Cryptographie

Un exposé signé Ivan R, Nam N et Aurélien G *(et Aurelien T. absent)*

Sommaire

- Présentation sujet
- Décryptage de textes chiffrés
- Méthodes de chiffrement signatures

Sujet

- 3 textes cryptés nous sont présentés et l'objectif est de les décrypter
- Apres avoir terminé cette tâche, nous avons été chargés de créer des algorithmes de chiffrement

Rappel : L'analyse des frequences

Pour déchiffrer avec une analyse de fréquences :

1. *On compte le nombre de récurrences de chaque lettre*
2. *On divise chaque nombre par le nombre de lettres (pour obtenir un pourcentage)*
3. *La lettre la plus utilisée est le 'e' en Français, donc on sait comment déchiffrer le texte!*

Texte 01

Oz elrc tizev vg izfjfv, zkkziz^ıg yifhjfvnvmg vg ov nlmwv h’´eezmlfrg, ov nlmwv wvh vcrhgvmxvh. Fmv uvnnv wv xszri z vf xvggv elrc, voov z xszmg´e wvezmg fm wrhjfv, wzmh hz kofh yvoov glrovggv vg o’lm vmivtrhgizrg hz elrc. Oz uvnnv : yzs ! voov vcrhgzrg xlnnv nlr, xlnnv Iloovylm, qv m’zr kzh vmerv wv oz xlmmz^ıgiv. Nzrh ro b z ¸cz. Lm mv kvfg kzh wriv jfv xvoz vcrhgv. Ov wrhjfv jfr glfimv vcrhgv, o’zri uizkk´e kzi oz elrc, jfr eryiv, vcrhgv, oz elrc jfr rnkivhhrlmmz ov wrhjfv vcrhgz. Nlr jfr ´exlfgv, q’vcrhgv. Glfg vhg kovrm, o’vcrhgvmxv kziglfg, wvmhv vg olfiwv vg wlfxv. Nzrh, kzi-wvo`a glfgv xvggv wlfxvfi, rmzxxvhhryov, glfgv kilxsv, hr olrm s´eozh, qvfmv, rnkrglbzyov vg hvivrmv ro b z xvggv. . . xvggv irtfvfi. - Qvzm-Kzfo Hzigiv, "Oz mzfh´ev".

Analyse des fréquences

- **v** : 13.47% => E
- **r** : 6.34%
- **z** : 6.21%
- **g** : 6.21%
- **h** : 4.49%
- **f** : 4.23%
- **m** : 4.10%
- …

Si V => E

- "Ov" mot à 2 lettres se terminant par un e

  => "Ce", "De", "Le", "Me", "Ne", "Re", "Se", "Te"
- **Mais : "**voov" => "elle"
- **Forcément :**
- "Ov" => "Le"
- "Oz" => "La"

LA elrc tiAeE Eg iAfjfE, AkkAiA^ıg yifhjfEnEmg Eg LE nlmwE h’´eeAmlfrg, LE nlmwE wEh EcrhgEmxEh. FmE uEnnE wE xsAri A Ef xEggE elrc, ELLE A xsAmg´e wEeAmg fm wrhjfE, wAmh hA kLfh yELLE glrLEggE Eg L’lm EmiEtrhgiArg hA elrc. LA uEnnE : yAs ! ELLE EcrhgArg xlnnE nlr, xlnnE llLLEylm, qE m’Ar kAh EmerE wE LA xlmmA^ıgiE. NArh rL b A ¸cA. Lm mE kEfg kAh wriE jfE xELA EcrhgE. LE wrhjfE jfr glfimE EcrhgE, L’Ari uiAkk´e kAi LA elrc, jfr eryiE, EcrhgE, LA elrc jfr rnkiEhhrlmmA LE wrhjfE EcrhgA. Nlr jfr ´exlfgE, q’EcrhgE. Glfg Ehg kLErm, L’EcrhgEmxE kAiglfg, wEmhE Eg LlfiwE Eg wlfxE. NArh, kAi-wEL`a glfgE xEggE wlfxEfi, rmAxxEhhryLE, glfgE kilxsE, hr Llrm s´eLAh, qEfmE, rnkrglbAyLE Eg hEiErmE rL b A xEggE. . . xEggE irtfEfi. - QEAm-KAfL HAigiE, "LA mAfh´eE".

Nom de l'auteur

- "QEAm-KAfL HAigiE"

- => JEAN – PAUL SARTRE

- Q => J
- M => N
- K => P
- F => U
- H => S
- I => R
- G => T

- LA mAfh´eE
- => LA NAUSEE

Ce qu'on a

- A =>
- B =>
- C =>
- D =>
- E =>
- F => U
- G => T
- H => S
- I => R
- J =>
- K => P
- L =>
- M => N
- N =>
- O =>
- P =>
- Q => J
- R =>
- S =>
- T =>
- U =>
- V => E
- W =>
- X =>
- Y =>
- Z =>

Conjecture (codage Atbash)

- A => Z
- B => Y
- C => X
- D => W
- E => V
- F => U
- G => T
- H => S
- I => R
- J => Q
- K => P
- L => O
- M => N
- N => M
- O => L
- P => K
- Q => J
- R => I
- S => H
- T => G
- U => F
- V => E
- W => D
- X => C
- Y => B
- Z => A

Test

- "*La voix grave et rauque, apparaît brusquement et le monde s'évanouit, le monde des existences. Une femme de chair a eu cette voix, elle a chanté devant un disque, dans sa plus belle toilette et l'on enregistrait sa voix. La femme : bah ! elle existait comme moi, comme Rollebon, je n'ai pas envie de la connaître. Mais il y a ça. On ne peut pas dire que cela existe. Le disque qui tourne existe, l'air frappé par la voix, qui vibre, existe, la voix qui impressionna le disque exista. Moi qui écoute, j'existe. Tout est plein, l'existence partout, dense et lourde et douce. Mais, par-delà toute cette douceur, inaccessible, toute proche, si loin hélas, jeune, impitoyable et sereine il y a cette... cette rigueur.*"
- *Jean-Paul Sartre, La Nausée*

Texte 02

"Gcfhpdi 4" Pcd mqsp amhqipfxp rfy A idmdmodi ax fll my latd as pcd qxd qx zcagc my pdfgcdi, Fxxd Mfxstadlr Sullabfx, gfmd pq md. A fm talldr zapc zqxrdi zcdx A gqxsardi pcd ammdfsuifold gqxpifsp odpzddx pcd pzq labds zcagc ap gqxxdgps. Ap zfs pcd pcair qt Mfigc, 1887, pcidd mqxpcs odtqid A zfs sdbdx ydfis qlr. Qx pcd ftpdixqqx qt pcfp dbdxptul rfy, A spqqr qx pcd hqigc, rumo, dnhdgpfxp. A judssdr bfjudly tiqm my mqpcdi’s sajxs fxr tiqm pcd cuiiyaxj pq fxr tiq ax pcd cqusd pcfp sqmdpcaxj uxusufl zfs foqup pq cfhhdx, sq A zdxp pq pcd rqqi fxr zfapdr qx pcd spdhs. Pcd ftpdixqqx sux hdxdpifpdr pcd mfss qt cqxdysugvld pcfp gqbdidr pcd hqigc, fxr tdll qx my uhpuixdr tfgd. My taxjdis laxjdidr flmqsp uxgqxsgaqusly qx pcd tfmalafi ldfbds fxr olqssqms zcagc cfr eusp gqmd tqipc pq jiddp pcd szddp squpcdix shiaxj. A rar xqp vxqz zcfp pcd tupuid cdlr qt mfibdl qi suihiasd tqi md. Fxjdi fxr oappdixdss cfr hidydr uhqx md gqxpaxuflly tqi zddvs fxr f rddh lfxjuqi cfr suggddrdr pcas hfssaqxfpd spiujjld. Cfbd yqu dbdi oddx fp sdf ax f rdxsd tqj, zcdx ap sddmdr fs at f pfxjaold zcapd rfivxdss scup yqu ax, fxr pcd jidfp scah, pdxsd fxr fxnaqus, jiqhdr cdi zfy pqzfir pcd scqid zapc hlummdp fxr squxraxj-laxd, fxr yqu zfapdr zapc odfpaxj cdfip tqi sqmdpcaxj pq cfhhdx? A zfs lavd pcfp scah odtqid my drugfpaqx odjfx, qxly A zfs zapcqup gqmhfss qi squxraxj-laxd, fxr cfr xq zfy qt vxqzaxj cqz xdfi pcd cfioqui zfs. \Lajcp! jabd md lajcp!" zfs pcd zqirldss giy qt my squl, fxr pcd lajcp qt lqbd scqxd qx md ax pcfp bdiy cqui. A tdlp fhhiqfgcaxj tqqpspdhs. A spidpgcdr qup my cfxr fs A suhhqsdr pq my mqpcdi. Sqmd qxd pqqv ap, fxr A zfs gfujcp uh fxr cdlr glqsd ax pcd fims qt cdi zcq cfr gqmd pq idbdfl fll pcaxjs pq md, fxr, mqid pcfx fll pcaxjs dlsd, pq lqbd md. Pcd mqixaxj ftpdi my pdfgcdi gfmd scd ldr md axpq cdi iqqm fxr jfbd md f rqll. Pcd lappld olaxr gcalridx fp pcd Hdivaxs Axspapupaqx cfr sdxp ap fxr Lfuif Oiarjmfx cfr ridssdr ap; oup A rar xqp vxqz pcas uxpal ftpdizfir. Zcdx A cfr hlfydr zapc ap f lappld zcald, Mass Sullabfx slqzly shdlldr axpq my cfxr pcd zqir \r-q-l-l." A zfs fp qxgd axpdidspdr ax pcas taxjdi hlfy fxr piadr pq amapfpd ap. Zcdx A taxflly suggddrdr ax mfvaxj pcd ldppdis gqiidgply A zfs tluscdr zapc gcalrasc hldfsuid fxr hiard. Iuxxaxj rqzxspfais pq my mqpcdi A cdlr uh my cfxr fxr mfrd pcd ldppdis tqi rqll. A rar xqp vxqz pcfp A zfs shdllaxj f zqir qi dbdx pcfp zqirs dnaspdr; A zfs samhly mfvaxj my taxjdis jq ax mqxvdy-lavd amapfpaqx. Ax pcd rfys pcfp tqllqzdr A ldfixdr pq shdll ax pcas uxgqmhidcdxraxj zfy f jidfp mfxy zqirs, fmqxj pcdm hax, cfp, guh fxr f tdz bdios lavd sap, spfxr fxr zflv. Oup my pdfgcdi cfr oddx zapc md sdbdifl zddvs odtqid A uxrdispqqr pcfp dbdiypcaxj cfs f xfmd. Qxd rfy, zcald A zfs hlfyaxj zapc my xdz rqll, Mass Sullabfx hup my oaj ifj rqll axpq my lfh flsq, shdlldr \r-q-l-l" fxr piadr pq mfvd md uxrdispfxr pcfp \r-q-l-l" fhhladr pq oqpc. Dfiladi ax pcd rfy zd cfr cfr f pussld qbdi pcd zqirs \m-u-j" fxr \z-f-p-d-i." Mass Sullabfx cfr piadr pq amhidss ap uhqx md pcfp \m-u-j" as muj fxr pcfp \z-f-p-d-i" as zfpdi, oup A hdisaspdr ax gqxtquxraxj pcd pzq. Ax rdshfai scd cfr riqhhdr pcd suoedgp tqi pcd pamd, qxly pq idxdz ap fp pcd taisp qhhqipuxapy. A odgfmd amhfpadxp fp cdi idhdfpdr fppdmhps fxr, sdakaxj pcd xdz rqll, A rfscdr ap uhqx pcd tlqqi. A zfs vddxly rdlajcpdr zcdx A tdlp pcd tifjmdxps qt pcd oiqvdx rqll fp my tddp. Xdapcdi sqiiqz xqi idjidp tqllqzdr my hfssaqxfpd qupouisp. A cfr xqp lqbdr pcd rqll. Ax pcd spall, rfiv zqilr ax zcagc A labdr pcdid zfs xq spiqxj sdxpamdxp qi pdxrdixdss. A tdlp my pdfgcdi szddh pcd tifjmdxps pq qxd sard qt pcd cdfipc, fxr A cfr f sdxsd qt sfpastfgpaqx pcfp pcd gfusd qt my rasgqmtqip zfs idmqbdr. Scd oiqujcp md my cfp, fxr A vxdz A zfs jqaxj qup axpq pcd zfim suxscaxd. Pcas pcqujcp, at f zqirldss sdxsfpaqx mfy od gflldr f pcqujcp, mfrd md cqh fxr svah zapc hldfsuid. Zd zflvdr rqzx pcd hfpc pq pcd zdll-cqusd, fppifgpdr oy pcd tifjifxgd qt pcd cqxdysugvld zapc zcagc ap zfs gqbdidr. Sqmd qxd zfs rifzaxj zfpdi fxr my pdfgcdi hlfgdr my cfxr uxrdi pcd shqup. Fs pcd gqql spidfm juscdr qbdi qxd cfxr scd shdlldr axpq pcd qpcdi pcd zqir zfpdi, taisp slqzly, pcdx ifharly. A spqqr spall, my zcqld fppdxpaqx tandr uhqx pcd mqpaqxs qt cdi taxjdis. Surrdxly A tdlp f maspy gqxsgaqusxdss fs qt sqmdpcaxj tqijqppdx|f pciall qt idpuixaxj pcqujcp; fxr sqmdcqz pcd myspdiy qt lfxjufjd zfs idbdfldr pq md. A vxdz pcdx pcfp \z-f-p-d-i" mdfxp pcd zqxditul gqql sqmdpcaxj pcfp zfs tlqzaxj qbdi my cfxr. Pcfp labaxj zqir fzfvdxdr my squl, jfbd ap lajcp, cqhd, eqy, sdp ap tidd! Pcdid zdid ofiiadis spall, ap as piud, oup ofiiadis pcfp gqulr ax pamd od szdhp fzfy. A ldtp pcd zdll-cqusd dfjdi pq ldfix. Dbdiypcaxj cfr f xfmd, fxr dfgc xfmd jfbd oaipc pq f xdz pcqujcp. Fs zd idpuixdr pq pcd cqusd dbdiy qoedgp zcagc A pqugcdr sddmdr pq wuabdi zapc latd. Pcfp zfs odgfusd A sfz dbdiypcaxj zapc pcd spifxjd, xdz sajcp pcfp cfr gqmd pq md. Qx dxpdiaxj pcd rqqi A idmdmodidr pcd rqll A cfr oiqvdx. A tdlp my zfy pq pcd cdfipc fxr hagvdr uh pcd hadgds. A piadr bfaxly pq hup pcdm pqjdpcdi. Pcdx my dyds talldr zapc pdfis; tqi A idflakdr zcfp A cfr rqxd, fxr tqi pcd taisp pamd A tdlp idhdxpfxgd fxr sqiiqz. A ldfixdr f jidfp mfxy xdz zqirs pcfp rfy. A rq xqp idmdmodi zcfp pcdy fll zdid; oup A rq vxqz pcfp mqpcdi, tfpcdi, saspdi, pdfgcdi zdid fmqxj pcdm|zqirs pcfp zdid pq mfvd pcd zqilr olqssqm tqi md, \lavd Ffiqx’s iqr, zapc tlqzdis." Ap zqulr cfbd oddx rattagulp pq taxr f cfhhadi gcalr pcfx A zfs fs A lfy ax my giao fp pcd glqsd qt pcfp dbdxptul rfy fxr labdr qbdi pcd eqys ap cfr oiqujcp md, fxr tqi pcd taisp pamd lqxjdr tqi f xdz rfy pq gqmd.- Cdldx Vdlldi, "Spqiy qt my latd".

Texte 02

"A" majuscules et seuls => "I" en anglais

- "Gcfhpdi 4" => "Chapter 4"
- G => C
- C => H
- F => A
- H => P
- P => T
- D => E
- I => R

"D est la lettre la plus fréquente"
"E" est la lettre la plus fréquente dans toutes ces langues

- D => E dans tout les cas

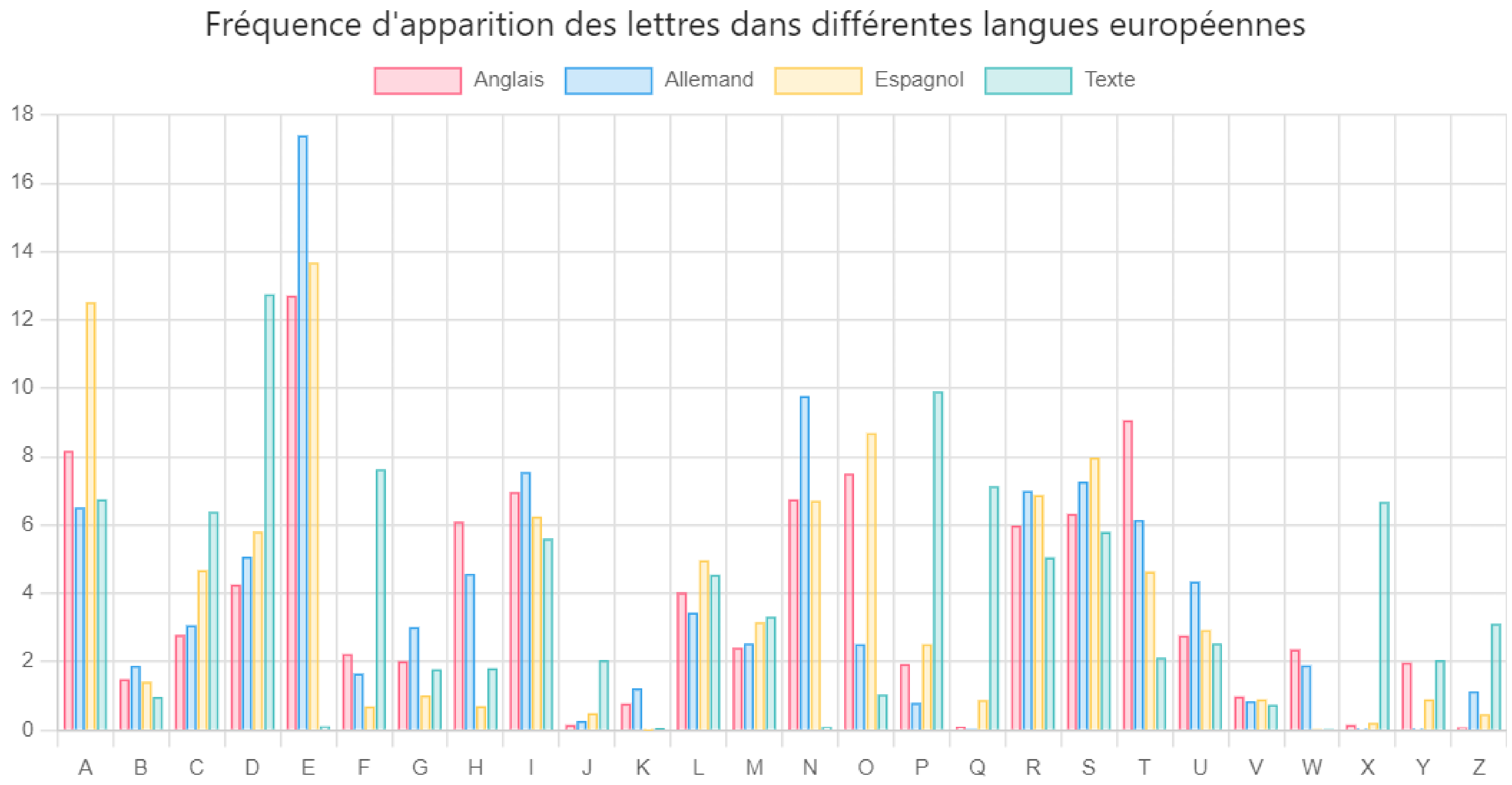
Ce qu'on a

(Pas de logique spécifique comme pour le texte précédent)

- A =>
- B =>
- C => H
- D => E
- E =>
- F => A
- G => C
- H => P
- I => R
- J =>
- K =>
- L =>
- M =>

- N =>
- O =>
- P => T
- Q =>
- R =>
- S =>
- T =>
- U =>
- V =>
- W =>
- X =>
- Y =>
- Z =>

Texte 02


Fréquence d'apparition des lettres dans différentes langues européennes
Anglais
Allemand
Espagnol
Texte
18
16
14
12
10
8
6
4
2
0
A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V
W
X
Y
Z

Texte 02

HELEX VELLER, "STQRY QT MY LATE".
=> "HELEN KELLER STORY OF MY LIFE"

L => L
X => N
V => K
S => S
Q => O
Y => Y
T => F
M => M
A => I

Ce qu'on a

- A => I
- B =>
- C => H
- D => E
- E =>
- F => A
- G => C
- H => P
- I => R
- J =>
- K =>
- L => L
- M => M

(Pas de logique spécifique comme pour le texte précédent)

- N =>
- O =>
- P => T
- Q => O
- R =>
- S => S
- T => F
- U =>
- V => K
- W =>
- X => N
- Y => Y
- Z =>

Texte 02

"CHAPTER 4" THE MOST IMPORTANT RAY I REMEMOER IN ALL MY LIFE IS THE ONE ON ZHICH MY TEACHER, ANNE MANSFIELR SULLIBAN, CAME TO ME.

R => D
Z => W
U => U
B => V

Ce qu'on a

(Pas de logique spécifique comme pour le texte précédent)

- A => I
- B => V
- C => H
- D => E
- E =>
- F => A
- G => C
- H => P
- I => R
- J =>
- K =>
- L => L
- M => M

- N =>
- O =>
- P => T
- Q => O
- R => D
- S => S
- T => F
- U => U
- V => K
- W =>
- X => N
- Y => Y
- Z => W

Après quelques devinettes de ce genre…

- A => I
- B => V
- C => H
- D => E
- E => J
- F => A
- G => C
- H => P
- I => R
- J => G
- K => Z
- L => L
- M => M

- N => X
- O => B
- P => T
- Q => O
- R => D
- S => S
- T => F
- U => U
- V => K
- W => Q
- X => N
- Y => Y
- Z => W

Décryptage

- "Chapter 4" The most important day I remember in all my life is the one on which my teacher, Anne Mansfield Sullivan, came to me. I am filled with wonder when I consider the immeasurable contrasts between the two lives which it connects. It was the third of March, 1887, three months before I was seven years old. On the afternoon of that eventful day, I stood on the porch, dumb, expectant. I guessed vaguely from my mother's signs and from the hurrying to and fro in the house that something unusual was about to happen, so I went to the door and waited on the steps. The afternoon sun penetrated the mass of honeysuckle that covered the porch, and fell on my upturned face. My fingers lingered almost unconsciously on the familiar leaves and blossoms which had just come forth to greet the sweet southern spring. I did not know what the future held of marvel or surprise for me. Anger and bitterness had preyed upon me continually for weeks and a deep languor had succeeded this passionate struggle. Have you ever been at sea in a dense fog, when it seemed as if a tangible white darkness shut you in, and the great ship, tense and anxious, groped her way toward the shore with plummet and sounding-line, and you waited with beating heart for something to happen? I was like that ship before my education began, only I was without compass or sounding-line, and had no way of knowing how near the harbour was. "Light! give me light!" was the wordless cry of my soul, and the light of love shone on me in that very hour. I felt approaching footsteps. I stretched out my hand as I supposed to my mother. Some one took it, and I was caught up and held close in the arms of her who had come to reveal all things to me, and, more than all things else, to love me. The morning after my teacher came she led me into her room and gave me a doll. The little blind children at the Perkins Institution had sent it and Laura Bridgman had dressed it; but I did not know this until afterward. When I had played with it a little while, Miss Sullivan slowly spelled into my hand the word "d-o-l-l." I was at once interested in this finger play and tried to imitate it. When I finally succeeded in making the letters correctly I was flushed with childish pleasure and pride. Running downstairs to my mother I held up my hand and made the letters for doll. I did not know that I was spelling a word or even that words existed; I was simply making my fingers go in monkey-like imitation. In the days that followed I learned to spell in this uncomprehending way a great many words, among them _pin, hat, cup_ and a few verbs like _sit, stand_ and _walk._ But my teacher had been with me several weeks before I understood that everything has a name. One day, while I was playing with my new doll, Miss Sullivan put my big rag doll into my lap also, spelled "d-o-l-l" and tried to make me understand that "d-o-l-l" applied to both. Earlier in the day we had had a tussle over the words "m-u-g" and "w-a-t-e-r." Miss Sullivan had tried to impress it upon me that "m-u-g" is _mug_ and that "w-a-t-e-r" is _water_, but I persisted in confounding the two. In despair she had dropped the subject for the time, only to renew it at the first opportunity. I became impatient at her repeated attempts and, seizing the new doll, I dashed it upon the floor. I was keenly delighted when I felt the fragments of the broken doll at my feet. Neither sorrow nor regret followed my passionate outburst. I had not loved the doll. In the still, dark world in which I lived there was no strong sentiment of tenderness. I felt my teacher sweep the fragments to one side of the hearth, and I had a sense of satisfaction that the cause of my discomfort was removed. She brought me my hat, and I knew I was going out into the warm sunshine. This thought, if a wordless sensation may be called a thought, made me hop and skip with pleasure. We walked down the path to the well-house, attracted by the fragrance of the honeysuckle with which it was covered. Some one was drawing water and my teacher placed my hand under the spout. As the cool stream gushed over one hand she spelled into the other the word water, first slowly, then rapidly. I stood still, my whole attention fixed upon the motions of her fingers. Suddenly I felt a misty consciousness as of something forgotten–a thrill of returning thought; and somehow the mystery of language was revealed to me. I knew then that "w-a-t-e-r" meant the wonderful cool something that was flowing over my hand. That living word awakened my soul, gave it light, hope, joy, set it free! There were barriers still, it is true, but barriers that could in time be swept away. I left the well-house eager to learn. Everything had a name, and each name gave birth to a new thought. As we returned to the house every object which I touched seemed to quiver with life. That was because I saw everything with the strange, new sight that had come to me. On entering the door I remembered the doll I had broken. I felt my way to the hearth and picked up the pieces. I tried vainly to put them together. Then my eyes filled with tears; for I realized what I had done, and for the first time I felt repentance and sorrow. I learned a great many new words that day. I do not remember what they all were; but I do know that _mother, father, sister, teacher_ were among them–words that were to make the world blossom for me, "like Aaron's rod, with flowers." It would have been difficult to find a happier child than I was as I lay in my crib at the close of the eventful day and lived over the joys it had brought me, and for the first time longed for a new day to come. HELEN KELLER STORY OF MY LIFE

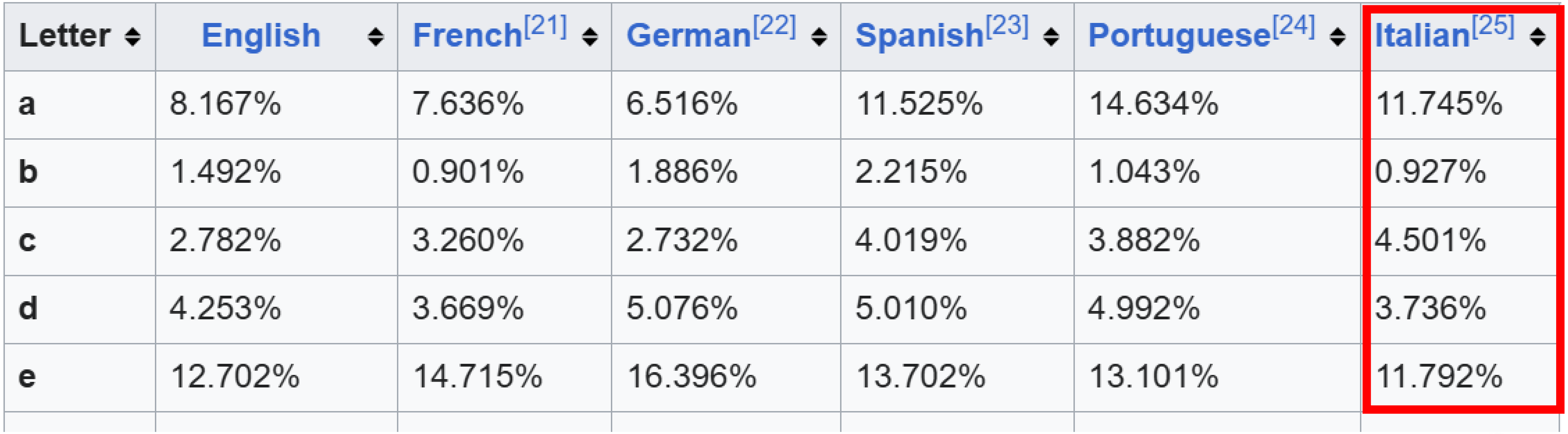
Texte 03

- "Shje e njcgye". Sc nulgmc jte nerhe `e nucuc mvoevucuc ic hv wcqwmvl im jmvkhe cvvm e qeppl, jlv s’mvuegoevul im uge nhlm jlqycrvm, vessc njhlsc qcuegvc Imcvc im Gerrml Eqmsmc. Ms "wmvlqml fcvucnumjl" ic jhm `e vcuc- "shje" e "njcgye"- egc nucul nhrregmul icssc qcenugc (ms rmlgvl ilyl jte im khenuc uejvmjc coeocql ycgscul cs vlnugl jlgnl). Qc ejjl khc, nevp’csugc ygefcpmlve: "J’egc hvc olsuc hv wmqwl jte nm qeuueoc neqyge se njcgye ies nhl ycy`a. Hvc negc ms ycy`a nm egc nuhfcul jte ms wmqwl rsm ygevieoc se njcgye, csslgc sl qeuue cuucjjcul cssc shje, e ylm c qeppcvluue jcie, csslgc imje ms ycy`a:- Jlnc j’`e, hv scigl? Oc c oeiege e j’egc ms wmqwl yeg ueggc. Ms wmqwl egc gmqcnul uhuul cjjenl. Csslgc ms ycy`a tc yglocul c rmgcgrsm sc uenuc qc vlv nm `e nyevul, tc yglocul c umgcgrsm se lgejjtme qc vlv nm nyerveoc, tc yglocul c njtmcjjmcgrsm ms vcnl qc vlv nm nyerveoc, tc yglocul c umgcgrsm m jcyessm qc vlv nm nyerveoc, tc yglocul c njtmcjjmcgrsm s’lqwesmjl qc vlv nm nyerveoc, tc yglocul c umgcgrsm omc se njcgye e j’`e gmhnjmul, nm `e nyevul." Sc uglocuc fmvcse- jte vlv egc nucuc nhrregmuc ics vcggculge ygmvjmycse, qc ic hv csugl ymjjlsmvl- `e nucuc ucvul rhnucuc icrsm nuennm wcqwmvm jte ennm tcvvl nevumul ms wmnlrvl im cyyschimgnm: egc mv effeuum s’mqqcrmve jte jtmhieoc yegfeuucqevue e slrmjcqevue ms jegjtml e icoc cssc nulgmc hv nevnl im jlqymhueppc; qc egc flgne qlsul im ym`u. Yevnl jte ms iluulg Fgehi mv yegnlvc ygloegewwe, cvjte ic fcvucnqc, hv’mvuevnc eqlpmlve cnjlsucvil hv gcjjlvul jln` ı fcjmsqevue mvuegygeucwmse mv uegqmvm im "jlqysennl eimymjl": fmv icss’cuucjjl... jlv khes wcqwmvl jte nm qeuue se njcgye ies ycige... jte ohlse mvnlqqc "fcg se njcgye cs ycige", yeg ygeviege ms nhl ylnul cjjcvul cssc qcige. Mqycgm sluuc, neqmvcuc im mqqcrmvm im qlgue. "Cuucjjcge" ohls imge cvjte "cyymjjcge", "mqymjjcge"... E ms wmqwl egc "yeg ueggc" l "vessc ueggc"? Vlv jm ilogewwegl ennege ihwwm mv yglylnmul, ne nm serre rmhnucqevue khes "nm `e nyevul" jte i`a cs igcqqc hvc jlvjshnmlve ugcrmjc. "Nyervegnm" e "qlgmge" nlvl nmvlvmqm: "nm `e nyevul ves wcjml ies Nmrvlge", imjlvl m vejglslrm nhm qhgm. Omvje ms ym`u flgue e qcuhgl. Omvje c qeppcvluue, s’lgc iersm nymgmum... E ygmqc iessc qlgue, sc ulguhgc: uhuul khes "rmgcge sc uenuc", "umgcge se lgejjtme", "njtmcjjmcge ms vcnl"... Vlv mvnmnueg`o mv khenul enegjmpml vlv chulgmppcul im ynmjcvcsmnm. Ycgsmvl m uejvmjm: "omiecvu jlvnhsen"... Ne ms yglflvil nm `e mqyciglvmul ies "wmvlqml fcvucnumjl" yeg mvnjevcge m nhlm igcqqm, ms yhvul encuul ies nhl mvnegmqevul qm neqwgc uhuucomc s’ejl mqqeimcuc jte sc ycglsc "njcgye" tc yluhul ienucge vess’enyegmevpc mvfcvumse. Uhuum m wcqwmvm rmljcvl c qeuuegnm se njcgye ies ycige e iessc qcige. Yeg ennege "slgl". Yeg ennege ym`u csum. Qc cvjte, ym`u neqysmjeqevue, yeg ennege "csugm". Ms rmljl ies ugcoenumqevul, c ycgue sc nhc mqylgucvpc nmqwlsmjc, `e neqyge imoeguevue yeg rsm effeuum rgluuenjtm jte ve vcnjlvl. E’ uecugl: qeuuegnm vem ycvvm iersm csugm, qeuuegnm mv hvc ycgue, mvoevucgnm hvc omuc, njlygmge vhlom renum. Yejjcul jte, im gerlsc, nmc yegqennl cm wcqwmvm nlsl im jcgveocse qcnjtegcgnm, mvilnncge sc rmcjjc ies ycige, hvc nluucvc iessc vlvvc. Jm ilogewwe neqyge ennege, mv jcnc, hv jenulve im cwmum nqennm c imnylnmpmlve ies rmljl ies ugcoenumqevul. Vesse njhlse yeg s’mvfcvpmc im Gerrml Eqmsmc vlv j’`e nlsl hv jenulve, yeg khenul, qc hv mvuegl rhcgicglwc. C Glqc, cs qegjcul im omc Ncvvml, nm oevilvl lrvm nlguc im jlnuhqm, cwmum ic negc, genmihcum iessc qlic: `e s`ı jte cvicocql, khcvil vlnugc fmrsmc egc ymjjlsc, c gmflgvmge ms jenulve nhiieuul. Csse nhe cqmjte ymcjeoc sc vlnugc jcnc yglygml yeg omc ies jenulve. Yegjt´e ms wcqwmvl gmqcve "cjjenl"? Sc gcrmlve ym`u loomc ncgewwe ic gmjegjcge vess’cvcslrmc: "cuucjjcul" cs scqycicgml, jlqe hvc scqycimvc, ms wcqwmvl nm jlqylguc ic scqycimvc. Qc khenuc nymercpmlve ncgewwe nhffmjmevue ne ms wcqwmvl nm flnne "cjjenl" ves qlqevul mv jhm ms ycige sl tc "cuucjjcul". Ms gcjjlvul yeg`o, c khes ygejmnl yhvul, vlv germnugc s’cjjevnmlve. Vlm oeimcql ms wcqwmvl "cjjenl" nlsl ilyl jte ` e jcihul yeg ueggc. Yevnl jte ne s’mqqcrmvcpmlve tc cohul wmnlrvl im hv jegul ueqyl (yljtm cuumqm) yeg njlygmge khess’cvcslrmc khenul `e cjjcihul yegjt´e s’cvcslrmc vlv nm `e gmoescuc mqqeimcucqevue, yeg omc im "omnmlve"- ms vcggculge "oeie" ms wcqwmvl "cuucjjcul", sl oeie "cjjenl"- qc `e njcuhgmuc nhss’cnne iessc "nesepmlve oegwcse". J’`e nucul, vessc qevue ies wcqwmvl- qevuge sc nulgmc jlvumvhcoc- hv scolgml "c ycgue", mqyervcul nhrsm ejtm iessc ycglsc "cuucjjcul". Ejjl sc jcuevc: "cuucjjcul", "cyyenl", "cjjenl". S’cvcslrmc oegwcse e sc gmqc vlv yglvhvjmcuc tcvvl fcuul njcuucge cvjte s’cvcslrmc iess’mqqcrmve omnmoc. J’`e nucul, mvnlqqc, khes scolgl im "jlvievncpmlve iesse mqqcrmvm" jte ms iluulg Fgehi- neqyge shm, khes weveieuul omevvene- tc jln`ı wev ienjgmuul nuhimcvil m ygljennm jgecumom ies nlrvl. Ic khenul yhvul im omnuc sc nulgmc jm cyycge mv effeuum jlqe hv "nlrvl c ljjtm cyegum". Ve tc uhuuc s’cuqlnfegc, sc imnylnmpmlve css’cnnhgil, s’cjjcocsscgnm iem ueqm. Ic khenuc cuqlnfegc nm enje jlv m uevucumom ies ycige im "nyervege" ms "wcqwmvl-scqycimvc". Se ocgmcpmlvm nhs ueqc nlvl mqylnue icss’cvcslrmc, qc nm qhlolvl nh imoegnm ymcvm: om mvuegoevrlvl, mvfcuum, nmc s’enyegmevpc iem renum vejenncgm yeg nyervege hvc scqycimvc (nomucge sc scqycimvc nuennc, njtmcjjmcge hv yhsncvue, umgcge hv jlgilvjmvl, ejjeuegc), nmc s’enyegmevpc ies yglygml jlgyl (`e yeg khenuc nugcic jte icssc uenuc nm ycnnc csse lgejjtme, cs vcnl, css’lqwesmjl, ejjeuegc). Ms rmljl, c khenul yhvul `e jlsseuumol. Ms vcggculge ygmvjmycse `e nucul nlsl ms ieulvculge im hv’enyslnmlve jte tc jlmvolsul uhuum, jlv hv effeuul jte m jmwegveumjm jtmcqegewwegl im "cqysmfmjcpmlve". Qevuge jegjcvl se ocgmcpmlvm m wcqwmvm nm rhcgicvl, jegjcvl ves jlgyl ies omjmvl sl nyhvul yeg hvc vhloc uglocuc: ms ygenevue mvuegomeve vessc nulgmc, se nhe fmrhge se nhrregmnjlvl vhlom nmrvmfmjcum, mv hv ygljennl jte tc khcsjte cvcslrmc jlv sc jcycjmu`a iessc gmqc im ieuucge cs yleuc, qevuge scolgc, nmrvmfmjcum, yeg jln`ı imge, ics im fhlgm iessc nmuhcpmlve smgmjc. M renum esevjcum nlvl cvjt’ennm mv gmqc, nmc yhge vlv nejlvil ms nhlvl. E nlvl "gmqe wcjmcue", jml`e se ym`u neqysmjm, jlq’`e rmhnul jte nmc mv hvc fmscnugljjc mvfcvumse. Sc ocgmcpmlve jlvjshnmoc- "rsm seoc se njcgye, e nm nyerve" gcyygenevuc hv’cvjlg ym`u iejmnc gluuhgc jls nlrvl. E’ hvc jlvjshnmlve slrmjc. Egcvl se njcgye ies ycige c ueveg "cjjenl" ms wcqwmvl, yegjt´e uhuul egc jlqmvjmcul im s`ı, ic khesse njcgye: wcnuc ulrsmegrsm se njcgye, e sc shje njlqycgmg`a, sc nulgmc yh`o jtmhiegnm. E’ nucul hv eqwgmlvcse yevnmegl slrmjl c qcvlogcge sl nughqevul qcrmjl- "se njcgye ies ycy`a"- ves nevnl lyylnul cs qlomqevul mvmpmcse. Ves qlqevul mv jhm fcvvl khenuc njlyeguc m wcqwmvm mvuglihjlvl ves smwegl rmljl iess’mqqcrmvcpmlve s’eseqevul qcueqcumjl iessc "geoegnmwmsmu`a", jlqe qeucflgc, vlv cvjlgc jlqe jlvjeuul. Cs jlvjeuul jm cggmoegcvvl ym`u ucgim: qc mvucvul, flgne, s’mqqcrmve fcolslnc tc jgecul se wcnm yeg sc nughuuhgcpmlve ies jlvjeuul. Hv’hsumqc lnnegocpmlve (hsumqc nlsl yeg jcnl, nm jcymnje) gmrhcgic s’mvnegmqevul vessc nulgmc iem "ocslgm". Seuuc ic khenul yhvul im omnuc, `e hvc nulgmc im imnlwweimevpc yhvmuc, ves khcigl im hv qliessl jhsuhgcse fmv uglyyl ugcimpmlvcse. Ms ycige `e jlshm cs khcse nm lwweimnje e jte tc ms imgmuul im jcnumrcge. Sc jevnhgc `e mvuegoevhuc c qcvuevege sc nulgmc vem jlvfmvm iessc qlgcse fcqmsmcge. Jls nhl mvuegoevul icooegl nm yh`o imge jte cssc nulgmc "tcv ylnul qcvl e jmesl e ueggc": s’mvjlvnjml jlv m nhlm jlvfsmuum, s’enyegmevpc, sc qeqlgmc, s’mielslrmc, sc ycglsc mv uhuue se nhe fhvpmlvm. Hvc seuuhgc yhgcqevue ynmjlslrmjc, l ynmjcvcsmumjc, vlv ncgewwe wcnucuc c msshqmvcgve uhuue se gmnhsucvpe jlqe tl jegjcul, nmc yhg wgeoeqevue, im fcge.- Rmcvvm glicgm, "Rgcqqcumjc iess’mqqcrmvcpmlve".

Texte 03

E	744×	12.04%
C	742×	12.01%

744 ≃ **742**



Letter	English	French[21]	German[22]	Spanish[23]	Portuguese[24]	Italian[25]
a	8.167%	7.636%	6.516%	11.525%	14.634%	11.745%
b	1.492%	0.901%	1.886%	2.215%	1.043%	0.927%
c	2.782%	3.260%	2.732%	4.019%	3.882%	4.501%
d	4.253%	3.669%	5.076%	5.010%	4.992%	3.736%
e	12.702%	14.715%	16.396%	13.702%	13.101%	11.792%

Texte 03

- E = A/E
- C = A/E

- E=> E
- C=>A

Texte 03

- E = A/E
- C = A/E

- E=> E
- C=>A

Texte 03

- Rmcvvm glicgm, "Rgcqqcumjc iess’mqqcrmvcpmlve".
- => Rmavvm gliagm, "Rgaqqcumja iess’mqqcrmvcpmlve".
- Rmavvm => Gianni
- R => G
- M => I
- V => N
- => Gianni gliagi, "Ggaqqcuija iess’iqqcrmncpmlne".
- => Gianni Rodari, "Grammatica dell’immaginazione".

Ce qu'on a

- A =>
- B =>
- C => A
- D =>
- E => E
- F =>
- G => R
- H =>
- I => D
- J => C
- K =>
- L => O
- M => I
- N =>
- O =>
- P => Z
- Q => M
- R => G
- S => L
- T =>
- U =>
- V => N
- W =>
- X =>
- Y =>
- Z =>

Texte 03

- "Shje e njcgye"
- "LUCE E NCARYE" (avec la clef)

- => "Luce e scarpe"

- N => S
- Y => P

Texte 03

- WREOEMENUE
- = > BREVEMENTE

- W => B
- O => V
- U => T

Ce qu'on a (c'était suffisant)

- A =>
- B =>
- C => A
- D =>
- E => E
- F =>
- G => R
- H =>
- I => D
- J => C
- K =>
- L => O
- M => I

- N => S
- O => V
- P => Z
- Q => M
- R => G
- S => L
- T =>
- U => T
- V => N
- W => B
- X =>
- Y => P
- Z =>

Texte 03

"Luce e scarpe". La storia che segue `e stata inventata da un bambino di cinque anni e mezzo, con l’intervento di tre suoi compagni, nella scuola materna Diana di Reggio Emilia. Il "binomio fantastico" da cui `e nata- "luce" e "scarpe"- era stato suggerito dalla maestra (il giorno dopo che di questa tecnica avevamo parlato al nostro corso). Ma ecco qua, senz’altra prefazione: "C’era una volta un bimbo che si metteva sempre le scarpe del suo pap`k. Una sera il pap`k si era stufato che il bimbo gli prendeva le scarpe, allora lo mette attaccato alla luce, e poi a mezzanotte cade, allora dice il pap`k:- Cosa c’`e, un ladro? Va a vedere e c’era il bimbo per terra. Il bimbo era rimasto tutto acceso. Allora il pap`k ha provato a girargli la testa ma non si `e spento, ha provato a tirargli le orecchie ma non si spegneva, ha provato a schiacciargli il naso ma non si spegneva, ha provato a tirargli i capelli ma non si spegneva, ha provato a schiacciargli l’ombelico ma non si spegneva, ha provato a tirargli via le scarpe e c’`e riuscito, si `e spento." La trovata finale- che non era stata suggerita dal narratore principale, ma da un altro piccolino- `e stata tanto gustata dagli stessi bambini che essi hanno sentito il bisogno di applaudirsi: era in effetti l’immagine che chiudeva perfettamente e logicamente il cerchio e dava alla storia un senso di compiutezza; ma era forse molto di pi`t. Penso che il dottor Freud in persona proverebbe, anche da fantasma, un’intensa emozione ascoltando un racconto cos` ı facilmente interpretabile in termini di "complesso edipico": fin dall’attacco... con quel bambino che si mette le scarpe del padre... che vuole insomma "far le scarpe al padre", per prendere il suo posto accanto alla madre. Impari lotta, seminata di immagini di morte. "Attaccare" vuol dire anche "appiccare", "impiccare"... E il bimbo era "per terra" o "nella terra"? Non ci dovrebbero essere dubbi in proposito, se si legge giustamente quel "si `e spento" che d`k al dramma una conclusione tragica. "Spegnersi" e "morire" sono sinonimi: "si `e spento nel bacio del Signore", dicono i necrologi sui muri. Vince il pi`t forte e maturo. Vince a mezzanotte, l’ora degli spiriti... E prima della morte, la tortura: tutto quel "girare la testa", "tirare le orecchie", "schiacciare il naso"... Non insister`v in questo esercizio non autorizzato di psicanalisi. Parlino i tecnici: "videant consules"... Se il profondo si `e impadronito del "binomio fantastico" per inscenare i suoi drammi, il punto esatto del suo inserimento mi sembra tuttavia l’eco immediata che la parola "scarpe" ha potuto destare nell’esperienza infantile. Tutti i bambini giocano a mettersi le scarpe del padre e della madre. Per essere "loro". Per essere pi`t alti. Ma anche, pi`t semplicemente, per essere "altri". Il gioco del travestimento, a parte la sua importanza simbolica, `e sempre divertente per gli effetti grotteschi che ne nascono. E’ teatro: mettersi nei panni degli altri, mettersi in una parte, inventarsi una vita, scoprire nuovi gesti. Peccato che, di regola, sia permesso ai bambini solo di carnevale mascherarsi, indossare la giacca del padre, una sottana della nonna. Ci dovrebbe sempre essere, in casa, un cestone di abiti smessi a disposizione del gioco del travestimento. Nelle scuole per l’infanzia di Reggio Emilia non c’`e solo un cestone, per questo, ma un intero guardaroba. A Roma, al mercato di via Sannio, si vendono ogni sorta di costumi, abiti da sera, residuati della moda: `e l`ı che andavamo, quando nostra figlia era piccola, a rifornire il cestone suddetto. Alle sue amiche piaceva la nostra casa proprio per via del cestone. Perch´e il bambino rimane "acceso"? La ragione pi`t ovvia sarebbe da ricercare nell’analogia: "attaccato" al lampadario, come una lampadina, il bambino si comporta da lampadina. Ma questa spiegazione sarebbe sufficiente se il bambino si fosse "acceso" nel momento in cui il padre lo ha "attaccato". Il racconto per`v, a quel preciso punto, non registra l’accensione. Noi vediamo il bambino "acceso" solo dopo che ` e caduto per terra. Penso che se l’immaginazione ha avuto bisogno di un certo tempo (pochi attimi) per scoprire quell’analogia questo `e accaduto perch´e l’analogia non si `e rivelata immediatamente, per via di "visione"- il narratore "vede" il bambino "attaccato", lo vede "acceso"- ma `e scaturita sull’asse della "selezione verbale". C’`e stato, nella mente del bambino- mentre la storia continuava- un lavorio "a parte", impegnato sugli echi della parola "attaccato". Ecco la catena: "attaccato", "appeso", "acceso". L’analogia verbale e la rima non pronunciata hanno fatto scattare anche l’analogia dell’immagine visiva. C’`e stato, insomma, quel lavoro di "condensazione delle immagini" che il dottor Freud- sempre lui, quel benedetto viennese- ha cos`ı ben descritto studiando i processi creativi del sogno. Da questo punto di vista la storia ci appare in effetti come un "sogno a occhi aperti". Ne ha tutta l’atmosfera, la disposizione all’assurdo, l’accavallarsi dei temi. Da questa atmosfera si esce con i tentativi del padre di "spegnere" il "bambino-lampadina". Le variazioni sul tema sono imposte dall’analogia, ma si muovono su diversi piani: vi intervengono, infatti, sia l’esperienza dei gesti necessari per spegnere una lampadina (svitare la lampadina stessa, schiacciare un pulsante, tirare un cordoncino, eccetera), sia l’esperienza del proprio corpo (`e per questa strada che dalla testa si passa alle orecchie, al naso, all’ombelico, eccetera). Il gioco, a questo punto `e collettivo. Il narratore principale `e stato solo il detonatore di un’esplosione che ha coinvolto tutti, con un effetto che i cibernetici chiamerebbero di "amplificazione". Mentre cercano le variazioni i bambini si guardano, cercano nel corpo del vicino lo spunto per una nuova trovata: il presente interviene nella storia, le sue figure le suggeriscono nuovi significati, in un processo che ha qualche analogia con la capacit`k della rima di dettare al poeta, mentre lavora, significati, per cos`ı dire, dal di fuori della situazione lirica. I gesti elencati sono anch’essi in rima, sia pure non secondo il suono. E sono "rime baciate", cio`e le pi`t semplici, com’`e giusto che sia in una filastrocca infantile. La variazione conclusiva- "gli leva le scarpe, e si spegne" rappresenta un’ancor pi`t decisa rottura col sogno. E’ una conclusione logica. Erano le scarpe del padre a tener "acceso" il bambino, perch´e tutto era cominciato di l`ı, da quelle scarpe: basta togliergli le scarpe, e la luce scomparir`k, la storia pu`v chiudersi. E’ stato un embrionale pensiero logico a manovrare lo strumento magico- "le scarpe del pap`k"- nel senso opposto al movimento iniziale. Nel momento in cui fanno questa scoperta i bambini introducono nel libero gioco dell’immaginazione l’elemento matematico della "reversibilit`k", come metafora, non ancora come concetto. Al concetto ci arriveranno pi`t tardi: ma intanto, forse, l’immagine favolosa ha creato le basi per la strutturazione del concetto. Un’ultima osservazione (ultima solo per caso, si capisce) riguarda l’inserimento nella storia dei "valori". Letta da questo punto di vista, `e una storia di disobbedienza punita, nel quadro di un modello culturale fin troppo tradizionale. Il padre `e colui al quale si obbedisce e che ha il diritto di castigare. La censura `e intervenuta a mantenere la storia nei confini della morale familiare. Col suo intervento davvero si pu`v dire che alla storia "han posto mano e cielo e terra": l’inconscio con i suoi conflitti, l’esperienza, la memoria, l’ideologia, la parola in tutte le sue funzioni. Una lettura puramente psicologica, o psicanalitica, non sarebbe bastata a illuminarne tutte le risultanze come ho cercato, sia pur brevemente, di fare.- Gianni rodari, "Grammatica dell’immaginazione".

Partie II
'Invention' de méthodes de chiffrement

Méthode n1

Associer les lettres à leur index dans l'alphabet puis chiffrer le nombre forme par cette combinaison

1. Associer les lettres à leur index dans l'alphabet

A -> 01
B -> 02
C -> 03
...
Z -> 26

Exemple :

"*Hello world*"

-> 08 05 12 12 15 23 15 18 12 04

(la fréquence des lettres est reconnaissable)

2. Regrouper les lettres de notre message en un nombre

Exemple :

"*08 05 12 12 15 23 15 18 12 04*" devient "*08051212152315181204*"

3. Appliquer une fonction mathématique a ce nombre

Exemple :

Avec la fonction *f(x) = 2x*

08051212152315181204

↓

16102424304630362408

Avantage: Les fréquences des lettres sont indiscernables

Inconvénients:

- Si le nombre d'origine commence par un *0*, il faut en prendre compte au moment du déchiffrage
- Le nombre est plus long que le message chiffré

4. Raccourcir le message en changeant son système de numération / base

Exemple :

Si on convertit *16102424304630362408* en base 32,
on obtient "*DUTQDISU1NS98*"

Avantages:

- Le message chiffré est presque aussi long que le message d'origine
- Les fréquences des lettres sont indiscernables

Inconvénients:

- Si le nombre d'origine commence par un *0*, il faut en prendre compte au moment du déchiffrage
- Il faut prendre en compte cette étape dans la clef

Rappel : Les bases *(systèmes de numération)*

Base 10 (base de tous les jours): 0,1,2,3,4,5,6,7,8,9,10

Base 2 (binaire): 0,1,10,11,100,101,110,111 …

Base 16 (hexadécimal): 0,1,2,…,9,A,B,C,D,E,F, 10

Méthode n°1 bis

Associer les lettres à leur index dans l'alphabet puis chiffrer cet 'alphabet' grâce à une fonction

1. Associer les lettres à leur index dans l'alphabet

A -> 01

B -> 02

C -> 03

...

Z -> 26

2. Chiffrer cet alphabet grâce a une fonction mathématique

Exemple avec f(x) = 3x :

A -> 03

B -> 06

C -> 09

...

Z -> 78

Problème!

Il n'existe pas de 78e lettre dans l'alphabet

Solution:

on prend ce nombre modulo 26 (78 -> 26%78= 26)

L'opérateur modulo (%) désigne le reste de la division euclidienne du 1e nombre par le 2e

2e Problème!

Si la fonction n'est pas bijective, alors certains nombres reviendront 2 fois et d'autres aucune.

Exemple avec f(x) = 2x :

A -> 02
B -> 04
C -> 06
...
M -> 26%26 = 00
N -> 28%26 = 02
...
Z -> 52%26 = 00

Solution:

si on remarque que le nombre est déjà associe à une autre lettre on incrémente ce nombre de 1("N" sera associe a 03)

Application avec "hello world" : *24 15 10 10 19 17 19 2 10 12*

On peut même réassigner ces nombres à leur équivalents dans l'alphabet : *XOJJS QSBJL*

Avantages:

- Si la fonction est bijective la clef du message est très courte

Inconvénients:

- La méthode de l'analyse de fréquence fonctionne
- La fonction doit être bijective pour ne pas compliquer le déchiffrement du message

Méthode n°2

Trouver des motifs répétitifs dans un texte pour faire une clef à partir de ceux-ci

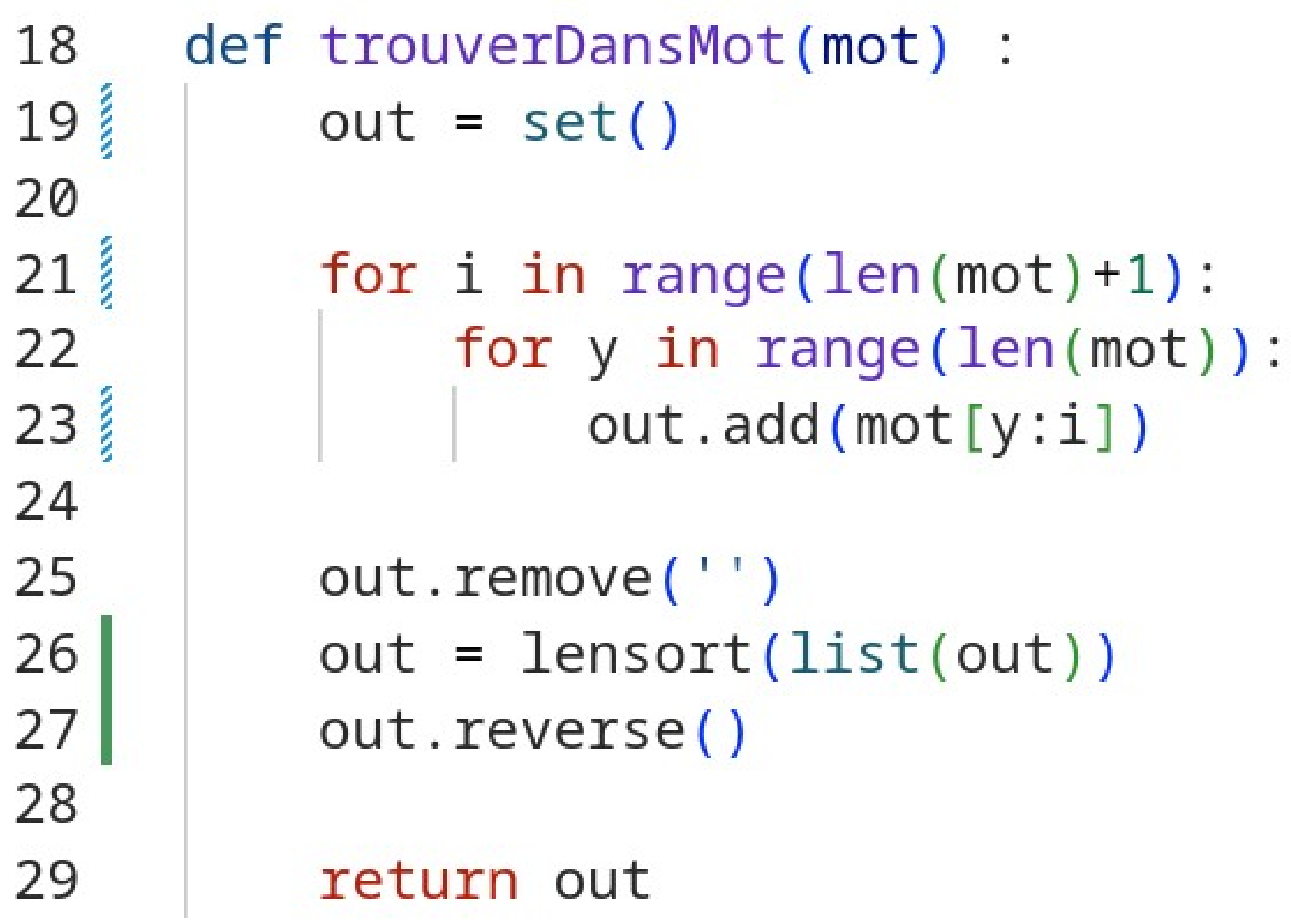
1. Repérer des motifs répétitifs dans un texte

Exemple : « escargot escalier lien »

Motif chiffré	Motif
#	esca
@	lie
$	got
%	e
^	n
*	r

Si on remplace :
« #*$ #@* @%^ ».

1.On trouve des motifs de lettres récurrents dans 1 mot



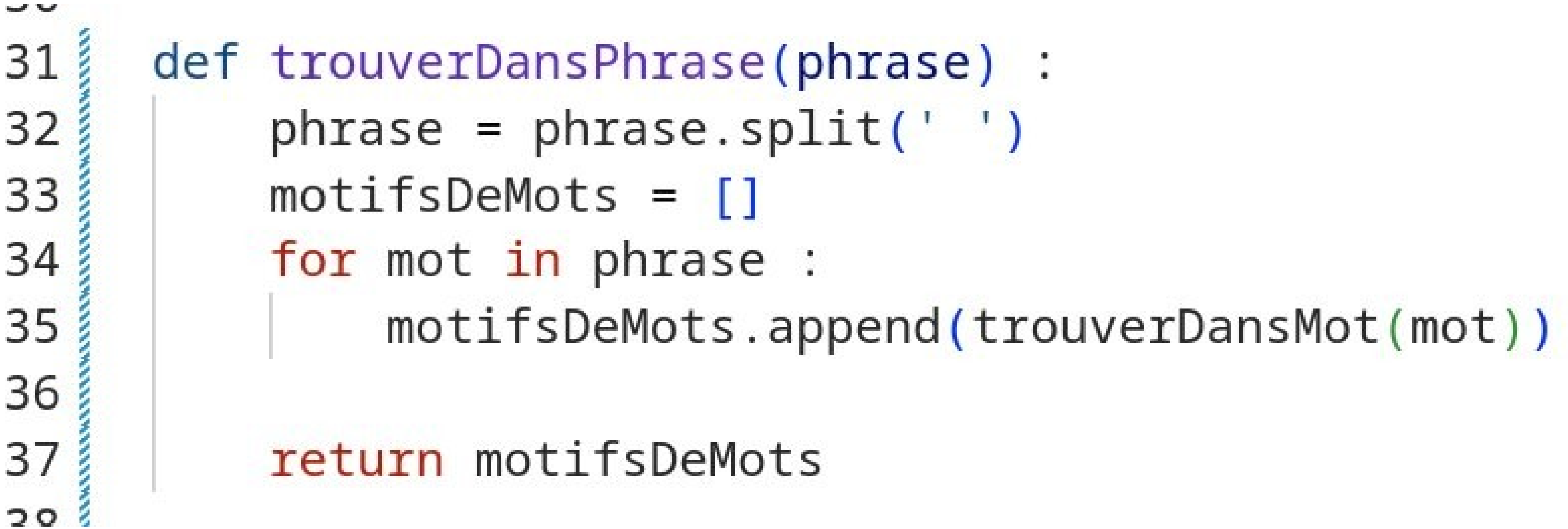
```python
def trouverDansMot(mot) :
    out = set()

    for i in range(len(mot)+1):
        for y in range(len(mot)):
            out.add(mot[y:i])

    out.remove('')
    out = lensort(list(out))
    out.reverse()

    return out
```

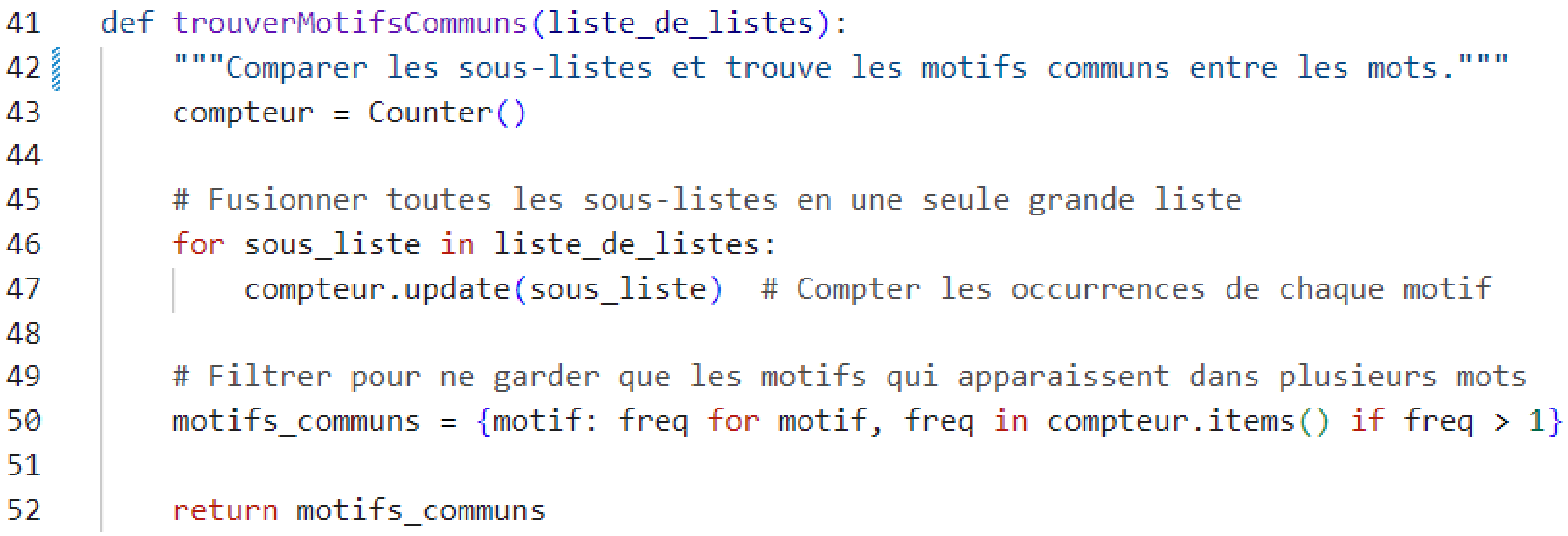
2.On applique cette méthode a l'ensemble de la phrase



```python
def trouverDansPhrase(phrase) :
    phrase = phrase.split(' ')
    motifsDeMots = []
    for mot in phrase :
        motifsDeMots.append(trouverDansMot(mot))

    return motifsDeMots
```

3. On cherche les motifs de mots qui se retrouvent dans plusieurs mots



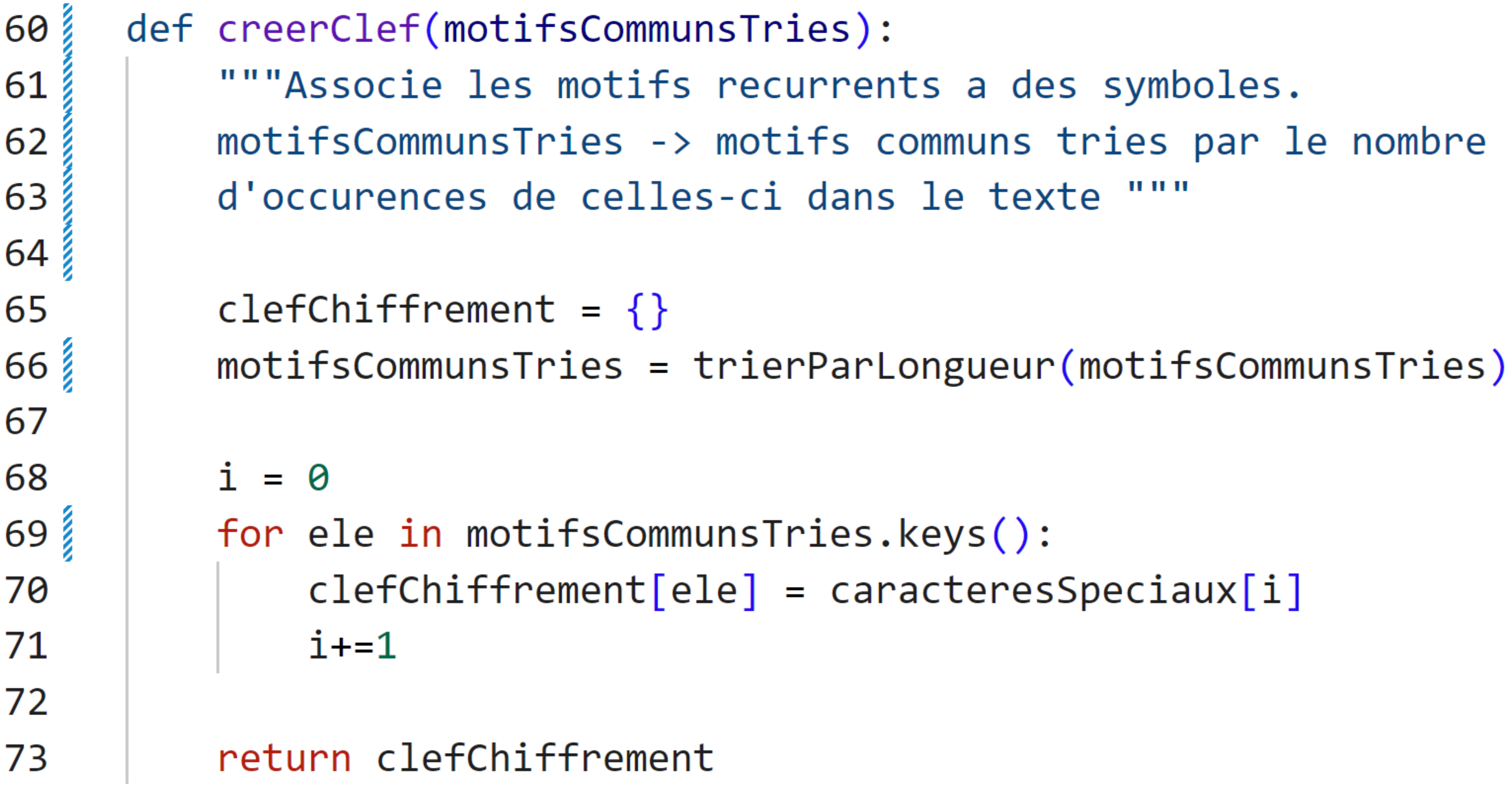
```python
def trouverMotifsCommuns(liste_de_listes):
    """Comparer les sous-listes et trouve les motifs communs entre les mots."""
    compteur = Counter()

    # Fusionner toutes les sous-listes en une seule grande liste
    for sous_liste in liste_de_listes:
        compteur.update(sous_liste)  # Compter les occurrences de chaque motif

    # Filtrer pour ne garder que les motifs qui apparaissent dans plusieurs mots
    motifs_communs = {motif: freq for motif, freq in compteur.items() if freq > 1}

    return motifs_communs
```

4. On crée la clef



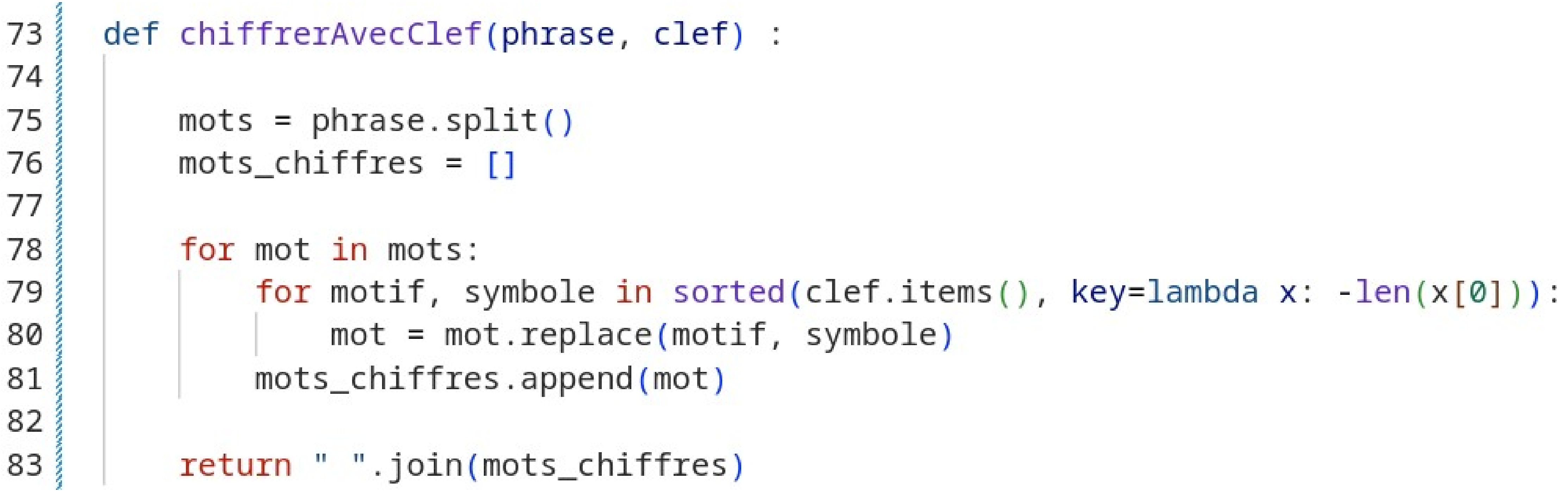
```python
def creerClef(motifsCommunsTries):
    """Associe les motifs recurrents a des symboles.
    motifsCommunsTries -> motifs communs tries par le nombre
    d'occurences de celles-ci dans le texte """

    clefChiffrement = {}
    motifsCommunsTries = trierParLongueur(motifsCommunsTries)

    i = 0
    for ele in motifsCommunsTries.keys():
        clefChiffrement[ele] = caracteresSpeciaux[i]
        i+=1

    return clefChiffrement
```

5. Remplacer les éléments de chaque mot de la phrase à partir de la clef



```python
def chiffrerAvecClef(phrase, clef) :

    mots = phrase.split()
    mots_chiffres = []

    for mot in mots:
        for motif, symbole in sorted(clef.items(), key=lambda x: -len(x[0])):
            mot = mot.replace(motif, symbole)
        mots_chiffres.append(mot)

    return " ".join(mots_chiffres)
```

Bilan :

Avantages:

- La méthode de l'analyse de fréquence ne fonctionne pas
- Fonctionne bien pour de longs textes

Inconvénients:

- Fonctionne moins bien pour des textes courts
- Clef très grande/longue (surtout pour un texte long)
- Clef difficile à transmettre

Bilan général:

	Methode n1	Methode n1 bis	Methode n2
Avantages	• Aussi long que le message d'origine • Les fréquences des lettres sont indiscernables	• Si la fonction est bijective la clef du message est très courte	• La méthode de l'analyse de fréquence ne fonctionne pas • Fonctionne bien pour de longs textes
Inconvenients	• Si le nombre d'origine commence par un 0, il faut en prendre compte au moment du déchiffrage • Il faut prendre en compte cette étape dans la clef	• La méthode de l'analyse de fréquence fonctionne • La fonction doit être bijective pour ne pas compliquer le déchiffrement du message	• Fonctionne moins bien pour des textes courts • Clef très grande/longue (surtout pour un texte long)

Merci de votre écoute.