Criptografia bàsica

Artur Travesa

(versió 2024-07)

Apèndix 1: Solució a un problema de desxifratge

A1.0. Introducció

Aquest notebook conté una solució de l'exercici proposat al capítol 2.

A1.1. Criptosistema de Vigenère

Proporcionem les funcions del tutorial per al xifratge i el desxifratge.

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

```

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

```

A1.2. L'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**.

In [3]:
```
TextXifrat = "\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
```

In [4]:
```
TextXifrat
```

Out[4]:
```
"\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
```

A1.3. Una solució

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

In [5]:
```
lta=[ord(v) for v in TextXifrat]
```

In [6]:
```
print(lta)
```

```
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 18, 1114108, 2, 1114043,
1114106, 79, 14, 0, 1114094, 0, 5, 1114101, 1114100, 83, 1114058, 1
114110, 3, 8, 1114109, 76, 4, 82, 1114026, 1114051, 1114051, 111405
3, 1114051, 25, 1114067, 1114021, 1114044, 1114076, 2, 83, 4, 192,
1114109, 1114043, 1114079, 1114093, 1114111, 67, 18, 1114043, 11140
49, 1114043, 1114079, 65, 4, 77, 1114105, 9, 1114043, 1114006, 1114
007, 54, 15, 7, 1114105, 14, 1114029, 69, 1114043, 86, 1114095, 9,
6, 1114111, 1114029, 72, 11, 9, 1114036, 8, 1114108, 83, 1114043, 6
8, 1114095, 14, 1114107, 1114099, 0, 0, 13, 10, 1, 11, 1114105, 73,
13, 12, 1114004, 1, 1114099, 1114097, 1114107, 84, 1114058, 1114110
, 1114101, 8, 1114102, 78, 14, 0, 1114094, 16, 1114100, 0, 1114108,
83, 25, 14, 1114036, 11, 1114098, 82, 1114043, 76, 1114091, 1114043
, 1114111, 1114093, 1114111, 14, 1114036, 1114088, 1114105, 14, 1,
82, 0, 0, 1114099, 1114043, 2, 1114107, 1114107, 69, 24, 15, 111403
6, 1114110, 1114108, 78, 15, 82, 1114091, 1114043, 1114102, 1114035
, 1114098, 76, 22, 14, 1114036, 17, 1114098, 73, 2, 0, 1114091, 13,
1114111, 1114093, 1114111, 27, 1114036, 19, 1114101, 7, 1114108, 67
, 1114055, 0, 1114102, 7, 1114103, 2, 1114094, 78, 30, 1114055, 111
4036, 7, 1114108, 83, 1114043, 68, 1114095, 16, 1114103, 1114106, 1
```

Els primers 14 caràcters del text xifrat són iguals, de manera que la clau Vigenère xifra els primers 14 caràcters del text pla de manera que proporcionen el mateix caràcter xifrat. Això diu que els 14 primers caràcters de la clau són els complementaris (a 1114112) dels primers del text pla.

No és fora de lloc pensar que la clau és de 14 caràcters, i que s'obtindria d'aquesta manera. Ho provarem.

Comencem per trencar el missatge en els 14 missatges que s'haurien xifrat amb un Cèsar cadascun.

In [7]:
```
blocs = transpose(matrix(ZZ, len(lta) // 14, 14, lta[0:len(lta)-
```

Mirem quins caràcters i amb quina freqüència apareixen a cada bloc.

In [8]:
```
fr=[[j,[(i, list(blocs[j]).count(i)) for i in set(blocs[j])]] fo
```

In [9]:
```
1 print(fr)
```

[[0, [(0, 1), (11, 5), (12, 1), (13, 2), (14, 2), (15, 9), (18, 2), (19, 4), (147, 1), (22, 4), (23, 4), (24, 5), (25, 4), (26, 2), (28, 6), (29, 5), (30, 3), (31, 5), (32, 3), (157, 1), (1114036, 4), (1114058, 16), (1114067, 1), (1114070, 2), (1114071, 1), (1114072, 2), (1114091, 1)]], [1, [(0, 7), (1, 1), (130, 1), (7, 5), (8, 3), (9, 7), (10, 5), (11, 1), (12, 1), (13, 4), (14, 7), (15, 8), (16, 2), (17, 2), (142, 1), (19, 2), (1114021, 4), (1114043, 15), (1114055, 3), (1114088, 1), (123, 1), (1114108, 7), (1114109, 1), (1114110, 6), (1114111, 1)]], [2, [(0, 6), (1, 3), (2, 6), (3, 6), (5, 1), (6, 8), (7, 9), (8, 4), (135, 1), (10, 2), (9, 1), (1114014, 3), (1114036, 16), (1114043, 1), (1114044, 1), (1114048, 1), (1114049, 1), (1114050, 1), (1114101, 7), (1114103, 1), (1114104, 3), (1114105, 8), (1114109, 3), (1114110, 3)]], [3, [(0, 16), (1, 1), (131, 1), (4, 1), (7, 4), (8, 5), (9, 5), (10, 5), (11, 3), (13, 5), (14, 7), (15, 5), (16, 1), (17, 1), (142, 1), (1114021, 3), (1114043, 17), (1114050, 1), (1114055, 1), (1114069, 1), (1114076, 1), (1114077, 1), (1114084, 1), (1114108, 7), (1114110, 2)]], [4, [(0, 7), (1, 3), (2, 3), (3, 2), (1114007, 2), (1114029, 19), (1114043, 3), (1114071, 1), (1114079, 1), (109, 1), (1114094, 8), (1114096, 5), (1114097, 3), (1114098, 7), (117, 1), (1114102, 2), (118, 2), (1114105, 2), (1114106, 6), (1114107, 4), (1114108, 6), (1114109, 3), (1114110, 1), (1114111, 4)]], [5, [(0, 20), (12, 2), (27, 1), (192, 1), (65, 7), (67, 2), (68, 2), (69, 11), (73, 5), (76, 7), (77, 2), (78, 6), (79, 5), (80, 1), (82, 6), (83, 5), (84, 3), (85, 2), (211, 2), (86, 1), (88, 1), (1114090, 4)]], [6, [(0, 5), (1, 1), (2, 1), (4, 6), (132, 1), (5, 1), (7, 3), (8, 5), (9, 6), (10, 6), (12, 3), (13, 7), (14, 7), (15, 6), (142, 1), (16, 1), (1114021, 4), (1114043, 18), (1114050, 1), (1114055, 1), (1114080, 1), (1114094, 1), (123, 1), (1114108, 4), (1114109, 1), (1114110, 3), (1114111, 1)]], [7, [(0, 22), (12, 2), (26, 1), (33, 1), (192, 1), (65, 4), (67, 1), (68, 4), (69, 7), (73, 2), (74, 1), (76, 1), (77, 6), (79, 9), (80, 3), (81, 1), (82, 6), (83, 10), (84, 4), (85, 4), (86, 4), (1114090, 2)]], [8, [(0, 1), (1114004, 2), (1114026, 13), (1114033, 1), (1114091, 9), (1114092, 1), (1114093, 1), (1114094, 4), (1114095, 16), (1114096, 1), (1114097, 1), (1114098, 1), (1114099, 4), (1114109, 5), (1114102, 4), (1114103, 7), (1114104, 2), (1114105, 6), (1114106, 3), (1114107, 1), (1114108, 7), (125, 4), (1114110, 1), (1114111, 1)]], [9, [(0, 8), (1, 1), (4, 4), (132, 2), (5, 2), (7, 3), (9, 9), (10, 4), (11, 1), (12, 1), (13, 9), (14, 5), (15, 3), (16, 5), (17, 2), (1114043, 18), (1114051, 1), (1114055, 1), (1114069, 2), (1114076, 1), (123, 1), (1114108, 8), (1114109, 1), (1114110, 2), (1114111, 2)]], [10, [(0, 6), (1, 6), (2, 2), (3, 1), (4, 6), (5, 4), (6, 11), (7, 4), (8, 1), (10, 1), (1114012, 3), (1114034, 16), (1114043, 1), (1114046, 3), (1114048, 1), (1114051, 1), (1114079, 1), (1114099, 6), (1114100, 2), (1114101, 1), (1114102, 1), (1114103, 7), (1114105, 2), (1114107, 2), (1114110, 3), (1114111, 4)]], [11, [(0, 7), (1, 4), (2, 2), (1114006, 3), (1114028, 13), (1114035, 1), (1114040, 3), (1114042, 1), (1114053, 1), (108, 1), (1114093, 9), (1114095, 1), (1114096, 1), (1114097, 6), (1114098, 1), (1114099, 2), (1114101, 6), (1114102, 4), (1114104, 2), (1114106, 7), (1114107, 6), (1114108, 2), (1114109, 1), (1114110, 2), (1114111, 10)]], [12, [(0, 5), (1, 5), (2, 3), (3, 2), (1114007, 6), (1114029, 14), (1114041, 1), (1114043, 1), (1114051, 1), (1114094, 3), (1114095, 1), (1114097, 2), (1114098, 7), (1114099, 2), (1114100, 2), (117, 1), (1114102, 1), (1114105, 7), (1114106, 2), (1114107, 5), (1114108, 10), (1114109, 3), (1114110, 1), (1114111, 11)]], [13, [(0, 13), (7, 1), (12, 2), (14, 1), (151, 1), (25, 1), (27, 1), (33, 1), (39, 1), (54, 1), (192, 2), (65, 4), (67, 5), (68, 1), (69, 10), (71, 1), (72, 1), (201, 1), (76, 2), (77, 2), (78, 5), (79, 4), (80, 5), (81, 2), (82, 10), (83, 9), (84, 2), (85, 2), (211, 2), (86,

```
1), (1114090, 2)]]]
```

Mirem quina és la màxima freqüència amb què apareix algun caràcter en cada bloc.

In [10]:
```
u=[transpose(matrix(fr[v][1])) for v in range(14)]
```

In [11]:
```
[max(u[v][1]) for v in range(14)]
```

Out[11]:
```
[16, 15, 16, 17, 19, 20, 18, 22, 16, 18, 16, 13, 14, 13]
```

A fi de saber quin és el caràcter més freqüent de cada bloc, que, probablement, es correspondrà amb l'espai blanc, o sigui, el de codi 32, mirem a on apareix per primer cop el caràcter de cada bloc que apareix més sovint; després mirem quin és.

In [12]:
```
[list(u[v][1]).index(max(u[v][1])) for v in range(14)]
```

Out[12]:
```
[21, 17, 12, 16, 5, 0, 17, 0, 8, 15, 11, 4, 5, 0]
```

In [13]:
```
ClauXifratge=[((u[v][0][list(u[v][1]).index(max(u[v][1]))] -32) %
```

In [14]:
```
print(ClauXifratge)
```

```
[1114026, 1114011, 1114004, 1114011, 1113997, 1114080, 1114011, 111
4080, 1114063, 1114011, 1114002, 1113996, 1113997, 1114080]
```

Si fem el complementari a 1114112, i sumem 32, obtindrem (el complementari de) la clau estimada, o sigui, el començament del text pla.

In [15]:
```
[(32-u[v][0][list(u[v][1]).index(max(u[v][1]))])%1114112 for v in
```

Out[15]:
```
[86, 101, 108, 101, 115, 32, 101, 32, 49, 101, 110, 116, 115, 32]
```

In [16]:
```
ClauEstimada=""
```

In [17]:
```
for v in range(14):
    ClauEstimada=ClauEstimada+chr((32-u[v][0][list(u[v][1]).index
```

In [18]:
```
ClauEstimada
```

Out[18]:
```
'Veles e 1ents '
```

In [19]:
```
[ord(v) for v in ClauEstimada]
```

Out[19]:
```
[86, 101, 108, 101, 115, 32, 101, 32, 49, 101, 110, 116, 115, 32]
```

Potser no sembla la més possible (el nombre "1" hi és estrany); de totes maneres, provem-la:

In [20]:
```
1 print(VigenereDX(TextXifrat,ClauXifratge))
```

```
Veles e 1ents han mos esigs complir(1969)
(Ausià. March - Raim*n)

Veles e v nts han mos d sigs complir,faent camins ubtosos per l m
ar.
Mestre $ ponent contr d'ells veig rmar;
xaloc, 'levant, los d uen subvenir
b llurs amicslo grec e lo (igjorn,
fent #umils precs a' vent tramuntnal
que en so) bufar los si parcial
e qu  tots cinc co(plesquen mon -etorn.

Bulli-à el mar com 'a cassola en !orn,
mudant c*lor e l'estatnatural,
e mo.trarà voler t*ta res mal
qu  sobre si atu- un punt al j*rn.
Grans e p*cs peixs a reors correran
  cercaran ama"atalls secret.:
fugint al mr, on són nod-its e fets,
p r gran remei  n terra eixirn.

Amor de v®s jo en sent (és que no en .é,
de què la +art pitjor men romandrà;
ede vós sap loqui sens vós  stà.
A joc dedaus vos acom+araré.

Io te( la mort per )o ser-vos abs nt,
perquè am*r per mort éslanul·lat:
masjo no creu qu  mon voler sorat
pusca ess r per tal deprtiment.
Jo s® gelós de vos/re escàs vole-,
que, jo mor$nt, no meta m$ en oblit.
So' est pensar m  tol del món elit,
car nósvivint, no cr u se pusca fe-:
aprés ma mo-t, d'amar perau poder,
e s$a tost en iraconvertit.
E,jo forçat d'a,uest món ser  ixit,
tot lo (eu mal serà v®s no veer.

A(or, de vós joen sent més q0e no en sé,
d  què la part +itjor me'n ro(andrà,
e de v®s sap lo qui .ens vós està:A joc de dausvos acomparar¤.
```

Efectivament, sembla que hi ha un caràcter erroni (el novè, en el lloc 8).

Canviem-lo. En lloc d'un "1" provem una "v". Per a això, és suficient canviar el valor del caràcter (complementari) de manera adient:

In [21]:
```
1 ClauNovaX='Veles e vents '
```

In [22]:
```
1 ClauNova=[ClauXifratge[v] for v in range(14)]
```

In [23]:
```
1 ClauNova[8]=ClauNova[8]-ord('v')+ord('1')
```

In [24]:
```
1 print(VigenereDX(TextXifrat,ClauNova))
```

```
Veles e vents han mos desigs complir (1969)
(Ausiàs March - Raimon)

Veles e vents han mos desigs complir,
faent camins dubtosos per la mar.
Mestre i ponent contra d'ells veig armar;
xaloc, llevant, los deuen subvenir
ab llurs amics lo grec e lo migjorn,
fent humils precs al vent tramuntanal
que en son bufar los sia parcial
e que tots cinc complesquen mon retorn.

Bullirà el mar com la cassola en forn,
mudant color e l'estat natural,
e mostrarà voler tota res mal
que sobre si atur un punt al jorn.
Grans e pocs peixs a recors correran
e cercaran amagatalls secrets:
fugint al mar, on són nodrits e fets,
per gran remei en terra eixiran
```

Efectivament, sembla que hem desxifrat correctament.

Fi de l'apèndix 1