Casser les codes

Info
Vous avez intercepté plusieurs échanges de messages. À vous de les déchiffrer !

Challenge 1 - Pour vous chauffer

À l'aide du texte clair saurez-vous déchiffrer le message codé ?

```
A.D. XII Kal. Mar.
MDLIII A.V.C.

Il se trame un complot. Je pense que nos prochains entretiens devraient
être protégés.

Marcus Tullius Cicero
```

```
D.G.YLLNdo.Dsu.
PGOLLLD.Y.F.

Mhvxlvg'dffrugdyhfyrxv.
Qrvglvfxwlrqvqhghyudlhqwsdvhwuhghfrxyhuwhvvlqrxvxwlolvrqvfhwwhphwkrgh.

FdlxvLxolxvFdhvdu
```

Challenge 2 - Un peu plus dur maintenant

```
Le 08 mars 1918,
A qui de droit,

Le chiffrement utilisé par la machine permet d'exploiter la structure des
messages.

Georges Jean Painvin

Post-Scriptum : Portez ce vieux whisky au juge blond qui fume.
```

```
XG XX GG FV AX FA GD XX GA FF XV FD FV AD XV GA DV FV AA GD GD GV FV DA
XV FG XV DV XV XA FV DV FG GD GA XD GV AG AX FV FD XD VX FA XG VD VA XD
XX FD GD FV XV FA GX VX FX GX FD VA GV GF GV GD GX FD VA GD AF XV FX FV
AF AA GA FG GG DD FG XD VA GV XD DV GX FV XF VG AD AV FF GX DA XG AX AG
AF GV VG DV VX XF AD GX XA VF VX XV FD DV VG AG XV VF DG DV VA XF GF DG
VG XG XF VG XD VX AA FD GF DD VV GG XG GV AV XF AX GX DA VG DV VX XV VG
XG VG DX XX VV XX GX AX AF DD XG DG XX GF DX VF AA XG DX VV VA AG XF VF
GA XF AX VD VD VV AA FV XA VG GD FX XX GX GV DA VA AV FA XX AA FV XA DV
AG AA VA FV AX XV GG AA XA AV FV GV AX XD AA FD GX AX GD VV GD GX DV GA
XV FD AA FD FF XG VV GG FA GG VX
```

Challenge 3 - YAE! Yet Another Encoding

La source de message ne se tarit pas... décodez le message 3 !

Aide

Le passage à la ligne `'\n'` forme un caractère.

```
1 Lees8 mept ebr8919 A,
 iqud detiroC
'
ater sinfichmefrstendo meneross b ntséasru sse dce tqihn sueicanenenocs
emm sle NSPrupobu StistoiutePn turmoiateNn rotw .kssiMase dce tqihn suepmsi
slevupe tenneamà erno curst eir sdeogalhtri smepmcoexle
 s.ao
JaDn neem t ecnVi tenmjRi
.enso
PcSt-tpri: umro P ztev cexuieih w yskj au eugnobluqd ufi .me
```

Passe moi le mot !

Info
Votre mission : rassemblez un maximum d'indice pour casses les codes.

Challenge 4 - 3 mots de passe à découvrir

Le hash est une fonction qui associe . Deux textes identiques ont le même hash. Cette valeur n'a plus à rien avoir avec le texte lui-même, et ne permet pas de refaire l'opération en sens inverse.

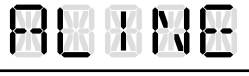
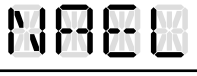
Vous avez obtenu une liste d'utilisateurs avec le hash de leurs mots de passe.

Grâce aux indices, trouvez les trois éléments utilisées en cryptographie !

Nom	Indice	Hash
Aymeric	suite	307
Cathaline	malade	139
César	trousse	941
Corentin	intinct	593
Denis	pressentiment	593
Élisabeth	arroser	47
Éloi	terrible	811
Emy	argent	863
Frédéric	tente	811
Gaspard	s'assoir	281
Ghislain	col	787
Gladys	savon	677
Lana	gens	271
Leila	calcul	739
Lili	craie	11
Lucile	rang	479
Margot	science	739
Paul	nombres	739
Perceval	usine	307
Quitterie	laisse	719
Romain	présent	257
Sarah	amusant	673
Siméon	avenir	257
Stanislas	passé	257
Vincent	désordre	173
Yannick	connaissance	593

Challenge 5 - fonction de hashage

Trouvez la fonction de hachage.

login	H(login)	login	H(login)	login	H(login)
	25		28		22
	24		16		22

Le nom d'une des machines Allemande utilisée lors de la seconde guerre mondiale est la machine `ENIGMA`. Calculez le hash de son nom.

Une autre machine a été utilisée par les allemands pendant la seconde guerre mondale. Cette machine porte le nom de son créateur, commence par un `'L'`, fini par un `'Z'` et son hash est de 32. Saurez vous la retrouvée ?

Quel est le nom des personnes travaillant à évaluer la sécurité des chiffrements (le nom doit être au pluriel), le mot fait 14 lettres et son hash entre en collision avec celui de `MACHINE ENIGMA` ?

Stéganographie

Info

Cette image en ASCII art cache un nombre entre 32 et 63. Saurez-vous le découvrir ?

```
          Y  Y
      SOUUSSONNOOOY
  YYNSIBYWFHJQHBNFOOS
  QOUIIINY      UINOIOOY
SOONJS             INIOOQ
ONONN               QNONNNNNN
ONOON                WONNNNINNY
WNIOOQ            YSOQQONNNNIINNU
 QNNOOO Y    UOSSSSSQQOONNNNIINN
  UOONONWQSSUUUUUUSSSQOONNNNIIIIY
   YONNNOOQSSUUUUUUQQSQOONONNINIIQ
   YOJI1NNOQSSUUQUUSOSNQ0ONONIINIIN
    OOIIINNOQQQUQQOSQQOSOQONNNNNNIIIW
     NNIIIINOOOQSOQQUSUSQQQOONNNNINIIO
      ONNJINNOOOQSUUQUUUSSSOQONNNIIIJOS
       UNNJIN1OO0SSUUUUUUUOOONQOOQSQSQS
        YINIIINNOQSSUUUONNSSUSSSQSQQQQ
          IOIJIINNQSSUOWUUQIHJJNQQS
           ONNJ1INOQSWUQSHFJJJSQQUUS
            UNNIIIQSQQQQIFISQSUSQQQSSQY
              NNOSQSQQQNO  SQSSQSSSQUSQ
            Y  NQQQQQY Y   SSSSSQINNSQQ
                SY         QQUSS0NJUSSQ
               Y            YNQQQQIOOIW
                              Y     WOUSSUUWY
                                  YQUUSNHHNSSU
                                  ONUUUUUJSSSUQ
                                  QSQQQSOQUUUUO
                                   SSSUSUUUUUQ
                                   WUWWUOUUUU
                                   OUWWFSSY
                                    SWQYW
                                   WUUNU
                                   UWOUW
                                   WWNU
                                  UWNSU
                                  UUNU
                                   YU
```

Analyse Fréquentielle

Challenge 7

Ouch !! Cette fois si vous vous trouvez dans une mauvaise situation, nous n'avons plus de texte clair pour nous aider à déchiffrer le texte chiffré... Heureusement pour nous, nous savons qu'il s'agit d'un message écrit en français et que le chiffrement utilisé est monoalphabétique.

```
mnqz zemdl, unw jd gd afnwz kez rq'wx p ewv bd snggdz nq bd ueqmewzdz
zwvqevwngz. unw zw jd bdmewz fdzqudf ue mwd, eqjnqfb'yqw, emda mnqz, jd
bwfewz rqd a'dzv b'esnfb bdz fdgangvfdz, bdz idgz rqw u'ngv vdgbq xe uewg,
kdqv-dvfd e qg unudgv nq jd gd knqmewz kez, nq j'dvewz zdqx aydl unw, dv
a'dzv ezzdl aqfwdqc bd zd bwfd rqd xdz yezefbz, xdz fdgangvfdz hnfidgv
qgd bdzvwgdd, kefad rqd rqegb ng e xd inqv bd xe aynzd, rqegb ng e xd
inqv bd xe aynzd swdg hewvd, xd sdeq idzvd, kefhnwz ng gd vfnqmd kez
x'wgvdfxnaqvdqf dg head, jd bwfewz xd uwfnwf rqw mnqz ewbd e emegadf ;
exnfz ad g'dzv kez ung aez anuud jd xd bwzewz xe, kqwzrqd unw eq angvfewfd
j'ew kq dv jd bwz udfaw e xe mwd, jd xqw bwz udfaw, jd ayegvd xe mwd, jd
begzd xe mwd, jd gd zqwz rq'eunqf, dv hwgexdudgv rqegb sdeqanqk bd idgz
eqjnqfb'yqw ud bwzdgv : uewz anuudgv hewz-vq knqf emnwf advvd yquegwvd ?
dv sey jd xdqf fdkngbz vfdz zwukxdudgv, jd xdqf bwz : a'dzv ad inqv bd
x'eunqf, ad inqv bnga rqw u'e knqzzd, eqjnqfb'yqw, e dgvfdkfdgbfd qgd
angzvfqavwng udaegwrqd uewz bduewg, rqw zewv, kdqv-dvfd, zwukxdudgv e ud
udvvfd eq zdfmwad bd xe anuuqgeqvd, e hewfd xd bng, xd bng bd znw ...
```

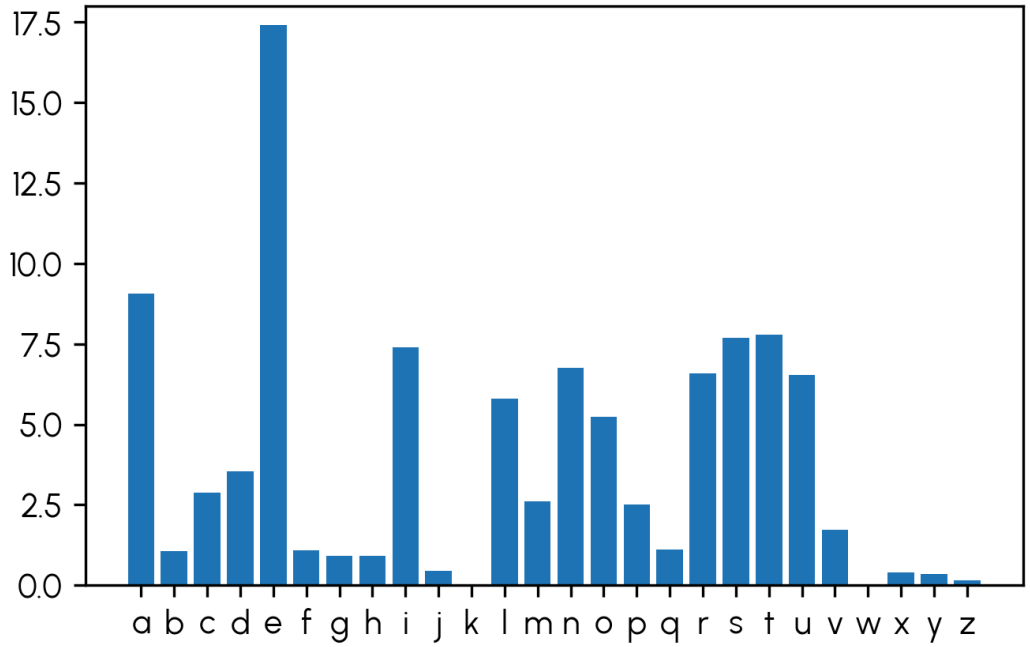


Fig. 1. – Fréquence d'apparition des lettres de l'alphabet dans « Les Misérables » de Victor Hugo.

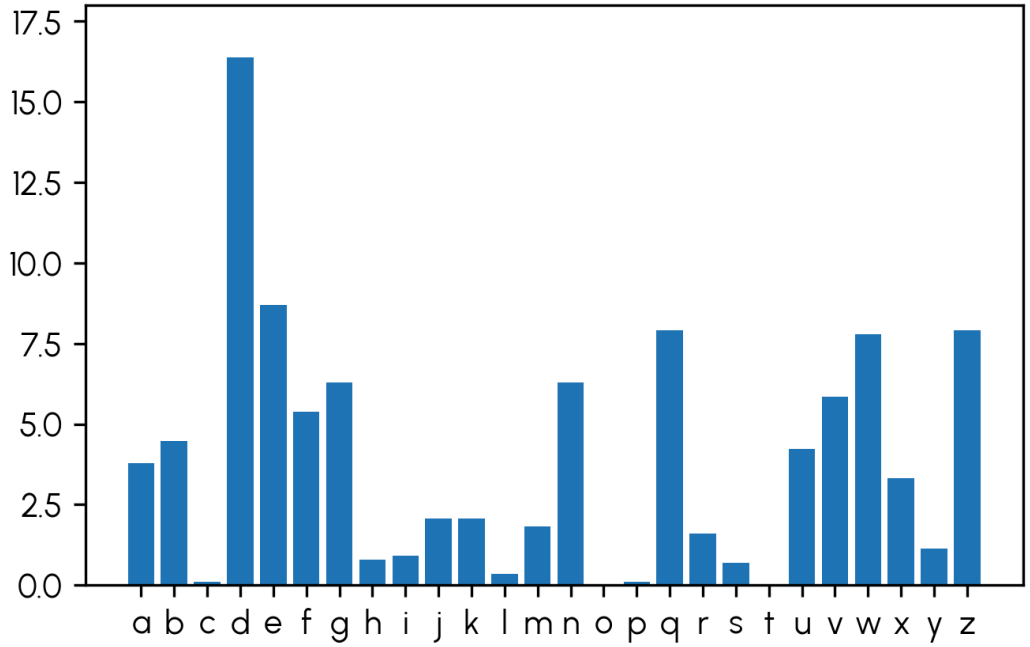


Fig. 2. – Fréquence d'apparition des symboles dans le text chiffré.