Testimonio de medio siglo: de la Perlustración al Cifrado cuántico

Fausto Montoya
Instituto de Seguridad de la Información
Consejo Superior de Investigaciones Científicas,
Email: fausto@iec.csic.es

***Abstract*—En este artículo se presenta una visión personal de la criptografía en España en los últimos 50 años, introducida con una sucinta historia mundial y española. Se informa de fuentes de artículos, congresos y programas útiles, y se sugieren líneas de actuación para futuros criptólogos.**

I. Introducción

La criptografía y la seguridad de la información, son materias muy diferentes al resto de las tecnologías y doctrinas científicas. Eso hace que los criptólogos sean una raza aparte entre los científicos.

Cualquier ciencia consiste en la acumulación de conocimientos hacia un fin; todos los investigadores colaboran para perfeccionar los modelos matemáticos de los hechos observados. Cuando se encuentra algún error se propone su corrección y se continúa avanzando. Los modelos consolidados raramente se cuestionan y ello solo se actúa para perfeccionarlos o ampliar su campo de acción. Así las leyes de Newton siguen siendo válidas y solo se cambian por la Ley de la relatividad para hacer cálculos a grandes velocidades.

En cambio la criptografía es otra cosa, hay muy pocos principios que se puedan considerar inamovibles:

- El principio de Kerckhoffs ([1], [2]): La efectividad del sistema no debe depender de que su diseño permanezca en secreto, es decir solo la clave es desconocida.
- El sistema de cifrado de Vernam es el único seguro matemáticamente.
- Las aportaciones básicas de Claude Shannon sobre la Cantidad de información, la entropía, la longitud mínima de clave y la distancia de unicidad; publicadas en 1949 en su artículo *Communication Theory of Secrecy Systems*, que era una versión desclasificada de su trabajo durante la segunda guerra mundial ([3], [4]).

Por su propia naturaleza, la criptografía es un enfrentamiento entre dos fuerzas, cada una de las cuales busca derrotar a la otra. La investigación en criptografía es algo así como el ajedrez, unos buscan ataques y otros encuentran defensas. Alguien propone una cifra y cientos se aplican a su rotura.

Salvo el sistema de Vernam, todos los criptosistemas tienen una seguridad limitada, que hemos convenido en denominar *seguridad práctica*, es decir, que solo son seguros frente a ataques con las máquinas de cálculo actuales o las de un cercano futuro.

La cruda realidad, es que con los años y el esfuerzo, todos los sistemas de cifrado se van rompiendo, o al menos van perdiendo robusted. La tecnología informática avanza a una velocidad extrema y lo que hace unos pocos años nos parecían misiones imposibles, hoy son tareas rutinarias.

El superordenador más rápido en 1993, el CM-5/1024 de Thinking Machines Co. realizaba 6 x 10^{10} operaciones de coma flotante por segundo. Hoy, 19 años después, el Sequoia de IBM, realiza 1,62 x 10^{16} operaciones por segundo, es decir es 270.000 veces más rápido. La próxima amenaza es el ordenador cuántico, que cuando aparezca, seguramente obligará a reformar la mayoría de los algoritmos criptográficos.

Esto que parece un panorama amenazador, no lo es en realidad para aquellos que se dediquen a la criptología. Es una buena nueva, que garantiza que siempre habrá trabajo. Siempre será necesario diseñar nuevos criptosistemas. Y siempre habrá nuevos criptosistemas recién diseñados listos para ser descriptados.

La verdad es que este autor tiene muchos más trabajos de criptoanálisis que de diseño, porque siempre resulta fácil encontrar ingenuas propuestas de criptosistemas —publicadas en revistas indexadas de primer orden— cuyo diseño no consideró todas las posibles vías de análisis y ataque, que un cripto-analista ha podido llegar a desarrollar y dominar a lo largo de los años.

En resumen, se puede concluir que la Criptología, además de ser una ciencia, es un arte.

II. Hitos de la criptología

Se puede admitir que la criptografía es tan antigua como el lenguaje escrito, surgió en múltiples lugares: Egipto, India, Mesopotamia, Persia, Esparta, Siam, Suecia..., en algunos casos como simple cifra y en otros combinada con la esteganografía.

Los primeros en usar un verdadero sistema matemático de cifra fueron los romanos con la cifra de César y la de Augusto. Pero no se avanzó nada en este campo hasta la aparición de al–Kindi

El califato Abásida, de 750 al 1258, fue la época más esplendorosa científicamente en el Islam, se relajó el ansia de conquista y se primó el desarrollo, florecieron todas las ciencias. Destacó un filósofo y matemático, Abu Yusuf Yaqub ibn-Ishaq al-Kindi (801–873); entre sus muchos trabajos tenemos que destacar un *Manual descifrado de mensajes cifra-*

dos en donde analiza la frecuencia de aparición de las letras y lo aplica en la rotura de cifrados de sustitución.

Más tarde, Ali ibn-Adlan (1187–1268) publicó otro libro de criptoanálisis, también basado en la frecuencia letras, explica que un criptoanálisis con éxito requiere que el texto claro tuviese, al menos, 90 letras, con al menos, 3 repeticiones de cada letra.

Ali ibn-Muhammad ibn-al-Durayhim (1312–1361) citado por Ali ben Ahmad Abd Allah al-Qalqashandi (1355–1418), analiza detalladamente 8 cifrados de sustitución, recoge los conocimientos de al Kindi y de ibn-Adlan. Fue precursor del sistema conocido como tabla de Vigenere.

En los sombríos tiempos de la alta edad media europea, la criptografía romana se mantuvo entre los monjes cristianos, algunas veces simplificada reduciéndola sencillamente a la eliminación de las vocales. Pero al llegar la baja edad media y luego el Renacimiento, empezó a florecer la criptografía en Europa, fundamentalmente en Italia, inicialmente con las luchas entre Güelfos y Gibelinos y seguidamente con la lucha entre papas en el Cisma de Occidente.

El primer cifrado por sustitución polialfabético conocido es obra de Leon Battista Alberti —*abreviador apostólico* de 3 papas, arquitecto, lingüista, músico y arqueólogo— publicado en su tratado *De Cifris* en 1466. Le siguieron Johannes Trithemius, que en su tratado *Poligraphia* describe la *tabula recta* y Giovan Battista Belasso que en 1553 publicó *La cifra del Sig. Giovan Battista* —conocida erróneamente como el cifrado de Vigenère—.

Giambattista della Porta 1563, con su tratado en cuatro tomos sobre criptografía *De Furtivis Literarum Notis: vulgo de ziferis*, es el primer criptólogo formal. Analiza y clasifica los procedimientos de cifrado, e inicia las leyes del criptoanálisis, apoyándose en las características lingüísticas que facilitan el descifrado.

En el siglo XVI todos los reinos cristianos empleaban la criptografía y el criptoanálisis, su uso era generalizado. Fue el momento de los *nomenclator*, una mezcla cifra de sustitución y código. Famosa es la rotura de la *clave general* de Felipe II por el criptoanalista papal Triphon Bencio; por el matemático Fraçois Viète trabajando para el rey francés Enrique IV; por el flamenco Philips Van Marnix secretario de Gillermo de Orange; y también por el inglés Thomas Phelippes, que servía a Isabel I de Inglaterra, a través de su secretario Francis Walsingham (1530–1590).

Fue a este último equipo al que cupo el mérito de realizar la primera *invención de mensaje* documentada. Una vez que Thomas Phelippes hubo roto la cifra de María Estuardo, reina de Escocia —que estaba presa de su prima Isabel I en Londres— inventaron un mensaje cifrado atribuido a María, que sirvió para demostrar al parlamento inglés que ésta conspiraba desde su prisión para derrocar a Isabel, lo que le valió ser decapitada. Hay que reconocer que su complot era cierto, pero la prueba fue falsa.

En los siglos siguientes se fueron creando todos los sistemas clásicos de cifrado manual, hasta hoy conocidos. La aparición de sistemas mecánicos de computación se inicia con Charles Babbage (1791–1871), que creó la *analytical engine*. Babbage rompió la cifra auto-clave de Vigenère, que hasta entonces se creía indescifrable; aunque el mérito se lo llevó Friedrich Wilhelm Kasiski (1805–1881) oficial de infantería prusiana, quien también descifró este sistema criptográfico y describió la forma de realizarlo, algunos años después, en *Die Geheimschriften und die Dechiffrierkunst* (1863).

Otro truco criptográfico inglés fue el causante de la entrada de Estados Unidos en la primera guerra mundial. Esta vez el mensaje cifrado era cierto, se trataba de un telegrama del ministro de asuntos exteriores alemán, Arthur Zimmermann, del 16 de enero de 1917, al embajador alemán en México, Heinrich von Eckardt; en él se ordenaba al embajador que propusiera al gobierno mejicano formar una alianza militar contra los Estados Unidos, para recuperar Tejas, Nuevo Méjico y Arizona.

El telegrama fue enviado cifrado desde la embajada estadounidense de Berlín hasta la embajada alemana en Washington por una línea del Departamento de Estado de EEUU —que el presidente Wilson, había puesto gentilmente a disposición de los alemanes para transmitir mensajes entre Washington y Berlín que ayudaran a la causa de la paz estadounidense— y desde allí a Ciudad de Méjico. Los británicos espiaban sistemáticamente esta línea diplomática estadounidense, interceptando todos los mensajes, así copiaron y descifraron el telegrama de Zimmermann. El problema es que no se lo podían entregar al gobierno de EEUU, pues eso revelaría que estaban espiando sus comunicaciones diplomáticas, los británicos simularon simplemente que el telegrama se había obtenido en Ciudad de Méjico y lo entregaron al gobierno de EEUU, que declaró la guerra al Imperio Alemán.

1919 y 1920 fueron años memorables en la criptografía: Gilbert Vernam y Joseph Mauborgne (oficial del Signal Corps de EEUU) patentaron para la AT&T Bell Labs, el único sistema de cifrado seguro matemáticamente demostrable: la cifra aditiva del mensaje con una secuencia aleatoria, de un solo uso, conocida como cifra de Vernam. Una particularidad de este cifrado es que se podía llevar a cabo automáticamente mediante un teletipo modificado, que leía una cinta con el mensaje en claro y la combinaba con otra cinta aleatoria que leía en paralelo. La combinación era la suma módulo dos bit a bit.

Desde la primera guerra mundial hasta pasada la segunda, prácticamente todos los sistemas criptográficos que se desarrollaron consistieron en máquinas cifradoras: una de las primeras fue diseñada y patentada en 1923 por Arthur Scherbius, fundando la Compañía Alemana de Máquinas Cifradoras, que empezó a venderla a particulares; para luego hacerlo para el gobierno alemán ya perfeccionada y convertida en la *Enigma*.

La demostración de que el principio de Kerckhoffs es ineludible lo aporta la Enigma, cuyo diseño fue vendido a Francia por un traidor por dinero llamado Hans Thilo-Schmidt. El diseño llegó a manos del criptoanalista polaco Marian Rejewski, que estuvo rompiendo las claves y descifrando los mensajes del ejército alemán hasta el principio de la segunda

guerra mundial; para ello diseño una máquina que denominó *bomba kryptologiczna*.

En 1937, los japoneses habían puesto a punto una máquina similar, a la que los estadounidenses llamaron *Púrpura* y que fue utilizada por la Marina y el Ministerio de Asuntos Exteriores japoneses. En 1941, los expertos estadounidenses ya habían descubierto la clave diplomática japonesa Púrpura. Las réplicas inglesas y estadounidenses de Enigma, llamadas respectivamente Typex y Sigaba, nunca fueron descifradas por sus enemigos.

La Enigma original tenía 3 únicos rotores, que se podían cambiar de posición de acuerdo a la clave; pero al comenzar la segunda guerra mundial, los alemanes la complicaron añadiendo 2 nuevos rotores de recambio, de forma que se podían elegir 3 entre 5, aumentando así considerablemente el número de claves y haciendo inviable el ataque con la bomba kryptologiczna. Mas adelante, fabricaron la Enigma naval, en la que se usaban 4 rotores elegidos entre un total de ocho, con lo que las claves aumentaban tremendamente.

Alan Turing (1912–1954) fue un matemático inglés, famoso por formalizar la solución al Entscheidungsproblem planteado por Kurt Gödel en 1936. Para ello se basó en la llamada máquina de Turing, que era la creación teórica de la que se considera la base de los actuales ordenadores. Al llegar la segunda guerra mundial fue nombrado director de la sección *Naval Enigma* del centro británico de criptoanálisis Bletchley Park. Su trabajo consistió en descriptar los mensajes alemanes, cifrados con la Enigma naval, que guiaban a los submarinos alemanes para hundir los convoyes navales transatlánticos aliados. Para ello construyó una serie de equipos electromecánicos, a los que llamó *bombes*, que eran máquinas de calcular con programa fijo. Se admite que sin su ayuda la guerra podía haber durado de dos a cuatro años más, y su final podría haber sido diferente.

El pasado 23 de junio de 2012 se ha celebrado mundialmente el aniversario del nacimiento de Alan Turing (http://www.turingcentenary.eu/). La incomprensión a cerca de sus tendencias sexuales, por parte de la sociedad y legislación británica de la época, le condujeron al suicidio por ingestión de una manzana envenenada con cianuro, el 7 de junio de 1954. Se especula con que lo hizo emulando a Blancanieves, envenenada con una manzana por la reina hechicera. Una leyenda urbana atribuye el logotipo de la manzana arcoiris mordida, de Apple Computer Inc., a un homenaje *cifrado*, de Turing mordiendo su última manzana.

En 1968 se estrena la película de Stanley Kubrick y Arthur Clarke *2001: A Space Odyssey*, donde el ordenador HAL 9000 canta la misma canción (Daisy Bell) que un ordenador real, el IBM 7094, cantó por primera vez en 1961. Si se cifra HAL con la cifra de Augusto, se obtiene IBM.

Hasta 1970 la criptografía fue una utilidad únicamente necesaria para diplomáticos, militares, papas y delincuentes. Pero a partir de entonces es imprescindible para el uso del público general. Hoy día se incluye en el DNI, pasaporte, actas notariales, firma estatal electrónica, medios de pago electrónicos, telefonía móvil, banca, correo electrónico, Internet y a no tardar en la "computación en la nube" y en las etiquetas RFID del comercio.

Esto ha dado lugar a la generalización explosiva de la criptografía. En 1974 aparece el cifrado en bloque con el *Data Encription Standard* (DES), seguido por el cifrado asimétrico en 1976, la distribución cuántica de claves en 1984 y el cifrado caótico en 1993. En 2002 el DES es sustituido por el *Advanced Encryption Standard* (AES).

Los interesados en la historia de la criptografía pueden consultar las obras de Juan Carlos Galende [5], de David Kahn [6] y Simon Singh [7].

III. La criptografía en España hasta la segunda guerra mundial

Los escritos españoles cifrados más antiguos que se conservan corresponden a los Reyes Católicos, que utilizaban un nomenclator. Carlos I (1516 -1556) continuó con la tecnología de sus abuelos, que fue netamente mejorada en el reinado de Felipe II, aunque como se ha dicho anteriormente no era suficientemente segura.

Curiosamente, en esa época también los futuros santos se servían de la criptografía para eludir a la Inquisición. Se conservan los escritos de Teresa de Ávila (1515–1582), dirigidos a Juan de Yepes (conocido como San Juan de la Cruz) y a Francisco de Borja, III General de la Compañía de Jesús ([8], [9],). Estos escritos eran una combinación de escritura en claro y términos en código, el código estaba elegido de tal manera que un lector poco enterado no apreciaba que el texto estaba cifrado.

En siglos posteriores hay pocos testimonios de la criptografía española. Hoy es fácil encontrar la edición facsímil de un libro de Francisco de Paula ([10]) que describe el uso de cifrados de sustitución y tintas simpáticas. A partir de entonces, vale la pena destacar el libro del militar Cesareo Huecas Carmona, que con el alias de Joaquín García Carmona, escribió en el año 1894; se recomienda adquirir su reedición en facsímil, publicada por el Ministerio de Defensa en 2011 ([11]).

Durante el primer tercio del siglo XX se siguieron usando sistemas de cifrado manual y continuaron usándose durante la guerra civil por ambos bandos, aunque el bando nacionalista utilizó para las comunicaciones de alto nivel máquinas enigma comerciales, así como algunas máquinas Kryha.

Es del mayor interés el libro de Pedro Serrano Garcia *Policiología, Criptografía y Perlustración* ([12]), que es un compendio de los cifrados manuales conocidos en España después de la guerra civil. Hay que destacar que no se trata de un libro militar, sino de un libro destinado a la policía y guardia civil, que en aquella época eran las encargadas de la represión de los restos del ejército republicano que aún resistían en el monte y la ciudad, comunicándose y recibiendo cierto apoyo de los aliados.

Una relación muy completa de libros de criptografía en español se puede encontrar en http://www.criptohistoria.es/libros_de_criptografia.html

IV. Criptografía moderna en España

Terminada la segunda guerra mundial, se sustituyeron las máquinas Enigma por otras máquinas más modernas, fundamentalmente la Hagelin CX-52 y similares. Por los años 60 se empezó a usar sistemas de criptofonía, de seguridad muy reducida, pues eran analógicos, estaban basados en la inversión de banda y en la división en bandas parciales.

Las comunicaciones estatales de alto nivel de seguridad utilizaban el sistema de Vernam para teleimpresor, fabricándose las cintas aleatorias en el Alto Estado Mayor de Madrid. Los rollos de cinta se distribuían con un ingenioso método de comprobación de la privacidad e integridad, que consistía en imprimir varios sellos de tinta en los laterales del rollo de cinta perforada; si la cinta se desenrollaba y se volvía a enrollar era imposible reconstruir la forma de los sellos, si los sellos llegaban perfectamente dibujados la cinta estaba intacta. El único problema es que no aseguraba la autenticidad, si alguien disponía de una buena copia del sello podía falsificar los rollos.

En las décadas de los 70 y 80 se empezaron a fabricar por compañías españolas equipos de cifrado totalmente digitales para los tres ejércitos y la policía, algunos diseñados por sus propios ingenieros y otros diseñados por centros del CSIC y Universidades. Estos sistemas eran tanto para datos como para voz.

Fueron unos años muy interesantes para los diseñadores, pues había clientes y se podía hacer investigación genuinamente española. La tecnología electrónica permitía hacer diseños hardware rápidos y eficaces; se fue pasado de hacer diseños que utilizaban centenares de circuitos integrados, a diseños más condensados utilizando microprocesadores, e incluso fabricando circuitos ASIC.

El estado del arte en transmisión de voz era una limitación importante para la criptofonía, pues los modems para circuitos telefónicos o de radioteléfono, trabajaban a muy poca velocidad en los años 70 (2.400, a 4.800 baudios), de manera que si se deseaba hacer un criptófono, había que elegir entre transmisión analógica y digitalización de la voz mediante un vocoder, que proporcionaba un sonido limpio pero maquinal, poco aceptado por los usuarios.

Al principio se hicieron crptófonos analógicos, combinando la permutación en frecuencia de 5 subbandas, con la permutación temporal de 64 fragmentos de cada segundo. Todas estas operaciones se hacían digitalmente, con una voz digitalizada a alta velocidad, ya fuera en modulación delta o PCM diferencial; una vez terminado el proceso se volvía a convertir la voz en analógico, para transmitir normalmente. La seguridad era baja pero la transmisión era fácil, incluso con radios de banda lateral única (BLU).

Cuando los módems comerciales alcanzaron la velocidad de 9.600 baudios, se pasó a digitalizar la voz con modulación delta comprimida, para después cifrarla en flujo con una secuencia pseudoaleatoria y, finalmente, transmitirla digitalmente con la ayuda del modem. Al aumentar la velocidad de los modems se fue mejorando la frecuencia de digitalización y por tanto la calidad de la voz, aumentando relación señal/ruido y el ancho de banda.

Hasta los 80, el mercado criptológico había sido muy reducido y también el club de los diseñadores; pues solo había un cliente prácticamente, que era el Estado.

Pero en los 80 con la aparición de los sistemas de clave asimétrica y el DES, la criptología pasó al mercado público. Primero se incorporó al cifrado de datos de las tarjetas de crédito y débito, para que fuera posible pagar desde cualquier tienda o sacar dinero desde cualquier cajero automático. En segundo lugar los ordenadores se hicieron omnipresentes en todos los ambientes y era necesario hacer protocolos de permiso de acceso a los archivos, así como proteger los documentos guardados. Al final de la década apareció la Internet y con ella el correo electrónico, concretamente fue en 1988 cuando se creó el programa IRIS (convertido en RedIRIS en 1990), sobre la red IBERPAC.

Al llegar los años 90 la criptología ya era mayor de edad en España, la prueba de ello fue la Primera Reunión Española sobre Criptología —que mas tarde se convirtió en RECSI— que tuvo lugar en Octubre de 1991 en Palma de Mallorca, organizada por la Universidad de las Islas Baleares y el CSIC. Hubo 22 ponencias cuyos autores provenían de 6 Universidades, del CSIC, de 6 empresas, del Ministerio de Defensa y de Administraciones Locales.

En este mismo año Phil Zimmerman publica su Pretty Good Privacy (PGP), ganándose una reprimenda del gobierno de EEUU por exportar software criptográfico en formato electrónico.

Un poco mas tarde, en 1996, apareció la WWW, que desató el crecimiento especulativo de la *Burbuja.com* de las empresas de Internet. La burbuja llegó a su máximo en el 2000, en el 2001 comenzó a desinflarse para y pincharse y desaparecer en 2005. ¿Estaremos asistiendo al inflado de otra nueva burbuja, la *RedesSociales.com*?

En la última década un tema de moda es el de los ataques a criptosistemas contenidos en un chip mediante canales laterales, estudiando su forma y las contramedidas adecuadas. Es decir los ataques a las tarjetas de crédito, débito, monedero, DNI y pasaporte electrónicos, mediante un acceso físico al circuito electrónico o su perturbación mediante manipulación de la alimentación, introducción de transitorios, lectura de su radiación electromagnética localizada, reacción al frío o calor excesivos, etc., con el fin de leer las claves en ellas contenidas, total o parcialmente. Estos ataque pueden comprometer la seguridad de los dispositivos, y se están haciendo grandes esfuerzos en impedirlo. El campo de trabajo es complicado pero muy interesante, pues es un tema de frontera entre especialidades y hace falta combinar las habilidades del criptólogo con las del microelectrónico y las del físico.

V. Caminos paralelos

El interés mundial por la criptología ha generado intereses y caminos paralelos en la investigación. El primero ha sido el de la criptografía caótica, que consiste fundamentalmente en sustituir los generadores pseudoaleatorios por sistemas caóticos. Se pueden distinguir dos clases: la primera corresponde a los criptosistemas caóticos en tiempo continuo,

que son fundamentalmente analógicos, aunque pueden estar simulados digitalmente, se puede afirmar que todos son inseguros, además de lentos. La segunda clase la integran los criptosistemas en tiempo discreto, que consisten fundamentalmente en generadores pseudoaleatorios construidos con aplicaciones caóticas; éstos pueden ser tan seguros y rápidos como los mejores generadores pseudoaleatorios del momento.

El problema fundamental encontrado en estos criptosistemas tiene su raíz en la poca comunicación entre las comunidades de criptólogos y los estudiosos de los sistemas dinámicos caóticos. Muchos de los criptosistemas caóticos propuestos —que normalmente se publican en revistas de física de alto impacto— no tienen en cuenta los principios básicos de la criptología y la efectividad de las técnicas de criptoanálisis, por lo que resultan inseguros.

Otro camino paralelo es el de la criptografía cuántica. Consiste en enviar fotones individuales en un estado cuántico desconocido, que se fija en el momento de su medida. Sirve para establecer claves simétricas sin necesidad de terceros, con absoluta privacidad. Hoy por hoy presenta dos escollos. El primero consiste en la autenticación, que se consigue comparando bits de una secuencia aleatoria almacenada en cada extremo, el problema es que cuando éstos se acaban, se sustituyen por bits generados por el funcionamiento del propio sistema; lo que constituye una violación de normas de seguridad: equivale a transmitir la clave de mañana cifrada con la clave de hoy, si la de hoy estaba comprometida también lo estará la de mañana.

El segundo escollo es el alcance de las transmisiones fotónicas, ya sea por fibra óptica o por aire, que al día de hoy están limitadas a unas decenas de kilómetros —ténganse en cuenta que no se pueden poner amplificadores por el camino, pues se destruiría la seguridad—.

La criptografía cuántica también es un tema de frontera entre telecomunicación, física y criptología y por ello desafiante y con una interesante oferta de trabajo.

VI. Recetas para futuros criptólogos

La criptología es una disciplina en continua expansión, la realidad es que va a remolque del desarrollo de las comunicaciones, pero justamente en este momento estamos asistiendo a un crecimiento explosivo de ellas; y lo que contemplamos hoy no es nada en relación a lo que se avecina, como la computación y almacenamiento en la nube, la generalización de las firmas electrónicas, implantación de RFID en los productos comerciales y el reconocimiento biométrico de personas. Todos estos desarrollos prometen una fuente de trabajo creciente para los jóvenes criptólogos.

Cuando este autor empezó a trabajar en criptología, en los años 70, España era un desierto de información sobre la especialidad. No había una biblioteca a la que acudir preferentemente; era necesario recorrer unas cuantas para poder leerse todos los números de las *Transactions del IEEE*, o del *The Bell System Technical Journal* o de *Electronics*. Con un poco de suerte se podían ir encontrando artículos sueltos y con sus referencias ir buscando otros artículos, enredados como las cerezas.

Al llegar los años 80 la tarea se fue simplificando. En 1981 tuvo lugar en EEUU el primer congreso *CRYPTO* y en 1982 el primer *Eurocrypt*. A partir de entonces basta ir a estos congresos, o abonarse a sus actas, para mantenerse al día. En 1982 se fundó en uno de estos congresos la *International Association for Cryptologic Research* (IACR).

Si se está interesado en hardware criptológico, el congreso apropiado es el *Workshop on Cryptographic Hardware and Embedded Systems* (CHES), también organizado por la IACR desde 1999 (http://www.chesworkshop.org/).

El primer consejo para un futuro criptólogo es asegurarse el acceso a las actas de todos los congresos de la IACR, ya sea en papel, o mejor en electrónico. Las actas en papel se pueden adquirir de la editorial Springer que las recoge en su colección *Lecture Notes in Computer Science* (http://www.springerlink.com/content/0302-9743/). Pero la IACR también ofrece desde el año 2000 las actas gratuitamente, aunque con dos años de retraso, en http://www.iacr.org/archive/ y en http://www.iacr.org/proceedings/. Y también en https://secure.iacr.org/membership/members/springer.html, si se es socio de la IACR. Igualmente, son de sumo interés las *IACR Newsletter*, que publicadas semestralmente y distribuidas gratuitamente desde http://www.iacr.org/newsletter/ proporcionan una información mundial de eventos y publicaciones.

Hoy, gracias a la Web, se puede encontrar cantidades ingentes de información criptológica. Pero ahora el problema es el contrario: separar el grano de la paja.

El segundo consejo es dotarse de unos pocos libros de criptología fundamentales tales como: [13], [14] y [15], para los interesados en números aleatorios: [16] y para los interesados en historia: [6].

El tercer consejo es utilizar los repositorios de artículos en la web, que se pueden obtener de forma gratuita; el fundamental para criptología es el portal de la IACR http://eprint.iacr.org/complete/ donde se envían los preprints de artículos que luego se publican en revistas indexadas, se pueden encontrar artículos desde 1996. Otro repositorio interesante de preprints es el arXiv http://arxiv.org/, en sus apartados de *Mathematics* y *Computer Science*, se pueden encontrar artículos de criptología, especialmente en el apartado de *Cryptography and Security* http://arxiv.org/list/cs.CR/recent.

Los anteriores repositorios no están sujetos a revisión por pares antes de publicarse y no se admiten duplicados de artículos aceptados; pueden ser un buen sitio para empezar a publicar de forma rápida y así evitar los largos periodos de espera de algunas revistas. También tienen la ventaja de hacer llegar las propias publicaciones a personas que no tienen capacidad de adquirir artículos de revistas indexadas y en general de difundir los propios trabajos en la web, al quedar catalogados por todos los buscadores.

Hay excelentes lugares para encontrar artículos sobre criptología —en este caso los artículos pueden ser gratis o de pago— como son: *The Collection of Computer Science Bibliographies* (http://liinwww.ira.uka.de/bibliography/index.html#

about), *The DBLP Computer Science Bibliography* de la universidad de Trier (http://www.informatik.uni-trier.de/~ley/db/index.html). También hay otros útiles buscadores de ciencia en general como los siguientes: *Jstor* (http://www.jstor.org/), Google Académico (http://scholar.google.es/), Citeulike (http://www.citeulike.org/), *Scirus* (http://www.scirus.com/srsapp/) y *Scopus* (http://www.scopus.com/home.url). Y, finalmente, resulta muy útil buscar publicaciones gratuitas científicas en general, en PDF, en el portal *FreeFullPDF* (http://www.freefullpdf.com/).

El cuarto consejo es utilizar sistemas de organización bibliográfica, cosa indispensable después de unos meses de estar almacenando artículos desde los anteriores repositorios y portales. El principal es el programa gratuito *Mendeley Desktop*, que gestiona referencias y PDF; es visor de PDF, extrae metadatos de los PDF, hace búsqueda inteligente de términos en la biblioteca de PDF, genera citas para BibTeX y Word, hace copias de seguridad, sincroniza los archivos de varios ordenadores, permite compartir bibliografía en grupos de trabajo, hace búsquedas en repositorios Web y hace estadísticas (http://www.mendeley.com/). El *JabRef* es un software de gestión bibliográfica gratuito, que complementa al *Mendeley Desktop*, es especialmente apropiado para los archivos BibTeX, además importa archivos de referencias en 15 formatos distintos, exporta a formato OpenOffice y otros formatos, y enlaza a recursos externos URL, DOI y PDF (http://jabref.sourceforge.net/).

El quinto consejo es descargarse la familia de programas CRYPTOOL, disponibles en http://www.cryptool.org/en/, que permiten experimentar gratuita y cómodamente multitud de herramientas de cifrado y criptoanálisis. No menos importante es obtener el *Diehard Battery of Tests of Randomness*, herramienta indispensable para analizar secuencias pseudoaleatorias, diseñada por George Marsaglia, disponible en http://stat.fsu.edu/pub/diehard/.

Finalmente, he de señalar, que mi trayectoria profesional es la consecuencia de haber leído, a mis 20 años, la séptima edición del discurso *Los tónicos de la voluntad, reglas y consejos sobre la investigación científica*, que Santiago Ramón y Cajal pronunció, con ocasión de su ingreso en la *Real Academia de Ciencias Exactas, Físicas y Naturales* en 1897. Hoy, 115 años después, sigue teniendo la máxima vigencia; no en vano, de la mano de su autor España entró en la era de la ciencia. Está disponible la 16ª edición del año 2000, con prólogo de Severo Ochoa ([17]).

AGRADECIMIENTOS

El autor agradece al comité organizador de la RECSI 2012 su invitación para dar esta conferencia.

REFERENCIAS

[1] A. Kerckhoffs, "La cryptographie militaire," *Journal des sciences militaires*, vol. IX, pp. 5–83, Enero 1883.

[2] ——, "La cryptographie militaire," *Journal des sciences militaires*, vol. IX, pp. 161–191, Febrero 1883.

[3] C. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 1, pp. 3–55, 2001. [Online]. Available: http://portal.acm.org/citation.cfm?id=584093

[4] C. E. Shannon, *Communication theory of secrecy systems*. AT and T, 1949, no. 1.

[5] J. C. Galende Díaz, *Criptografía, Historia de la escritura cifrada*. Editorial Complutense, 1995.

[6] D. Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, 3rd ed. Scribner's and Sons, 1996.

[7] S. Singh, *The Code book, the secret history of codes and code-breaking*, paperback ed. Fourth Estate, HarperCollins, 2000.

[8] T. Álvarez, *Diccionario de Santa teresa de Jesús*. Monte Carmelo, 2000, ch. Criptónimos, pp. 446–449.

[9] C. A. Moreyra, *Los criptogramas de Santa Teresa*. Carlos Alberto Moreyra, 1964.

[10] F. de Paula Martí, *Poligrfía ó arte de escribir en cifra en diferentes modos*. Imprenta de Sancha, Madrid, 1808.

[11] J. G. Carmona, *Tratado de criptografía con aplicación especial al ejército*. Ministerio de Defensa, 2011.

[12] P. Serrano García, *Policiología, Criptografía y Perlustración*. La Xilográfica, Septiembre 1943.

[13] J. Katz y Y. Lindell, *Introduction to Modern Cryptography*. Chapman & Hall/CRC Cryptography and Network Security Series, 2007. [Online]. Available: http://www.cs.umd.edu/~jkatz/imc/chap1.pdf

[14] C. Paar, *Understanding Cryptography, A Textbook for Students and Practitioners*. Springer. [Online]. Available: http://www.cryptography-textbook.com/

[15] A. J. Menezes, P. C. van Oorschot y S. A. Vanstone, *Applied Crytography*. CRC Press, 2001. [Online]. Available: http://cacr.uwaterloo.ca/hac/

[16] D. Knuth, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, 3rd ed. Addison-Wesley, 1997.

[17] S. Ramón y Cajal, *Los tónicos de la voluntad, reglas y consejos sobre la investigación científica*, 16th ed. Espasa Calpe, colección Austral, 2000.