

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

Algorithmes de Cryptanalyse

- Hill Climbing
- Recuit Simulé

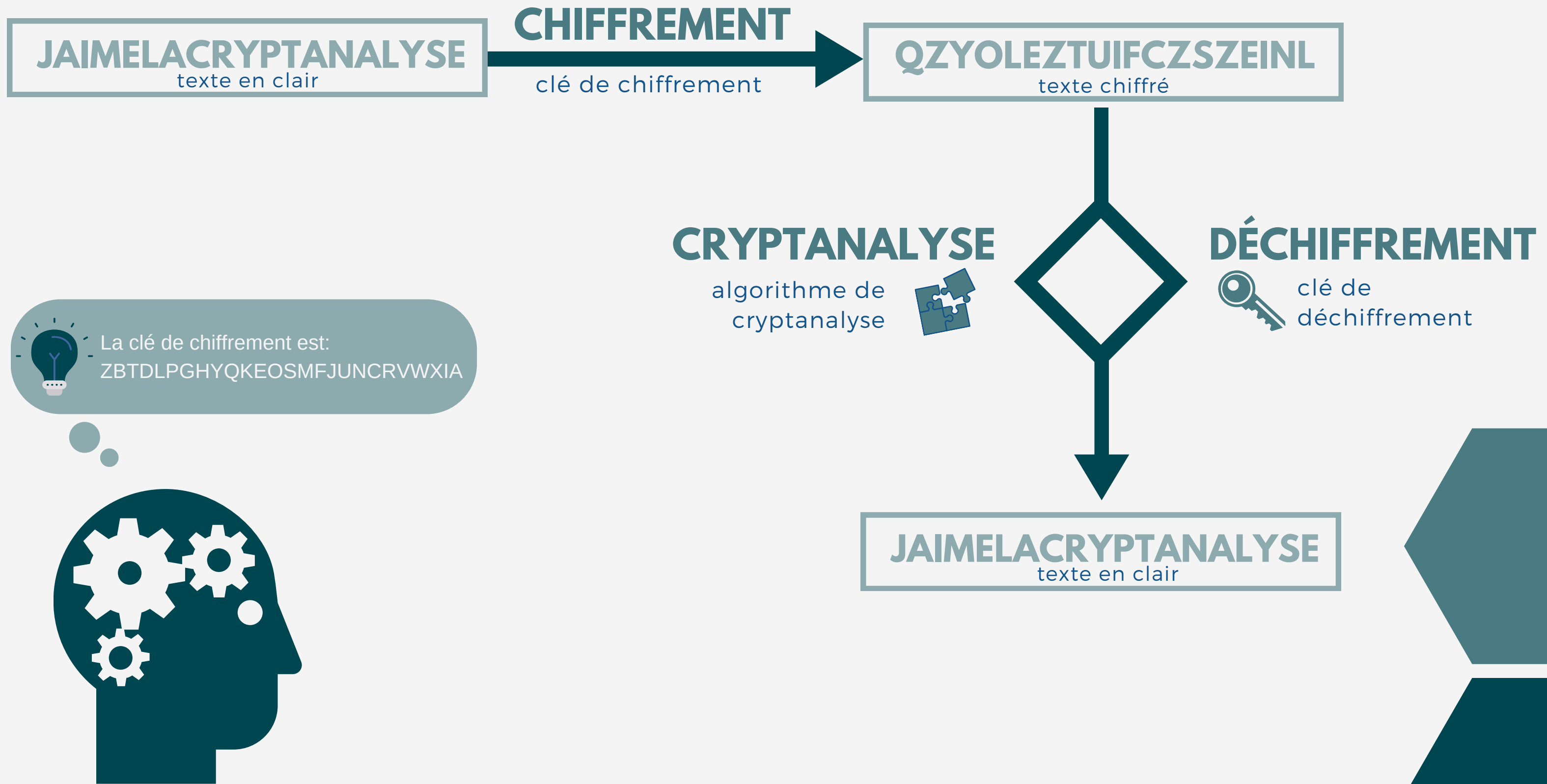
Fonctions Fitness

- Méthode des N-grammes
- Corrélation de Pearson

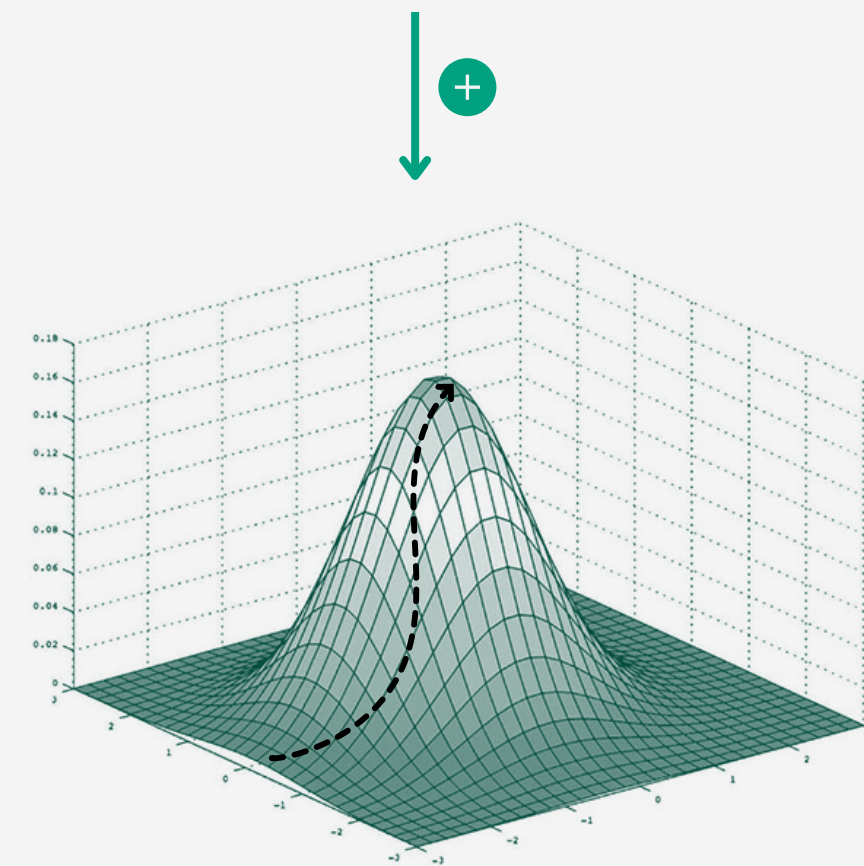
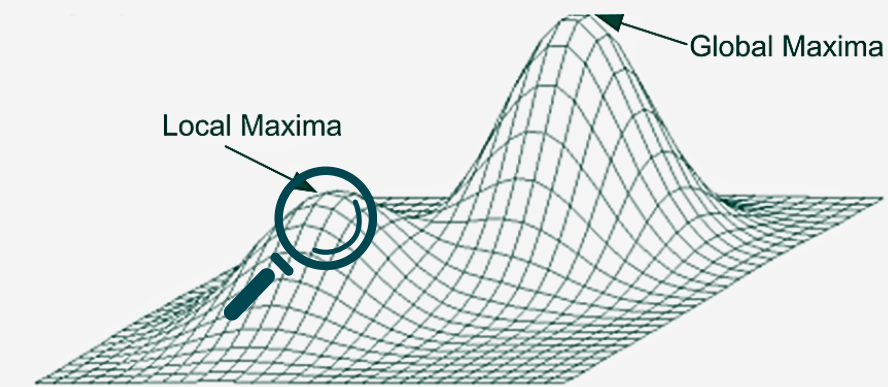
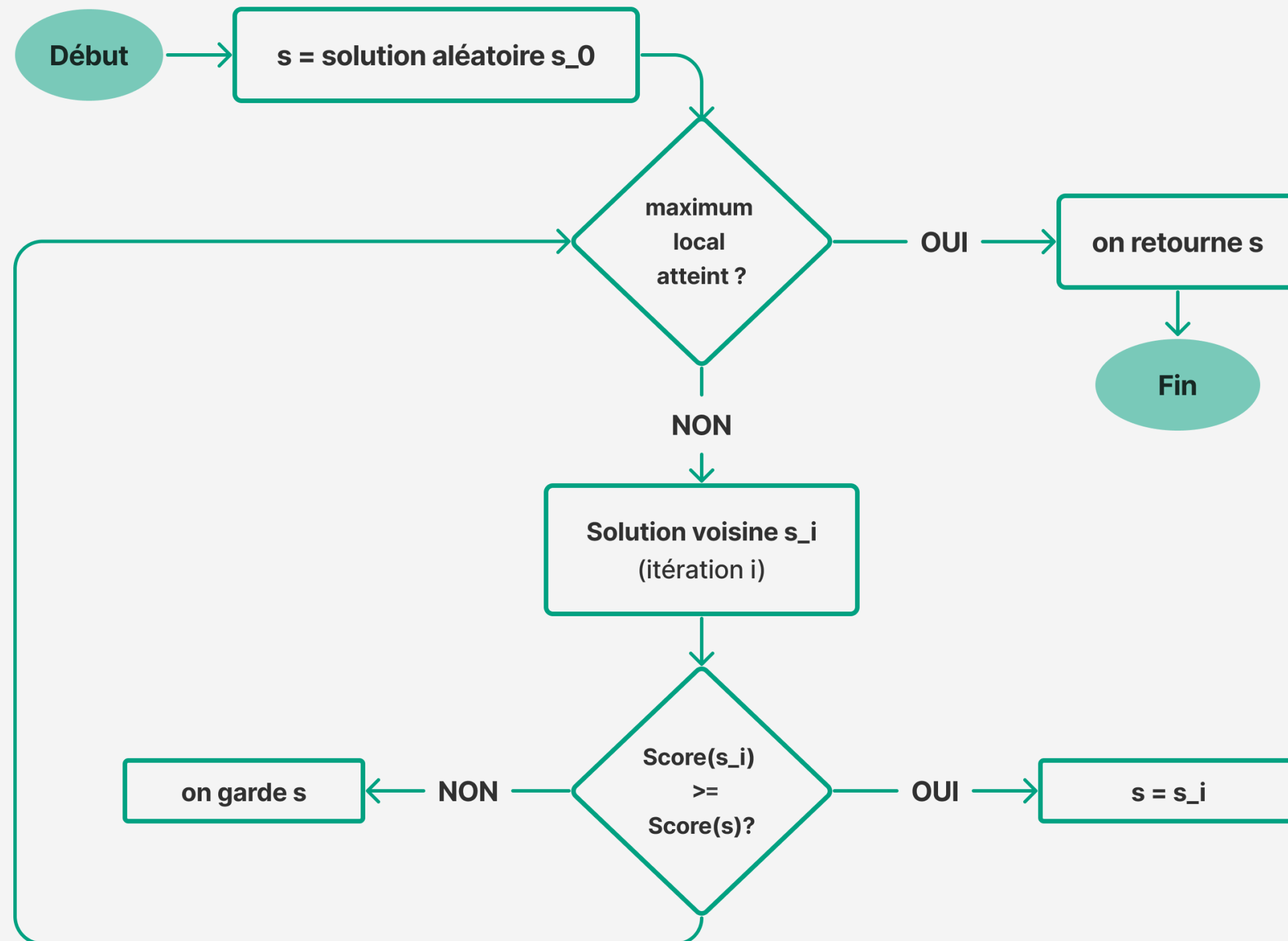
Résultats

Conclusion

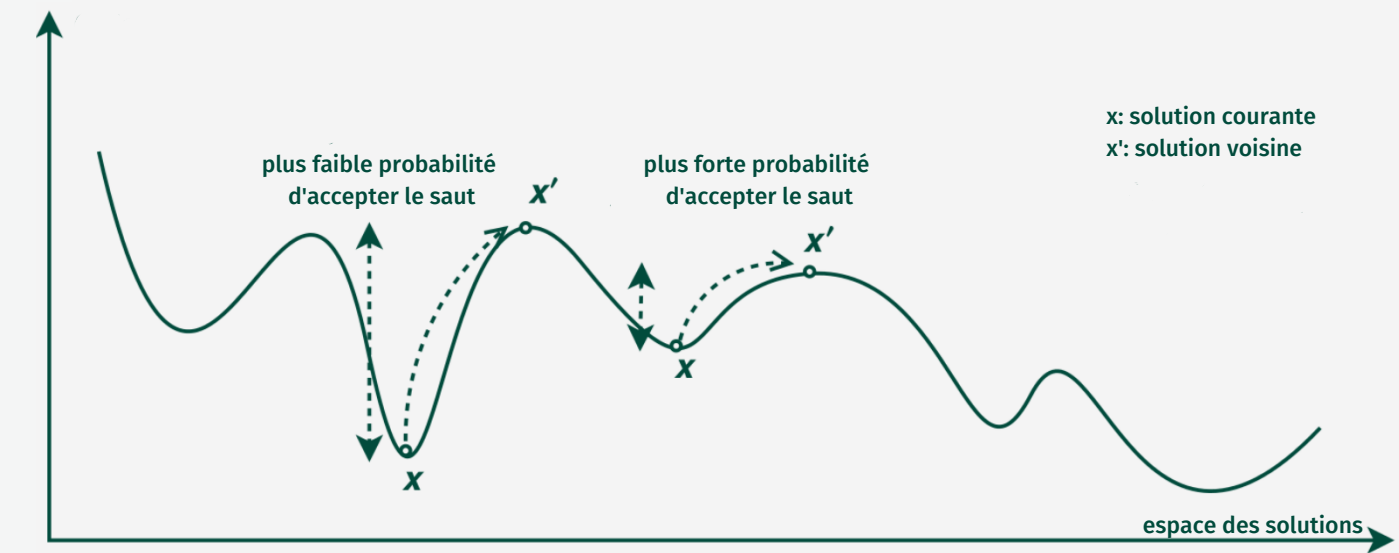
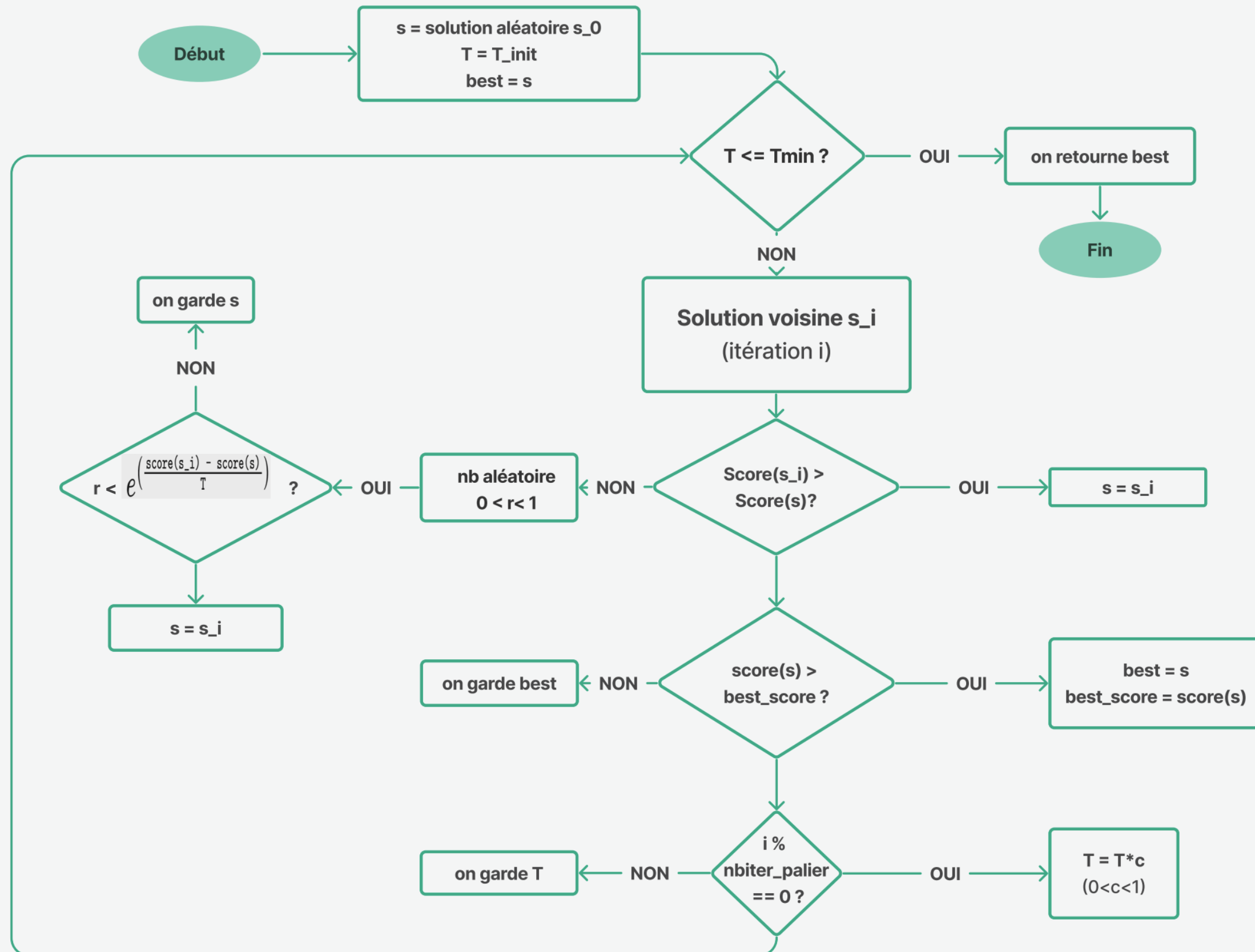
La Cryptanalyse, c'est quoi ?



Principe de l'algorithme

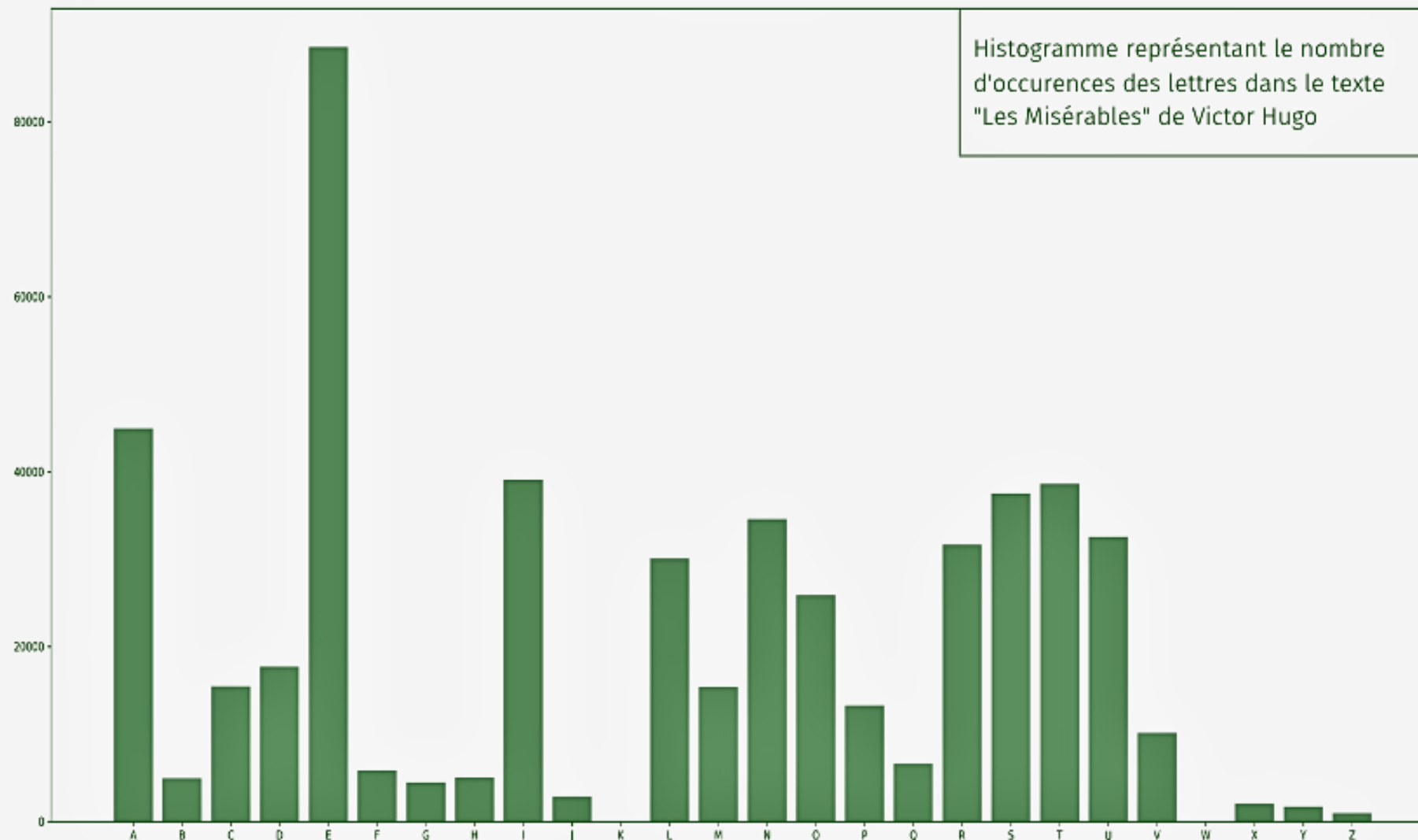


Principe de l'algorithme



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

[C[H[U]T]C]ESTUNSECRET

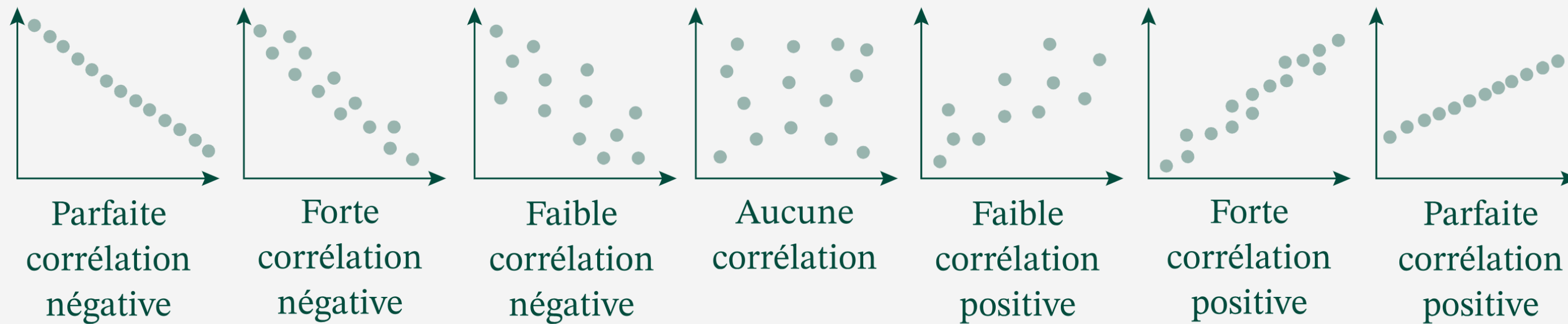
$$\prod_{i=0}^{\text{len}(\text{texte})} \text{fréquences}(\text{texte}[i:i+n])$$

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



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
QEQSJTDQDDQPNUWUZSXMQSXUDRJQDONUWHQOZUSQWNSCNJEXUDDNJKNJOWTJZHJDQ
OTQZZQWZXJSXTTUVQSDXOOUEQXZXTXLQVQYDOXTDUNSJSQTONJTXWWQXZZXUDXOOQ
DQOZQDOXEXUZCQSVXSDJSLOXSVRJXODVAQJOQQSHXWVJDQOOUJSWUZQSTQWQDXUDP
XUDZQWMNJZUSQJOWSQHOXSZXUQSDCZJWZQWDOQDQXJYVJSONJZQMQSDCONZNSLQ

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

```
PS C:\Users\mache\Desktop\Projet-013_nv> & C:/Use
rs/mache/AppData/Local/Programs/Python/Python311/p
ython.exe c:/Users/mache/Desktop/Projet-013_nv/ma
in2.py
IRQFMQNTJRQBMVQRVVRNMJIRJNMRMCJSFLFMQNFTQBRVCRLRBV
NFVQBRVFCADBUDJGRJFIFJQETRIRVWRTZJDIQTBJRVNRVOFSV
NRCFADTMCCRRQNTWRBLDTVRQRVORTQRQBRNRCFYRCKMETRBROB
MQNRBBMRBRRQMRJJRCRIAFBRRQMRBETMRQFMQBRLRJTIQQQRWD
MVMCJFGRJFMQETRQBDMVYRBCMJRVDJODTLFMQQDTHDTBVITCYT
QRBIRCCRVCFJTJFIIMNRJQFBBMLRFCFIFKRNZRQBFIQMDJTJRIB
DTIFVVRFCFCFMQFBBRQRBCRQBFLFMCORJNFJQTJKBFIJNETFBQNA
RTBRRJYFVNTQRBBMTJVMCRJIRVRQFMQWFMQCRVGDTCMJRTBVJR
YBFJCFMRJQOCTVCRVQBRQRFTZNTJBDTCRGRJQOBDCDJKR
```

taille	cle_utilisee	cle_trouvee	%_caracteres_egaux	score_final
743	WKRGO ^{DM} VB ^{AUI} XNCSFYLPJETHZQ	LYCW ^{OR} GJXKHAMIBPVUZTQFDNES	4,17	0,73859927
743	WKRGO ^{DM} VB ^{AUI} XNCSFYLPJETHZQ	ABLD ^R FOQ ^G UTCMJHPNESKIVWXYZ	0	0,709749721
743	WKRGO ^{DM} VB ^{AUI} XNCSFYLPJETHZQ	TYCDNAGS ^B QKLIOWPJHRFUMEXVZ	4,17	0,771041585
743	WKRGO ^{DM} VB ^{AUI} XNCSFYLPJETHZQ	MHYAEIDNLGKOFJBTCZSWRVUQXP	0	0,719364556
743	WKRGO ^{DM} VB ^{AUI} XNCSFYLPJETHZQ	ZAIHBFXMYDKLOWVJNRC ^P UTQGSE	4,17	0,730500994
743	WKRGO ^{DM} VB ^{AUI} XNCSFYLPJETHZQ	AICBXS ^K GTPRVLJDZQEFUWMNOYH	0	0,815697535
743	WKRGO ^{DM} VB ^{AUI} XNCSFYLPJETHZQ	LBGHSFNEMJWOIAZRQUVKYPDTCX	0	0,756435704
743	WKRGO ^{DM} VB ^{AUI} XNCSFYLPJETHZQ	WBDNJSKIAYZLQMOVHXUTECGRPF	4,17	0,752553219
743	WKRGO ^{DM} VB ^{AUI} XNCSFYLPJETHZQ	XBCWFTG ^V ZJ ^K IMNOPLRESYHUQDA	12,5	0,748859374
743	WKRGO ^{DM} VB ^{AUI} XNCSFYLPJETHZQ	LAT ^G MOJ ^V QSKI ^C PEZBRWNYFHUXD	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
OQWZQEOWVXWDOQWXZANOUFNSMQSXTXSDRJQTQWP
QJYSNTDJOSQWVQWCXBWVQZXANJUZZQQDVJPQOENJWQ
DQWCQJDQDOQVQZXHQZLURJQOQCOUDVQOOUQOQQDU
QSSQZQTAXOOQDUQORJUQDXUDOQEQSJTQDDQPNUWUZ
SXMQSXUDRJQDONUWHQOZUSQWNSCNJEXUDDNJKNJOW
TJZHJDQOTQZZQWZXJSXTTUVQSDXOOUEQXZXTXLQVQYD
OXTDUNSJSQTONJTXWWQXZZXUDXOOQDQOZQDOXEXUZC
QSVXSDJSLOXSVRJXODVAQJOQQSHXWVJDQOOUJSWUZQS
TQWQDXUDPXUDZQWMNJZUSQJOWSQHOXSZXUQSDCZJW
ZQWDOQDQXJYVJSONJZQMMSDCONZNSLQ

- 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
ROHYAURREETDACEJYASETESPEATETLEDEROBERGUF AELEPLUTD
ELLUELEETUENNEREIHOLLETUELFAUETOUTLEJENAIETTECYUSUR
NOMENOUTFAETLYUSBELRUNESYNPYAJOUTTYAKYALSIARBATELIE
RRESROANOI IUDENTOLLUJEOROIOGEDEVTL OITUYNANEILYATIOSS
EORROUTOLLETETELRETLOJOURPENDONTANGLONDFAOLDHEALEENB
OSDATELLUANSURENIESETOUTCOUTRESMYARUNEALSNEBLONROUE
NTPRASRESTLETEOAVDANLYAREMENTPLYRYNGE
PS C:\Users\mache\Desktop\Projet-013> & C:/Users/mache/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
ASDUTERRIUNSILENCESETAITFAITLESMOULINEURSNEBRANLATE
NTPLUSLESTRETEAUXDUNROULEMENTPROLONGE
```

Résultats : N-grammes

Texte Chiffré de départ

TQDXUDVJSQDOUWDQWWQVUSTQSVUQUZSBXEXUDVXJD
OQWZQEQQOWVXWDOQWXZANOUFNSMQSXTXSDRJQTQWP
QJYSNTDJOSQWVQWCXBWVQZXANJUZZQQDVJPQOENJWQ
DQWCQJDQDOQVQZXHQZLURJQOQCOUDVQOOUQOQQDU
QSSQZQTAXOOQDUQORJUQDXUDOQEQSJTQDDQPNUWUZ
SXMQSXUDRJQDONUWHQOZUSQWNSCNJEXUDDNJKNJOW
TJZHJDQOTQZZQWZXJSXTTUVQSDXOOUEQXZXTXLQVQYD
OXTDUNSJSQTONJTXWWQXZZXUDXOOQDQOZQDOXEXUZC
QSVXSDJSLOXSVRJXODVAQJOQQSHXWVJDQOOUJSWUZQS
TQWQDXUDPXUDZQWMNJZUSQJOWSQHOXSZXUQSDCZJW
ZQWDOQDQXJYVJSONJZQMMSDCONZNSLQ

- 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/mache/AppData/Local/Programs/Python/Python311/python.exe c:/Users/mache/Desktop/Projet-013/main.py
CETAITDUSETRINTENNEDISCESDIEILSYAVAITDAUTRENLEVERNDA
NTRENALHORIZOSMESACASTQUEECENBEUF SOCTURSENDENPAYNDELA
HOUILLEETDUBERVOUNETENPEUTETREDELABELGIQUEREPRITDERR
IEREETIESSELECHARRETIERQUIETAITREVESUCETTEBOINILSAME
SAITQUETROINGERLISENOSPPOUVAITTOUJOURNCULGUTERCELLENL
AUSACCIDESTARRIVEALACAXEDEFTRACTIOSUSECROUCANNEALLAI
TARRETERLETRAVAILPESDASTUSXRASDQUARTDHEUREESGANDUTER
RIUSNILESCENETAITBAITLENMOULISEURNSEGRASLAIESTPLUNLE
NTRETEAUF DUSROULEMESTPROLOSXE
PS C:\Users\mache\Desktop\Projet-013> & C:/Users/mache/AppData/Local/Programs/Python/Python311/python.exe c:/Users/mache/Desktop/Projet-013/main.py
CETAITDUNETRISTESSEDINCENDIEILNYAVAITDAUTRESLEVERSDA
STRESALHORIWONMENACANTQUEECESFEUXNOCTURNESDESPAYSDELA
HOUILLEETDUFERVOUSETESPEUTETREDELABELGIQUEREPRITDERR
IEREETIENNELECHARRETIERQUIETAITREVENUCETTEFOISILNAME
NAITQUETROISBERLINESONPOUVAITTOUJOURSCULBUTERCELLES
AUNACCIDENTARRIVEALACAGEDEXTRACTIONUNECROUCASSEALLAI
TARRETERLETRAVAILPENDANTUNGRANDQUARTDHEUREENBASDUTER
RIUNSIENCESETAITFAITLES MOULINEURSNEBRANLAIENTPLUSLE
STRETEAUXDUNROULEMENTPROLONGE
```


Conclusion

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

