Iniciació a la Criptografia

Artur Travesa

(versió 2024-07)

Capítol 2. El criptosistema de Vigenère

2.0. Introducció

El criptosistema de Vigenère s'anomena així a partir del s. XIX, però, de fet, ja s'havia descrit i es feia servir des del s. XV.

I, com acostuma a succeir en aquests casos, hi ha motes versions que, essencialment, coincideixen amb aquest criptosistema.

Malgrat que se l'ha anomenat sovint "indesxifrable", la realitat és que és un criptosistema generalment molt feble, sobretot, degut al fet que sovint no s'empra(va) amb la cura necessària i, per exemple, es repeteixen les claus per a missatges diferents. O bé les claus són massa curtes per al tipus de missatges que cal xifrar.

2.1. Descripció del criptosistema

El criptosistema de Vigenère és alhora una generalització i una millora del criptosistema de Cèsar.

S'utilitza un alfabet i es xifren successivament els caràcters de l'alfabet que conformen el text pla.

Per a xifrar un missatge amb aquest criptosistema cal, en primer lloc, triar una paraula clau (això és, una successió de caràcters de l'alfabet, que no cal que tingui cap sentit). Sigui k la longitud (el nombre de caràcters) d'aquesta paraula clau.

A continuació, es prenen de k en k els caràcters del missatge pla, de manera que aquest resta dividit en blocs de k caràcters excepte, potser, el darrer bloc, que només conté la quantitat de caràcters que resten de la divisió de la longitud total del missatge entre k.

Seguidament, es consideren els k missatges formats pels primers, els segons, ..., els k-èsims caràcters del missatge original.

A continuació, s'aplica a cadascun dels $i = 0, 1, ..., k - 1$ missatges nous la transformació de Cèsar que correspon a la clau Cèsar donada pel caràcter i-èsim de la clau Vigenère.

I, finalment, es construeix el missatge xifrat en intercalar els caràcters així obtinguts: primerament, el primer de cadascun dels k missatges xifrats; després, els segons; després, els tercers; etcètera.

2.2. Les funcions de xifratge i de desifratge

Es tracta d'escriure una funció VigenereX(mis,clau) per a xifrar amb el criptosistema de Vigenère, i la funció inversa, VigenereDX(mis,clau), per a desxifrar amb el criptosistema de Vigenère anterior.

In [1]:
```
def VigenereX(mis,clau):
    m=1114112
    if type(mis)==str:
        lta=[ord(i) for i in mis]
        b=1
    else:
        lta=mis
        b=0
    if type(clau)==str:
        cc=[ord(i) for i in clau]
    else:
        cc=clau
    lc=len(cc)
    vgn=[(lta[i]+cc[i%lc])%m for i in range(len(lta))]
    if b==0:
        xif=vgn
    else:
        xif=""
        for i in range(len(vgn)):
            xif=xif+chr(vgn[i])
    return xif

```

In [2]:
```
def VigenereDX(mis,clau):
    m=1114112
    if type(mis)==str:
        lta=[ord(i) for i in mis]
    else:
        lta=mis
    if type(clau)==str:
        cc=[ord(i) for i in clau]
    else:
        cc=clau
    lc=len(cc)
    vgn=[(lta[i]-cc[i%lc])%m for i in range(len(lta))]
    desx=""
    for i in range(len(vgn)):
        desx=desx+chr(vgn[i])
    return desx

```

2.2.0. Exemples

Comprovem que, efectivament, les funcions xifren i desxifren correctament.

In [3]:
```
1 mis="Això és un primer text de prova per al criptosistema de Vig
```

In [4]:
```
1 cl="ab!1"
```

In [5]:
```
1 misx=VigenereX(mis,cl)
```

In [6]:
```
1 misx
```

Out[6]:
```
'¢Ë\x99ģ\x81ŋ\x94QÖÐA¡ÓË\x8e\x96Ó\x82\x95\x96ÙÖA\x95Æ\x82\x91£ÐØ\x8
2QÑÇ\x93QÂÎA\x94ÓË\x91¥ÐÕ\x8a¤ÕÇ\x8e\x92\x81Æ\x86Q·Ë\x88\x96ÏŋJ\x93
\x96\x8f'
```

In [7]:
```
1 VigenereDX(misx,cl)
```

Out[7]:
```
'Això és un primer text de prova per al criptosistema de Vigenère.'
```

Notem que la clau [0,0,0] no "xifra" (com ha de ser).

In [8]:
```
1 VigenereX(mis,[0,0,0])
```

Out[8]:
```
'Això és un primer text de prova per al criptosistema de Vigenère.'
```

2.3. Seguretat?

Es demana intentar desxifrar el missatge xifrat següent, que se sap que és xifrat amb una paraula clau de longitud 25. Quina és aquesta paraula clau?

xifrat='\x88Þ\x89ÓæØãÝâçÎàÕ\x85ÑÆ@ºÎ\x87»×ŏ×ÓïäÎ\x90ŝâ\x93ÞáÕ\x85ÔÆ\x8eÉ×\x81Â
\x85ÀÆ\x87ÙÎ\x84·ÖÌÓâË\x92Ê¶\x92ÌßââÜÍØæÊÛ\x81\x85ÐØ@𝒮\x89ÔÎáśÓÙª×Ü\x90ÚÞåĊ
\xa0\x9f\x89¥
\xa0\x85\x9b\x8fN\x90\x85𝑸vÖÐØáȵnæÌ¨å\x89Þãäæ\x89ßÕ\x85áÓ\x81ÒØ\x86ÅÛÔÆÑőť\x8

Observació. No s'ha d'intentar usar la força bruta. Cal notar que paraules de 25 caràcters entre els 1114112 possibles n'hi ha 1114112^{25}, o sigui, "aproximadament" $14,9 \cdot 10^{150}$. I si poguéssim provar 10^{12} claus per segon (!), necessitaríem aproximadament $5,9 \cdot 10^{106}$ anys per a provar-les totes (l'edat estimada de l'univers és "només" de $1,37 \cdot 10^{10}$ anys).

In [9]:
```
1 xifrat ='\x88Þ\x89ÓæØãÝâçÎàÕ\x85ÑÆ@ºÎ\x87»×ŏ×ÓïäÎ\x90ŝâ\x93ÞáÕ\
```

2.3.0. Una solució

In [10]:
```
1 xifrat
```

Out[10]:
```
'\x88Þ\x89ÓæØãÝâçÎàÕ\x85ÑÆ@ºÎ\x87»×ŏ×ÓīäÎ\x90ŝâ\x93ÞáÕ\x85ÔÆ\x8eÉ
×\x81ÂÒÛßÏŋÛŘcÛ\x89åâÐ\x93ÖÜàÑÜÓ\x81\x84É\x85Â\x89Ê××ŘæÔ¶ÛÜäÙÜÛ\x89
×Ù\x85°ƞ\x93Å×Nv¹Ì×\x8eƞ\x92Ý¬ØÛÑæ\x8fè×\x93áÎàÔ\x81ØÌ\x85vÊÔÇ\x8eƞ
ãÚ¨åÝ\x90×áÜÙçãØÖÔ\x94ÉÒ\x81vÌÈÑ\x9aĈ×ÓcâÛÙáÔå\x89ßàÔÐ\x8d@Ø×\x89·Û
\x87ÚÜƞ\x92Õ¤äÊåàÐ\x93ÌßÕÚ\x8d\x89\x81ÍÝĒvŒÚ\x91\x8eŝàÆcåÞÓ×ÔæÜÜŧ\x
85ÑÆ@ÇÆ\x92ĶÌÛÊàś\x92É¨\x92Õ\x97ÕÛÙÊÕÙÙ\x99\x81\x91ÙÊ@ÄØ\x87ÈÏŔ\x92
Ö¸×\x89äÝÝÚÞÜ\x94ÈÎÑ@×Ê\x8eÊÒÛ\x8e\x9cĈÅÎªçÒ\x90𝓌\x8fßÊ\x93àÔÛÈ\x89
ØÚ\x84v\x91ÌÑ\x8eĶáÒ¥äÎ\x90ØÔ\x93ÌÔæŊÐÕ\x85ÖØIvÍ\x8eÆßŝ×Ø·Ó\x89àÕáÔ
ÞßÕ\x85ÐÍ\x81Ù\x93@\x97\x89ÊÔÜŜÛÓ¸ÓÌÚŧ\x9b\x93Îæ\x94ÕßÆ\x8eÉÓ@ºÎ\x8
7𝓱\x8eōà\x85𝔃\x92ÎÜç\x8fÖÊåŔÈáÆ\x92×\x85\x84»Õ\x87Ò×śåÆ·ÙÎ\x90äÛÔ\x
95\x93ØÊ\x8dÎ\x81ÒÊ\x92·\x89ØÚÓĈÓÖ¸×Üä\x94áØÜçÕ\x85ÑÊ\x96ÍÉ\x89Ê\x8
9ÌÓ\x8eŋÞÔ¦å\x89ÔÙ\x8f𝓌\x89ÖÕ×ōÄ\x94É×\x93vÎßÈÓŘæÊo\x92ÙßèâØÛ\x9f\x
94ÊÙ\x81\x84Å×\x92»Û\x87ÇÚŗÕ\x91cãÞÕ\x94ÝâÖŜç\x85ÐĐ\x8eØŎ@ÂÊ\x87Öã'n
àÙ¬æÊä\x94ÓØ\x89ÖÕ×ōÄ\x94É×\x93vÚÜÊ\x8eŚ×Ø·××\x90ØÔ\x93ÕÔ\x94ÉÖ×\x8
9×ÎēvÍÌ\x85Ú'n\x92Ñ²àÐÙèä×\x89çãÙÎÍ@ÈÊ\x8cvÖÐØá'næÌ¨\x92ÎÞèáØ\x89𝓌¢\x
85ÀÆ\x87ÙÎ\x84·ÖÌÓâĚ\x92Ê¶\x92ÌßââÜÍØæÊÛ\x81\x85ÐØ@𝒫\x89ÔÎáśÓÙª×Ü\x
90ÚÞåÖÔèØ\x8dÑ\x85ÐØ@ÆÛĐÒÓŚå\x91c×Õã\x94âØÐââØ\x99\x81N\x92\x93LvÎÓ
Ø\x8eⅡ\x9fō¶ÛÖã\x94ÒÔÛœ×ÙÒÓ\x93\x84É\x85Â\x89ÔÎáśÓÙª×\x89ßæØÚÒáÕÑ\x
9b\x81a\x84È\x8fÄÝÐÓã'nÕÎĶ\x9e\x89ã\x9bÐãÕÜ×Æ\x8dÂ@ÇÆ\x84·ÜÊÚÜĈÖÊ¯å
\x89𝓆±\xa0\x9f\x89¥\xa0\x85\x9b\x8fN\x90\x85𝑸vÖÐØá'næÌ¨å\x89Þãäæ\x89
ßÕ\x85áÓ\x81ÒØ\x86ÅÛÔÆÑőť\x85§×\x89³ŜâÔÛ\x93åÚÒ\x81\x83Ó×\x92»Ü×ÔÜĈ
Ó\x85¯Ó\x89ÓàÐè\x89¶ŜØÎÓ@ÈÔ\x8e·ÍÈ\x85ÞōÞ\x85¦ÓÛŐ×ãØÛ\x93𝓊\x92ŕÔ\x8
9Ñ\x85\x84»\x89ÓÆ\x8eŋÞÆ¸\x92¿ÙÛÔáőåÙ\x93\x8dªL\x84Ë\x89ÄĚÓÒÓŖæ\x91
c×Ü\x90×ÞáÜçæÚÒÊ\x98\x84Ê\x8cvÖÐØá'næÌ¨\x92áÙÚáÔÝ\x93ÙÓ\x8dÊ\x8eØÊ\x
92¹ÊÓÆàĈ×Ñ¶\x92ÌÑæŏÖÝØæØ\x8dÂ\x89ÜŒ@ÅËÛÎÜŏçÙ¶¬\x89àæØàÎåÕÒÒÏ\x94\x9
0\x85\x85Â\x89×××ŕ××cÖÎ\x90×Ð×Êæ×ÚÛ\x81\x84ÉÑ\x93v𝓡\x87Ò×śåÆ·ÙÎã\x94
çÜÏåÕÙà\x9c@ÈÊ\x93ÆÛŐØ\x9aĈ×Ñ¶\x92ÜÕÛÞáÜ®\x94ÉÒÔ\x90ÖÕ\x93\x82\x89Ì
ÑáĈæÊµÕÎâçª\x93Îç×ōáÆ\x92Å\x93'
```

Comencem per convertir el missatge xifrat en una llista de codis numèrics.

In [11]:
```
1 lta=[ord(i) for i in xifrat]
```

In [12]:
```
1 print(lta)
```

[136, 222, 137, 211, 230, 216, 227, 221, 226, 231, 206, 224, 213, 1
33, 209, 198, 64, 186, 206, 135, 187, 215, 335, 215, 211, 299, 228,
206, 144, 349, 226, 147, 222, 225, 213, 133, 212, 198, 142, 201, 21
5, 129, 194, 210, 219, 223, 207, 331, 219, 344, 99, 219, 137, 229,
226, 208, 147, 214, 220, 224, 209, 220, 211, 129, 132, 201, 133, 19
4, 137, 202, 215, 215, 344, 230, 212, 182, 219, 220, 228, 217, 220,
212, 137, 215, 217, 133, 176, 329, 147, 197, 215, 78, 118, 185, 204
, 215, 142, 329, 146, 221, 172, 216, 219, 209, 230, 143, 232, 215,
147, 225, 206, 224, 212, 129, 216, 204, 133, 118, 202, 212, 199, 14
2, 329, 227, 218, 168, 229, 221, 144, 215, 225, 220, 217, 231, 227,
216, 214, 212, 148, 201, 210, 129, 118, 204, 200, 209, 154, 264, 21
5, 211, 99, 226, 219, 217, 225, 212, 229, 137, 223, 224, 212, 208,
141, 64, 216, 215, 137, 183, 219, 135, 218, 220, 329, 146, 213, 164
, 228, 202, 229, 224, 208, 147, 204, 223, 213, 218, 141, 137, 129,
205, 221, 274, 118, 338, 218, 145, 142, 349, 224, 198, 99, 229, 222
, 211, 215, 212, 230, 220, 220, 359, 133, 209, 198, 64, 199, 198, 1
46, 310, 204, 219, 202, 224, 347, 146, 201, 168, 146, 213, 151, 213
, 219, 217, 202, 213, 217, 217, 153, 129, 145, 217, 202, 64, 196, 2
16, 135, 200, 207, 340, 146, 214, 184, 215, 137, 228, 221, 221, 218
, 222, 220, 148, 200, 206, 209, 64, 215, 202, 142, 202, 210, 219, 1
42, 156, 264, 197, 206, 170, 231, 210, 144, 120012, 143, 223, 202,
147, 224, 212, 219, 200, 137, 216, 218, 132, 118, 145, 204, 209, 14
2, 342, 225, 210, 165, 228, 206, 144, 216, 212, 147, 204, 212, 230,
325, 208, 213, 133, 214, 216, 73, 118, 205, 142, 198, 223, 349, 215
, 216, 183, 211, 137, 224, 213, 225, 212, 222, 223, 213, 133, 208,
205, 129, 217, 147, 64, 151, 137, 202, 212, 220, 348, 219, 211, 184
, 211, 204, 217, 359, 155, 147, 206, 230, 148, 213, 223, 198, 142,
201, 211, 64, 186, 206, 135, 119997, 142, 333, 224, 133, 119963, 14
6, 206, 220, 231, 143, 214, 202, 229, 340, 200, 225, 198, 146, 215,
133, 132, 187, 213, 135, 210, 215, 347, 229, 198, 183, 217, 206, 14
4, 228, 219, 212, 149, 147, 216, 202, 141, 206, 129, 210, 202, 146,
183, 137, 216, 218, 211, 264, 211, 214, 184, 215, 220, 228, 148, 22
5, 216, 220, 231, 213, 133, 209, 202, 150, 205, 201, 137, 202, 137,
204, 211, 142, 330, 222, 212, 166, 229, 137, 212, 217, 143, 120011,
137, 214, 213, 215, 333, 196, 148, 201, 215, 147, 118, 206, 223, 20
0, 211, 344, 230, 202, 111, 146, 217, 223, 232, 226, 216, 219, 159,
148, 202, 217, 129, 132, 197, 215, 146, 187, 219, 135, 199, 218, 34
3, 213, 145, 99, 227, 222, 213, 148, 221, 226, 214, 348, 231, 133,
208, 208, 142, 216, 334, 64, 194, 202, 135, 214, 227, 329, 224, 217
, 172, 230, 202, 228, 148, 211, 216, 137, 214, 213, 215, 333, 196,
148, 201, 215, 147, 118, 218, 220, 202, 142, 346, 215, 216, 183, 21
5, 215, 144, 216, 212, 147, 213, 212, 148, 201, 214, 215, 137, 215,
206, 275, 118, 205, 204, 133, 218, 329, 146, 209, 178, 224, 208, 21
7, 232, 228, 215, 137, 231, 227, 217, 206, 205, 64, 200, 202, 140,
118, 214, 208, 216, 225, 329, 230, 204, 168, 146, 206, 222, 232, 22
5, 216, 137, 120011, 162, 133, 192, 198, 135, 217, 206, 132, 183, 2
14, 204, 211, 226, 276, 146, 202, 182, 146, 204, 223, 226, 226, 220
, 205, 216, 230, 202, 219, 129, 133, 208, 216, 64, 119982, 137, 212
, 206, 225, 347, 211, 217, 170, 215, 220, 144, 218, 222, 229, 214,
212, 232, 216, 141, 209, 133, 208, 216, 64, 198, 219, 208, 210, 211
, 346, 229, 145, 99, 215, 213, 227, 148, 226, 216, 208, 226, 226, 2
16, 153, 129, 78, 146, 147, 76, 118, 206, 211, 216, 142, 120128, 15
9, 333, 182, 219, 214, 227, 148, 210, 212, 219, 339, 215, 217, 210,
211, 147, 132, 201, 133, 194, 137, 212, 206, 225, 347, 211, 217, 17
0, 215, 137, 223, 230, 216, 218, 210, 225, 213, 209, 155, 129, 97,
132, 200, 143, 196, 221, 208, 211, 227, 329, 213, 206, 310, 158, 13
7, 227, 155, 208, 227, 213, 220, 215, 198, 141, 194, 64, 199, 198,
132, 183, 220, 202, 218, 220, 264, 214, 202, 175, 229, 137, 120006,
177, 160, 159, 137, 165, 160, 133, 155, 143, 78, 144, 133, 119928,
118, 214, 208, 216, 225, 329, 230, 204, 168, 229, 137, 222, 227, 22

```
8, 230, 137, 223, 213, 133, 225, 211, 129, 210, 216, 134, 197, 219,
212, 198, 209, 337, 357, 133, 167, 215, 137, 179, 348, 226, 212, 21
9, 147, 229, 218, 210, 129, 131, 211, 215, 146, 187, 220, 215, 212,
220, 264, 211, 133, 175, 211, 137, 211, 224, 208, 232, 137, 182, 34
8, 216, 206, 211, 64, 200, 212, 142, 183, 205, 200, 133, 222, 333,
222, 133, 166, 211, 219, 336, 215, 227, 216, 219, 147, 120010, 146,
341, 212, 137, 209, 133, 132, 187, 137, 211, 198, 142, 331, 222, 19
8, 184, 146, 191, 217, 219, 212, 225, 337, 229, 217, 147, 141, 170,
76, 132, 203, 137, 196, 202, 211, 210, 211, 342, 230, 145, 99, 215,
220, 144, 215, 222, 225, 220, 231, 230, 218, 210, 202, 152, 132, 20
2, 140, 118, 214, 208, 216, 225, 329, 230, 204, 168, 146, 225, 217,
218, 225, 212, 221, 147, 217, 211, 141, 202, 142, 216, 202, 146, 18
5, 202, 211, 198, 224, 264, 215, 209, 182, 146, 204, 209, 230, 335,
214, 221, 216, 230, 216, 141, 194, 137, 220, 338, 64, 197, 203, 219
, 206, 220, 335, 231, 217, 182, 172, 137, 224, 230, 216, 224, 206,
229, 213, 210, 210, 207, 148, 144, 133, 133, 194, 137, 215, 215, 21
5, 341, 215, 215, 99, 214, 206, 144, 215, 208, 215, 202, 230, 215,
218, 219, 129, 132, 201, 209, 147, 118, 120001, 135, 210, 215, 347,
229, 198, 183, 217, 206, 227, 148, 231, 220, 207, 229, 213, 217, 22
4, 156, 64, 200, 202, 147, 198, 219, 336, 216, 154, 264, 215, 209,
182, 146, 220, 213, 219, 222, 225, 220, 174, 148, 201, 210, 212, 14
4, 214, 334, 147, 130, 137, 204, 209, 225, 264, 230, 202, 181, 213,
206, 226, 231, 170, 147, 206, 231, 215, 333, 225, 198, 146, 197, 14
7]
```

Ara, com que sabem la longitud de la clau, 25, podem considerar els 25 missatges xifrats amb criptosistemes de Cèsar (llevat del tros final). Els utilitzarem per a (intentar) esbrinar la clau.

In [13]:
```
1 blocs = transpose(matrix(ZZ, len(lta) // 25, 25, lta[0:len(lta)-
```

Mirem quins són els codis que corresponen als caràcters alfabètics generals (sense accents).

In [14]:
```
1 [ord("A"),ord("Z"),ord("a"),ord("z")]
```

Out[14]:
```
[65, 90, 97, 122]
```

Ens imaginem que la paraula clau estarà formada majoritàriament per alguns d'aquests caràcters. Mirem com estan de lluny dels caràcters ASCII imprimibles els caràcters xifrats.

In [15]:
```
1 [max(blocs[0])-32,min(blocs[0])-32]
```

Out[15]:
```
[119931, 67]
```

L'espai en blanc es transforma (sembla) en el caràcter de codi 67, que correspon a la C (majúscula). Provem de desxifrar aquest bloc amb aquesta clau.

In [16]:
```
1 VigenereDX(blocs[0],"C")
```

Out[16]:
```
'Eè sie a eugbtuktuc, itoesg sgóledlcu ess ts'
```

Sembla que tingui sentit! (només apareixen caràcters usuals de text!) Repetim amb els altres blocs (intentem esbrinar la lletra de la paraula clau i la provem.)

In [17]:
```
clau=[chr(min(blocs[v])-32) for v in range(25)]
```

In [18]:
```
print(clau)
```

```
['C', 'r', 'i', 'p', 't', 'o', 's', 'i', 's', 't', 'e', 'm', 'a', '
', 'd', 'e', ' ', 'V', 'i', 'g', 'e', 'n', 'è', 'r', 'e']
```

Té sentit! Provem-la!

In [19]:
```
VigenereDX(xifrat,"Criptosistema de Vigenère")
```

Out[19]:
```
"El criptosistema de Vigenère és una generalització i una millora d
el criptosistema de Cèsar. Per a xifrar un missatge amb aquest crip
tosistema cal, en primer lloc, triar una paraula clau (això és, una
successió de caràcters de l'alfabet, que no cal que tingui cap sent
it). Sigui k la longitud (el nombre de caràcters) d'aquesta paraula
clau. A continuació, es prenen de k en k els caràcters del missatge
pla, de manera que aquest resta dividit en blocs de k caràcters exc
epte, potser, el darrer bloc, que només conté la quantitat de caràc
ters que resten de la divisió de la longitud total del missatge ent
re k. Seguidament, es consideren els k missatges formats pels prime
rs, els segons, ..., els k-èsims caràcters del missatge original. A
continuació, s'aplica a cadascun dels i=1, 2, ..., k missatges nous
la transformació de Cèsar que correspon a la clau Cèsar donada pel
caràcter i-èsim de la clau Vigenère. I, finalment, es construeix el
missatge xifrat en intercalar els caràcters així obtinguts: primera
ment, el primer de cadascun dels k missatges xifrats; després, els
segons; després, els tercers; etcètera."
```

Efectivament, no era gaire difícil.

Una raó és perquè el missatge és de text i la clau també, i senzilla (amb caràcters habituals, i a més a més, una paraula amb sentit).

Ara bé, si la clau fos aleatòria i de mida tan gran com (o més que) el missatge que es vol xifrar, estariem en el cas d'un xifrat de tipus Vernam.

Deixem per a una altra ocasió comentar el xifrat de Vernam. La dificultat pràctica més gran que té és la transmissió de la clau al destinatari del missatge. Si algun actor intercepta la clau, podrà desxifrar el missatge. Per tant, la clau s'ha de transmetre de forma segura, i prèviament al missatge xifrat.

2.4. Exercici proposat

La llista següent, TextXifrat, correspon a un missatge xifrat amb el criptosistema de Vigenère. No en coneixem ni tan sols la longitud de la clau. Però,

(a) podríem desxifrar-lo?

(b) Sabríem dir quina és la clau? I com s'ha obtingut?

Observació. Caldrà treballar amb esperit **crí**(p)**t**(ogràf)**ic**.

TextXifrat="\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x12\U0010fffc\x02\U(
\x17\n\x06\U0010ffbb\U0010fff1E\U0010ffbbV}\x0e\U0010ffb2\U0010fff6\U0010fffc\x00\x0f\t\
\n\x07\U0010ffbb\U0010ffeeC\nM\U0010fffa\U0010fffc\x04\U0010ffed\U0010ffffÉ\U0010ffd8\
\n\x00\x00\U0010ffff\x00\x0eO\U0010ffec\r\U0010fff3\x00\U0010ff97P\x1f\x0e\U0010fff7\U0(
\x00\U0010fff9\r\U0010ffbb\U0010ffea\U0010ffa5!
\U0010fff7\n\x04\U0010ffb8\U0010ffadD\x0f\U0010ffbb\n\x8e\x00\x00\x05O\U0010ffaa\x00\x

In [20]:
```
TextXifrat = "\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x12\U0010fffc\x02\U0010ffbb\U0010fffaO\x0e\x00\U0010ffee\x00\x05\U0010fff5\U0010fff4S\U0010ffca\U0010fffe\x03\x08\U0010fffdL\x04R\U0010ffaa\U0010ffc3\U0010ffc3\U0010ffc5\U0010ffc3\x19\U0010ffd3\U0010ffa5\U0010ffbc\U0010ffdc\x02S\x04À\U0010fffd\U0010ffbb\U0010ffdf\U0010ffed\U0010ffffC\x12\U0010ffbb\U0010ffc1\U0010ffbb\U0010ffdfA\x04M\U0010fff9\t\U0010ffbb\U0010ff96\U0010ff976\x0f\x07\U0010fff9\x0e\U0010ffadE
\U0010ffbbV\U0010ffef\t\x06\U0010ffff\U0010ffadH\x0b\t\U0010ffb4\x08\U0010fffcS\U0010ffbbD\U0010ffef\x0e\U0010fffb\U0010fff3\x00\x00\r\n\x01\x0b\U0010fff9I\r\x0c\U0010ff94\x01\U0010fff3\U0010fff1\U0010fffbT\U0010ffca\U0010fffe\U0010fff5\x08\U0010fff6N\x0e\x00\U0010ffee\x10\U0010fff4\x00\U0010fffcS\x19\x0e\U0010ffb4\x0b\U0010fff2R\U0010ffbbL\U0010ffeb\U0010ffbb\U0010ffff\U0010ffed\U0010ffff\x0e\U0010ffb4\U0010ffe8\U0010fff9\x0e\x01R\x00\x00\U0010fff3\U0010ffbb\x02\U0010fffb\U0010fffbE\x18\x0f\U0010ffb4\U0010fffe\U0010fffcN\x0fR\U0010ffeb\U0010ffbb\U0010fff6\U0010ffb3\U0010fff2L\x16\x0e\U0010ffb4\x11\U0010fff2I\x02\x00\U0010ffeb\r\U0010ffff\U0010ffed\U0010ffff\x1b\U0010ffb4\x13\U0010fff5\x07\U0010fffcC\U0010ffc7\x00\U0010fff6\x07\U0010fff7\x02\U0010ffeeN\x1e\U0010ffc7\U0010ffb4\x07\U0010fffcS\U0
```

In [21]:
```
TextXifrat
```

Out[21]:
```
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x12\U0010
fffc\x02\U0010ffbb\U0010fffaO\x0e\x00\U0010ffee\x00\x05\U0010fff5\U
0010fff4S\U0010ffca\U0010fffe\x03\x08\U0010fffdL\x04R\U0010ffaa\U00
10ffc3\U0010ffc3\U0010ffc5\U0010ffc3\x19\U0010ffd3\U0010ffa5\U0010f
fbc\U0010ffdc\x02S\x04À\U0010fffd\U0010ffbb\U0010ffdf\U0010ffed\U00
10ffffC\x12\U0010ffbb\U0010ffc1\U0010ffbb\U0010ffdfA\x04M\U0010fff9
\t\U0010ffbb\U0010ff96\U0010ff976\x0f\x07\U0010fff9\x0e\U0010ffadE
\U0010ffbbV\U0010ffef\t\x06\U0010ffff\U0010ffadH\x0b\t\U0010ffb4\x0
8\U0010fffcS\U0010ffbbD\U0010ffef\x0e\U0010fffb\U0010fff3\x00\x00\r
\n\x01\x0b\U0010fff9I\r\x0c\U0010ff94\x01\U0010fff3\U0010fff1\U0010
fffbT\U0010ffca\U0010fffe\U0010fff5\x08\U0010fff6N\x0e\x00\U0010ffe
e\x10\U0010fff4\x00\U0010fffcS\x19\x0e\U0010ffb4\x0b\U0010fff2R\U00
10ffbbL\U0010ffeb\U0010ffbb\U0010ffff\U0010ffed\U0010ffff\x0e\U0010
ffb4\U0010ffe8\U0010fff9\x0e\x01R\x00\x00\U0010fff3\U0010ffbb\x02\U
0010fffb\U0010fffbE\x18\x0f\U0010ffb4\U0010fffe\U0010fffcN\x0fR\U00
10ffeb\U0010ffbb\U0010fff6\U0010ffb3\U0010fff2L\x16\x0e\U0010ffb4\x
11\U0010fff2I\x02\x00\U0010ffeb\r\U0010ffff\U0010ffed\U0010ffff\x1b
\U0010ffb4\x13\U0010fff5\x07\U0010fffcC\U0010ffc7\x00\U0010fff6\x07
\U0010fff7\x02\U0010ffeeN\x1e\U0010ffc7\U0010ffb4\x07\U0010fffcS\U0
```

Fi del capítol 2