MAT^2

MATerials MATemàtics
Volum 2009, treball no. 1, 25 pp. ISSN: 1887-1097
Publicació electrònica de divulgació del Departament de Matemàtiques
de la Universitat Autònoma de Barcelona
www.mat.uab.cat/matmat

Dels jeroglífics egipcis a la compartició de secrets

David Juher

Introducció

La criptografia (del grec *kryptos*, "amagat", i *graphein*, "escriure") és l'estudi de les tècniques de comunicació secreta que asseguren que el destinatari legítim d'un missatge és l'única persona que serà capaç de llegir-lo i entendre'l. Es tracta d'una disciplina molt antiga, que tradicionalment ha estat utilitzada en èpoques de conflicte bèl·lic o per assegurar la confidencialitat de les comunicacions diplomàtiques i les transaccions bancàries [8], [5], [12]. Actualment, però, la criptografia ha deixat de ser patrimoni exclusiu de diplomàtics i militars, i, encara que no en siguem conscients, ha entrat a formar part de les nostres vides: les converses que mantenim per telèfon mòbil estan xifrades, les imatges que emeten les televisions de pagament també ho estan (només l'usuari que ha pagat té la clau necessària per desxifrar-les), i totes les compres, transaccions i tràmits que realitzem a través de la xarxa Internet també estan protegits amb tècniques criptogràfiques.

La disciplina "dual", que de fet es pot considerar com una branca de la criptografia, és la *criptoanàlisi*, que, en lloc de proposar mètodes de codificació nous, més potents i segurs, es dedica a estudiar com es poden atacar els que ja existeixen. Per a qui tingui dubtes sobre la dignitat de la criptoanàlisi

Figura 1: Sant Andreu de la Barroca

com a disciplina científica, cal recordar que el desxiframent de codis secrets, a part d'haver protagonitzat alguns arguments apassionants de la novel·la de ficció de tots els temps ([3], [6], [11]), ha servit entre altres coses per derrotar l'exèrcit de Hitler en batalles decisives, o per entendre el significat de l'escriptura d'antigues civilitzacions perdudes.

Malgrat les seves profundes arrels humanístiques de caràcter històric, lingüístic, religiós i fins i tot esotèric, actualment la criptografia es pot considerar una branca de la matemàtica. De fet, és una aplicació de la teoria de nombres, amb ramificacions cap a l'estadística, la teoria de la informació, la complexitat algorísmica i la física quàntica, entre d'altres. Mentre que la majoria de mètodes clàssics són encantadorament artesanals (aplegueu les lletres dels paràgrafs anteriors que estan marcades amb un petit punt i apareixerà una salutació al lector), hi ha situacions en què el llenguatge matemàtic esdevé una eina de treball imprescindible o, si més no, poderosa.

En aquest article presentaré tres d'aquestes situacions. A la secció 1 parlarem d'un jeroglífic inscrit als laterals de la llinda de Sant Andreu de la Barroca, una petita església perduda en un indret recòndit de la Vall del Llémena, a la Garrotxa. A propòsit d'aquest petit enigma ludolingüístic, plantejarem (i finalment resoldrem) un problema de naturalesa combinatòria que el lector interessat pot provar de resoldre com a exercici. A la secció 2 farem un breu repàs de la història del desxiframent d'escriptures de civilitzacions antigues. Aprofitarem l'avinentesa per introduir els conceptes d'*entropia* i *redundància* del llenguatge, que ens ajudaran a entendre per què, tard o d'hora, qualsevol escriptura antiga finalment acaba essent desxifrada quan es té una conjectu-

ra raonable sobre quina és la llengua que transcriu. Finalment, a la secció 3 definirem el concepte d'*esquema de compartició de secrets*, un problema de criptografia moderna en el qual un conjunt de persones gestiona petits fragments d'informació compartida, i que es resol aplicant de manera brillant una idea que prové del món de l'àlgebra lineal més elemental.

1 El jeroglífic de la Barroca

1.1 Plantejament i antecedents

El professor Josep Tarrés, del Departament d'Arquitectura i Enginyeria de la Construcció de la Universitat de Girona, em va informar [9] de l'existència d'un parell d'inscripcions situades a banda i banda de la porta d'accés a l'església de Sant Andreu de la Barroca, un petit indret situat a redós del Puig d'Elena, a la part més meridional de la comarca de la Garrotxa. Es tracta d'una mena de sopa de lletres quadriculada, de mida 5×5, que recorda molt el famós quadrat màgic de la *fórmula Sator*:

S	A	T	O	R
A	R	E	P	O
T	E	N	E	T
O	P	E	R	A
R	O	T	A	S

El quadrat Sator es pot llegir *bustrofèdicament* (aquesta paraula terrible significa que el sentit de lectura de les línies de text s'alterna d'esquerra a dreta i de dreta a esquerra), amb la qual cosa s'obté la frase llatina SATOR OPERA TENET AREPO ROTAS, o bé a la manera tradicional (d'esquerra a dreta i de dalt a abaix), obtenint en aquest cas SATOR AREPO TENET OPERA ROTAS. La mateixa frase apareix quan el sentit de lectura és vertical, tant d'abaix a dalt com en sentit contrari. Ambdues frases llatines són palíndroms (presenten simetria respecte de la N central). La versió més antiga d'aquesta inscripció s'ha trobat a les parets d'algunes cases romanes de les ruïnes de Pompeia, i el mateix quadrat apareix a Santiago de Compostel·la, al castell de Rochemaure, a la catedral de Siena, a les ruïnes romanes de Cirencester... Desgraciadament, no hi ha consens sobre el significat exacte del palíndrom, perquè no està clara la traducció de la paraula "Arepo". Una traducció força lliure de la frase produeix *Aquell que guia l'arada planta*

la llavor, en referència a un passatge evangèlic. Més interessants són altres frases obtingudes recorrent les lletres del jeroglífic en sentits més arbitraris (permutant les lletres o, dit d'una altra manera, fent anagrames): *Ora, operare, ostenta te, pastor*, o bé *Retro Satana, toto opere asper*, o fins i tot la més dramàtica *Satan, ter oro te, reparato opes!* ("Satanàs, t'ho demano tres cops: repara la meva fortuna!")...

Molt probablement, el jeroglífic de la Barroca està inspirat en aquesta mena de quadrats màgics que apareixen en alguns edificis de la cristiandat d'arreu d'Europa. De fet no es tracta d'un quadrat, sinó de dos, cada un dels quals té la mateixa mida que el quadrat Sator, tot i que la simplicitat de les normes que en aquest cas cal aplicar el converteixen en una mena de versió casolana del quadrat Sator. Tècnicament, en el món de la ludolingüística se'l classifica dins la família dels *laberints* o *multiacròstics* [7]. Aquí en podeu veure una reproducció:

S	*U*	*S*	*U*	*S*
U	*S*	*E*	*S*	*U*
S	*E*	*I*	*E*	*S*
U	*S*	*E*	*S*	*U*
S	*U*	*S*	*U*	*S*

A	*I*	*R*	*I*	*A*
I	*R*	*A*	*R*	*I*
R	*A*	*M*	*A*	*R*
I	*R*	*A*	*R*	*I*
A	*I*	*R*	*I*	*A*

Fins i tot sense tenir ni idea de llatí, el lector hi reconeixerà fàcilment les paraules IESUS i MARIA, respectivament. Ambdós quadrats segueixen el mateix esquema diguem-ne geomètric: una lletra central, la M, i successives "capes" o nivells concèntrics en forma de rombe, cada un format per la següent lletra de la corresponent paraula. Aquí podeu observar-hi requadrades les lletres del nivell 0 (la M central) i del nivell 2 (format per 8 lletres R). I, en negreta, les 4 lletres A del nivell 1:

A	I	R	I	A
I	R	**A**	R	I
R	**A**	M	**A**	R
I	R	**A**	R	I
A	I	R	I	A

Les normes per confegir la paraula màgica semblen clares: cal partir de la lletra central, "saltar" a una de les lletres veïnes del següent nivell, i procedir

així successivament fins a arribar a una de les quatre cantonades del quadrat. Per exemple, aquí teniu dues maneres d'obtenir la paraula MARIA:

A	**I**	**R**	I	A
I	R	**A**	R	I
R	A	**M**	**A**	R
I	R	A	**R**	**I**
A	I	R	I	**A**

1.2 Càlcul del nombre de possibilitats

És obvi que, per tal de poder organitzar les lletres en forma de quadrat, cal que la paraula màgica tingui un nombre senar de lletres. En la documentació que el professor Tarrés em va fer arribar a propòsit del jeroglífic de la Barroca, en una nota a peu de pàgina s'hi llegia la següent afirmació: si tenim un quadrat màgic generat a partir d'una paraula de n lletres, on n és un nombre senar, llavors el nombre de possibilitats que tenim per formar la paraula és igual a quatre vegades el coeficient central del polinomi $(a+b)^{n-1}$. En el cas del quadrat de la Barroca, com que

$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4,$$

resulta que tenim $4 \times 6 = 24$ maneres de confegir la paraula MARIA seguint les normes prefixades, afirmació que es pot corroborar experimentalment de manera trivial.

Si el nombre de lletres no és senar, ens haurem de conformar amb un *rectangle màgic*. Aquí tenim dos possibles rectangles que oculten la paraula EUREKA:

A	*K*	*E*	*R*	*U*	*R*	*E*	*K*	*A*
K	*E*	*R*	*U*	**E**	*U*	*R*	*E*	*K*
A	*K*	*E*	*R*	*U*	*R*	*E*	*K*	*A*

A	*K*	*E*	*K*	*A*
K	*E*	*R*	*E*	*K*
E	*R*	*U*	*R*	*E*
R	*U*	**E**	*U*	*R*
E	*R*	*U*	*R*	*E*
K	*E*	*R*	*E*	*K*
A	*K*	*E*	*K*	*A*

El dia 11 de setembre de 1975, quan s'estava restaurant el temple asturià de Santianes de Pravia, va aparèixer sota l'altar major la inscripció en pedra que tot seguit podeu veure reproduïda:

```
T I C E F S P E C N C E P S F E C I T
I C E F S P E C N I N C E P S F E C I
C E F S P E C N I R I N C E P S F E C
E F S P E C N I R P R I N C E P S F E
F S P E C N I R P O P R I N C E P S F
S P E C N I R P O L O P R I N C E P S
P E C N I R P O L I L O P R I N C E P
E C N I R P O L I S I L O P R I N C E
P E C N I R P O L I L O P R I N C E P
S P E C N I R P O L O P R I N C E P S
F S P E C N I R P O P R I N C E P S F
E F S P E C N I R P R I N C E P S F E
C E F S P E C N I R I N C E P S F E C
I C E F S P E C N I N C E P S F E C I
T I C E F S P E C N C E P S F E C I T
```

Es tracta d'un altre rectangle màgic, generat a partir de la frase SILO PRINCEPS FECIT ("el príncep Silo em va fer"). Es tracta del príncep visigot Silo, que va fer construir el laberint a l'entorn de l'any 780. L'autor d'aquest laberint va triar d'organitzar les lletres en un rectangle de mida 19×15 (malgrat que, com que la frase consta de 17 lletres, es podrien haver organitzat en forma de quadrat). A la "enciclopedia de Oviedo" [13] se'ns diu que "En la iglesia de San Juan Evangelista, que el mismo Silo, rey de Oviedo (774-783), fundó en Santianes, a dos kilómetros de Pravia, figura la lápida donde la inscripción *Silo princeps fecit* aparece escrita de doscientas maneras (según otros, hasta 2024)". En canvi, en una altra afirmació a peu de pàgina de la documentació de Josep Tarrés, es diu que "en tractar-se d'un conjunt de lletres en 15 files per 19 columnes, el nombre de maneres de confegir la frase a cada quadrant correspon no al coeficient central del polinomi $(a+b)^{16}$, sinó al següent coeficient, 11440. Per tant, en total tenim 45760 possibilitats". En efecte, $(a+b)^{16} = a^{16} + 16ba^{15} + \ldots + 11440b^7a^9 + 12870b^8a^8 + 11440b^9a^7 + \ldots + 16b^{15}a + b^{16}$. Màrius Serra, a [7], també dóna 45760 com a nombre de possibles reconstruccions diferents de la frase llatina.

Ha arribat l'hora d'intentar respondre amb total generalitat a la pregunta: de quantes maneres podem formar la frase generada per un rectangle d'aquest

tipus? El lector interessat pot intentar de resoldre aquest problema i obtenir una fórmula que, presumiblement, dependrà del nombre n de lletres de la frase, i de l'amplada i alçada del rectangle.

Tot seguit resolem aquest problema purament combinatori. Segons les anotacions de Tarrés, el nombre buscat sempre és igual a 4 vegades un coeficient del polinomi $(a+b)^n$. Òbviament, el fet de multiplicar per 4 obeeix a la simetria central amb què estan distribuïdes les lletres: és suficient triar una de les cantonades del rectangle (diguem, la superior dreta), comptar el nombre de recorreguts diferents que, al quadrant superior dret, connecten la lletra central del rectangle màgic a la lletra situada en aquesta cantonada, i multiplicar per 4. El fet que els coeficients del polinomi $(a+b)^n$ siguin nombres combinatoris ens dóna una pista valuosa. Recordem que aquests nombres es poden representar en forma de triangle de Pascal, del qual reproduïm aquí les 6 primeres fileres:

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}
$$

Cada nombre combinatori present en aquest triangle és igual a la suma dels dos nombres contigus de la filera immediatament superior. Ara relacionarem el triangle de Pascal amb els nostres quadrats màgics. Preneu el jeroglífic corresponent a la paraula MARIA i quedeu-vos només amb un dels 4 quadrants (per exemple, el superior dret). Preneu també el triangle de Pascal, apliqueu-li una rotació de 135 graus en sentit antihorari i superposeu-lo al jeroglífic, fent coincidir l'1 del vèrtex "superior" amb la M de la cantonada inferior esquerra del quadrant (la M central del jeroglífic complet):

$$
\begin{array}{|ccccc|}
\hline
A & I & R & I & A \\
I & R & A & R & I \\
R & A & M & A & R \\
I & R & A & R & I \\
A & I & R & I & A \\
\hline
\end{array}
\quad + \quad
\begin{array}{ccccc}
 & & 1 & & \\
 & 1 & & 4 & \\
1 & & 3 & & 6 \\
 & 1 & & 2 & \\
 & & 1 & & \\
\end{array}
\quad \longrightarrow \quad
\begin{array}{|ccccc|}
\hline
A & I & R^{1} & I^{3} & A^{6} \\
I & R & A^{1} & R^{2} & I^{3} \\
R & A & M^{1} & A^{1} & R^{1} \\
I & R & A & R & I \\
A & I & R & I & A \\
\hline
\end{array}
$$

Observeu que, ara, els successius nivells del quadrat màgic coincideixen exactament amb les successives fileres del triangle de Pascal. Observeu també que el coeficient corresponent a la cantonada superior dreta, 6, coincideix amb el nombre de maneres diferents de formar la paraula MARIA partint de la M central. Per què això és així? Justament, per les normes que regeixen els moviments a dins del jeroglífic. A una lletra donada s'hi pot arribar saltant-hi des de dues lletres: la situada a la seva esquerra i la situada a sota. Per tant, tenim la següent relació de recurrència: el nombre de maneres d'arribar a una lletra de nivell k és igual a la suma del nombre de maneres d'arribar a les dues lletres contigües del nivell $k-1$. Com que ara els "nivells" corresponen a les fileres del triangle de Pascal, ja tenim el problema resolt.

Per obtenir una fórmula general que ens doni el nombre de recorreguts en funció del nombre de lletres de la paraula, n, i de l'amplada i l'alçada de cada quadrant, i i j respectivament, aplicarem un altre raonament, que de fet és absolutament equivalent a l'anterior. Aquest raonament té un enfoc una mica més analític, però té l'avantatge que es pot estendre fàcilment al cas en què les lletres estan organitzades en forma de *cub màgic* (o, més generalment, *prisma rectangular màgic*), que és la versió tridimensional d'aquest tipus de laberints.

Imagineu que la lletra central del jeroglífic està situada al punt $(0,0)$ d'un sistema de coordenades (diguem, X i Y) definides per dos eixos perpendiculars que divideixen el rectangle màgic en quatre quadrants iguals. Aleshores, la lletra de la cantonada superior dreta estarà situada al punt de coordenades enteres (i,j). Un "recorregut" des del punt $(0,0)$ fins al punt (i,j) correspon a una manera d'anar sumant 1 a la coordenada vertical del punt, o bé a la coordenada horitzontal, de manera que finalment arribem al punt (i,j) després d'haver fet i sumes a la coordenada X i j sumes a la coordenada Y. Dit encara d'una altra manera: el que busquem correspon al nombre de paraules de longitud $i+j$ que es poden formar amb els símbols X i Y, si disposem de i símbols X i j símbols Y. En el jeroglífic de la Barroca, la A de la cantonada superior dreta està situada en el punt $(2,2)$, o sigui que $i=j=2$. Per tant, disposem de dues X i de dues Y, i les paraules que podem formar amb aquestes restriccions són $XXYY$, $XYXY$, $XYYX$, $YXXY$, $YXYX$ i $YYXX$. En total, 6 paraules, que corresponen als 6 recorreguts que podem fer des de la M central fins a la A. Per exemple, la paraula XYYX correspondria al recorregut "dreta–amunt–amunt–dreta". És ben conegut que aquest tipus de distribucions s'anomenen *permutacions amb repetició*, i no és gens difícil

demostrar que n'hi ha $\dfrac{(i+j)!}{i!j!}$ de diferents.

Finalment, si tenim en compte que de fet i i j no són independents, sinó que estan lligats per la relació $i + j = n - 1$, aplegant tot el que hem dit podem assegurar que la fórmula que buscàvem és

$$\frac{4 \cdot (n-1)!}{i!\,(n-1-i)!}$$

on n és la longitud de la frase màgica i i és l'amplada d'un quadrant del laberint. Naturalment, aquesta fórmula coincideix amb 4 vegades el nombre combinatori $\binom{n-1}{i}$.

1.3 Cubs màgics

Els conceptes de quadrat màgic i rectangle màgic es poden estendre sense dificultat als de *cub màgic* i *prisma rectangular màgic*. En aquest cas, les lletres del laberint s'organitzen en un espai tridimensional, en el qual la primera lletra de la frase ocupa l'origen de coordenades $(0, 0, 0)$, i la resta de lletres s'expandeixen en nivells o capes successives, simètricament en els 8 octants. A la Figura 2 hi teniu el cub màgic engendrat per la paraula DALÍ.

L'objectiu és fer recorreguts des de la lletra central del prisma rectangular fins a la lletra final de la frase màgica, 8 còpies de la qual estan situades a cada una de les 8 cantonades del prisma. Si diem i i j, respectivament, a l'amplada i l'alçada d'un dels octants, i n al nombre de lletres de la frase màgica, llavors la lletra de la cantonada d'un dels octants està situada en el punt de coordenades enteres $(i, j, n - 1 - i - j)$. Observeu que per tal que una frase pugui generar un cub màgic la seva longitud ha de tenir la forma $3k + 1$.

En aquesta situació, si repetim els raonaments que ja havíem aplicat en el cas dels rectangles màgics, veurem que el nombre de maneres de formar una frase de n lletres organitzades en forma de prisma rectangular màgic amb octants d'amplada i i alçada j és

$$\frac{8 \cdot (n-1)!}{i!\,j!\,(n-1-i-j)!}.$$

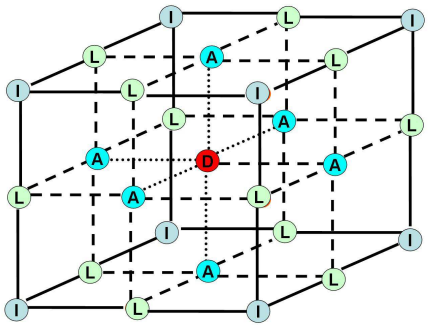

Figura 2: Cub màgic (autor: Josep Tarrés)

2 Desxiframent d'escriptures antigues

2.1 Escriptures i llengües

Hi ha escriptures molt antigues el significat de les quals no s'ha perdut mai: els alfabets grec, llatí, hebreu, cirílic o àrab, els caràcters xinesos, els *kana* japonesos, etc. En canvi, n'hi ha d'altres que, per una o altra raó, en algun moment de la història molt posterior al moment en què van deixar de ser utilitzades, finalment van deixar de ser enteses. En aquest segon grup hi tenim els jeroglífics egipcis, els petròglifs maies, el lineal B de l'illa de Creta, l'íber, l'etrusc, les inscripcions en pedra de l'illa de Pàsqua, etc.

Partint de la base que un determinat sistema simbòlic transcriu una llengua parlada, es poden presentar aquests quatre casos:

	llengua coneguda	llengua desconeguda
escriptura coneguda	CAS 1	CAS 2
escriptura desconeguda	CAS 3	CAS 4

En el cas 1 òbviament no hi ha res a dir. El cas 2 és, per exemple, el de l'escriptura etrusca. La civilització etrusca, que provenia del nord de la península itàlica i que va tenir el seu moment de màxima esplendor al voltant del segle VII aC, utilitzava un alfabet molt proper a l'alfabet grec. És per això que diem que l'escriptura etrusca és "coneguda": podem llegir en veu alta les més de 13000 inscripcions etrusques de què els arqueòlegs disposen,

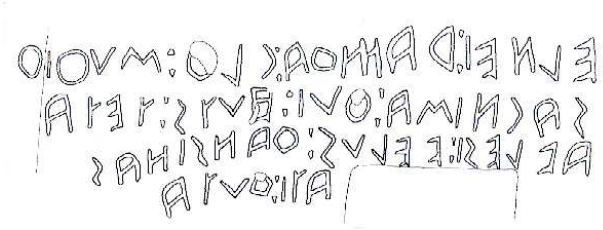

Figura 3: La inscripció etrusca de San Giuliano

però no tenim ni idea del que estem dient, perquè no coneixem absolutament res de la llengua etrusca. Per exemple, si sabeu una mica de grec podreu llegir la famosa inscripció de San Giuliano, del segle III aC, que reproduïm a la Figura 3: *Elnei Ramtha clth suthith sacnisa thui huts teta Avlesi Velus Thansinas ati thuta* (tingueu present que el sentit de lectura és de dreta a esquerra). Desgraciadament, no sabem el que estem dient quan pronunciem aquesta frase.

El cas 4 és el més frustrant de tots. El disc d'Efaistos n'és un exemple famós. Es tracta d'un disc de terra cuita d'uns 30 cm de diàmetre, que va ser trobat l'any 1908 a les restes minoiques de Creta. Vegeu-ne una reproducció i una fotografia a la Figura 4. Conté inscripcions en ambdues cares, però no se saben interpretar. Per la distribució no gens uniforme dels símbols que hi apareixen, s'accepta la hipòtesi que aquest sistema simbòlic transcriu una llengua, però ni tan sols se sap quina civilització és la responsable d'haver creat el disc. A diferència del que és habitual, no s'han trobat altres restes que continguin aquest tipus d'escriptura, ni a Creta ni enlloc més. De manera que el disc podria haver arribat a l'illa, per exemple, després que el vaixell que el transportava, provinent de no se sap on, hagués naufragat.

És impossible desxifrar una escriptura en el cas 4 si no s'aconsegueix reduir el problema al cas 3 (escriptura desconeguda que transcriu una llengua coneguda). Per tant, és imprescindible fer conjectures raonables, basades en hipòtesis de tipus arqueològic, històric, etnogràfic o lingüístic, sobre quina és la llengua que l'escriptura en qüestió transcriu. Precisament, el cas 3 és el més interessant des d'una òptica matemàtica. Perquè resulta que, *tard o d'hora, qualsevol sistema simbòlic del qual es desconeix el significat acaba essent desxifrat quan se sap quina és la llengua que transcriu.*

Potser l'exemple més paradigmàtic d'aquest cas és l'escriptura monumen-

Figura 4: El disc d'Efaistos (Evans, 1908)

tal egípcia: els famosos i bellíssims *jeroglífics* gravats a les parets dels temples religiosos de la civilització del Nil durant el període 3100 aC – 400 dC. Fins al segle XIX, no hi havia ningú que fos capaç d'entendre aquesta escriptura. Al segle XVII, l'erudit Athanasius Kircher havia conjecturat que la llengua que transcrivien els jeroglífics era el copte (llengua parlada pels primers cristians egipcis, i que encara avui dia s'utilitza residualment en la litúrgia de l'Església Copta), però no va ser capaç de desxifrar-los. L'any 1799 els soldats napoleònics van descobrir la Pedra Rosetta, un monòlit de granit on hi havia gravat, en tres escriptures diferents (jeroglífica, demòtica i grega), un decret del rei egipci Ptolemeu V, del 196 aC. Com que tant la llengua com l'alfabet grec són ben coneguts, la pedra Rosetta (juntament amb la hipòtesi, encertada, que els jeroglífics transcriuen la llengua copta) va esdevenir la clau per al desxiframent de l'escriptura jeroglífica egípcia.

Es tracta d'un complicadíssim sistema de pictogrames, la majoria dels quals representen animals, objectes naturals i artificials, figures geomètriques simples o figures antropomòrfiques. Les inscripcions escrites en jeroglífic no estan organitzades sistemàticament, sinó segons criteris estètics. Per exemple, el sentit de lectura dels símbols pot ser vertical o horitzontal, a vegades d'esquerra a dreta, a vegades en sentit contrari, o fins i tot en bustrofèdon. El sentit de lectura ve indicat per la direcció de la mirada dels animals. Un mateix símbol, per exemple un lleó, pot representar la paraula "lleó" (ideograma) o bé el so que correspon a la nostra lletra "l" (fonograma). Alguns

Figura 5: Escriptura jeroglífica egípcia

símbols tenen un valor metafòric: una ploma d'estruç equival a la paraula "justícia", ja que a l'antic Egipte es creia que aquests animals tenen totes les plomes exactament iguals.

El desxiframent de l'escriptura jeroglífica va constituir un esforç intel·lectual sense precedents al qual van contribuir successivament Silvestre de Sacy, J.D. Akerblad, Thomas Young, Jean-François Champollion i molts altres erudits. Actualment, encara queden milers d'inscripcions per desxifrar.

El cas de l'escriptura glífica maia és similar: el seu desxiframent va ser un procés llarg i laboriós, que va començar a ser factible quan es va descobrir que els antics còdexs maies transcrivien el dialecte *cholan*. Actualment, unes tres quartes parts de les inscripcions murals existents a les selves d'Amèrica Central se saben interpretar amb un cert grau de precisió.

Tot i que a anys-llum de distància, el procés per descobrir el significat d'una escriptura antiga és similar a la cadena de raonaments que els protagonistes de la novel·la de Poe *L'escarabat d'or* han d'aplicar per resoldre el següent criptograma, que saben que oculta unes instruccions en llengua anglesa per localitzar un tresor amagat:

```
53!!+305))6* ;4826)4!.)4!);806* ; 48+8#60))85;1!(;:!* 8+
83(88)5*+;46(;88*96*?;8)*!(;485);5*+2:*!(;4956*2(5*-4)88
*;4069285);)6+8)4!!;1(9;48081;8:8!1;48+85;4)485+528806*8
1(!9;48;(88;4(!?34;48)4!;161;:188;!?;
```

El primer raonament que fan és que, molt probablement, el símbol més freqüent del criptograma, el 8, ha de correspondre a la lletra que apareix

amb més freqüència en la llengua anglesa, la *e*. Conjecturen, doncs, que 8 = *e*. Això és coherent amb el fet que el criptograma conté diverses vegades el grup 88, perquè en anglès el grup *ee* és força freqüent (*three*, *tree*, *see*). A partir d'aquí, i tenint en compte les normes ortogràfiques de la llengua anglesa i el fet que algunes estructures (per exemple, paraules curtes com *the*) apareixen amb molta freqüència en els textos anglesos, els desxifradors són capaços d'anar endevinant progressivament més i més símbols, fins que finalment resolen l'enigma.

2.2 La ineficiència del llenguatge natural

Ha arribat el moment de fer-se la següent pregunta: per què sempre s'acaba desxifrant un criptograma quan se sap quina és la llengua en què està escrit el text que es pretén ocultar? O bé: per què sempre s'acaba entenent el significat d'una escriptura quan se sap quina és la llengua que transcriu? La resposta és la següent: perquè, independentment dels símbols concrets que codifiquen els missatges, el text és transcripció d'un *llenguatge natural* (o sigui, humà), i el llenguatge natural és *redundant* i *ineficient*.

Què volem dir quan diem que el llenguatge natural és redundant? Volem dir això:

EL T_XT ES P_T LL_GIR ENC_RA Q_E FALTI_ L_ETR_S.

En teoria caldrien molts menys símbols per expressar amb tota precisió les mateixes idees.

I què volem dir quan diem que el llenguatge natural és ineficient? Volem dir que les normes ortogràfiques són purament arbitràries i no estan orientades a l'eficiència (economia d'espai, velocitat de transcripció, etc). Per exemple, la norma que imposa que després d'una Q sempre hi va una U és una arbitrarietat innecessària des d'un punt de vista purament utilitari: estem utilitzant dos símbols que *sempre* van junts, i per tant n'hi hauria prou d'escriure un únic símbol, per exemple Q.

2.3 Entropia i redundància

Per precisar una mica més el concepte de *redundància*, començarem introduint un concepte previ, el d'*entropia* [10]. Es tracta d'una noció molt important en ciència: probablement haureu sentit la paraula *entropia* en diferents

contextos. Hi ha, per exemple, l'entropia de les lleis de la termodinàmica, l'entropia de Boltzmann, la d'un sistema dinàmic continu o discret, o la de la teoria de la informació. Cada disciplina defineix el concepte segons els seus postulats, però, en general, tots aquests conceptes impliquen alguna idea de mesura del desordre o la complicació d'algun sistema físic o matemàtic, i, de fet, totes les formulacions són equivalents en algun sentit.

Per als lectors no avesats al llenguatge matemàtic, en aquest punt recordarem que una *variable aleatòria* és un experiment aleatori (per exemple, el llançament d'un dau) que té un nombre finit de possibles resultats o *estats* (en el cas del dau, hi ha 6 possibles resultats), cada un amb la seva probabilitat (en el cas del dau, tots els resultats tenen la mateixa probabilitat, 1/6). Els experiments en què tots els possibles resultats tenen la mateixa probabilitat s'anomenen *equiprobables*.

Qualsevol llenguatge humà, posem per cas el *català*, també es considera una variable aleatòria. Podeu imaginar que estem fent el següent experiment aleatori: prenem un text escrit en català, triem a l'atzar una lletra d'aquest text, i observem quina lletra és. Com que el català escrit utilitza l'alfabet a–z de 27 lletres (hi comptem la ce trencada), el nostre experiment aleatori pot tenir 27 possibles resultats ("lletra *a*", "lletra *b*", etc). La característica fonamental dels llenguatges naturals considerats com a variables aleatòries és que no són gens equiprobables. Les lletres a–z no estan uniformement distribuïdes en els textos catalans. Per exemple, la lletra més freqüent, la *e*, apareix amb una probabilitat del 13.891%, mentre que la lletra *z* té una freqüència de tan sols el 0.006%. Podeu comprovar que aquest text està plagat de lletres *e*, i en canvi us costarà molt trobar-hi una *z* fora d'aquest paràgraf.

Doncs bé: si X és una variable aleatòria amb un nombre finit d'estats $x_1, \ldots, x_n$ amb probabilitats respectives $p_1, \ldots, p_n$, es defineix l'*entropia de* X, i es denota $H(X)$, com:

$$H(X) = -\sum_{i=1}^{n} p_i \cdot \log_2(p_i).$$

Fixeu-vos que la fórmula conté logaritmes en base 2. Aquesta base no és important, de manera que també podríem haver pres logaritmes neperians o decimals. Apliquem la fórmula en un parell d'exemples. Calculem l'entropia del llançament d'un dau. Anomenen X aquest experiment. Té 6 possibles resultats, $x_1, x_2, \ldots, x_6$, amb probabilitats $p_1 = p_2 = \ldots = p_6 = 1/6$. Per

tant, la seva entropia és

$$H(X) = -\sum_{i=1}^{6} \frac{1}{6} \log_2\left(\frac{1}{6}\right) = -\log_2\left(\frac{1}{6}\right) = \log_2(6) \simeq 2.58.$$

Posem un altre exemple. Al campus politècnic d'una universitat hi ha matriculats 10000 alumnes, distribuïts així: 4500 alumnes d'Enginyeria Industrial (EI), 1800 d'Arquitectura Tècnica (AT), 500 de Ponts i Camins (PC), 200 d'Informàtica (I), 900 d'Arquitectura (A) i 300 de Matemàtiques (M). Ara considerem un experiment aleatori, Y, que consisteix a triar a l'atzar un alumne d'aquest campus i preguntar-li quina carrera estudia. Hi ha 6 possibles respostes: $y_1 = \text{EI}$, $y_2 = \text{AT}$, $y_3 = \text{PC}$, $y_4 = \text{I}$, $y_5 = \text{A}$ i $y_6 = \text{M}$. Les probabilitats respectives són $p_1 = 0.45$, $p_2 = 0.18$, $p_3 = 0.05$, $p_4 = 0.2$, $p_5 = 0.09$, $p_6 = 0.03$. Per tant, l'entropia de la variable Y és

$$H(Y) = -0.45 \log_2(0.45) - 0.18 \log_2(0.18) - \ldots - 0.03 \log_2(0.03) \simeq 2.10.$$

Observeu que X, que era un experiment equiprobable de 6 resultats, tenia una entropia de 2.58, mentre que Y, que és un altre experiment amb 6 resultats, en aquest cas no equiprobables, té una entropia menor, 2.10. Aquest fet és general: es pot demostrar que *de tots els experiments aleatoris amb n possibles resultats, el que té entropia màxima és l'equiprobable*. Vegem tot seguit per què això és així[1].

Si només hi ha dos resultats possibles, amb probabilitats $x \geq 0$ i $1-x \geq 0$, aleshores hem de buscar el màxim de la funció

$$0 \leq h(x) = -x \log_2(x) - (1-x) \log_2(1-x), \quad \text{per a} \quad 0 \leq x \leq 1. \qquad (1)$$

Estudiant el límits als extrems de l'interval, tenim que $h(0) = h(1) = 0$. Per tant, el màxim d'aquesta funció a l'interval $[0, 1]$ es donarà al seu interior, a un punt on la derivada s'anul·li. Calculem, doncs, els extrems de $h(x)$.

$$h'(x) = -\log_2(x) - \log_2(e) + \log_2(1-x) + \log_2(e) = 0.$$

Aquesta equació és equivalent a

$$\log_2\left(\frac{1-x}{x}\right) = 0,$$

[1] Hi ha demostracions molt més elegants que la que presentem, però que requereixen més bagatge matemàtic. Per exemple, el resultat és una conseqüència quasi directa de la desigualtat de Jensen.

d'on obtenim que $1-x=x$ i, en conseqüència, $x=1/2$. Per tant, l'entropia màxima és $h(1/2)=-\log_2(1/2)=\log_2(2)=1$ i és dona quan les probabilitats són totes dues iguals a $1/2$.

En lloc de fer el cas general, estudiarem només el cas en què l'experiment té tres resultats possibles, amb probabilitats $x\geq 0$, $y\geq 0$ i $1-x-y\geq 0$. La demostració és fàcilment extensible al cas general.

Hem de trobar el valor màxim de la funció

$$h(x,y)=-x\log_2(x)-y\log_2(y)-(1-x-y)\log_2(1-x-y),$$

sobre el triangle delimitat per les rectes $x=0$, $y=0$ i $1-x-y=0$. Observem primer que sobre cadascun dels costats del triangle la funció $h(x,y)$ es redueix a l'estudiada en el cas anterior (1). Per tant, a la vora del triangle, l'entropia h val zero als tres vèrtexs, i el seu valor màxim és 1, que es pren als punts $(0,1/2)$, $(1/2,0)$ i $(1/2,1/2)$. Per veure quin és el seu valor màxim a l'interior del triangle hem de calcular de nou els extrems de h, que vénen donats per la solució del sistema

$$\begin{cases} \dfrac{\partial h(x,y)}{\partial x}=-\log_2(x)-\log_2(e)+\log_2(1-x-y)+\log_2(e)=0, \\ \dfrac{\partial h(x,y)}{\partial y}=-\log_2(y)-\log_2(e)+\log_2(1-x-y)+\log_2(e)=0. \end{cases}$$

Aquest sistema és equivalent a

$$\frac{1-x-y}{x}=1, \quad \frac{1-x-y}{y}=1,$$

que té per solució $x=y=1/3$. Sobre aquest punt la funció h val $h(1/3,1/3)=-\log_2(1/3)=\log_2(3)>1$, i per tant és el valor màxim. En resum: hem provat, tal com volíem, que el cas equiprobable, amb probabilitats $1/3$, $1/3$ i $1/3$, és el que té màxima entropia.

Primera interpretació de l'entropia: incertesa

L'entropia mesura la incertesa que es té *a priori* sobre el resultat d'un experiment aleatori. Dit d'una altra manera, l'entropia mesura fins a quin punt estem insegurs del resultat que tindrà un experiment aleatori, abans que es produeixi l'experiment. Reforcem aquesta interpretació del concepte d'entropia amb una altra interpretació equivalent.

Segona interpretació de l'entropia: nombre de preguntes binàries

Quan s'ha produït un experiment aleatori que ha tingut un resultat concret, i nosaltres ignorem quin ha estat aquest resultat, l'entropia mesura el nombre mitjà de preguntes binàries (amb resposta SÍ/NO) que, amb la millor estratègia possible, haurem de formular a un observador que conegui quin ha estat el resultat de l'experiment, per tal d'endevinar aquest resultat. Posem-ne un exemple. Considerem el següent experiment, Z. Suposem que tenim una bossa tancada que conté quatre boles, dues de color negre, una de color blanc i una de color vermell. Una persona extreu a l'atzar una bola de dins de la bossa i observa el seu color. Quina és l'entropia d'aquest experiment? Hi ha 3 possibles resultats: z_1 = negre, amb probabilitat $p_1 = 1/2$, z_2 = blanc, amb probabilitat $p_2 = 1/4$, i z_3 = vermell, amb probabilitat $p_3 = 1/4$. Calculem l'entropia de Z:

$$H(Z) = -\frac{1}{2}\log_2\left(\frac{1}{2}\right) - \frac{1}{4}\log_2\left(\frac{1}{4}\right) - \frac{1}{4}\log_2\left(\frac{1}{4}\right) = \frac{3}{2} = 1.5.$$

Nosaltres volem saber el resultat de l'experiment, i hem de fer preguntes (amb resposta SÍ/NO) a la persona que ha vist quin color té la bola extreta. Quina és la millor estratègia possible? Si ho penseu un moment, està clar que la primera pregunta que cal fer és *la bola extreta és de color negre?* En un 50% dels casos, la resposta serà SÍ, i en aquest cas ja haurem endevinat el resultat de l'experiment: color negre. En canvi, en un 50% dels casos la resposta serà NO, i en aquests casos caldrà fer una altra pregunta, per exemple *la bola extreta és de color blanc?* Tant si la resposta és SÍ com si és NO, ja no caldrà fer més preguntes perquè ja haurem endevinat el resultat: color blanc en el primer cas i color vermell en el segon. Així doncs, la meitat de les vegades haurem hagut de fer una sola pregunta, i la meitat de les vegades ens caldrà fer dues preguntes. En mitjana, doncs, haurem de fer 1.5 preguntes. Observeu que l'entropia de Z és exactament 1.5.

Tercera interpretació de l'entropia: llargada d'un codi òptim

Quan tenim un sistema simbòlic o alfabet amb el qual escrivim missatges en una determinada llengua, i volem recodificar aquests missatges utilitzant un sistema de només 2 símbols (diguem, 0 i 1) que d'ara endavant anomenarem *bits*, l'entropia d'aquest alfabet mesura el nombre mitjà de bits per símbol que cal utilitzar amb la millor de les codificacions possibles. Vegem-ho.

Suposem, per simplificar, que estem escrivint textos en una llengua extraterrestre que utilitza un alfabet de només 4 símbols: A, B, C i D. A més, tal com passa amb les llengües terrícoles, les freqüències d'aquests 4 símbols no són uniformes: la A apareix amb una freqüència del 50%, la B amb una freqüència del 25% i la C i la D amb una freqüència del 12.5%. Aquí tenim un exemple de missatge escrit en aquesta llengua:

CABAADA BAD BACAA ABBA

Calculem l'entropia d'aquesta llengua:

$$-\frac{1}{2}\log_2\left(\frac{1}{2}\right)-\frac{1}{4}\log_2\left(\frac{1}{4}\right)-2\cdot\frac{1}{8}\log_2\left(\frac{1}{8}\right)=\frac{7}{4}=1.75.$$

Bé, ara proposem una recodificació binària d'aquesta llengua: canviarem el símbol A per 00, el símbol B per 01, el símbol C per 10 i el símbol D per 11. De manera que, per exemple, el missatge CABAADA BAD BACAA ABBA quedaria escrit així:

10000100001100010011010010000000010100

La longitud mitjana d'aquesta codificació és 2, perquè tots els símbols tenen 2 bits de longitud. L'entropia, en canvi, ens havia sortit 1.75. Això vol dir, segons la interpretació de l'entropia que estem donant aquí, que ha d'existir una altra codificació binària d'aquest alfabet, més eficient en el sentit que la longitud mitjana dels símbols ha de ser menor, de només 1.75 bits. Vegem quina pot ser aquesta codificació òptima:

símbol	freqüència	codi	longitud
A	0.5	0	1
B	0.25	10	2
C	0.125	110	3
D	0.125	111	3

Quina és la longitud mitjana d'aquesta codificació? Atenció! Per al càlcul de la longitud mitjana cal tenir en compte amb quina probabilitat apareix cada un dels 4 símbols. Així, tenim una longitud mitjana de $0.5\cdot 1+0.25\cdot 2+2\cdot 0.125\cdot 3=1.75$ bits. Hem igualat l'entropia!! Observem com quedaria escrit el missatge CABAADA BAD BACAA ABBA en aquesta nova codificació:

11001000111010011110011000010100

Us adonareu que la longitud del missatge s'ha escurçat sensiblement. És una codificació més eficient. Si una comissió de científics terrícoles intenta desxifrar aquests missatges escrits en llengua extraterrestre, els serà molt més difícil fer-ho en aquest segon cas.

En aquest punt potser algun lector intentarà proposar encara una altra codificació alternativa que superi l'anterior. És a dir, una codificació per a la qual la longitud mitjana dels símbols sigui menor que 1.75. Per què no? Aquí en tenim un exemple:

símbol	freqüència	codi	longitud
A	0.5	0	1
B	0.25	10	2
C	0.125	11	2
D	0.125	001	3

Amb aquesta brillant idea, hem aconseguit una codificació que té per longitud mitjana $0.5 \cdot 1 + 0.25 \cdot 2 + 0.125 \cdot 2 + 0.125 \cdot 3 = 1.625$ bits, menor que l'entropia! Però resulta que ens hem passat de llestos: amb aquesta nova codificació, si rebem el missatge 0010 no serem capaços de decidir si correspon a la paraula extraterrestre AAB (0–0–10) o bé a la paraula DA (001–0). Els missatges no tenen una interpretació única! Es diu que aquest codi no és *unívocament interpretable*. Hi ha un teorema que afirma que l'entropia d'una font aleatòria sempre serà menor o igual que la longitud de qualsevol sistema simbòlic unívocament interpretable que codifiqui la font. L'entropia constitueix una barrera infranquejable [1].

Redundància

Tal com havíem dit, acabem aquest apartat definint rigorosament el concepte de *redundància* d'una llengua. Aquesta noció quantifica en quina mesura la llengua en qüestió s'allunya d'una llengua *ideal* que utilizi el mateix alfabet i que sigui absolutament aleatòria, en el sentit que totes les lletres d'aquest alfabet apareixin amb la mateixa freqüència.

Més precisament: prenem un llenguatge natural, per exemple el català, que s'expressa mitjançant l'alfabet a–z de 27 símbols, i definim la *ràtio absoluta* R de la llengua catalana com l'entropia d'un experiment equiprobable

amb 27 possibles resultats. Això és,

$$R = -\sum_{i=1}^{27} \frac{1}{27} \log_2 \left(\frac{1}{27}\right) = \log_2(27) \simeq 4.75.$$

Òbviament aquesta quantitat és la mateixa per a qualsevol llengua que utilitzi el mateix alfabet a–z, per exemple el francès, ja que només depèn del nombre de símbols que conté aquest alfabet. En canvi, ara definirem una altra quantitat, la *ràtio del llenguatge*, r, que sí és pròpia de cada llengua en particular. Prenem un altre cop l'exemple del català. La distribució estadística de les lletres en els textos catalans és la següent: E 13.89%, A 12.55%, S 8.43%, R 7.74%, I 6.99%, L 6.76%, N 6.40%, T 6.11%, O 5.71%, U 4.18%, D 3.94%, C 3.60%, M 3.16%, P 2.72%, V 1.40%, Q 1.35%, B 1.32%, G 1.28%, Ç 1.06%, F 1%, H 0.72%, X 0.52%, J 0.30%, Y 0.18%, Z 0.006%, K 0.004%, W 0.001%. Si calculeu l'entropia tenint en compte aquesta distribució de probabilitats, obtindreu 3.99. Com ja sabíem, surt més baixa que la ràtio absoluta.

Però alguna cosa no acaba de funcionar del tot bé. Algun lector podria sospitar que l'entropia del català és encara menor que 3.99, i tindria raó. Pensem que, si només tenim en compte la distribució de les lletres individuals, llavors si en un text veiem una lletra Q i algú ens pregunta *quina lletra vindrà a continuació?*, haurem de respondre: *No ho sé: potser una E amb probabilitat 13.89%, potser una A amb probabilitat 12.55%...* No estem tenint en compte cap regla ortogràfica ni cap de les rigideses constructives que fan que el llenguatge natural sigui encara molt més redundant.

Fem el següent: considerem no pas la distribució estadística de les lletres individuals, sinó la distribució dels $27^2 = 729$ possibles parells de lletres AA, AB, AC, ... ZX, ZY, ZZ. Es tractaria de prendre textos escrits en català i fer una estadística de les freqüències d'aparició de tots i cada un d'aquests parells de lletres. Per exemple, la probabilitat del parell QS serà zero, mentre que les probabilitats dels parells PA, RE o LL seran positives. Si calculem l'entropia d'aquest nou alfabet de 729 símbols, i dividim per 2, obtindrem una mena d'entropia mitjana per caràcter, que s'anomena *ràtio per a missatges de longitud 2*, i si ens prenguéssim la molèstia de calcular-la (cosa que no farem) trobaríem que és menor que 3.99. Considerant parells de lletres ja estem incorporant algunes de les normes ortogràfiques del català: assignant probabilitat zero a tots els parells en què la primera lletra és una Q i la segona no és una U ja estem incorporant la norma "després d'una Q sempre s'escriu una U".

Aquest procediment es pot estendre a les $27^3 = 19683$ possibles ternes AAA, AAB, ... ZZZ per tal d'obtenir la ràtio per a missatges de longitud 3, i així successivament. Un teorema clàssic de Teoria de la Informació ens assegura que la *ràtio per a missatges de longitud n* decreix monòtonament a mesura que n creix, i s'acosta asimptòticament a un límit. Aquest límit és el que s'anomena *ràtio del llenguatge*, i el denotarem amb la lletra r. Com més gran és la n considerada, més normes ortogràfiques de la llengua en qüestió estarem incorporant. És obvi que el càlcul d'aquestes ràtios ha de ser, necessàriament, de naturalesa empírica i aproximada.

La *redundància* del llenguatge es defineix com la diferència $R - r$. S'ha comprovat (experimentalment) que la majoria de llengües tenen una ràtio r a l'entorn d'1.5. Com més gran és la redundància d'una llengua, més allunyada està d'una llengua aleatòria. I més fàcil serà desxifrar un text que transcrigui aquesta llengua.

3 Esquemes de compartició de secrets

La necessitat d'introduir la noció d'*esquema de compartició de secrets* respon al següent axioma criptogràfic: *una informació molt important no pot estar en mans d'una única persona*. Per exemple, és inconcebible pensar que els codis numèrics que activen el llançament de l'arsenal nuclear dels Estats Units d'Amèrica siguin coneguts només pel seu president. Posem un altre exemple més casolà, que he extret textualment de [4]. Una oficina bancària té contractats 5 treballadors (Nil, Ot, Pau, Quim i Rut). La feina es distribueix en torns diaris i durant cada jornada laboral només hi ha 3 persones treballant a l'oficina (cada dia descansen dues persones diferents). La combinació de la caixa forta és un nombre de 6 xifres, diguem 121314. El que pretenem és "trencar" aquesta informació (el nombre 121314) en bocins i distribuir-los d'alguna manera entre els 5 treballadors, però, i això és el més important, no volem que un treballador aïllat pugui recuperar el nombre ell sol, i que tampoc ho puguin fer dos treballadors si reuneixen els seus respectius bocins. Volem que faci falta reunir a com mínim 3 d'aquestes persones per poder reconstruir la combinació de la caixa forta. Però, a més a més (i aquest és el requisit més important i més restrictiu), com que cada dia hi ha 3 persones diferents a l'oficina, volem que la combinació de la caixa forta es pugui reconstruir *siguin quines siguin les 3 persones que es reuneixen*.

Formalitzem, doncs, la noció que ens ocupa: un *esquema de compartició*

de secrets és una situació en la qual el secret està repartit entre N persones, i coneixent els fragments d'informació de només M d'elles (on $M < N$) es pot recuperar el secret, siguin quines siguin aquestes M persones.

Si hi esteu interessats, podeu intentar resoldre el problema de dissenyar un mecanisme, protocol o algorisme que implementi un esquema de compartició de secrets. Tot seguit donarem una pista que us pot ajudar (i finalment resoldrem completament el problema, proposant un d'aquests mecanismes). La pista és la següent: podem pensar que una *equació* com $x + 2y - z = 20$ és una certa quantitat d'informació sobre unes quantitats numèriques indeterminades (x, y i z) que ens agradaria conèixer. En aquest exemple, la informació proporcionada (que si restem la primera quantitat de la tercera i hi sumem el doble de la segona, el resultat és 20) no és suficient per determinar unívocament el valor de les incògnites: els valors $x = 0$, $y = 10$ i $z = 0$ compleixen l'equació, però també la compleixen els valors $x = 25$, $y = 0$, $z = 5$. De fet, hi ha infinites possibilitats. Per tant, si volem saber més coses sobre el valor que s'amaga al darrere de les incògnites x, y i z, ens hauran de donar més informació. I, com ja hem dit, informació = equació... Aquí s'acaba la pista per als lectors agosarats.

El protocol que proposem com a solució al problema és el següent: trenquem la combinació de la caixa forta, 121314, en tres fragments, $(12, 13, 14)$. A cada un dels 5 treballadors li proporcionem una equació lineal en 3 incògnites: $x-y+z = 13$ (Nil), $2x-y+z = 25$ (Ot), $z-x = 2$ (Pau), $x+2y-2z = 10$ (Quim), i $x + y - z = 11$ (Rut). Observem que $x = 12, y = 13, z = 14$ és una solució de cada una d'aquestes equacions. Dit d'una altra manera, cada una d'aquestes equacions proporciona informació sobre els 3 valors de què consta la combinació secreta. En Nil, utilitzant la informació de què disposa, $x-y+z = 13$, no podrà deduir la combinació secreta, perquè aquesta equació té infinites solucions. Tan sols podrà deduir que si restem el primer tros de la combinació secreta del segon tros, i hi sumem el tercer tros, el resultat serà 13. En Nil encara estarà perdut si decideix adquirir més informació reunint-se amb qualsevol dels altres treballadors, diguem la Rut, i posant en comú les seves respectives informacions:

$$\begin{cases} x - y + z &= 13 \\ x + y - z &= 11 \end{cases}$$

El sistema d'equacions resultant encara té infinites solucions, i en Nil

i la Rut no podran recuperar el secret[2]. Caldrà encara adjuntar l'equació provinent d'un tercer treballador per tal que el sistema resultant tingui una solució única. Resolent el sistema, els 3 treballadors reunits determinaran que $x = 12$, $y = 13$ i $z = 14$, amb la qual cosa ja hauran reconstruït la combinació: 121314.

Naturalment, aquestes equacions han estat triades de manera que el sistema format per les 5 equacions és compatible determinat i qualsevol subsistema de 3 o més equacions també ho és. Com a exercici final, el lector interessat pot intentar visualitzar geomètricament en quina posició relativa estaran situats a l'espai $\mathbb{R}^3$ els 5 plans que defineixen cada una d'aquestes 5 equacions.

Referències

[1] J. M. Brunat, E. Ventura, *Informació i codis*, ed. UPC, Barcelona, 2001.

[2] L. J. Calvet, *Historia de la escritura*, Paidós, Barcelona, 2007.

[3] A. Conan Doyle, *El regreso de Sherlock Holmes* (conté *La aventura de los monigotes*), ed. Anaya, Madrid 2008.

[4] J. Domingo, J. Herrera, *Criptografia per als serveis telemàtics i el comerç electrònic*, Universitat Oberta de Catalunya, Barcelona, 1999.

[5] D. Juher, *L'art de la comunicació secreta*, Llibres de l'Índex, Barcelona, 2004.

[6] E. A. Poe, *Contes* (conté *L'escarabat d'or*), Quaderns Crema, Barcelona, 1999.

[7] M. Serra, *Verbàlia*, ed. Empúries, Barcelona, 2000.

[8] S. Singh, *Los códigos secretos*, Debate, Madrid, 2000.

[2] De fet, ajuntant la seva informació, en Nil i la Ruth arriben a deduir que $x = 12$ i que $y = z + 1$. Per tant, sabent que la combinació de la caixa té sis xifres, han obtingut 99 possibles combinacions, $120100, 120201, \ldots 129998$, una de les quals ha d'obrir la caixa forta. És clar que el nombre de possibilitats podria disminuir si els treballadors tinguessin targes amb altres equacions lineals. Els sistemes lineals amb coeficients enters, per als quals busquem només solucions enteres, s'anomenen sistemes lineals diofàntics, i apareixen sovint a diversos problemes pràctics.

[9] J. Tarrés (obra col·lectiva), catàleg de l'exposició *Ciència recreativa de Josep Estalella al segle XXI*, Fundació Caixa de Girona, Girona, 2008.

[10] J. C. A. Van der Lubbe, *Information theory*, Cambridge University Press, 1997.

[11] J. Verne, *La jangada*, ed. Porrua, Mèxic, 1986.

[12] http://www.iec.csic.es/criptonomicon/ Pàgina del CSIC que conté un butlletí periòdic gratuït amb entrades de tot tipus, des d'anècdotes històriques fins a novetats tecnològiques amb detalls tècnics.

[13] http://el.tesorodeoviedo.es Informació i documentació impulsades per l'ajuntament d'Oviedo en el marc del projecte Oviedo Doce Siglos.

Dept. d'Informàtica i Matemàtica Aplicada
Universitat de Girona
17071-Girona
Web: ima.udg.edu/~juher
juher@ima.udg.edu

Publicat el 11 de març de 2009