Lightning Talk #2

Déchiffrement de lettres historiques

Maxence MONCEL & Loïc ROUQUETTE
EPITA - Laboratoire de Recherche de l'EPITA (LRE)
20 mai 2026

Lightning Talk #2 © 2026 Maxence MONCEL & Loïc ROUQUETTE is licensed under CC BY 4.0.
To view a copy of this license, visit https ://creativecommons.org/licenses/by/4.0/.

Table des matières

Rappel sujet

Progrès depuis la dernière fois

Perplexité naïve

Article

État de l'art

Cas de base : Substitutions simples

Méthode déchiffrement substitution homophonique basique

Prochaine étape

Bibliographie

licensed under CC BY 4.0

Rappel sujet

- Lettres chiffrées du XVIII-XIXème siècle
- Chiffrement par **nomenclator & substitution homo-phonique** [Pierrot et al., 2025]
- Environ 850 symboles clairs
- Nous n'avons pas la clé

licensed under CC BY 4.0

Progrès depuis la dernière fois

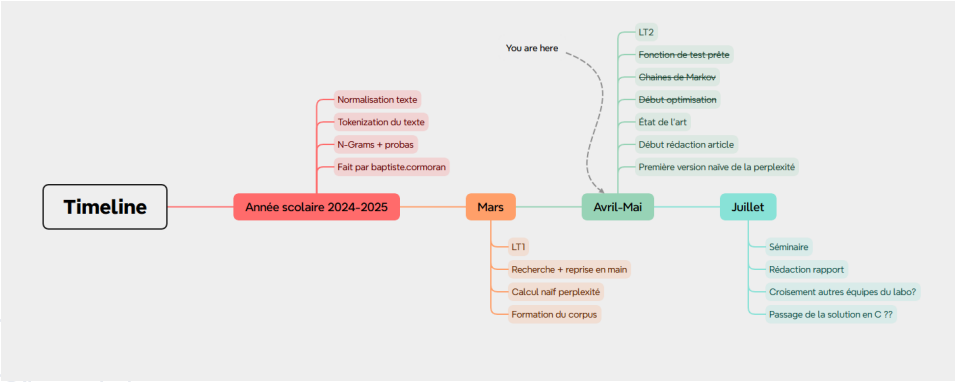

Figure 1 : La timeline réajustée du parcours recherche

licensed under CC BY 4.0

Perplexité naïve

- Entraîner un algorithme sur du texte sur le thème de la lettre
- Faire la perplexité moyenne de tous les n-grams possibles du texte
- Tester sur des sections de texte diverses
- Résultats surprenamment bons et cohérents

licensed under CC BY 4.0

Perplexité naïve (Bis)

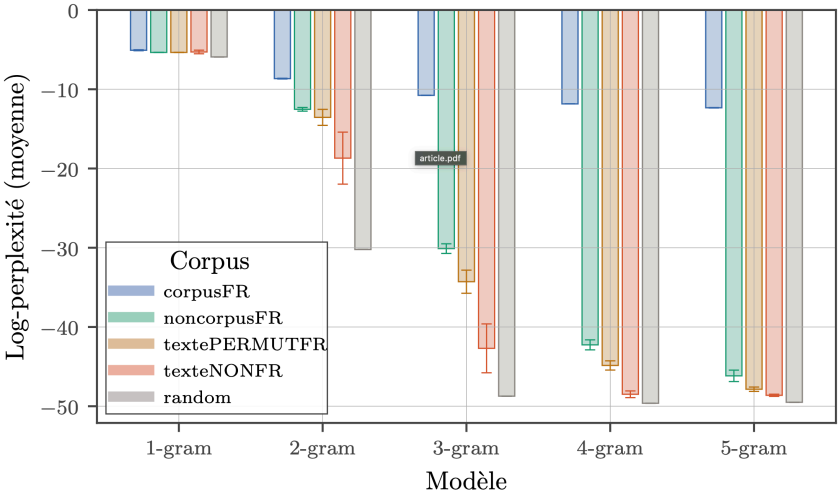

Figure 2 : Perplexité en fonction de la taille des n-grams

licensed under CC BY 4.0

Article

- Garder des traces de ce qui est fait
- Rendre le travail reproductible
- Intégration automatique des résultats
- Rolling release paper

licensed under CC BY 4.0

État de l'art

- Préparer la prochaine étape
- Savoir ce qui se fait
- Partir sur des bases solides

licensed under CC BY 4.0

Cas de base : Substitutions simples

- Écrit par **Michael Lucks** [Lucks, 1988]
- Se concentre sur le chiffrement par substitution simple
- Considère les lettres déjà trouvées dans les mots comme des contraintes
- Test cohérence du texte avec dictionnaire de mots
- Explore les clés possibles en rajoutant des contraintes et en retire si la résolution devient impossible

Bon à savoir

- Méthode exhaustive lente (surtout avec 850 symboles)
- Méthode plutôt intéressante considérant que l'on a (en grande partie) le dictionnaire de symboles clairs

licensed under CC BY 4.0

Méthode déchiffrement substitution homophonique basique

- Écrit par **A Dhavare, RM Low, M Stamp** [Dhavare et al., 2013]
- Algorithme en 3 parties
- Analyser le nombre de symboles chiffrés pour chaque symbol clair
- Création de plusieurs points de départ
- Hill climbing plus traditionnel

Bon à savoir

- La méthode de l'article ne parle pas du cas des symboles nuls
- Il suffit de déchiffrer **environ 80%** du texte pour que un humain puisse le finir à la main

licensed under CC BY 4.0

Prochaine étape

- Finir les recherches/état de l'art (divers algos de hill climbing) [Russell et Norvig, 2020]
- Finir d'implémenter hill climbing naïf
- Continuer rédaction du rapport
- Prendre une toute nouvelle approche ?

licensed under CC BY 4.0

Merci pour votre attention

Bibliographie i

- Dhavare, A., Low, R. M., & Stamp, M. (2013)
  Efficient cryptanalysis of homophonic substitution ciphers.
  Cryptologia.

- Lucks, M. (1988)
  A constraint satisfaction algorithm for the automated decryption of simple substitution ciphers.
  Conference on the Theory and Application of Cryptography.

- Pierrot, C., Damoiseau-Malraux, G., Mekhail, P., Chaline, O., & Perret, L. (2025)
  A Caribbean Directory-based Encryption during the American War of Independence.
  International Conference on Historical Cryptology (HistoCrypt 2025).

- Russell, S., & Norvig, P. (2020)
  Artificial Intelligence : A Modern Approach (4th Edition)
  .Pearson.

licensed under CC BY 4.0