SIGNATURES DIGITALS, L'ART DE SIGNAR D'AVUI

Pilar Bayer

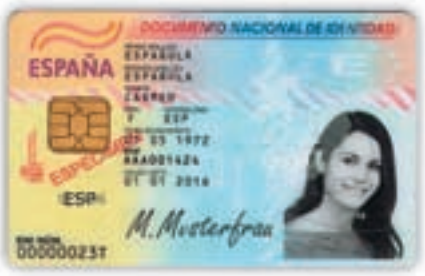
La implantació de les noves tecnologies comporta un seguit de canvis significatius en els nostres usos i costums. Un d'ells afecta l'art de signar. Internet ofereix la possibilitat de signar documents sense la presència física de les persones implicades. Però, perquè aquest tipus de signatures siguin reconegudes, cal que es realitzin amb garanties. Les signatures digitals plantegen problemes legals, científics i tècnics dignes de consideració. En aquest article comentem alguns aspectes de la base matemàtica que els és inherent.

«LA SIGNATURA ELECTRÒNICA ÉS UN CONJUNT DE CARÀCTERS QUE S'AFEGEIXEN A UN DOCUMENT ELECTRÒNIC I QUE PERMETEN AUTENTIFICAR LA IDENTITAT DEL "SIGNATARI"»

Per il·lustrar un dels protocols més emprats en les signatures electròniques hem elaborat un petit relat protagonitzat per dos personatges de ficció: Tintín i el capità Haddock. Tintín rep un missatge misteriós, xifrat i signat per Haddock; per esbrinar si la signatura és autèntica recorrerà als coneixements del professor Tornassol. L'episodi no és extret de cap de les populars narracions d'Hergé, però sí que ho és el contingut del missatge; de ben segur que els seguidors d'aquest heroi no tindran cap dificultat per identificar-lo.

SIGNATURES ELECTRÒNIQUES, D'ACORD AMB LA LLEI

El 17 de setembre de 1999, el Consell de Ministres aprovà el Reial Decret Llei 14/1999 sobre signatura electrònica (BOE 224/1999, de 18 de setembre). El 20 de juny de 2003, un Projecte de Llei de signatura electrònica fou publicat en el BOCG 158-1. El 19 de desembre de 2003, s'aprovava la Llei 59/2003 sobre signatura electrònica (BOE 304/2003, de 20 de desembre). El 13 de febrer de 2004, el Consell de Ministres donà llum verda al DNI electrònic, la implantació del qual s'iniciarà aquest any.



El DNI electrònic serà una targeta que portarà un xip amb informació digital. Entre altres dades identificadores de caràcter personal, el xip inclourà un certificat electrònic, per autentificar la identitat del ciutadà; un certificat electrònic reconegut, per emetre signatures electròniques reconegudes, i claus criptogràfiques per a l'emissió i verificació de les signatures.

Òbviament, sota el nom *signatura electrònica* no es contempla el fet d'escriure el nostre nom a la fi d'un missatge electrònic, acte que està mancat de tot valor legal. La signatura electrònica és un conjunt de caràcters que s'afegeixen a un document electrònic i que permeten autentificar la identitat del *signatari*. El signatari és una persona física, que pot actuar en nom propi o en nom d'una persona física o jurídica a la qual representa.

La llei distingeix entre signatura electrònica i *signatura electrònica reconeguda*. La signatura electrònica reconeguda és la signatura electrònica basada en un *certificat electrònic reconegut*; té el mateix valor legal que la signatura manuscrita. Els certificats electrònics reconeguts són documents signats electrònicament que han de complir una sèrie de requisits. Permeten: (I) l'autentificació de les parts, és a dir, que l'emissor i el receptor del missatge són qui realment diuen ser; (II) garantir la integritat del missatge; és a dir, que aquest no és alterat després de ser signat; (III) garantir la confidencialitat del missatge; és a dir, que només l'emissor i el receptor hi tenen accés; (IV) garantir la irrefutabilitat del missatge; és a dir, que el signatari no en pugui negar l'autoria.

En l'emissió d'una signatura electrònica la llei contempla, a més, el *prestador de serveis de certificació* i els dispositius de *creació i verificació* de la signatura.

El prestador de serveis de certificació és una persona física o jurídica que expedeix certificats electrònics als signataris i els presta el suport necessari en relació a la signatura electrònica. Els certificats electrònics donen fe de la identitat dels usuaris i poden proporcionar, a més, les eines de signatura electrònica. Els dispositius físics de creació de signatures poden variar d'uns casos a altres; es poden utilitzar targetes intel·ligents, màquines lectores, CD,

PIN, etc. L'entitat prestadora de serveis facilita el software necessari per a la creació i verificació de les signatures (generalment via Internet), de manera que l'usuari pugui quedar al marge dels aspectes tècnics.

EL DNI ELECTRÒNIC

El suport del DNI electrònic serà una targeta de la mateixa mesura que les actuals. L'anvers portarà un xip amb informació digital. Entre altres dades identificadores de caràcter personal, el xip inclourà un certificat electrònic, per autentificar la identitat del ciutadà; un certificat electrònic reconegut, per emetre signatures electròniques reconegudes, i claus criptogràfiques per a l'emissió i verificació de les signatures. Es preveu que es constituirà una autoritat de certificació electrònica personalitzada en el Ministeri de l'Interior, a través de la Direcció General de Policia. La implantació del DNI electrònic serà gradual els propers anys.

Explicarem tot seguit, per mitjà d'un exemple, els aspectes matemàtics que possibiliten l'existència de signatures electròniques digitals.

DIGITALITZACIÓ DE MISSATGES

Suposem que volem enviar un text a través de la xarxa, escrit amb caràcters del nostre alfabet (lletres i nombres). A fi que sigui transmissible telemàticament, cal començar reconvertint el seu contingut en una successió de zeros i uns; és a dir, hem de codificar el text en un missatge binari. La taula 1 ofereix un text *X* codificat en el sistema de numeració binari. La taula 2 ofereix el mateix text codificat en el sistema de numeració decimal. En aquesta exposició, utilitzarem la representació decimal dels nombres per fer els càlculs més fàcils de seguir i perquè les taules ens ocupin menys espai.

01101011	01101011	00001100	01010001	00101001	00011101	
00011111	00100110	00100110	00000000	01110110	00101101	
00000000	00011011	00000000	00100110	00011011	00000000	
00100001	01110101	00011100	00100011	00011011	01000100	
01101011	01101011	00010011	00100011	00100001	00101000	
00011011	00101110	01000110	00000000	00000011	00011011	
00101010	00100011	00101110	01110101	00000000	00001000	
00011011	00011110	00011110	00101001	00011101	00100101	
01101011	01101011	01101011	01101011	01101011	01101011	

Taula 1. Codificació binària d'un missatge *X*.

107	107	012	081	041	029	031	038	038
000	118	045	000	027	000	038	027	000
033	117	028	035	027	068	107	107	019
035	033	040	027	046	070	000	003	027
042	035	046	117	000	008	027	030	030
041	029	037	107	107	107	107	107	107

Taula 2. *x* = Codificació decimal de *X*.

La codificació d'un missatge alfabètic en un missatge numèric es coneix com a *digitalització*. La simple digitalització dels missatges no proporciona cap tipus de confidencialitat enfront de tercers. En principi, se suposa que tots els usuaris d'una xarxa són capaços de codificar un missatge alfabètic en un missatge digital i de descodificar un missatge digital en un missatge alfabètic. El diccionari més generalment emprat per a tal fi és l'anomenat codi ASCII (*American Standard Code for Information Interchange*), accessible per Internet. En els exemples de les taules 1 i 2 s'ha emprat un codi de 149 caràcters similar a l'ASCII, però una mica simplificat.

«LA SIGNATURA ELECTRÒNICA RECONEGUDA TÉ EL MATEIX VALOR LEGAL QUE LA SIGNATURA MANUSCRITA.»

CONNEXIONS SEGURES

Per aconseguir que la transmissió per xarxa d'un missatge digitalitzat *x* sigui confidencial es recorre a la *criptografia* o escriptura secreta. Donat un text accessible per a tothom (text clar), la criptografia s'encarrega de transformar-lo en un criptograma, o text inaccessible per als adversaris. La transformació de missatges clars en criptogrames i viceversa es porta a terme mitjançant claus criptogràfiques, que poden ser molt diverses.

Al llarg dels temps, la criptografia ha estat emprada primordialment per governs i societats secretes. Amb la introducció de les noves tecnologies, aquest art mil·lenari ha experimentat canvis significatius i el seu ús es va generalitzant. Cada cop més sovint, les nostres dades i els nostres pagaments viatgen xifrats per la xarxa.

Per xifrar els missatges electrònics hi ha diversos protocols. Mitjançant programes informàtics, aquests protocols efectuen operacions aritmètiques en un missatge digitalitzat, amb el propòsit d'amagar-ne el contingut. El missatge digitalitzat es transforma així en un missatge digital xifrat, que és el que viatja.

La taula 3 conté un missatge *y* obtingut xifrant el missatge *x* de la taula 2. Descodificant *y* obtindríem

un criptograma del missatge *X*, totalment incomprensible.

105	009	025	116	024	074	005	044	037	121	031	066	067	142
022	061	066	051	057	034	011	045	000	000				
050	091	104	135	105	106	047	146	095	113	088	046	116	025
073	010	003	056	109	055	061	048	000	000				
118	041	112	112	124	137	100	036	030	032	025	026	127	096
092	076	134	013	032	134	037	050	000	000				
041	068	050	133	037	012	066	004	146	010	116	114	029	001
126	080	125	064	024	038	003	027	000	000				
071	015	060	130	068	005	078	060	025	120	068	057	052	066
076	075	086	148	104	017	127	042	000	000				
071	008	066	021	087	105	015	010	136	113	063	126	046	079
045	075	127	093	105	022	067	047	000	000				

Taula 3. *y* = xifratge del missatge *X*.

CRIPTOGRAFIA DE CLAU PÚBLICA; CRIPTOGRAFIA DE CLAU PRIVADA

El desenvolupament de la criptografia ha conegut dues etapes ben diferenciades: abans de l'any 1975, dita l'etapa clàssica, i a partir d'aquesta data, en què s'inicià la *criptografia de clau pública* o asimètrica.

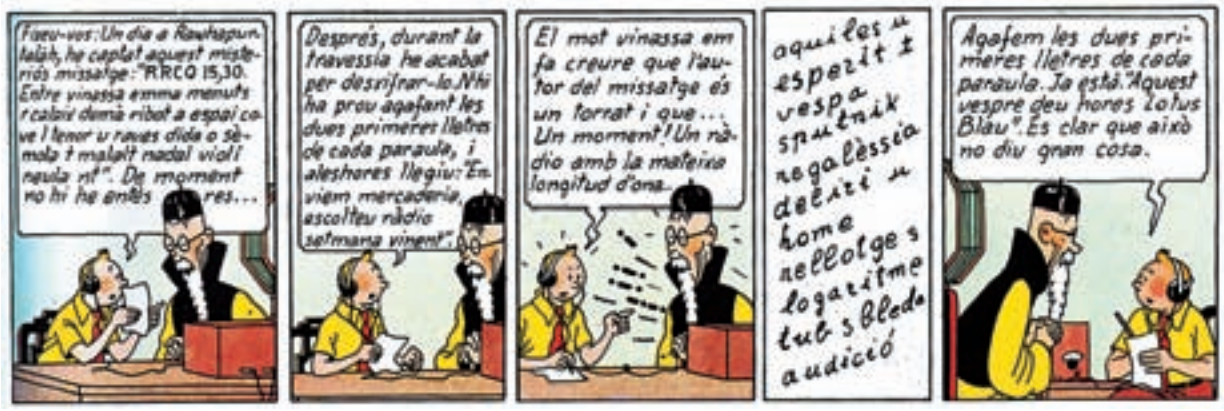
La criptografia clàssica empra uns protocols en què l'emissor i el receptor d'un missatge acorden prèviament la clau. La informació continguda en la clau serveix tant per a xifrar el missatge com per a desxifrar-lo. La transmissió de les claus sol estar en mans d'agents especials; les claus s'apleguen en llibres de codis o similars (que són sempre font de problemes).

La criptografia de clau pública neix l'any 1976 per mà de W. Diffie i M. E. Hellman. La proposta de Diffie i Hellman fou la creació d'uns protocols que permetessin deixar a la llum les claus necessàries per a xifrar els missatges i amagar les claus necessàries per a desxifrar-los. Les claus privades serien exclusives de cada usuari. De fet, Diffie i Hellman no sabien com portar a la pràctica la idea de la criptografia de clau asimètrica. Es tractava de construir una mena d'autopistes d'anada, però sense retorn, excepte per a una sola persona (la receptora del missatge).

NOMBRES PRIMERS SECRETS

L'any 1978, R. Rivest, A. Shamir i L. Adleman[1] ideaven un protocol per implementar la criptografia de clau pública. La seva proposta fou utilitzar els nombres primers com a dades secretes per a la creació de claus asimètriques. El protocol RSA (**R**ivest, **S**hamir i **A**dleman) segueix l'esquema de Diffie i Hellman: cada usuari té assignada una clau pública i una clau privada. La clau pública consta d'un parell de nombres (n, e), que estan a l'abast de tothom en un directori. El nombre n s'obté multiplicant dos nombres primers: $n=p\cdot q$. El nombre e s'escull de manera que el màxim comú divisor de e i del nombre $(p-1)(q-1)$ sigui igual a 1. Els nombres primers p, q no es revelen; són una dada exclusiva de la identitat de l'usuari. A partir d'ells es calcula el nombre secret d per la condició que $e\cdot d-1$ sigui un múltiple de $(p-1)(q-1)$. El parell (n, d) constitueix la clau privada de cada usuari. Com veurem, el coneixement de d serà imprescindible per desxifrar els missatges.[2]

La asimetria de les claus resulta del fet següent: donats dos nombres primers p, q, és molt fàcil multiplicar-los i obtenir el nombre n. En canvi, donat un



En el còmic de Tintín «El lotus blau» es parla de missatges xifrats.
Hergé, 1974, «El lotus blau» dins *Tintín a Amèrica*. Editorial Joventut, Barcelona. Traducció catalana de Joaquim Ventalló.

[1] RIVEST, R.; SHAMIR, A., ADLEMAN, L., 1978, «A method for obtaining digital signatures and public-key cryptosystems» in *Communications of the ACM*, 21 (2): 120-126.

[2] Es tracta d'un càlcul mòdul $m=(p-1)(q-1)$. En general, en els càlculs mòdul m, cada vegada que s'arriba a m es torna a començar. Per exemple, calculem les hores mòdul 12; així, les 13 h equivalen a la 1 h; i si a les 11 h n'hi sumem tres, obtenim les 2 h, etc.

nombre n «prou gran» que sigui producte de dos primers p, q de la mateixa mida, es tarda «molt temps» per calcular p, q. Per exemple, descompondre un nombre de 1024 bits (unes 300 xifres decimals) requereix unes 2^{100} operacions bàsiques en el millor dels algoritmes que avui coneixem. Sense conèixer p, q no se sap calcular d. Per tant, el coneixement d'una clau pública RSA, (n, e), ben construïda i amb n prou gran, no permet avui el càlcul de la clau privada (n, d) associada.

La taula 4 és un directori de claus públiques RSA amb dos usuaris: el reporter Tintín i el capità Haddock.[3] El parell (n_t, e_t) és la clau pública de Tintín; el parell (n_h, e_h) és la clau pública de Haddock. D'acord amb el seu esperit, no mostrem les claus privades ni de Tintín: (n_t, d_t), ni del capità Haddock: (n_h, d_h).

Tintín

$n_t = 25550796051464997470779643997475848687481075517 3$

$e_t = 52318457$

Haddock

$n_h = 2894437459173461746770921838169208262186574927 4689$

$e_h = 15826584155627$

Taula 4. Un directori de claus públiques RSA.

EL PROTOCOL RSA PER XIFRAR MISSATGES DIGITALS

Estem ara en condicions d'explicar el funcionament del protocol RSA; començarem per dir com se xifra un missatge x coneguda la clau pública (n, e) del receptor: es multiplica el missatge x per ell mateix e vegades, realitzant sempre els càlculs mòdul n; el resultat és el missatge xifrat: $y = x^e \bmod n$. El missatge de la taula 3 s'ha generat a partir del missatge de la taula 2 amb la clau pública de Tintín, de la taula 4. Per calcular-lo, s'ha dividit el missatge de la taula 2 en 6 blocs de 9 xifres en base 149, i s'ha interpretat cada bloc com un nombre més petit que n_t. Cada bloc s'ha multiplicat per ell mateix e_t vegades, reduint sempre els càlculs mòdul n_t. Han sorgit així els 6 blocs de 24 xifres en base 149 de la taula 3.

Quan el receptor rep un missatge xifrat $y = x^e \bmod n$, desconeix el valor de x. Per recuperar-lo ha de calcular l'arrel e del missatge y rebut. Atès que els càlculs es fan mòdul n, aquesta arrel és difícil de calcular, llevat que es coneguin els primers p i q. La recuperació del missatge x, un cop conegut el nombre d, que és el secret de n, es basa en la identitat $\sqrt[e]{y} = x = x^{e \cdot d} \bmod n$, descoberta pel matemàtic Leonhard Euler en el segle XVIII. L'any 1977, el MIT sol·licità la patent del protocol RSA, un fet insòlit en matemàtiques, car era el primer algoritme patentat en la història d'aquesta ciència.

Missatge digitalitzat: x
Clau pública: (n, e)
Missatge xifrat: $y = x^e \bmod n$
Secret: p, q, nombres primers tals que $n = p \cdot q$
Clau privada: (n, d), on $d \cdot e = 1 \bmod (p-1)(q-1)$
Missatge desxifrat: $y^d = x \bmod n$

Taula 5. El protocol RSA.

EL PROTOCOL RSA DE SIGNATURA DIGITAL

L'autenticitat de les signatures autògrafes s'estableix per mitjà d'una anàlisi grafològica. Explicaremara com la criptografia de clau pública fa possible l'emissió i l'autentificació de signatures digitals. La signatura digital és emesa pel signatari amb l'ús de la seva clau privada. L'autenticitat d'una signatura digital pot ser verificada per qualsevol persona amb l'ús de la clau pública del signatari.[4] La taula 6 explicita l'esquema de signatura RSA per signar un missatge digital i verificar-ne la signatura.

Missatge digital: x
Clau (pública i privada) del signatari : (n, e, d)
Missatge signat: $(x, x^d \bmod n)$
Verificació de la signatura: $(x^e \bmod n, x^{d \cdot e} = x \bmod n)$

Taula 6. El protocol de signatura RSA

La taula 7 mostra el missatge x de la taula 2 signat amb la clau privada del capità Haddock.

107 107 012 081 041 029 031 038 038 000 118 045 000 027 000
038 027 000 033 117 028 035 027 068 107 107 019 035 033 040
027 046 070 000 003 027 042 035 046 117 000 008 027 030 030
041 029 037 107 107 107 107 107 107
101 148 099 103 055 097 140 032 085 055 069 007 105 079 122
143 060 119 125 100 132 099 016 000 120 098 021 006 125 057
067 025 092 120 036 030 054 007 145 125 104 073 042 082 007
112 040 000 061 032 028 049 134 138 011 144 135 114 009 107
083 021 054 079 122 021 114 144 061 039 031 000 136 087 007
006 034 128 047 006 026 119 033 099 026 143 122 077 029 115
047 079 060 008 000 000 006 097 004 040 086 100 087 141 113
125 128 074 038 114 056 028 131 049 000 016 040 044 002 000
019 083 035 039 014 135 052 007 015 069 111 028 111 036 031
041 145 105 125 133 067 111 022 000

Taula 7. Haddock signa el missatge codificat: $(x, x^{dh} \bmod n_h)$

[3] HERGÉ (Georges Rémy): *Les aventures de Tintín*. Editorial Joventut. Traducció catalana de Joaquim Ventalló. Primera aparició de Tintín: 10 de gener de 1929.
[4] Prescindim en aquesta exposició de l'ús de funcions resum (*hash*).

TRAMESA D'INFORMACIÓ SIGNADA I XIFRADA: SIGNATURES RECONEGUDES

Podem ara combinar el protocol RSA de signatures digitals amb el protocol RSA de xifratge de missatges digitals. Estarem, així, en la situació de l'emissió i verificació del que la llei anomena una signatura electrònica reconeguda. Les taules que segueixen n'ofereixen un exemple.

105 009 025 116 024 074 005 044 037 121 031 066 067 142 022
061 066 051 057 034 011 045 000 000
050 091 104 135 105 106 047 146 095 113 088 046 116 025 073
010 003 056 109 055 061 048 000 000
118 041 112 112 124 137 100 036 030 032 025 026 127 096 092
076 134 013 032 134 037 050 000 000
041 068 050 133 037 012 066 004 146 010 116 114 029 001 126
080 125 064 024 038 003 027 000 000
071 015 060 130 068 005 078 060 025 120 068 057 052 066 076
075 086 148 104 017 127 042 000 000
071 008 066 021 087 105 015 010 136 113 063 126 046 079 045
075 127 093 105 022 067 047 000 000
143 032 057 051 014 090 042 034 050 060 106 004 043 036 135
088 085 024 101 122 091 002 000 000
105 119 011 062 111 037 102 038 103 088 127 045 007 097 082
117 115 037 049 058 094 046 000 000
095 100 138 082 015 062 109 011 021 031 111 118 078 128 003
053 109 028 050 052 130 050 000 000
129 116 023 065 138 067 143 089 108 100 143 128 064 071 106
124 114 100 142 100 119 017 000 000
137 146 109 093 001 070 104 085 013 104 107 142 025 107 000
071 009 119 116 005 111 043 000 000
058 063 081 077 024 138 117 044 024 045 115 131 008 013 060
045 021 114 144 074 032 037 000 000
112 008 098 075 124 133 120 126 029 062 044 116 095 018 001
108 107 120 093 118 106 021 000 000
130 024 057 144 098 085 014 126 123 068 078 147 015 031 113
096 088 012 135 007 098 011 000 000
074 044 094 011 077 094 127 049 147 018 060 091 112 136 037
026 063 130 089 118 096 058 000 000
127 036 021 049 084 124 063 043 035 044 094 059 134 081 110
146 101 128 054 126 128 040 000 000
113 045 047 079 119 036 114 128 141 131 145 105 122 070 016
007 079 078 127 113 142 004 000 000
088 041 075 127 017 105 005 058 091 067 070 077 116 031 138
117 053 109 106 028 001 056 000 000
035 003 051 045 103 062 035 030 048 145 011 120 003 013 047
004 032 062 125 086 099 020 000 000
011 111 022 098 094 073 056 033 145 134 084 083 145 142 039
117 143 108 090 013 070 024 000 000
061 086 053 050 118 025 059 076 032 131 017 101 064 079 055
147 069 003 026 128 028 018 000 000
144 142 041 088 122 131 125 113 110 096 126 097 139 120 040
121 033 051 085 000 078 001 000 000

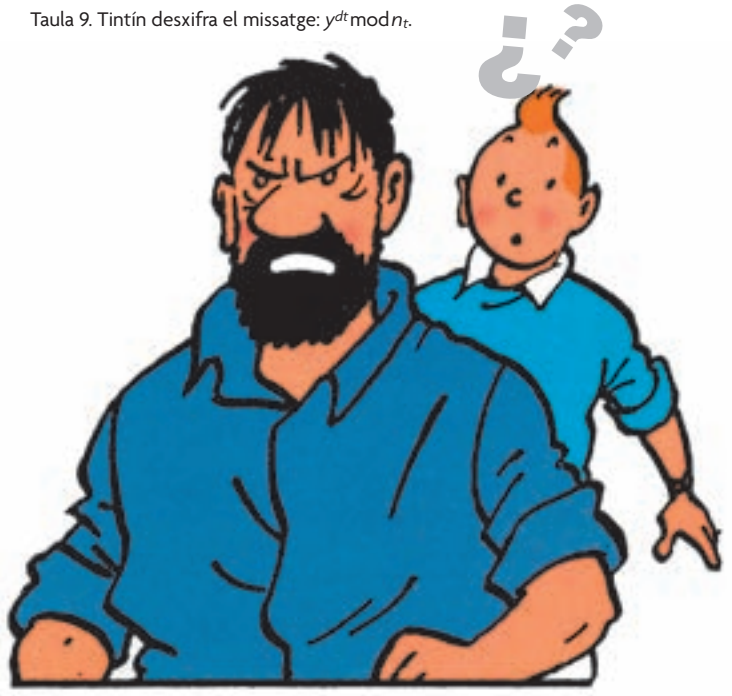
Taula 8. Tintín rep un missatge codificat: $y = (x^{et} \bmod n_t, x^{dh\ et} \bmod n_t)$.

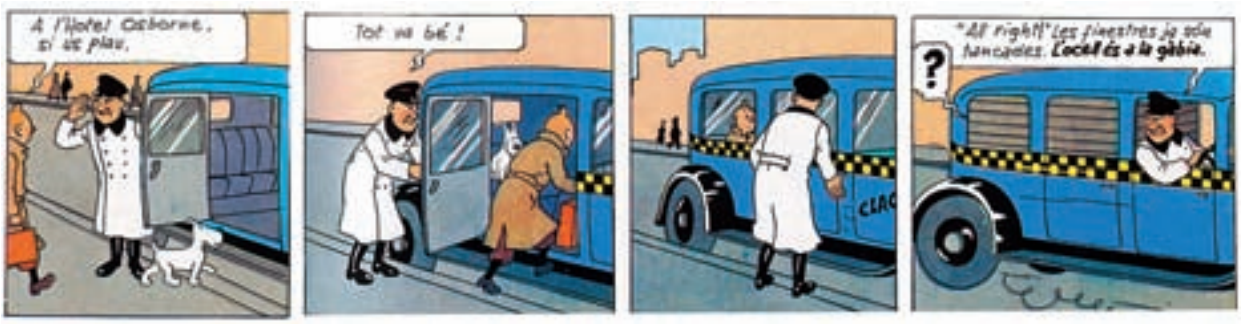
@IYÖX¨ErkØe9,"V49y0hKs x/_,@#uŒ]ë+tÖY!JC¥·€4v
éoãã¶¢>jdfYZâ{lï Mf kx o.x—kL9DŒJÖµcA?~Ò7XlCa
;O3?.E^3YÓ.0z9ï?(–_Qâp ;H9U)@OJ¡ë6?tùs?â\\@V,u
∞f0yN*phx3#Dqj,+ÄX%™/B @?K5?k$l&+âsG}®à?kw1[t
]>£®O5·KUe?é^êC€·bxz?x …ÖW8£,??\108>?ê7;#¶µ>"">?Q
¢Œ·\\A:_ÄM_
"Y
;I?ÖE?q 16''X£àrXs??HM3sUµƒ¨fk ãH=?¶—Ó?c5rÖ]RA\108
Ó\\é#U ?X0ƒ=ÄN??.^"Oeë{+L,G=K ¨r[K`[âw"R3/ã¡kZ6??é{1
âjUw-¶6qir[2 'ÔŒ%ê‡?ên ësuù?jµê‹?^@™:PGù^âë"D
+o?âQ@E1/,;`Öe£à€·#bA¥ iCys&5idv^KÓCMuDf5Ò(<T
K?V=[!¥g^ -¯^"mà?\108*M:X 4(€xéY2if?Q%7ù€"úCZêbR
ƒ"o+™?ÒëÔ{?}„ÓnØgyÄ ^A

Taula 9. Tintín descodifica el missatge y i obté un criptograma: Y.

107 107 107 012 081 041 029 031 038 038 000 118 045 000 027
000 038 027 000 033 117 028 035 027
068 107 107 019 035 033 040 027 046 070 000 003 027 042 035
046 117 000 008 027 030 030 041 029
037 107 107 107 107 107 107 107 107 107 107 107 107 107 107
107 107 107 107 107 107 107 107 107
101 148 099 103 055 097 140 032 085 055 069 007 105 079 122
143 060 119 125 100 132 099 016 000
120 098 021 006 125 057 067 025 092 120 036 030 054 007 145
125 104 073 042 082 007 112 040 000
061 032 028 049 134 138 011 144 135 114 009 107 083 021 054
079 122 021 114 144 061 039 031 000
136 087 007 006 034 128 047 006 026 119 033 099 026 143 122
077 029 115 047 079 060 008 000 000
006 097 004 040 086 100 087 141 113 125 128 074 038 114 056
028 131 049 000 016 040 044 002 000
019 083 035 039 014 135 052 007 015 069 111 028 111 036 031
041 145 105 125 133 067 111 022 000

Taula 9. Tintín desxifra el missatge: $y^{dt} \bmod n_t$.





"L'ocell és a la gàbia" és un dels missatges xifrats que Hergé fa servir per als còmics de Tintín. Si les seues aventures estigueren ambientades en l'actualitat, de ben segur que Tintín es faria servir de la signatura digital per protegir els seus missatges.

HERGÉ, 1968, *Tintín a Amèrica*. Editorial Joventut, Barcelona. Traducció catalana de Joaquim Ventalló.

L'ocell és a la gàbia.
Signat: Capità Haddock

%–<&€}‰fÄ€úG@ù™?3?Ò>•<P
Ó=UFÒ0,YlÓjd‡GˆÒ_!p®Gãn 4fbw £Kf,μI
¯U‡ù™Uμf4me ¡)GFhêuFZ?g<Z?™`c?uù3H
F}Dn(>)‹ëÒê¨lμ¥b?w PnrB S¯imN,zGOú?b?jeoˆ@Ò—,?V

Taula 10. Tintín descodifica el missatge desxifrat i obté un missatge signat: $Y^{dt} = (X, S)$.

El gargot que apareix sota el text clar de la taula 10 és la signatura electrònica del missatge. Cal, doncs, verificar-la. Com que això ho pot fer tothom, deixarem que ho faci el professor Tornassol:

089 041 056 040 002 081 033 108 091 107 007 120 145 036 026
026 014 052 125 137 013 067 016 142 007 099 037 107 107 012
081 041 029 031 038 038 000 118 045 000 027 000 038 027 000
033 117 028 035 027 068 107 107 019 035 033 040 027 046 070
000 003 027 042 035 046 117 000 008 027 030 030 041 029 037
107 107 107 107 107 107

Taula 11. Tornassol verifica la signatura: $y^{dt\,eh} = (x^{eh} \bmod n_h\,,\, x^{dh\,eh} \bmod n_h)$.

Cal descodificar el text obtingut. Si tot és correcte, el text clar apareixerà en segon terme.

∂o¥nB'g\108/
GÓˆjZZNzÒ¢M,P"G<k

L'ocell és a la gàbia.
Signat: Capità Haddock

Taula 12. Tornassol autentifica la signatura electrònica de Haddock!: (X^{eh}, X).

QÜESTIONS DE SEGURETAT

La seguretat del protocol RSA es basa en un desconeixement. En l'actualitat, els algoritmes per descompondre els nombres en factors primers no són prou ràpids quan s'executen en els nostres ordinadors. Així, les claus RSA esdevenen segures quan el nombre n té unes 300 xifres decimals (1024 bits). L'ús d'ordinadors molt més potents, o una millora significativa dels algoritmes de factorització, repercutiria en la inseguretat d'aquestes claus.

En el nostre exemple, els nombres n del directori tenen de l'ordre de 50 xifres decimals. Amb la potència de càlcul actual, les claus del directori són insegures (les del nostre DNI seran molt més grans). Tornassol s'assessora[5] i, com a resultat, obté la clau privada de Haddock mitjançant un conegut algoritme de factorització (MPQS). Aquest trenca el nombre n_h i deixa al descobert el secret del capità: el nombre d_h.

$n_h = 289443745917346174677092183816920826218657492746 89$
$d_h = 167176801271034114925914871025317101882075741163 07$

Taula 13. L'algoritme MPQS ha trencat la clau del capità Haddock.

Amb altres paraules, el missatge del capità Haddock podria, molt bé, ser apòcrif. Caldrà, doncs, investigar els coneixements aritmètics i la capacitat de càlcul dels adversaris: Rastapopulos, Peggy, el Sindicat de Gàngsters de Chicago, etc.

Amb posterioritat al RSA, s'han dissenyat altres protocols criptogràfics que ofereixen la mateixa seguretat que el RSA amb claus molt més petites. Aquests protocols utilitzen propietats sofisticades dels nombres, estudiades en el decurs dels segles XIX i XX.

CONCLUSIÓ

Els mètodes actuals de signatures digitals es basen en l'existència de problemes aritmètics, la resolució dels quals comporta massa temps i espai amb els mitjans actuals. Millores en el coneixement teòric dels nombres, o en la potència de càlcul dels ordinadors, poden fer variar el seu grau de seguretat. Les possibles repercussions criptogràfiques dels avenços aritmètics han d'ésser estudiades amb cura i tingudes en compte, en tant que sistemes criptogràfics avui segurs poden deixar de ser-ho en un futur no gaire llunyà.

[5] TRAVESA, A., 1998, *Aritmètica*. Col·lecció UB. Edicions Univesitat de Barcelona.

Pilar Bayer. Dep. d'Àlgebra i Geometria, Facultat de Matemàtiques, Universitat de Barcelona.