Criptografia bàsica (1)
Exercici de desxifratge (solució)

Artur Travesa

(versió 2021-04)

Referències

Aquest notebook conté una solució de l'exercici proposat en el *notebook*
[Cripto- 1]*:* Travesa, A.: CriptografiaBasica-1 ; accessible en forma notebook o en format pdf des de https://travesa.cat/notes/

Criptosistema de Vigenère

Proporcionem en aquest *notebook* les funcions del tutorial.

Funcions per al criptosistema de Vigenère

(a)

In[1]:=
```
VigenereX[missatge_, clau_] := Module[{b = 2^16},
  lta = If[Head[missatge] === List, missatge,
    If[Head[missatge] === String, ToCharacterCode[missatge],
     Print["El missatge ha de ser una tira de caràcters o bé una llista de codis"];
     Return[]]]; cc = If[Head[clau] === List, clau,
    If[Head[clau] === String, ToCharacterCode[clau], Print[
      "La clau ha de ser una tira de caràcters o bé una llista de codis"]; Return[]]];
  longclau = Length[cc];
  Table[Mod[lta[[i]] + cc[[Mod[i, longclau, 1]]], b], {i, 1, Length[lta]}]
 ]
```

(b)

In[2]:=
```
VigenereDX[missatge_, clau_] := Module[{b = 2^16},
  lta = If[Head[missatge] === List, missatge,
    If[Head[missatge] === String, ToCharacterCode[missatge],
     Print["El missatge ha de ser una tira de caràcters o bé una llista de codis"];
     Return[]]]; cc = If[Head[clau] === List, clau,
    If[Head[clau] === String, ToCharacterCode[clau], Print[
      "La clau ha de ser una tira de caràcters o bé una llista de codis"]; Return[]]];
  longclau = Length[cc];
  FromCharacterCode[
   Table[Mod[lta[[i]] - cc[[Mod[i, longclau, 1]]], b], {i, 1, Length[lta]}]]
 ]
```

Exercici

- **Exercici**

  La llista següent, **TextXifrat**, correspon a un missatge xifrat amb el criptosistema de Vigenère. No en coneixem ni 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 = {0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 18, 65532, 2, 65467, 65530, 79, 14, 0,
   65518, 0, 5, 65525, 65524, 83, 65482, 65534, 3, 8, 65533, 76, 4, 82, 65450, 65475,
   65475, 65477, 65475, 25, 65491, 65445, 65468, 65500, 2, 83, 4, 192, 65533, 65467,
   65503, 65517, 65535, 67, 18, 65467, 65473, 65467, 65503, 65, 4, 77, 65529, 9, 65467,
   65430, 65431, 54, 15, 7, 65529, 14, 65453, 69, 65467, 86, 65519, 9, 6, 65535, 65453,
   72, 11, 9, 65460, 8, 65532, 83, 65467, 68, 65519, 14, 65531, 65523, 0, 0, 13, 10,
   1, 11, 65529, 73, 13, 12, 65428, 1, 65523, 65521, 65531, 84, 65482, 65534, 65525,
   8, 65526, 78, 14, 0, 65518, 16, 65524, 0, 65532, 83, 25, 14, 65460, 11, 65522, 82,
   65467, 76, 65515, 65467, 65535, 65517, 65535, 14, 65460, 65512, 65529, 14, 1, 82,
   0, 0, 65523, 65467, 2, 65531, 65531, 69, 24, 15, 65460, 65534, 65532, 78, 15, 82,
   65515, 65467, 65526, 65459, 65522, 76, 22, 14, 65460, 17, 65522, 73, 2, 0, 65515,
   13, 65535, 65517, 65535, 27, 65460, 19, 65525, 7, 65532, 67, 65479, 0, 65526, 7,
   65527, 2, 65518, 78, 30, 65479, 65460, 7, 65532, 83, 65467, 68, 65519, 16, 65527,
   65530, 65453, 83, 31, 65533, 10, 0, 65531, 73, 13, 65514, 65515, 65533, 65458, 65528,
   65529, 85, 28, 14, 65460, 65532, 65530, 73, 65534, 83, 65450, 7, 1, 65452, 65524,
   82, 15, 65534, 65460, 0, 65453, 76, 10, 0, 65527, 4, 65529, 65526, 65532, 82, 24,
```

```
65 479, 65 438, 1, 65 522, 78, 15, 0, 65 522, 16, 65 535, 65 525, 65 529, 83, 65 482, 11,
6, 0, 65 520, 83, 65 467, 65, 65 526, 65 467, 8, 65 521, 65 531, 84, 65 482, 15, 6, 65 532,
65 530, 85, 9, 84, 65 515, 9, 65 523, 65 528, 65 431, 81, 31, 0, 65 460, 0, 65 531, 0, 14,
79, 65 528, 65 467, 65 524, 1, 65 523, 65, 28, 65 467, 0, 10, 0, 0, 14, 73, 65 515, 65 467,
2, 65 517, 65 535, 67, 19, 65 532, 0, 65 445, 65 522, 0, 12, 85, 65 519, 65 467, 6, 65 531,
1, 83, 65 482, 65 534, 65 533, 9, 65 520, 0, 65 534, 79, 65 527, 11, 65 534, 65 521, 0,
81, 31, 0, 2, 65 467, 65 530, 79, 9, 0, 65 532, 0, 6, 65 531, 65 535, 78, 65 496, 65 445,
65 438, 65 501, 2, 76, 7, 73, 65 532, 123, 65 458, 65 521, 65 529, 0, 23, 65 532, 6, 65 467,
65 520, 79, 8, 0, 65 526, 65 532, 65 458, 65 519, 65 518, 83, 29, 10, 0, 65 532, 65 453, 69,
9, 0, 65 520, 10, 4, 65 530, 65 465, 65 514, 23, 16, 65 528, 65 532, 65 531, 84, 65 467,
67, 65 529, 7, 1, 65 534, 65 453, 69, 65 482, 7, 65 467, 0, 0, 84, 65 532, 84, 65 450, 9,
65 523, 0, 2, 82, 11, 7, 65 472, 65 445, 65 522, 0, 8, 79, 65 533, 15, 4, 65 517, 65 535,
192, 65 482, 17, 3, 7, 65 522, 82, 65 467, 84, 65 529, 15, 65 523, 65 452, 65 535, 69,
29, 65 467, 1, 65 532, 65 529, 65 514, 12, 85, 65 519, 65 467, 5, 65 531, 65 519, 82, 15,
65 467, 7, 4, 65 453, 65, 15, 85, 65 532, 65 467, 7, 65 530, 65 453, 80, 31, 9, 8, 65 467,
65 518, 76, 65 467, 74, 65 529, 13, 0, 65 466, 65 431, 39, 28, 65 532, 2, 14, 65 453, 69,
65 467, 80, 65 529, 65 534, 5, 65 452, 65 533, 69, 19, 19, 7, 65 467, 65 518, 0, 13, 69,
65 517, 10, 4, 65 535, 65 453, 67, 25, 13, 6, 0, 65 535, 65, 9, 65 514, 65 519, 65 467,
65 525, 65 521, 65 535, 67, 11, 13, 65 525, 9, 65 453, 65, 8, 65, 65 521, 65 532, 6, 65 517,
65 529, 76, 29, 65 467, 7, 0, 65 520, 82, 0, 84, 65 533, 65 493, 65 436, 65 522, 2, 71,
19, 9, 8, 65 467, 65 518, 76, 65 467, 77, 65 515, 13, 65 470, 65 452, 65 532, 78, 65 482,
14, 135, 9, 65 453, 78, 10, 68, 65 532, 4, 6, 65 535, 65 453, 69, 65 482, 1, 65 529, 15,
0, 12, 65 445, 80, 65 519, 13, 65 458, 65 523, 65 535, 65, 24, 65 467, 6, 0, 65 530, 69,
4, 0, 65 519, 9, 65 458, 0, 65 522, 82, 28, 65 532, 65 460, 0, 65 526, 88, 4, 82, 65 515,
9, 65 472, 65 430, 65 431, 33, 23, 10, 6, 65 467, 65 521, 69, 65 467, 86, 125, 14, 65 458,
65 526, 65 532, 0, 15, 9, 65 460, 14, 65 522, 78, 15, 0, 65 527, 132, 5, 65 452, 65 534,
85, 15, 65 467, 2, 10, 65 453, 69, 9, 0, 65 533, 132, 65 470, 65 430, 65 521, 69, 65 482,
12, 9, 131, 65 453, 76, 65 532, 0, 65 530, 65 532, 4, 0, 65 453, 80, 19, 15, 65 534, 10,
65 535, 0, 8, 69, 65 457, 9, 65 458, 65 534, 65 532, 77, 11, 9, 65 528, 13, 109, 27,
65 445, 69, 65 450, 65 535, 65 527, 65 452, 3, 211, 29, 65 467, 7, 65 532, 65 533, 0, 7,
79, 65 450, 12, 7, 65 525, 65 453, 83, 15, 9, 7, 65 467, 3, 211, 14, 0, 65 519, 14, 6, 108,
65 467, 65 514, 65 515, 65 467, 65 534, 10, 65 520, 0, 65 535, 69, 65 450, 65 535, 65 523,
1, 0, 0, 32, 10, 7, 65 467, 65 518, 67, 10, 77, 65 530, 65 532, 4, 65 517, 65 535, 201,
```

```
65496, 65445, 65438, 65508, 65532, 0, 15, 69, 65527, 65467, 65534, 65517, 65453,
77, 25, 13, 8, 65467, 65533, 69, 13, 0, 65528, 10, 65458, 65535, 65522, 82, 65495,
17, 3, 14, 65453, 65, 65533, 83, 65519, 9, 6, 65464, 65431, 80, 15, 13, 5, 16, 117,
0, 65532, 77, 65529, 13, 65458, 65532, 65522, 82, 65482, 8, 3, 13, 1, 0, 132, 83,
65450, 65532, 0, 1, 65529, 151, 22, 65532, 8, 65493, 65431, 77, 65532, 83, 65450, 5,
1, 65452, 65531, 79, 65482, 65534, 6, 0, 2, 0, 12, 85, 65519, 65467, 65535, 65531,
65531, 0, 32, 10, 0, 0, 65535, 0, 14, 79, 65516, 13, 65523, 0, 65431, 80, 31, 14,
65527, 65532, 65453, 69, 14, 83, 65519, 13, 65458, 65532, 65522, 82, 65482, 15,
65525, 7, 65453, 68, 0, 80, 65515, 13, 6, 65525, 65530, 69, 24, 15, 65474, 65445,
65495, 79, 65467, 83, 125, 65467, 65529, 65521, 65529, 211, 29, 65467, 65528, 0,
65453, 86, 10, 83, 65534, 13, 65527, 65452, 65522, 83, 13, 123, 7, 65467, 3, 79,
7, 69, 65532, 65479, 65436, 65533, 2, 69, 65494, 65467, 65534, 10, 65453, 77, 10,
82, 65523, 9, 6, 65464, 65453, 78, 25, 65467, 1, 0, 1, 65, 65467, 77, 65523, 65467,
65527, 65530, 65453, 79, 12, 7, 65533, 15, 65467, 65514, 65518, 79, 65526, 65467,
65527, 65535, 1, 0, 26, 0, 2, 14, 65518, 82, 65467, 77, 65519, 65467, 6, 65531,
65529, 0, 14, 0, 0, 65467, 65530, 211, 9, 0, 65518, 0, 65534, 65525, 1, 12, 65460,
65534, 65525, 13, 65453, 78, 142, 83, 65450, 17, 65531, 2, 65526, 78, 30, 65479,
65460, 9, 65532, 0, 65534, 82, 65519, 16, 65458, 65535, 65522, 0, 26, 16, 7, 65534,
65518, 0, 1, 69, 65532, 65493, 65436, 65517, 65533, 82, 147, 14, 65460, 8, 65518,
0, 8, 79, 65532, 15, 65470, 65452, 65521, 7, 11, 8, 65525, 13, 65453, 80, 0, 82,
65518, 65532, 7, 65452, 65533, 79, 14, 0, 6, 65479, 65431, 69, 65467, 83, 65523,
65532, 65458, 0, 65532, 83, 30, 65467, 65529, 9, 65453, 73, 13, 65, 65450, 65534,
1, 65530, 3, 69, 28, 15, 65533, 15, 65467, 65514, 65504, 12, 65450, 5, 1, 65452,
65523, 79, 28, 130, 65525, 15, 65453, 68, 65474, 65, 65531, 16, 65527, 65535, 1,
0, 23, 142, 2, 65467, 0, 69, 13, 0, 65519, 4, 10, 65525, 1, 12, 65460, 15, 3, 15,
65453, 76, 10, 0, 65527, 0, 7, 65452, 65530, 65, 22, 65467, 7, 0, 65535, 192, 65467,
86, 125, 14, 65458, 65530, 65532, 0, 32, 0, 65529, 13, 65467, 65514, 65445, 33,
65527, 10, 4, 65464, 65453, 68, 15, 65467, 10, 142, 0, 0, 5, 79, 65450, 0, 0, 65452,
0, 69, 24, 15, 65460, 8, 118, 83, 65467, 81, 65535, 0, 65458, 65530, 65532, 0, 15,
9, 65460, 14, 118, 12, 65445, 68, 65519, 65467, 3, 1, 117, 0, 22, 65532, 65460, 11,
65518, 82, 15, 0, 65530, 4, 6, 65526, 65532, 82, 65482, 8, 65529, 65474, 65531, 0,
13, 79, 65527, 65532, 0, 65520, 65535, 192, 65494, 65445, 65529, 65467, 65521,
69, 65467, 86, 125, 14, 65458, 65535, 65518, 80, 65482, 7, 3, 65467, 65534, 85, 4,
```

```
0, 65533, 0, 0, 65535, 65453, 86, 157, 14, 65460, 0, 0, 84, 123, 26, 65428, 65500,
65458, 65526, 65532, 67, 65482, 65535, 65529, 65467, 65521, 65, 16, 83, 65450,
17, 1, 65535, 65453, 65, 13, 10, 1, 11, 65518, 82, 65532, 82, 115, 65481, 65458};
```

Solució de l'exercici

Ens imaginem que la paraula clau estarà formada pels 14 caràcters complementaris (a 65536) dels primers 14 del text pla, a fi que tots es xifrin igual... Això faria que la clau fos de 14 caràcters. Ho provarem. Comencem per trencar el missatge en els 14 missatges que s'han xifrat amb un Cèsar cadascun.

In[4]:=
```
blocs = Transpose[Partition[TextXifrat, 14]];
```

Siguin $a_1,...,a_{14}$ els primers caràcters del text pla; llavors, la clau de xifratge és $x_1,...,x_{14}$ de manera que x_i=65536- a_i.

In[5]:=
```
ToCharacterCode["AZaz "]
```

Out[5]=
```
{65, 90, 97, 122, 32}
```

O sigui, que, majoritàriament, els codis dels caràcters a_i pertanyen als intervals **[65,90]** o bé **[97,122]**; i potser algun altre caràcter: espai blanc=32, lletres accentuades,...

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

In[6]:=
```
fr = Table[
  {j, Table[{i, Count[Mod[blocs[[j]], 65536], i]}, {i, Union[blocs[[j]]]}]}, {j, 1, 14}]
```

Out[6]=
```
{{1, {{0, 1}, {11, 5}, {12, 1}, {13, 2}, {14, 2}, {15, 9}, {18, 2}, {19, 4},
   {22, 4}, {23, 4}, {24, 5}, {25, 4}, {26, 2}, {28, 6}, {29, 5}, {30, 3}, {31, 5}, {32, 3}, {147, 1},
   {157, 1}, {65460, 4}, {65482, 16}, {65491, 1}, {65494, 2}, {65495, 1}, {65496, 2}, {65515, 1}}},
 {2, {{0, 7}, {1, 1}, {7, 5}, {8, 3}, {9, 7}, {10, 5}, {11, 1}, {12, 1}, {13, 4}, {14, 7}, {15, 8},
   {16, 2}, {17, 2}, {19, 2}, {123, 1}, {130, 1}, {142, 1}, {65445, 4}, {65467, 15},
   {65479, 3}, {65512, 1}, {65532, 7}, {65533, 1}, {65534, 6}, {65535, 1}}}, {3,
  {{0, 6}, {1, 3}, {2, 6}, {3, 6}, {5, 1}, {6, 8}, {7, 9}, {8, 4}, {9, 1}, {10, 2}, {135, 1}, {65438, 3}, {65460, 16}, {65467, 1},
   {65468, 1}, {65472, 1}, {65473, 1}, {65474, 1}, {65525, 7}, {65527, 1}, {65528, 3}, {65529, 8}, {65533, 3}, {65534, 3}}},
 {4, {{0, 16}, {1, 1}, {4, 1}, {7, 4}, {8, 5}, {9, 5}, {10, 5}, {11, 3}, {13, 5}, {14, 7}, {15, 5},
   {16, 1}, {17, 1}, {131, 1}, {142, 1}, {65445, 3}, {65467, 17}, {65474, 1}, {65479, 1},
   {65493, 1}, {65500, 1}, {65501, 1}, {65508, 1}, {65532, 7}, {65534, 2}}},
 {5, {{0, 7}, {1, 3}, {2, 3}, {3, 2}, {109, 1}, {117, 1}, {118, 2}, {65431, 2}, {65453, 19}, {65467, 3},
   {65495, 1}, {65503, 1}, {65518, 8}, {65520, 5}, {65521, 3}, {65522, 7}, {65526, 2},
   {65529, 2}, {65530, 6}, {65531, 4}, {65532, 6}, {65533, 3}, {65534, 1}, {65535, 4}}},
 {6, {{0, 20}, {12, 2}, {27, 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}, {86, 1}, {88, 1}, {192, 1}, {211, 2}, {65514, 4}}},
 {7, {{0, 5}, {1, 1}, {2, 1}, {4, 6}, {5, 1}, {7, 3}, {8, 5}, {9, 6}, {10, 6}, {12, 3}, {13, 7}, {14, 7},
   {15, 6}, {16, 1}, {123, 1}, {132, 1}, {142, 1}, {65445, 4}, {65467, 18}, {65474, 1},
   {65479, 1}, {65504, 1}, {65518, 1}, {65532, 4}, {65533, 1}, {65534, 3}, {65535, 1}}},
 {8, {{0, 22}, {12, 2}, {26, 1}, {33, 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}, {192, 1}, {65514, 2}}},
 {9, {{0, 1}, {125, 4}, {65428, 2}, {65450, 13}, {65457, 1}, {65515, 9}, {65516, 1}, {65517, 1}, {65518, 4},
   {65519, 16}, {65520, 1}, {65521, 1}, {65522, 1}, {65523, 4}, {65526, 4}, {65527, 7}, {65528, 2},
   {65529, 6}, {65530, 3}, {65531, 1}, {65532, 7}, {65533, 5}, {65534, 1}, {65535, 1}}}, {10,
  {{0, 8}, {1, 1}, {4, 4}, {5, 2}, {7, 3}, {9, 9}, {10, 4}, {11, 1}, {12, 1}, {13, 9}, {14, 5}, {15, 3}, {16, 5}, {17, 2}, {123, 1},
   {132, 2}, {65467, 18}, {65475, 1}, {65479, 1}, {65493, 2}, {65500, 1}, {65532, 8}, {65533, 1}, {65534, 2}, {65535, 2}}},
 {11, {{0, 6}, {1, 6}, {2, 2}, {3, 1}, {4, 6}, {5, 4}, {6, 11}, {7, 4}, {8, 1}, {10, 1}, {65436, 3},
   {65458, 16}, {65467, 1}, {65470, 3}, {65472, 1}, {65475, 1}, {65503, 1}, {65523, 6}, {65524, 2},
   {65525, 1}, {65526, 1}, {65527, 7}, {65529, 2}, {65531, 2}, {65534, 3}, {65535, 4}}},
 {12, {{0, 7}, {1, 4}, {2, 2}, {108, 1}, {65430, 3}, {65452, 13}, {65459, 1}, {65464, 3}, {65466, 1},
   {65477, 1}, {65517, 9}, {65519, 1}, {65520, 1}, {65521, 6}, {65522, 1}, {65523, 2}, {65525, 6},
   {65526, 4}, {65528, 2}, {65530, 7}, {65531, 6}, {65532, 2}, {65533, 1}, {65534, 2}, {65535, 10}}},
 {13, {{0, 5}, {1, 5}, {2, 3}, {3, 2}, {117, 1}, {65431, 6}, {65453, 14}, {65465, 1}, {65467, 1},
   {65475, 1}, {65518, 3}, {65519, 1}, {65521, 2}, {65522, 7}, {65523, 2}, {65524, 2}, {65526, 1},
   {65529, 7}, {65530, 2}, {65531, 5}, {65532, 10}, {65533, 3}, {65534, 1}, {65535, 11}}},
 {14, {{0, 13}, {7, 1}, {12, 2}, {14, 1}, {25, 1}, {27, 1}, {33, 1}, {39, 1}, {54, 1}, {65, 4}, {67, 5},
   {68, 1}, {69, 10}, {71, 1}, {72, 1}, {76, 2}, {77, 2}, {78, 5}, {79, 4}, {80, 5}, {81, 2}, {82, 10},
   {83, 9}, {84, 2}, {85, 2}, {86, 1}, {151, 1}, {192, 2}, {201, 1}, {211, 2}, {65514, 2}}}}
```

El caràcter més freqüent potser hauria de ser l'espai en blanc; o sigui, el de codi 32. La diferència amb el codi del caràcter més freqüent hauria de ser el codi del caràcter corresponent de la clau. Provem-ho. Comencem pel primer bloc.

Escrivim en una matriu els (codis dels) caràcters i les freqüències.

In[7]:=
```
u = Transpose[fr[[1, 2]]]
```

Out[7]=
```
{{0, 11, 12, 13, 14, 15, 18, 19, 22, 23, 24, 25, 26, 28, 29, 30, 31, 32, 147, 157, 65460, 65482, 65491,
  65494, 65495, 65496, 65515}, {1, 5, 1, 2, 2, 9, 2, 4, 4, 4, 5, 4, 2, 6, 5, 3, 5, 3, 1, 1, 4, 16, 1, 2, 1, 2, 1}}
```

Mirem la freqüència del caràcter més freqüent.

In[8]:=
```
m = Max[u[[2]]]
```

Out[8]=
```
16
```

Mirem el codi del caràcter més freqüent.

In[9]:=
```
c = u[[1]][[Position[u[[2]], m][[1, 1]] ]]
```

Out[9]=
```
65482
```

Si suposem que el caràcter més freqüent hauria de ser l'espai en blanc, trobem quin és el codi del caràcter que correspon a la clau.

In[10]:=
```
x = Mod[32 - c, 65536]
```

Out[10]=
```
86
```

i el caràcter corresponent.

In[11]:=
```
lletra = FromCharacterCode[x]
```

Out[11]=
```
V
```

Intentem automatitzar el procés per a tots els blocs.

In[12]:=
```
Clauestimada = Table[Module[{u, m, cx, lletra},
    u = Transpose[fr[[i, 2]]];
    m = Max[u[[2]]];
    c = u[[1]][[Position[u[[2]], m][[1, 1]] ]];
    x = Mod[32 - c, 65536];
    lletra = FromCharacterCode[x]
   ], {i, 1, 14}]
```

Out[12]=
```
{V, e, l, e, s,  , e,  , 1, e, n, t, s,  }
```

Provem- ho:

In[13]:=
```
Clest = 65536 - Flatten[ToCharacterCode[Clauestimada]]
```

Out[13]=
```
{65450, 65435, 65428, 65435, 65421, 65504, 65435, 65504, 65487, 65435, 65426, 65420, 65421, 65504}
```

In[14]:=
```
text = VigenereDX[TextXifrat, Clest]
```

Out[14]=
```
Veles e 1ents han mos  esigscomplir■ (1969)
(Ausià. March – Raim⋆n)

Veles e v nts han mos d sigs complir,■faent  camins  ubtososper l  mar.
Mestre $ ponent contr  d'ells veig  rma
xaloc, 'levant, los d uen subvenir
 bllurs amics■lo  grec e lo (igjorn,
fent ⌗umils precs a' vent tramunt nal
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'estat■natural,
e mo.trarà voler t⋆ta res mal
qu  sobre si atu– un punt al j⋆rn.
Grans e p⋆cs peixs a re orscorreran
  cercaran ama"atalls secret.:
fugint al m  on són nod–its e fets,
p r gran remei  n terra eixir ¤

Amor de v®s jo en sent (és que no en .é,
de què la ⁺art pitjor me■n  romandrà;
e■de  vós sap lo■qui  sens vós  stà.
A joc de■daus  vos acom⁺araré.

Io te( la mort per )o ser–vos abs nt,
perquè am⋆r per mort és■anul·lat:
mas■jo  no creu qu  mon voler so rat
pusca ess r per tal dep rtiment
Jo s® gelós de vos/re escàs vole–,
que, jo mor$nt, no meta m$ en oblit.
So' est pensar m  tol del món  eli
car nós■vivint, no cr u se pusca fe–:
aprés ma mo–t, d'amar per aupoder,
e s$a tost en ira■convertit.
E,■jo  forçat d'a,uest món ser  ixit,
tot lo (eu mal serà v®s no veer.

A(or, de vós jo■en  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 daus■vos  acomparar¤.
```

Sembla que hi ha un caràcter equivocat a la clau...
Potser no és "l", sinó "v":

In[15]:=
```
textbo = VigenereDX[TextXifrat, 65 536 - ToCharacterCode["Veles e vents "]]
```

Out[15]=

```
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.

Amor de vós jo en sent més que no en sé,
de què la part pitjor me'n romandrà;
e de vós sap lo qui sens vós està.
A joc de daus vos acompararé.

Io tem la mort per no ser-vos absent,
perquè amor per mort és anul·lat:
mas jo no creu que mon voler sobrat
pusca esser per tal departiment.
Jo só gelós de vostre escàs voler,
que, jo morint, no meta mi en oblit.
Sol est pensar me tol del món delit,
car nós vivint, no creu se pusca fer:
aprés ma mort, d'amar perdau poder,
e sia tost en ira convertit.
E, jo forçat d'aquest món ser eixit,
tot lo meu mal serà vós no veer.

Amor, de vós jo en sent més que no en sé,
de què la part pitjor me'n romandrà,
e de vós sap lo qui sens vós està:
A joc de daus vos acompararé.
```

Efectivament, el caràcter més freqüent del nové bloc no correspon al caràcter blanc, sinó a la lletra "e" minúscula. Ho comprovem a continuació, a tall d'exemple. (Tot i que sembla que no calgui, perquè ja hem esbrinat la clau.)

In[16]:=
```
u = Transpose[fr[[9, 2]]]
```
Out[16]=
```
{{0, 125, 65428, 65450, 65457, 65515, 65516, 65517, 65518, 65519, 65520, 65521, 65522, 65523, 65526, 65527, 65528, 65529,
  65530, 65531, 65532, 65533, 65534, 65535}, {1, 4, 2, 13, 1, 9, 1, 1, 4, 16, 1, 1, 1, 4, 4, 7, 2, 6, 3, 1, 7, 5, 1, 1}}
```

In[17]:=
```
m = Max[u[[2]]]
```
Out[17]=
```
16
```

In[18]:=
```
c = u[[1]][[Position[u[[2]], m][[1, 1]] ]]
```
Out[18]=
```
65519
```

Mirem el codi que correspon a la lletra "e" minúscula.

In[19]:=
```
x = Mod[ToCharacterCode["e"] - c, 65536]
```
Out[19]=
```
{118}
```

In[20]:=
```
lletra = FromCharacterCode[x]
```
Out[20]=
```
v
```