Automatisation de la cryptanalyse des cryptosystèmes classiques à l'aide d'algorithmes modernes

CHEMALI Maïssa, DAHER Sarah, SOUAIBY Christina

Encadrante : Valérie Ménissier-Morain

Sommaire

Introduction

La Cryptanalyse, c'est quoi ?

JAIMELACRYPTANALYSE
texte en clair

CHIFFREMENT
clé de chiffrement

QZYOLEZTUIFCZSZEINL
texte chiffré

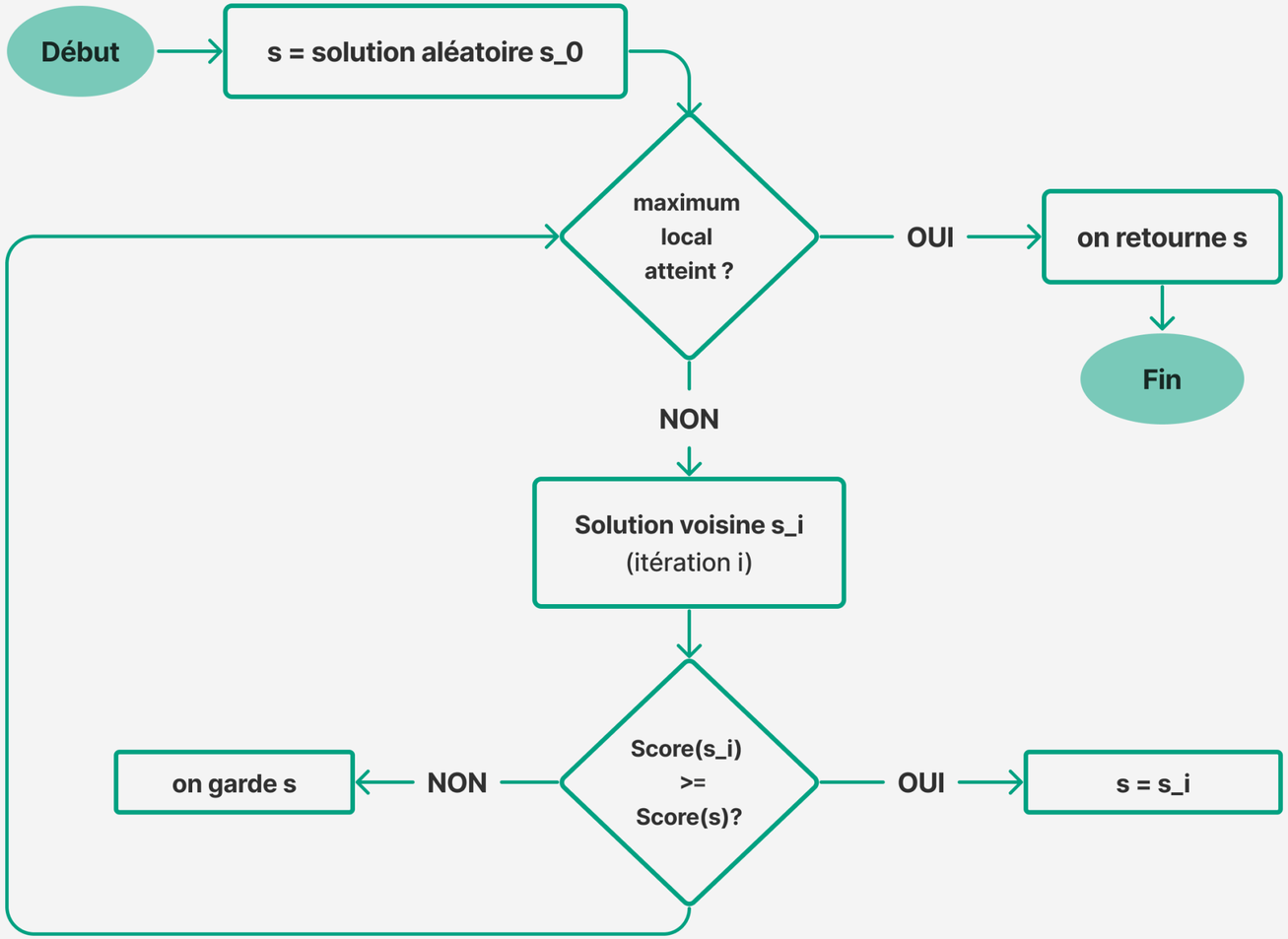
CRYPTANALYSE
algorithme de cryptanalyse

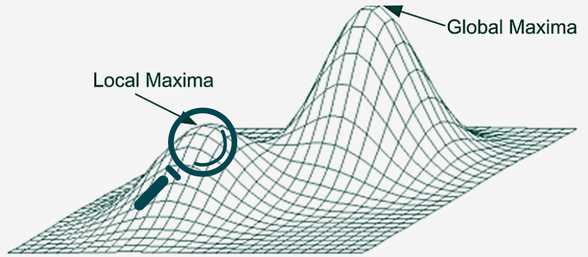
DÉCHIFFREMENT
clé de déchiffrement

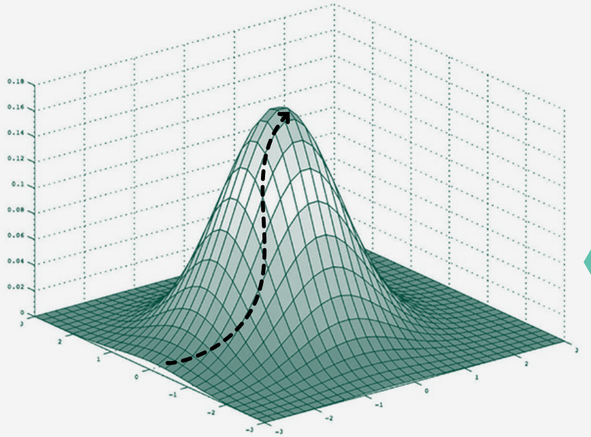
JAIMELACRYPTANALYSE
texte en clair

La clé de chiffrement est:
ZBTDLPGHYQKEOSMFJUNCRVWXIA

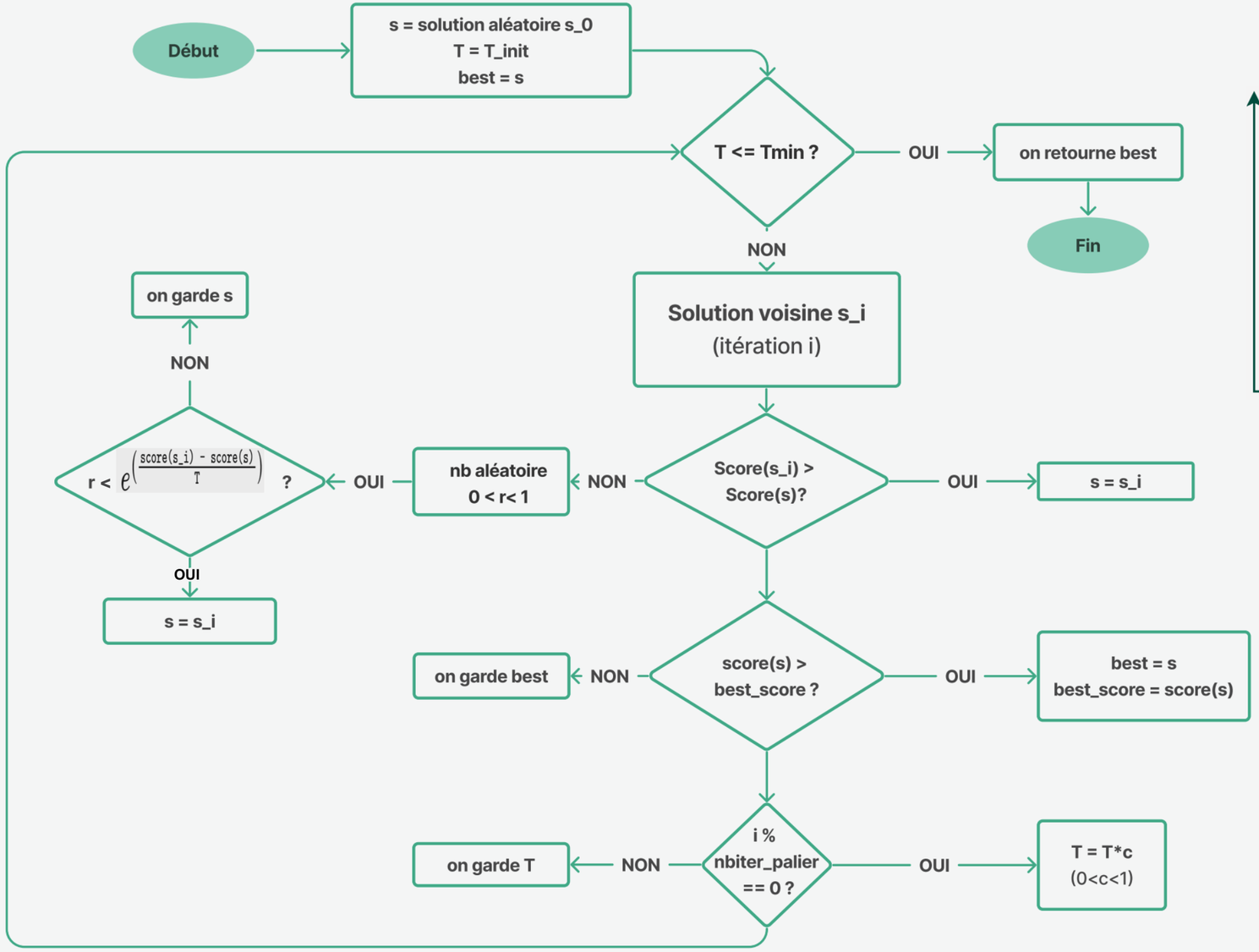
Principe de l'algorithme

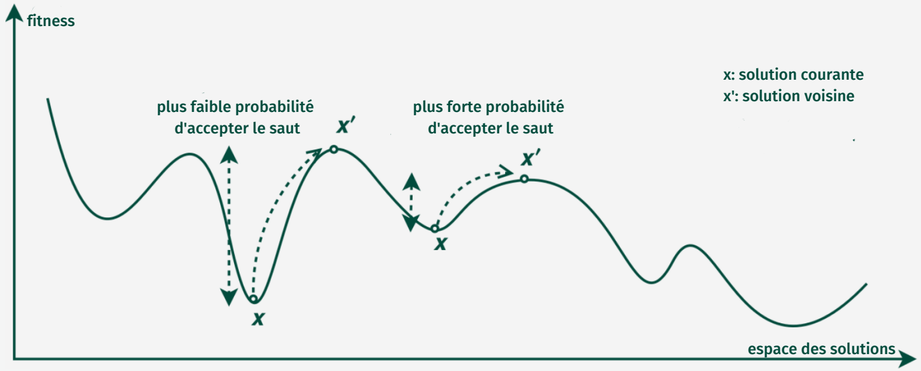






Principe de l'algorithme

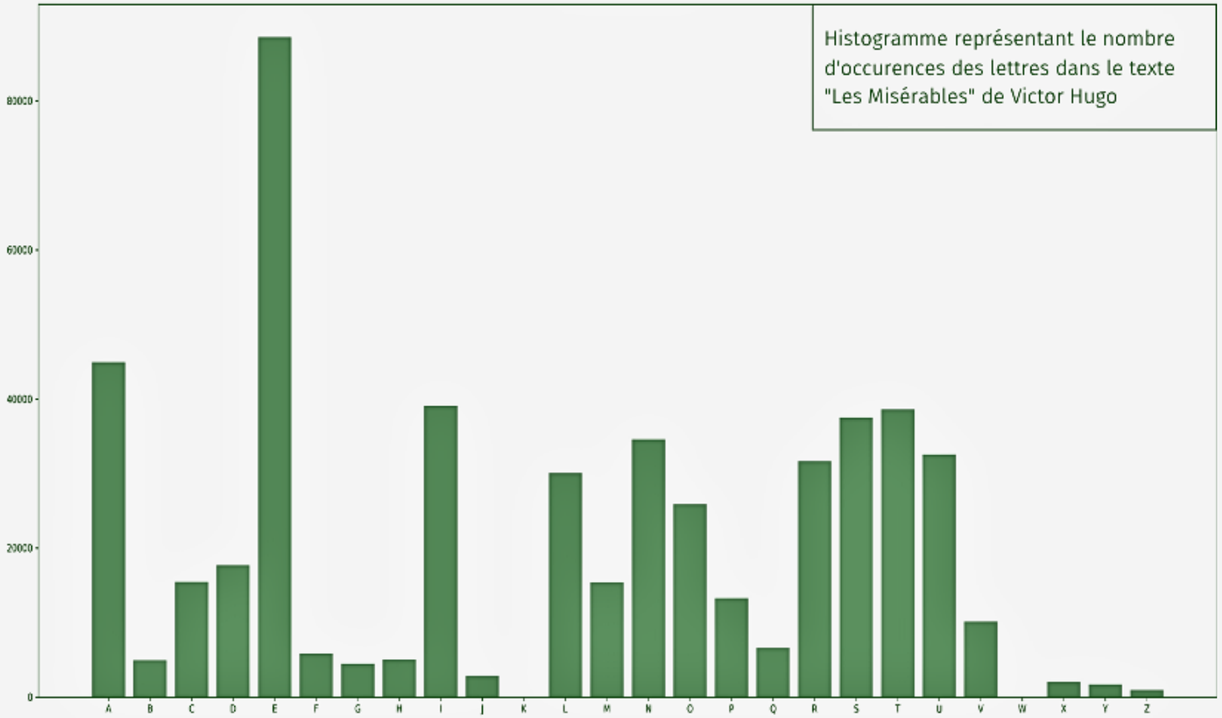




Fonction Fitness

Définition

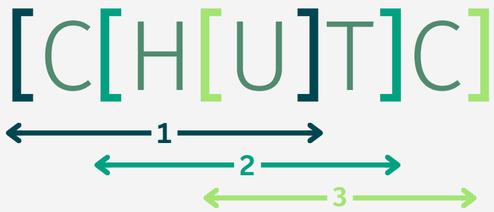
C'est une fonction qui a pour but d'attribuer une valeur quantitative à la qualité d'une solution.



La qualité est mesurée par la ressemblance du texte à un texte de la langue française.

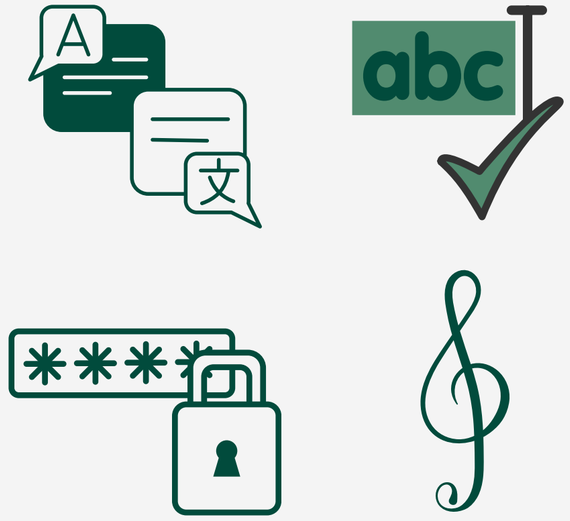
Les N-grammes

Principe de la méthode



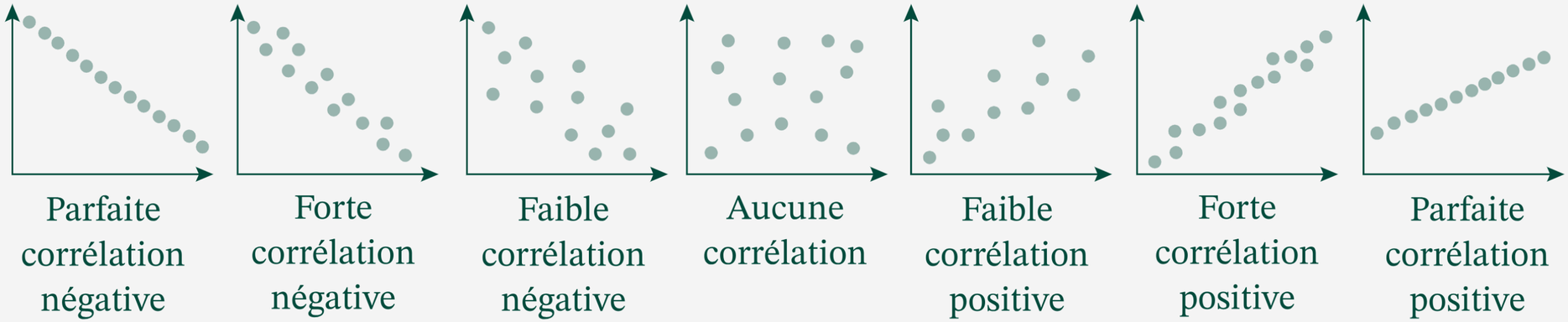
$$\prod_{i=0}^{\text{len(texte)-n}} \text{fréquences(texte[i:i+n])}$$

$$\sum_{i=0}^{\text{len(texte)-n}} \log(\text{occurrences(texte[i:i+n])})$$



La Corrélation de Pearson

Principe de la méthode



$$\frac{\sum (X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum (X_i - \bar{X})^2 \sum (Y_i - \bar{Y})^2}}$$

X_i : fréquence des lettres dans le texte en cours de transformation

Y_i : fréquence des lettres dans le texte de référence de la langue française

Résultats : Corrélation de Pearson

Texte Chiffré de départ :

TQDXUDVJSQDOUWDQWWQVUSTQSVUQUZSBXEXUDVXJDOQWZQEQOWVXWDOQWXZANO
UFNSMQSXTXSDRJQTQWPQJYSNTDJOSQWVQWCXBWVQZXANJUZZQQDVJPQOENJWQDQW
CQJDQDOQVQZXHQZLURJQOQCOUDVQOOUQOQQDUQSSQZQTAXOOQDUQORJUQDXUDO
QEQSJTQDDQPNUWUZSXMQSXUDRJQDONUWHQOZUSQWNSCNJEXUDDNJKNJOWTJZHJDQ
OTQZZQWZXJSXTTUVQSDXOOUEQXZXTXLQVQYDOXTDUNSJSQTONJTXWWQXZZXUDXOOQ
DQOZQDOXEXUZCQSVXSDJSLOXSVRJXODVAQJOQQSHXWVJDQOOUJSWUZQSTQWQDXUDP
XUDZQWMNJZUSQJOWSQHOXSZXUQSDCZJWZQWDOQDQXJYVJSONJZQMQSDCONZNSLQ

- Taille : 445 caractères
- Fonction fitness Choisie : Pearson
- Algorithme Choisi : Recuit Simulé

```
PS C:\Users\mache\Desktop\Projet-013_nvv> & C:/Users/mache/AppData/Local/Programs/Python/Python311/python.exe c:/Users/mache/Desktop/Projet-013_nvv/main2.py
IRQFMQNTJRQBMVQRVVRNMJIRJNMRMCJSFLFMQNFTQBRVCRLRBV
NFVQBRVFCADBMUDJGRJFIFJQETRIRVWRTZJDIQTBJRVNRVOFSV
NRCFADTMCCRRQNTWRBLDTVRQRVORTQRQBRNRCFYRCKMETRBROB
MQNRBBMRBRRQMRJJRCRIAFBBRQMRBETMRQFMQBRLRJTIRQQRWD
MVMCJFGRJFMQETRQBDMVYRBCMJRVDJODTLFMQQDTHDTBVITCYT
QRBIRCCRVCFTJFIIMNRJQFBBMLRFCFIFKRNRZQBFIQMDJTJRIB
DTIFVVRFCCFMQFBBRQRBCRQBFLFMCORJNFJQTJKBFJNETFBQNA
RTBRRJYFVNTQRBBMTJVMCRJIRVRQFMQWFMQCRVGDTCMJRTBVJR
YBFJCFMRJQOCTVCRVQBRQRFTZNTJBDTCRGRJQOBDCDJKR
```

taille	cle_utilisee	cle_trouvee	%_caracteres_egaux	score_final
743	WKRGODMVBAUIXNCSFYLPJETHZQ	LYCWORGJXKHAMIBPVUZTQFDNES	4,17	0,73859927
743	WKRGODMVBAUIXNCSFYLPJETHZQ	ABLDRFOQGUTCMJHPNESKIVWXYZ	0	0,709749721
743	WKRGODMVBAUIXNCSFYLPJETHZQ	TYCDNAGSBQKLIOWPJHRFUMEXVZ	4,17	0,771041585
743	WKRGODMVBAUIXNCSFYLPJETHZQ	MHYAEIDNLGKOFJBTCZSWRVUQXP	0	0,719364556
743	WKRGODMVBAUIXNCSFYLPJETHZQ	ZAIHBFXMYDKLOWVJNRCPUTQGSE	4,17	0,730500994
743	WKRGODMVBAUIXNCSFYLPJETHZQ	AICBXSKGTPRVLJDZQEFUWMNOYH	0	0,815697535
743	WKRGODMVBAUIXNCSFYLPJETHZQ	LBGHSFNEMJWOIAZRQUVKYPDTCX	0	0,756435704
743	WKRGODMVBAUIXNCSFYLPJETHZQ	WBDNJSKIAYZLQMOVHXUTECGRPF	4,17	0,752553219
743	WKRGODMVBAUIXNCSFYLPJETHZQ	XBCWFTGVZJKIMNOPLRESYHUQDA	12,5	0,748859374
743	WKRGODMVBAUIXNCSFYLPJETHZQ	LATGMOJVQSKICPEZBRWNYFHUXD	12,5	0,807771991
			4,168	

Série de 10 tests réalisés avec Hill Climbing sur un même texte

Légende
%MIN
%MAX
%MOYEN

Résultats : N-grammes

Texte Chiffré de départ

TQDXUDVJSQDOUWDQWWQVUSTQSVUQUZSBXEXUDVXJD
OQWZQEQOWVXWDOQWXZANOUFNSMQSXTXSDRJQTQWP
QJYSNTDJOSQWVQWCXBWVQZXANJUZZQQDVJPQOENJWQ
DQWCQJDQDOQVQZXHQZLURJQOQCOUDVQOOUQOQQDU
QSSQZQTAXOOQDUQORJUQDXUDOQEQSJTQDDQPNUWUZ
SXMQSXUDRJQDONUWHQOZUSQWNSCNJEXUDDNJKNJOW
TJZHJDQOTQZZQWZXJSXTTUVQSDXOOUEQXZXTXLQVQYD
OXTDUNSJSQTONJTXWWQXZZXUDXOOQDQOZQDOXEXUZC
QSVXSDJSLOXSVRJXODVAQJOQQSHXWVJDQOOUJSWUZQS
TQWQDXUDPXUDZQWMNJZUSQJOWSQHOXSZXUQSDCZJW
ZQWDOQDQXJYVJSONJZQMQSDCONZNSLQ

- **Taille : 445 caractères**
- **Fonction fitness Choisie : 4-grammes**
- **Algortihme choisi : Hill Climbing**
- **Paramètres :**
  Max_iter = 2000
  Max_stagnations = 250

```
exe c:/Users/mache/Desktop/Projet-013/main.py
On a stagné  250  fois
IETOUTDANETLUSTESSEDUNIENDUEURNXOJOUTDOATLESREJELSD
OSTLESORHYLUZYNMENOIONTFAEIESCEAVNYITALNESDESPOXSDE
ROHYAURREETDACELJYASETESPEATETLEDEROBERGUFAELEPLUTD
ELLUELEETUENNEREIHOLLETUELFAUETOUTLEJENAIETTECYUSUR
NOMENOUTFAETLYUSBELRUNESYNPYAJOUTTYAKYALSIARBATELIE
RRESROANOIIUDENTOLLUJEOROIOGEDEVTLOITUYNANEILYAIOSS
EORROUTOLLETELRETLOJOURPENDONTANGLONDFAOLTDHEALEENB
OSDATELLUANSURENIESETOUTCOUTRESMYARUNEALSNEBLONROUE
NTPRASRESTLETEOAVDANLYAREMENTPLYRYNGE
PS C:\Users\mache\Desktop\Projet-013> & C:/Users/ma
che/AppData/Local/Programs/Python/Python311/python.
exe c:/Users/mache/Desktop/Projet-013/main.py
Le score final apres  1227  iterations est  1773.82
On a stagné  250  fois
CETAITDUNETRISTESSEDINCENDIEILNYAVAITDAUTRESLEVERSD
ASTRESALHORIZONMENACANTQUECESFEUXNOCTURNESDESPAYSDE
LAHOUILLEETDUFERVOUSETESPEUTETREDELABELGIQUEREPRITD
ERRIEREETIENNELECHARRETIERQUIETAITREVENUCETTEFOISIL
NAMENAITQUETROISBERLINESONPOUVAITTOUJOURSCULBUTERCE
LLESLAUNACCIDENTARRIVEALACAGEDEXTRACTIONUNECROUCASS
EALLAITARRETERLETRAVAILPENDANTUNGRANDQUARTDHEUREENB
ASDUTERRIUNSILENCESETAITFAITLESMOULINEURSNEBRANLAIE
NTPLUSLESTRETEAUXDUNROULEMENTPROLONGE
```

Résultats : N-grammes

Texte Chiffré de départ

TQDXUDVJSQDOUWDQWWQVUSTQSVUQUZSBXEXUDVXJD
OQWZQEQOWVXWDOQWXZANOUFNSMQSXTXSDRJQTQWP
QJYSNTDJOSQWVQWCXBWVQZXANJUZZQQDVJPQOENJWQ
DQWCQJDQDOQVQZXHQZLURJQOQCOUDVQOOUQOQQDU
QSSQZQTAXOOQDUQORJUQDXUDOQEQSJTQDDQPNUWUZ
SXMQSXUDRJQDONUWHQOZUSQWNSCNJEXUDDNJKNJOW
TJZHJDQOTQZZQWZXJSXTTUVQSDXOOUEQXZXTXLQVQYD
OXTDUNSJSQTONJTXWWQXZZXUDXOOQDQOZQDOXEXUZC
QSVXSDJSLOXSVRJXODVAQJOQQSHXWVJDQOOUJSWUZQS
TQWQDXUDPXUDZQWMNJZUSQJOWSQHOXSZXUQSDCZJW
ZQWDOQDQXJYVJSONJZQMQSDCONZNSLQ

- **Taille : 445 caractères**
- **Fonction fitness Choisie : 4-grammes**
- **Algortihme choisi : Recuit Simulé**
- **Paramètres :**
  nb_iter_par_palier = 100
  Tmin = 1, Tinit = 1000 , c = 0.8

```
PS C:\Users\mache\Desktop\Projet-013> & C:/Users/mac
he/AppData/Local/Programs/Python/Python311/python.ex
e c:/Users/mache/Desktop/Projet-013/main.py
CETAITDUSETRINTENNEDISCESDIEILSYAVAITDAUTRENLEVERNDA
NTRENALHORIZOSMESACASTQUECENBEUFSOCTURSENDENPAYNDELA
HOUILLEETDUBERVOUNETENPEUTETREDELAGELXIQUEREPRITDERR
IEREETIESSELECHARRETIERQUIETAITREVESUCETTEBOINILSAME
SAITQUETROINGERLISENOSPOUVAITTOUJOURNCULGUTERCELLENL
AUSACCIDESTARRIVEALACAXEDEFTRACTIOSUSECROUCANNEALLAI
TARRETERLETRAVAILPESDASTUSXRASDQUARTDHEUREESGANDUTER
RIUSNILESCENETAITBAITLENMOULISEURNSEGRASLAIESTPLUNLE
NTRETEAUFDUSROULEMESTPROLOSXE
PS C:\Users\mache\Desktop\Projet-013> & C:/Users/mac
he/AppData/Local/Programs/Python/Python311/python.ex
e c:/Users/mache/Desktop/Projet-013/main.py
CETAITDUNETRISTESSEDINCENDIEILNYAVAITDAUTRESLEVERSDA
STRESALHORIWONMENACANTQUECESFEUXNOCTURNESDESPAYSDELA
HOUILLEETDUFERVOUSETESPEUTETREDELABELGIQUEREPRITDERR
IEREETIENNELECHARRETIERQUIETAITREVENUCETTEFOISILNAME
NAITQUETROISBERLINESONPOUVAITTOUJOURSCULBUTERCELLESL
AUNACCIDENTARRIVEALACAGEDEXTRACTIONUNECROUCASSEALLAI
TARRETERLETRAVAILPENDANTUNGRANDQUARTDHEUREENBASDUTER
RIUNSILENCESETAITFAITLESMOULINEURSNEBRANLAIENTPLUSLE
STRETEAUXDUNROULEMENTPROLONGE
```

Conclusion

	Recuit simulé	Hill Climbing
Qualité optimale	✓	
Efficacité temporelle		✓
N-grammes	✓	✓
Pearson		
Texte Court		
Texte Long	✓	✓