

Iniciació a la Criptografia

Artur Travesa

(versió 2024-07)

Capítol 0. Codificació

0.0. Introducció

La idea bàsica que guia aquest primer capítol de les notes és descriure l'aplicació d'eines d'Aritmètica bàsica que són fonamentals per a les transmissions d'informació, xifrades o no.

I per a la transmissió d'informació, cal tenir en compte, en primer lloc, quin tipus de missatges es volen transmetre i com es poden transcriure de manera que se'n pugui fer un estudi i una manipulació raonablement còmodes; és a dir, com estan *codificats*.

Centrem, doncs, el contingut, en la descripció de la codificació bàsica que considerarem per als missatges.

0.1. Codificació de missatges

Sembla evident que la codificació dels missatges dependrà en gran manera de quin tipus de missatges es volen transmetre. Per exemple, és molt difícil pensar com un actor pot transmetre una olor, o una sensació tàctil, o un gust, o una emoció qualsevol, almenys, de manera exacta o, fins i tot, prou acurada, a algun altre.

Fins i tot, un missatge tan senzill (de dir) com "t'estimo", no es pot transmetre amb tota la seva profunditat sense la presència en directe de l'emissor i el receptor del missatge; en efecte, no només és la frase concreta, sinó la mirada, el to, el timbre de veu, i el context, per posar només un exemple, allò que fa que el missatge arribi completament al seu destinatari. I, fins i tot així, potser el missatge rebut no és exactament el missatge enviat! La "codificació" del missatge no és prou precisa perquè el missatge pugui arribar íntegrament al seu destinatari, tal com el vol transmetre l'emissor.

Observació. Per als missatges criptogràfics, això no és possible. En efecte, **CAL** que el missatge desxifrat sigui exactament igual que el missatge que es xifra; per tant, el codificador i el descodificador hauran de ser adequats a fi de fer això possible. En particular, això limitarà el tipus de missatge que es pot xifrar/desxifrar.

Doncs, sembla evident que cal que l'emissor disposi d'un "codificador" adaptat al tipus de missatge que vol transmetre, i que el destinatari disposi d'un "descodificador" adequat que recuperi el missatge enviat, si és que això és possible.

Per exemple, per a la transmissió oral d'informació, cal que l'emissor i el receptor disposin d'una llengua comuna per a la transmissió del missatge; en aquest cas, la llengua actua com a codificador i també com a descodificador del missatge. Notem, també, que, tot i així, el procés de codificació i descodificació no sempre aconsegueix una transmissió perfecta del missatge.

Però encara que els dos actors disposin d'aquesta llengua comuna, la transmissió del missatge no és xifrada; només és codificada. De fet, qualsevol altre actor que conegui aquesta llengua comuna podria descodificar el missatge i aquest no li seria críptic. És a dir, qualsevol actor que conegui el sistema de codificació del missatge el pot descodificar sense conèixer cap altra informació complementària. En aquest cas, no parlem de Criptografia, sinó només de Codificació.

I abans de fer críptics els missatges per a altres actors, cal que el missatge sigui codificat d'alguna manera adequada a la seva transmissió.

Per a començar un estudi matemàtic de la criptografia, cal concretar bé quin tipus de missatges podem tractar, a fi de poder-los codificar de manera adequada i, després, fer-los críptics a tercers actors.

Un dels fets bàsics que s'han de tenir presents, és que la codificació pot dependre molt del tipus de missatge que es vol transmetre. Per exemple, potser cal transmetre dades bancàries per a una transacció comercial (NIF, números de comptes corrents, números de targetes de crèdit, quantitats que cal transferir entre comptes diferents, etcètera), o bé cal transmetre informacions confidencials alfanumèriques en general (informes de seguiment de projectes, cartes de recomanació, sol·licituds de beques), o bé cal transmetre claus privades per a l'ús de certes funcions criptogràfiques (per exemple, en les comunicacions xifrades entre diferents ordinadors), etcètera.

Observació. Això obvia, clarament, quin és el procés bàsic de codificació al qual s'han de sotmetre prèviament els missatges. Per exemple, un text alfanumèric es codifica, sovint, amb un processador de textos concret, que li dóna una forma tal que qualsevol altre actor amb el mateix processador de textos el pot recuperar íntegrament; però potser no el pot recuperar amb un processador diferent. És conegut que per a evitar aquest tipus de problemes "d'incompatibilitat" entre els sistemes diferents, es poden fer servir formats de tipus estàndard. I, encara ens podem trobar amb més dificultats si volem tractar altres tipus de missatges; per exemple, de so, o d'imatge; o bé d'arxius executables en un determinat sistema operatiu.

0.1.0. Tipus de missatges

Actualment, la majoria de les comunicacions s'estableixen entre ordinadors, i les dades que cal transmetre són, sovint, arxius (de text, o executables, o multimèdia comprimits, o del tipus que sigui). Per tant, volem suposar, i ho farem sovint, que les dades que cal transmetre són successions de zeros i uns.

A fi de poder *simular* còmodament aquest fet, en aquest tutorial usarem les funcions incorporades `chr()` i `ord()`. Cal notar que *SageMath* usa els 1114112 codis numèrics Unicode, entre els valors 0 i $16^5 + 16^4 - 1 = 1114111 = 0x10ffff$, inclosos; o sigui en el

rang (en el tipus de dades de *SageMath*) $0 \leq \text{codi} < 1114112$.

Notem que es tracta només d'una *simulació*. En un cas real, caldria treballar directament sobre els bits (o, potser, sobre els bytes) de l'arxiu origen. En efecte, els diferents programaris *interpreten* d'alguna manera les successions de bits que constitueixen l'arxiu i ens el presenten visualment; però usualment no ens ensenyen la successió original de bits. De fet, nosaltres treballarem sobre aquesta *interpretació*.

0.2. La llista dels caràcters de *SageMath*: de codis a caràcters

0.2.0. Els caràcters ASCII

Els caràcters ASCII (American Standard Code for Information Interchange) imprimibles són els caràcters de codis entre el 32 (caràcter blanc=espai) i el 126 (títol). Fem-ne una llista.

```
In [1]: 1 print([[i,chr(i)] for i in range(32,127)])
```

```
[[32, ' '], [33, '!'], [34, '"'], [35, '#'], [36, '$'], [37, '%'], [38, '&'], [39, "'"], [40, '('], [41, ')'], [42, '*'], [43, '+'], [44, ','], [45, '-'], [46, '.'], [47, '/'], [48, '0'], [49, '1'], [50, '2'], [51, '3'], [52, '4'], [53, '5'], [54, '6'], [55, '7'], [56, '8'], [57, '9'], [58, ':'], [59, ';'], [60, '<'], [61, '='], [62, '>'], [63, '?'], [64, '@'], [65, 'A'], [66, 'B'], [67, 'C'], [68, 'D'], [69, 'E'], [70, 'F'], [71, 'G'], [72, 'H'], [73, 'I'], [74, 'J'], [75, 'K'], [76, 'L'], [77, 'M'], [78, 'N'], [79, 'O'], [80, 'P'], [81, 'Q'], [82, 'R'], [83, 'S'], [84, 'T'], [85, 'U'], [86, 'V'], [87, 'W'], [88, 'X'], [89, 'Y'], [90, 'Z'], [91, '['], [92, '\\'], [93, ']'], [94, '^'], [95, '_'], [96, '`'], [97, 'a'], [98, 'b'], [99, 'c'], [100, 'd'], [101, 'e'], [102, 'f'], [103, 'g'], [104, 'h'], [105, 'i'], [106, 'j'], [107, 'k'], [108, 'l'], [109, 'm'], [110, 'n'], [111, 'o'], [112, 'p'], [113, 'q'], [114, 'r'], [115, 's'], [116, 't'], [117, 'u'], [118, 'v'], [119, 'w'], [120, 'x'], [121, 'y'], [122, 'z'], [123, '{'], [124, '|'], [125, '}'], [126, '~']]
```

Abans dels caràcters ASCII imprimibles (del 0 al 31), i després (només el 127), hi ha els diferents caràcters ASCII de control; mirem-nos-els, i notem que *SageMath* ens en dóna una interpretació en format hexadecimal d'un sol byte, excepte dels codis *tabulador*, \t, *línia nova*, \n, i *retorn de carro*, \r.

```
In [2]: 1 print([[i,chr(i)] for i in range(0,32)]+[[127,chr(127)]])
```

```
[[0, '\x00'], [1, '\x01'], [2, '\x02'], [3, '\x03'], [4, '\x04'], [5, '\x05'], [6, '\x06'], [7, '\x07'], [8, '\x08'], [9, '\t'], [10, '\n'], [11, '\x0b'], [12, '\x0c'], [13, '\r'], [14, '\x0e'], [15, '\x0f'], [16, '\x10'], [17, '\x11'], [18, '\x12'], [19, '\x13'], [20, '\x14'], [21, '\x15'], [22, '\x16'], [23, '\x17'], [24, '\x18'], [25, '\x19'], [26, '\x1a'], [27, '\x1b'], [28, '\x1c'], [29, '\x1d'], [30, '\x1e'], [31, '\x1f'], [127, '\x7f']]
```


I per a valors més grans, hi ha caràcters interpretats en format unicode de 8 caràcters hexadecimals (per exemple, \U0001000c).

```
In [9]: 1 print([chr(v) for v in range(2^16,2^16+256)])  
['𐀀', '𐀁', '𐀂', '𐀃', '𐀄', '𐀅', '𐀆', '𐀇', '𐀈', '𐀉', '𐀊', '𐀋', '\U0001000c', '𐀌', '𐀍', '𐀎', '𐀏', '𐀐', '𐀑', '𐀒', '𐀓', '𐀔', '𐀕', '𐀖', '𐀗', '𐀘', '𐀙', '𐀚', '𐀛', '𐀜', '𐀝', '𐀞', '𐀟', '𐀠', '𐀡', '𐀢', '𐀣', '𐀤', '𐀥', '𐀦', '𐀧', '𐀨', '𐀩', '𐀪', '𐀫', '𐀬', '𐀭', '𐀮', '𐀯', '𐀰', '𐀱', '𐀲', '𐀳', '𐀴', '𐀵', '𐀶', '𐀷', '𐀸', '𐀹', '𐀺', '𐀻', '𐀼', '𐀽', '𐀾', '𐀿', '\U00010027', '𐀿', '𐁀', '𐁁', '𐁂', '𐁃', '𐁄', '𐁅', '𐁆', '𐁇', '𐁈', '𐁉', '𐁊', '𐁋', '𐁌', '𐁍', '𐁎', '𐁏', '𐁐', '𐁑', '𐁒', '𐁓', '𐁔', '𐁕', '𐁖', '𐁗', '𐁘', '𐁙', '𐁚', '𐁛', '𐁜', '𐁝', '𐁞', '𐁟', '𐁠', '𐁡', '𐁢', '𐁣', '𐁤', '𐁥', '𐁦', '𐁧', '𐁨', '𐁩', '𐁪', '𐁫', '𐁬', '𐁭', '𐁮', '𐁯', '𐁰', '𐁱', '𐁲', '𐁳', '𐁴', '𐁵', '𐁶', '𐁷', '𐁸', '𐁹', '𐁺', '𐁻', '𐁼', '𐁽', '𐁾', '𐁿', '\U0001003e', '𐂀', '𐂁', '𐂂', '𐂃', '𐂄', '𐂅', '𐂆', '𐂇', '𐂈', '𐂉', '𐂊', '𐂋', '𐂌', '𐂍', '𐂎', '𐂏', '𐂐', '𐂑', '𐂒', '𐂓', '𐂔', '𐂕', '𐂖', '𐂗', '𐂘', '𐂙', '𐂚', '𐂛', '𐂜', '𐂝', '𐂞', '𐂟', '𐂠', '𐂡', '𐂢', '𐂣', '𐂤', '𐂥', '𐂦', '𐂧', '𐂨', '𐂩', '𐂪', '𐂫', '𐂬', '𐂭', '𐂮', '𐂯', '𐂰', '𐂱', '𐂲', '𐂳', '𐂴', '𐂵', '𐂶', '𐂷', '𐂸', '𐂹', '𐂺', '𐂻', '𐂼', '𐂽', '𐂾', '𐂿', '\U0001004e', '\U0001004f', '𐃀', '𐃁', '𐃂', '𐃃', '𐃄', '𐃅', '𐃆', '𐃇', '𐃈', '𐃉', '𐃊', '𐃋', '𐃌', '𐃍', '𐃎', '𐃏', '𐃐', '𐃑', '𐃒', '𐃓', '𐃔', '𐃕', '𐃖', '𐃗', '𐃘', '𐃙', '𐃚', '𐃛', '𐃜', '𐃝', '𐃞', '𐃟', '𐃠', '𐃡', '𐃢', '𐃣', '𐃤', '𐃥', '𐃦', '𐃧', '𐃨', '𐃩', '𐃪', '𐃫', '𐃬', '𐃭', '𐃮', '𐃯', '𐃰', '𐃱', '𐃲', '𐃳', '𐃴', '𐃵', '𐃶', '𐃷', '𐃸', '𐃹', '𐃺', '𐃻', '𐃼', '𐃽', '𐃾', '𐃿', '\U0001005e', '\U0001005f', '\U00010060', '\U00010061', '\U00010062', '\U00010063', '\U00010064', '\U00010065', '\U00010066', '\U00010067', '\U00010068', '\U00010069', '\U0001006a', '\U0001006b', '\U0001006c', '\U0001006d', '\U0001006e', '\U0001006f', '\U00010070', '\U00010071', '\U00010072', '\U00010073', '\U00010074', '\U00010075', '\U00010076', '\U00010077', '\U00010078', '\U00010079', '\U0001007a', '\U0001007b', '\U0001007c', '\U0001007d', '\U0001007e', '\U0001007f', '𐄀', '𐄁', '𐄂', '𐄃', '𐄄', '𐄅', '𐄆', '𐄇', '𐄈', '𐄉', '𐄊', '𐄋', '𐄌', '𐄍', '𐄎', '𐄏', '𐄐', '𐄑', '𐄒', '𐄓', '𐄔', '𐄕', '𐄖', '𐄗', '𐄘', '𐄙', '𐄚', '𐄛', '𐄜', '𐄝', '𐄞', '𐄟', '𐄠', '𐄡', '𐄢', '𐄣', '𐄤', '𐄥', '𐄦', '𐄧', '𐄨', '𐄩', '𐄪', '𐄫', '𐄬', '𐄭', '𐄮', '𐄯', '𐄰', '𐄱', '𐄲', '𐄳', '𐄴', '𐄵', '𐄶', '𐄷', '𐄸', '𐄹', '𐄺', '𐄻', '𐄼', '𐄽', '𐄾', '𐄿', '\U000100fb', '\U000100fc', '\U000100fd', '\U000100fe', '\U000100ff']
```

Mirem-nos els darrers possibles (el darrer és \U0010ffff):


```
In [10]: 1 print([chr(v) for v in range(16^5+16^4-256,16^5+16^4)])
```

```
['\U0010ff00', '\U0010ff01', '\U0010ff02', '\U0010ff03', '\U0010ff04', '\U0010ff05', '\U0010ff06', '\U0010ff07', '\U0010ff08', '\U0010ff09', '\U0010ff0a', '\U0010ff0b', '\U0010ff0c', '\U0010ff0d', '\U0010ff0e', '\U0010ff0f', '\U0010ff10', '\U0010ff11', '\U0010ff12', '\U0010ff13', '\U0010ff14', '\U0010ff15', '\U0010ff16', '\U0010ff17', '\U0010ff18', '\U0010ff19', '\U0010ff1a', '\U0010ff1b', '\U0010ff1c', '\U0010ff1d', '\U0010ff1e', '\U0010ff1f', '\U0010ff20', '\U0010ff21', '\U0010ff22', '\U0010ff23', '\U0010ff24', '\U0010ff25', '\U0010ff26', '\U0010ff27', '\U0010ff28', '\U0010ff29', '\U0010ff2a', '\U0010ff2b', '\U0010ff2c', '\U0010ff2d', '\U0010ff2e', '\U0010ff2f', '\U0010ff30', '\U0010ff31', '\U0010ff32', '\U0010ff33', '\U0010ff34', '\U0010ff35', '\U0010ff36', '\U0010ff37', '\U0010ff38', '\U0010ff39', '\U0010ff3a', '\U0010ff3b', '\U0010ff3c', '\U0010ff3d', '\U0010ff3e', '\U0010ff3f', '\U0010ff40', '\U0010ff41', '\U0010ff42', '\U0010ff43', '\U0010ff44', '\U0010ff45', '\U0010ff46', '\U0010ff47', '\U0010ff48', '\U0010ff49', '\U0010ff4a', '\U0010ff4b', '\U0010ff4c', '\U0010ff4d', '\U0010ff4e', '\U0010ff4f', '\U0010ff50', '\U0010ff51', '\U0010ff52', '\U0010ff53', '\U0010ff54', '\U0010ff55', '\U0010ff56', '\U0010ff57', '\U0010ff58', '\U0010ff59', '\U0010ff5a', '\U0010ff5b', '\U0010ff5c', '\U0010ff5d', '\U0010ff5e', '\U0010ff5f', '\U0010ff60', '\U0010ff61', '\U0010ff62', '\U0010ff63', '\U0010ff64', '\U0010ff65', '\U0010ff66', '\U0010ff67', '\U0010ff68', '\U0010ff69', '\U0010ff6a', '\U0010ff6b', '\U0010ff6c', '\U0010ff6d', '\U0010ff6e', '\U0010ff6f', '\U0010ff70', '\U0010ff71', '\U0010ff72', '\U0010ff73', '\U0010ff74', '\U0010ff75', '\U0010ff76', '\U0010ff77', '\U0010ff78', '\U0010ff79', '\U0010ff7a', '\U0010ff7b', '\U0010ff7c', '\U0010ff7d', '\U0010ff7e', '\U0010ff7f', '\U0010ff80', '\U0010ff81', '\U0010ff82', '\U0010ff83', '\U0010ff84', '\U0010ff85', '\U0010ff86', '\U0010ff87', '\U0010ff88', '\U0010ff89', '\U0010ff8a', '\U0010ff8b', '\U0010ff8c', '\U0010ff8d', '\U0010ff8e', '\U0010ff8f', '\U0010ff90', '\U0010ff91', '\U0010ff92', '\U0010ff93', '\U0010ff94', '\U0010ff95', '\U0010ff96', '\U0010ff97', '\U0010ff98', '\U0010ff99', '\U0010ffa0', '\U0010ffa1', '\U0010ffa2', '\U0010ffa3', '\U0010ffa4', '\U0010ffa5', '\U0010ffa6', '\U0010ffa7', '\U0010ffa8', '\U0010ffa9', '\U0010ffaa', '\U0010ffab', '\U0010ffac', '\U0010ffad', '\U0010ffae', '\U0010ffaf', '\U0010ffb0', '\U0010ffb1', '\U0010ffb2', '\U0010ffb3', '\U0010ffb4', '\U0010ffb5', '\U0010ffb6', '\U0010ffb7', '\U0010ffb8', '\U0010ffb9', '\U0010ffba', '\U0010ffbb', '\U0010ffbc', '\U0010ffbd', '\U0010ffbe', '\U0010ffbf', '\U0010ffc0', '\U0010ffc1', '\U0010ffc2', '\U0010ffc3', '\U0010ffc4', '\U0010ffc5', '\U0010ffc6', '\U0010ffc7', '\U0010ffc8', '\U0010ffc9', '\U0010ffca', '\U0010ffcb', '\U0010ffcc', '\U0010ffcd', '\U0010ffce', '\U0010ffcf', '\U0010ffd0', '\U0010ffd1', '\U0010ffd2', '\U0010ffd3', '\U0010ffd4', '\U0010ffd5', '\U0010ffd6', '\U0010ffd7', '\U0010ffd8', '\U0010ffd9', '\U0010ffda', '\U0010ffdb', '\U0010ffdc', '\U0010ffdd', '\U0010ffde', '\U0010ffdf', '\U0010ffe0', '\U0010ffe1', '\U0010ffe2', '\U0010ffe3', '\U0010ffe4', '\U0010ffe5', '\U0010ffe6', '\U0010ffe7', '\U0010ffe8', '\U0010ffe9', '\U0010ffea', '\U0010ffeb', '\U0010ffec', '\U0010ffed', '\U0010ffee', '\U0010ffef', '\U0010fff0', '\U0010fff1', '\U0010fff2', '\U0010fff3', '\U0010fff4', '\U0010fff5', '\U0010fff6', '\U0010fff7', '\U0010fff8', '\U0010fff9', '\U0010fffa', '\U0010fffb', '\U0010fffc', '\U0010fffd', '\U0010fffe', '\U0010ffff']
```

Però si intentem veure'n un de posterior, obtenim un error (òbviament).

```
In [11]: 1 print(chr(16^5+16^4))

-----
-----
ValueError                                Traceback (most recent ca
ll last)
/tmp/ipykernel_29741/2710118598.py in <module>
----> 1 print(chr(Integer(16)**Integer(5)+Integer(16)**Integer(4)))

ValueError: chr() arg not in range(0x110000)
```

0.3. La llista dels caràcters de *SageMath*: de caràcters a codis

La funció `ord()` de *SageMath* proporciona el valor (decimal) del codi d'un caràcter. En cas de voler els codis d'un text, cal fer-ho caràcter a caràcter. Per tant, caldrà fer un petit programa.

```
In [12]: 1 llista=[ord(i) for i in "Llista de caràcters."]
          2 print(llista)

[76, 108, 105, 115, 116, 97, 32, 100, 101, 32, 99, 97, 114, 224, 99,
, 116, 101, 114, 115, 46]
```

Notem que el caràcter de codi més petit és l'espai (de codi 32), i que hi ha algun caràcter que no és ASCII (de codi 224), i que correspon a una vocal minúscula accentuada, à.

```
In [13]: 1 print([min(llista), max(llista)])

[32, 224]
```

Veiem quins codis numèrics tenen (en *SageMath*) les vocals accentuades:

```
In [14]: 1 vocals="ÀÁÂÃÈÉÊËÌÍÎÏÐÒÓÔÕÙÚÛÜàáâäèéêëìíîïðóôõùúü"
```

```
In [15]: 1 cc=[ord(v) for v in vocals]
          2 print(cc)

[192, 193, 194, 196, 200, 201, 202, 203, 204, 205, 206, 207, 210, 2
11, 212, 214, 217, 218, 219, 220, 224, 225, 226, 228, 232, 233, 234
, 235, 236, 237, 238, 239, 242, 243, 244, 246, 249, 250, 251, 252]
```

```
In [16]: 1 print([min(cc), max(cc)])

[192, 252]
```

Notem que les (nostres) vocals accentuades no esgoten la llista de codis (per exemple, quins caràcters corresponen al codis 195, 197, 198, 199, etcètera?. Fem la llista de tots els caràcters amb aquests codis:

```
In [17]: 1 ll=""
         2 for v in range(192,253):
         3     ll=ll+chr(v)
         4 print(ll)
```

ÀÁÂÃÄÅÆÇÈÉÊËÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâãäåæçèéêëìíîïðñòóôõö÷øùúü

0.4. Les funcions Codis(text) i Caracters(codis)

Es tracta de definir una funció Codis(text) que, aplicada a una tira de caràcters, text, en proporioni la llista de codis numèrics.

I també, definir una funció inversa, Caracters(codis) que, aplicada a una llista de codis en proporioni la tira de caràcters de la qual prové.

Observació. A fi que la llista sigui de codis, els elements de la llista han de ser del rang $0 \leq \text{codi} < m := 11141112$; però, en algun dels usos posteriors, la llista podria contenir valors fora d'aquest rang. A fi d'estalviar-nos feina i no fer una programació més feixuga (hauríem de comprovar que els codis són correctes i proporcionar, si cal, missatges d'error), ens limitarem a prendre el residu de la divisió per m de cadascun dels elements de la llista.

0.4.0. La funció Codis(text)

```
In [18]: 1 def Codis(text):
         2     return [ord(i) for i in text]
```

0.4.1. La funció Caracters(codis)

```
In [19]: 1 def Caracters(codis):
         2     m=11141112
         3     cars=""
         4     for i in range(len(codis)):
         5         cars=cars+chr(codis[i]%m)
         6     return cars
```

0.4.2. Exemples

Es tracta de comprovar en alguns exemples que les funcions són inverses l'una de l'altra (per a valors del rang $0 \leq \text{codi} < m$).

0.4.2.0.

```
In [20]: 1 text="Un text de prova."
         2 print(text)
```

Un text de prova.

```
In [21]: 1 codis=Codis(text)
         2 print(codis)

[85, 110, 32, 116, 101, 120, 116, 32, 100, 101, 32, 112, 114, 111,
118, 97, 46]
```

```
In [22]: 1 retext=Caracters(codis)
         2 print(retext)

Un text de prova.
```

```
In [23]: 1 text==retext

Out[23]: True
```

Notem, a continuació, que per a valors fora del rang, les funcions no són (no ho poden ser) inverses l'una de l'altra: la composició Codis(Caracters(lta1)) no és la identitat sobre lta1.

```
In [24]: 1 lta1=[65,65+1114112]
         2 print(lta1)

[65, 1114177]
```

```
In [25]: 1 txt1=Caracters(lta1)
         2 print(txt1)

AA
```

```
In [26]: 1 lta2=Codis(txt1)
         2 print(lta2)

[65, 65]
```

```
In [27]: 1 lta2==lta1

Out[27]: False
```

```
In [28]: 1 Codis(Caracters(lta1))==lta1

Out[28]: False
```

0.4.2.1.

Descodifiquem la llista següent de caràcters: [69, 102, 101, 99, 116, 105, 118, 97, 109, 101, 110, 116, 44, 32, 110, 111, 109, 233, 115, 32, 99, 97, 108, 105, 97, 32, 97, 112, 108, 105, 99, 97, 114, 45, 108, 105, 32, 108, 97, 32, 102, 117, 110, 99, 105, 243, 32, 67, 97, 114, 97, 99, 116, 101, 114, 115, 40, 32, 41].

```
In [29]: 1 lta=[69, 102, 101, 99, 116, 105, 118, 97, 109, 101, 110, 116, 44
```

```
In [30]: 1 Caracters(lta)

Out[30]: 'Efectivament, només calia aplicar-li la funció Caracters( )'
```

Fi del capítol 0