>36</sup> Among Alleaume’s effects Peiresc lists several works of Viète; since Alleaume worked with Viète on decryption it might well be that these “Règles” were among these posthumous papers. Thus 1627-1628 might be a good estimate of the date Peiresc encountered Viète’s cryptanalytic techniques.<sup>37</sup>

These “Règles” agree with Viète’s own account and provide a few interesting sidelights on it as well. It begins by observing that “Monsr. Viète had rules for deciphering all sorts of ciphers that were so sure that they were almost infallible.” If indeed this document reflects how Viète’s methods were viewed by the generation that immediately followed him, it confirms that it is his *methods*, and their infallibility, that are more to be remarked than his individual feats of cryptanalysis. The writer clearly indicates that this method enabled Viète to accomplish his prodigious feats – a method that du Lys, one of Viète’s secretaries, could also

<sup>35</sup> For Peiresc’s activities in Egyptology see Sydney Aufrère, “Peiresc et sa connaissance de l’Égypte,” in *Peiresc ou la passion de connaître*, ed. Anne Reinbold (Paris: Librairie Philosophique J. Vrin, 1990), 139-152, who notes at 147 that Peiresc had the prescience to realize that “the decipherment of ancient Egyptian goes through knowledge of Coptic.” For Kircher’s work in cryptology and hieroglyphs see Kahn, 154, 904-905.

<sup>36</sup> See Peiresc’s letter of November 11, 1627, in *Lettres de Peiresc aux Frères Dupuy*, ed. Philippe Tamizey de Larroque (Paris: Imprimerie Nationale, 1888), 1:408-409. Jacques Dupuy’s reply of December 28, 1627, at 895-896. De Thou also mentions that Aleaume was entrusted with the publication of Viète’s manuscripts by his heirs.

<sup>37</sup> It may well be that the “Règles” are not the original text of Peiresc but notes taken by the Dupuy brothers, perhaps copied from material sent them by Peiresc, as is suggested by Francis W. Gravit, “The Peiresc Papers,” *The University of Michigan Contributions in Modern Philology*, No. 14 (February, 1950), 1-57, at 18-20, 55. The other materials in Ms. Dupuy 661 are dated 1628-1629; Ms. Dupuy 243 includes material on the history of the League, presumably copied from Peiresc. Gravit also mentions (at 17) that Ms. nouv. acq. fr. 3283, which includes the “Règles,” contains some of the notorious *feuilles volantes* stolen in 1830-1846 by Guillaume Libri from the Bibliothèque de Carpentras. Libri also purloined about 1738 other folios of Peiresc material from Carpentras.

employ to cryptanalyze nearly as fast as Viète himself. Thus Viète was able not only to set forth his method but to instill it in others very effectively.<sup>38</sup>

In its account of his methods, the Dupuy manuscript is more elementary than Viète's memoir. It contents itself with a description of the simple process of determining the frequency of each character, together with an interesting simile for recording those frequencies. "He set up a paper as if it were for writing notes of music," presumably with many staves on which one could tally the occurrences of each character systematically.<sup>39</sup> From this one realizes that the elementary process of recording frequencies was, for the writer and probably many of his readers, quite novel and had to be spelled out at such length. For the rest, only the most elementary aspect of the deduction from frequencies is mentioned, that "the most frequent stood for the vowels. Following the most frequent vowel ('e' in French and 'o' in Italian) [he found] also the others; the less frequent stood for the consonants, and the most varied those which are not put in use except very rarely." The use of the frequencies of groups of letters "like *ss*, or different letters like *qu*" is mentioned in passing, though with some indication that Viète used this test "principally."

The "Règles" conclude with the statement that the king's couriers would wait while Viète worked on the intercepted dispatches that they brought. Another remark marvels that Viète "deciphered in languages which were unknown to him, principally in Spanish, where one day he suddenly found out a word and at once acquired the language and deciphered all the rest of the cipher in fifteen days." Here the writer is struck with the strange power Viète's method has given him to read even in unknown languages; one recalls Voltaire's utter disbelief in such a feat. Both opinions manifest a lack of prior acquaintance with cryptanalytic methods, confusing them with the ordinary process of reading. Also recorded in the "Règles" as a marvel is Viète's ability to decipher "up to decuples"—apparently ciphers that use as many as ten homophone substitutions for a single letter—"which is something almost incomprehensible." The manuscript ends

---

<sup>38</sup> Grisard, 26, gives a helpful note on these secretaries, naming them as M. Charles du Lys (in the "Règles" called du Liz, a collateral descendent of Joan of Arc through her brother Pierre) and Pierre Aleaume (elsewhere called Jacques); Ritter mentions at 270 that du Lys and Aleaume translated Viète's mathematical works into French and published them in 1600 "with the agreement of the author." Peiresc himself corresponded with du Lis (his spelling), to whom he forwarded some anagrams, indicating another aspect of their common interest in decryption; see Tamizey de Larroque, 1:404 (Peiresc to Dupuy, October 16, 1627), 64-66 (Peiresc to Dupuy, July 26, 1625), 891 (Dupuy to Peiresc, November 9, 1627), and the mention at 65 n. 1 of Peiresc's letters to du Lis from 1612-1627.

<sup>39</sup> Here one wonders whether Viète was familiar with those Spanish ciphers that used musical notation on staves, such as the *Cifra particular* of 1564, given in Devos, 219. The *Argentis* also used a kind of cipher with musical staves; see Devos, 69-70, and Aloys Meister, *Die Geheimschrift im Dienste der Päpstlichen Kurie* (Paderborn: Ferdinand Schöningh, 1906), 112-113. See also Eric Sams, "Cryptography, musical" in *The New Grove Dictionary of Music and Musicians*, ed. Stanley Sadie (London: Macmillan, 1980), 5:78-82 at 78.



with a mention of the use of nulls to make detection of double letters more difficult.

In their brevity and elementary character these “Rules” may have been intended merely as a sketch for diplomats rather than a more comprehensive and advanced instruction for working cryptanalysts. Nonetheless, this document confirms how novel and amazing Viète’s methods seemed even to those contemporaries who had some basic knowledge. It attests to his success in drawing attention to the existence and nature of such fundamental rules of cryptanalysis. Though cognizant of the primacy of method over inscrutable individual abilities, the writer of the “Règles” still seems incredulous that the technique is powerful enough to accomplish such feats as decryption of a ten-fold cipher. Viète’s powers remain, in that writer’s view, still “almost incomprehensible,” the product of more than mere methodical application.

## COMPARISON WITH EARLIER CRYPTANALYTIC RULES

Among Viète’s compatriots and near contemporaries both Philibert Babou, first secretary of state for Francis I, and one Chorrin accomplished notable decryptions.<sup>40</sup> Vigenère’s account of Babou’s amazing solutions in languages “he did not understand any of . . . or very little” does not acknowledge that systematic cryptanalysis could replace such individual talent.

Viète does not give any sources for his methods, leaving open the possibilities that he may have discovered them independently or that he developed certain known basic principles. It is remarkable that he does not refer to the cryptological work of Porta; certainly Vigenère was well aware of it.<sup>41</sup> Even if he did know this earlier writing, though, interesting differences of style and scope set Viète’s work apart. These contrasts clarify what is original in Viète’s approach.

Though by his time nomenclators had been elaborated considerably, methodical treatments of cryptanalysis lagged behind. The earliest Western writing on cryptanalysis, Leon Battista Alberti’s *De cifris* (ca. 1466), contains detailed observations on Latin word structure, notably that “for the most part not more than one consonant occurs between two vowels in the same word. You will frequently find two consonants, but rarely three, between the vowels in the same word, and

---

<sup>40</sup>Théodore Agrippa d’Aubigné, *Histoire universelle* (1616-1618, reprinted Paris: Renouard, 1919), 8:201 and the *Confession du Sieur de Sancy* in his *Œuvres* (Paris: Éditions Gallimard, 1969), 581, note at 1285; Vigenère, ff. 34v-35r. Eugène Vaillé, *Le Cabinet noir* (Paris: Presses Universitaires de France, 1950), 47; Kahn, 151, 111-112.

<sup>41</sup>Vigenère, f. 12r, refers specifically to Porta’s *De furtivis literarum notis* as well as to Trithemius and Cardan.

four much more rarely still.”<sup>42</sup> However, though here Alberti has noticed the same linguistic structure that Viète exploits in his “infallible rule,” Alberti does not embed it in a systematic procedure. Other early rules for cryptanalysis include simple sets of recipes for isolating telltale words or syllables (such as *che* or *non* in Italian) that would lead to easy solution of monoalphabetic substitutions. Cicco Simonetta’s rules of 1474 are of this kind; he is aware, though, that it is possible to evade such techniques by using homophonic substitutions.<sup>43</sup> Such compilations of rules were not restricted to Italy; the earliest French example of which I am aware is the “*Regles de deschifrement*” in the papers of Dominique de Gabre, bishop of Lodève and ambassador of Henry II to Venice about 1550.<sup>44</sup> In de Gabre’s “*Regles*,” the principle of frequency analysis is already present in the identification of the most frequent ciphertext character with plaintext *e* (in French); there are also lists of useful words which are readily identified by patterns of repeated letters or other conspicuous characteristics.

Sixteenth-century Italian manuscripts on cryptology also emphasize the enumeration of “regole,” rules that should make ciphers more secure. Both Fedele Piccolomini and Matteo Argenti set forth such lists.<sup>45</sup> Argenti also has a separate essay on cryptanalysis that delineates an approach based on probable words and simple frequency analysis including 62 numbered “conjectures and considerations.” The manuscript of Matteo Argenti, who was the papal cipher secretary from 1591 to 1605, is of particular value to compare with Viète’s since their work was contemporaneous and presumably independent; Argenti also reveals the methods of his mentor and uncle Giovanni Battista Argenti, papal cipher secretary from 1585 to 1595. It is also interesting to realize that Cardinal Cinzio Aldobrandini, nephew of Pope Clement VIII, asked that Matteo accompany him during his service as the papal nuncio to France in 1600.<sup>46</sup> Since Viète expressly

---

<sup>42</sup>The Latin text of Alberti’s *De cifris* is included in Meister, 125-141 at 133, and in a collated version in Leon Battista Alberti, *Dello Scrivere in Cifra*, ed. Augusto Buonofalce (Turin: Galimberti Tipografi Editori, 1994); I give the translation of Charles J. Mendelsohn in his unpublished notes on Alberti, at f. 18, in his miscellaneous manuscripts in the Special Collections of the Van Pelt Library at the University of Pennsylvania, whom I thank for permission to quote.

<sup>43</sup>Kahn, 100-111. See also P.-M. Perret, “Les Règles de Cicco Simonetta pour le déchiffrement des écritures secrètes,” *Bibliothèque de l’École des Chartes*, 51 (1890), 516-525, containing the Latin text of his rules at 523-525; for a more recent edition see *I Diari di Cicco Simonetta*, ed. A. R. Natale (Milan: A. Giuffrè, 1962), 1:124-126. The manuscript of Simonetta’s “Regulae ad extrahendum litteras ziferatas sine exemplo” can be found in Bibliothèque Nationale, Ms. italien 1595, ff. 441-442. See also Walter Höflechner, “Die ‘Regulae ad extrahendo litteras ziferatas sine exemplo,’” *Mitteilungen des Österreichischen Staatsarchivs* 23(1970), 377-384.

<sup>44</sup>Reprinted in Pierre Speziali, “Aspects de la Cryptographie au XVI<sup>e</sup> siècle,” *Bibliothèque d’Humanisme et Renaissance*, 17 (May, 1955), 188-206 at 198-202.

<sup>45</sup>Their brief treatises are included in Meister, 142-170.

<sup>46</sup>See Speziali, 191, and Meister, 60.

mentions details of the ciphers of Aldobrandini at the end of his 1603 memoir, the distinct likelihood emerges that Viète had, in fact, cryptanalyzed Argenti's ciphers.<sup>47</sup> And since Viète presented his writings on calendrical reform to Cardinal Aldobrandini at Lyon in 1600 the piquant possibility exists that Argenti and Viète might have met and even compared notes!<sup>48</sup>

In comparison with Viète's rules, Argenti's are less rigorous, more miscellaneous, and altogether far more indebted to the use of probable words than to reliance on frequency analysis. Argenti has nothing to compare with Viète's "infallible rule"; presumably, Argenti could cryptanalyze quite successfully without needing to employ or formulate such an abstract method. In fact, in many cases shrewd guesses of probable words were more rapid than Viète's method. Nevertheless, Viète's formulation shows his turn of mind to have been notably different than Argenti's; where Argenti is informal and verbal, Viète in contrast aims for "syllogistic" methods whose formal scope will make solution more nearly certain than probable words, no matter how inspired the guesses. More broadly expressed, these techniques share the methodical and symbolic quality of the new "analytic art" of algebra which Viète was engaged in founding.

Thus in one general rule Viète aims to comprehend what Argenti treats in 62 miscellaneous items. The particular advantage of Viète's compact analysis emerges more clearly when considering ciphers with homophonic substitutions. Viète's method is more powerful because it can be extended to such cases of a "complex" cipher; his analysis of triads and dyads will still locate the vowels as elements of diphthongs even under this more artful disguise. As such, it may represent one of the earliest expressions of the full generality of frequency analysis, extending to a greater range of complex ciphers what had been for the Italians a more rudimentary device. It is certain that they had already been able to solve complex ciphers; what seems to be new about Viète's work is the formulation of these solutions under a single general rule, rather than as a congeries of less systematic attempts.

---

<sup>47</sup> Argenti also made nomenclators for several other papal nuncios in France throughout the period of Viète's known cryptanalytic activity; though there is no direct evidence, it seems likely that any attempt by Viète to read papal instructions regarding the activities of the League would also have shown him samples of Argenti's cryptologic art. See Meister, 341-342 (general cipher for nuncios in 1585-86), 345-348 (1585), 370-374 (1586), 393-394 (1587), 420-426 (1589); this nuncio, Cardinal Caetano, was sent by Pope Sixtus V specifically to guide the activities of the League against Henry of Navarre, though soon thereafter the situation changed as a result of Henry's reconciliation with the Roman see, 437-442 (1591). Meister does not include any cipher by Argenti for Cardinal Hypolito Aldobrandini except for one used during his tenure as legate in Poland in 1588 (400-402). On the other hand, it was Chorrin, rather than Viète, who solved the ciphered dispatches to Cardinal Caetano in 1589; see Kahn, 151.

<sup>48</sup> Interestingly, Argenti expressed great admiration for the state of cryptological knowledge in France, which might indicate his awareness of Viète's work; see Yves Gylden, "Cryptologues italiens aux XV<sup>e</sup> et XVI<sup>e</sup> siècles," *Revue Internationale de Criminalistique*, 4 (1932), 195-205 at 197. The story about Viète presenting his writings to Aldobrandini is found in de Thou and in Ritter, "Viète," 271-272.

Even if Viète had read Porta's *De Furtivis Literarum Notis* (1563), he would not have encountered the sort of rules he himself formulated but rather the same situational strategies as Argenti sets forth. Indeed, Porta specifically asserts that no one could boast of having any such infallible rules for cryptanalysis "without exposing himself to a charge of insanity."<sup>49</sup> If indeed Viète thus disdained Porta's insight as a cryptanalyst, he was not alone in his opinion. Writing in 1653, the distinguished English mathematician and cryptanalyst John Wallis also considered Porta as having no "general Directions" for cryptanalysis except

such as were obvious from the Nature of the Thing, and which I had before of myself taken Notice of, and made use of so farre as the Nature of an intricate Cipher would permit. But the Truth of it is, there are scarce any of his Rules, which the present Way of Cipher (which is now much improved, beyond what, it seemes, it was in his Days) doth not in a Manner wholly elude . . . those being onely fitted to such a Kind of Cipher, as it seemes, was at that time in Use, . . . but can afford little or no Help in those perplexed Ciphers, which are now used.<sup>50</sup>

Interestingly, though his experience—like Viète's—seems to have been limited to nomenclators and occasional monoalphabetic, yet Wallis wrote that, in his view, in general a cipher "doth not admit any constant Method for the finding of it out," leaving the cryptanalyst only to "make the best Conjectures hee can, till hee shall happen upon something that hee may conclude for Truth." If this statement can be taken at face value, Viète's systematic aspirations exceeded anything Wallis thought possible even 50 years later.<sup>51</sup>

---

<sup>49</sup> Giovanni Battista Porta, *De Furtivi Literarum Notis* (Naples: Apud Ioan. Mariam Scotum, 1563), Book III; the quote given is found at 153 of a translation by Keith Preston (1916), "On Secret Notations for Letters, Commonly Called Ciphers," whose typescript is in the Fabyan Collection (No. 511) of The Library of Congress. I thank Paul Corley for his kind assistance in examining this manuscript for me.

<sup>50</sup> John Wallis, "A Collection of Letters and other Papers, which were at severall times intecepted, written in Cipher," 1653, Oxford University, Bodleian Library, Ms. e Mus. 203, in preface, which is reprinted under the heading "A Discourse of Dr. Wallis" in John Davys, *An Essay on the Art of Decyphering* (London: Gulliver & Clarke, 1737), 9-23 at 13-14.

<sup>51</sup> For Wallis's cryptanalytic career see Kahn, 166-169. Wallis's disclaimer of a general method may have been intended in part to conceal his own methods; see my "Secrets, Symbols, and Systems: Parallels between Cryptanalysis and Algebra, 1580-1700," as yet unpublished. One Spanish treatise dated 1668 asserts that "the general rules [of cryptanalysis] are uncertain and faulty"; another Spanish work dated between 1676 and 1714 describes the science of cryptanalysis as "the most difficult of all" since "the decipherer has nothing to back up his researches; he works in the unknown" (H. Seligmann, "Un traité de déchiffrement du XVII<sup>e</sup> siècle," *Revue des Bibliothèques et Archives de Belgique* 6 (1908), 1-19 at 4-9). This second treatise is given in its entirety in J. P. Devos and H. Seligman, *L'Art de Deschiffrer* (Louvain: Publications Universitaires de Louvain, 1967), and at 14-22 gives eleven maxims which, though less telling than Viète's "infallible rule," supply generalities concerning repetition and frequency in relation to groups of letters.

## CONCLUSION

Viète does not seem to have been aware of polyalphabetic ciphers; if he had been, he might have been more diffident about the scope of his “infallible rule.” In contrast, Vigenère’s scepticism about cryptanalysis perhaps reflects his cognizance of these far more intractable ciphers. However, the further development of cryptanalysis generally confirms Viète’s confidence. Even though his rules were not adequate to polyalphabetics, later, more sophisticated, rules were eventually able to solve them. Those later rules of Kasiski and Kerckhoffs share with Viète’s rules the same fundamental approach, which relies on systematic symbolic examination rather than on ingenious guesswork. They also rely on mathematical deduction rather than on semantic artifice, since polyalphabetic ciphers efface almost all outward trace of the language underneath. Thus the paradigm for cryptanalysis moved from chance and hypothesis towards the rigor of modern algebra.

Viète’s cryptanalytic work may have informed his foundational work in algebra, and vice versa.<sup>52</sup> His “infallible rule” of decryption manifests the same ambitious methodicalness as the “analytical art, or new algebra” that he pioneered. Both these enterprises could bear the bold motto which concludes Viète’s seminal algebraic work, *In Artem Analyticem Isagoge* (1591), which claimed to appropriate “to itself by right the proud problem of problems, which is: TO LEAVE NO PROBLEM UNSOLVED.”<sup>53</sup> These new documents suggest that this interpenetration of cryptanalysis by mathematics was begun by Viète, but it did not end with him. This connection was not lost on those who, like Wallis and Leibniz, concerned themselves with both of these enterprises after Viète’s death. Wallis and Leibniz corresponded about the possibilities of methodical cryptanalysis; they discussed a review of Wallis’ *Treatise on Algebra* (1685) that compared Viète to Wallis, who “excels in solving or (as is vulgarly said) deciphering cryptograms, and this science has a great affinity with those [mathematical sciences] which are handed down in this work.”<sup>54</sup> Leibniz was clearly interested in cryptology as a model for his nascent universal mathematics. And cryptanalysis continues today

---

<sup>52</sup>See “Secrets, Symbols, and Systems.”

<sup>53</sup>François Viète, *In artem analyticem Isagoge, Seorsim excussa ab opere restitutae Mathematicae Analyseos, seu Algebra Nova* (Tours: Jamet Mettayer, 1591), in *Francisci Vietae Opera Mathematica*, ed. F. van Schooten (Leyden: Elzevir, 1646 [reprinted Hildesheim: Georg Olms Verlag, 1970]), at 12. For a seminal discussion of Viète’s mathematical achievement see Jacob Klein, *Greek Mathematical Thought and the Origin of Algebra*, tr. Eva Brann (New York: Dover Publications, 1992), 150-185; this volume includes a fine annotated translation of Viète’s *Isagoge* by J. Winfree Smith at 313-353 (the passage cited is at 353; capital letters in original).

<sup>54</sup>This anonymous review of John Wallis’ *A Treatise of Algebra* (1685) in the *Acta Eruditorum* (June, 1686), 289, is quoted in a letter from Leibniz to Wallis dated March 19/29, 1697 in John Wallis, *Opera mathematica* (Oxford: 1685 [reprinted Hildesheim: Georg Olms Verlag, 1972]), 3:674.

to consummate its union with mathematics.<sup>55</sup>

Viewed purely within the domain of cryptanalysis, Viète's "infallible rule" represents a critical breakthrough of self-aware method that dared to formulate precise ways to leave no cipher unsolved. Though secret, Viète's memoir could well have had an important influence on his immediate successors, as further documents may yet illuminate. His decryptions were noticed throughout Europe and could not have escaped the attention of other cryptanalysts. Though not privy to his secrets, from those remarkable solutions his peers divined that Viète was not merely a notable talent but that he had shaped a new and puissant art. Viète devised for the first time techniques that aimed to be fully general and sufficient to solve any nomenclator. By implementing this new level of generality he deserves to be considered the originator of modern cryptanalysis.

**TRANSLATION OF VIÈTE'S MEMOIRE OF 1603  
AS TRANSCRIBED BY FRÉDÉRIC RITTER  
BIBLIOTHÈQUE DE L'INSTITUT DE FRANCE, MS. 2009**

[182]

[F.R.] ... [Viète] addressed (in the beginning of 1603) to Sully a memoir for the use of persons to whom the King wished to entrust the decipherment of dispatches. Indeed, he died in February 1603 and his autograph memoir which we have before our eyes is without doubt the last work from the pen of a great citizen still thinking in his last moments of the interests of his king and country, and which rightly ought to be piously preserved and transmitted to posterity. Here it is:

The manner of solving the ciphers  
of Spain and Italy  
for the good of the service of the king and of  
the State of France  
presented to Monsieur de Rosni [Sully] at the beginning  
of the year 1603

[183]

During the recent troubles I solved for the king as faithfully as I could the dispatches of Spain and Italy written in cipher, where he has seen almost all of that which was attempted to the prejudice of his service and of the good of the state. I never have at all hidden the way which I have taken but I have always shown the light to those who asked me on behalf of the king. And if this service

<sup>55</sup> At a meeting of the American Mathematical Society in 1941, Adrian Albert argued that "cryptography is more than a subject permitting mathematical formulation, for indeed it would not be an exaggeration to state that abstract cryptography is identical with abstract mathematics" (Kahn, 410, 1046).

has profited or not, no one will know better than Monsieur de Mayne [the duke of Mayenne] to whom by command of his majesty several packets were shown, in order that he might know the conspiracies which his own followers were making against him, so that he prevented them from breaking up the state and opposed it with all his means. On the other side, the king of Spain wanted that [breakup], which he would complete by sending in his forces to conquer all. The advice of the duke of Parma was to enter into the kingdom and there make war against both sides, but he was not heard. He was suspected and [the king of Spain] himself doubted whether [the duke of Parma] did not want to make conquests for himself and believed rather Bernardin Mendossi, the duke of Fibia and Jehan Baptiste de Tassis, who counselled on the contrary the maintenance of the division, each however in his own way. For the duke of Feria wanted the ruin of the duke of Mayenne as a step toward achieving this; Tassis [wished] to temporize; Ernesti, that faith should be kept with him. But they all, in fact, tried many feints and deceptions on the French which finally the duke of Mayenne and his brothers perceived clearly with the aid of the deciphered packets. Those who were more competent in this work than I are no longer alive and I myself am not going to last long. And though many came to me to whom I showed very willingly that which I knew, nevertheless some did not understand and others lacked enough discretion and trustworthiness to entrust them with state secrets. That is why I compose this little memoir very gladly [184] to aid those in whom the king has more confidence. The Spaniard is quite subtle in the composition of his ciphers but crude in using them. The Italian is very subtle in his composition and very subtle in his usage. Once the composition [of these ciphers] has been understood in one instance, solution is not difficult.

### **The composition of the ciphers of Spain**

In the composition of the ciphers of Spain the king of Spain hardly uses any cipher but one general cipher for all his viceroys and ambassadors and all the viceroys and ambassadors for him.

For each letter of the alphabet they put three or four figures and for the vowels as well as the liquids [the consonants r, l] several more.

Then they form the syllables and for each syllable they put there one or two figures.

Then they make two jargons, one of the most frequent words and the other of proper names.

At the beginning they only put for syllables Ba Be Bi Bo Bu, Ca Ce Cu Co Cu &c. And when they wish to double the letter [they] put there either a “v” or an “s” or a “l’C” after the vowel, or for a mute they put accents over

the figures, other accents over the words, and struck out others for the essential numbers [*chiffres essentiels*]. Since they have been discovered they make syllables beginning with the vowels, ab, ac, ad, af, ag, ah, al, am, an, ap, aq, ar, as, at, eb, ec, ed, ef, eg, &c.

They have also since added not only the syllables of two letters beginning with consonants, but also syllables of three or four letters like bac, bad, baf, bal, bam, ban, bas, &c, band, &c.

And this is the cipher which they use now so well that they can disguise a single word in diverse forms, as for "Aldobrandino" they put "al do bran di no", as they do more commonly, or "al do b ra n din o" and other variations. [185]

Now this would be difficult to decipher if they were as fine and nimble in the usage of their ciphers as they are in composing them. But here are the observations by which I have always surprised them.

### First observation

When Tassis or another ambassador writes to his king he is not content to send the same letter one time. He would send it two, three, or four times until he learned that it had been received and he called them, in order, the duplicate or triplicate, &c. In this way one letter can be intercepted two or three times, which, when it happens, one must compare the one with the other. For although the letter may be written in the same alphabet, nevertheless one finds diversity when one of the clerks has put a word in long form, the other has put it in jargon, as "mo" which stands for "Cardinal" the other clerk has put it in the long form "Cardinal" and another has put "Card in al," which will already be a great light on the abbreviations and the form of disguises of the same word and the diversity of figures for the expression of the same term or syllable.

### Second observation

In ciphers there are always some essential numbers [*chiffres essentiels*], that is to say, [a figure] which is equivalent essentially to a number like four thousand, five hundred, one hundred thousand. An essential number is easy to recognize whether by the end of the letters for the date or by the coupling of the cipher [i.e., the joining of figures]. For in order to put "one hundred thousand" they put in long form "100,000" or for "five hundred" "500" and for "thirteen" they put "13". And because the same "13" stands for a syllable sometimes, in this case to distinguish the number from the syllable requires some kind of accent or other mark on the number, which being discovered if "13" is the essential number when one sees "12 m 38 13" at once one knows that "m 38" stands for



the word “o” which signifies “or” [ou] and that one has the words “twelve [186] or thirteen”.

And when one sees “4000” and nearby “500” one judges well that they speak of four thousand infantry and five hundred horses, and therefore the figures which follow “4000” stand for “fanti” [“infantry” in Spanish] and those which follow “500” stand for “cavalli” [“horses”].

But when one sees “100,000” that will not be a hundred thousand men, for men do not swarm in this number. This will be one hundred thousand ducats of which it will speak, and therefore the figures which follow “100,000” stand for “ducats”. In dates the letters which one judges after the essential cipher 13 or 14 indicate the month, so that if we are in March it is likely that it is January or February of which they speak. This is another great light.

### Third observation

In the packets of the king of Spain to his ambassadors often are found dispatches written in articles. On seeing this deployment one can judge that the paper [comprises] memoirs and instructions, for they are numbered and marked in their ciphers and jargons above and at the beginning. One who sets down that this mark or jargon stands for “memorial y instruction” will not be deceived by its position. And if one see often the same figure at the beginning of an article that figure stands for the words “que que” as we say in French “Item, Item” [“moreover”]. Likewise the ambassadors send to the king copies of letters which can be known by inspection. The mark or jargon or figure stands for “copy of the said letter or of the said articles” so that if there is “Na” that says at once that “Na” stands for “copia” and the letters which follow “de la lettera” [“of the letter”] or “de los capitulos” [“of the articles”].

### The fourth and general observation

When one does not have occasion for any of the preceding observations solution will be more difficult. But here is the general method for success. One must [187] note all the sorts of figures, whether ciphers or jargon, and number how many times they occur, then note all the sorts of figures which precede or which follow and compare the most frequent in order to discover the same words, and the same values. Don’t spare either labor or paper. By this one recognizes in any way the form of the composition which [governs] the cipher. And even the syllables which begin with consonants can be discerned by this from those which begin with vowels. Finally by hypotheses ( )<sup>56</sup> one can succeed in

<sup>56</sup>This erasure indicates that the document is the copy of a record [F. R.]

resolving [the cipher]. The hypotheses are made principally by the words which one sees repeated and by the beginning of the letter or notebook, and by the ends, notwithstanding [the fact that] they by artifice introduce nulls [into them]. But that is crude and is discerned at once by the order and succession of other words which one judges quite probably to be significant. That is seen better by usage than by precepts, as will be expedient to put to the test in the first packet which presents itself in order that it will yield double fruit, the one for the art [of deciphering] in general, the other for the particulars of the matter at hand.

Furthermore, there remain the number of letters [of Tassis] which I had to represent and, in a manner of speaking, spell out even before succeeding in reading them. These letters have made me form a judgement that he is very dangerous for France and the peace and tranquillity of the state. For he appears to me to be a very shrewd statesman and very subtle, knowing the characters of the French, even those who are of his party. His letters depict admirably to his king the moods, beliefs, weaknesses, and powers of the French. He has represented the state of France in maxims that the most witty might have been hindered from understanding.<sup>57</sup> Also he has succeeded in gaining peace, [188] having urged his king to content himself this time with Combray, assuring him that it would be easy for him to return later to the other, more advantageous, factions. I can still produce the originals of the six letters which prove this.

### Composition of the ciphers of Italy

The Italians hardly use any but the ten characters 1.2.3.4.5.6.7.8.9.0 but they join them together admirably to represent the most frequent letters, syllables, proper names, and words. Also there are ordinarily two characters which only serve to distinguish words and sentences. In order to decipher one must follow the method given above, [being] particularly alert to remark the two or three or four characters which precede each figure and the three or four which follow. By comparison the orders and connections of the same kinds are judged and the distribution of the final letters, and by hypotheses one will succeed in reading [the cipher].

### Infallible rule when the ciphers are simple

When the ciphers are simple let five or six triads of diverse characters be chosen and examine only the dyads. It follows syllogistically that in these chosen triplets are the five vowels (or six, if "y" is counted as a vowel). Because of this, if another

---

<sup>57</sup>[This somewhat obscure sentence may simply mean that Tassis phrased his dispatches so cleverly that they might escape detection even if read in the plain.]

triplet of characters is found quite different from [these] five triplets [just found] one [of those five] will infallibly be a vowel. Thus the vowels are distinguished from the consonants and then by marking the finals [and by] hypotheses vowels are distinguished from vowels and consonants from consonants both by their rarity as well as by their individual frequency.

### **Extension of the rule when the ciphers are composite**

The same rule can be extended to double ciphers; [189] that is to say, when the numbers or characters represent two letters or syllables or words, for the number of triads of different characters or of dyads themselves (particularly in Italian and Spanish idiom) reveals that there are the same number of different characters to represent the vowels or syllables or entire words.

### **Advice concerning the latest ciphers of Spain and Italy**

In the latest ciphers of Spain which I have seen “67” stands for “en”, “e6y2v45” stands for “dom Cesar”, “t7p22” for “Ferrari”, “con” for “as”, “do” and “m21” for “a”. I do not know if they have changed them since then.

In the latest ciphers of Aldobrandino and of the Borghesi which I have seen the 3 and 4 were nulls and [indicated] word divisions.

In the ciphers of Aldobrandino and of the patriarch of Alexandria, papal nuncio in Spain, the 4 and the five were nulls.

## **TRANSLATION OF RÈGLES DE VIÈTE POUR LE DÉCHIFFREMENT DES ÉCRITURES SECRÈTES BIBLIOTHÈQUE NATIONALE, PARIS, MS. DUPUY 661**

[folio 219 recto]

Monsr. Viète had rules for deciphering all sorts of ciphers which were so sure that they were almost infallible.

When there were simple words in cipher among other writing, or lines [of cipher text] divided into words he succeeded as quickly as Monsr. du Liz himself, whom he used to write at his direction on some occasions [and who] deciphered them almost as easily as did Mr. Viète [by following his rules]. [This was done] by selecting the final letters and those of the beginnings of words, and later penetrating to the middle parts, grouped by their last [letters] such as L, S & T [-lt, -st], C & T [-ct], Q & V [qu-], as well as double letters such as SS, RR, NN,

MM, CC, FF, LL, TT. The rest of the frequency of characters revealed quite soon the vowels, more or less frequent, and afterwards the consonants.

When [the cipher] comprised lines run on without word divisions more work was required. He had made for him a good number of copies of the cipher text as it was written in the original, then he set up a paper as if it were for writing notes of music [i.e., with many lines] and taking one page of cipher text, as many times as he found one character he marked it on one line, then he marked another character on the second line, as many times as he could find it on the said page, after which he would do the same on a third line with another character. And thus [he did] with the other characters until all were done. Then he counted the reiterations of the same character and judged that [219v] the most frequent stood for the vowels. Following the most frequent vowel (“e” in French and “o” in Italian) [he found] also the others; the less frequent stood for the consonants, and the most infrequent those which are not put in use except very rarely. Finally he conjectured the nulls

aaaaaaaaa

bbbb

cccccccc

dddd<sup>58</sup>

and likewise others. In the end he attempted his conjectures on one of the copies of the cipher and marked the vowels, then the consonants, and if he didn’t succeed in reconstructing it, he tried another. But after he deciphered one word, all [the rest] followed immediately. He employed principally the rule of assembling [groups of] similar letters, like SS, or [groups of] different [letters], like “qu”, together with the final letters. And he acquitted himself so successfully that the deceased king often sent to him couriers expressly to bring to him intercepted dispatches in cipher. [These couriers] waited two or three days until he had solved the cipher, and brought the solutions back [to the king].

In the past he deciphered in languages which were unknown to him, mainly in Spanish, where one day he suddenly solved a word and at once acquired the language and deciphered all the rest of the cipher in fifteen days. He has deciphered [ciphers] up to decuples<sup>59</sup> which is something almost [220r] incomprehensible.

To foil these rules any [ciphers] always interlace some null between the double letters, “qu” and others.<sup>60</sup>

<sup>58</sup>[The text shows these letters repeated in just this way; it is not clear how this helps with the problem of finding the null letters, but perhaps what is meant is that one can compare the observed frequency with that expected in normal usage and thus locate the nulls, which will tend to show up with uncharacteristic frequency.]

<sup>59</sup>["These are doubtless ciphers where the same letter is represented by ten different characters" – note by Ritter in his copy, Bibliothèque de l’Institut de France MS 2009, f. 182]

<sup>60</sup>[The sense seems to be that the rules could be thwarted if one put a null letter between double letters of

He printed a little treatise with Mettayer, which one must try to see.<sup>61</sup>

### ACKNOWLEDGMENTS

I would like to thank David Kahn for his encouragement and many helpful suggestions. I also thank Margo Chávez Charles for her help with obtaining materials in Paris, as well as Nancy Buchenauer, H. L. L. Busard, Paul Corley, Jean Fleming, Basia Miller, Milena Boyovic Pesic, B. Matija Peterlin, Martine Voiret, and Ssu Weng, for their generous assistance.

### BIOGRAPHICAL SKETCH

Peter Pesic was educated at Harvard and Stanford, where he received a doctorate in physics. He has been a Tutor at St. John's College in Santa Fe NM since 1980. Also active as a pianist, he has been Musician-in-Residence there since 1984.

---

the plain text, or between other obviously paired letters like "qu"; for example, if one interlaces the null letter "x" in the ciphered version of "tt" or of "qu"; the meaningless letter x turns the telltale pairs "tt" and "qu" into "txt" and "qxu", which makes deciphering far more difficult.]

<sup>61</sup>[See note 8.]