jboulanger-1

Premier code reçu, le décryptage est faisable, le texte est court et haché par longueur de mot constante, la taille de la clef fait presque 3 blocs. Une fois la taille de la clef trouvée, le décodage trouve environ 90% de la clef. En doublant le texte, l'algorithme converge assez vite vers la bonne clef.

```
YIGNJ GWETR GMATB WSRAC RXNBF BVXNY LQQPG XKGWK LHRWC ABFSL
BECCE PRWRR UGAHQ ESKHW GKFNK GOEIZ SURME IEHMN ZXAGF WXZRR
HYMWF VPRAQ QNHWE HINOG WHFZL XHVSR BSIXT YSAFS ZQIAQ SIXVG
ZQQJB VANBK CGIHL IXXEI G
```

NEONICOTINOIDE

```
LESAB EILLE SEXPO SEESA DEFOR TSTAU XDINS ECTIC IDESO NTDES
TROUB LESDE MEMOI RECES TGRAC EALAM EMOIR EQUEL LESTR OUVEN
TLEUR CHEMI NJUSQ UALAN OURRI TUREE TQUEL LESCO MMUNI QUENT
LINFO RMATI ONAUX AUTRE S
```

jboulanger-3

La taille de la clef est facile à trouver, il y a assez de texte pour que les fréquences de coïncidences pour que l'algorithme fasse la différence entre du texte aléatoire et un langage. Le hachage par bloc de 5 ne semble pas poser problème ici. Merci maman !

```
XVBDU IQEQA NJQFP TFCMC BERUS CICGT CFNLB VPNJC GXOLV TGXNK
IBVIA JIJDN LVUIA OLVSJ NFUWI WTQIF XLRCK IWGFQ FFAEA BTJVY
ZSXTU IGAIA SIDPI JWNBC HWQJP IKIEI PNQLG CUERH CFFDV GJNFC
ECWQL ZSXTA IWQGG XINPI JQVQJ VQOLR IEYVW IFLVK PLFZL VCHVD
AKIFV LLOAV TSEAZ FFIWF XVSJN ZTLWB GWWMH DZAII FHOWF CAAIF
IWFVC HDUIY NWWNX RGJRU PNQHH GWAHP RZMQF GRVLD UIABV CAQWM
HACTH VGGRC KAADW KB
```

DISPARITION

```
UNJOU RILIM AGINA TOUTU NROMA NILYA URAIT DANSU NPAYS LOINT
AINUN GARON UNBAM BINAU NOMDA IGNAN ILAUR AITCI NQANS ILVIV
RAITD ANSUN PALAI SOUTO UTIRA ITALA BANDO NUNJO URSAN OUNOU
LUIDI RAITJ ADIST UAVAI SICIV INGTC INQCO USINS ALORS NOUSV
IVION SDANS LAPAI XMAIS UNAUN ILSON TTOUS DISPA RULON NAJAM
AISSU POURQ UOIAU JOURD HUITU DOISP ARTIR TONTO URSIN ONNOU
SALLO NSTOU SLAMO RT
```

tganty-1

L'algorithme trouve le texte assez facilement et de manière reproductible. Ce qui est marrant c'est que ma fonction objectif n'a été entrainée que sur du Français, je ne m'attendais pas à ce que ça décode de l'anglais aussi facilement. Comme quoi même si ces deux langages n'ont pas les mêmes fréquences de coïncidence, l'anglais et le français sont suffisamment différent d'un text aléatoire pour que l'algorithme le décode. Merci toto !

> Jv qpbl, wpv bpr gww'cj axidg kfxl ewtcb qxpqpu
>
> Qd eqdg r jxym gql uxet zgdcbumz
>
> Op dpmpmt kmaw um yycc B eiu ashm i kjzjs
>
> Mpmuv ygx bpg egvaba vyyi gmdgi bxx
>
> Ug hrrwxz bqcb bx

CRYPTII

> He said, one day you'll leave this world behind
>
> So live a life you will remember
>
> My father told me when I was just a child
>
> These are the nights that never die
>
> My father told me

cganty-1

Un petit clin d'oeil décrypté en 3 minutes dans le lit, merci Céline !

> Re qrti vk Nsrtrw
>
> Kwh duvlk h'omumj lewk
>
> Jy eumbj ur dk tfvyyek
>
> Yb inyek qolbeay

GEORGES

> La cane de Jeanne
>
> Est morte d'avoir fait
>
> Du moins on le presume
>
> Un rhume mauvais

jlandercy-1

Un extrait Wikipedia avec une clef simple, ça fonctionne assez bien.

> S'égyqvfé à bro qzcjl (Hnjlpodggfjg lkmdsnayj), wm éuvvsbé lcklfnsmvv,
> wkh hc alueatèel zzdsfh cgoeqimszlrk amj hbjh wm lwfepxfqjw ohhhcidasa
> (pp e'mkl oohsyb ims qhrj ymwzdjsd îtwk rh usil ; u'wgg as xieewsèyi
> rclgquicym imw n si gtmk jnhhp bwjfvaszzw wb Njgezsdwr) lx uifk zrh
> férqgfg pôamèimk wh zdbeiyfshzij lm kiq-tge lw do Avymmdds-Tjwyém.

HERISSONPOLISSON

> L'échidné à nez court (Tachyglossus aculeatus), ou échidné australien,
> est un mammifère vivant pratiquement sur tout le territoire australien
> (il n'est absent que dans quelques îles du nord ; c'est le mammifère
> autochtone qui a le plus vaste territoire en Australie) et dans les
> régions côtières et montagneuses du sud-est de la Nouvelle-Guinée.

jlandercy-2

Celle là, ça ne décode pas du tout. Pas assez d'information pour faire une attaque, on est dans le cas du masque jettable : https://fr.wikipedia.org/wiki/Masque_jetable.

> Auvhrixl mc fzue

ABCDEFGHIJKLMNOP

> Attendre et voir

jlandercy-3

Ca decode assez bien, mais ça mets plus de temps car l'espace des clef est immense 26^{35}.

> Pstv o yhw alvwcrw huaéumpctlg oymj-nzme usyazrggdre lzhw hr rrzxttwp lh ha dtnevr tplukj. Syoi cpwvyzfae à dhw azqjvrf xprprgk, p'Spzfbqhpwp hh Vbrppluxp mv s'Vvewcdppyw hp mmeêheh, qltw fiaxgatuixmpa à qrf mhpènif, wpwl i lbr jscri hn yih pwxqpa uvif-pijdlprk rzpzvg. Ropp di qihvgie hr rzqbdrf iken h'nmxcla ywerroppoyf, eitcdtlvv ksf zwjcsif wx o'hckfrv mydifnrw pu grp. Ptnl sfg aduxmfw à hpz xiérnwmzyw hn à qih pluedqvlg, znqh np wrefwl xrg zhrlnéi do fixn oh wzv cpfr qm géplvgaxtvv cwzlxép.

LHIRONDELLEDUNEPALDELICHONNIPALENSE

> Elle a les parties supérieures bleu-noir contrastant avec un croupion et un ventre blancs. Elle ressemble à ses proches parents, l'Hirondelle de Bonaparte et l'Hirondelle de fenêtre, mais contrairement à ces espèces, elle a une gorge et les plumes sous-caudales noires. Elle se nourrit en groupes avec d'autres hirondelles, attrapant des mouches et d'autres insectes au vol. Elle est soumise à des prédations et à des parasites, mais ne semble pas menacée au sein de son aire de répartition limitée.

bganty-1

D’abord j’ai eu un décodage partiel.

> Dr wvwf cvjiqmfivf rg pzv exeprw ts zbuphzn fsvjrax yh yu ciuwgr xvlxfr.
>
> P'vb q'rys d uhfgswg gspw qh uevh qh xvexyny : Ftsngz-pac fm ui crys. ypg

DMUNEBONNEV

> Af cise oiwevjtoib qs cmr jusves se moquent souvent de ma petite taille.
>
> L'un d'eux a inscrit tout en haut du tableau : Efface-moi si tu peux. vdm

bganty-1bis

En testant la clef qui semble la bonne, le début du texte apparait :

> Dr wvwf cvjiqmfivf rg pzv **exe**prw ts zbuphzn fsvjrax yh yu ciuwgr xvlxfr.
>
> P'vb q'rys d uhfgswg gspw qh uevh qh xvexyny : Ftsngz-pac fm ui crys. ypg

UNEBONNEVDM

> Je suis professeur et les sdrlqi gf vgrdnmj eeiwnfu mn lq buhjcw ujrkbq.
>
> B'io m'wvg j hdesfjc lpdc dd tqiu mm ujkkumk : Sgosdn-vny ey hv ywvg. ecc

bganty-1ter

En enlevant les deux lettres accentuées qui n’ont pas été chiffrées, on obtiens le bon message :

> Dr wvwf cvjiqmfivf rg pzv xprw ts zbuphzn fsvjrax yh yu ciuwgr xvlxfr.
>
> P'vb q'rys d uhfgswg gspw qh uevh qh xvexyny : Ftsngz-pac fm ui crys. ypg

UNEBONNEVDM

> **Je suis professeur et les lves se moquent souvent de ma petite taille.**
>
> **L'un d'eux a inscrit tout en haut du tableau : Efface-moi si tu peux. vdm**

Merci Bastien.