Unsealing the Secret: Rebuilding the Renaissance French Cryptographic Sources (1530-1630)

Camille Desenclos

Unsealing the Secret: Rebuilding the Renaissance French Cryptographic Sources (1530-1630)

Camille Desenclos
CRÉSAT (EA-3436)
Université de Haute-Alsace
camille.desenclos@uha.fr

Abstract

Neither political nor diplomatic historians can avoid working with enciphered sources. However, we mostly study their content and not their writing processes. In the wake of a new history of political information, ciphers and, more broadly, cryptographic usages, practices and cultures should be embraced by historians. By considering cryptographic sources as significant witnesses of a culture of political information, we can no longer look at them as information repositories or instances for cryptanalysis but as complex scientific and political objects.

In that respect, Renaissance French ciphers form perfect study objects. They are not yet as complex and technical as in the mid-seventeenth or eighteenth century and show a representative variety of goals (political or diplomatic), systems (jargon, simple substitution, homophonic substitution, …) and usages. As any other early modern source, however, cryptographic sources are dispersed, incomplete and, sometimes, hardly understandable at first sight. By studying many ciphering tables, by observing encryption and decipherment practices within a correspondence, by matching the enciphered letters and the related ciphering table, by comparing cryptographic systems, we hope to rebuild, at least partly, the Renaissance French cryptographic practices.

1 Introduction

Anyone who works on Renaissance political or diplomatic correspondences has faced, at least once, ciphers or enciphered letters. The Kingdom of France, as any other European state, has provided favorable conditions to the rise of a wide, diverse and frequent cryptographic practice. The implementation of permanent diplomatic representations all over Europe – there were twelve French permanent diplomatic agents at the beginning of the 17th century – has entailed the development of new strategies and tools for the protection of information. The more the circulation of diplomatic correspondences increased, the more ciphers became essential. During the 16th century, enciphered letters thus progressed from an extraordinary use to common practice by the French diplomacy. In addition to this increased usage in diplomatic correspondence, the political and religious disorders within the French Kingdom during the second half of the 16th century led high-ranking but rebellious noblemen to make use of ciphers, too, in order to cover up their intentions and plots to their King and his spies.

Although ciphers cannot be distinguished from epistolary writing nor from the political or diplomatic writing usages, they have been neglected by French historians for a long time. The importance of ciphers for the protection of information was recognized, but their functioning as well as their writing processes are still ignored, as ciphers were studied only in an intellectual and not material perspective. By studying them only for their content rather than considering them as significant objects, ciphers could not be entirely understood and were narrowed to their ability to protect information and secrets (Tallon, 2010). Thus studies dedicated at most a few pages, nay a couple of lines, to ciphers and cryptographic usages and practices, mostly in addition to a presentation of the various ways of transmission: postal routes, special couriers … (Martin, 2010). Ciphers were not only exclusively associated with the protection of information but with diplomacy also, at the expense of a wider analysis of the cryptographic practices and usages within the French administration and high nobility, especially during political, social and/or religious disorders. However, French history, with its wars of religion, provides significant examples to be analyzed by historians.

While historians have not yet seized on the subject, historical cryptography and even more historical cryptanalysis (Nachef et al., 2016) arouse more interest. The history of cryptography has been clearly studied more than once. However, those noteworthy but international studies embrace its whole history. Yet the main focus relies on the modern era (Kahn, 1996) and/or on cryptographic theoretical treatises. Although this global perspective allows for the better understanding of each step of the cryptographic evolution, French cryptographic practices during the 16th century until Rossignol's works are, at best, briefly mentioned in these global analyses. These studies do not present the cryptographic patterns in detail and thus cannot meet the needs of historians. If some studies have indeed been devoted to Renaissance practical cryptography (Devos, 1950; Monts-de-Savasse, 1997), they only describe the ciphers and cipher-text characters and/or focus on very specific case studies. They certainly promote a better knowledge of general processes and cryptographic semantics. This remains nevertheless technical and narrowly focused knowledge, far from the expectations and needs of historians. The impact of encrypting letters on the writing and circulation of information does not seem to have been noticeable in diplomatic or political history. Nevertheless, some historians (Ribera, 2007; Hugon, 2004) proceed from diplomatic history to an early modern history of political information. They analyze indeed ciphers in relation to their concrete uses as ways to write and protect political information. By considering both their technical and political dimensions, ciphers can become a new object of study within a new field cutting across boundaries: the history of information. The presence of cipher-text and plain-text in one and a same letter reveals the essential balance between public and private spheres, public decisions and secret actions. Beyond secrecy, elaborating stronger ciphers as well as encrypting a portion of text resulted from the same decision: protecting what could be valuable information. But what caused the French cryptographic practices to evolve? The increasing circulation of information? The structuring of diplomatic and intelligence systems? Was secrecy more needed? Or did the political writing process itself evolve? The aim of this paper will thus be to demonstrate the methodological and historical benefits of matching the history of cryptography with the history of information and to reposition Renaissance cryptography as a significant practice in French political writing.

2 French Cryptographic Treatises

A study of Renaissance French cryptographic uses and practices faces some difficulties in regard to the absence and/or dispersion of sources. Many enciphered letters, even some ciphering tables, have been preserved, but without their related documentation. Ciphering tables[1] did not document the way they were used, and neither did diplomatic instructions describe the way ciphers had to be employed. The basic principles appear to be obvious. In most cases, ciphers rely on homophonic substitutions. But when a plain-text letter could be represented by two or three cipher-text characters, how was the cipher-text character chosen? Their concrete functioning stays unclear as it was probably explained orally before the correspondence or the embassy started. Moreover, we cannot find any recommendation about the nature of information which had to be enciphered, the required proportion of cipher-text within letters, and so on. Cryptographic practice relied certainly on a subjective interpretation by each user, but many aspects were common to Renaissance political and diplomatic society.

Moreover, no secondary sources have apparently been preserved in the French archives or libraries. The diplomatic treatises, which have become the main sources about the process of political writing, never describe the cryptographic uses and practices nor the influence of encryption on diplomatic writing. As a technical process, which belonged to the daily diplomatic routine, encryption was apparently not considered as part of the art of diplomacy. Some general recommendations were expressed in later works only (Callières, 1716). Callière's treatise dedicated almost two pages to cryptography, even if the main concern remained the diverse and general ways to protect information. Neither the purpose of encryption nor the functioning of ciphers were mentioned. Only the strategies to protect information were introduced. François de Callières did not mention the encryption process and its technical implementation. In addition to the technical aspects of cryptographic practices that were not

[1]A few ciphering tables present a quick documentation, mostly about the use of specific cipher-text characters. However, they are more the exception to the rule than actual documentation.

part of the art of diplomacy, this information needed to remain secret. Otherwise it would help other countries to break the French ciphers. That can easily – though only partly – explain the silence of these theoretical works.

Cryptographic treatises could therefore be useful sources both to learn how Renaissance people understood the encryption process and how and why they used it. The first such work, written in French, was nevertheless published only at the very end of the 16th century (Vigenère, 1586). Blaise de Vigenère – like François Viète a few years after him – was in the service of the French King for several years. Their proximity to centers of power suggests an influence or even a participation in the conception of ciphering tables. However, these treatises seem to have remained strictly theoretical, even though some rare implementations could be observed, at least in the 17th century (De Leeuw 2015). They conceived complex cryptographic systems, but they cannot be considered as practical encryption manuals. Vigenère's work did indeed describe theoretical cryptographic mechanisms and tried to conceive of a perfect, unbreakable, and thus almost ideal cipher[2]. Although Vigenère's work was clearly not intended for regular users but only for other scholars or scientists, noblemen and diplomats could not use Vigenère's proposals, anyway, because of their lacks of mathematical skills and their restricted writing time. Yet if these works strictly remained theoretical and had no influence on the cryptographic practice, Vigenère or Viète knew real-life cryptography though not as authors of cryptographic treatises but rather by working directly with the regular creators of ciphers while decrypting enciphered letters for the Duke of Nevers (Vigenère) or for the French King (Viète).

Several technical diplomatic treatises, however, such as *Traicté des chiffres* by Charles Brulart de Léon (circa 1630)[3] intended to provide practical solutions to the issues of daily cryptographic writing, which needed to be fast and simple, after all. Through its many examples[4] Brulart de Léon's treatise describes cryptographic mechanisms, recommended cipher-text characters, and so on. Following Cicco Simonetta's work, this treatise went further. It presents practical encryption processes which should enhance the protection of information such as not leaving any space within the cipher-text; frequently using cipher-text characters without any value (so-called nulls) so that rarely used characters would not lead to their value or nature; disguising the frequency of cipher-text characters, and so on. Brulart de Léon thus proposed concrete rules for encryption. By following these recommendations, the writer could hide the origin of his letter and prevent any interception. Brulart de Léon, as Cicco Simonetta before him, probably dedicated his work to the state office. As a former diplomat, Brulart de Léon[5] claimed to take advantage of his own diplomatic experience and to propose various solutions to the main issues of the daily encryption practice that he himself has been faced. But even if Brulart de Léon's recommendations paid better heed to the concrete diplomatic needs, they remained complex, constraining and hardly compatible with the speed requested by diplomatic writing. Whatever its initial or real goal, Brulart de Léon's work has stayed off the record. Only the original handwritten version has been preserved, and no written or printed copy has apparently been produced. Furthermore, its form looks more like a personal memorandum: there is no introduction and no inscription; the work has been preserved in the same manuscript along with other personal notes and memorandums. If Brulart de Léon's work was used by the state office, it would have been preserved with the state office archives. Anyway, just like any other theoretical cryptographic treatise, Brulart de Léon's manuscript highlights only one aspect of cryptographic practice. It describes the technical aspects (how to choose cipher-text characters

[2] Blaise de Vigenère explained it quite clearly in his dedicace to Antoine Séguier: "Ce traicté donques sera de semblables usages de chiffres, diversifiez en plusieurs manieres; tant pour incidemment parcourir ce qui se presentera à propos de ces beaux et cachez mysteres, adombrez sous l'escorce de l'escriture; que pour à l'imitation de cela en trasser beaucoup de rares et à peu de gens divulguez artifices […] et la plus grand' part provenans de nostre forge et meditation; non encore que nous scachions touchez jusques icy d'aucun" (Vigenère, 1586, page 4).

[3] French National Library, fr. 17538, fol. 48sq.

[4] Brulart de Léon's treatise, however, does not only present standard methods but also rare systems like a ciphering wheel.

[5] Brulart de Léon has been ambassador to the Republic of Venice from 1611 to 1620, then extraordinary ambassador to the city of Avignon (1625) and to Switzerland (1628-1630).

while conceiving ciphering tables, how to write cipher-text while drafting a letter) and tried to improve them in order to increase the protection of information. But it never questions general aspects: what kind of information has to be enciphered? Why? According to which principles? How were the ciphering tables used and how were encryption and decipherment operated?

3 What About Primary Sources?

Unlike their contemporary documentation about the cryptographic uses and practices, a substantial amount of Renaissance French enciphered letters has been preserved. By chance, most of them have survived with their deciphered text (in margins, between the lines or on a separate sheet). However, even if letters, like no other sources, transcribe perfectly the Renaissance cryptographic culture and practices, enciphered letters present to historians a major issue. Not all letters contain a decipherment or, at least, their separate deciphered text has been lost. That can prevent the reading and understanding of the content of such sources.

Upon receipt the state office systematically wrote the decipherment on the letter so that the state secretary could more easily read the whole piece. But if the recipient deciphered the letter himself, there was no need to rewrite the deciphered text on the original letter. The separate sheet on which the recipient processed the decipherment could easily be lost, deleted or even integrated into another set of documents. The original enciphered letter thus becomes unreadable for historians without the ciphering table or cryptanalytic skills. Many letters still have kept their secrets[6].

For several letters, however, their related ciphering tables still exist. Although they should be deleted at the end of each embassy or long-term correspondence, they have often been preserved, sometimes by the state office itself, and are now one of the most reliable sources of cryptographic uses and mechanisms. More than enciphered letters, ciphering tables make the understanding of the cryptographic systems and their contextual or structural adaptations easier. However, the ciphering tables have faced different fates and their identification can be tricky. They are rarely preserved within the same manuscript (or box) along with the related enciphered letters. For example, the cipher of Jean Hotman, the French resident to the Holy Roman Empire between 1609 and 1614, can be found in the French National Library within the manuscript fr. 4030. On the other hand, his enciphered correspondence with the French King is now kept in manuscripts fr. 15924 to fr. 15930. Moreover, the manifold Renaissance denominations for the ciphering tables ("jargon"[7], "cipher"[8], "key"[9]...) and the absence of any name and/or date on the verso or on the top of the ciphering tables seem to prevent historians from identifying the origins and usages of these tables. Even more, the Renaissance designations often mix tables and enciphered letters. Both can be designated as ciphers ("chiffres")[10]. Thus identifying the right typology of the cryptographic sources and matching enciphered letters to their related ciphering tables are real issues for historians.

We have counted the cryptographic sources which were already described and identified at the French National Library. In 2014, the catalog mentioned only 60 ciphering tables, a great deal less than their actual holdings. In fact, only one fifth of the manuscripts are fully described in the catalog. In addition to cursory descriptions of the other manuscripts, some mistakes and omissions (some bibliographic records were written in the 19th century) have distorted these results, which do not represent the diversity of political and diplomatic sources. Most of the diplomatic correspondences, for example, are only described in a few words[11]. As usual, primary

[6] No letter from Henri IV to François Savary de Brèves, French ambassador to the Ottoman Empire, can be read, as the decipherment has not been written directly on the enciphered letters (French National Library, fr. 3541).

[7] French National Library, Cinq-Cent Colbert 474, fol. 1: "Jargon au deschifre" [Deciphering jargon].

[8] French National Library, fr. 4053, fol. 57: "Chiffre de monseigneur le marechal" [Cipher of M. the marshal].

[9] French National Library, fr. 3629, fol. 42: "Clef pour deschiffrer les lettres de Madame de Raiz" [Deciphering key for the letters of Ms. de Raiz].

[10] French National Library, fr. 3634, fol. 5: "Chiffre reçu le dernier octobre à Meun par le duc de Nevers" [Cipher which was received the last day of October in Meun by the duke of Nevers]. This cipher is thus a fully enciphered letter written to the Duke of Nevers.

[11] The manuscript fr. 16113, for example, is labelled "Dépêches originales adressées à la Cour par divers ambassadeurs et agents français en Espagne" [Original letters from several French ambassadors and agents in Spain

cryptographic sources are widely dispersed, poorly described or identified, or even completely missing.

Because of the need to access and analyze cryptographic primary sources materially and intellectually, a long-term research project is currently conducted in collaboration with the French National Library in order to re-establish a direct contact with Renaissance French cryptographic sources. The French National Library counts as the main repository for political and diplomatic sources (until the mid-1620's). According to the Renaissance archival practices, almost all diplomatic correspondences and reports before 1626 have made their way to the French National Library, along with several political correspondences from the second half of the 16th century. Both kinds of sources are now preserved in the collections of "manuscrits français" [French manuscripts] and "nouvelles acquisitions françaises" [French new acquisitions]. The "collection d'érudits" [scholars' collection] presents exceptional documents, too[12]. In fact, a major part of the French cryptographic sources (before the 1630's) is kept at the French National Library and forms a vast and representative corpus of Renaissance cryptographic uses and practices, even if further research in the French National Archives and in the French Diplomatic Archives will be mandatory. By studying the remaining ciphering tables, by observing actual encryption practices, by analyzing additions on the verso or top of ciphering tables, by comparing cryptographic systems, we hope to rebuild, at least partly, the Renaissance French cryptographic practices, uses and cultures. In that perspective, comparisons with other European cryptographic practices through case studies or similar projects such as the one conducted by Benedek Lang (2018) on Hungarian Early Modern cryptographic practices, could lead to a useful, if not essential, distinction between European, "national" and contextual cryptographic patterns.

As a first step in this ongoing project, we are locating, identifying and dating every preserved ciphering table and enciphered letter. Every manuscript whose description suggests cryptographic documents (mention of original correspondences or reports) is systematically checked. So far, 179 ciphering tables and more than 2 100 enciphered letters (including circa 200 non-deciphered letters) have been found and described. At this stage, we presume that 50 non-deciphered letters, and probably more in the future, could be deciphered. Wherever possible, this identification work leads to the correction of some incomplete bibliographic records. In addition we mention the presence of cipher-text and/or decipherment, add dates and names if they can be restored, and so on. Nevertheless, only the bibliographic records which already present a full description will be corrected. The aim of this project is not to completely describe the political and diplomatic collections at the French National Library but to re-connect the cryptographic sources to each other.

Thanks to this identification work, we should be able to cross-check ciphering tables and enciphered letters and link the letters to their related tables. Each enciphered letter whose ciphering table has not yet been found, will be compared to the anonymous ciphering tables. The cross-checking (through cryptographic systems and no more by names) will not be successful for each enciphered letter. More enciphered letters from different writers than ciphering tables have been preserved. Nevertheless, some ciphering tables, if still missing, could be reconstructed thanks to the decipherment in the letters. By comparing the cipher-text and the deciphered text, the cryptographic patterns could be understood and restored to a great extent.

4 First Results

Our first results, though still incomplete, have confirmed the real necessity to embrace cryptographic sources as material objects and to look at them in a broader perspective. They are not only the implementation of cryptographic patterns, which could interest the history of sciences or technology, but a true testimony of a culture of political information. Facing only the technical mechanisms is not enough. Of course, both the history of technology and the history of sciences are essential to the understanding of the technical mechanisms and their evolutions. The cryptographic sources, however, deserve to be subjected to different approaches and methodologies in order to merely surpass political history or the history of technology. More than any other political source,

to the French Court]. However, it contains a ciphering table of André de Cochefilet, baron of Vaucelas, ambassador to Spain from 1609 to 1615.

[12] The manuscript Clairambault 360 for example preserves the ciphering table of Henri IV and Maurice of Hesse.

cryptographic ones do indeed involve political, diplomatic, scientific, social and cultural history.

Identifying cryptographic sources at the French National Library has required prior research. In order to prevent hypotheses based on better known, but modern, practices and uses, we first needed to reassess the Renaissance patterns: which words referred to ciphers and cryptographic practices? Did these denominations possess any specific value? Specific words can already be highlighted: "jargon", "chiffre" [cipher], "clef" [key], "deschiffre" [deciphered text], "table". The word "jargon" especially referred systematically to the same object and practice: a ciphering table using a substitution system, by words and not by characters (for example: the word rose for the French King). Such tables were never called anything else but "jargon". On the contrary, the word "chiffre" had many uses. If the main use, according to our modern practice, concerned ciphering tables, fully enciphered reports or anonymous letters were sometimes designated (on the verso) as "chiffres", too. The origin of this confusion could be related to the use, by diplomats mostly, of the expression "en chiffre" [with cipher]. Moreover, if "deschiffre" is an early modern word for both decipherment and deciphered text, the cipher-text was hardly ever designated by "chiffre" but by "en chiffre" [with cipher/enciphered]. The denominations of cryptographic tools and productions were not yet standardized: marginal mentions rarely described the typology of documents in detail but provided names or dates[13]. These mentions aimed to make the identification of the document easier and quicker for the state office, the diplomats or more generally its recipient. Ciphering tables were often sent as attachment or handed over in person; there was then no need for any additional mentions. At last, the expression "ciphering table" comes from modern usages. Renaissance cryptography was not yet practiced as an applied science. It still relied on a spontaneous approach as shown by the alphabetical and thematic organization within ciphering tables. Everyone had to be able to use such tables, even without any cryptographic or algorithmic knowledge. Thus the distinction between ciphering tables and deciphering tables was probably spontaneous; both were indeed designated as "chiffre" only. In the future, however, we must find out if both ciphering and deciphering tables were conceived and written systematically, as they will be beginning with Rossignol, or if the existence of one or the other relied on specific uses or users.

Beyond the denominations, defining similarities between the cryptographic processes is essential for the upcoming cross-checks. If the French cryptographic systems were mostly based on substitution, they became more complex and rational during the 16th century. At the beginning of the 16th century, ciphers only presented few cipher-text characters (simple substitution and limited nomenclator). In the second half of the 16th century, though, especially from the 1580's, homophonic substitution was introduced (two to five cipher-text characters for one single plain-text letter), nomenclators were extended (around one hundred words on an average) and new cipher-text characters appeared: characters without any value, canceling characters, repeating characters[14]. These improvements, however, did not go as far as the theoretical recommendations of cryptographers were concerned. A large majority of ciphers, even in the 1620's, still relied on homophonic substitution, much simpler for diplomats and noblemen.

The fast technical evolution of French cryptographic practices makes the identification of ciphering tables easier and confers to our study an extra historical perspective. For each ciphering table, its main features are highlighted and analyzed: enciphering pattern (simple substitution, homophonic substitution, jargon, nomenclators), type of cipher-text characters (Latin and/or Greek alphabet and/or numbers and/or symbols). Most of the time, a careful analysis can lead to a precise dating (to within one or two decades at most). In addition to this first analysis, we get a closer look at the cipher-text characters as they give us the best clues for the cross-checking stage. In the same way that encryption patterns have been improved, the form of the cipher-text characters has become more and more rational and easy to generate so that they can be written and read faster. From symbols or highly-modified Latin characters[15],

[13] French National Library, fr. 3462, n.f.: "Chiffre reformé pour Levant duquel a esté envoyé un double à Monsieur de Breves ambassadeur en avril 1604" [Modified cipher for the Levant whose duplicate has been sent to M. de Breves, ambassador in April 1604].

[14] See for example, French National Library, fr. 3668, fol. 72: Cipher of the count of Tillières and the French King, 1625.

[15] See, for example, French National Library, fr. 3329, fol. 2: Cipher of Jacques d'Humières and François de Balzac.

cipher-text characters were increasingly transformed into numbers. Symbolic characters, which are easy to spot, are thus a specific feature of the first half of the 16th century, even if, until the 1580's, some examples, mostly in political ciphers, can still be found. From the 1560's on, however, symbols gradually disappeared and were replaced by numbers or Latin or Greek characters. Therefore the presence of symbols within a cipher is a significant clue about the date or, for ciphers after 1590, a real specific feature. Nomenclators finally help dating the ciphering tables. The names within the nomenclators represented indeed the main noblemen, ministers, clergymen or diplomats from a specific time. For example, the anonymous ciphering table in the manuscript fr. 3329 can be dated from 1574-1577 as the nomenclator includes the marshal of Montluc. Blaise de Montluc had been appointed marshal in 1574 and died in 1577. Such a precise dating is of course not always possible, especially for the oldest ciphers which did not use large nomenclators. A date range can still be defined in those cases. At last, nomenclators, as well as the improvements of the cryptographic patterns and characters, inform on the circumstances of their usage. A high proportion of foreign names reveals a diplomatic use, and if a country, for instance Spain, is more represented, it is highly likely the cipher was used by a French ambassador to Spain.

But whatever its rise, cryptography is not used in every Renaissance correspondence. The operation remained arduous both for writers and readers and was limited to what was considered as crucial or secret information. Thus the presence and amount of cipher-text reveal the significant political value of the text. However, this was not representative of a specific time. Fully enciphered letters were already written in the first half of the 16th century, and an integral encryption never became a standard. In addition to their long and arduous writing, ciphers did not need to be systematical but, on the contrary, had to adapt themselves as much as possible to the evolving contextual needs: diplomatic conflict, war, insecure postal routes, and so on. Information was not by nature secret; only the collecting of information and/or its use within a given context made its veiling inevitable. In the future, these usage hypotheses will require broader statistics, but the persistent general writing patterns seem logical for now. Moreover, the amount of cipher-text within a given letter (few lines, one page or the whole letter) will help to better understand the needs for writing secret information.

Diplomacy was obviously the main, and by the way first, user of ciphers. The oldest enciphered letter which so far we have found in the French National Library, dates from 1526 and comes from a French diplomatic agent in Rome[16]. A vast majority of enciphered letters from the first half of the 16th century and beyond that from the first decades of the 17th century comes from the diplomatic practice. However, if ciphers were an essential tool for diplomacy, they were not used systematically and on a daily basis. Not every diplomatic agent was provided with a ciphering table. Only the high-ranking diplomats possessed one or several such instruments. In fact, ciphering tables replicated the diplomatic hierarchy. On the contrary, the political use of ciphers was not based on hierarchy but only on needs, as it was not linked to professional or temporary tenure. Although ciphers were only used by the French diplomacy during the first half of the 16th century, the French nobility started to also use ciphers during the second half of the 16th century. Noblemen did not yet use ciphers for personal matters (Lang, 2014) but only for political purposes. Far from being anecdotal this use increased from the end of the 1570's and became more diversified in its practices and the origin of its users. That reveals how deeply ciphers were interwoven with the custom of political writing. The agitated political context in France substantially explains this evolution: noblemen were watched by the royal power, French or foreign factions were watching each other …. Thus ciphers became essential to the political correspondence: they protected information, reputation and sometimes physical integrity. Further counts and identifications will insert these examples from the 1580's in a broader perspective. The corpus that is finally expected should provide some more information about the proportion of each use (political or diplomatic). We hope thereby to be able to predict more precisely the motivations for the political use of ciphers and confirm, or invalidate, the current example of the 1580's. The political use of ciphers could be permanent or strictly limited to momentary needs (mostly during disorders).

[16] French National Library, fr. 2984: letters from Nicolas Raincé to Anne de Montmorency. Nicolas Raincé was the secretary of Jean du Bellay, cardinal and French representative in Rome.

Anyway, political ciphers were not as advanced as their diplomatic counterparts. The needs were very different: users were not "professional" agents; they had not been trained and this political use was still rather new. Above all the main need remained speed, before safety. Except in some rare cases like Vigenère who served the Duke of Nevers in the 1580's, cryptographers served the French King, not other noblemen. The reduced complexity of their ciphering tables was completely logical: there were more symbols; nomenclators were shorter, and homophonic substitution was less advanced. The differences between political ciphers, mostly the ones during the Catholic League, and diplomatic ciphers reveal how French diplomacy mastered the cryptographic practice and did its best to meet the agents' daily needs by constantly improving the protection of information and facilitating the encryption and decipherment operations. Renaissance French diplomacy acted like a laboratory in which ciphers and their implementation were constantly tested and improved. Its practices and patterns were then reused in wider circles, few years or decades after their conception by the French diplomacy.

5 Conclusion

Two essential elements have been highlighted during these first years of our research project: the need for a methodology which is adapted to the cryptographic features (in order to proceed successfully to the identification, analysis and cross-checking of our ongoing corpus) as well as the need for studying not only the ciphers but the general context in which they were employed. If this research project is far from completion, some hypotheses can be stated about the general uses and issues of cryptography within the political and diplomatic society of the French Renaissance. Building on these first results and future findings, we aim to study the encryption mechanisms and their improvements until cryptography became an applied science. We will thus be able to observe the intellectual evolution of French cryptography: its increased use in political and diplomatic correspondences; the dichotomy between the practiced cryptography and its theory; the variations between the diplomatic or political cryptographic uses. We hope to highlight the adaptation of ciphers to geographical locations and/or to political and diplomatic context and finally to understand the refinement and complexity of cryptography as practiced in Renaissance France. We aim to bridge a substantial divide between the production and collect of information and the decision-making process: the material process of the writing of political information. From then we could re-build a history of Renaissance French cryptography, not only in the perspective of the history of sciences but also as part of a global history of information.

Acknowledgments

Part of the project has been supported by a Mark Pigott Research Grant (2015). We would like to thank Gerhard F. Straßer and the anonymous reviewers for their valuable comments, suggestions and help with grammatical and lexical issues.

References

François de Callières. 1716. *De la manière de négocier avec les souverains*. La Compagnie, Amsterdam.

Jean-Pierre Devos. 1950. *Les chiffres de Philippe II (1555-1598) et du Despacho universal durant le XVII^e siècle*. Académie royale de Belgique, Bruxelles.

Alain Hugon. 2004. *Au service du Roi Catholique, "honorables ambassadeurs" et "divins espions": représentations diplomatiques et service secret dans les relations hispano-françaises de 1598 à 1635*. Casa de Velasquez, Madrid.

David Kahn. 1996. *The Codebreakers*. Simon and Schuster, New York.

Benedek Lang. 2014. "People's Secrets: Towards a Social History of Early Modern Cryptography". In *The Sixteenth Century Journal*. 45.2: 291-308.

Benedek Lang. 2018. "Real-Life Cryptology: Enciphering Practice in Early Modern Hungary". In Katherine Ellison and Susan Kim (eds), *A Material History of Medieval and Early Modern Ciphers: Cryptography and the History of Literacy*. Routledge, New York/London, pages 223-240.

Karl de Leeuw. 2014. "Books, Science, and the Rise of the Black Chambers in Early Modern Europe". In Anne-Simone Rous and Martin Mulsow (dir.), *Geheime Post: Kryptologie und Steganographie der diplomatischen Korrespondenz europaïscher Höfe während der Frühen Neuzeit*. Duncker & Humblot, Berlin, pages 87-99.

Claire Martin. 2010. *Mémoires de Benjamin Aubéry du Maurier, ambassadeur protestant de Louis XIII (1566-1636)*. Droz, Genève.

Jacques de Monts-de-Savasse, “Les chiffres de la correspondance diplomatique des ambassadeurs d'Henri IV en l'année 1590”. In Pierre Albert (dir.). 1997. *Correspondance jadis et naguère: congrès national des sociétés historiques et scientifiques*. Comité des travaux historiques et scientifiques. Paris, pages 219-228.

Valérie Nachef, Jacques Patarin and Armel Dubois-Nayt. 2016. “Mary of Guise's Enciphered Letters”. In Peter Y. A. Ryan, David Naccache and Jean-Jacques Quisquater (eds.). *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday.* Springer, Berlin, pages 3-24.

Jean-Michel Ribera. 2007. *Diplomatie et espionnage: les ambassadeurs du roi de France auprès de Philippe II du traité du Cateau-Cambrésis (1559) à la mort de Henri III (1589)*. Honoré Champion, Paris.

Alain Tallon. 2010. *L'Europe au XVIe siècle: États et relations internationales*. Presses universitaires de France, Paris.

Blaise de Vigenère. 1586. *Traicté des chiffres ou secretes manieres d'escrire*. Abel L'Angelier, Paris.