Criptografia bàsica (1)

Artur Travesa

(versió 2021-04)

Introducció general

L'origen d'aquestes notes es remunta a diferents cursos d'Aritmètica o de Criptografia, a càrrec de l'autor, per a estudiants de Matemàtiques o d'Informàtica de la Universitat de Barcelona.

La idea bàsica és descriure algunes aplicacions importants de l'Aritmètica bàsica (diguem, de nivell de primer curs) a les transmissions xifrades d'informació.

En cap cas es tracta d'un curs de Criptografia, que caldria encabir en espais més amplis de coneixements, que haurien d'incloure, probablement, parts de teoria de la comunicació, de complexitat algorítmica o computacional, d'aprenentatge automàtic, o d'estudi de teories de compartició de secrets, entre d'altres.

El format triat per a la presentació és el d'un *notebook* de *Mathematica*, per la facilitat que té aquest programari per a poder desenvolupar els càlculs no trivials de manera prou senzilla i entenedora, d'una banda, i per a permetre fer una presentació escrita prou raonable des del punt de vista de material escrit, de l'altra. En particular, la possibilitat d'incloure els càlculs dins del text de manera natural en fan una bona eina comunicativa i, alhora, facilita molt el càlcul amb exemples no trivials.

A fi de veure tot el contingut del *notebook* convé executar-lo. Això es pot fer de cop o bé, més recomanable, cel·la a cel·la a mesura que s'avança en la lectura i comprensió dels diferents continguts.

Observació: Per al cas en què no es disposi del programari, hi ha la versió executada del *notebook* en format pdf.

Amb la finalitat doble d'una banda, de no fer textos molt llargs o amb molts continguts, i de l'altra de poder ampliar de manera senzilla els continguts que s'hi tractin, el material s'ha dividit en diferents *notebooks*, que desrivim a continuació, en l'apartat de referències.

Referències

[Cripto- 1]: **Criptografia bàsica (1)**.
Travesa, A.: CriptografiaBasica-1; accessible en forma *notebook* o en format pdf des de https://travesa.cat/notes/
Contingut: Una iniciació a la codificació de missatges. El criptosistema de Cèsar. El criptosistema de Vigenère.

[Cripto- 2]: **Criptografia bàsica (2)**.
Travesa, A.:CriptografiaBasica-2; accessible en forma *notebook* o en format pdf des de https://travesa.cat/notes/
Contingut: Els criptosistemes lineals. Els criptosistemes afins. Sufixació de missatges. Farciment de missatges.

[Eratostenes]: **Un garbell d'Eratòstenes.**
Travesa, A.: Eratostenes; accessible en forma *notebook* o en format pdf des de https://travesa.cat/notes/
Contingut: Un garbell d'Eratòstenes.

[Cripto- 3]: **Primeritat. Construcció de primers**.
Travesa, A.:ConstruccioDePrimers; accessible en forma *notebook* o en format pdf des de https://travesa.cat/notes/
Contingut: Test de primeritat de Solovay-Strassen. Test de primeritat de Miller-Rabin. Un certificat congruencial de primeritat. Construcció certificada de nombres primers de mida prefixada. Aplicació al càlcul de claus RSA. Aplicació (exercici) al càlcul de claus ElGamal.

[Cripto- 4]: **Factorització**.
Travesa, A.: Factoritzacio; accessible en forma *notebook* o en format pdf des de https://travesa.cat/notes/
Contingut: Un garbell d'Eratòstenes. Tests de primeritat de Solovay-Strassen i de Miller-Rabin. Un certificat congruencial de primeritat. Un algoritme bàsic de divisó per nombres primers petits. Un algoritme bàsic de divisó per nombres petits. El mètode de factorització de Fermat. El mètode de factorització p-1 de Pollard. El mètode de factorització rho de Pollard.

[RSA]: **Criptosistemes de tipus RSA**.
Travesa, RSA; accessible en forma *notebook* o en format pdf des de https://travesa.cat/notes/
Contingut: Una descripció bàsica dels criptosistemes de tipus RSA: les claus; xifratge; desxifratge; observacions sobre la seguretat.

[ElGamal]: **El criptosistema ElGamal**.
Travesa, A.: ElGamal; accessible en forma *notebook* o en format pdf des de https://travesa.cat/notes/
Contingut: Logaritmes discrets. Una descripció bàsica del criptosistema ElGamal: el grup cíclic; les claus; xifratge i desxifratge.

[Tr-1]: Travesa, A.: *Aritmetica*. Edicions de la Universitat de Barelona, col·lecció UB, n. 25. Barcelona, 1998. ISBN:84-8338-031-5.

1. Introducció

Entendrem per criptografia la disciplina que estudia l'intercanvi d'informació de manera que només l'entitat emissora i la destinatària (que no cal confondre amb la receptora) puguin conèixer aquesta informació.

Així, doncs, en aquest estudi caldrà tenir en compte alguns actors importants. D'una banda, l'**emissor** del missatge; d'altra banda, el **destinatari** del missatge; i en tercer lloc, i molt important, els possibles **receptors** o **interceptors** del missatge. I encara cal tenir en compte altres possibles actors, sovint **atacants** actius, que intentin fer-se passar per l'emissor o pel destinatari del missatge a fi d'obtenir la informació confidencial.

Difícilment es podria estudiar criptografia científicament si no poguéssim manipular els missatges d'una manera coherent, mesurar el grau de dificultat dels processos de xifratge i de desxifratge dels missatges, o disposar d'eines per a construir (o destruir) criptosistemes cada cop més robustos.

A fi de mostrar la potència de les matemàtiques i, en particular, de l'Aritmètica, en aquestes qüestions, començarem amb un estudi elemental dels criptosistemes clàssics, i veurem que podem permetre'ns assegurar que la majoria d'aquests criptosistemes clàssics són realment molt febles. De fet, això fa que cap d'ells no sigui emprat en l'actualitat.

Més endavant veurem altres criptosistemes que encara es fan servir de manera habitual en el moment d'escriure aquest tutorial, però que segurament deixaran de ser-ho en un futur més o menys proper, probablement substituïts per criptosistemes quàntics. Però no ens avancem en el temps, ni en aconteixements (futurs?).

2. Codificació de missatges

Introducció

Un dels fets bàsics que cal tenir presents en criptografia és la **codificació** dels missatges; i això pot dependre molt del tipus de missatges que cal 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.

En les comunicacions entre ordinadors, les dades que cal transmetre són, sovint, arxius (de text, o executables, o del tipus que sigui). Per tant, volem suposar, i ho fem, 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 **FromCharacterCode** i **ToCharacterCode**. Cal notar que *Mathematica* usa codis numèrics entre els valors 0 i $2^{16}-1=65535$ (setze bits), però no els fa servir tots.

Exercici 1.1

(a) Què fan les funcions **FromCharacterCode** i **ToCharacterCode**? Quina és la seva sintaxi? Quins són els caràcters de codis entre 32 i 126?
(b) Quins codis numèrics tenen (en *Mathematica)* les vocals accentuades?
(c) Es demana descodificar 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, 70, 114, 111, 109, 67, 104, 97, 114, 97, 99, 116, 101, 114, 67, 111, 100, 101, 46}.
(d) ¿Quina diferència hi ha entre el missatge anterior i el missatge {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, 63425, 63433, 63432, 10, 83, 116, 121, 108, 101, 66, 111, 120, 91, 34, 97, 112, 108, 105, 99, 97, 114, 34, 44, 10, 70, 111, 110, 116, 83, 108, 97, 110, 116, 45, 62, 34, 73, 116, 97, 108, 105, 99, 34, 93, 63424, 63425, 63433, 63432, 10, 83, 116, 121, 108, 101, 66, 111, 120, 91, 34, 45, 34, 44, 10, 70, 111, 110, 116, 83, 108, 97, 110, 116, 45, 62, 34, 73, 116, 97, 108, 105, 99, 34, 93, 63424, 63425, 63433, 63432, 10, 83, 116, 121, 108, 101, 66, 111, 120, 91, 34, 108, 105, 34, 44, 10, 70, 111, 110, 116, 83, 108, 97, 110, 116, 45, 62, 34, 73, 116, 97, 108, 105, 99, 34, 93, 63424, 32, 108, 97, 32, 102, 117, 110, 99, 105, 243, 32, 70, 114, 111, 109, 67, 104, 97, 114, 97, 99, 116, 101, 114, 67, 111, 100, 101, 46}?
(e) Es demana descodificar el missatge següent: {76, 97, 32, 100, 105, 102, 101, 114, 232, 110, 99, 105, 97, 32, 233, 115, 32, 108, 97, 32, 112, 114, 101, 115, 232, 110, 99, 105, 97, 44, 32, 101, 110, 32, 101, 108, 32, 115, 101, 103, 111, 110, 32, 109, 105, 115, 115, 97, 116, 103, 101, 44, 32, 100, 101, 32, 108, 108, 101, 116, 114, 101, 115, 32, 99, 117, 114, 115, 105, 118, 101, 115, 46}.

(a) (Una solució)

In[1]:=
```
?FromCharacterCode
```

```
FromCharacterCode[n] gives a string consisting of the character with integer code n.
FromCharacterCode[{n1, n2,  }] gives a string consisting of the sequence of characters with codes ni.
FromCharacterCode[{{n11, n12,  }, {n21,  },  }] gives a list of strings.
FromCharacterCode[  , "encoding"] uses the specified character encoding.  ≫
```

In[2]:=
```
? ToCharacterCode
```

```
ToCharacterCode["string"] gives a list of the integer codes corresponding to the characters in a string.
ToCharacterCode["string", "encoding"] gives integer codes according to the specified encoding.  ≫
```

In[3]:=
```
FromCharacterCode[Table[n, {n, 32, 126}]]
```

Out[3]=
```
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
```

Resposta: Són els caràcters ASCII imprimibles.

(b) (Una solució)

In[4]:=
```
ToCharacterCode["ÀÁÄÈÉËÌÍÏÒÓÖÙÚÜàáäèéëìíïòóöùúü"]
```

Out[4]=
```
{192, 193, 196, 200, 201, 203, 204, 205, 207, 210, 211, 214, 217,
 218, 220, 224, 225, 228, 232, 233, 235, 236, 237, 239, 242, 243, 246, 249, 250, 252}
```

Comprovem-ho (i una miqueta més).

In[5]:=
```
FromCharacterCode[Table[n, {n, 192, 255}]]
```

Out[5]=
```
ÀÁÂÃÄÅÆÇÈÉÊËÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâãäåæçèéêëìíîïðñòóôõö÷øùúûüýþÿ
```

(c) (Una solució)

In[6]:=
```
FromCharacterCode[{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, 70,
  114, 111, 109, 67, 104, 97, 114, 97, 99, 116, 101, 114, 67, 111, 100, 101, 46}]
```

Out[6]=
```
Efectivament, només calia aplicar-li la funció FromCharacterCode.
```

(d) (Una solució)

In[7]:=
```
FromCharacterCode[{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, 63425, 63433, 63432, 10, 83, 116, 121,
  108, 101, 66, 111, 120, 91, 34, 97, 112, 108, 105, 99, 97, 114, 34, 44, 10, 70, 111,
  110, 116, 83, 108, 97, 110, 116, 45, 62, 34, 73, 116, 97, 108, 105, 99, 34, 93, 63424,
  63425, 63433, 63432, 10, 83, 116, 121, 108, 101, 66, 111, 120, 91, 34, 45, 34, 44,
  10, 70, 111, 110, 116, 83, 108, 97, 110, 116, 45, 62, 34, 73, 116, 97, 108, 105, 99,
  34, 93, 63424, 63425, 63433, 63432, 10, 83, 116, 121, 108, 101, 66, 111, 120, 91, 34,
  108, 105, 34, 44, 10, 70, 111, 110, 116, 83, 108, 97, 110, 116, 45, 62, 34, 73, 116,
  97, 108, 105, 99, 34, 93, 63424, 32, 108, 97, 32, 102, 117, 110, 99, 105, 243, 32,
  70, 114, 111, 109, 67, 104, 97, 114, 97, 99, 116, 101, 114, 67, 111, 100, 101, 46}]
```

Out[7]=
Efectivament, només calia *aplicar-li* la funció FromCharacterCode.

(e) (Una solució)

In[8]:=
```
FromCharacterCode[{76, 97, 32, 100, 105, 102, 101, 114, 232, 110, 99, 105, 97, 32, 233, 115,
  32, 108, 97, 32, 112, 114, 101, 115, 232, 110, 99, 105, 97, 44, 32, 101, 110, 32, 101, 108,
  32, 115, 101, 103, 111, 110, 32, 109, 105, 115, 115, 97, 116, 103, 101, 44, 32, 100, 101,
  32, 108, 108, 101, 116, 114, 101, 115, 32, 99, 117, 114, 115, 105, 118, 101, 115, 46}]
```

Out[8]=
La diferència és la presència, en el segon missatge, de lletres cursives.

Exercici 1.2

(Aquest exercici no és estrictament necessari per a seguir el tutorial; és, doncs, opcional. La temàtica és, sobretot, per a nivell informatiu o per a usos més reals.)
A fi de simular millor un fitxer de dades, convé convertir els codis numèrics a successions de zeros i uns. I si tenim en compte que 65536=2^16, podem usar 16 bits per a escriure cadascun dels caràcters numèrics. Notem que això pot depen-dre del tipus de dades; per exemple, codificacions com utf-7 o utf-8 fan servir 6 o 8 o 16 o 32 o 64 bits.
(a) Es demana escriure una funció **Codifica** que, aplicada a un missatge alfanumèric, proporcioni, en una sola llista numèrica (i no en una llista de llistes), la seva codificació utilitzant setze caràcters (zeros i uns) per a cadascun dels codis numèrics que assigna *Mathematica*. Es demana també un exemple de codificació d'una frase curta.
(b) Es demana escriure una funció **Descodifica** inversa de l'anterior; cal que aquesta funció faci el control de si la quantitat de caràcters total és múltiple de setze; en cas que no ho sigui, cal afegir (**Prepend**) zeros al començament. Es demana descodificar la frase codificada anteriorment i comprovar que la funció definida va bé encara que s'eliminin zeros a l'esquerra.

(a) (Una solució)

Donem una funció que s'apica a una successió de caràcters (String).

In[9]:=
```
Codifica[m_String] := Module[{lta = ToCharacterCode[m]},
  Flatten[Table[IntegerDigits[lta[[i]], 2, 16], {i, 1, Length[lta]}]]
 ]
```

In[10]:=
```
m = "Una prova de codificació de missatges.";
```

In[11]:=
```
c = Codifica[m]
```

Out[11]=
```
{0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1,
 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1,
 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0,
 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0,
 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0}
```

(b) (Una solució)

Donem una funció que s'apica a una llista de nombres, que han de ser zeros o uns.

In[12]:=
```
Descodifica[lta_List] := Module[{x},
  x = Partition[Flatten[Prepend[lta, Table[0, {i, 1, Mod[-Length[lta], 16]}]]], 16];
  FromCharacterCode[Table[FromDigits[x[[i]], 2], {i, 1, Length[x]}]]
 ]
```

In[13]:=
```
Descodifica[c]
```

Out[13]=
```
Una prova de codificació de missatges.
```

Cal comprovar que, efectivament, descodifica bé.

In[14]:=
```
Descodifica[c] == m
```

Out[14]=
```
True
```

3. El criptosistema de Cèsar

- **Exercici 1.3**

Se suposa que els missatges estan escrits en algun alfabet (això és, un conjunt finit i no buit de símbols). Per exemple, podem pensar en l'alfabet (grec), o l'abecedari (llatí), o en altres alfabets. Per exemple, durant molts anys, es consideraven ch, ll i ñ com a caràcters de l'abecedari castellà; això feia un abecedari de 29 lletres.
Però podem pensar en altres llengües o alfabets: ciríl·lic, europeus orientals, escandinaus, hebreu, àrabs, xinesos, coreà, japonès, tais, bràmics, altres alfabets orientals, i molts altres africans, amerindis, malaisians, etcètera, dels quals ni en conec l'existència.
I, si es vol, encara caldria pensar en tots els caràcters accentuats o modificats d'alguna manera. Sense anar més lluny, com es consideren ç o ny en català? Com un caràcter senzill o com un caràcter modificat (equivalent a accentuat) l'un? I com un caràcter o com un dígraf, l'altre? El diccionari de l'IEC considera ç com una c amb un accent i ny com un dígraf (almenys, en algunes paraules que jo he consultat).

D'altra banda, els alfabets s'aprenen sovint en un cert ordre; és a dir, se suposa que els caràcters de l'alfabet en qüestió estan ordenats d'una certa manera estàndard; per exemple, l'ordre alfabètic, si es tracta de l'alfabet (grec) o l'abecedari (llatí), o altres ordres depenent de l'alfabet que es faci servir. Per exemple, quan es consideren ch, ll i ñ com a caràcters de l'abecedari castellà, es col·loquen entre la c i la d, la ch, entre la l i la m, la ll, i entre la n i la o, la ñ; això determina un ordre en l'abecedari castellà de 29 lletres.

Però no tothom coneix l'ordre dels caràcters ni el considera de la mateixa manera. Segons quina aplicació o quin programa d'ordinador es fa servir, ens podem trobar que la ch es pensa com dues lletres (i, per tant, se situa entre cg i ci), o bé com una de sola (i se situa entre cz i d). I anàlogament amb les ll i ñ, o les lletres accentuades (i en quin ordre van els accents?). Caldrà tenir això present. Per tant, suposarem que treballem amb un alfabet i amb un ordre determinat en aquest alfabet. En aquest tutorial, l'alfabet és el conjunt dels 65536(=2^16) caràcters (possibles) que fa servir *Mathematica,* i l'ordre, el natural: 1<2<3<...<65536.

El criptosistema de Cèsar consisteix a fer córrer cíclicament els caràcters d'un missatge una quantitat fixa de caràcters; aquesta quantitat és la clau secreta. Per exemple, es pot usar la funció següent, que s'aplica a un missatge pla sense codificar i proporciona un missatge xifrat, també *sense codificar*. (Això de *sense codificar* és una mala praxi, perquè podem intentar usar codis que corresponen a caràcters no imprimibles... però ja hi tornarem, a aquest punt.)

Òbviament, doncs, la clau secreta és un nombre enter entre 0 i 65535; de fet, i per la propietat de ciclicitat que hem anomenat més amunt, la clau és un nombre enter qualsevol, del qual només compta la seva classe residual mòdul 65536.

In[15]:=
```
Cesar[missatge_String, clau_Integer] := Module[{b = 2^16, lta = ToCharacterCode[missatge]},
  FromCharacterCode[Table[Mod[lta[[i]] + clau, b], {i, 1, Length[lta]}]]
 ]
```

Per exemple, podem xifrar amb la clau que sovint s'atribueix a l'emperador romà Juli Cèsar (clau=3) el missatge "VENIVIDIVINCI", que també se li atribueix a ell. D'aquí el nom del criptosistema.

In[16]:=
```
Cesar["VENIVIDIVINCI", 3]
```

Out[16]=
```
YHQLYLGLYLQFL
```

Qui no ha jugat a intentar desxifrar missatges xifrats amb el criptosistema de Cèsar i l'alfabet llatí de 26 lletres? Sembla extraordinàriament "senzill"; de fet, només hi ha 26 claus possibles, de manera que s'acaba aviat. O no? Algú ha intentat esbrinar perquè l'ordinador de *2001: A space Oddysey,* d'Arthur C. Clarke, es diu HAL i és de la sèrie 9000?

Hom pot pensar que serà molt difícil desxifrar un missatge xifrat amb el criptosistema de Cèsar i una clau desconeguda, ja que aquesta s'ha pogut triar entre les 65536 possibles. Caldrà provar les 65536 claus?

(a) Es demana intentar desxifrar el text següent, que ha estat xifrat amb la funció Cesar anterior i una clau menor que 65536.

In[17]:=
```
x = "寶尅尉尅■■■小對■導小■■尔■■封導■射尉将■■尉■察          "
```

Out[17]=
```
寶尅尉尅■■■小對■導小■■尔■■封導■射尉将■■尉■察
```

(a) (Una solució)

Comencem per conèixer els caràcters numèrics (que, de fet, és allò que compta) asssociats al missatge xifrat.

In[18]:=
```
lta = ToCharacterCode[x]
```
Out[18]=
```
{23542, 23557, 23561, 23557, 23573, 23488, 23555, 23567, 23565, 23488, 23566, 23567, 23488, 23689,
 23571, 23488, 23572, 23553, 23566, 23488, 23556, 23561, 23558, 23693, 23555, 23561, 23564, 23519}
```

Ara, mirem com són els caràcters numèrics associats a un text de prova.

In[19]:=
```
ToCharacterCode["A veure què succeeix."]
```
Out[19]=
```
{65, 32, 118, 101, 117, 114, 101, 32, 113, 117, 232, 32, 115, 117, 99, 99, 101, 101, 105, 120, 46}
```

Notem que el menor caràcter és el 32, i correspon a l'espai en blanc.

Si el missatge xifrat és un text (com diu l'enunciat), deu tenir espais en blanc i, per tant, el menor dels codis hauria de correspondre a l'espai blanc. Això hauria de fer senzill proporcionar-nos la clau.

In[20]:=
```
{Max[lta], Min[lta]} - 32
```
Out[20]=
```
{23661, 23456}
```

La clau podria ser 23456.

In[21]:=
```
y = Cesar[x, -23456]
```
Out[21]=
```
Veieu com no és tan difícil?
```

- **Observació**

  Cal notar que els missatges poden ser molt més complicats que simples textos; però els codis associats als caràcters que els componguin difícilment pertanyeran a intervals molt grans, de manera que es poden provar claus en intervals petits (i per a parts petites dels missatges). Deixo oberta una reflexió més profunda sobre tot això.

4. El criptosistema de Vigenère

- **Exercici 1.4**

El criptosistema de Vigenère és una generalització i una millora del criptosistema de Cèsar. 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 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-è sims 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-è sim 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.

(a) Es demana escriure una funció **VigenereX** per a xifrar amb el criptosistema de Vigenère.
(b) Es demana escriure la funció inversa, **VigenereDX**, per a desxifrar amb el criptosistema de Vigenère anterior.
(c) Es demana intentar desxifrar el missatge **xifrat** següent, xifrat amb una paraula clau de longitud 25. Quina és aquesta paraula clau?

Observació. Cal que no s'intenti usar la força bruta. Cal notar que paraules de 25 caràcters entre els 65536 possibles n'hi ha $65\,536^{25}$; aproximadament, $\mathbf{2.58225 \times 10^{120}}$. I si poguéssim provar $\mathbf{10^{12}}$ claus per segon, necessitaríem aproximadament $\mathbf{8.18 \times 10^{100}}$ anys per a provar-les totes (l'edat estimada de l'univers és "només" de $\mathbf{1.37 \times 10^{10}}$ anys).

In[22]:=
```
xifrat =
  "[illegible]";
```

(a) (Una solució)

In[23]:=
```
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) (Una solució)

In[24]:=
```
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]}]]
 ]
```

(c) (Una solució)

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

In[25]:=
```
lta = ToCharacterCode[xifrat]
```

Out[25]=
```
{136, 222, 137, 211, 230, 216, 227, 221, 226, 231, 206, 224, 213, 133, 209, 198, 64, 186, 206, 135, 187, 215, 335, 215, 211,
 299, 228, 206, 144, 349, 226, 147, 222, 225, 213, 133, 218, 202, 140, 208, 212, 146, 183, 137, 203, 202, 218, 264, 213,
 215, 172, 226, 221, 223, 231, 216, 230, 221, 216, 225, 198, 141, 197, 133, 132, 168, 264, 201, 202, 217, 147, 142, 312,
 215, 215, 99, 211, 137, 232, 221, 213, 229, 202, 229, 148, 218, 219, 129, 141, 205, 216, 147, 183, 221, 206, 202, 142,
 329, 223, 199, 99, 211, 218, 229, 217, 226, 231, 137, 214, 230, 206, 221, 213, 143, 215, 206, 147, 202, 206, 212, 198,
 142, 331, 211, 209, 111, 146, 206, 222, 148, 223, 229, 210, 224, 217, 215, 141, 205, 140, 211, 200, 76, 118, 221, 217,
 206, 207, 346, 146, 218, 177, 211, 137, 224, 213, 225, 212, 222, 223, 213, 133, 208, 205, 129, 217, 147, 64, 169, 210,
 206, 218, 215, 264, 221, 133, 175, 211, 137, 220, 227, 221, 218, 210, 231, 233, 201, 141, 197, 71, 197, 214, 149, 187,
 220, 219, 198, 142, 344, 211, 215, 164, 231, 213, 209, 148, 210, 223, 202, 232, 162, 133, 174, 129, 131, 211, 211, 148,
 191, 215, 220, 198, 209, 337, 357, 145, 99, 215, 220, 144, 228, 225, 216, 215, 216, 226, 133, 209, 198, 64, 207, 133,
 133, 196, 137, 210, 133, 211, 340, 229, 133, 166, 211, 219, 336, 215, 227, 216, 219, 230, 148, 201, 210, 205, 64, 209,
 206, 147, 201, 202, 219, 204, 211, 264, 226, 209, 164, 158, 137, 212, 217, 143, 224, 202, 225, 217, 215, 206, 129, 145,
 217, 202, 64, 183, 218, 220, 202, 225, 348, 146, 215, 168, 229, 221, 209, 148, 211, 220, 223, 220, 216, 206, 225, 129,
 133, 210, 133, 130, 194, 216, 202, 216, 142, 332, 215, 133, 174, 146, 204, 209, 230, 335, 214, 221, 216, 230, 216, 141,
 198, 152, 199, 202, 144, 202, 206, 147, 133, 222, 343, 230, 216, 168, 228, 149, 144, 217, 219, 147, 205, 212, 230, 215,
 210, 211, 64, 198, 209, 143, 185, 149, 135, 214, 227, 333, 146, 211, 178, 223, 338, 227, 148, 210, 226, 215, 231, 349,
 133, 217, 194, 64, 213, 218, 129, 196, 221, 208, 217, 207, 348, 146, 201, 168, 146, 204, 209, 230, 335, 214, 221, 216,
 230, 216, 141, 210, 149, 201, 133, 146, 187, 220, 219, 202, 220, 264, 214, 202, 99, 222, 202, 144, 216, 216, 233, 210,
 230, 221, 344, 141, 197, 133, 132, 209, 129, 118, 213, 214, 211, 213, 337, 230, 218, 167, 146, 221, 223, 232, 208, 223,
 137, 215, 217, 209, 141, 206, 137, 215, 216, 129, 202, 208, 204, 133, 211, 342, 230, 215, 168, 146, 212, 158, 148,
 194, 216, 208, 232, 221, 201, 206, 206, 133, 210, 217, 76, 118, 206, 218, 133, 209, 343, 224, 216, 172, 214, 206, 226,
 217, 221, 147, 206, 223, 231, 133, 216, 129, 141, 205, 216, 147, 183, 221, 206, 202, 225, 264, 216, 212, 181, 223, 202,
 228, 231, 143, 227, 206, 223, 231, 133, 221, 211, 137, 209, 202, 146, 201, 149, 135, 202, 218, 347, 146, 216, 168,
 217, 216, 222, 231, 155, 147, 151, 161, 162, 145, 141, 198, 140, 215, 133, 139, 131, 337, 218, 206, 219, 347, 146, 200,
 164, 228, 329, 211, 232, 212, 229, 220, 147, 216, 202, 217, 129, 141, 205, 216, 147, 183, 221, 206, 202, 142, 343, 228,
 206, 170, 219, 215, 209, 224, 157, 147, 170, 147, 215, 212, 219, 213, 137, 210, 218, 129, 185, 210, 346, 145, 142, 347,
 153, 198, 179, 222, 210, 211, 213, 143, 212, 137, 214, 213, 201, 206, 212, 131, 217, 211, 64, 186, 206, 211, 216, 142,
 337, 175, 150, 111, 146, 155, 156, 148, 157, 161, 151, 159, 148, 208, 141, 206, 137, 215, 216, 129, 202, 208, 204, 216,
 142, 342, 225, 218, 182, 146, 213, 209, 148, 227, 229, 202, 225, 231, 203, 220, 211, 141, 197, 200, 137, 329, 137, 203,
 202, 142, 299, 346, 216, 164, 228, 137, 225, 233, 212, 147, 204, 226, 230, 215, 210, 212, 144, 211, 211, 64, 183, 137,
 211, 198, 142, 331, 222, 198, 184, 146, 172, 344, 231, 208, 229, 137, 215, 227, 211, 206, 197, 129, 132, 213, 133, 194,
 137, 202, 198, 224, 456, 213, 217, 168, 228, 137, 217, 161, 343, 230, 210, 224, 148, 201, 210, 129, 140, 197, 133, 131,
 194, 202, 220, 133, 196, 337, 217, 202, 177, 346, 219, 213, 162, 143, 188, 149, 147, 218, 206, 219, 194, 140, 209, 202,
 142, 202, 149, 135, 202, 225, 264, 213, 212, 177, 229, 221, 226, 233, 212, 220, 225, 147, 217, 209, 141, 206, 137, 215,
 216, 129, 202, 208, 204, 133, 230, 337, 216, 215, 164, 230, 137, 213, 226, 143, 220, 215, 231, 217, 215, 208, 194, 140,
 197, 215, 64, 187, 213, 218, 133, 209, 329, 228, 325, 166, 230, 206, 226, 231, 143, 212, 210, 235, 353, 133, 220, 195, 148,
 205, 211, 135, 203, 221, 218, 159, 142, 344, 228, 206, 176, 215, 219, 209, 225, 212, 225, 221, 159, 148, 202, 217, 129,
 144, 214, 206, 141, 187, 219, 135, 201, 211, 264, 213, 198, 167, 211, 220, 211, 233, 221, 147, 205, 216, 224, 216, 141,
 204, 64, 209, 206, 147, 201, 202, 219, 204, 211, 347, 146, 221, 172, 216, 219, 209, 232, 226, 174, 137, 215, 217, 216,
 221, 211, 265, 215, 145, 64, 187, 213, 218, 133, 225, 333, 217, 212, 177, 229, 164, 144, 216, 212, 230, 217, 229, 349,
 216, 153, 129, 133, 208, 216, 64, 202, 206, 217, 200, 211, 346, 229, 160, 99, 215, 221, 211, 348, 227, 216, 219, 212, 162}
```

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

In[26]:=
```
blocs = Transpose[Partition[lta, 25]]
```

Out[26]=
```
{{136, 299, 172, 99, 99, 111, 177, 175, 164, 99, 166, 164, 168, 174, 168, 178, 168, 99, 167,
  168, 172, 181, 168, 164, 170, 179, 111, 182, 164, 184, 168, 177, 177, 164, 166, 176, 167, 172, 177},
 {222, 228, 226, 211, 211, 146, 211, 211, 231, 215, 211, 158, 229, 146, 228, 223, 146, 222, 146, 146,
  214, 223, 217, 228, 219, 222, 146, 146, 228, 146, 228, 346, 229, 230, 230, 215, 211, 216, 229},
 {137, 206, 221, 137, 218, 206, 137, 137, 213, 220, 219, 137, 221, 204, 149, 338, 204, 202, 221, 212,
  206, 202, 216, 329, 215, 210, 155, 213, 137, 172, 137, 219, 221, 137, 206, 219, 220, 219, 164},
 {211, 144, 223, 232, 229, 222, 224, 220, 209, 144, 336, 212, 209, 209, 144, 227, 209, 144, 223, 158,
  226, 228, 222, 211, 209, 211, 156, 209, 225, 344, 217, 213, 226, 213, 226, 209, 211, 209, 144},
 {230, 349, 231, 221, 217, 148, 213, 227, 148, 228, 215, 217, 148, 230, 217, 148, 230, 216, 232, 148,
  217, 231, 231, 232, 224, 213, 148, 148, 233, 231, 161, 162, 233, 226, 231, 225, 233, 232, 216},
 {216, 226, 216, 213, 226, 223, 225, 221, 210, 225, 227, 143, 211, 335, 219, 210, 335, 216, 208, 194,
  221, 143, 155, 212, 157, 143, 157, 227, 212, 208, 343, 143, 212, 143, 143, 212, 221, 226, 212},
 {227, 147, 230, 229, 231, 229, 212, 218, 223, 216, 216, 224, 220, 214, 147, 226, 214, 233, 223, 216,
  147, 227, 147, 229, 147, 212, 161, 229, 147, 229, 230, 188, 220, 220, 212, 225, 147, 174, 230},
 {221, 222, 221, 202, 137, 210, 222, 210, 202, 215, 219, 202, 223, 221, 205, 215, 221, 210, 137, 208,
  206, 206, 151, 220, 170, 137, 151, 202, 204, 137, 210, 149, 225, 215, 210, 221, 205, 137, 217},
 {226, 225, 216, 229, 214, 224, 223, 231, 232, 216, 230, 225, 220, 216, 212, 231, 216, 230, 215, 232,
  223, 223, 161, 147, 147, 214, 159, 225, 226, 215, 224, 147, 147, 231, 235, 159, 216, 215, 229},
 {231, 213, 225, 148, 230, 217, 213, 233, 162, 226, 148, 217, 216, 230, 230, 349, 230, 221, 217, 221,
  231, 231, 162, 216, 215, 213, 148, 231, 230, 227, 148, 218, 217, 217, 353, 148, 224, 217, 349},
 {206, 133, 198, 218, 206, 215, 133, 201, 133, 133, 201, 215, 206, 216, 215, 133, 216, 344, 209, 201,
  133, 133, 145, 202, 212, 201, 208, 203, 215, 211, 201, 206, 209, 215, 133, 202, 216, 216, 216},
 {224, 218, 141, 219, 221, 141, 208, 141, 174, 209, 210, 206, 225, 141, 210, 217, 141, 141, 141, 206,
  216, 221, 141, 217, 219, 206, 141, 220, 210, 206, 210, 219, 141, 208, 220, 217, 141, 221, 153},
 {213, 202, 197, 129, 213, 205, 205, 197, 129, 198, 205, 129, 129, 198, 211, 194, 210, 197, 206, 206,
  129, 211, 198, 129, 213, 212, 206, 211, 212, 197, 129, 194, 206, 194, 195, 129, 204, 211, 129},
 {133, 140, 133, 141, 143, 140, 129, 71, 131, 64, 64, 145, 133, 152, 64, 64, 149, 133, 137, 133, 141,
  137, 140, 141, 137, 131, 137, 141, 144, 129, 140, 140, 137, 140, 148, 144, 64, 265, 133},
 {209, 208, 132, 205, 215, 211, 217, 197, 211, 207, 209, 217, 210, 199, 198, 213, 201, 132, 215, 210,
  205, 209, 215, 205, 210, 217, 215, 197, 211, 132, 197, 209, 215, 197, 205, 214, 209, 215, 208},
 {198, 212, 168, 216, 206, 200, 147, 214, 211, 133, 206, 202, 133, 202, 209, 218, 133, 209, 216, 217,
  216, 202, 133, 216, 218, 211, 216, 200, 211, 213, 133, 202, 216, 215, 211, 206, 206, 145, 216},
 {64, 146, 264, 147, 147, 76, 64, 149, 148, 133, 147, 64, 130, 144, 143, 129, 146, 129, 129, 76,
  147, 146, 139, 147, 129, 64, 129, 137, 64, 133, 131, 142, 129, 64, 135, 141, 147, 64, 64},
 {186, 183, 201, 183, 202, 118, 169, 187, 191, 196, 201, 183, 194, 202, 185, 196, 187, 118, 202, 118,
  183, 201, 131, 183, 185, 186, 202, 329, 183, 194, 194, 202, 202, 187, 203, 187, 201, 187, 202},
 {206, 137, 202, 221, 206, 221, 210, 220, 215, 137, 202, 218, 216, 206, 149, 221, 220, 213, 208, 206,
  221, 149, 337, 221, 210, 206, 208, 137, 137, 137, 202, 149, 208, 213, 221, 219, 202, 213, 206},
 {135, 203, 217, 206, 212, 217, 206, 219, 220, 210, 219, 220, 202, 147, 135, 208, 219, 214, 204, 218,
  206, 135, 218, 206, 346, 211, 204, 203, 211, 202, 220, 135, 204, 218, 218, 135, 219, 218, 217},
 {187, 202, 147, 202, 198, 206, 218, 198, 198, 133, 204, 202, 216, 133, 214, 217, 202, 211, 133, 133,
  202, 202, 206, 202, 145, 216, 216, 202, 198, 198, 133, 202, 133, 133, 159, 201, 204, 133, 200},
 {215, 218, 142, 142, 142, 207, 215, 142, 209, 211, 211, 225, 142, 222, 227, 207, 220, 213, 211, 209,
  225, 218, 219, 142, 142, 142, 142, 142, 142, 224, 196, 225, 230, 209, 142, 211, 211, 225, 211},
 {335, 264, 312, 329, 331, 346, 264, 344, 337, 340, 264, 348, 332, 343, 333, 348, 264, 337, 342, 343,
  264, 347, 347, 343, 347, 337, 342, 299, 331, 456, 337, 264, 337, 329, 344, 264, 347, 333, 346},
 {215, 213, 215, 223, 211, 146, 221, 211, 357, 229, 226, 146, 215, 230, 146, 146, 214, 230, 230, 224,
  216, 146, 146, 228, 153, 175, 225, 346, 222, 213, 217, 213, 216, 228, 228, 213, 146, 217, 229},
 {211, 215, 215, 199, 209, 218, 133, 215, 145, 133, 209, 215, 133, 216, 211, 201, 202, 218, 215, 216,
  212, 216, 200, 206, 198, 150, 218, 216, 198, 217, 202, 212, 215, 325, 206, 198, 221, 212, 160}}
```

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

In[27]:=
```
ToCharacterCode["AZaz"]
```
Out[27]=
```
{65, 90, 97, 122}
```

Ens imaginem que la paraula clau estarà formada majoritàriament per alguns d'aquests caràcters.

In[28]:=
```
{Max[blocs[[1]]], Min[blocs[[1]]]}
```
Out[28]=
```
{299, 99}
```

Sembla que el primer caràcter de la paraula clau és una lletra majúscula. A més, deu ser un caràcter imprimible, de manera que el seu codi és més gran que 32; això deixa poques possibilitats:

In[29]:=
```
{Max[blocs[[1]]], Min[blocs[[1]]]} - 32
```
Out[29]=
```
{267, 67}
```

Les provem totes:

In[30]:=
```
Table[{n, FromCharacterCode[blocs[[1]] - n]}, {n, 65, 67}] // MatrixForm
```
Out[30]//MatrixForm=
```
65  Gêk"".pnc"ecgmgqg"fgktgcir.ucwgppceofkp
66  Féj!!-omb!dbflfpf!efjsfbhq-tbvfoobdnejo
67  Eèi  ,nla caekeoe deireagp,sauennacmdin
```

La més versemblant és la tercera; correspon al caràcter "C". (A més a més, correspon al fet que el caràcter més usual en el missatge pla sigui l'espai blanc).

In[31]:=
```
FromCharacterCode[67]
```
Out[31]=
```
C
```

Repetim amb els altres blocs. Sembla que la majoria dels caràcters corresponents de la paraula clau siguin lletres minúscules.

In[32]:=
```
Table[FromCharacterCode[Min[blocs[[i]]] - 32], {i, 2, 25}]
```

Out[32]=
```
{r, i, p, t, o, s, i, s, t, e, m, a,  , d, e,  , V, i, g, e, n, è, r, e}
```

In[33]:=
```
clau = FromCharacterCode[Table[Min[blocs[[i]]] - 32, {i, 1, 25}]]
```

Out[33]=
```
Criptosistema de Vigenère
```

La paraula clau seria la paraula "Criptosistema de Vigenère".
I el missatge pla el següent:

In[34]:=
```
VigenereDX[xifrat, clau]
```

Out[34]=
```
El criptosistema de Vigenère és una millora del criptosistema de Cèsar. Per a xifrar un missatge amb aquest
  criptosistema cal, en primer lloc, triar una paraula clau. Sigui k la longitud 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=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:
  primerament, el primer de cadascun dels k missatges xifrats; després, els segons; després, els tercers; etcètera.
```

5. Exercici

- **Exercici 1.5**

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[35]:=

```
TextXifrat = {0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 18, 65 532, 2, 65 467, 65 530, 79, 14, 0,
   65 518, 0, 5, 65 525, 65 524, 83, 65 482, 65 534, 3, 8, 65 533, 76, 4, 82, 65 450, 65 475,
   65 475, 65 477, 65 475, 25, 65 491, 65 445, 65 468, 65 500, 2, 83, 4, 192, 65 533, 65 467,
   65 503, 65 517, 65 535, 67, 18, 65 467, 65 473, 65 467, 65 503, 65, 4, 77, 65 529, 9, 65 467,
   65 430, 65 431, 54, 15, 7, 65 529, 14, 65 453, 69, 65 467, 86, 65 519, 9, 6, 65 535, 65 453,
   72, 11, 9, 65 460, 8, 65 532, 83, 65 467, 68, 65 519, 14, 65 531, 65 523, 0, 0, 13, 10,
   1, 11, 65 529, 73, 13, 12, 65 428, 1, 65 523, 65 521, 65 531, 84, 65 482, 65 534, 65 525,
   8, 65 526, 78, 14, 0, 65 518, 16, 65 524, 0, 65 532, 83, 25, 14, 65 460, 11, 65 522, 82,
   65 467, 76, 65 515, 65 467, 65 535, 65 517, 65 535, 14, 65 460, 65 512, 65 529, 14, 1, 82,
   0, 0, 65 523, 65 467, 2, 65 531, 65 531, 69, 24, 15, 65 460, 65 534, 65 532, 78, 15, 82,
   65 515, 65 467, 65 526, 65 459, 65 522, 76, 22, 14, 65 460, 17, 65 522, 73, 2, 0, 65 515,
   13, 65 535, 65 517, 65 535, 27, 65 460, 19, 65 525, 7, 65 532, 67, 65 479, 0, 65 526, 7,
   65 527, 2, 65 518, 78, 30, 65 479, 65 460, 7, 65 532, 83, 65 467, 68, 65 519, 16, 65 527,
   65 530, 65 453, 83, 31, 65 533, 10, 0, 65 531, 73, 13, 65 514, 65 515, 65 533, 65 458, 65 528,
   65 529, 85, 28, 14, 65 460, 65 532, 65 530, 73, 65 534, 83, 65 450, 7, 1, 65 452, 65 524,
   82, 15, 65 534, 65 460, 0, 65 453, 76, 10, 0, 65 527, 4, 65 529, 65 526, 65 532, 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};
```