

José N. Alonso Álvarez
Miguel Á. Mirás Calvo

sensefronteres

Els secrets de la criptografia



**Premi Europeu
de Divulgació Científica
Estudi General**

OCULTAR I DESVELAR

Els anteriors caràcters, segons que tots poden endevinar fàcilment, formen una xifra, és a dir, contenen un significat [...]

Les circumstàncies i una certa predisposició mental m'han portat a interessar-me per algunes endevinalles i és, en realitat, dubtós, que el geni humà pugui crear un enigma semblant que el mateix enginy humà no sigui capaç de resoldre amb una aplicació adequada.

EDGAR ALLAN POE

L'escarabat d'or

És un fet ben conegut que la base de les societats humanes és la comunicació entre els seus membres. Però, sovint, les persones no desitgen que algú alié a la comunitat tinga accés a les comunicacions que comparteixen. Es crea, aleshores, la necessitat de mantindre en secret el contingut d'aquesta comunicació. A voltes no és gens complicat; n'hi ha prou amb trobar un lloc on les persones que volen mantindre el secret s'hi puguin veure soles; però segons que les societats van assolint una complexitat més gran, aquesta opció deixa de ser viable i la informació s'ha de transmetre mitjançant canals que en garantisquen la seguretat. Podem pensar en molts contextos diferents: religió, política, economia, exèrcit,

màgia... I aquesta necessitat va generar l'origen d'una nova ciència: la criptologia.

1.1. CRIPTOLOGIA

Podríem definir la criptologia (del grec *kriptos*, 'ocult', i *logos*, 'estudi') com la ciència que estudia tant els mètodes per a mantindre en secret la informació continguda en un missatge i assegurar la privacitat de les nostres comunicacions, com just el contrari, és a dir, les tècniques que podem utilitzar per a trencar aquesta privacitat i accedir a una informació sense estar-hi autoritzats.

Al principi, la criptologia abastava un espai clarament delimitat. En primer lloc, perquè el nombre de missatges era escàs i perquè solien circumscriure's als membres d'una mateixa comunitat. D'altra banda, tampoc no abundaven els suports sobre els quals transmetre la informació, com ara pergamins o pells d'animals. I, a pesar que al cap d'un temps va aparèixer el paper, tampoc no calia ocultar la informació amb mitjans excessivament sofisticats, perquè una gran part de les persones no sabia llegir ni escriure, de manera que, per a la majoria, un text escrit ja era, per ell mateix, un missatge impossible de desxifrar.

El primer text que podríem relacionar amb la criptologia data dels voltants de l'any 1900 abans de la nostra era. Es tracta d'un gravat sobre pedra que va ser descobert a la recambra de la tomba del noble egipci Khnumhotep II, a Menet Khufu, com mostrem en la figura 1.1.



Fig. 1.1. Tomba de Khnumhotep II (Kurohito. Llicència Creative Commons).

En sentit estricte no es tracta de criptologia perquè el gravador no pretenia en absolut ocultar un missatge. En realitat, probablement només intentava cridar l'atenció per tal que els visitants llegiren el text perquè, per als egipcis, la lectura de les oracions fúnebres ajudava el difunt en el més enllà, i per això hi va incorporar un dels elements essencials de la criptologia: una transformació deliberada de l'escriptura, en alternar alguns símbols jeroglífics comuns amb alguns altres no tan quotidians. En l'actualitat, encara fem una cosa semblant; per exemple, si pensem en les plaques d'inauguració de molts edificis, en les quals, a més de fer servir sovint la numeració romana, utilitzem un llenguatge pompós de l'estil: «Aquest edifici va ser inaugurat quan era president l'Excel·lentíssim Senyor...».

Amb el pas del temps, va anar afegint-se en diversos gravats funeraris el segon element: la intenció d'amagar un missatge, en molts casos per a augmentar els poders màgics dels escrits religiosos (de la mateixa forma com, ara, s'inicien els encantaments amb la paraula *abracadabra*, o algunes

fórmules semblants, per a despertar la curiositat del lector). Però el costum va decaure a Egipte i les inscripcions d'aquesta classe van desaparèixer dels epitafis.

El xiquet que volia llegir els jeroglífics

Departament d'Isère, França, any 1802. Joseph Fourier (1768-1830), matemàtic de renom, acabava de tornar de l'expedició de Napoleó Bonaparte (1769-1821) a Egipte, en la qual havia participat com a científic reputat. En la seua condició de prefecte d'Isère, va decidir convidar a gaudir de la seua col·lecció d'antiguitats un xiquet de dotze anys considerat un prodigi, Jean-François Champollion (1790-1832), que destacava entre els estudiants de les escoles de la regió perquè semblava posseir un do especial per a les llengües orientals. L'afortunat jove, que s'identificava amb el nom de Champollion le Jeune (Champollion el Jove), va quedar impressionat pels objectes que atresorava el seu amfitrió. Les inscripcions el fascinaren i va preguntar: «Què signifiquen?», i Fourier li va respondre: «No ho sap ningú».

Amb el pas del temps, Champollion es va convertir en un fantàstic lingüista, capaç de parlar amb fluïdesa llatí, grec, hebreu, siríac, àrab, copte i caldeu. En 1799, un soldat francès havia descobert una pedra de basalt d'un metre d'altura en una ciutat situada al delta del Nil que els europeus anomenaven Rosetta. La gran llosa mostrava un text que semblava ser el mateix missatge en tres escriptures diferents: jeroglífics en la part superior, demòtic en la d'enmig i grec en la inferior. Champollion, inspirant-se en el treball de Thomas Young (1773-1829), va comparar sistemàticament els símbols de les tres parts de la pedra de Rosetta, fent servir el grec com la clau per a desxifrar l'escriptura jeroglífica egípcia. El Champollion

adult estava en condicions de respondre a la pregunta que el Champollion jove havia formulat a Fourier. Aquells símbols, inintel·ligibles fins aquell moment, revelaven els misteris de l'extraordinària cultura que els havia inventat feia mil·lennis.



Si avancem en el temps, trobem a Mesopotàmia una taula del 1500 abans de la nostra era, amb escriptura cuneïforme que mostra la fórmula per a fabricar esmalts de ceràmica (fig. 1.2). Està escrita canviant sons i amb algunes altres modificacions amb les quals l'escriba pretén mantindre en secret la tècnica; per això podem considerar el text com el primer exemple de document criptològic.



Fig. 1.2. Taula amb escriptura cuneïforme.

A poc a poc, segons que les societats assoleixen un grau de sofisticació més gran, els mètodes per a ocultar una informació van començar a ser d'ús freqüent, de manera que la criptologia es va incorporar a contextos cada vegada més diferents. Al principi, probablement va ser utilitzada en textos religiosos per a transmetre coneixements als iniciats o, en l'àmbit de la màgia, per a mantindre el secret dels conjurs i els encantaments. Més endavant, devien entrar en joc l'alquímia i l'economia, de manera que només els membres d'un gremi o d'una família pogueren conèixer les fórmules magistrals utilitzades en un apòzema o en un procés de fabricació. Tampoc no hem d'oblidar l'ús militar, per a la comunicació, en secret, dels diversos cossos de l'exèrcit o en l'espionatge entre estats. Per descomptat, també podem assenyalar la necessitat de mantindre la privacitat dels missatges amorosos entre amants, bé per a preservar la intimitat, bé perquè es tractava d'afectes prohibits. I, per a rematar una llista que sempre estarà incompleta, la criptologia era imprescindible perquè els conspiradors polítics o els membres d'una societat perseguida tingueren la possibilitat de comunicar-se sense arriscar les vides.

Tot això ens aboca a pensar que un assumpte que, en principi, podia haver començat com un joc, va anar complicant-se cada vegada més fins a convertir-se en una ciència. I aquesta ciència va assolir tanta importància que en els nostres dies podem dir, sense exagerar gens ni miqueta, que sense ella, la societat contemporània no funcionaria de la manera com estem acostumats a veure-la funcionar. Qualsevol transacció bancària, la firma digital d'un document, una compra per internet, el DNI electrònic (fig. 1.3) són exemples de la presència de la criptologia en el nostre quefer diari.

- Esteganografia. De *steganos*, ‘encobert’, i *grafo*, ‘escriure’. Estudia les tècniques per a ocultar físicament els missatges de manera que no puguin ser interceptats. El resultat d’aplicar aquestes tècniques s’anomena *esteganograma*.
- Esteganoanàlisi. La tècnica contrària a l’anterior. S’ocupa de detectar els missatges ocults.
- Criptografia. Estudia els mètodes per a protegir una informació sense necessitat d’ocultar-la, la manera de fer-la intel·ligible per a una persona no autoritzada. La informació protegida amb aquesta tècnica s’anomena *criptograma*.
- Criptoanàlisi. Una vegada més ens trobem amb la tècnica oposada a l’anterior perquè, ara, estudiem les tècniques per a accedir a la informació que amaga un criptograma.

En resum, ens trobem davant de dues forces que actuen sempre en un sentit contrari, oposat. Els esteganògrafs i els criptògrafs, que volen protegir la informació, i els esteganoanalistes i criptoanalistes, que pretenen accedir a la informació sense estar-hi autoritzats.

En el nostre llibre, tot i que recopilarem alguns dels mètodes esteganogràfics més coneguts, centrarem la nostra atenció en els criptogràfics.

1.2. ALICE, BOB I EVE

Havent establert el nostre camp de treball, presentarem els nostres personatges perquè, d’una manera diferent de com passa en alguns altres camps científics, la criptologia sempre té present que els problemes que resol tenen una utilitat social

evident, i per això és habitual humanitzar-la. Tot va començar quan, l'any 1978, en un treball de Ronald Rivest (Nova York, 1947) per tal d'evitar dir «la persona A vol enviar un missatge a la persona B», va utilitzar la fórmula següent: «Alice vol enviar un missatge a Bob». A partir d'aquell moment, van anar afegint-se més persones a la trama. La més important va ser Eve, que interceptava els missatges i tractava de desxifrar-los sense permís. El nom escollit deriva, probablement, de la semblança en la pronúncia del nom amb l'inici de la paraula *eavesdropper*, 'espia' en anglès. Durant molts anys, les aventures dels tres personatges han sigut molt variades. Alice i Bob han estat casats i divorciats, contents i tristos, pròxims i distants... Però, independentment del seu estat civil o anímic, sempre s'han enviat missatges: d'amor, d'odi, amb informacions econòmiques, amb conjurs, etcètera... A propòsit d'Eve, sempre és capaç d'interceptar els missatges, d'accedir al contingut, tant si pot desxifrar-los com si no, encara que, en general, és presentada com una intrusa sense malícia, més com la típica xafardera que no com una persona malvada. Honesta, però curiosa, com solen dir en l'argot criptològic.

De manera que, en els llibres de criptologia, és corrent utilitzar Alice, Bob i Eve per a descriure les diverses situacions. En la majoria de les llengües s'han fet servir els mateixos noms. En algunes altres llengües, s'han adaptat, i per això podem trobar Alice, Bernard i Carol en francès; o Alicia, Benito i Eva en espanyol, que són els noms que farem servir en el nostre llibre, adaptats al català: Alícia, Benet i Eva.

Descrivim, per tant, la situació. Alícia, Benet i Eva són tres vells companys d'institut. Els dos primers continuen

mantenint un contacte regular i Eva tracta de clavar-se entremig sempre que pot. Ja ho ha aconseguit més d'una vegada, de manera que Alícia decideix buscar ajuda per a comunicar-se amb Benet amb garanties, és a dir, que encara que Eva intercepte els missatges que s'intercanvien, una situació que dona per feta, no siga capaç d'interpretar-los. Al llarg del llibre intentarem ajudar Alícia i li proposarem diverses estratègies, des de les més senzilles fins a les més complexes. Per a fer-ho, anirem detallant els principals mètodes criptogràfics que pot utilitzar. Però, abans, per la importància històrica que té, començarem per donar a conèixer una breu informació sobre els mètodes estegano-gràfics més coneguts.

Grândola, vila morena

Lisboa, 1974. A les 00:25 hores del 25 d'abril, Rádio Renascença transmet una cançó del cantautor José Zeca Afonso (1929-1987), prohibida per la dictadura, que comença amb els versos següents:

Grândola, vila morena
terra de fraternidade
o povo é quem mais ordena
dentro de ti, ó cidade

És el senyal acordat per a començar l'alçament contra el règim dictatorial que governa Portugal i que va passar a la història com la Revolució dels Clavells. La idea no era original, una acció semblant havien fet els aliats per a comunicar als membres de la resistència francesa l'imminent inici del desembarcament de Normandia.

En realitat, no estem davant d'un mètode criptogràfic o estegano-gràfic, perquè la informació no està xifrada com un

criptograma i la difusió es fa a la vista de tots; però comparteix amb la criptologia una característica fonamental: la transmissió d'una informació secreta. I, d'altra banda, resulta molt eficaç. Durant els conflictes del segle xx, va ser corrent comunicar secrets emetent cançons per la ràdio, enviant telegrams o publicant anuncis als diaris.

El treball del criptoanalista, en el cas present, no és desxifrar el missatge o trobar-ne l'amagatall, sinó impedir que arribi al receptor o, almenys, si el receptor el rep, que siga un missatge alterat i sense cap utilitat. Durant les dues guerres mundials, milers de persones, els coneguts amb el nom de censors, es van dedicar a exercir la censura d'aquesta forma. Conscients que es tractava d'un treball molt difícil, les autoritats els ajudaven posant obstacles de moltes maneres a la difusió dels missatges. Per exemple, es van prohibir les partides internacionals d'escacs per correu i els segells de les cartes van ser substituïts per uns altres iguals, però amb uns altres números de sèrie. Si es tractava de missatges d'enamorats que indicaven que calia entregar un ram de flors a una persona, s'hi eliminaven les referències a qualsevol classe de flor i la data d'entrega, de manera que el florista ho havia de decidir ell mateix. I, en els telegrams, els censors canviaven algunes paraules per paraules diferents, però amb el mateix significat. El cas era que totes aquelles precaucions eren necessàries. És conegut el cas d'un telegrama que indicava «Ha mort el pare» i que va ser canviat per «Ha faltat el pare». Poc de temps després d'haver-lo enviat, l'oficina de telègrafs va rebre una nova comunicació que preguntava: «El pare ha mort o ha faltat?», una pregunta que demostrava que el primer missatge amagava un significat ocult.