An early French digit cipher: deciphering a letter from the King of France to the Duke of Nevers (1592)

Camille Desenclos
University of Picardie Jules-Verne
camille.desenclos@u-picardie.fr

George Lasry
The DECRYPT Project
george.lasry@gmail.com

Abstract

We deciphered a single letter written in 1592 by Henry IV, King of France, to Louis de Gonzague, Duke of Nevers, held in the Bibliothèque Nationale de France (BnF). The ciphertext mostly consists of contiguous digits, and demonstrates an early use of digit ciphers in 16th-century France. In this letter, Henri IV exposes some parts of his current military strategy against the Catholic League. After deciphering the letter, we were able to locate the original cipher table in another BnF manuscript, illustrating how codebreaking may assist historical research both to reconstruct the content of encrypted letters and to identify anonymous cipher tables.

1 Introduction

Louis de Gonzague, Duke of Nevers played an important role in the French early modern history, particularly because of his political and diplomatic activity during the French Wars of Religion (Boltanski, 2006). Moreover, he was one of the main players in cryptographic practice in the last two decades of the 16th century: dozens of manuscripts (now preserved at the BnF) contain encrypted letters addressed to or written by the Duke of Nevers, and one of them (BnF, fr. 3995) even contains 68 cipher tables which were used by him.

While the letters of the Duke of Nevers are well known to historians (Boltanski, 2006; Le Person, 2002; Le Roux, 2000; Wolfe, 1988), and the majority of these letters has been deciphered as soon as they were received by the recipient (see for instance the interlinear decipherment in the letter from Henri IV to the Duke of Nevers (19 April 1591) at BnF, fr. 3615, fol. 52), one letter written by Henri IV to the Duke of Nevers stands out in this corpus. Not only hasn't been this letter deciphered (or at least its original decipherment hasn't been preserved along with the letter) but, above all, the cipher did not match the one used in the other encrypted letters from the French King to the Duke.

It would certainly have been possible to directly compare this letter with the cipher tables that are preserved in the BnF collections. However, the use of digits makes comparisons more complex, or at least more time-consuming than symbols which are easier to spot in cipher tables. Another approach has therefore been chosen: deciphering the letter with cryptanalytic methods (and thus contributing to the DECRYPT project), and then comparing the reconstructed key with the preserved tables. This approach also has the advantage of questioning the use of cipher keys: for instance, are all the characters well represented in the table? As shown in Pierrot et al. (2023), the decryption of letters and, more broadly, the collaboration between cryptographers and historians not only gives access to the content of a letter, but also provides a better understanding of how a cipher works and was used in practice and contributes to the consolidation of the development and application of modern codebreaking techniques. This paper describes each stage of this collaborative effort. In Section 2, we present the letter, its writer and recipient and their correspondence. In Section 3, we describe how we deciphered the letter, and in Section 4, we compare the reconstructed key with the original cipher table which we later found in the BnF. In Section 5, we present the deciphered letter and the analysis of its contents. We summarize our findings in Section 6.

2 A sensitive correspondence at the end of the French Religion Wars

Since August 1589 and Henri IV's accession to the throne, many noblemen rallied the new King, while the Catholic League, with the support of Spain, kept fighting and denying any acceptance of Henri IV as the legitimate King of France. In September 1592, Henri IV whom many cities including Paris still refused to surrender, was thus campaigning against the Catholic League's armies. In 1591, after reconquering Noyon, among other cities, Henri IV tried from November 1591 to April 1592 to besiege Rouen, without any success, due to the help of Spanish armies led by the Duke of Parma, governor of the Spanish Netherlands. However, the situation started improving for the new King as the royal armies gained some successes both East and South of the Kingdom. The King was then in Noyon and, notably, tried to prevent any Spanish assistance to the League's armies, in Picardy (led by the Duke of Aumale) and in Brittany (led by the Duke of Mercœur).

To contribute to this reconquest of his own Kingdom, Henri IV could rely, among others, on the Duke of Nevers whose catholicity however made him long hesitant between his faith (and rallying the League) and his loyalty to the French Monarchy. Despite some acquaintances with the League in the late 1580's, Nevers didn't join the League, but he didn't rally immediately, at least in an official way, to the new King either (Boltanski, 2006). In May 1590, Nevers finally rallied to Henri IV and acted for him in three different ways: fighting against the Catholic League in his lands (duchy of Nevers) and the lands of his son (government of Champagne), encouraging his clients to rally to the King, and helping the negotiations with some moderate representative of the League.

Many letters from Henry IV to the Duke of Nevers from this specific period have been preserved in the BnF. In particular, the "Manuscrit français 3620" (fr. 3620) especially contains 73 letters from the King to the Duke from May 1590 to February 1593. However, only the letter written on 1592, September 12 (folios 70-71) is encrypted (see Appendix 1). It presents itself as a two-page text (folio 70 recto and verso) and an address (folio 71 verso). According to the handwriting, the letter has been written by one or several clerks (from the Secretary of State for War) and then signed both by the King and by his Secretary of State for War and "Maison du roi", Martin Ruzé de Beaulieu. A later marginal addition at the top of the letter (probably added when receiving the letter or soon after[1]), as well as a mention within the letter, allows us to qualify it as a partial duplicate: the same letter has already been sent to the Duke of Nevers through another way. However, when sending it again, a postscript has been added to it, making our letter both a duplicate and a unique letter. As of today, the initial version of this duplicate hasn't been found. On the contrary, we have been able to locate two copies of the first letter (which doesn't contain the postscript) in BnF, fr. 3615, fol. 89 and in BnF, fr. 4003, fol. 10-11. The first copy is only identified as a "12 September" letter and is, moreover, preserved along letters from 1591. In addition, a copy, not of the whole duplicate, but only of the postscript, has been found in BnF, fr. 4003, fol. 17[2].

The first page of the letter was almost fully encrypted, without any decipherment, whereas the second page was surprisingly in cleartext. If the use of ciphers for the first page makes perfectly sense as detailed above (neither the sickness of the French King nor the military strategy can be broadly known by the Catholic League), ciphers could have been used of protect military information in the second page. Some hypotheses can be formulated to explain the sudden end of ciphertext with a new page. Unlike the information on the first page, the one on the second page could have been already more broadly spread within the French Kingdom. It may also have been written in cleartext to threaten any opponent in case of interception and demonstrate the French King's military preparation. It could finally be a way to preserve information by splitting the writing process: a confident clerk who knows the cipher and copies it by writing the first page; another clerk who writes the second page. The apparent difference between the handwritings (the cleartext within the ciphertext vs the cleartext in page 2) seems to confirm this hypothesis but without excluding the other ones.

Finally, the cipher in use in this letter mostly consists of continuous segments of digits, making cryptanalysis more challenging. There are occasional short segments of cleartext. A few of the digits have a o-looking diacritic on top.

[1] Additional mentions are often written by one of the recipient's clerks on margins or on the back of letters. They identify the sender, the date (the sending and sometimes the receiving date), and the nature of the document (duplicate, copy). Sometimes a short abstract of the letter is written above. Theses mentions are mostly written to help with mail management (reading, classifying).

[2] These copies have been compared to our transcription after decipherment. There is a perfect match.

3 Deciphering the letter

Homophonic ciphers in 16th-century France usually consisted of a set of symbols to represent letters of the alphabet – more than one per letter, as well as a nomenclature with symbols representing common words, persons, places, punctuation signs (Desenclos, 2021). Those ciphers often included nulls, which have no meaning and should be ignored when deciphering an encrypted message. In the 1590s, French diplomatic letters (Monts de Savasse, 2004) and, even more, other letters from Henri IV to the Duke of Nevers[3] are still encrypted in that way. None of these letters, however, used the same cipher as the 1592 letter; it remains thus the only use we have found so far of this cipher table.

Despite the use of digits (Latin and/or Greek characters and/or symbols are the most commonly used at that time in France), we assumed that the 1592 letter from Henri IV to the Duke of Nevers might have been encrypted with a homophonic cipher, with or without a nomenclature. The first challenge was to decompose the contiguous segments of digits into groups of digits, each group representing a letter of the alphabet, a combination of letters, a word, a person, a place, or a null. This process is trivial if it is known, upfront, that all those groups of digits have the same number of digits, e.g., two digits. In such a case, the length of any segment of digits between two segments of cleartext should be even (divisible by two). We determined that this was not the case with this ciphertext.[4]

Next, we assumed that one of the digits (0 to 9) might be a null symbol. After removing the digit presumed to be a null, we would expect the length of the digits segments between the cleartext parts to be even.[5] As this experiment did not yield any result, it became apparent that the groups may have a variable number of digits, maybe some groups having two digits (10, 11, etc.) and some having 3 digits (100, 101, etc.). The task of decomposing segments of continuous digits into groups of digits in such a case is highly challenging, and to date, no method exists to do that automatically.[6]

Lasry et al. (2021) had shown that in several cases of papal ciphers, groups of digits representing nomenclature elements (e.g., words, places, or people) would always start with the same digit and would be longer than the homophones (groups of digits representing letters of the alphabets), e.g., three digits vs. two digits. Accordingly, we then assumed that nomenclature elements in the current cipher were encoded with three digits and always started with the digit 1, while homophones consisted of two digits, and would not start with the digit 1.[7]

This assumption, which later turned out to be only partially correct, was quite useful. Not only could we consistently decompose segments between cleartext parts, but also single lines of digits, or segments between the beginning of a line and a cleartext segment on that line.[8] We then transcribed the resulting groups of digits (742 groups in total), and fed them into an algorithm which recovers the key of a homophonic cipher from ciphertext only (Kopal, 2019), obtaining meaningful fragments of Middle French text. With additional manual processing, we were able to recover the full key, shown in Appendix 2.

Our assumption about groups of three digits which start with 1 representing nomenclature elements (words, places, people) or nulls, while useful, turned out to be mostly wrong. While 121, 124, and 130 indeed are nulls, the other groups with three digits are homophones, e.g., 100, 101, and 102 representing P, or 106, 107, and 08 representing R. The symbols with a "o" on top were found to represent doubled consonants, e.g. LL or SS. Also, we found that the letter E was represented by ten homophones, the letter A by eight homophones, I and V by seven each. Curiously, the writer used only two homophones for O, but we suspected that the original table would have included ten

[3] 110 letters from Henri IV to the Duke of Nevers (1589-1594), including 9 encrypted letters, can also be found in BnF, fr. 3615 and fr. 3626.

[4] Neither was the length of those segments divisible by three, assuming that all groups of digits contain three digits.

[5] Or divisible by three.

[6] For more details on such variable-length homophonic ciphers, see (Lasry et al., 2021).

[7] At this stage, we ignored the digits with a "o" on top.

[8] If the clerk enciphering the letter would not split the digits of a single homophone into two lines. This assumption turned out to be correct.

homophones for each vowel.[9] One group, 51 with a dot on top, was assumed to be a place, which could be interpreted ("Picardye") only after finding the original table.

4 An original digit cipher

Taking advantage of the reconstructed key, we were able to local the original cipher table in the BnF, fr. 3995, fol. 141, shown in Appendix 3 and now referred to as the 1592-cipher. Although this letter could have been deciphered by comparing it with all the cipher tables held at the BnF or by looking for copies of the letter, the current work had two benefits. Firstly, the table on fol. 141 was not identified as a "cipher between the King of France and the Duke of Nevers" but as a "chiffre commun entre messieurs les secrétaires d'Estat et messieurs du conseil. Pour bailler à monsieur de Nevers" [transl.: common cipher between the Secretaries of State and the members of the Council. To be given to the Duke of Nevers]. If this mention doesn't date the cipher, its creation date can be put between May 1590 (death of the previous cardinal de Bourbon who wouldn't have been listed in the nomenclature along with Henri IV's supports) and June 1592 (death of François de Bourbon, Duke of Montpensier). According to Nevers' position (he is one of the members of the Council), this sharing makes perfect sense; sharing a similar cipher between several people certainly weakens the security granted by the encryption but it eases and shortens the writing and encryption process. It questions mostly about the possible use of such a cipher: was it intended to be used for global correspondence (the same letter written and sent to every member of the Council) and/or for specific correspondence (any correspondence with any member of the Council)? This letter would indicate the later use but doesn't explain why the 1592-cipher was used when a specific cipher between the King and the Duke already existed (the 1591-cipher, see above).

In fact, having deciphered a letter encrypted with the 1592-cipher not only demonstrates how the cipher was used in practice but also helps to understand how and why the 1592-cipher has been used for this letter. The reconstructed key is essentially correct, but incomplete, as would have been expected given that it was recovered from a short letter with only 742 groups. As expected, in the original table there are 10 homophones for each vowel (A, E, I/J, O, U/V). There are three homophones per consonant, except for X, Y, and Z which have only two. The original table also lists additional groups for nulls and for doubled consonants.

The 1592-cipher also includes symbols for names of people ("Noms"), cities ("Villes"), and provinces ("Provinces"), but used only once ("Picardye") in the letter, although there are several names and places spelled out in cipher. However, this isn't a misusage of the cipher table but the result of one of the limitations of any cipher table. Cipher tables are indeed conceived at one specific time and had to consider both the time situation (names and places that are the most subject to be frequently used) and usability. This final criterion is even more important in a war context when letters must be encrypted and deciphered quickly and when names of places are as important as names of persons but cannot always be anticipated. It is thus understandable not a have a symbol for Sancy's name (Nicolas de Harlay, sieur de Sancy has been one of the King's representatives towards European protestant princes and helps as well in negotiations within the Kingdom). On the contrary, the absence of any symbol for Charles de Lorraine, Duke of Aumale, governor of Picardy and one of the Catholic League's leaders, is more surprising. As Aumale's name is present in the nomenclature of the 1591-cipher used between the King and the Duke, the use of the 1592-cipher raises some questions.

The nature of our letter as a duplicate could be a reason. To secure the contents as much as possible, using another cipher can level up the difficulty of cryptanalysis and preventing the understanding of the letter as a duplicate of a previous one. As both the King and the Duke already possessed the 1592-cipher, it was easier to use it again without putting at jeopardy a new cipher table by sending it via unsecure roads. In fact, the reason for this change of cipher doesn't seem much to be linked to the military context but to the writing context. All the encrypted letters from the King to the Duke, from 1591 (BnF, fr. 3615, fol. 52) to 1594 (BnF, fr. 3626, fol. 53) have been countersigned by Louis Potier de Gesvres and thus encrypted and written by his clerks. In contrast, the 1592 letter has been

[9] For example, A is represented by 90 to 93 as well as by 96 to 99. We were expecting that A should be represented by the full range of 90 to 99, including the missing 94 and 95.

countersigned by Martin Ruzé de Beaulieu. We may thus assume that Ruzé didn't have access to Potier's cipher table (1591-cipher) and needed then to use the only table he already possessed and could use with the Duke of Nevers, in this case the common table between Secretaries of State and members of the Council.

As for the 1592 letter, we have been able to find back the cipher table (1591-cipher) used for the encrypted letters from the King to the Duke that have been countersigned by Potier and encrypted by his clerks; it can be found in BnF, fr. 3995, fol. 67 and it is shown in Appendix 4. According to a mention on the previous folio, this cipher was used between the King and the Duke of Nevers and had been created in January 1591. Unlike the 1592-cipher but like the vast majority of ciphers that have been created at the same time for King's correspondence (Monts de Savasse, 2004), the 1591-cipher consists mostly of graphical symbols, except for double letters and common words which employ groups of digits. Vowels have five or six homophones (vs. 10 in the digit cipher), and three homophones per consonant. Unlike the 1592-cipher, this one proposes encryption options for common words (here entitled "monosylabes"), for double letters and for the intitulatios. These later encryption options were often used, especially during French Wars of Religion but they were rarely mentioned on cipher tables. In fact, there is the only example in BnF, fr. 3995 (68 cipher tables), and only two provide encryption options for the intitulatios but on the attached guidelines rather than directly on the cipher tables. Finally, the most interesting feature of the 1591-cipher is the use of false plaintext words to represent names and words, such as *les*[10] to represent the city Metz, or *ny*[11] for word *estrangers*[12]. False plaintext words like *tout*[13] or *ce*[14] are also employed as nulls, resulting in a mix between traditional ciphers and jargons. But unlike common jargons, rather than metaphorical words (plants, animals, names from the Bible, etc.), common words are used, that can be easily confused with other parts of the letter, especially if there is only a single word on the middle of ciphertext. However, the global security of the 1591-cipher isn't higher than the 1592-cipher. The size of the nomenclature is quite the same: 59 names for each and only a dozen of common words in supplement in the 1591-cipher. In fact, although the 1591-cipher seems more secure as it relies on more different features, the 1592-cipher provides a higher degree of cryptographic security, as the digits were written continuously without any visual clue as to how to separate them into groups.

Moreover, the 1592-cipher and its use, even if limited, confirm the expansion, in France, of an encryption experiment - digit ciphers - at the turn of the 1590's. Although ciphers still use letters and symbols (Monts de Savasse, 2004), they quickly rationalize themselves by using digits (Desenclos, 2021). In fact, several exclusively digit ciphers have been created and/or used and some of them have been created slightly earlier than we initially thought. At least 23 encrypted letters (using only digits) are sent to the Duke of Nevers in 1589-1591 (BnF, fr. 3422, fr. 3614, fr. 3616, fr. 3623, fr. 3633, fr. 3634, fr. 3646, fr. 3976, fr. 3977) and one of them was written to François de Montholon, keeper of the seals of Henri III.[15] However, in the BnF collections, we have found only two instances of the use of digit ciphers in France in the 1580's/1590's: some of Nevers' correspondence, and another correspondence from Spain.[16] In these years, the Duke of Nevers uses digit ciphers with the French Monarchy (like Montholon or La Vieuville[17] but the latter belongs as well to Nevers' patronage), with Italians such as the Duke of Mantua[18] and Camillo Volta, his agent in Rome[19], or with his wife.[20] Moreover, several cipher tables, using only digits, have been identified in the BnF, fr. 3995, and all belong to the Duke of Nevers. The 1592-cipher is thus, for now, the only documented example of a cipher

[10] Plural of *the*.

[11] Middle French spelling for *ni* (*neither*).

[12] Strangers.

[13] All.

[14] This.

[15] BnF, fr. 3614, fol. 89, 20 April 1589.

[16] BnF, fr. 3977, fol. 130, letter from Bernardino de Mendoza to the duke of Parma, 17 April 1589.

[17] BnF, fr. 3977, fol. 191, letter from La Vieuville to the duke of Nevers, 13 August 1589.

[18] BnF, fr. 3646, fol. 93, 10 November 1589.

[19] The French manuscript 4689 held for example 16 letters from Camillo Volta to the Duke of Nevers from 1585 to 1589. They are written in Italian and use only digits in their encryption.

[20] BnF, fr. 3634, fol. 63. The letter may be earlier than 1589 but we can only estimate its date between 1587 and 1592. Two cipher tables (digits only) for the correspondence between the duke and its wife can be found in BnF, fr. 3995, fol. 2 and 10.

which has certainly been used by the Duke of Nevers but has been created neither by him nor for its sole use as it was intended for the members of the King's Council. Moreover, three letters written by Armand de Gontaut, Duke of Biron, to Henri IV in 28 September and 7 October 1591 (BnF, fr. 3645, fol. 15 and 33) and by de Jean de Chaumont, sieur de Guitry, Jean de Gontaut-Biron, baron de Salagnac and Jean de Vivonne, marquis de Pisani to Henri IV in 9 November 1591 (BnF, fr. 3645, fol. 92) confirm the shared use of this 1592-cipher. Not only is this cipher used beyond the sole entourage of the Duke of Nevers but it is one of the rare examples of a shared use between several people of the same cipher.

However, we don't know yet if the use of digit ciphers had been introduced by the Duke of Nevers, the Monarchy, or by the Catholic League with whom the Duke of Nevers held an encrypted correspondence in the late 1580's.[21] Another cipher table, probably produced in 1589-1590 and using only digits except for 3 symbols (BnF, fr. 3413, fol. 109), weakens this last hypothesis as names of both Protestants and Catholics are mixed in the nomenclator. The presence of the names of Italian princes (Mantua, Parma, etc.), still in the nomenclator, suggests a link with the Duke of Nevers but this table equally fulfills the needs of the French monarchy and rationalizing the cipher by using digits might be a suggestion from François Viète, Henri IV's main cryptographer whose work made him aware of the advantages of digit ciphers. However, without excluding the two other hypotheses, Nevers' letters, as well as a 1562 letter from the Duchess of Mantua to the Duke of Nevers (her son)[22] provides evidence at least of his significant role in the broader diffusion of digit ciphers in France and a strong Italian influence[23]. Nevertheless, relying on the analysis of Nevers' ciphers and his use of digit cipher requires some caution: Nevers's letters and cipher tables form the main part of the letters and cipher tables that we have found and identified yet for the 1580's and 1590's. As the research project is still ongoing, the Duke of Nevers cannot be considered as the sole or main user and creator of these digit ciphers even though he is one of the main actors of the French cryptographic practices.

At this point, we can only affirm that using digit ciphers remains until the mid-1590's, without overshadowing the common use of Latin/Greek letters and symbols, or combining them with digits (e.g., mostly digits but some Latin letters as in BnF, fr. 3625). From this period, we can only find some very intermittent uses of digits until a new experiment in the 1610's and their systematic use in the mid-17th century.

5 The deciphered letter

As often while deciphering early modern letters, the encrypted parts don't hide some state secrets and this letter is no exception. Moreover, this one doesn't differ from the regular letters that the King was sending, especially at war, and that consisted mainly of status reports from the King. As a member of the Council, Nevers needed indeed to be kept informed, so that he could still fight against the League's armies and reinsure some noblemen about the King's intention.

The letter starts thus with some information about the King's health. If this is quite common, it is here particularly significant as a fever has delayed the King's departure towards the North of his Kingdom. The main part of the encrypted text, however, reports about the military strategy of both the King and the Duke of Nevers, according to the information the latter provided to the King and conversely. As extra protection, in addition to the encryption, no specific information (name, location) is given except for the location of the rebel armies. As they are the ones that would like to intercept the letter, it won't harm the King's interests if this information was discovered.

The second part of the letter (in cleartext) keeps going with the status report, now elaborating on the League's military situation and making clear the King's effort to oppose it. In fact, the information in cleartext does not portray the League in an advantageous light (which explains the absence of encryption): their armies in Picardy would be diminished, the King's officer prepared to face them. Moreover, the Spanish army wouldn't be able to help them as Coeverden has been taken back by the Dutch armies as part of the Eighty Years War. The

[21] See for example BnF, fr. 3976.

[22] BnF, fr. 4687, fol. 5, 10 January 1562.

[23] If the recent publications and current research haven't revealed an important use of digit cipher in France, their use in Italy, moreover much earlier, has been demonstrated. See Meister (1906) and Lasry and al. (2021).

letter, whose full transcription is given above, ends with two pieces of information: the King's recovery and the late arrival of the Duke of Bouillon to the King's camp. As the King isn't sick anymore and Bouillon would have arrived before the letter could be intercepted, this isn't confidential and is thus mentioned in clear: none of this could be used by the Catholic League against the King or the Duke.

Transcription[24]

[Mention marginale en haut de la lettre]
Dupplicata horsmis ce qui est adjousté à la fin

Mon cousin,

Je pensois monter à cheval ce matin *pour* aller à Chauny[25] et retourner dès ce soir en ceste ville pour en partir demain et me rendre lundy à Crecy[26] mais *une* grosse fievre m'a pris et me tient il y a quatorze heures sans apparence de diminution ni que les medecins sache[n]t dire quelle elle sera à ce soir ou demain matin *je vous en mandray des nouvelles.*

Cependant je trouve tres bon vostre advés[27] de passer mon armee où vous m'avez escrit pour les raisons que vous me mandez *et* pour oster tout umbrage à celuy duquel vous m'avez envoyé le double *de* la lettre qu'il m'escrit au subjet de laquelle je vous asseure n'avoir jamais pensé *comme* je le luy fais entendre par ma response et mande encores au sieur de Sancy *qui est* de ses amis de le luy dire de ma part. Vous pouvez executer vostre desseing sans peril *car* le duc d'Aumalle s'est retiré avec toutes les forces d[e] Picardye en telle diligence qu'il n'a osé sejourner en aucun lieu que une heure à La Fere; encores a il laissé de ses plumes à la garnison de Chauny.

Le reste de leur armée est fort diminué et s'est logé le long de la riviere d'Esne[28] tirant de Soissons à Retheil. Toutesfois de peur qu'elle n'entrepreigne quelque chose ou qu'elle donne allarme à ceux de mes villes de Challons, d'Esparnay[29] et autres lieux de mon pais de Champagne, nous voyans esloignez, j'escris aux sieurs de Thommasin[30], de Vignolles[31], à ma court de parlement[32] et de madite ville de Challons qu'ilz soyent diligens à se garder de surprise et qu'ilz s'asseurent de mon brief retour comme je le leur ay promis. Les nouvelles du Pais Bas continuent la prise de Couverden[33] et la deffaicte des trois regimens de lansquenetz et de la cavallerie qui estoit envoyée pour le secourir s'il est ainsy le duc de Parme[34] ne peult entreprendre de venir en mon royaume de plus de trois moys ; j'ay adverty mon cousin le cardinal de Bourbon[35], les sieurs de mon conseil et do[36] de se trouver aujourd'huy ou demain à Senlis afin de les y prendre et de les mener avec moy à Meleun[37] où il me tarde que je ne sois desja arrivé.
Priant, sur ce, Nostre Seigneur, qu'il vous ayt, mon cousin en sa sainte et digne garde. Escrit à Noyon le XII^e^ jour de septembre 1592.

[Signé] *Henry*

Mon cousin, depuis la presente escritte et fermée qui est le dupplicata de celle que je vous ay envoyée par une aultre voye et que j'ay gardée jusques à ce jourd'huy pour la vous faire tenir par ceste commodité, ma fievre, graces à Dieu, m'a quicté du tout et espere qu'elle ne me reprendra plus de façon que je partiray demain sans faillir pour me rendre en mon armée suivant ce que je vous ay mandé. Encores fusse je party dès aujourd'huy si mon cousin le duc de Bouillon[38] fust arrivé hier comme je l'attendois pour donner ordre à noz garnison mais s'estant voulu purger il ne sera icy que tantost.

[Signé] *Henry*
[Signé] *Ruzé*

[24] The parts in *italics* are in clear and the text have been edited according to the rules in Barbiche 1980.
[25] Chauny, Aisne, France. It's 20 km away from Noyon where the King is staying.
[26] Crécy-sur-Serre, Aisne, France. It is 50km away from Noyon and mostly close to La Fère (which is mentioned later in the letter).
[27] To be understood as "advis".
[28] To be understood as "Aisne".
[29] Epernay, Marne, France.
[30] Philippe de Thomassin, governor of Châlons.
[31] Bertrand de Vignoles, governor of Épernay.
[32] Since 1589, the magistrates who have stayed faithful to the King (and not to the Catholic League) have settled in Tours for one part and in Châlons for this other part.
[33] Coeverden, Drenthe, Netherlands. It doesn't concern the French Wars of Religion but the Eighty Year's War that opposed Spain to the rebel Norther Provinces of the Netherlands. In early September 1592, Coeverden has been taken back by the rebel armies.
[34] Alexander Farnese, Duke of Parma and governor of the Spanish Netherlands.
[35] Charles II of Bourbon, cardinal de Bourbon since 1590.
[36] It is either a writing mistake or a symbol that hasn't been written in the nomenclature.
[37] Melun, Seine-et-Marne, France.
[38] Henri de La Tour d'Auvergne, Duke of Bouillon.

Translation

[Marginal note above the letter] *Duplicate except for what is added at the end.*

My cousin,

I thought of riding this morning to Chauny and going back from this city already from this evening, and leaving Crecy on Monday, but I have caught a high fever which started 14 hours ago, without any sign of abating, and the physicians not knowing whether it will continue until this evening or tomorrow morning. I will update you on this.

Nevertheless, I found highly appropriate your advice to move my army to the place you wrote to me, for the reasons you mentioned and to avoid any suspicion from the person from which you have sent me a duplicate of a letter, about the topic which I assure you of never thinking of, as I asserted in my response, and having asked Sieur of Sancy, who is one of his friends, to convey to him on my behalf. You will be able to carry your designs without any risk as the Duke of Aumalle has retired with all his forces from Picardy, so diligently that he has not dared to stay in any place rather that one hour in La Fere and he has lost some men while facing the garrison of Chauny.

The remainder of their army is significantly diminished and has taken position along the Aisne rive, from Soissons to Rethel. However, out of concern that it [this army] main underact some action or that it may cause my people in the cities of Chalons, Epernay, and other places in my Champagne country to be alarmed, seeing us afar, I am writing to the sieurs de Thommasin, de Vignolles, to the court of my parlement, and of the said city of Challons that they must be diligently avoid being surprised, and that the should be confident of my return soon, as I have promised to them. The news from the Low Countries follows the capture of Coeverden and the defeat of the three regiments of Lansquenets and of the cavalry sent to save it, so that the Duke of Parma will not be able to enter my realm the next three months. I have instructed my cousin the Cardinal de Bourbon, the members of my council, and 'do' to be today or tomorrow in Senlis to take them and bring them to me to Melun where I soon arrive soon.

With this, praying Our Lord to keep you, my cousin, in his holy and worthy guard. Written at Noyon, the twelfth day of September 1592.

[Signed] *Henry*

My cousin, since writing and sealing the current letter which is a duplicate of the letter I had sent you via another channel and that I had kept until today in order to hand it over to you with this commodity, my fever, thanks God, has gone, and I hope it will not return so that I can without fault leave tomorrow to join my army as I had informed you. Also, I would have departed today if my cousin the Duke of Bouillon had arrived yesterday as I was expecting to assume the command of my garrison, but having wanted to purge himself, this will not happen soon.

[Signed] *Henry*
[Signed] *Ruzé*

6 Conclusion

With a systematic survey of encrypted documents as well as cipher tables in archives and libraries, it is sometimes possible to match an encrypted letter with its original cipher table, even if cipher tables were not systematically preserved by their users nor passed to archives and libraries. If deciphering can be performed without the original cipher table, it helps accurately decipher the document and sometimes better identify its origins.[39] For this letter, it allowed us to understand the reason for this uncommon use of a digit cipher in the correspondence between the King and the Duke as well as the dissemination of digit ciphers in France at the end of 16th century and to document an effective shared use of a same cipher between, at least, 6 persons.

In terms of cryptanalysis, digit ciphers, especially when documents consist of contiguous segments of digits, present more challenges, as opposed to homophonic ciphers employing graphical symbols, which can be compared more easily. In this work, finding the original cipher table was much easier after deciphering the letter using cryptanalytic means.

Finally, the main challenge in cryptanalysis was the fact that the homophones have variable lengths, and a breakthrough was possible only

[39] Especially if the encrypted document does not mention the sender or recipient in cleartext, and those can be identified only after the document is deciphered.

via lucky guesses and trial-and-errors. A generic algorithm to decompose contiguous sequences of digits would be helpful in solving other similar challenging cases.[40]

As for the historical part, while it hasn't led to a breakthrough in the understanding of the French Wars of Religion, it has enabled us to lay the foundations for a better understanding of some cryptographic issues in times of civil war.

Funding

The work of one of the authors has been supported by the Swedish Research Council, grant 2018-06074, DECRYPT – Decryption of Historical Manuscripts.

References

Bernard Barbiche, 1980. *Conseils pour l'édition des documents français de l'époque moderne* [http://theleme.enc.sorbonne.fr/cours/edition_epoque_moderne/edition_des_textes]

Arianne Boltanski, 2006. *Les ducs de Nevers et l'État royal : genèse d'un compromis (ca 1550-ca 1600).* Genève, Droz.

Camille Desenclos, 2021. Écrire le secret quoditien. Pratiques de la cryptographie au sein de la diplomatie française (XVI^{e} siècle – premier XVII^{e} siècle), *in* Guido Braun and Susanne Lachenicht (ed.), *Spies, espionnage and secret diplomacy in the early modern period.* Stuttgart, Kohlhammer, 85-103.

Nils Kopal, 2019. Cryptanalysis of homophonic substitution ciphers using simulated annealing with fixed temperature, *in Proceedings of the 2nd International Conference on Historical Cryptology,* 107-116.

George Lasry, Béata Megyesi and Nils Kopal, 2021. Deciphering papal ciphers from the 16th to the 18th Century, *Cryptologia*, 45:6, 479-540.

Aloys Meister. 1906. *Die Geheimschrift im Dienste der Päpstlichen Kurie von Ihren Anfängen bis zum Ende des XVI. Jahrhunderts,* volume 11. F. Schöningh, Paderborn, 1906.

Xavier Le Person, 2002. *« Practiques » et « practiqueurs » : la vie politique à la fin du règne de Henri III (1584-1589).* Genève, Droz.

Cécile Pierrot, Camille Desenclos, Pierrick Gaudry and Paul Zimmermann, 2023. Deciphering Charles Quint (A diplomatic letter from 1547), *in Proceedings of the 6th International Conference on Historical Cryptology,* 148-1459.

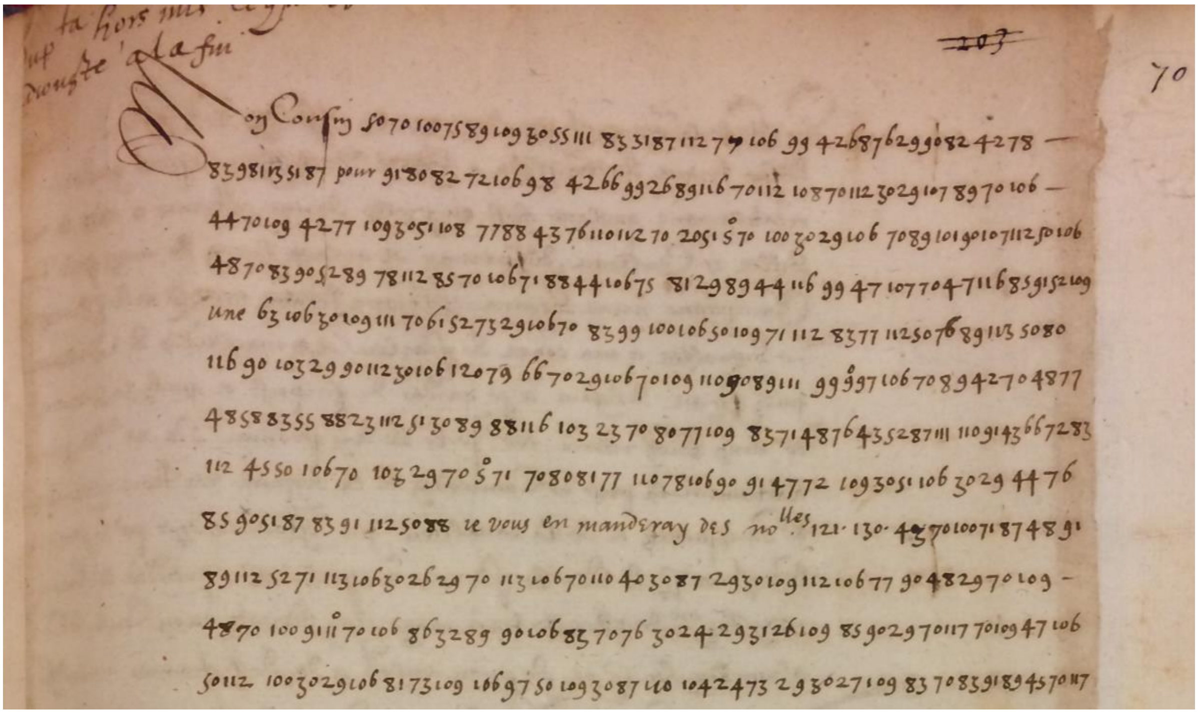
Nicolas Le Roux, 2000. *La faveur du roi : mignons et courtisans au temps des derniers Valois (vers 1547-vers 1589).* Seyssel, Éditions Champ-Vallon.

Jacques de Monts de Savasse (ed.), 2004. *L'Europe d'Henri IV : la correspondance diplomatique du secrétaire d'État Louis de Revol, 1588-1593.* Grenoble, Presses universitaires de Grenoble.

Michael Wolfe, 1988. "Piety and political allegiance: the duc de Nevers and the protestant Henri IV, 1589-93", *French history,* 2:1, 1-21.

[40] For additional examples, see Lasry & al, 2021.

Appendix 1 – Letter from Henri IV to the Duke of Nevers, 12 September 1592 (beginning of the first page)



ta hors mis
Jouste a la fin

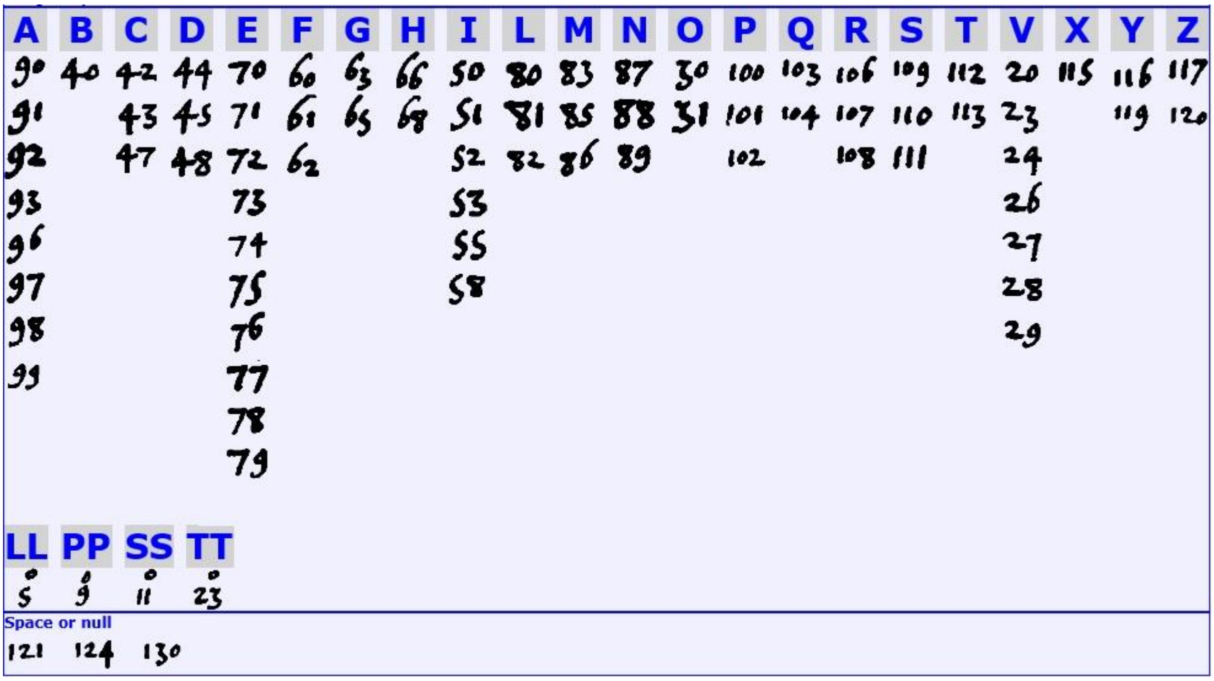
~~203~~

70

Mon Cousin 5070 10075 89 109 3055111 8331871127 9 106 99 4268762990824278 —
8398113 51 87 pour 91 80 82 72106 98 4266 9926 89116 70112 10870112 3029107 89 70 106 —
4470109 4277 10930 51 108 7788 4376110112 70 2051 570 100 3029 106 7089 101 90107112 50106
4870 83 90 52 89 78112 85 70 106 71 88 44106 75 81 29 89 44 116 99 47 107 70 47116 85 91 52109
une 63106 30109111 70 61 52 73 29106 70 83 99 100106 50109 71 112 83 77 112 50 76 89113 5080
116 90 103 29 90112 30106 12079 66 70 29106 70109 110 90 89111 99 97 106 70 89 42 70 4877
48 58 83 55 88 23 112 51 30 89 88116 103 23 70 80 77109 83 71 48 76 43 52 87 111 110 91 43 66 72 83
112 45 50 106 70 103 29 70 $\overset{\circ}{5}$71 70 80 81 77 110 78106 90 91 47 72 109 30 51 106 30 29 44 76
85 90 51 87 83 91 112 50 88 ie vous en manderay des no^lles 121· 130· 43 70 100 71 87 48 91
89 112 52 71 113 106 30 26 29 70 113 106 70 110 40 30 87 29 30 109 112 106 77 90 48 29 70 109 —
48 70 100 91$\overset{\circ}{11}$70 106 86 32 89 90106 85 70 76 30 24 29 31 26109 85 90 29 70117 70109 47 106
50112 100 30 29106 81 73109 106 97 50 109 30 87 110 104 24 73 29 30 27109 83 70 83 91 89 45 70117

Source: BnF, fr. 3620, fol. 70

Appendix 2 – The reconstructed key of the 1592 cipher



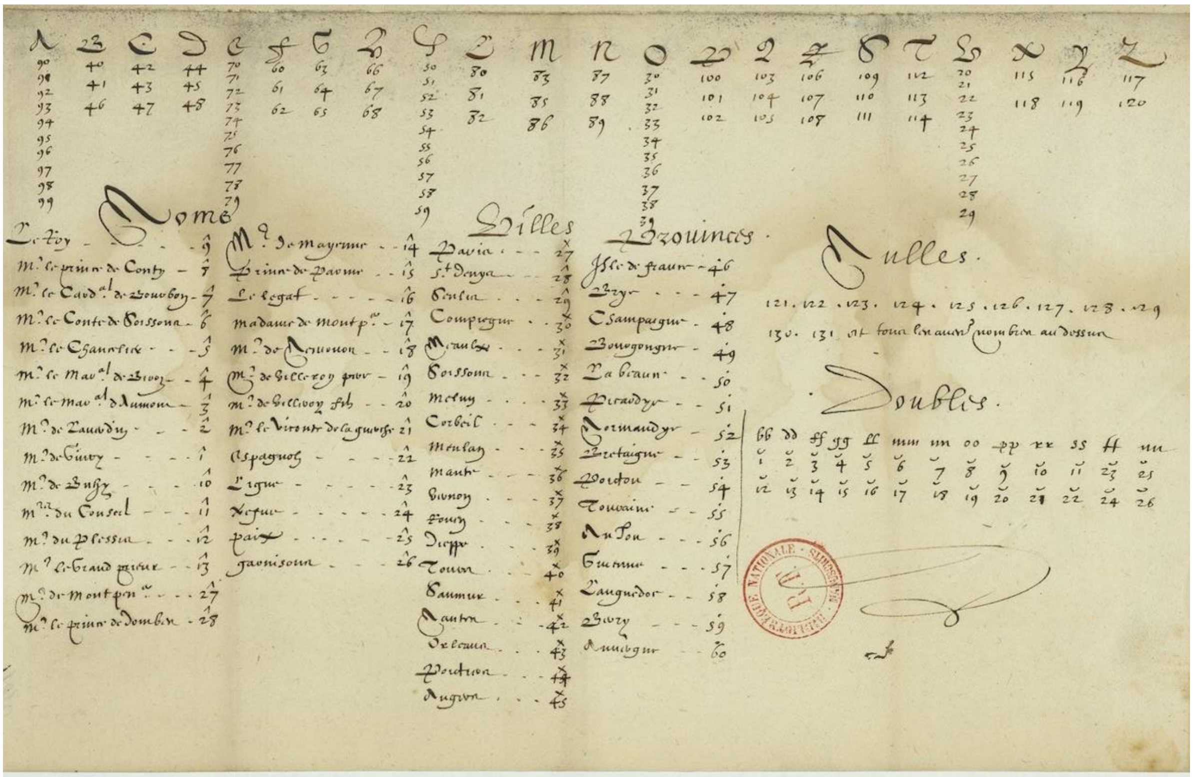
A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	Y	Z
90	40	42	44	70	60	63	66	50	80	83	87	30	100	103	106	109	112	20	115	116	117
91		43	45	71	61	65	68	51	81	85	88	31	101	104	107	110	113	23		119	120
92		47	48	72	62			52	82	86	89		102		108	111		24			
93				73				53										26			
96				74				55										27			
97				75				58										28			
98				76														29			
99				77																	
				78																	
				79																	

LL	PP	SS	TT
$\overset{\circ}{5}$	$\overset{\circ}{9}$	$\overset{\circ}{11}$	$\overset{\circ}{23}$

Space or null		
121	124	130

Source: The authors

Appendix 3 – The 1592 cipher - “Chiffre commun entre messieurs les secrétaires d’Estat et messieurs du conseil. Pour bailler à monsieur de Nevers” (ca. 1590-1592)



A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	Y	Z
90 91 92 93 94 95 96 97 98 99	40 41 46	42 43 47	44 45 48	70 71 72 73 74 75 76 77 78 79	60 61 62	63 64 65	66 67 68	50 51 52 53 54 55 56 57 58 59	80 81 82	83 85 86	87 88 89	30 31 32 33 34 35 36 37 38 39	100 101 102	103 104 105	106 107 108	109 110 111	112 113 114	20 21 22 23 24 25 26 27 28 29	115 118	116 119	117 120

Nome

Le Roy	9	M.r de Mayenne	14
M.r le prince de Conty	8	Prince de Parme	15
M.r le Card.al de Bourbon	7	Le Legat	16
M.r le Conte de Soissons	6	madame de Montp.er	17
M.r le Chancelier	5	M.r de Nemours	18
M.r le Mar.al de Biron	4	M.r de Villeroy pere	19
M.r le mar.al d'Aumont	3	M.r de Villeroy filz	20
M.r de Lavardin	2	M.r le Viconte de la guierche	21
M.r de Givry	1	Espagnolz	22
M.r de Buhy	10	Ligue	23
M.rs du Conseil	11	Secours	24
M.r du Plessis	12	paix	25
M.r le Grand prieur	13	garnison	26
M.e de Montpen.er	27		
M.r le prince de Dombes	28		

Villes

Paris	27
S.t Denys	28
Senlis	29
Compiegne	30
Meaulx	31
Soissons	32
Melun	33
Corbeil	34
Meulan	35
Mante	36
Vernon	37
Rouen	38
Dieppe	39
Tours	40
Saumur	41
Nantes	42
Orleans	43
Poictiers	44
Angers	45

Provinces.

Isle de France	46
Brye	47
Champaigne	48
Bourgongne	49
La Beausse	50
Picardye	51
Normandye	52
Bretaigne	53
Poictou	54
Touraine	55
Anjou	56
Guyenne	57
Languedoc	58
Berry	59
Auvergne	60

Nulles.

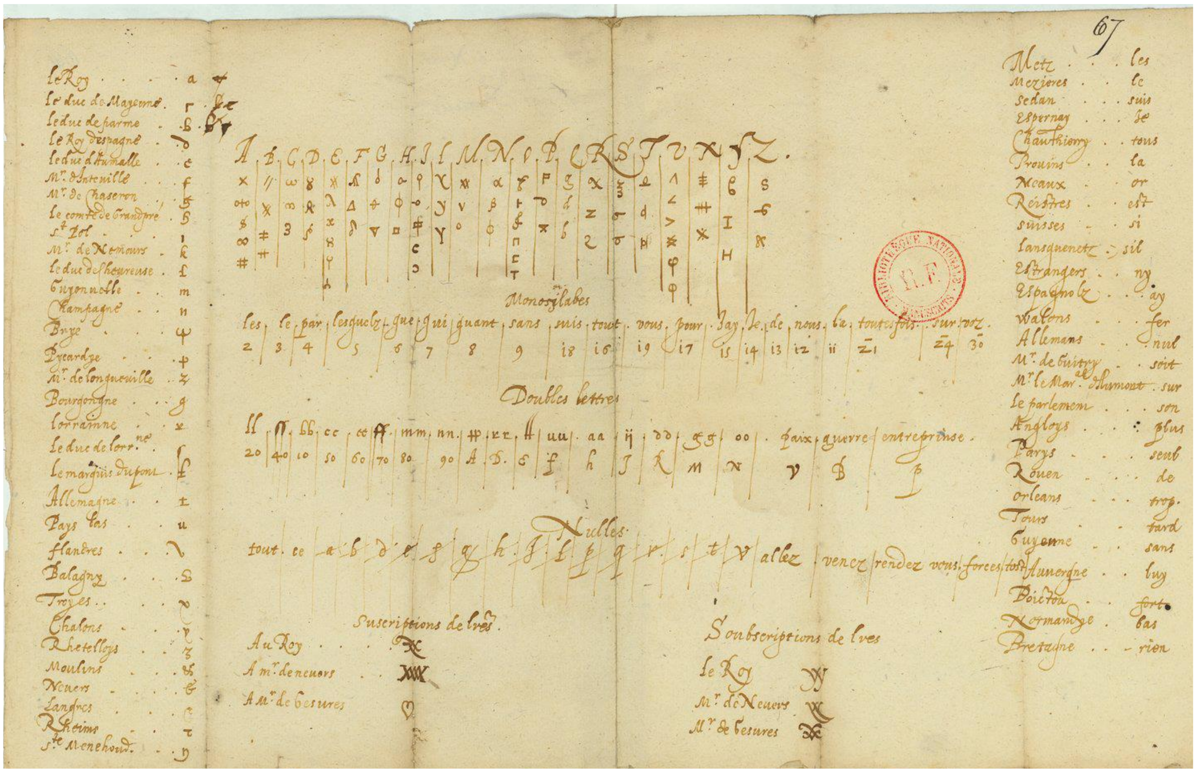
121. 122. 123. 124. 125. 126. 127. 128. 129
130. 131 et tous les autres nombres au dessus

Doubles.

bb	dd	ff	gg	ll	mm	nn	oo	pp	rr	ss	tt	uu
1	2	3	4	5	6	7	8	9	10	11	23	25
12	13	14	15	16	17	18	19	20	21	22	24	26

Source: BnF, fr. 3995, fol. 141 (©Gallica)

Appendix 4 – The 1591 cipher used between Henri IV and the Duke of Nevers, January 1591



67

le Roy	a
le duc de Mayenne	r
le duc de parme	ß
le Roy despagne	∂
le duc d'Aumalle	c
M.r d'Antenille	f
M.r de Chaseron	ſ
le comte de Grandpré	ß
S.t Pol	i
M.r de Nemours	k
le duc de Cheureuse	£
Guyonnelle	m
Champagne	n
Brye	ψ
Pycardye	+
M.r de longueville	z
Bourgongne	g
lorraine	x
le duc de lorr.ne	ſ
le marquis du pont	£
Allemagne	t
Pays bas	u
flandres	∖
Balagny	S
Troyes	∂
Chalons	y
Rhetelloys	z
Moulins	&
Neuers	&
Langres	c
Rheims	τ
S.te Menehoud	y

A B C D E F G H I L M N O P Q R S T V X Y Z.

Monosyllabes

les	le	par	lesquelz	que	qui	quant	sans	suis	tout	vous	pour	J'ay	Je	de	nous	la	toutesfois	sur	voz
2	3	4	5	6	7	8	9	18	16	19	17	15	14	13	12	11	21	24	30

Doubles lettres

ll	ſſ	bb	cc	ee	ff	mm	nn	pp	rr	tt	uu	aa	ii	dd	gg	oo	paix	guerre	entreprinse
20	40	10	50	60	70	80	90	A	D	ε	f	h	J	R	M	N	V	B	P

Nulles

tout. ce. a. b. d. e. g. q. h. i. l. p. q. r. s. t. v. allez. venez. rendez vous. forces. tost.

Suscriptions de l[ett]res

Au Roy
A m.r de neuers
A M.r de Gesures

Soubscriptions de l[ett]res

le Roy
M.r de Neuers
M.r de Gesures

Metz	les
Mezieres	le
Sedan	suis
Espernay	Je
Chauthiery	tous
Prouins	la
Meaux	or
Reistres	est
suisses	si
lansquenetz	sil
Estrangers	ny
Espagnolz	ay
Walons	fer
Allemans	nul
M.r de Guitry	soit
M.r le Mar.al d'Aumont	sur
le parlement	son
Angloys	plus
Parys	seul
Rouen	de
orleans	trop.
Tours	tard
Guyenne	sans
Auuergne	luy
Poictou	fort
Normandye	bas
Bretagne	rien

Source: BnF, fr. 3995, fol. 67 (©Gallica)