Decipherment of an Encrypted Letter from 1724 Found in UCL Special Collections' Brougham Archive

Nils Kopal
University of Siegen
Siegen, Germany
nils.kopal@uni-siegen.de

Katy Makin
UCL Special Collections
London, United Kingdom
k.makin@ucl.ac.uk

Abstract

This paper shows the decipherment of a 1724 encrypted letter, discovered recently in the Brougham Archive at University College London (UCL) Special Collections. The letter's content hints at political intrigue and possibly relates to the Jacobite movement during George I's reign in Great Britain. However, as all individuals mentioned in the letter are referred to by code names, except for Madame de Prie, their true identities remain unknown to the authors. Therefore, any connection to the Jacobites remains speculative. The paper covers the cipher's security, historical context, and unresolved inquiries surrounding the letter.

1 Introduction

Members of the DECRYPT research project (Megyesi et al., 2020) assist other researchers and historians when faced with encrypted texts discovered in archives and libraries. Often, these individuals find themselves unable to decipher the found scripts on their own (Megyesi et al., 2024). This is where the expertise of the DECRYPT project comes into play. An example of successful collaboration between DECRYPT experts and a historian is the decryption of the Ramanacoil cipher, a ciphertext from the Dutch East India Company from 1674 (Dinnissen and Kopal, 2021). Other examples for fruitful collaborations are the decipherment of the Codex Copiale (Knight et al., 2011), an encrypted manuscript from the 18th century, the decipherment of letters of Holy Roman Emperor Maximilian II written in 1575 (Kopal and Waldispühl, 2022), as well as the recent breakthrough in deciphering newly found Mary Stuart ciphers (Lasry et al., 2023).

Members of the DECRYPT project are actively engaged in the search for such encrypted manuscripts within archives and libraries. Occasionally, encrypted manuscripts also find their way to DECRYPT researchers through other ways. In 2023, the first author of this paper came across a call for assistance from UCL Library on X (formerly Twitter). The call sought help in deciphering a letter discovered in one of their archives, the Brougham Archive. The first author undertook the task of deciphering the pages of the letter presented on X but realized that these pages were not the complete document. Subsequently, the author contacted the archivist, who is also the co-author of this article, and obtained scans of all available pages, along with valuable background information. This paper discusses the decipherment and content of this letter.

2 UCL Special Collections and Brougham Archive

The letter was found in a box of family documents in the archive of Henry Brougham, 1st Baron Brougham and Vaux (1778-1868), one of the founders of UCL. The collection is a true 'family archive', containing both Henry Brougham's working papers and extensive correspondence, and also letters, deeds and estate papers belonging to his siblings and ancestors. At around 160 linear meters, it is the largest and one of the most important archives at UCL Special Collections. It is currently in the process of being cataloged, which is how the letter came to light. As the encrypted letter predates Henry Brougham by over 50 years, it seems likely that it belonged to an ancestor. The other items in the box where it was found provide no clues to its origins, being a miscellaneous assortment of 19th century notes, deeds and bills. However, in the 18th century the Brougham family had connections to the Dukes of Norfolk, prominent Catholics and Jacobite supporters who were involved in the uprising of 1715.

3 The letter

The encrypted letter is written on paper that has aged to a yellow hue over time, with noticeable ink bleed-through visible on the pages. Figure 1 shows the first page of the letter. The letter comprises a total of 16 pages of ciphertext, written in numbers separated by dots and dashes. In some places between these numbers, there are a few simple words written in cleartext. Examples are ”and”, ”the”, and ”whatever”. Also, there are names like ”Mons Garnet and Gee” and ”Mons Grandy and Gay”. The letter’s last five pages are damaged, so we were not able to transcribe and decipher everything with 100% accuracy, but were able to deduce the missing text parts with high confidence. Further analysis indicates that the letter is incomplete, suggesting the existence of additional pages that, regrettably, were not found in the UCL Brougham archive. At the top of the first page, the letter is dated February 24, 1724. Additionally, the first letter includes a unique form of signature we are unable to identify its meaning. The pages are sequentially numbered, ranging from 2 on the second page to 14 on the fourteenth page. These numbers are located either on the top left or right side of each page. Pages 15 and 16 likely had page numbers, but due to the damage to the papers, these no longer exist.

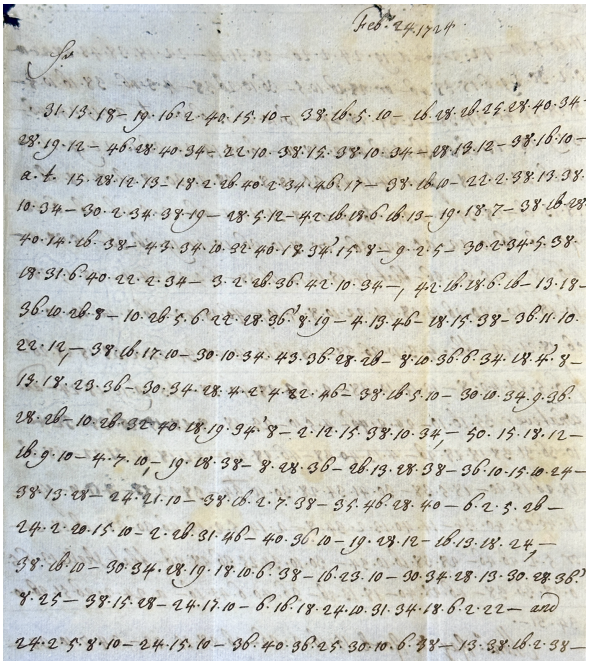

Figure 1: First page of the encrypted letter. UCL Special Collections, Brougham Archive [uncatalogued] (Cipher ID-6317, 1724)

4 Transcription

For the transcription of the letter, a manual process was conducted. All the numbers were meticulously entered along with the dots and dashes between them into a text editor. Cleartext elements were also accurately transcribed. At points where the ciphertext was damaged, question marks were inserted. Throughout the transcription process, care was taken to maintain the original line and page layout.

5 Cryptanalysis

For the cryptanalysis of the letter, we employed our open-source tool, CrypTool 2 (Kopal, 2018) and its Homophonic Substitution Analyzer component, which uses heuristics (hill climbing; simulated annealing) for automated cryptanalysis (Kopal, 2019). Given the large number of different numbers present in the ciphertext (totaling 52), we hypothesized that the cipher used is a homophonic substitution cipher. We also worked under the assumption that the plaintext was in English, as the letter originated from University College London and the readable cleartext parts of the letter are written in English. Consequently, we set our analysis components to English for the cryptanalysis.

Initially, the automatic analysis with the Homophonic Substitution Analyzer yielded no results (Figure 3 shows the cryptanalysis in CrypTool 2). After several restarts, we began to see English words emerge, but they were separated by incorrect letters. Upon closer examination of these separations and the corresponding ciphertext numbers, we noticed that characters separating words were always represented by odd numbers in the ciphertext. This led us to hypothesize that all odd numbers were ’nulls’, meaning they were characters without meaning, intended to confuse a cryptanalyst during cryptanalysis. We then marked all odd numbers as nulls, instructing the Homophonic Substitution Analyzer to ignore them during automated analysis. Additionally, we configured the initial key of the cryptanalysis algorithm to assign only one letter for each ciphertext symbol in the letter distribution. These adjustments allowed us to decipher the full text, revealing that it was encrypted using only a simple monoalphabetic substitution. Figure 2 presents a graph depicting the

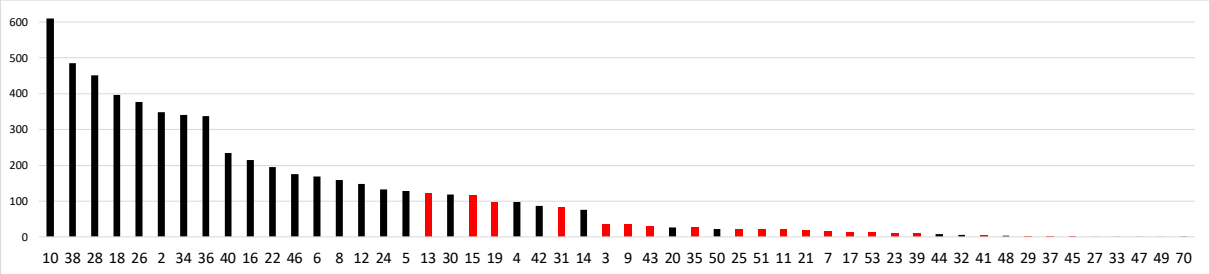

Figure 2: Ciphertext number frequencies: black bars for symbols, red bars for nulls.

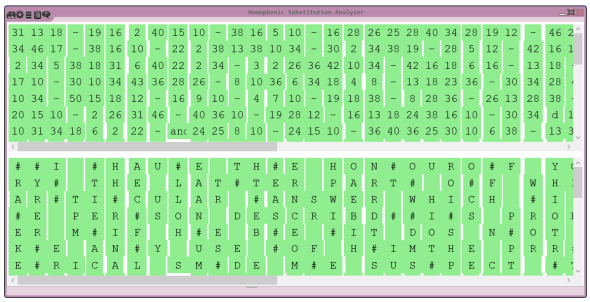

Figure 3: CrypTool 2's Homophonic Substitution Analyzer analyzing the ciphertext

distribution of numbers in the ciphertext. The graph utilizes black bars to represent actual ciphertext symbols, while red bars are used to denote nulls. In the deciphered text, the letter pairs 'i' and 'j', as well as 'u' and 'v', are each encrypted with the same ciphertext symbol, a characteristic typical of ciphers of that period.

In the following, we present the cipher's key:

`nulls = odd numbers; A = 2; B = 4; C = 6;`
`D = 8; E = 10; F = 12; G = 14; H = 16; I = 18;`
`K = 20; L = 22; M = 24; N = 26; O = 28;`
`P = 30; Q = 32; R = 34; S = 36; T = 38;`
`U = 40; W = 42; X = 44; Y = 46; Z = 48; & = 50`

As can be observed in the shown key, the distribution of ciphertext symbols (numbers) onto plaintext characters (letters) follows a highly regular pattern: 'A' starts with 2, 'B' follows with 4, 'C' with 6... and 'Z' ends with 48. In other words, a simple consecutive numbering scheme (using even numbers) was employed for the creation of the cipher. It's evident that this approach is quite careless and even in the time of its creation was not a recommended method for generating a cipher. The consistent pattern simplifies the cryptanalysis process once the cryptanalyst recognizes it. Significantly, the word 'and' is the only word assigned its distinct ciphertext symbol (50).

We also closely examined the cleartext words appearing within the ciphertext numbers. The simple words among these fit syntactically into the sentences where they are placed, acting as regular parts of these sentences. But the code names that appear also integrate smoothly into the flow of the letter's text. Based on their positioning, we suspect that these names might refer to either people or places, even if only personal names are used as code words. Interestingly, most of the code words in the text appear as pairs and as alliterations, meaning each name of a code word starts with the same initial letter, such as in the example "Waller and Wall."

We also concluded that these code words serve as the so-called 'nomenclature elements' of the letter. They still represent the most significant mystery of the letter yet to be solved. Without additional context or the original key used, we cannot ascertain the meaning of these names. Historians should look at the deciphered letter's cleartext to possibly learn more about these code names and give more meaning to them.

6 Edition of the letter

This section presents an edited version of the first two pages of the decrypted letter. All decrypted plaintext letters are capitalized for clarity. The code words found in the text are written in their original form. All nulls were removed from the text. Additionally, punctuation (full stops for endings of sentences) has been added to enhance readability. Typos were left in the text:

Page 1:

```
Feb 24 1724
I HAUE THE HONOUR OF YOUR LETTER OF THE a.t.
OF IANUARY THE LATTER PART OF WHICH I THOUGHT
REQUIRED A PARTICULAR ANSWER WHICH I SEND
ENCLOS BY ITSELF. THE PERSON DESCRIBD IS
PROBABLY THE PERSON ENQUIRD AFTER AND IF HE
BE IT DOS NOT SEEM TO ME THAT YOU CAN MAKE
ANY USE OF HIM. THE PROIECT HE PROPOSD TO ME
CHIMERICAL and MADE ME SUSPECT THAT
```

Page 2:
HE WAS a MAN OF LITTLE CAPACITY OR ONE SENT
BY THE COURT FROM HENCE TO TRY TO INSINUATE
HIMSELF INTO YOUR GOOD OPINION IN ORDER TO
BETRAY ANY CIUNSELLS OR DESIGNS OF YOURS THAT
MIGHT COME TO HIS KNOWLEDGE YOU HAUE. NOBA
THE BEST INFORMATION JCOUD GET ABOUT HIM and
whatever HE MAY BE I DONT QUESTION BUT YOU
WILL THINK IT PROPER TO BE upon YOUR GUARD
AGAINST HIA OR ANY OTHER PERSON THAT SHALL
COST YOU IN SUCH A MANNER.
Mons Ray & Rook HAS NOW MET

To facilitate reading the complete letter, the letter as well as its plaintext and all the photos of the ciphertext pages have been uploaded to the DECODE database (Héder and Megyesi, 2022), a repository for historical ciphers and keys (see (**?**)).

7 Content of the letter

Here are some interesting points mentioned in the letter. The use of code names makes it unclear who the involved individuals are and who is being referred to.

- An unknown individual proposed an unrealistic project, raising suspicions of potential betrayal.
- Mention is made of the political situation, with Mons. Ray & Rook (unidentified individuals) being inactive for six weeks.
- The Mons. Garnet and Gee, and the Mons. Grandy and Gay (unidentified – perhaps organs of government?) have committed 4,000 men to the cause.
- The Monsieur Waller & Wall group (unidentified individuals) had become cautious and hesitant in discussions.
- Success relied on public sentiment and external support, not just prominent allies.
- Caution was urged when dealing with loyal yet doubting friends.
- Nevertheless, the current political situation looked hopeful and it would soon be a good time to take action.
- Mr Echard and Mr Patington (unidentified individuals) could be persuaded if they were offered terms not prejudicial to the English interests.
- It is mentioned that Madame De Prie is inclined to support the cause mentioned but may require encouragement through financial incentives, which should be offered discreetly and skillfully.

Both the sender(s) and the recipient(s) of the letter remain unclear to us. The letter lacks salutations, with the mentioned individuals referred to only by code names (except for the mentioned Madame de Prie). Additionally, the letter ends abruptly due to missing pages, leaving us unaware of the identity of the author(s).

8 Historical Context

The letter, composed in 1724 during the reign of George I of Great Britain, coincided with a period marked by the looming threat of the Jacobite movement. The Jacobites, loyal to the exiled Stuart dynasty, were actively striving to reinstate a Stuart monarch on the British throne. This era witnessed significant Jacobite uprisings, most notably the rebellions of 1715 and 1745. The contents of the letter hint at potential connections to this movement, as the sender seeks French assistance, particularly from Madame de Prie, in their endeavors. Madame de Prie (1698-1727), also known as Jeanne Agnès Berthelot de Pléneuf, was a prominent figure in the French court during the 18th century, being the mistress of Louis Henri, Duke of Bourbon (1692-1740; "Monsieur le Duc"), who was prime minister of France. She held significant influence on him and played a crucial role in the political affairs of her time.

9 Conclusion

In summary, we can conclude that the letter was relatively easy to decipher, as the cipher used was weak even for its time. However, the letter leaves many unanswered questions, as we do not know the sender or the recipient, and the referenced individuals cannot be identified due to the use of code names. We suspect that the letter was sent within the Jacobite movement. Nevertheless, it is certain that the letter was neither written nor received by Henry Brougham (in whose archive the letter was found) since he was born in 1778, long after the letter was sent. It is possible that one of his ancestors had a connection to the Jacobites, leading to the letter's presence in his archive. Now, historians should analyze the letter, conduct background research, and solve the remaining mysteries.

Acknowledgments

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

References

Cipher ID-6317. 1724. Reproduced image from Ciphertext found in the UCL Special Collections' Brougham Archive. DECODE ID 6317, link: https://de-crypt.org/r/6317.

Jörgen Dinnissen and Nils Kopal. 2021. Island Ramanacoil a Bridge too Far. A Dutch Ciphertext from 1674. In *International Conference on Historical Cryptology*, pages 48–57.

Mihály Héder and Beáta Megyesi. 2022. The DECODE Database of Historical Ciphers and Keys: Version 2. In *International Conference on Historical Cryptology*, pages 111–114.

Kevin Knight, Beáta Megyesi, and Christiane Schaefer. 2011. The Copiale Cipher. In *Proceedings of the 4th Workshop on Building and Using Comparable Corpora: Comparable Corpora and the Web*, pages 2–9.

Nils Kopal and Michelle Waldispühl. 2022. Deciphering Three Diplomatic Letters Sent by Maximilian II in 1575. *Cryptologia*, 46(2):103–127.

Nils Kopal. 2018. Solving Classical Ciphers with CrypTool 2. In *Proceedings of the 1st International Conference on Historical Cryptology HistoCrypt 2018*, number 149, pages 29–38. Linköping University Electronic Press.

Nils Kopal. 2019. Cryptanalysis of Homophonic Substitution Ciphers Using Simulated Annealing with Fixed Temperature. In *Proceedings of the 2nd International Conference on Historical Cryptology, HistoCrypt*, pages 107–16.

George Lasry, Norbert Biermann, and Satoshi Tomokiyo. 2023. Deciphering Mary Stuart's Lost Letters From 1578-1584. *Cryptologia*, 47(2):101–202.

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*, 0(0):1–15.

Beáta Megyesi, Alicia Fornés, Nils Kopal, Benedek Láng, Michelle Waldispühl, Vasily Mikhalev, and Bernhard Esslinger. 2024. Historical Cryptology. In *Chapter 3 of Bernhard Esslinger, Learning and Experiencing Cryptography with CrypTool and SageMath*, pages 97–138. Artech House, Norwood.