

Lightning Talk #1

Déchiffrement de lettres historiques



Maxence MONCEL & Loïc ROUQUETTE

EPITA - Laboratoire de Recherche de l'EPITA (LRE)

12 mars 2026

Déchiffrement de lettres historiques

Problème...

Objectifs

Roadmap

Conclusion & Perspectives



- Lettres chiffrées du XVIII-XIXème
- Chiffrement par **nomenclator & substitution homo-phonique/par dictionnaire** [5]
- Déjà des pistes de déchiffrement à l'époque
- Des méthodes de chiffrement (parfois) très inventives

Fun fact

Certains chiffrements n'étaient pas très sécurisés à l'époque... Leur but était plus de **re-tarder** la mise au claire du texte que de rendre le contenu indéchiffrable, les clés étant parfois produites à la chaîne. [6]

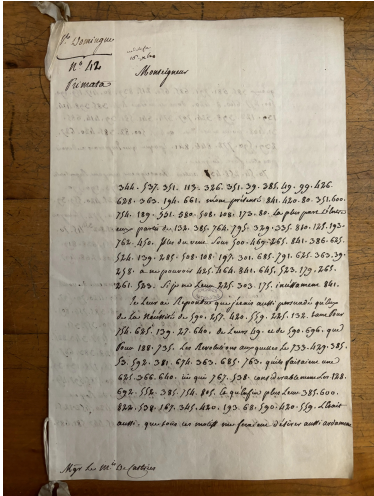


Figure 1: Un exemple de lettres chiffrées [5].

- Facile de vérifier que on a la bonne clé : Texte clair = Texte déchiffré
- Cependant, **nous n'avons pas la clé** (perdue ou jamais dévoilée)
- On va aussi devoir vérifier la cohérence du texte obtenu (proche du langage naturel)

Attention

Certains codes/symboles du chiffrement sont **nuls** et servent simplement à rendre le déchiffrement plus fastidieux. De plus, certains variantes pouvaient **ne pas délimiter les codes** et leur donner des tailles variables. [2]

Lightning Talk #1

- Créer une fonction testant la clé obtenue
- Se baser sur un système à base de n-grams [4] [1]
- Essayer d'optimiser/minimiser cette fonction (recherche locale)

Projet DECRYPT

Le déchiffrement de lettres est un sujet d'actualité! Le projet **DECRYPT** est une collection de textes chiffrés, clés de déchiffrement et de quelques outils informatiques visant à faciliter le déchiffrement de documents. [3]

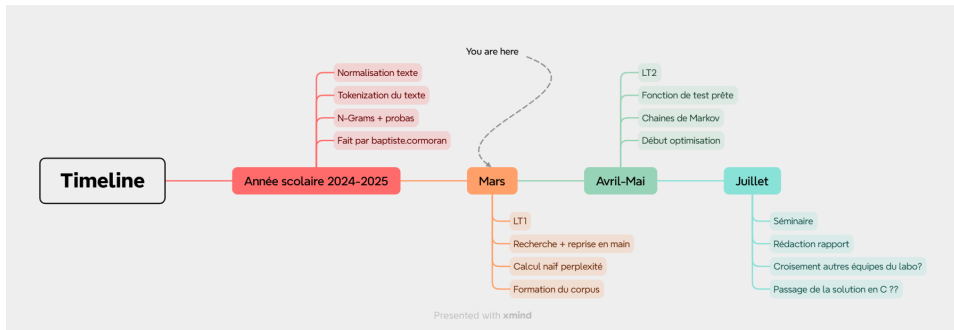


Figure 3 : Timeline du travail fait par mon prédécesseur et du travail à venir

Info

Cette timeline est **optimiste** et part du principe que tout avance à très bon rythme.

- Reprise d'un parcours entamé par Baptiste C.
- Déchiffrement de lettres du XVIII-XIXème par diverses méthodes
- Ajout d'un "Human in the loop"
- OCR pour lire la lettre [7]

Merci pour votre attention



- [1] Mohand Boughanem, Wessel Kraaij et Jian-Yun Nie. « Modèles de langue pour la recherche d'information ». In : *Les systemes de recherche d'informations* (2004), p. 163-182.
- [2] Camille Desenclos et George Lasry. « An early French digit cipher : deciphering a letter from the King of France to the Duke of Nevers (1592) ». In : ().
- [3] Beáta Megyesi et al. « Decryption of historical manuscripts : the DECRYPT project ». In : *Cryptologia* 44.6 (2020), p. 545-559. doi : [10.1080/01611194.2020.1716410](https://doi.org/10.1080/01611194.2020.1716410). eprint : <https://doi.org/10.1080/01611194.2020.1716410>. url : <https://doi.org/10.1080/01611194.2020.1716410>.
- [4] Beáta Megyesi et al. « Historical Language Models in Cryptanalysis : Case Studies on English and German ». In : *International Conference on Historical Cryptology*. 2023, p. 120-129.
- [5] Cécile Pierrot et al. « A Caribbean Directory-based Encryption during the American War of Independence ». In : *International Conference on Historical Cryptology (HistoCrypt 2025)*. Poznan, Poland, juin 2025. url : <https://hal.science/hal-05058227>.
- [6] Cécile Pierrot et al. « Deciphering Charles Quint (A diplomatic letter from 1547) ». In : *Linköping Electronic Conference Proceedings*. Sous la dir. de Carola Dahlke et Matthias Göggerle. T. 195. Munich, Germany, juin 2023, p. 148-158. doi : [10.3384/ecp195704](https://doi.org/10.3384/ecp195704). url : <https://hal.science/hal-04083014>.
- [7] Xusen Yin et al. « Decipherment of historical manuscript images ». In : *2019 International Conference on Document Analysis and Recognition (ICDAR)*. IEEE. 2019, p. 78-85.