Deciphering a Letter from the French Wars of Religion

George Lasry
The CrypTool and DECRYT Projects
george.lasry@cryptool.org

Abstract

A collection held at the Bibliothèque Nationale de France contains the deciphered version of messages related to negotiations of the Catholic League, Henry III's enemy, with Spain and the Catholic Church in Rome. At least one of those messages was deciphered by Viète. Two other letters in the collection contain enciphered passages without the corresponding plaintext. Using computerized techniques, the author deciphered one of them, from Claude de Bauffremont, baron de Sennecey, ambassador of the League in Rome. In this article, the author describes the process of recovering the key, and of deciphering most parts of the letter, which includes a report of Sennecey's activities in Rome. The cipher used to encode this letter turnout out to be a homophonic cipher with a relatively high number of homophones, making its codebreaking somehow challenging.

1 Introduction

The French Religious Wars were a series of conflicts and intermittent wars, in the 16th Century, involving a succession crisis, a violent struggle between Protestants and Catholics, large-scale massacres (Saint-Barthélemy, 1572), the assassination of the head of the Catholic League (le Duc de Guise, 1588) and the assassination of the king of France (Henry III, 1589). Foreign powers such as Spain were also involved in the conflict, supporting the Catholic League (Holt, 2005).

The Colbert 500/33 collection in the Bibliothèque Nationale de France (BnF) includes several letters related to negotiations between the Catholic League, and Spain and the Holy See, from 1588 to 1594. The decipherment of one of the letters is attributed to François Viète. François Viète (1540-1603) was a renowned French mathematician, also famous for his codebreaking achievements in the service of Henry III and Henry IV, France's kings. For more details on Viète's codebreaking work, see (Pesic, 1997; Kahn, 1996; Tomokiyo, 2020; Godard, 2002). The BnF catalog also mentions that the letters were collected by Jacques-Auguste De Thou (1553-1617), Viète's friend.[1]

One of the letters (BnF Colbert 500/33 f555) is from Claude de Bauffremont, baron de Sennecey (1546-1596), the ambassador of the Catholic League in Rome. It consists of unencrypted cleartext, with several ciphertext passages. Those ciphertext passages were left unsolved, unlike for almost all of the other letters in the collection. It is unclear whether this letter was historically deciphered via cryptanalysis, maybe by Viète himself, or that it could not be solved.

2 Computerized Decipherment

As shown in Figure 1, the ciphertext segments consist of graphic symbols. First, the encrypted segments were transcribed by the author. There are a total of 858 symbols, with 86 unique distinct symbols.

The relatively high number of distinct symbols clearly ruled out the possibility that a simple substitution cipher was employed. Based on the analysis of contemporary enciphering methods (e.g., papal ciphers (Lasry et al., 2020), it was deemed to be likely the result of encipherment using a homophonic cipher, with multiple homophones per letter of the alphabet. As part of the DECRYPT project, various tools have been developed for the recovery of the homophonic cipher keys, from ciphertexts (Megyesi et al., 2020).

The primary codebreaking tool requires a refer-

[1] Jacques Auguste de Thou (1553-1617) was a French historian, book collector and president of the Parliament of Paris. In *Historiarum sui temporis*, his major history work covering the years 1549–1584, he provides biographical details about Viète (University of St Andrews, Scotland, 2022).

ence corpus, composed of texts in the target language. For that purpose, we employed a corpus of French books from the Gutenberg project. The tool uses this corpus to compute the frequencies $R_{i,j,k}$ of all possible trigrams of consecutive letters i, j, and k (e.g., UNE, ENT, etc...), and uses them to search for an optimal key solution, using a simulated annealing algorithm and a fitness score $Score(K)$ that is computed for a candidate key K, as follows:

- Decode the ciphertext using the candidate key K.
- Compute the frequencies of all the trigrams of letters - $F_{i,j,k}$ in the resulting decrypted text.
- Compute $S(K)$, the fitness score for K, as follows: $S(K) = \Sigma_{i,j,k}(F_{i,j,k} \cdot \log(R_{i,j,k}))$

During the simulated-annealing search, the tool performs transformations (or changes) in keys, looking to improve the fitness score. The following transformations are tested at each iteration:

- Swap the assignments of any two homophones. For example, if $x \rightarrow T$ and $y \rightarrow E$ (ciphertext symbol x represents T, and ciphertext symbol y represents E) before the transformation), then after the transformation: $x \rightarrow E$ and $y \rightarrow T$.[2]
- Change the assignment of a single homophone, e.g., instead of $a \rightarrow N$ (before the transformation), we will have $a \rightarrow R$ after the transformation.[3]

Given a long enough ciphertext, this algorithm is likely to correctly recover most of the key mappings between the homophones and the alphabet letters. More details on the technique may be found in (Lasry et al., 2020). For more details on simulated annealing algorithms for codebreaking, see (Lasry, 2018).

However, applying this tool on the given ciphertext did not yield any success. It was hypothesized that because the ciphertext was relatively short, and the number distinct symbols being relatively high (compared to contemporary homophonic ciphers), a more powerful method was required.

The original codebreaking algorithm was adapted to use 5-grams (five consecutive letters, such as "ETLES", or "ITION"), instead of trigrams, for scoring. This attempt online produced some partial results, that confirmed the hypothesis of a homophonic cipher, but this was not enough to read the encoded parts.

Next, the algorithm was adapted to use French texts from a corpus of historical French books, from the Gutenberg Project, instead of a generic French corpus. With this last improvement, and some manual processing, the majority of the enciphered text could be finally deciphered so that it was mostly readable. The recovered (tentative) key is shown in Figure 2.

It can be seen that for each letter of the French alphabet there are two to six homophones. Some of the symbols likely represent prepositions, and the meaning of several symbols could not be successfully identified. There are several encryption errors, e.g., the symbol representing "T" being wrongly used in some places to represent the letter "F". Contemporary homophonic ciphers at the time often had only one homophone for most letters, and usually at most two or three for a few high-frequency letters. In this cipher the vast majority of the letters have three or more homophones assigned to them, improving the security of the cipher.

A tentative decryption of the deciphered passages, as well as a transcription of the cleartext parts, are given in Figure 3. Work is in progress to improve the decryption and to analyze the deciphered text, which describes the ambassador's discussions and meetings in Rome. Unfortunately, the date is unclear, but the collections states that all the letters were from between 1588 and 1594.

3 Conclusion

A well-designed homophonic cipher can be challenging for cryptanalysis, as exemplified in this letter, that required the improvement of modern computerized algorithms, that could solve other contemporary homophonic ciphers, without those improvements. This cipher might also have been challenging for contemporary codebreakers.

Additional work by historians is required to evaluate the contents of this letter, in the context of the involvement of foreign powers in the French Wars

[2] Note that this operation does not change the number of homophones mapped to E or T.

[3] Note that this transformation increases the number of homophones assigned to R, and decreases the number of homophones assigned to N. To ensure that the key is well balanced in terms of distribution of homophone assignments, a certain maximum number of homophones per regular element is specified when running the algorithm.

of Religion.

Funding

This work has been supported by the Swedish Research Council, Grant 2018-06074, DECRYPT – Decryption of historical manuscripts.

Acknowledgments

The author would like to thank Satoshi Tomokiyo for introducing this cipher, and for his valuable comments to an early draft of this paper. The author would also like to thank Camille Desenclos, Satoshi Tomokiyo, and Norbert Biermann for their assistance in improving the decryption and transcribing the cleartext parts.

References

Gaston Godard. 2002. François Viète (1540-1603), père de l'algèbre moderne. *Recherches vendéennes*, (9):297–346.

Mack P Holt. 2005. *The French wars of religion, 1562–1629*, volume 36. Cambridge University Press.

David Kahn. 1996. *The Codebreakers: The comprehensive history of secret communication from ancient times to the internet.* Simon and Schuster.

George Lasry, Beáta Megyesi, and Nils Kopal. 2020. Deciphering papal ciphers from the 16th to the 18th Century. *Cryptologia*, pages 1–62.

George Lasry. 2018. *A Methodology for the Cryptanalysis of Classical Ciphers with Search Metaheuristics, Ph.D. thesis, University of Kassel, Germany*. Kassel University Press. `http://www.upress.uni-kassel.de/katalog/abstract.php?978-3-7376-0458-1`.

Beáta Megyesi, Bernhard Esslinger, Alicia Fornés, Nils Kopal, Benedek Láng, George Lasry, Karl de Leeuw, Eva Pettersson, Arno Wacker, and Michelle Waldispühl. 2020. Decryption of historical manuscripts: the DECRYPT project. *Cryptologia*, 44(6):545–559.

Peter Pesic. 1997. Francois Viete, Father of Modern Cryptanalysis-Two New Manuscripts. *Cryptologia*, 21(1):1–29.

Satoshi Tomokiyo. 2020. Ciphers Broken by François Viète. `http://cryptiana.web.fc2.com/code/viete.htm`, [Accessed: January, 14, 2022].

University of St Andrews, Scotland. 2022. De Thou on François Viète. `https://mathshistory.st-andrews.ac.uk/Extras/Viete_De_Thou/`, [Accessed: January, 14, 2022].

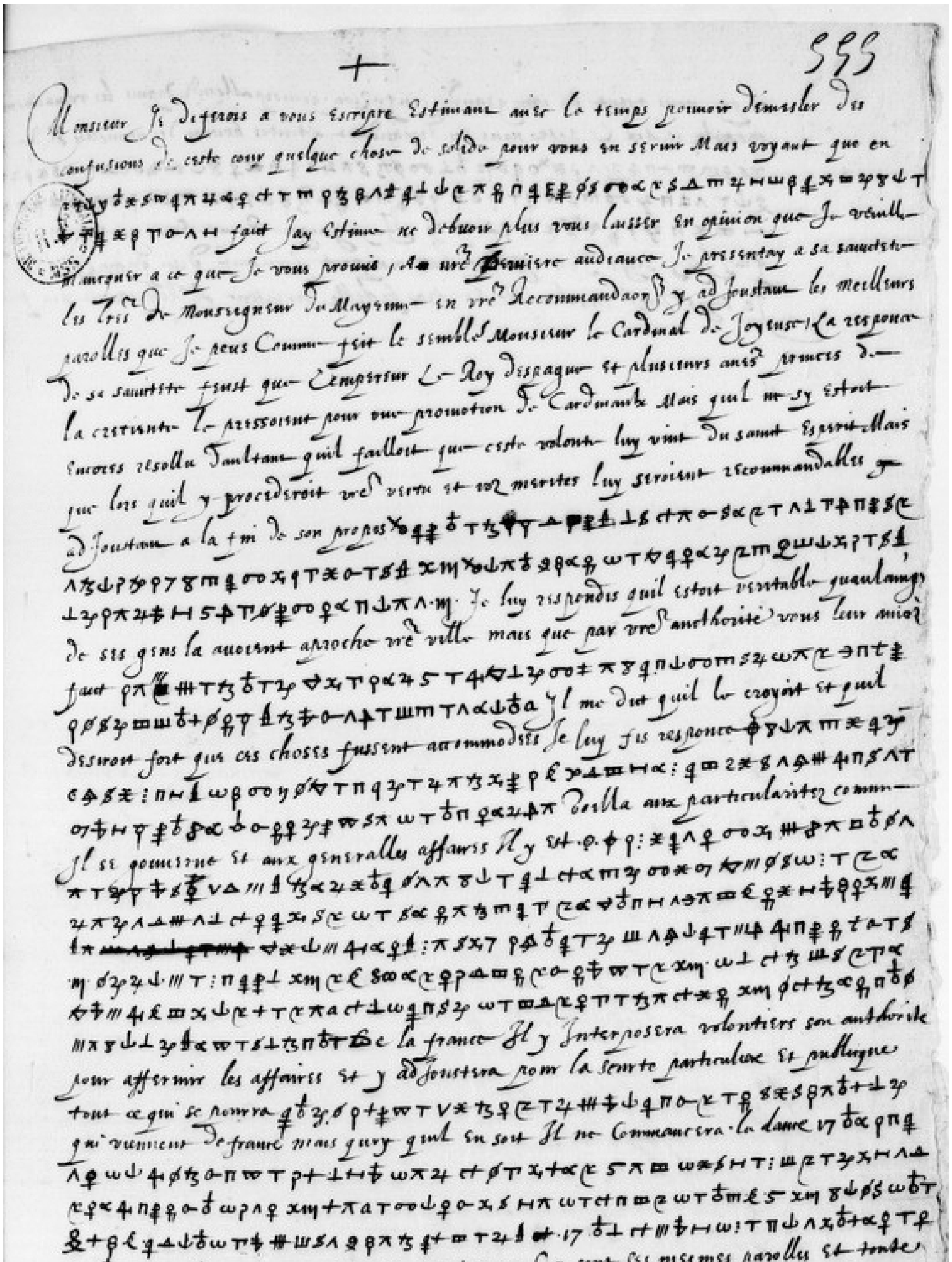


Figure 1: Letter from the Baron of Sennecey - Source: BnF Colbert 500/30 f555.

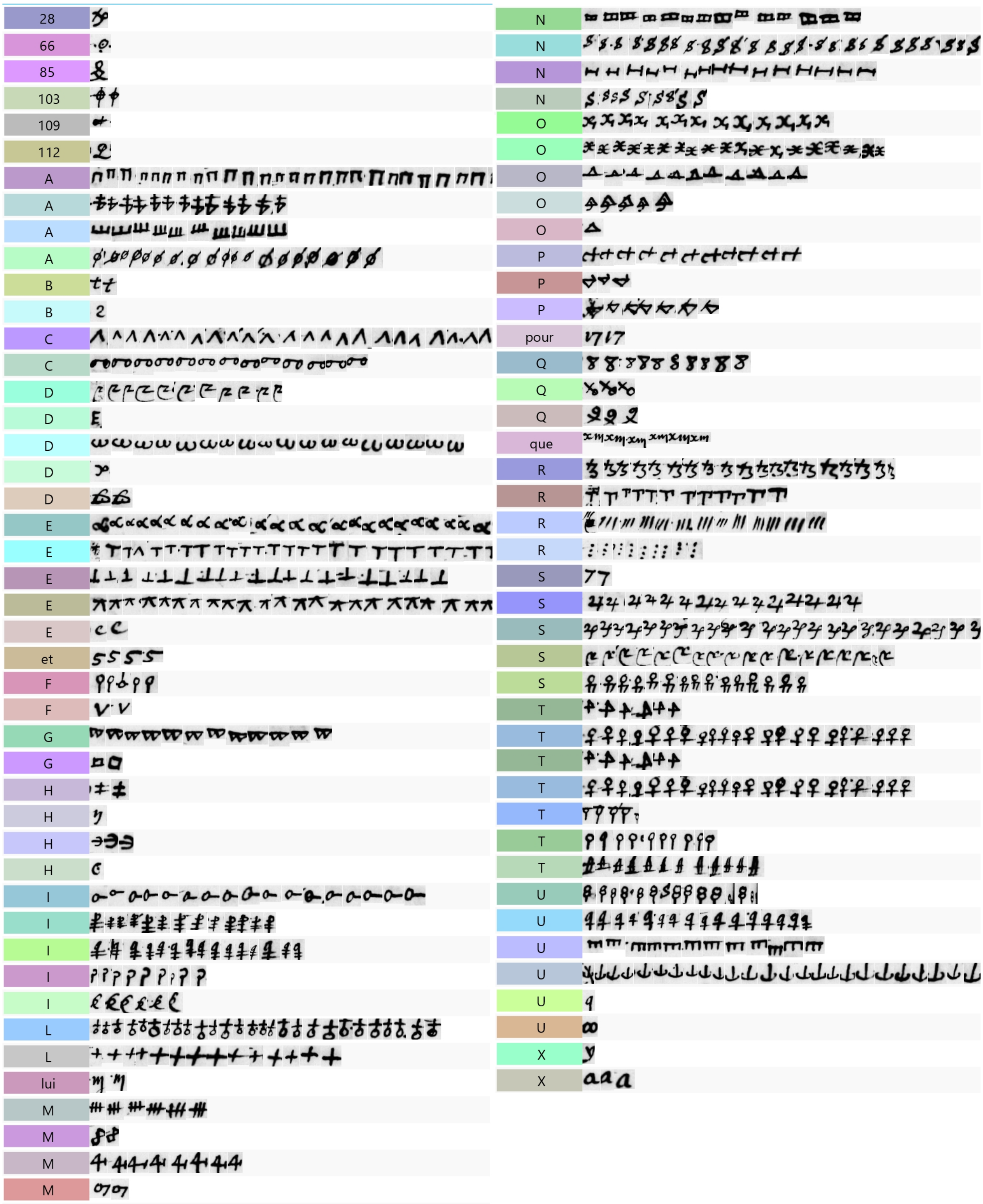
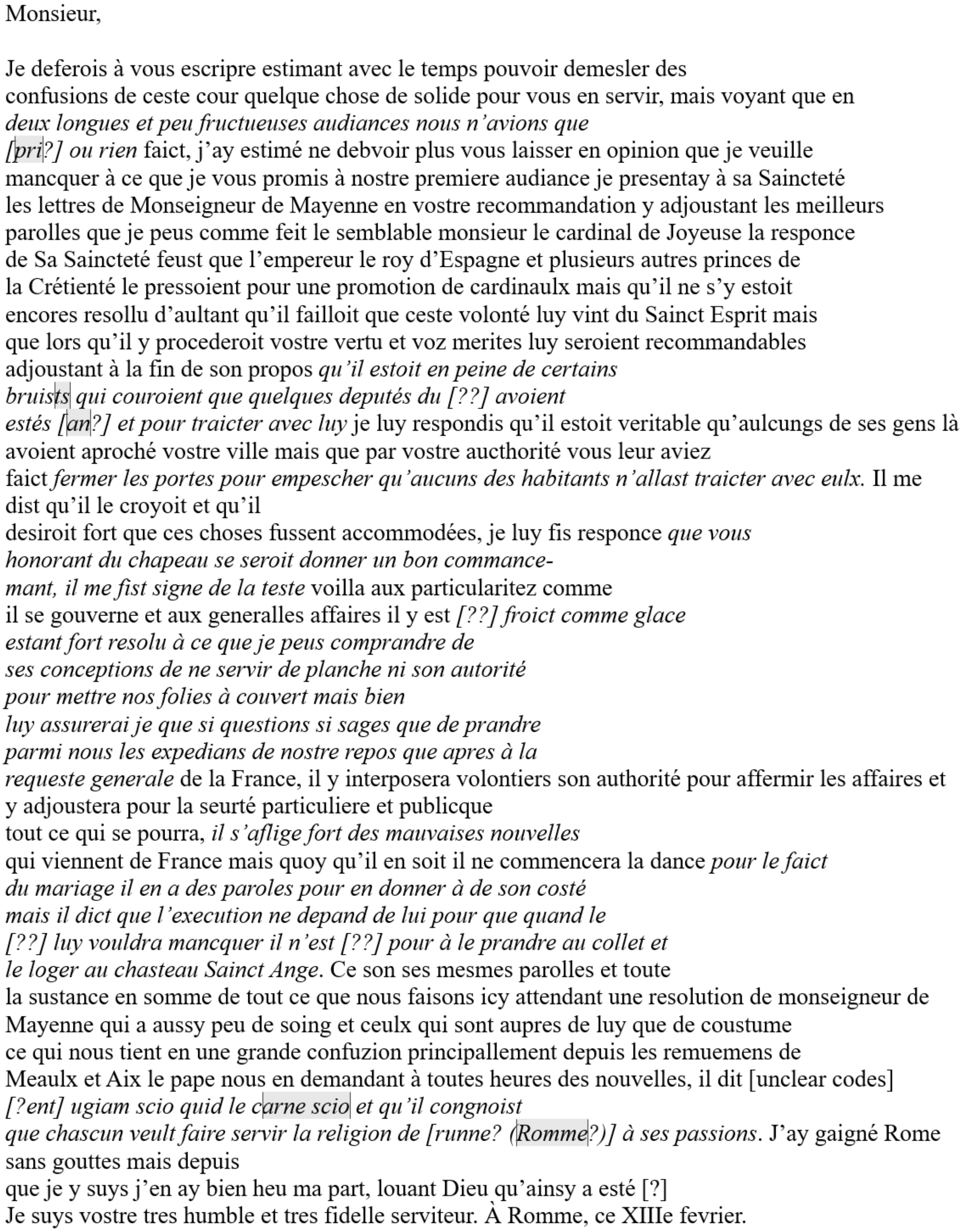

28
66
85
103
109
112
A
A
A
A
B
B
C
C
D
D
D
D
D
E
E
E
E
E
et
F
F
G
G
H
H
H
H
I
I
I
I
I
L
L
lui
M
M
M
M
N
N
N
N
O
O
O
O
O
P
P
P
pour
Q
Q
Q
que
R
R
R
R
S
S
S
S
S
T
T
T
T
T
T
T
U
U
U
U
U
U
X
X

Figure 2: Tentative Key.



Monsieur,

Je deferois à vous escripre estimant avec le temps pouvoir demesler des
confusions de ceste cour quelque chose de solide pour vous en servir, mais voyant que en
deux longues et peu fructueuses audiances nous n'avions que
[pri?] ou rien faict, j'ay estimé ne debvoir plus vous laisser en opinion que je veuille
mancquer à ce que je vous promis à nostre premiere audiance je presentay à sa Sainctеté
les lettres de Monseigneur de Mayenne en vostre recommandation y adjoustant les meilleurs
parolles que je peus comme feit le semblable monsieur le cardinal de Joyeuse la responce
de Sa Sainctеté feust que l'empereur le roy d'Espagne et plusieurs autres princes de
la Crétienté le pressoient pour une promotion de cardinaulx mais qu'il ne s'y estoit
encores resollu d'aultant qu'il failloit que ceste volonté luy vint du Sainct Esprit mais
que lors qu'il y procederoit vostre vertu et voz merites luy seroient recommandables
adjoustant à la fin de son propos *qu'il estoit en peine de certains*
bruists qui couroient que quelques deputés du [??] avoient
estés [an?] et pour traicter avec luy je luy respondis qu'il estoit veritable qu'aulcungs de ses gens là
avoient aproché vostre ville mais que par vostre aucthorité vous leur aviez
faict *fermer les portes pour empescher qu'aucuns des habitants n'allast traicter avec eulx.* Il me
dist qu'il le croyoit et qu'il
desiroit fort que ces choses fussent accommodées, je luy fis responce *que vous*
honorant du chapeau se seroit donner un bon commance-
mant, il me fist signe de la teste voilla aux particularitez comme
il se gouverne et aux generalles affaires il y est *[??] froict comme glace*
estant fort resolu à ce que je peus comprandre de
ses conceptions de ne servir de planche ni son autorité
pour mettre nos folies à couvert mais bien
luy assurerai je que si questions si sages que de prandre
parmi nous les expedians de nostre repos que apres à la
requeste generale de la France, il y interposera volontiers son authorité pour affermir les affaires et
y adjoustera pour la seurté particuliere et publicque
tout ce qui se pourra, *il s'aflige fort des mauvaises nouvelles*
qui viennent de France mais quoy qu'il en soit il ne commencera la dance *pour le faict*
du mariage il en a des paroles pour en donner à de son costé
mais il dict que l'execution ne depand de lui pour que quand le
[??] luy vouldra mancquer il n'est [??] pour à le prandre au collet et
le loger au chasteau Sainct Ange. Ce son ses mesmes parolles et toute
la sustance en somme de tout ce que nous faisons icy attendant une resolution de monseigneur de
Mayenne qui a aussy peu de soing et ceulx qui sont aupres de luy que de coustume
ce qui nous tient en une grande confuzion principallement depuis les remuemens de
Meaulx et Aix le pape nous en demandant à toutes heures des nouvelles, il dit [unclear codes]
[?ent] ugiam scio quid le carne scio et qu'il congnoist
que chascun veult faire servir la religion de [runne? (Romme?)] à ses passions. J'ay gaigné Rome
sans gouttes mais depuis
que je y suys j'en ay bien heu ma part, louant Dieu qu'ainsy a esté [?]
Je suys vostre tres humble et tres fidelle serviteur. À Romme, ce XIIIe fevrier.

Figure 3: Tentative Decryption.