NATIONAL GEOGRAPHIC

Matemáticos, espías y piratas informáticos

Codificación y criptografía

El mundo es matemático

FL
FreeLibros

Matemáticos, espías y piratas informáticos

NATIONAL GEOGRAPHIC

Matemáticos, espías y piratas informáticos

Codificación y criptografía

FL
FreeLibros

El mundo es matemático

A mi hijo Vicenç

© 2010, Joan Gómez Urgellés por el texto
© 2012, RBA Contenidos Editoriales y Audiovisuales, S.A.
© 2012, RBA Coleccionables, S.A.

Realización: EDITEC
Diseño cubierta: Llorenç Martí
Diseño interior: Babel, disseny i maquetació, S.L.
Créditos fotográficos: Age Fotostock 38, 70, 71, 85; Album 25; Album-Lessing 37, 48; Archivo militar de Ávila 62, 63i, 63d; Archivo RBA 15, 17a, 17b, 18, 42, 46, 93, 97, 100; Album-Akg 11, 50, 54, 114; Corbis 61i, 61d, 65, 72, 73, 108; iStockphoto 26, 28, 111; Joan Pejoan 115; National Crypologic Museum, Maryland 45, 69

Reservados todos los derechos. Ninguna parte de esta publicación puede ser reproducida, almacenada o transmitida por ningún medio sin permiso del editor

ISBN: 978-84-473-7731-2
Depósito legal: B 17017-2014

Impreso y encuadernado en Gráficas Estella

Impreso en España - *Printed in Spain*

Sumario

Prefacio

Un juego muy habitual en el patio de cualquier colegio es el de idear un alfabeto secreto con el que enviar y recibir mensajes confidenciales. El esfuerzo dedicado a estos códigos primerizos responde más al entusiasmo de los jóvenes espías que al interés de algún tercero por fisgonear la información así transmitida. En el mundo de los adultos, sin embargo, este interés existe, y la confidencialidad de las comunicaciones constituye un tema de extraordinaria importancia.

Antaño circunscritos a las actividades de una élite política y social, la llegada de la era de la información ha hecho de la los códigos y las cifras una necesidad de la sociedad en su conjunto. Este libro se propone explicar la historia de los códigos secretos de la mano del guía más cualificado para ello: las matemáticas.

La criptografía, es decir, el arte de escribir en clave, apareció con la escritura misma. Y aunque egipcios y mesopotámicos ya hicieron uso de métodos de cifrado, los primeros en aplicarse de lleno fueron los griegos y los romanos, culturas belicosas para las cuales comunicarse en secreto era un elemento clave para el éxito militar. Con ellos arrancó un conflicto de nuevo cuño: el que se declara entre los guardianes del secreto, los criptógrafos, y quienes pretenden desvelarlo, los criptoanalistas. Se trata de una lucha en la sombra que, en función de cada época, se decanta hacia un lado o hacia el otro sin acabar de resolverse nunca. En el siglo VIII, por ejemplo, el sabio árabe al-Kindi dio con una herramienta de descifrado, el análisis de frecuencias, que parecía que iba a dar al traste con las esperanzas de los codificadores. La respuesta de estos segundos, la cifra polialfabética, tardó siglos en llegar, y cuando lo hizo también pareció a su vez definitiva... hasta que una versión más sofisticada de criptoanálisis, alumbrada por un genio inglés en la intimidad de su despacho, de nuevo dio ventaja a los espías. Ya por aquel entonces el arma principal empleada por unos y otros fueron las matemáticas, de la estadística a la aritmética modular, pasando por la teoría de números.

Este toma y daca vivió un punto de inflexión con la aparición de las primeras máquinas de codificación, a las que siguieron, no mucho tiempo después, las dedicadas a la operación contraria. De estas últimas surgió el primer ordenador, el *Colossus*, ideado por los británicos para descifrar los mensajes de Enigma, el ingenio de cifrado alemán. Fue precisamente con la eclosión de la computación cuando los códigos adquirieron un papel protagonista en la transmisión de la información más allá de consideraciones relativas al secreto o a la confidencialidad. El auténtico len-

guaje universal de la sociedad moderna no emplea letras ni ideogramas, sino ceros y unos, y es un código: el binario.

¿Qué bando se ha beneficiado más del advenimiento de las nuevas tecnologías, el de los criptógrafos o el de los criptoanalistas? ¿Sigue siendo posible la seguridad en esta era de virus, piratas informáticos y superordenadores? Lo cierto es que sí, y de nuevo hay que darle las gracias a las matemáticas: en este caso, a los números primos y a sus peculiares características. ¿Cuánto durará esta hegemonía momentánea del secreto? La respuesta a esta pregunta nos llevará a los horizontes últimos de la ciencia actual, dominados por la mecánica cuántica, cuyas asombrosas paradojas marcarán el final de este apasionante viaje por las matemáticas de la seguridad y del secreto.

Este libro se completa con una bibliografía esencial para quienes deseen profundizar más en el mundo de la codificación y la criptografía, y con un índice analítico que facilitará la consulta.

Capítulo 1

¿Cuán segura es la información?

Criptografía: arte de escribir
con clave secreta o de un modo enigmático.
Diccionario de la Real Academia Española

El interés por transmitir un mensaje de forma que su significado quede oculto a los ojos de todo lector que no sea el destinatario o destinatarios es, posiblemente, tan antiguo como la propia escritura. De hecho, se tiene constancia de una serie de jeroglíficos «no estándar» de más de 4.500 años de antigüedad, aunque no se sabe con certeza si obedecían a un intento serio por ocultar información o si más bien respondían a algún tipo de ritual mistérico. Mayor seguridad se tiene con respecto a una tablilla babilónica fechada en el 2.500 a.C. En ella aparecen términos a los que se les ha sustraído la primera consonante, o se emplean caracteres en variantes poco habituales. Investigaciones posteriores han revelado que contiene la descripción de un método para la elaboración de cerámica vidriada, por lo que cabe pensar que fue grabada por un comerciante o tal vez un alfarero celoso de que otros competidores averiguaran los secretos de su oficio.

Con la expansión de la escritura y el nacimiento de grandes imperios en constante lucha fronteriza, la criptografía y, en general, la transmisión segura de información se convirtió en una prioridad creciente de gobiernos e individuos. Hoy en día, con el advenimiento de la era de la Información, la necesidad de proteger la integridad de las comunicaciones y mantener un adecuado nivel de privacidad es más importante que nunca. Apenas hay flujo de información que no se codifique de una forma u otra con el objeto de agilizar su transmisión y asegurar que ésta se produce de forma correcta; por ejemplo, convirtiéndola de texto a lenguaje binario, es decir, una ristra de ceros y unos que resulte comprensible para un ordenador. Una vez codificada, buena parte de esta información debe ser protegida de todo aquel que quiera interceptarla, es decir, debe ser *encriptada*. Por último, el receptor legítimo de la información debe ser capaz de entender aquello que se le

dice, y por tanto tiene que ser capaz de *desencriptarla*. Codificación, encriptación y desencriptación son los pasos básicos de una «danza de la información» que se repite millones de veces por segundo todos y cada uno de los minutos, las horas y los días del año. Y la música que acompaña y gobierna esta danza no es otra que la matemática.

Códigos, cifras y claves

Los entendidos en criptografía emplean el término *codificar* en una acepción distinta a la común. Para ellos, la codificación es un método de escritura en clave que consiste en sustituir unas palabras por otras. La alternativa a este método sería el *cifrado* o *cifra*, el cual sustituye letras o caracteres. Con el tiempo, este segundo se ha hecho tan prevalente que ha acabado por erigirse en sinónimo de escribir en clave. Si nos atenemos a la precisión anterior, el término correcto para este último caso sería *encriptar* (y *desencriptar* para el caso del proceso inverso). Excepto en aquellas ocasiones en que puedan inducir a confusión, en el presente libro se respetará el uso común de los diferentes términos para evitar pesadas reiteraciones.

Según lo visto, si quisiéramos transmitir de forma segura el mensaje «ATACAR», podríamos hacerlo de dos maneras básicas: sustituyendo la palabra (codificación) o sustituyendo alguna o la totalidad de las letras que la componen (cifrado). Una manera sencilla de codificar una palabra es traducirla a un idioma que los posibles «espías» desconozcan, mientras que para cifrarla bastaría, por ejemplo, con sustituir cada letra por otra situada más adelante en el alfabeto. En ambos casos es necesario

EL CÓDIGO BINARIO

Para que un ordenador entienda y procese información, ésta tiene que traducirse del lenguaje en el que esté escrita al denominado *lenguaje binario*. Este lenguaje se compone únicamente de dos caracteres: el cero y el uno. La expresión binaria de las diez primeras cifras del sistema decimal es la de la tabla adjunta.

Por consiguiente, el número 9.780 se expresaría, en código binario, como 10011000110100.

0	0
1	1
10	2
11	3
100	4
101	5
110	6
111	7
1000	8
1001	9
1010	10

¿TRADUCIR O DESENCRIPTAR?

Abordar la traducción de un texto escrito en un idioma cuya grafía nos es desconocida puede, en ocasiones, abordarse como un problema general de desencriptación: el mensaje original sería el texto ya traducido a nuestro idioma y el algoritmo de encriptación, las reglas gramaticales y sintácticas del idioma original. Las técnicas empleadas históricamente para uno y otro cometido (esto es, traducir y desencriptar) guardan muchas similitudes. En ambos casos, sin embargo, se tiene que dar una misma circunstancia: que emisor y receptor compartan, al menos, un idioma. Es por ello que la traducción de textos escritos en idiomas «perdidos», como el jeroglífico egipcio o el Linear B minoico, fue imposible hasta que se halló una correspondencia entre ellos y otro idioma conocido; en ambos casos, el griego. En la ilustración, tablilla hallada en Creta cuyas inscripciones corresponden al idioma conocido como Linear B.

que el destinatario conozca la regla que hemos empleado para encriptar el mensaje o corremos el riesgo de que no lo entienda. Si ya hemos acordado con él que íbamos a emplear una regla u otra («traducirla a otro idioma», «sustituir cada letra por otra situada más adelante en el alfabeto»), sólo necesitaremos comunicarle, en el primer caso, el idioma de destino, y en el segundo, el número de posiciones que hemos adelantado en el alfabeto para sustituir cada letra. En nuestro ejemplo de cifrado, si el destinatario recibe el mensaje «CVCECT», y sabe que hemos adelantado cada letra dos posiciones, podrá revertir el proceso fácilmente y desencriptar el mensaje.

La distinción que se ha establecido entre regla de encriptación (de aplicación general) y parámetro concreto de encriptación (específica de cada mensaje o de un grupo de mensajes) resulta de extrema utilidad, puesto que un eventual «espía» necesita conocer *las dos* para poder descifrar el mensaje. Así, el espía podría saber que la regla de cifrado es sustituir cada letra por la que le corresponde un número concreto x de posiciones más adelante en el alfabeto, pero si desconoce x deberá probar todas las combinaciones posibles: una para cada letra del alfabeto (si con-

¿CUÁNTAS CLAVES SE PRECISAN?

¿Cuál es el número mínimo de claves necesarias en un sistema de dos usuarios? ¿Y de tres? ¿Y de cuatro? Para que dos usuarios se comuniquen entre sí sólo se precisa una clave. Para el caso de tres, son necesarias tres de ellas: una para la comunicación entre A y B, otra para el par A y C, y una tercera para B y C. De forma análoga, cuatro usuarios necesitarán seis claves. Generalizando, para n usuarios se necesitarán tantas claves como combinaciones de n usuarios escogidos de dos en dos, es decir:

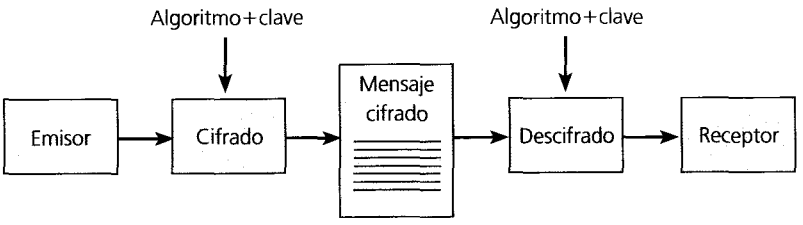
$$\binom{n}{2} = \frac{n(n-1)}{2}.$$

Así, un sistema relativamente pequeño de 10.000 usuarios interconectados requerirá 49.995.000 claves. Para el caso de una población mundial de 6.000 millones de individuos, la cifra resulta del todo mareante: 17.999.999.997.000.000.000.

tamos la ñ, un total de 27). En este ejemplo, la cifra es sencilla y agotar todas las posibilidades –lo que se denomina desencriptación *por fuerza bruta*– no resulta extremadamente laborioso. Sin embargo, para el caso de técnicas más complejas este tipo de ataque, o *criptoanálisis*, resulta a menudo imposible. Además, la intercepción y el eventual descifrado de mensajes están sujetos, habitualmente, a importantes restricciones de tiempo: la información debe ser obtenida con margen suficiente para actuar en consecuencia.

A la regla general de encriptación se la denomina a menudo *algoritmo de encriptación*, mientras que el parámetro concreto empleado para cifrar o codificar el mensaje (en nuestro ejemplo de cifrado, el número de posiciones adelantadas que ocupa la letra con la que sustituimos a la del mensaje original, es decir, 2) se denomina *clave*. Es obvio que, dado un mismo algoritmo de encriptación, el número de claves puede ser muy grande, y ya hemos visto que, a la hora de desencriptar un mensaje, conocer el algoritmo puede muy bien ser inútil a menos que se sepa también la clave empleada para encriptarlo. Siendo las claves por lo general más fáciles de cambiar y de distribuir, parece lógico concentrar los esfuerzos en proteger un sistema de encriptación que mantenga en secreto las claves. Este principio fue consagrado de forma definitiva a finales del siglo XIX por el lingüista neerlandés Auguste Kerckhoffs von Nieuwenhof, en el que se conoce como «principio de Kerckhoffs».

Como resumen de lo expuesto hasta el momento, podemos plantear un sistema general de encriptación definido por los elementos siguientes:



Es decir, un emisor y un receptor del mensaje, un algoritmo de encriptación y una clave definida que permiten al emisor cifrar el mensaje y al receptor, descifrarlo. Más adelante veremos como este esquema se ha visto modificado en tiempos recientes en razón de la naturaleza y función de la clave, pero hasta ese momento nos ceñiremos a él.

Claves privadas y claves públicas

El principio de Kerckhoffs consagra la clave como el elemento fundamental en la seguridad de un sistema criptográfico. Hasta tiempos relativamente recientes, las claves de un emisor y de un receptor en todos los sistemas criptográficos concebibles tenían que ser iguales o cuando menos simétricas; es decir, tenían que servir igualmente para encriptar y desencriptar. La clave era, pues, un secreto compartido entre emisor y receptor, y por tanto, el sistema criptográfico en cuestión era vulnerable, por así decirlo, por ambos lados. Este tipo de criptografía dependiente de una misma clave compartida por emisor y receptor se denomina *clásica* o de *clave privada* (o, también, de llave privada, por analogía con el término inglés original «key», llave).

¿CUÁNTAS CLAVES SE PRECISAN? 2ª PARTE

Como hemos visto, la criptografía clásica requería de un número enorme de claves. Sin embargo, en un sistema de criptografía pública, dos usuarios cualesquiera que intercambien mensajes necesitan sólo cuatro de ellas: sus respectivas claves públicas y privadas. En este caso tenemos que n usuarios «sólo» necesitan $2n$ claves.

Todos los sistemas criptográficos ideados por el hombre desde el inicio de los tiempos, con independencia del algoritmo que se empleara y de la complicación del mismo, compartían esta característica. Que la clave de un sistema tiene que ser la misma para receptor y emisor parece una cuestión de sentido común. Al fin y al cabo, ¿cómo es posible cifrar un mensaje de acuerdo con una clave y descifrarlo de acuerdo con otra, esperando que el significado del texto se mantenga? Durante miles de años, esta posibilidad se antojaba un absurdo lógico. Sin embargo, y como veremos con más detalle más adelante, hace apenas cinco décadas lo absurdo acabó por tornarse plausible, y lo plausible supo implementarse de forma práctica.

Hoy en día, los algoritmos de encriptación empleados en la mayoría de las comunicaciones consisten en, al menos, dos claves: una privada, como era tradicional, y otra pública que conoce todo el mundo. El mecanismo de transmisión es como sigue: un emisor se hace con la clave pública del receptor a quien desea enviar el mensaje, y la emplea para encriptarlo. El receptor coge ahora su clave privada y la utiliza para descifrar el mensaje recibido. Este sistema posee, además, una importantísima ventaja adicional: ni el emisor ni el receptor han tenido que verse previamente para acordar ninguna de las claves implicadas, con lo que la seguridad del sistema se refuerza todavía más. Esta forma de encriptación absolutamente revolucionaria se conoce como de *clave pública*, y constituye la base de la seguridad de las redes globales de comunicación contemporáneas.

En la base del desarrollo de esta tecnología revolucionaria se encuentran las matemáticas. En efecto, y como se explicará en detalle, la criptografía moderna descansa en dos pilares: la aritmética modular, por un lado, y la teoría de números –en especial, la parte de ella concerniente al estudio de los números primos–, por otro.

El «telegrama Zimmermann»

La criptografía es uno de los ámbitos de la matemática aplicada donde se hace más evidente el contraste entre la limpieza y «frialdad» de los principios teóricos que la gobiernan y la enormidad de las consecuencias humanas de su puesta en práctica. Al fin y al cabo, del éxito o fracaso a la hora de mantener seguras las comunicaciones a menudo pende el destino de naciones enteras. Uno de los ejemplos más espectaculares de cómo la criptografía cambió el rumbo de la historia contemporánea se dio hace aproximadamente un siglo, en el caso conocido desde entonces como «el telegrama Zimmermann».


"All the News That's Fit to Print."

The New York Times.

EXTRA 5:30 A.M.

LUSITANIA SUNK BY A SUBMARINE, PROBABLY 1,260 DEAD; TWICE TORPEDOED OFF IRISH COAST; SINKS IN 15 MINUTES; CAPT. TURNER SAVED, FROHMAN AND VANDERBILT MISSING; WASHINGTON BELIEVES THAT A GRAVE CRISIS IS AT HAND

SHOCKS THE PRESIDENT

Washington Deeply Stirred by the Loss of American Lives.

The Lost Cunard Steamship Lusitania

Portada del New York Times *dando noticia del hundimiento del* Lusitania.

El 7 de mayo de 1915, con media Europa sumida en un sangriento conflicto fraticida, un submarino alemán –los tristemente célebres U-Boat– torpedeó el barco de pasajeros *Lusitania*, que navegaba bajo bandera británica en las cercanías de Irlanda. El resultado fue una auténtica masacre: 1.198 civiles, de entre los cuales 124 eran de nacionalidad estadounidense, perdieron la vida en el naufragio. La noticia enfureció a la opinión pública de Estados Unidos, y el gobierno del presidente Woodrow Wilson advirtió a sus homólogos alemanes que cualquier acto similar llevaría consigo la inmediata entrada norteamericana en la guerra en el bando de los aliados. Además, Wilson exigió que los submarinos alemanes emergieran antes de llevar a cabo cualquier ataque, para evitar así nuevos hundimientos de navíos civiles. El potencial ofensivo de los U-Boat se veía, de este modo, seriamente comprometido.

En noviembre de 1916, Alemania designó a un nuevo ministro de Exteriores con fama de dialogante, Arthur Zimmermann. La noticia fue recibida con alborozo por la prensa estadounidense, que llegó a calificar su nombramiento como «un espléndido augurio de cara a las relaciones entre Alemania y Estados Unidos».

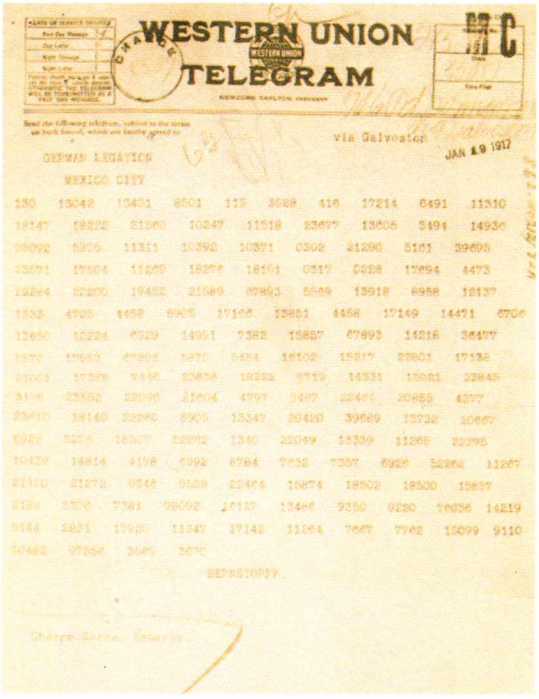
En enero de 1917, menos de dos años después de la tragedia del *Lusitania*, y con el conflicto en pleno auge, el embajador alemán en Washington, Johann von Bernstorff, recibió de Zimmermann el telegrama codificado siguiente, con instrucciones de remitirlo secretamente a su homólogo en México, Heinrich von Eckardt:

«Nos proponemos comenzar el primero de febrero la guerra submarina, sin restricción. No obstante, intentaremos mantener la neutralidad de los Estados Unidos de América.
En caso de no tener éxito, proponemos a México una alianza sobre las siguientes bases: hacer juntos la guerra, declarar juntos la paz. Aportaremos abundante ayuda financiera; y el entendimiento por nuestra parte de que México ha de reconquistar el territorio perdido en Nuevo México, Texas y Arizona. Los detalles del acuerdo quedan a su discreción [de Von Eckardt].
Queda usted encargado de informar al presidente [de México] de todo lo antedicho, de la forma más confidencial posible, tan pronto como el estallido de la guerra con los Estados Unidos de América sea un hecho seguro. Debe además sugerirle que tome la iniciativa de invitar a Japón a adherirse de forma inmediata a este plan, ofreciéndose al mismo tiempo como mediador entre Japón y nosotros.
Haga notar al Presidente que el uso despiadado de nuestros submarinos ya hace previsible que Inglaterra se vea obligada a pedir la paz en los próximos meses.»

En caso de hacerse público, este telegrama tendría como segura consecuencia el estallido de la guerra entre Alemania y Estados Unidos. Aunque el káiser Guillermo II sabía que ello sería inevitable una vez sus submarinos empezaran a operar sin emerger antes de un ataque, confiaba en que, por aquel entonces, el Reino Unido ya habría capitulado y, por tanto, no hubiera conflicto al que los norteamericanos pudieran sumarse. Si no se daba esta circunstancia, la amenaza activa de México a lo largo de la frontera sur de Estados Unidos podía igualmente disuadir a los norteamericanos de iniciar un doble conflicto a enorme distancia el uno del otro. Para ello, sin embargo, México iba a necesitar un mínimo de tiempo para organizar sus fuerzas. Por tanto, era vital que las intenciones germanas permanecieran en secreto el tiempo suficiente como para que la guerra submarina decantara la balanza del conflicto a su favor.

La Habitación 40 se pone a trabajar

El gobierno británico, no obstante, tenía otros planes. Desde poco después del inicio del conflicto, había bloqueado los cables telegráficos submarinos que conectaban Alemania con el hemisferio occidental, de modo que toda comunicación eléctrica tenía que circular por cables susceptibles de ser interceptados por los ingleses. Estados Unidos, en un intento



WESTERN UNION
TELEGRAM

via Galveston
JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13451 6501 115 3028 416 17214 6491 11310
18147 18202 21560 10847 11518 23677 13005 5494 14936
09092 5905 11311 10592 10371 0302 21290 5101 39695
23691 17504 11260 18278 18101 0319 0458 17694 4473
19264 22200 19452 21569 07803 5869 13918 8958 12137
1353 4705 1458 6905 17166 13851 1458 17149 14471 6705
15560 15224 6929 14991 7382 15857 67893 14216 36477
9370 17563 67293 5870 5454 16102 15017 22801 17138
21021 17388 9416 23676 18222 6719 14331 15081 23645
8148 23550 22098 21504 4797 9497 22464 20855 4377
23410 18140 22890 8905 13347 20420 39689 15732 20667
6967 5275 18927 12892 1340 22049 15339 11266 22795
10439 16814 4178 6992 8784 7852 7357 6926 52282 11267
21100 21272 9348 9509 22464 16874 18502 18500 15857
8188 5376 7581 98092 16127 13486 9350 9220 76036 14219
5144 2831 13520 11347 17142 11504 7667 7762 13099 9110
10480 97556 3569 3670

BERNSTORFF

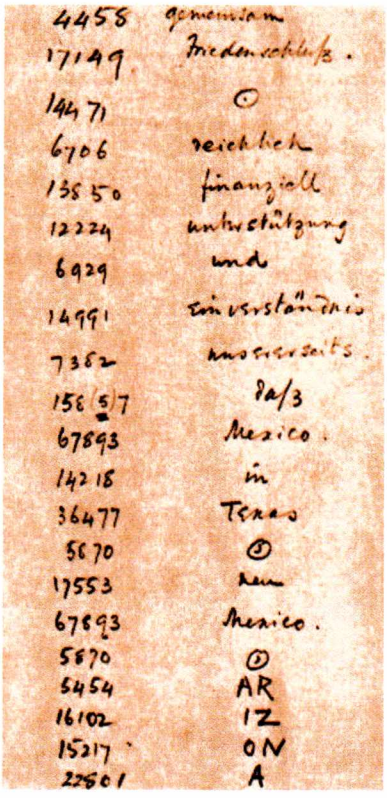
TELEGRAM RECEIVED.

M. CHILD
...ter 1-8-58
...rson, State Dept.
By Mack & Eckhoff Assistant
Date Oct. 27, 58

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate betwsen Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

Arriba, el telegrama Zimmermann en la versión que remitió el embajador alemán en Washington, Johann von Bernstorff, a su homólogo en México; abajo, la versión descifrada del mismo telegrama.



Parte del descifrado parcial del telegrama Zimmermann llevado a cabo por los británicos. En la parte inferior puede apreciarse cómo los alemanes, careciendo de un código para el término «Arizona», lo codificaron por partes: AR, IZ, ON, A.

por mantener viva la esperanza de un final pactado al conflicto, había proporcionado a Alemania la posibilidad de transmitir mensajes diplomáticos bajo el paraguas de su propio tráfico en este ámbito. Es por ello que el mensaje de Zimmermann se transmitió, por cable, a la legación alemana en Washington. Sin embargo, esta precaución se iba a demostrar insuficiente. El gobierno británico interceptó el mensaje y lo remitió ipso facto a su departamento de criptoanálisis, conocido como Habitación 40.

Los alemanes habían empleado para la encriptación el algoritmo convencional del ministerio de Exteriores y habían usado para el caso una clave denominada 0075, que los expertos de la Habitación 40 habían ya descifrado parcialmente con anterioridad. El algoritmo en cuestión combinaba la sustitución de palabras (codificación) con la de letras (cifrado), una práctica similar a la empleada en otra de las herramientas de

encriptación usadas a la sazón por los alemanes, la cifra ADFGVX, que se examinará en detalle más adelante.

Los británicos tardaron poco en descifrar el telegrama, aunque se mostraron reticentes a enseñarlo a los estadounidenses de inmediato. Había dos razones para ello: en primer lugar, el telegrama se había transmitido bajo la cobertura dada por Estados Unidos a los mensajes diplomáticos alemanes, privilegio del que los ingleses habían hecho caso omiso; en segundo lugar, de hacer público el telegrama, el gobierno alemán sabría de inmediato que sus códigos se habían visto comprometidos y cambiaría su sistema de encriptación. Así las cosas, los británicos lograron convencer a los americanos de que la versión interceptada y descifrada había sido la reenviada por Bernstorff a México, y a los alemanes de que el telegrama había sido interceptado, ya descifrado, en este último país.

A finales de febrero, el gobierno de Wilson filtró el contenido del telegrama a la prensa, parte de la cual –en especial los diarios pertenecientes al grupo Hearst, pacifistas y proalemanes– se mostró escéptica. Sin embargo, a mediados de marzo Zimmermann reconoció públicamente ser el autor del texto. Poco más de dos semanas después, el 6 de abril de 1917, el Congreso de Estados Unidos declaró la guerra a Alemania, y selló así el desenlace del conflicto.

Si bien extraordinario en sus circunstancias, el del «telegrama Zimmermann» es sólo uno más de los episodios históricos en los que la criptografía ha jugado un rol esencial. A lo largo de este libro se verán muchos otros, desperdigados a lo largo de los siglos y las culturas. Con todo, casi puede asegurarse que no están todos los que son. En buena parte, la historia de la criptografía es, como corresponde, una historia secreta.

Capítulo 2

La criptografía, de la Antigüedad al siglo XIX

Como ya se ha apuntado, la criptografía es una disciplina antigua, con toda probabilidad tan antigua como la necesidad de comunicarse. Sin embargo, no se trata del único método posible de transmitir información en secreto. Al fin y al cabo, todo texto debe tener un soporte, y si conseguimos hacer dicho soporte invisible a todo el mundo excepto al destinatario, habremos cumplido nuestro objetivo. A la técnica de ocultar la existencia misma del mensaje se la denomina *esteganografía*, y su origen probablemente corre parejo al de la criptografía.

La esteganografía

El griego Herodoto, considerado el padre de la historiografía gracias a sus investigaciones realizadas durante el siglo V a.C., hace constar en su crónica de las guerras entre griegos y persas dos curiosas instancias de esteganografía que denotan un ingenio considerable. En la primera, referida en el Libro III de su magna *Historia*, Histieo, el tirano de Mileto, ordenó a un hombre que se rapara la cabeza. A continuación, escribió en el cráneo del sujeto el mensaje que deseaba transmitir y esperó a que volviera a crecerle el cabello, momento en el cual despachó al hombre hacia su destino, el campamento de Aristágoras. Una vez a salvo, el mensajero advirtió de la treta y, rapada de nuevo la cabeza, mostró el ansiado mensaje a su destinatario. La segunda, de ser cierta, reviste todavía mayor importancia histórica, por cuanto le permitió a Demarato, rey espartano exiliado en Persia, advertir a sus compatriotas del proyecto de invasión del rey persa, Jerjes. Cuenta Herodoto en el Libro VII de la misma obra:

> «El caso es que no podía alertarlos así como así [Demarato], por lo que se le ocurrió la siguiente idea: cogió una tablilla de doble hoja, le raspó la cera y, acto seguido, puso por escrito, en la superficie de madera de la tablilla, los planes del monarca; hecho lo cual, volvió a recubrirla con cera derretida, tapando el mensaje, a fin de que el transporte de la tablilla, al estar en blanco,

> no ocasionase el menor contratiempo ante los cuerpos de guardia apostados en el camino. Cuando la tablilla llegó definitivamente a Lacedemonia [Esparta], los lacedemonios no acertaron a dar con una explicación, hasta que, según tengo entendido, al fin Gorgo [...] sugirió que raspasen la cera, porque encontrarían –les indicó– un mensaje grabado en la madera.»

Un recurso esteganográfico cuyo uso ha sobrevivido al paso de los siglos es el de la tinta invisible en todas sus formas. Inmortalizada en miles de relatos y películas, los materiales empleados para tal fin –jugo de limón, savia de plantas o incluso orines humanos– suelen tener origen orgánico, dado su alto contenido natural en carbono y, en consecuencia, su tendencia a tiznarse al ser sometidos a temperaturas modestamente altas, tales como la luz de una vela.

La esteganografía constituye, al fin, un recurso de indudable utilidad, aunque para el caso de un número masivo de comunicaciones es seguramente inviable. Además, empleada como recurso único, adolece de un importante defecto: en el caso de que el mensaje sea interceptado, el significado del mismo resulta transparente. Es por eso que la esteganografía suele emplearse principalmente como un método complementario a la criptografía para así reforzar la seguridad de la transmisión.

Como puede adivinarse por los casos anteriormente citados, el gran motor histórico de la transmisión segura de la información ha sido el conflicto armado. Siendo así, no es de extrañar que un pueblo guerrero por excelencia como los espartanos –de creer a Herodoto, ya de por sí maestros en el arte de la esteganografía– fueran pioneros en el desarrollo de la criptografía.

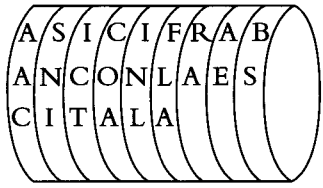
La criptografía por transposición

En la guerra que enfrentó a espartanos y atenienses por la hegemonía en el Peloponeso se hizo habitual el uso de largas tiras de papel sobre las que, una vez enrolladas en un bastón (*escitala*), se escribía el mensaje. El cifrado se basaba en la alteración del mensaje original mediante la inclusión de símbolos innecesarios que desaparecían al enrollar el mensaje en el bastón, de longitud y grosor prefijados. Aún sabiendo la técnica utilizada (esto es, el algoritmo de encriptación), si no se disponía de las dimensiones exactas de la escitala, al interceptor del mensaje le era muy difícil descifrar el mensaje. El grosor y la longitud de la escitala eran, al fin, la clave del sistema. Cuando se desenrollaba la tira, el mensaje resultaba ilegible para cualquiera que desconociera el método o no tuviera un bastón del mismo grosor.

CON LETRA PEQUEÑA

Durante los años de la Guerra Fría las películas de espías se llenaron de mensajes transmitidos a través de soportes casi invisibles dado su reducidísimo tamaño: los microfilms. Unas décadas antes, durante la Segunda Guerra Mundial, los agentes alemanes emplearon con frecuencia un recurso esteganográfico, conocido como *micropunto*, consistente en reducir la fotografía de un texto breve al tamaño de un punto tipográfico, que a continuación era incluido como un signo más de otro texto, éste sí inocuo.

En el dibujo, el mensaje que se desea transmitir es: «Así cifraban con la escitala», pero la tira desenrollada muestra en su lugar un galimatías incomprensible: «aac sni ict coa inl fla ra ae bs».



M = ASI CIFRABAN CON LA ESCITALA

C = AAC SNI ICT COA INL FLA RA AE BS

El de la escitala es un método criptográfico conocido como de transposición, y consiste en el reordenamiento de los caracteres del mensaje. Para hacernos una idea de la potencia de este método, nos plantearemos el caso sencillo de transponer tres caracteres: A, O y R. Una rápida probatura, sin necesidad de cálculo alguno, revela que existen hasta seis formas distintas de reordenarlos, a saber: AOR, ARO, OAR, ORA, ROA y RAO.

En abstracto, el proceso es como sigue: una vez situado en primer lugar uno de los tres caracteres posibles, para un total de tres disposiciones distintas, nos quedan dos caracteres que pueden a su vez ser reordenados de dos maneras distintas para un nuevo total de $3 \times 2 = 6$ disposiciones. Para el caso de un mensaje algo mayor de, por ejemplo, 10 caracteres, el número de reordenamientos posibles es ahora

MANUAL PARA SEÑORITAS

El *Kama-sutra* es un extenso manual que versa, entre otros temas, de los conocimientos que una mujer precisa para ser una buena esposa y compañera. Escrito alrededor del siglo IV a.C. por el brahmin Vatsyayana, recomienda hasta 64 habilidades distintas, entre las que se cuentan la música, la cocina o el ajedrez. La número 45 nos interesa especialmente, puesto que trata del arte de la escritura secreta o *mlecchita-vikalpa*. El sabio hindú recomienda diversos métodos, entre los que se cuenta el siguiente: dividir el alfabeto por la mitad, y emparejar las letras resultantes dos a dos de forma aleatoria. En este sistema, cada emparejamiento de letras constituye una clave. Una de ellas podría ser, por ejemplo, la siguiente.

A	S	C	D	N	F	G	X	I	J	K	Z	M
E	O	P	Q	R	B	T	U	V	W	H	Y	L

Para escribir el mensaje secreto, la dama sólo tendría que sustituir todas las A del texto original por E, las D por Q, las J por W, etc., y viceversa.

$10\times9\times8\times7\times6\times5\times4\times3\times2\times1$ (operación que en matemáticas se expresa con la notación 10!), para un total de 3.628.800. Generalizando, para un número n de caracteres existen $n!$ formas distintas de reordenarlos. Así, un mensaje de unos todavía modestos 40 caracteres arroja un número tal de reordenamientos que haría del todo inviable su eventual comprobación. ¿Acaso se ha hallado el método criptográfico perfecto?

No del todo. En efecto, un algoritmo de transposición aleatoria ofrece un elevado nivel de seguridad, pero ¿cuál es la clave que permite descifrarlo? La aleatoriedad del proceso es a la vez su fortaleza y su debilidad. Se necesitaba otro método de encriptación que permitiera generar claves sencillas, fáciles de recordar y de transmitir, sin sacrificar por ello grandes dosis de seguridad. Acababa de empezar la búsqueda del algoritmo perfecto, cuyos primeros protagonistas fueron los emperadores romanos.

Al César lo que es del César

Llegué, vi, vencí.
Julio César

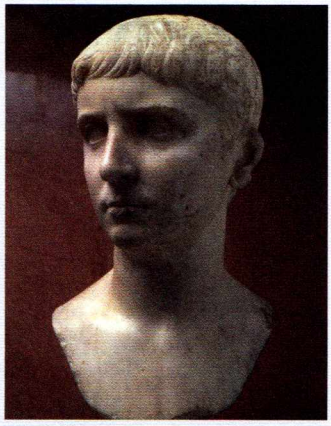
En paralelo a los cifrados por transposición se desarrollaron los llamados por sustitución. A diferencia de la transposición, la sustitución estricta cambia una letra por otra –en realidad, por un símbolo cualquiera–, con independencia de que esta

última se encuentre presente en el mensaje o no. A modo de recordatorio, se dirá que en la transposición la letra cambia su posición pero mantiene su rol (una misma letra significa lo mismo en el mensaje original y en el cifrado), mientras que en la sustitución la letra mantiene su posición pero cambia su rol (una misma letra significa una cosa en el mensaje original y otra, en el cifrado). Uno de los primeros algoritmos de sustitución de los que se tiene constancia es el denominado *cifrado de Polibio*, llamado así en honor del historiador griego homónimo (203-120 a.C.), que nos legó la documentación relativa al mismo. El método en cuestión se desarrolla en profundidad en los anexos del presente volumen.

Aproximadamente cincuenta años después del cifrado de Polibio, en el siglo I a.C., apareció otro cifrado por sustitución, conocido con el nombre genérico de *código César* por ser esta figura histórica uno de sus más asiduos practicantes. El código César es uno de los más estudiados en el ámbito de la criptografía, y resulta de gran utilidad porque permite ilustrar los principios de la aritmética modular, uno de los pilares del estudio matemático de la escritura en clave.

El cifrado César consiste en reasignar a cada letra del abecedario otra nueva resultante de desplazar éste un determinado número de lugares. Tal como hace constar el gran historiador Suetonio en su *Vida de los Césares*, Julio César cifraba su correspondencia particular mediante un algoritmo de sustitución de este tipo:

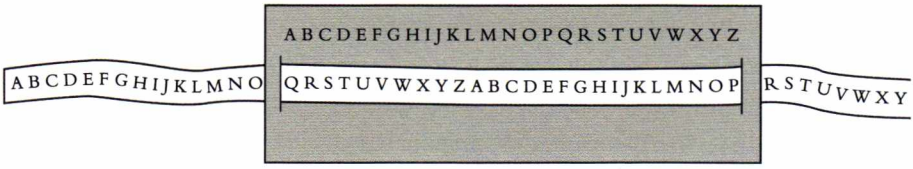
CAYO JULIO CÉSAR (100-44 A.C.)



Militar y político cuya dictadura puso fin a la República en Roma. Tras desempeñar el cargo de magistrado de la Hispania Ulterior, se unió a otros dos poderosos personajes de la época, Pompeyo y Craso, y formó con ellos el Primer Triunvirato, consolidado con el matrimonio de Julia, hija de César, con Pompeyo. Los tres se repartieron las zonas de influencia del imperio romano: Craso recibió el gobierno de los países de Oriente, Pompeyo permaneció en Roma y César asumió el mando militar de la Galia Cisalpina y el proconsulado de la Narbonense. Desde ese momento se inició una dura guerra contra los galos que duró ocho años, y que culminó en la conquista romana de la Galia. De ahí, César marchó con sus legiones hacia la capital, donde se instaló como dictador único.

cada letra del mensaje original era sustituida por la que la seguía tres posiciones más adelante en el alfabeto: la letra A era sustituida por D, la B por E, y así hasta la última letra.

El cifrado y descifrado de un mensaje así encriptado podía llevarse a cabo con un sencillísimo artefacto como el siguiente:

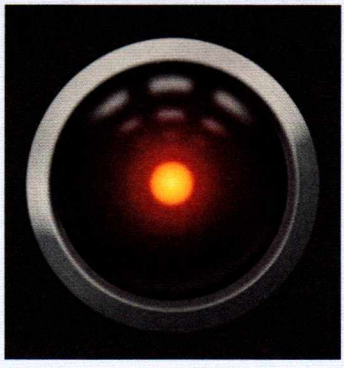


A continuación se examina el proceso con mayor detalle. En la tabla inferior se muestra el alfabeto de partida y la transformación que realiza un cifrado César de tres posiciones adelantadas para el alfabeto español de 27 letras. En la fila superior se muestra el alfabeto original y, en la inferior, el alfabeto cifrado.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

CÓDIGOS CINEMATOGRÁFICOS

En el clásico de la ciencia ficción cinematográfica *2001: Una odisea del espacio,* escrita y dirigida en 1968 por Stanley Kubrick, aparece un súper ordenador dotado de conciencia, bautizado como HAL 9000, que acaba por volverse loco e intenta matar a la tripulación de la nave espacial que monitoriza. Consideremos ahora un código César de clave B y tratemos la palabra «HAL» como un mensaje encriptado con dicho código. Se observará que a la letra H le corresponde la letra I; a la A, la letra B, y a la L, la letra M, es decir, «IBM», por aquel entonces un gran conglomerado industrial que monopolizaba la fabricación de ordenadores. ¿Estaba Kubrick intentando avisar a los espectadores acerca de los peligros de la inteligencia artificial desatada?



El ojo luminoso de HAL 9000 de la película 2001: Una odisea del espacio.

Así dispuestos ambos alfabetos, el original o *llano* y el cifrado, para encriptar un mensaje cualquiera simplemente es cuestión de cambiar los caracteres de uno por los del otro. La clave del cifrado es el carácter que corresponde al valor encriptado de la primera letra del alfabeto original: en este caso, la letra D, ya que es la que se corresponde con la letra A. La clásica expresión «AVE CÉSAR» quedaría cifrada como «DYH FHVDU». Por su parte, si el mensaje cifrado es «DUREN», se obtiene que el mensaje desencriptado, o llano, es «ARBOL». Para el caso de un cifrado César como el que se ha descrito, un criptoanalista que hubiera interceptado el mensaje y conociera el algoritmo empleado pero no la clave, debería probar todos los reordenamientos posibles hasta encontrar un mensaje con sentido; para ello, necesitaría explorar, como máximo, el número total de claves, esto es, desplazamientos. Para un alfabeto de n letras, n desplazamientos posibles que arrojan un mismo número de alfabetos cifrados o claves.

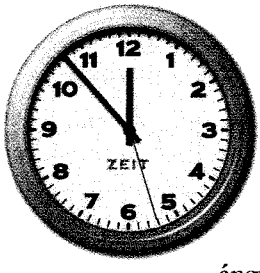
16 = 4. Aritmética modular y las matemáticas del cifrado César

¿16 = 4? y ¿2 = 14? No se trata de ninguna broma, ni de ningún sistema de numeración extraño. El funcionamiento de un código César puede formalizarse con una herramienta muy común en las matemáticas y todavía más en criptografía, la aritmética modular o «aritmética del reloj». Esta técnica tiene sus orígenes en el trabajo del matemático griego Euclides (325-265 a.C.), y es una de las bases fundamentales de los sistemas modernos de seguridad de la información. En este apartado se introducen, de forma llana, los conceptos matemáticos básicos relacionados con esta particular aritmética.

EL PADRE DE LA CRIPTOGRAFÍA ANALÍTICA

La obra principal de Euclides de Alejandría, los *Elementos,* está integrada por 13 volúmenes que versan sobre materias tales como la geometría plana, las proporciones en general, las propiedades de los números, las magnitudes inconmensurables y la geometría del espacio. Aunque principalmente asociado a este último ámbito, los trabajos del matemático griego relativos a la aritmética de operaciones realizadas sobre conjuntos numéricos finitos o *módulos* constituye uno de los pilares del estudio formal de la criptografía. Conocida y admirada por los árabes, la primera edición europea de las obras de Euclides emergió en Venecia en 1482. Tanto árabes como venecianos fueron, incidentalmente, grandes maestros de la criptografía.

Consideremos un clásico reloj analógico y comparémoslo con uno digital. La distribución horaria analógica divide la esfera en doce partes, que escribiremos como 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11. La equivalencia horaria entre un reloj analógico y otro digital se muestra en la tabla siguiente.



0	1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22	23

Cuando se dice, por ejemplo, que son las «16 horas» se está diciendo también que son las «4 de la tarde». Se maneja el mismo principio en el caso de las mediciones de ángulos: un ángulo de 370° es equivalente a otro de 10°, porque hay que descontar del segundo valor una vuelta completa de 360°. Nótese que $370 = (1 \cdot 360) + 10$ o, también, que 10 es el resto de dividir 370 por 360. ¿Cuántos grados equivalen a 750°? Descontadas las vueltas completas pertinentes, se obtiene que un ángulo de 750° es equivalente a otro de 30°. Se cumple que $750 = 2 \cdot 360 + 30$ y que 30 es el resto de dividir 750 por 360. En notación científica esta relación se escribe:

$$750 \equiv 30 \text{ (mód. 360)}.$$

Y se dice de ella que «750 es congruente con 30 módulo 360». En el caso del reloj escribiríamos $14 \equiv 2$ (mód. 12).

También se podría imaginar un reloj con números negativos. En este caso, ¿qué hora será cuándo la aguja del reloj marque el −7? O, lo que es lo mismo, ¿con quién sería congruente el −7 en módulo 12? Operemos recordando que el valor «0» en nuestro reloj de 12 partes equivale a «12»:

$$-7 = -7 + 0 \equiv -7 + 12 = 5.$$

CÁLCULOS CON MÓDULOS

¿Cómo calcular 231 en módulo 17 con una calculadora?

En primer lugar dividimos 231 entre 17, y obtenemos 13,58823529.

En segundo lugar, realizamos el producto $13 \cdot 17 = 221$. De este modo eliminamos los decimales de la operación.

Finalmente, hacemos la resta $231 - 221 = 10$, obteniendo así el resto de la división.

231 en módulo 17 es 10. Este dato se expresa como $231 \equiv 10$ (mód. 17).

La matemática de los cálculos con nuestro reloj analógico de 12 partes se denomina *aritmética en módulo 12.*

Generalizando, se dice que $a \equiv b$ (mód. m) si el resto de la división (o *división euclidea*) entre a y m es b, siendo a, b y m números enteros. El número b equivale al resto de dividir a entre m. Las siguientes afirmaciones son equivalentes

$$a \equiv b \text{ (mód. } m)$$
$$b \equiv a \text{ (mód. } m)$$
$$a - b \equiv 0 \text{ (mód. } m)$$
$$a - b \text{ es múltiplo de } m.$$

La pregunta «¿Qué hora analógica son las 19h?» es equivalente, en terminología matemática, a esta otra: «¿Con quién es congruente 19 en módulo 12?» Para responder a esa pregunta, se debe resolver la ecuación

$$19 \equiv x \text{ (mód. 12).}$$

Al dividir 19 entre 12 se obtiene de cociente 1 y de resto 7, en consecuencia:

$$19 \equiv 7 \text{ (mód. 12).}$$

¿Y para el caso de las 127h? Se divide 127 entre 12 y se obtiene de cociente 10 y de resto 7, luego

$$127 \equiv 7 \text{ (mód. 12).}$$

A título de repaso de lo hasta ahora expuesto, examínense las siguientes operaciones en módulo 7, resueltas más abajo:

(1) $3+3 \equiv 6$
(2) $3+14 \equiv 3$
(3) $3 \times 3 = 9 \equiv 2$
(4) $5 \times 4 = 20 \equiv 6$
(5) $7 \equiv 0$
(6) $35 \equiv 0$
(7) $-44 = -44+0 \equiv -44+7 \times 7 \equiv 5$
(8) $-33 = -33+0 \equiv -33+5 \times 7 \equiv 2$

(1) 6 es menor que el módulo, luego conserva su identidad.

(2) $3+14=17$; $17:7=14$ y el resto 3

(3) $3\times3=9$; $9:7=1$ y el resto 2

(4) $5\times4=20$; $20:7=2$ y el resto 6

(5) $7=7$; $7:7=1$ y el resto 0

(6) $35=35$; $35:7=5$ y el resto 0

(7) $-44=-44+0$; $-44+(7\times7)=5$

(8) $-33=-33+0$; $-33+(5\times7)=2$

TABLA DE MULTIPLICAR EN MÓDULO 5 Y APLICATIVO EXCEL

La tabla de multiplicar en módulo 5 tendría el siguiente aspecto:

	0	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Resulta sencillo construir esta y otras tablas similares con unos modestos conocimientos del entorno Excel.

Para el caso de nuestro ejemplo, la sintaxis de las instrucciones concretas en dicho entorno se muestran más abajo. El concepto «resto de dividir un número por 5» se traduce en el lenguaje propio de Excel por «=residuo(Num;5)». La instrucción para hallar el producto de 4 por 3 en módulo 5 sería, pues, «=residuo(4·3;5)», operación que nos devolvería el valor 2. Estas tablas resultan de gran ayuda a la hora de operar en aritmética modular.

	0	1	2	3	4
0	=RESIDUO(B$5*$A6;5)	=RESIDUO(C$5*$A6;5)	=RESIDUO(D$5*$A6;5)	=RESIDUO(E$5*$A6;5)	=RESIDUO(F$5*$A6;5)
1	=RESIDUO(B$5*$A7;5)	=RESIDUO(C$5*$A7;5)	=RESIDUO(D$5*$A7;5)	=RESIDUO(E$5*$A7;5)	=RESIDUO(F$5*$A7;5)
2	=RESIDUO(B$5*$A8;5)	=RESIDUO(C$5*$A8;5)	=RESIDUO(D$5*$A8;5)	=RESIDUO(E$5*$A8;5)	=RESIDUO(F$5*$A8;5)
3	=RESIDUO(B$5*$A9;5)	=RESIDUO(C$5*$A9;5)	=RESIDUO(D$5*$A9;5)	=RESIDUO(E$5*$A9;5)	=RESIDUO(F$5*$A9;5)
4	=RESIDUO(B$5*$A10;5)	=RESIDUO(C$5*$A10;5)	=RESIDUO(D$5*$A10;5)	=RESIDUO(E$5*$A10;5)	=RESIDUO(F$5*$A10;5)

¿Qué relación tiene la aritmética modular con el cifrado César? Para responder a la pregunta se dispone un alfabeto convencional y otro con un desplazamiento de 3 letras, a los cuales se añade, arriba, una correspondencia numérica para los 27 caracteres.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Se observa que la versión cifrada de un carácter de número x (en el alfabeto llano) es el carácter que ocupa la posición $x+3$ (también del alfabeto llano). Por tanto, interesa hallar una transformación tal que a cada valor numérico le asigne el mismo valor desplazado tres unidades, y tome el resultado en módulo 27. Nótese que 3 es la clave del cifrado. Se define así una función

$$C(x) = x + 3 \text{ (mód. 27)},$$

donde x es el valor sin codificar, y $C(x)$ el valor codificado. Basta con sustituir la letra por su equivalencia numérica y aplicar la transformación. Tomemos como ejemplo el mensaje «AZUL», y cifrémoslo.

La A sería el 0, $C(0) = 0+3 \equiv 3$ (mód. 27), que corresponde a la D.
La Z sería el 26, $C(26) = 26+3 = 29 \equiv 2$ (mód. 27), obteniendo así C.
La U sería el 21, $C(21) = 21+3 = 24 \equiv 24$ (mód. 27), obteniendo así X.
La L sería el 11, $C(11) = 11+3 \equiv 14$ (mód. 27), obteniendo así Ñ.

El mensaje «AZUL» cifrado con clave 3 es «DCXÑ».

En general, si x indica la posición de la letra que se desea cifrar (0 para la A, 1 para la B, etc.), la posición de la letra cifrada [denotada por C(x)] vendrá dada por la fórmula

$$C(x) = (x+k) \text{ (mód. } n)$$

donde n= longitud del alfabeto (27 para el castellano, incluyendo la ñ) y k= clave, en función de cuyo valor cambiará el mensaje cifrado.

El descifrado del mensaje es una operación contraria a la del cifrado. En términos de nuestro ejemplo, descifrar equivale a aplicar la fórmula inversa a la utilizada para cifrar, es decir:

$$C^{-1}(x) = (x - k) \text{ (mód. } n).$$

Para el caso del mensaje cifrado «DCXÑ», con un cifrado César de clave 3 sobre el alfabeto castellano, $k = 3$ y $n = 27$ y por tanto

$$C^{-1}(x) = (x - 3) \text{ (mód. } 27).$$

El proceso es como sigue:

Para D $x = 3$, $C^{-1}(3) = 3 - 3 \equiv 0$ (mód. 27), que corresponde a la A.
Para C $x = 2$, $C^{-1}(2) = 2 - 3 = -1 + 27 \equiv 26$ (mód. 27), con lo cual obtenemos la Z.
Para X $x = 24$, $C^{-1}(24) = 24 - 3 \equiv 21$ (mód. 27), obteniendo la U.
Para Ñ $x = 14$, $C^{-1}(14) = 14 - 3 \equiv 11$ (mód. 27), obteniendo la L.

El mensaje «DCXÑ» cifrado con un código César de clave 3 se corresponde, como ya se sabía, con el texto llano «AZUL».

Finalmente, y para concluir este primer acercamiento a las matemáticas de la criptografía, se puede establecer una nueva transformación, de nombre *cifrado afín*, que generaliza el cifrado de César. Dicha transformación se define como:

$$C_{(a,b)}(x) = (a \cdot x + b) \text{ (mód. } n)$$

siendo a y b dos números enteros menores que el número n de letras del alfabeto. El máximo común divisor entre a y n tiene que ser 1 [$\text{mcd}(a,n) = 1$], por que de lo contrario cabría la posibilidad de cifrar de forma diferente un mismo carácter, como se verá más adelante. La clave de cifrado viene determinada por el par (a, b). El cifrado César de clave 3 sería, pues, un cifrado afín de valores $a = 1$ y $b = 3$.

Los cifrados afines generales de la forma explicada ofrecen mayor seguridad que un código César convencional. ¿Por qué? Como ya se ha visto, la clave de un cifrado afín son los pares de números (a, b). Para el caso de un mensaje escrito en un alfabeto de 27 letras y encriptado mediante un cifrado afín, a y b pueden adoptar cualquier

MÁXIMO COMÚN DIVISOR (MCD)

El máximo común divisor de dos números se puede obtener, por ejemplo, con el algoritmo de Euclides. Este algoritmo consiste en dividir ambos números y realizar posteriormente divisiones sucesivas entre el cociente anterior y el nuevo resto. El proceso finaliza cuando algún resto es 0, siendo el divisor de la última división el máximo común divisor de ambos números. Por ejemplo,

mcd(48,30)?

Se divide 48 entre 30 y se obtiene de resto 18 y cociente 1.
Se divide 30 entre 18 y se obtiene de resto 12 y cociente 1.
Se divide 18 entre 12 y se obtiene de resto 6 y cociente 1.
Se divide 12 entre 6 y se obtiene de resto 0 y cociente 2. Hemos completado el algoritmo.

El mcd(48,30) es 6.

Si el mcd $(a,n)=1$ decimos que a y n son *primos* entre sí.
La igualdad de Bézout, de gran importancia en criptografía, establece que para dos enteros a y n mayores que 0, existen enteros k y q tales que $\text{mcd}(a,n)=ka+nq$.

valor comprendido entre 0 y 26. El número de claves posibles de este sistema de encriptación y para un alfabeto de 27 letras es, en consecuencia, $27 \times 27 = 729$. Como se observa, el número de claves para en un alfabeto de n letras es n veces mayor que el de un código César. El aumento es considerable, pero todavía susceptible de ser descifrado por fuerza bruta.

Jugando a espías

En el caso de los cifrados afines, ¿bajo qué condiciones es posible descifrar un mensaje, tanto si se es el receptor como si se es un espía? Profundizaremos en esta cuestión por medio de un ejemplo sencillo de cifrado para un alfabeto de seis letras como el siguiente.

0	1	2	3	4	5
A	B	C	D	E	F

Se encriptará el texto con un cifrado afín de expresión $C(x)=2x+1$ (mód. 6).

La A se cifra según $C(0)=2\times0+1\equiv1$ (mód. 6), que corresponde a B.
La B se cifra $C(1)=2\times1+1\equiv3$ (mód. 6), que corresponde a D.
La C se cifra $C(2)=2\times2+1\equiv5$ (mód. 6) que corresponde a F.
La D se cifra $C(3)=2\times3+1=7\equiv1$ (mód. 6) que corresponde a B.
La E se cifra $C(4)=2\times4+1=9\equiv3$ (mód. 6) que corresponde a D.
La F se cifra $C(5)=2\times5+1=11\equiv5$ (mód. 6) que corresponde a F.

Es decir, el cifrado afín propuesto encripta de igual manera los mensajes «ABC» y «DEF». Es imposible saber cuál es el mensaje original. ¿Qué ha ocurrido?

Si se trabaja como un cifrado de expresión $C_{(a,b)}(x)=(ax+b)$ (mód. n), se podrá descifrar el mensaje de forma unívoca si y sólo si $\text{mcd}(a,n)=1$. En el ejemplo, $\text{mcd}(2,6)=2$ y, por lo tanto, se incumple la restricción.

La operación matemática de descifrado equivale a hallar la incógnita x dado un valor numérico y en módulo n. Operando,

$$C_{(a,b)}(x)=(ax+b)=y \text{ (mód. } n)$$
$$(ax+b)=y \text{ (mód. } n)$$
$$ax=y-b \text{ (mód. } n).$$

Es decir, estamos buscando un valor a^{-1} (*inverso* de a) que cumpla $a^{-1}a=1$, de forma que

$$a^{-1}ax=a^{-1}(y-b) \text{ (mód. } n)$$
$$x=a^{-1}(y-b) \text{ (mód. } n).$$

En consecuencia, para tener éxito en el descifrado hay que calcular inversos de un número a en módulo n y, para no realizar esfuerzos inútiles, saber de antemano si realmente existen tales inversos. Un cifrado afín $C_{(a,b)}(x)=(ax+b)$ (mód. n), tendrá inverso si y sólo si $\text{mcd}(a,n)=1$.

En el caso del cifrado afín del ejemplo, $C(x)=2x+1$ (mód. 6), se desea saber si el número a, en nuestro caso 2, tiene inverso. Es decir, si hay algún entero n menor que 6 tal que $2\cdot n\equiv1$ (mód. 6). Para ello comprobamos todos los valores del módulo (0, 1, 2, 3, 4, 5):

$$2\cdot0=0,\ 2\cdot1=2,\ 2\cdot2=4,\ 2\cdot3=6\equiv0,\ 2\cdot4=8\equiv2,\ 2\cdot5=10\equiv4.$$

No existe tal valor, por lo que se concluye que 2 no tiene inverso. En realidad ya se sabía dado que $\text{mcd}(2,6)\neq1$.

Supondremos ahora que se ha interceptado el mensaje «YSFMG», que se sabe que ha sido encriptado con un cifrado afín de la forma $C(x) = 2x + 3$ y escrito sobre un alfabeto tradicional de 27 caracteres. ¿Cuál será el mensaje original? En primer lugar, calculamos el mcd(2,27), que es igual a 1. ¡El mensaje original puede descifrarse! Para ello se debe encontrar la función inversa de $C(x) = 2x + 3$ en módulo 27. Operando,

$$y = 2x + 3$$
$$2x = y - 3.$$

Para poder aislar la x es preciso multiplicar ambos lados de la expresión por el inverso de 2. El inverso de 2 en módulo 27 es un entero n tal que $2 \cdot n \equiv 1$ (mód. 27), es decir, 14, como se comprueba:

$$14 \cdot 2 = 28 \equiv 1.$$

En consecuencia,

$$x = 14(y - 3).$$

Ahora ya podemos descifrar el mensaje.

La letra Y ocupa la posición 25 y descifrada será $14(25 - 3) = 308 \equiv 11$ (mód. 27).
La letra que ocupa la posición 11 en el alfabeto es la L.
Para el caso de la letra S, $14(19 - 3) = 224 \equiv 8$ (mód. 27), que corresponde a la letra I.
Para el caso de F, $14(5 - 3) = 28 \equiv 1$ (mód. 27), que corresponde a B.
Para el caso de M, $14(12 - 3) = 126 \equiv 18$ (mód. 27), que corresponde a R.
Para el caso de G, $14(6 - 3) = 42 \equiv 15$ (mód. 27), que corresponde a O.

El mensaje descifrado es la palabra «LIBRO».

Más allá del cifrado afín

En la idea de César y su generalización en forma del cifrado afín, se basaron, durante muchos siglos, diversos sistemas de seguridad. Hoy en día se denomina código César a cualquier cifrado en el cual cada letra del mensaje original se sustituye por otra desplazada un número fijo de posiciones; no necesariamente tres.

Ahora bien, de entre las virtudes de un buen algoritmo de encriptación, una de las más importantes es que a partir de él se pueda generar una gran cantidad

de claves. Tanto el cifrado César convencional como el código afín (éste en menor medida) son vulnerables al criptoanálisis a causa del relativamente reducido número de claves que admiten.

Si eliminamos cualquier restricción relativa al orden de los caracteres del alfabeto cifrado, sin embargo, el número potencial de claves se dispara. Se observa que en total se tendría (usando la eñe): 27! = 10.888.869.450.418.352.160.768.000.000 alfabetos cifrados posibles, es decir, 10.888 cuatrillones de claves. Si no se emplea la eñe se tienen 26! = 403.291.461.126.605.635.584.000.000, es decir, 403 cuatrillones de claves. Un espía que comprobara una clave posible por segundo tardaría más de un billón de veces la vida esperada del universo en agotar todas las posibilidades.

Una clave posible de un algoritmo general de sustitución así definido podría ser la siguiente.

(1)	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
(2)	Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Ñ	Z	X	C	V	B	N	M

(1) Alfabeto llano. (2) Alfabeto cifrado.

Las seis primeras letras del alfabeto cifrado dan una pista sobre la ordenación elegida: se corresponde con el orden de las letras en un teclado convencional que sigue el estándar llamado QWERTY. Para cifrar el mensaje «VENI VIDI VINCI» con la clave QWERTY, se busca para cada letra del alfabeto convencional la que le corresponda en el alfabeto cifrado.

(1)	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
(2)	Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Ñ	Z	X	C	V	B	N	M

Se obtendría de este modo el siguiente mensaje cifrado:

CTFO CORO COFEO

Existe una forma muy sencilla de generar un número casi inagotable de claves fáciles de recordar para este método de cifrado. Basta con acordar una *palabra clave* cualquiera (puede ser también una frase) y situarla al principio del alfabeto cifrado, dejando que el resto del mismo siga la ordenación convencional a partir de la última letra de la palabra clave, con cuidado de no repetir ningún caracter. Un ejemplo sería «CIFRA ENERO». En primer lugar se eliminaría el espacio y los caracteres

repetidos, obteniendo así la palabra clave «CIFRAENO». El alfabeto cifrado resultante sería el siguiente.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	**I**	**F**	**R**	**A**	**E**	**N**	**O**	P	Q	S	T	U	V	W	X	Y	Z	B	D	F	G	H	J	K	L	M

El mensaje «VENI VIDI VINCI» quedaría ahora cifrado como «HAVP HPRP HPVFP». Este sistema de generación de claves puede organizarse de manera que el error de emisor y receptor sea improbable y su actualización muy sencilla. En el ejemplo que se ha visto, bastaría con cambiar la clave cada mes –de «CIFRA ENERO» a «CIFRA FEBRERO» y de ésta a «CIFRA MARZO», etc.– sin que los comunicantes debieran siquiera hablar más que en el momento de establecer la clave.

La fiabilidad y sencillez del algoritmo de sustitución por palabras clave hizo que fuera el sistema de encriptación preferido durante siglos. A lo largo de todo este tiempo, el consenso generalizado era que los criptógrafos habían ganado definitivamente la partida a los criptoanalistas.

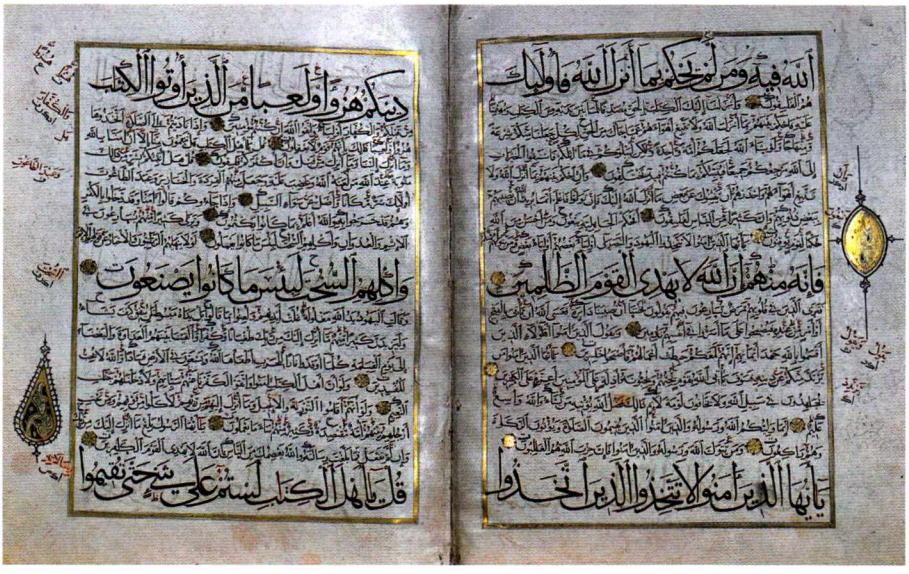
CIFRANDO LA PALABRA DE DIOS

Los criptoanalistas medievales creyeron ver cifras en el Antiguo Testamento, y no se equivocaron: en efecto, hay fragmentos del texto sagrado encriptados con un cifrado de sustitución llamado *atbash*. Este cifrado consiste en sustituir una letra cualquiera *n* por aquella que está a igual distancia del final del alfabeto de lo que *n* está del principio. Por ejemplo, y en un alfabeto convencional, la A se sustituiría por la Z, la B por la Y, etc. En el caso del Viejo Testamento original, las sustituciones se llevan a cabo, obviamente, con los caracteres del alfabeto hebreo. Así, en Jeremías (25, 26) la palabra «Babel» se cifra como «Seshach».

Biblia hebrea de inicios del siglo XVIII.

El análisis de frecuencias

El Corán se compone de 114 capítulos, cada uno de los cuales se corresponde con una de las revelaciones de Mahoma. Estas revelaciones fueron recogidas en vida del profeta por diversos escribas, y con posterioridad fueron reunidas por Abu Bakr, el primer califa. Umar y Uthman, el segundo y tercer califa respectivamente, completaron la labor. La naturaleza fragmentaria de los escritos originales estimuló el nacimiento de una rama de la teología dedicada a la datación exacta de las distintas revelaciones, para lo cual los estudiosos del Corán se sirvieron, entre otras técnicas, del estudio de la frecuencia de aparición de determinadas palabras consideradas de nuevo cuño. Si una revelación contenía un número suficiente de ellas, cabía suponer que era comparativamente tardía.



Corán manuscrito del siglo XIV.

Ésta y otras iniciativas relacionadas con el estudio detallado de los textos sagrados fueron el germen de la primera herramienta específica de criptoanálisis inventada por el hombre: el análisis de frecuencias. El primero en dejar constancia escrita de esta técnica revolucionaria fue un sabio nacido en Bagdad en el año 801, de nombre al-Kindi. Astrónomo, médico, matemático y lingüista, el oficio que no obstante le reportaría fama inmortal fue el de criptoanalista; si no el primero, sí el más importante de la historia.

Del papel pionero de al-Kindi se supo hace relativamente poco. En 1987 emergió en un archivo de Estambul una copia de un tratado suyo titulado *Sobre el descifra-miento de mensajes criptográficos*, del que se pudieron extraer fragmentos tan jugosos como el siguiente:

> «Una manera de resolver un mensaje cifrado, si sabemos en qué lengua está escrito, es encontrar un texto llano escrito en la misma lengua, suficientemente largo, y luego contar cuantas veces aparece cada letra. A la letra que aparece con más frecuencia la llamamos "primera", a la siguiente en frecuencia la llamaremos "segunda"... y así hasta que hayamos cubierto todas las letras que aparecen en nuestro texto. Luego observamos el texto cifrado que queremos resolver y clasi-ficamos sus símbolos de la misma manera. Encontramos el símbolo que aparece con mayor frecuencia y lo sustituimos por la "primera" de la de nuestro texto, hacemos lo mismo con la "segunda" y así sucesivamente, hasta que hayamos cubierto todos los símbolos del criptograma que queremos resolver.»

En páginas anteriores se afirma que en el método de cifrado por sustitución una letra del mensaje original «mantiene su posición pero cambia su rol», y es precisamente esta constancia en «mantener la posición» la que lo hace susceptible al criptoanálisis por frecuencias. El genio de al-Kindi invirtió el equilibrio de poder entre criptógrafos y criptoanalistas, decantándolo, al menos por el momento, del lado de estos últimos.

Un ejemplo en detalle

Las letras que más aparecen en textos en español por orden de más a menos frecuente son: E A O L S N D R U I T C P M Y Q B H G F V W J Z X K. Podemos observar los porcentajes de aparición de cada una en la siguiente tabla de frecuencias.

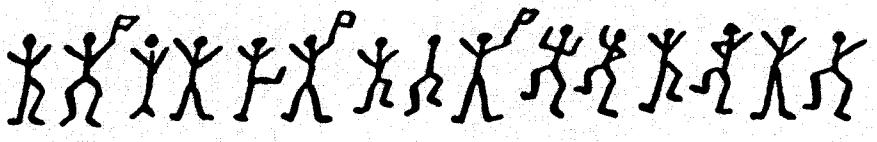
A 11,96%	H 0,89%	Ñ 0,29%	U 4,80%
B 0,92%	I 4,15%	O 8,69%	V 0,39%
C 2,92%	J 0,30%	P 2,77%	W 0,01%
D 6,87%	K 0,01%	Q 1,53%	X 0,06%
E 16,78%	L 8,37%	R 4,94%	Y 1,54%
F 0,52%	M 2,12%	S 7,88%	Z 0,15%
G 0,73%	N 7,01%	T 3,31%	

Si un mensaje ha sido cifrado por un algoritmo de sustitución como los examinados con anterioridad, es susceptible de ser descifrado en función de la frecuencia relativa de los caracteres del mensaje original. Basta con contar las apariciones de cada uno de los caracteres cifrados y compararlas con la tabla de frecuencia del idioma en que fue escrito. Así, si el carácter que aparece más a menudo en el texto cifrado es, por ejemplo, la J, la letra del mensaje original a la que más probablemente corresponda será, para el caso del castellano, la E. Si el segundo carácter más frecuente es la Z, por razonamiento análogo se concluye que la correspondencia más probable es la A. El proceso se repite para todos los caracteres del mensaje cifrado y se completa así el criptoanálisis.

Es obvio que el método de frecuencias no siempre podrá aplicarse de modo tan directo. Las frecuencias de la tabla anterior son exactas para la totalidad del idioma castellano. Textos breves como por ejemplo «*En Virginia, Vermont y Vancouver es vívido y vivificador el verde de la uva*» presentan frecuencias relativas de letras muy diferentes

SHERLOCK HOLMES, CRIPTOANALISTA

El descifrado por análisis de frecuencias es un método muy efectivo y espectacular que ha atraído la atención de numerosos literatos. Tal vez, la más célebre narración estructurada alrededor del criptoanálisis de un mensaje sea *El escarabajo de oro*, escrito en 1843 por el norteamericano Edgar Allan Poe. Impecable en su uso del análisis de frecuencias, los anexos del presente volumen recogen en detalle el mensaje ficcional planteado por Poe y su resolución. Otros narradores como Julio Verne o Arthur Conan Doyle emplearon también recursos similares para añadir suspense a sus argumentos. En *La aventura de los bailarines*, Conan Doyle enfrentó a su inmortal creación, Sherlock Holmes, a un cifrado por sustitución cuya resolución obligó al detective a acudir al análisis de frecuencias. Más de 1.000 años después, la idea de al-Kindi seguía sorprendiendo al público por su ingenio y eficacia.



El primero de los mensajes en clave que Sherlock Holmes debe descifrar en La aventura de los bailarines, *y cuya traducción no ofrecemos aquí por no revelar al lector desprevenido la solución del caso. Baste decir que los banderines que enarbolan algunas de las peculiares figuras constituyen un elemento importante de la clave.*

de las que caracterizan al idioma en su globalidad. De hecho, para textos de una extensión menor a los 100 caracteres, este análisis sencillo raramente es útil.

El análisis de frecuencias, sin embargo, no tiene por qué detenerse sólo en el estudio de las letras tomadas independientemente. Aún aceptando que es improbable que el carácter más frecuente en un texto cifrado corto sea la E, sí podemos afirmar con mayor seguridad que los cinco más frecuentes probablemente sean, sin saber con seguridad cuál corresponde a cuál, la A, la E, la L, la S o la O. De estas cinco letras, la única que se repite seguida en castellano es la L. Por tanto, si encontramos un carácter de entre los cinco más frecuentes que, además, aparece dos veces seguidas en alguna ocasión, podemos concluir tentativamente que se trata de una L en el original. Asimismo, es también probable que, por corto que sea el texto, las vocales tiendan a aparecer delante y detrás de un número mayor de otros caracteres que las consonantes, que suelen agruparse con otras vocales o con un número pequeño de caracteres. De este modo, tal vez se puedan identificar la A, la E y la O. A medida que se van descifrando con éxito algunos caracteres, aparecerán palabras donde sólo falte por descifrar una o dos letras y que nos permitirán establecer hipótesis sobre la naturaleza de estas últimas; la rapidez del descifrado, en consecuencia, aumenta más que proporcionalmente a medida que se descifran caracteres.

La aplicación de estas y otras particularidades en la frecuencia de aparición de letras o grupos de letras del idioma original puede resultar en un descifrado exitoso aún partiendo de un texto relativamente corto.

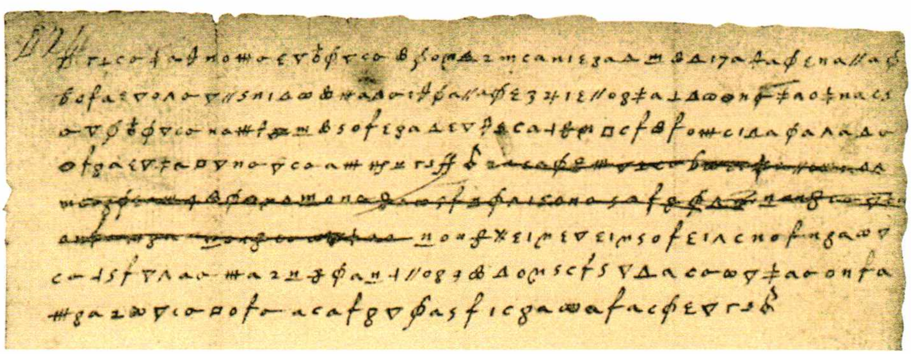
El cifrado polialfabético

El 8 de febrero de 1587 era decapitada en Londres María, reina de Escocia, tras ser declarada culpable de alta traición. El juicio que antecedió tan dramática acción había demostrado más allá de toda duda la connivencia de María con una banda de aristócratas católicos, encabezados por el joven Anthony Babington, que planeaba asesinar a la reina Isabel de Inglaterra para situar a María al frente de un reino católico de ingleses y escoceses. Las pruebas clave presentadas por el servicio de contraespionaje de la reina Isabel, liderado por el astuto Lord Walsingham, eran una serie de cartas de María dirigidas a Babington, de las cuales se desprendía que la joven reina escocesa conocía el plan y lo aprobaba. Las cartas en cuestión estaban cifradas con un algoritmo que combinaba cifrado y codificación, es decir, que no sólo intercambiaba letras por otros caracteres sino que también empleaba símbolos

únicos para referirse a ciertas palabras de uso común. El alfabeto cifrado de María se muestra a continuación.

a b c d e f g h i k l m n o p q r s t u x y z

Excepto por el hecho de emplear símbolos en lugar de letras, el alfabeto cifrado de María no era diferente de cualquiera de los empleados desde hacía siglos por los criptógrafos de todo el mundo. La joven reina y los conspiradores estaban convencidos de que la cifra era segura, pero, para su desgracia, el mejor criptoanalista de Isabel, Thomas Phelippes, conocía el método de análisis de frecuencias y pudo descifrar las cartas de María sin excesivos problemas. La resolución de lo que se conoció como «la conspiración Babington» no pudo sino lanzar una poderosa señal a los gobiernos y agentes de toda Europa: el algoritmo de sustitución convencional ya no era seguro. Los criptógrafos parecían impotentes ante el poder de las nuevas herramientas de descifrado.



Fragmento de una de las cartas de María de Escocia al conspirador Anthony Babington que la condenarían a muerte.

La aportación de Alberti

Lo cierto es que la solución al problema planteado por el análisis de frecuencias había sido dada hacía ya más de un siglo. El artífice del nuevo cifrado no era otro que el polifacético genio renacentista Leon Battista Alberti. Más conocido en su faceta de arquitecto, matemático y teórico de la perspectiva, Alberti había ideado

alrededor de 1460 un sistema de encriptación que consistía en añadir al alfabeto cifrado convencional un segundo, tal como se muestra en la tabla siguiente.

(1)	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
(2)	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
(3)	M	N	B	V	C	X	Z	Ñ	T	K	J	H	G	F	D	S	A	P	O	I	U	Y	L	R	E	W	Q

(1) Alfabeto llano. (2) Alfabeto cifrado 1. (3) Alfabeto cifrado 2.

Para encriptar un mensaje cualquiera, Alberti proponía alternar uno y otro alfabetos cifrados. Por ejemplo, para el caso de la palabra «MARCA», la cifra de la primera letra se buscaría en el primer alfabeto (O), la de la segunda en el segundo (M), y así sucesivamente. En nuestro ejemplo, «MARCA» quedaría cifrada como «OMUBD». La ventaja de este algoritmo de encriptación *polialfabético*, en comparación con los anteriores, es evidente a un primer vistazo: un mismo carácter del texto llano, A, queda cifrado de dos maneras distintas, M y D. Para mayor confusión de cualquier criptoanalista que se enfrentara al texto encriptado, un mismo carácter cifrado podría representar en realidad dos caracteres distintos del texto llano. El análisis de frecuencias perdía así buena parte de su utilidad. El desarrollo de la idea de Alberti no le correspondió al insigne italiano, que no dejó nunca escrito un tratado sobre la materia, sino a otros dos académicos contemporáneos aunque algo posteriores, el alemán Johannes Trithemius y el francés Blaise de Vigenère.

El cuadrado de De Vigenère

En un código César se emplea un cifrado monoalfabético: al alfabeto llano le corresponde un solo alfabeto cifrado, de modo que a cada letra le corresponde siempre el mismo carácter cifrado (en el César clásico, a la A siempre le correspondía la D, a la B la E, y así sucesivamente).

En el cifrado polialfabético, en cambio, a una letra determinada de un mensaje le pueden corresponder tantas asignaciones como alfabetos cifrados se quieran emplear. Para encriptar el texto se cambia de uno a otro alfabeto cifrado según se pasa de una letra del alfabeto llano a otra. El primer y más célebre sistema de cifrado polialfabético es el conocido como «cuadrado de De Vigenère». Esta plantilla de cifrado se componía de un alfabeto llano de *n* caracteres bajo el cual se distribuían *n* alfabetos cifrados, cada uno de ellos desplazados una letra a la izquierda. En otras

palabras, una matriz cuadrada de 26 filas y 26 columnas dispuestas tal como se muestra a continuación.

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
2	B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
3	C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
4	D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
5	E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
6	F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
7	G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
8	H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
9	I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
10	J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
11	K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
12	L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
13	M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
14	N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
15	O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
16	P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
17	Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
18	R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
19	S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
20	T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
21	U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
22	V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
23	W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
24	X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
25	Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
26	Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Nótese la simetría en la correspondencia de letras, es decir, el par (A, R) = (R, A), cumpliéndose esta relación para todas las letras.

Como se observa de inmediato, el cuadrado de De Vigenère consiste en un alfabeto llano de *n* caracteres a cada uno de los cuales se le aplica una transformación afín de parámetros crecientes. Así, el primer alfabeto cifrado serviría para aplicar un cifrado César de parámetros a = 1 y b = 2; el segundo equivaldría a cifrado César con b = 3, etc. La clave del cuadrado de De Vigenère consiste en saber qué letras del mensaje se cifran y cuántas filas nos desplazamos hacia abajo para buscar el carácter cifrado correspondiente. La clave más sencilla consiste en desplazarnos una fila hacia

JUGANDO CON DISCOS

Un modo práctico de implementar un cifrado polialfabético es el uso a tal efecto de artilugios conocidos como «discos de Alberti». Estos cifradores portátiles consisten de un armazón fijo en el que está grabado un alfabeto convencional, y unido a él una pieza circular concéntrica y móvil con otro alfabeto grabado. El emisor puede, mediante el giro del anillo móvil, emparejar el alfabeto llano con tantos alfabetos cifrados como giros distintos del anillo dé, hasta un máximo igual a los caracteres del alfabeto empleado. El cifrado obtenido por un disco de Alberti es muy resistente al análisis de frecuencias. Para poder desencriptar el mensaje el receptor sólo necesita realizar los mismos giros que el emisor. La seguridad de este cifrado, como del resto, depende de mantener secretas las claves, esto es, el orden del alfabeto del anillo móvil más los giros realizados.

Un disco de Alberti con un sólo anillo móvil grabado con un alfabeto ordenado de manera tradicional permite un cifrado César por giro. Artilugios similares se emplearon en conflictos tan recientes como la guerra de Secesión norteamericana, y aún hoy suelen incluirse en juegos de espías para niños.

Disco de Alberti empleado por los confederados en la guerra civil norteamericana.

abajo para cada letra del mensaje original. Así, la frase «VENIVIDIVINCI» se cifraría del siguiente modo:

Para cifrar la primera V buscamos su correspondencia en la fila 2: la W.
Para cifrar la E buscamos su correspondencia en la fila 3: la G.
Para cifrar la N buscamos su correspondencia en la fila 4: la Q.
I (fila 5) : M
V (fila 6): A
I (fila 7): O
D (fila 8): K
I (fila 9): Q
V (fila 10): E
I (fila 11): S
N (fila 12): Y
C (fila 13): O
I (fila 14): V

DIPLOMÁTICO Y CRIPTÓGRAFO

Blaise de Vigenère nació en Francia en 1523. En 1549 fue enviado por el gobierno francés en misión diplomática a Roma, donde se interesó por la criptografía y los mensajes cifrados. En 1585 escribió su obra fundamental, el *Traicté des Chiffres* («Tratado de las cifras»), que, entre otros, describe el sistema de encriptación al que dio su nombre. Este sistema de cifrado fue inexpugnable durante casi dos siglos, hasta que el británico Charles Babbage logró descifrarlo hacia 1854. Curiosamente, este hecho no se supo hasta avanzado el siglo XX, cuando un grupo de estudiosos revisaron las notas y apuntes personales de este último.

La frase original encriptada quedaría «WGQM AOKQ ESYOV». Como puede comprobarse fácilmente, la frecuencia de las letras del mensaje original se desvanece. Sin embargo, el interés de todo criptógrafo reside en generar claves fáciles de recordar, distribuir y actualizar. En el caso del cuadrado de De Vigenère ello derivó en cifras más cortas en la forma de palabras clave de un número de letras inferior o igual al mensaje que se desea cifrar. La palabra clave se emplea según la mecánica siguiente: se escribe la palabra debajo del texto llano, repitiéndose tantas veces como sea necesario, se toma la intersección entre la fila y columna correspondiente a modo de plano cartesiano y se obtiene así el mensaje cifrado. La fila correspondiente en este caso sería la que empieza por la letra del carácter de la palabra clave pertinente.

Por ejemplo, se desea cifrar el mensaje «ATACAD EL LUNES» mediante la palabra clave «FEBRERO»:

Mensaje original	A	T	A	C	A	D	E	L	L	U	N	E	S
Clave	F	E	B	R	E	R	O	F	E	B	R	E	R
Mensaje cifrado	F	X	B	T	E	U	S	Q	P	V	E	I	J

El mensaje cifrado queda como «FXBTEU SQ PVEIJ».

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n

Un cuadrado de De Vigenère con las filas definidas por la palabra clave «FEBRERO».

Como en el caso de todos los sistemas de encriptación clásicos, el descifrado de un mensaje encriptado con un cuadrado de De Vigenère es simétrico con respecto al cifrado. Por ejemplo, y para el caso del mensaje cifrado «SZBFIEMOPS» con la palabra clave «SILLA»:

Mensaje original	?	?	?	?	?	?	?	?	?	?
Clave	S	I	L	L	A	S	I	L	L	A
Mensaje cifrado	S	Z	B	F	I	E	M	O	P	S

Considérese ahora la primera fila. Se busca una incógnita «?» que verifique (?,S) = S. Para ello, buscamos en el cuadrado la fila de la S hasta donde aparezca la S y vemos a qué columna corresponde; la respuesta es A. Después, buscamos una letra «?» que verifique (?,I) = Z y obtenemos la R, y así sucesivamente, El mensaje original se revela como «ARQUIMEDES».

La importancia histórica del cuadrado de De Vigenère, que comparte en general con otros cifrados polialfabéticos como el de Gronsfeld (desarrollado en épocas similares y expuesto en detalle en los anexos de este libro), es su resistencia al análisis de frecuencias. En efecto, si un mismo carácter podía ser cifrado de más de una forma, sin por ello imposibilitar su descifrado posterior, ¿cómo podía llevarse a cabo un criptoanálisis efectivo? La pregunta quedaría sin respuesta durante más de 300 años.

Clasificar alfabetos

Aunque fuera con un retraso de cerca de ocho siglos, los cifrados polialfabéticos del estilo del cuadrado de De Vigenère habían logrado burlar por fin el análisis de

frecuencias. Curiosamente, el cifrado polialfabético aún tardaría años en establecerse definitivamente. Los sistemas monoalfabéticos tradicionales, a pesar de sus debilidades, tenían la ventaja de ser muy sencillos de implementar. Los criptógrafos se dedicaron, eso sí, a refinar los procedimientos y a cuajar sus algoritmos de trucos, pero en lo fundamental permanecieron fieles a las cifras conceptualmente más sencillas.

Una de las variantes más logradas del sistema monoalfabético fue la conocida como la cifra de sustitución *homofónica*, que buscaba contrarrestar el criptoanálisis estadístico por la vía de aumentar la ratio de sustitución de los caracteres de mayor frecuencia de aparición. Así, si la letra E representaba en promedio un 10% de un texto en un idioma cualquiera, la cifra por sustitución homofónica buscaba revertir la tendencia sustituyendo la E por 10 caracteres alternativos. Éste y otros métodos se mantuvieron como los preferidos hasta bien entrado el siglo XVIII.

LOS CRIPTÓGRAFOS DEL REY SOL

Aunque pocos fuera del entorno de Luis XIV sabían de su existencia, los hermanos Antoine y Bonaventure Rossignol eran dos de los hombres más temidos en la convulsa Europa del siglo XVII. Su capacidad para descifrar los mensajes de los enemigos de Francia (y de más de un enemigo personal del monarca) corría pareja a su inventiva como criptógrafos. A ellos se le debe la conocida como *La Grande Chiffre* («la gran cifra»), un complejo algoritmo de sustitución por sílabas empleado para encriptar los mensajes de mayor trascendencia emitidos por el rey. Con la muerte de ambos hermanos, empero, la cifra cayó en desuso hasta perderse su funcionamiento. No fue hasta 1890 cuando un experto criptógrafo, el militar retirado Étienne Bazeries, emprendió la ardua tarea de desencriptar los documentos cifrados y, tras años de arduo trabajo, se convirtió en receptor insospechado de los mensajes secretos del Rey Sol.

Luis XIV retratado por Mignard.

Esta resistencia a la innovación pronto se reveló como fútil. La emergencia de los grandes Estados-nación y de la diplomacia que los acompañaba estaba generando un drástico aumento de la demanda de comunicaciones seguras. Esta tendencia no hizo sino reforzarse con la aparición de nuevas tecnologías de comunicación, tales como el telégrafo, que elevaron el volumen de tráfico de mensajes hasta extremos inauditos. Las grandes naciones europeas se dotaron de las denominadas «habitaciones negras», centros neurálgicos de actividad de las que partían las comunicaciones más delicadas y adonde iban a parar los mensajes interceptados del enemigo. El trabajo experto de las habitaciones negras pronto hizo insegura cualquier forma de sustitución monoalfabética, por muy alterada que fuera. Poco a poco, los grandes agentes en el juego del intercambio de información fueron optando por los algoritmos polialfabéticos. Sustraída su arma más potente, el análisis de frecuencias, los criptoanalistas habían quedado inermes ante el embate de los criptógrafos.

El criptoanalista anónimo

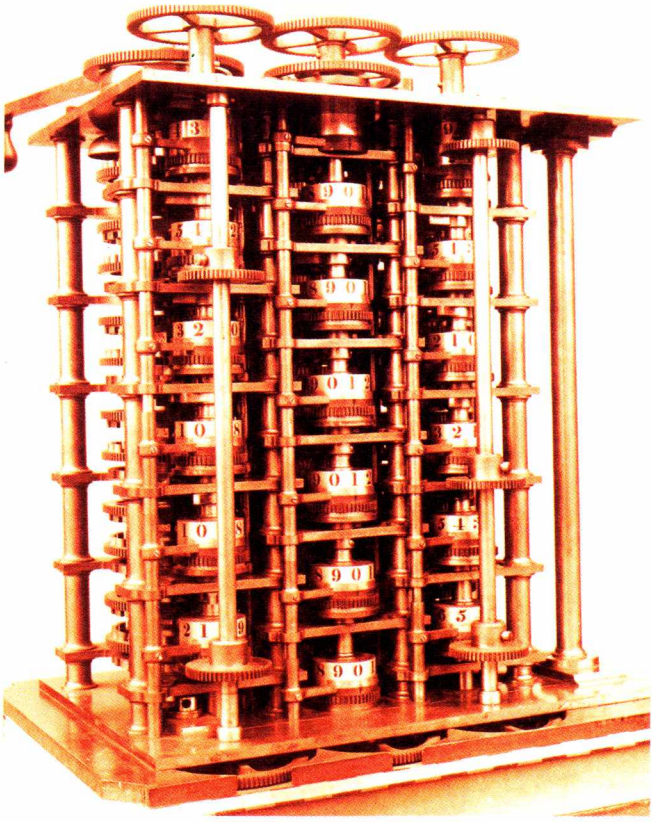
El británico Charles Babbage (1791-1871) fue una de las figuras científicas más extraordinarias del siglo XIX. Inventor de un prototipo de ordenador revolucionario para su tiempo, la conocida como «máquina diferencial», sus intereses se repartieron a lo largo y ancho de la matemática y la tecnología de su época. A raíz de un intercambio epistolar con un amigo, Babbage decidió aplicar su genio al descifrado de los algoritmos polialfabéticos, con el cuadrado de De Vigenère como objetivo primordial. Para ello, centró su escrutadora mirada en una característica de dicho cifrado. Recordemos que, para el caso de la cifra de De Vigenère, la longitud de la palabra clave escogida determinaba la cantidad de alfabetos cifrados empleados. Así, si la palabra clave fuera «MURO», cada carácter del mensaje original podía quedar cifrado hasta de 4 maneras distintas. Otro tanto ocurría con las palabras. Esta característica iba a ser la grieta en la que Babbage se apoyaría para escalar el muro del cifrado polialfabético. Veamos el siguiente ejemplo de mensaje cifrado con el cuadrado de De Vigenère.

Mensaje original	L	A	V	E	R	D	E	Y	L	A	R	O	J	A
Clave	M	U	R	O	M	U	R	O	M	U	R	O	M	U
Mensaje cifrado	X	U	P	S	D	X	V	M	X	U	I	C	V	U

De inmediato llama la atención que la partícula «LA» del mensaje original se cifra con los mismos caracteres en ambos casos, XU. Ello se debe a que la sepa-

ración entre ambas partículas en el mensaje original (ocho) es un múltiplo del número de caracteres de la clave empleada (cuatro). Con esta información, y dado un texto original lo bastante largo, es posible adivinar la longitud de la palabra clave. El procedimiento es el siguiente: se listan todos los caracteres repetidos y el espacio que queda entre ellos, y se buscan divisores enteros de los caracteres de los espacios. Los divisores comunes son los números candidatos a representar la longitud de la clave.

Supondremos que el candidato más probable, por ser el divisor común que más veces aparece, es el 5. Queda ahora adivinar a qué caracteres corresponde cada una de las cinco letras de la clave. Si recordamos el proceso de encriptación, cada letra de la clave del cuadrado de De Vigenère determina un cifrado monoalfabético del carácter correspondiente del mensaje original. Para el caso de nuestra clave hipotética de cinco caracteres (C1, C2, C3, C4, C5), el sexto carácter (C6) se cifra con el mismo alfabeto con el que se ha encriptado el primero (C1), el séptimo



La máquina diferencial de Babbage, construida en 1991 según los planos de su creador. El aparato permite aproximar funciones logarítmicas y trigonométricas y, por tanto, operar con tablas astronómicas. Babbage no la vio construida en vida.

(C7) con el empleado para cifrar el segundo (C2), etcétera. Por tanto, a lo que se enfrenta el criptoanalista en realidad es a cinco cifrados monoalfabéticos, todos ellos susceptibles de criptoanálisis.

El proceso se completa diseñando ahora sendas tablas de frecuencias para todos los caracteres del texto cifrados con el mismo carácter de la palabra clave (C1, C6, C11... y C2, C7, C12... hasta completar los cinco grupos de caracteres con el límite de la longitud del mensaje), y comparando dichas tablas con las propias del idioma del mensaje. Si la coincidencia no es clara, se descarta la longitud de la clave elegida y se toma la segunda más probable. La iteración de este proceso permite identificar al menos una palabra clave probable, y ya sólo resta descifrar el mensaje. La clave polialfabética había sido rota.

El asombroso ejercicio de Babbage, completado alrededor de 1854, iba a quedar no obstante en la oscuridad. En efecto, el excéntrico genio británico dejó sus hallazgos sin publicar, y sólo recientes revisiones de sus notas han permitido identificarle como el pionero en descifrar la clave polialfabética. Por suerte para los criptoanalistas del mundo entero, pocos años después, en 1863, el oficial prusiano Friedrich Krasiski hizo público un método similar.

Con independencia de quién fue el primero en lograrlo, la evidencia es que el cifrado polialfabético había dejado de ser impenetrable. A partir de ese momento, la fortaleza de una cifra iba a depender no tanto de grandes innovaciones en los algoritmos de encriptación, sino en el número de alfabetos cifrados posibles, el cual tenía que ser tan grande como para hacer totalmente impracticable el análisis de frecuencia y sus variantes. Al otro lado del flujo de información, el objetivo era hacerse con mecanismos que permitieran agilizar el criptoanálisis. Ambas búsquedas convergían hacia un mismo punto y dieron luz a un mismo proceso: la mecanización.

Capítulo 3

Máquinas que codifican

El siglo XIX iba a ampliar la utilidad de los códigos mucho más allá de la criptografía. La invención del telégrafo en el primer tercio de la centuria y, treinta años después, el desarrollo del telégrafo doble por parte de Thomas Alva Edison, revolucionó las comunicaciones y, por ende, el mundo. Comoquiera que el telégrafo funcionaba por impulsos eléctricos, hubo de implementarse un sistema que tradujera el contenido de los mensajes a un lenguaje que la máquina pudiera «entender»; es decir, se tuvo que establecer un código. De entre los diversos candidatos se impuso un sistema de rayas y puntos ideado por el pintor y físico estadounidense Samuel F. B. Morse. El código Morse puede considerarse un antecesor de los códigos que, décadas más tarde, permitirían a los usuarios introducir y extraer información de los computadores.

El código Morse

El código Morse representa las letras del alfabeto, los números y otros signos mediante una combinación de puntos, rayas y espacios. De este modo traduce varios alfabetos simbólicos a uno sólo, susceptible de ser escrito mediante señales luminosas, sonoras o eléctricas sencillas. Cada punto representa una unidad de tiempo de duración aproximada de 1/25 segundos, y cada raya, 3 unidades. Los espacios entre las letras son de 3 puntos, y entre las palabras, de 5.

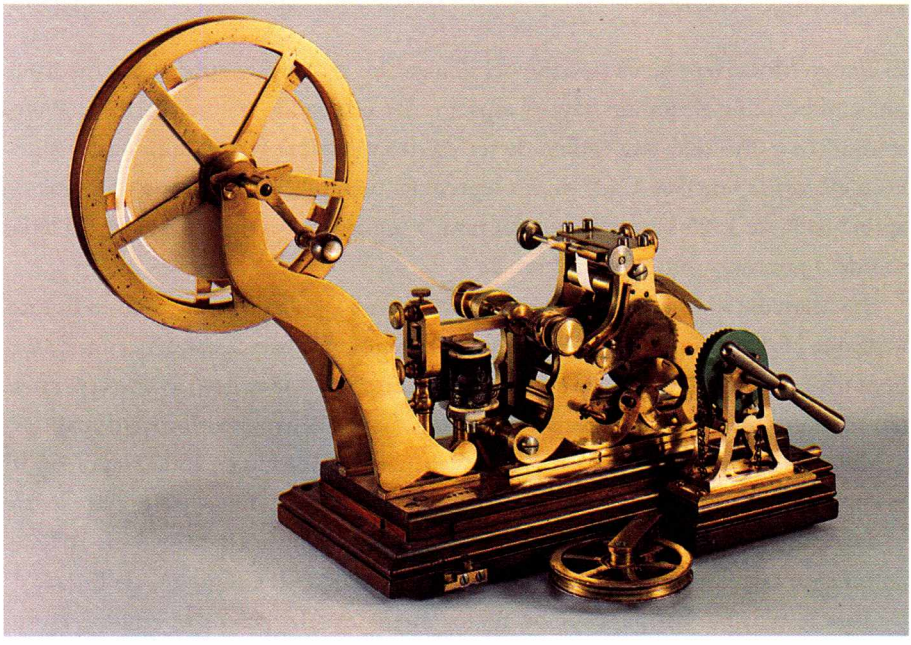
Inicialmente a Morse se le negó la patente tanto en Estados Unidos como en Europa, hasta que en 1843 consiguió financiación gubernamental para la construcción de una línea telegráfica entre Washington D.C. y Baltimore. En 1844 se llevó a cabo la primera transmisión y poco después se formó una compañía con el expreso objetivo de cubrir la totalidad de América del Norte con líneas telegráficas. Cuando en 1860 Napoleón III le concedió un justo premio de reconocimiento, Estados Unidos y Europa estaban ya entreverados de numerosos tendidos telegráficos. Al morir Morse en 1872, el continente americano estaba cruzado por más de 300.000 kilómetros de líneas.

Para la transmisión y recepción de los mensajes telegráficos se empleó en sus inicios un sencillo aparato inventado en 1844 por el propio Morse. Ese aparato

COMUNICACIÓN NO VERBAL

Debido a su sordera, Thomas Alva Edison (1847-1931) se comunicaba con su esposa Mary Stilwell por medio del código Morse. Durante el noviazgo de ambos, Edison le propuso matrimonio por medio de golpecitos en su mano, y ella le respondió de la misma manera. El código telegráfico se convirtió en un sistema de comunicación habitual en la pareja, hasta el extremo de que, cuando asistían a una obra de teatro, Edison apoyaba su mano sobre la rodilla de Mary para que ella pudiera «telegrafiarle» los diálogos de los actores.

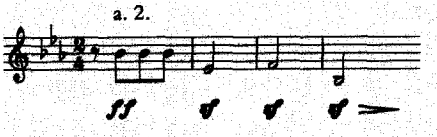
constaba de una llave telegráfica de transmisión, que hacía las veces de interruptor de la corriente eléctrica, y de un electroimán que recibía las señales. Cada vez que la llave se oprimía hacia abajo –por lo general, con los dedos índice y medio– se establecía un contacto eléctrico. Los impulsos intermitentes que se producían al oprimir la llave telegráfica se enviaban a un tendido eléctrico compuesto por dos alambres de cobre. Esos cables, soportados por postes de madera, unían las diferentes estaciones del telégrafo y a menudo se extendían cientos de kilómetros sin interrupción.



Primer telégrafo diseñado por Samuel F. B. Morse, en 1844.

SINFONÍA EN V MAYOR

Beethoven fue otro sordo célebre vinculado al telégrafo, aunque en su caso de un modo ciertamente indirecto. El caso es que los cuatro primeros acordes de la *Quinta Sinfonía* del genial compositor tienen una cadencia parecida a un mensaje en código Morse de «punto punto punto raya».



Esta sucesión de puntos y rayas se corresponde con la letra V, la inicial de la palabra inglesa *victory* («victoria»). Por ello, la emisora británica BBC la empleó como sintonía de apertura de sus emisiones a la Europa ocupada durante la Segunda Guerra Mundial.

El aparato receptor estaba formado por un electroimán con una bobina de alambre de cobre enrollada alrededor de un núcleo de hierro. Cuando la bobina recibía los impulsos de corriente eléctrica correspondientes a los puntos y las rayas, el núcleo de hierro se magnetizaba y atraía hacia sí una pieza móvil, también de hierro, que al golpear aquél emitía un sonido seco peculiar. Ese sonido era semejante a un *tac* corto cuado se recibía un punto, y uno más largo si se recibía una raya. Los telegramas tradicionales necesitaban un operador que pulsara la versión codificada del mensaje y, en el lado contrario, otro que la leyera.

La traducción de los caracteres convencionales a los propios del código Morse se hacía de acuerdo con la tabla siguiente.

SIGNO	CÓDIGO	SIGNO	CÓDIGO	SIGNO	CÓDIGO	SIGNO	CÓDIGO	SIGNO	CÓDIGO	SIGNO	CÓDIGO
A	·–	G	––·	N	–·	T	–	0	–––––	7	––···
B	–···	H	····	Ñ	––·––	U	··–	1	·––––	8	–––··
C	–·–·	I	··	O	–––	V	···–	2	··–––	9	––––·
CH	––––	J	·–––	P	·––·	W	·––	3	···––	.	·–·–·–
D	–··	K	–·–	Q	––·–	X	–··–	4	····–	,	––··––
E	·	L	·–··	R	·–·	Y	–·––	5	·····	?	··––··
F	··–·	M	––	S	···	Z	––··	6	–····	"	·–··–·

Así, el mensaje «Te quiero» se traduciría como:

T	e		q	u	i	e	r	o
–	·		– – · –	· · –	· ·	·	· – ·	– – –

Como ya se ha mencionado, el código Morse es, en cierto modo, una primera versión de los futuros sistemas de comunicaciones digitales. Para ejemplificar esta idea basta con asignar 1 al punto y 0 a la raya. La alternancia de ceros y unos resultará más familiar en los capítulos posteriores.

Ya entrado el siglo XX, la telegrafía tradicional fue sustituida por la comunicación inalámbrica impulsada por la invención de la radio; los telegrafistas de antaño pasaron a llamarse entonces radiotelegrafistas. Esta nueva tecnología permitió, además, la transmisión a grandes velocidades. Al viajar en forma de ondas electromagnéticas, los mensajes radiados eran relativamente fáciles de interceptar. Este hecho proporcionó a los criptoanalistas grandes dosis de material cifrado sobre el que trabajar y consolidó su posición de fuerza, dado que la mayoría de cifrados empleados por gobiernos y agentes privados, incluso los de naturaleza más delicada, se apoyaban en algoritmos ya conocidos. Es el caso, por ejemplo, de la cifra Playfair, ideada de forma conjunta por los británicos barón Lyon Playfair y Sir Charles Wheatstone; una ingeniosa variación del cifrado de Polibio, pero una variación al cabo (la cifra se expone en detalle en los anexos). A pesar de las considerables dosis de inventiva de sus creadores, la desencriptación de estas cifras «recicladas» era fundamentalmente una cuestión de tiempo y capacidad de cómputo. La historia criptográfica de la Primera Guerra Mundial ilustra a la perfección esta circunstancia. Ya se ha escrito acerca de la debilidad del cifrado diplomático alemán con ocasión del asunto del «telegrama Zimmermann». Lo que

SALVEN NUESTRAS ALMAS

La palabra más famosa del código Morse es la señal de auxilio SOS. Fue establecida con ese fin por una comisión de países europeos por la sencillez de su transmisión (tres puntos, tres rayas, tres puntos). La cultura popular le atribuyó, entre otros muchos, el significado *Save our souls*, literalmente «Salven nuestras almas». Más adelante, y dado su frecuente uso en navegación, se le supuso un significado alternativo, *Save Our Ship*, «Salven nuestro barco».

los propios alemanes no sospechaban es que otra de sus cifras de aquella época, conocida como ADFGVX y empleada para encriptar los más delicados mensajes destinados al frente, iba a ser también presa de los criptoanalistas enemigos a pesar de su supuesta invulnerabilidad. El doble fiasco alemán de la Primera Guerra Mundial hizo tomar conciencia a todas las partes de la necesidad de cifrar de forma todavía más segura, objetivo que se buscó, fundamentalmente, por la vía de dificultar el criptoanálisis.

La lucha entre unos y otros, criptógrafos y criptoanalistas, es la guerra oculta que subyace a los sangrientos conflictos mundiales de la primera mitad del siglo pasado.

A 80 kilómetros de París

En junio de 1918 las tropas alemanas se aprestaban a atacar la capital francesa. Para los aliados era fundamental interceptar sus comunicaciones y prever en qué lugares se producirían los envites. Los mensajes alemanes destinados al frente se encriptaban con una cifra conocida como ADFGVX, considerada irrompible.

El interés de esta cifra radica en que comparte algoritmos de sustitución y transposición. Se trata de uno de los métodos más sofisticados de la criptografía clásica. Introducido por los alemanes en marzo de 1918, nada más saber de su existencia los franceses se pusieron frenéticamente a intentar descifrarla. Por suerte para sus intereses, en la Oficina Central de Cifras trabajaba un talentoso criptoanalista de nombre George Painvin, que se dedicó a la tarea día y noche. La noche del 2 de junio del 1918, Painvin consiguió descifrar un primer mensaje. Su ominoso contenido era una orden dirigida al frente: «Envíen municiones rápidamente. Incluso durante el día si no os ven». En el preámbulo del mismo se indicaba que había sido enviado desde algún lugar situado entre Montdidier y Compiègne, a unos 80 kilómetros al norte de París. La hazaña de Painvin permitió a los franceses impedir el ataque, pudiendo de esta forma detener el avance alemán.

La cifra ADFGVX, como se ha mencionado, consta de dos partes: sustitución y transposición.

En una primera fase –la sustitución– se considera una cuadrícula dispuesta en siete filas y siete columnas, en la que la primera fila y la primera columna están formadas por los caracteres ADFGVX. A continuación, se rellena una tabla base de 36 elementos mediante una disposición aleatoria de 26 letras y los 10 prime-

ros dígitos. La disposición de los elementos constituye la clave del cifrado y el receptor, evidentemente, necesita de esta información para obtener el contenido del mensaje. Se supone la siguiente tabla base.

	A	D	F	G	V	X
A	O	P	F	0	Z	C
D	G	3	B	H	4	K
F	A	1	7	J	R	2
G	5	6	L	D	E	T
V	V	M	S	N	Q	I
X	U	W	9	X	Y	8

El cifrado consiste en traducir cada carácter del mensaje por un par de letras del conjunto ADFGVX en razón de su equivalencia «cartesiana». Así, se escribe en primer lugar la letra correspondiente a la fila y, en segundo lugar, la letra correspondiente a la columna. De esta manera, si se desea cifrar el número 4 se escribirá «DV». El mensaje «Objetivo París» se cifraría del modo siguiente.

O	b	j	e	t	i	v	o	P	a	r	í	s
AA	DF	FG	GV	GX	VX	VA	AA	AD	FA	FV	VX	VF

Hasta aquí se trata de una simple sustitución, y bastaría un análisis de frecuencias para descifrar el mensaje.

Sin embargo, la cifra contiene una segunda fase, esta vez por transposición. La transposición depende de una palabra clave acordada entre el emisor y el receptor. Esta segunda fase del cifrado se lleva a cabo del modo siguiente. En primer lugar, se construye una cuadrícula con tantas columnas como letras tenga la palabra clave, y se rellenan sus celdas con el texto cifrado. Las letras de la palabra clave se escriben en la fila superior de la nueva cuadrícula. Para el caso del ejemplo presente se empleará como clave la palabra BETA. Se construye una nueva tabla cuya primera fila consta de dicha palabra y las siguientes contienen los caracteres obtenidos al codificar el mensaje por sustitución. Las casillas vacías se completan con los caracteres del número cero, que como puede observarse en

la tabla inicial se simboliza como AG. A continuación se repasa todo el proceso para el mensaje «Objetivo París». Como se recordará, del cifrado por sustitución resultó:

AA	DF	FG	GV	GX	VX	VA	AA	AD	FA	FV	VX	VF

Adoptamos BETA como palabra clave y resulta una nueva tabla.

B	E	T	A
A	A	D	F
F	G	G	V
G	X	V	X
V	A	A	A
A	D	F	A
F	V	V	X
V	F	A	G

Proseguimos con el cifrado por transposición y se cambian las columnas de posición, de manera que las letras de la clave queden ordenadas por orden alfabético. Se obtiene así la siguiente tabla.

A	B	E	T
F	A	A	D
V	F	G	G
X	G	X	V
A	V	A	A
A	A	D	F
X	F	V	V
G	V	F	A

El mensaje cifrado es el resultante de tomar las letras de la cuadrícula por columnas. En el ejemplo, se obtiene:

FVXAAXGAFGVAFVAGXADVFDGVAFVA

Como puede verse, el mensaje consiste en una mezcla aparentemente aleatoria de los caracteres A, D, F, G, V y X. Como es lógico, se trata de un resultado buscado ex profeso y se deriva de la nomenclatura de las filas y columnas de la tabla base inicial.

Los alemanes escogieron estos seis caracteres porque su traducción respectiva al código Morse difería mucho, lo que permitía al receptor detectar más fácilmente hipotéticos errores de transmisión. Además, al constar únicamente de seis caracteres, su transmisión telegráfica era sencilla y por tanto, estaba al alcance de operarios noveles.

Si se consulta la tabla de código Morse del principio del capítulo se observa que la equivalencia de cada uno de los caracteres de la cifra ADFGVX es la siguiente.

A = · –
D = – · ·
F = · · – ·
G = – – ·
V = · · · –
X = – · · –

El receptor únicamente necesita la distribución aleatoria de caracteres de la tabla base y la palabra clave para revertir el encriptado y revelar el mensaje.

La máquina Enigma

En el año 1923 el ingeniero alemán Arthur Scherbius patentó una máquina diseñada para facilitar las comunicaciones seguras. Su nombre, Enigma, se ha convertido en sinónimo del secreto militar y evoca imágenes de laboratorios subterráneos y máquinas de enrevesada estructura. Con toda su sofisticación, Enigma es, en esencia, una versión mejorada del disco de Alberti, como tendremos ocasión de ver más adelante.

Por la relativa facilidad de su uso y la complejidad del cifrado resultante, Enigma fue la base escogida por el gobierno alemán para encriptar buena parte de su tráfico de comunicaciones militares durante la Segunda Guerra Mundial.

El descifrado de Enigma se convirtió por tanto en una prioridad absoluta de los gobiernos enfrentados a la Alemania nazi. Cuando al fin se logró el objetivo, los mensajes interceptados y descifrados por la inteligencia aliada resultaron decisivos a la hora de decidir la resolución final del conflicto. La historia del descifrado de Enigma es un relato fascinante en el que intervinieron sobre todo los departamentos de inteligencia de Polonia y Reino Unido, y tiene entre sus héroes a un matemático genial, Alan Turing, el hombre que es considerado el padre de la moderna computación. La aventura por romper el código Enigma dio como fruto, además, el primer ordenador de la historia, lo que puede considerarse como el episodio más espectacular de la larga y pintoresca historia del criptoanálisis militar.

Soldados alemanes transcribiendo mensajes cifrados mediante la máquina Enigma durante la Segunda Guerra Mundial. A la derecha, un modelo de cuatro rotores.

La máquina Enigma en sí era un artilugio electromecánico muy parecido a una máquina de escribir. Estaba constituido por un teclado y un tablero luminoso de 26 letras; tres *rotores* o *modificadores*, montados sobre sendos ejes, con 26 posiciones posibles, y un clavijero, instalado entre el teclado y el primer rotor, cuyo cometido era llevar a cabo un primer intercambio de letras en función del modo en que se dispusieran las clavijas.

El proceso físico de cifrado era relativamente sencillo. En primer lugar, el emisor disponía las clavijas y los rotores en una posición de salida especificada por el libro de claves que estuviera vigente en ese momento. A continuación, tecleaba la primera letra del mensaje llano y la máquina, de forma automática, generaba una letra alternativa que se mostraba en el tablero luminoso: la primera letra del mensaje cifrado.

EL CIFRADO «DE TRINCHERA»

En el frente, el uso de cifras tan complejas como la ADFGVX a menudo resultaba penoso. En la Guerra Civil española de 1936-1939, por ejemplo, abundaban algoritmos de sustitución elementales como el siguiente.

A	B	C	D	E	F	G	H	Y	J
53-91	12-70	40-86	31	27-43	24	16	11	40-59	22
L	M	N	O	P	Q	S	R	T	U
13	15	96-66	84-39	75	71	28-54	28-54	19	74-44

Como puede observarse, varias letras tienen más de una versión cifrada. La R, por ejemplo, se sustituye bien por 28, bien por 54. La palabra «GUERRA» se cifraría según la tabla como 167427285453. Estos códigos, principalmente por sustitución, se denominaban «de trinchera» y estaban orientados a usos muy puntuales.

COPIA DE LA CLAVE SECRETA EMPLEADA POR LA BRIGADA MIXTA nº104.

415 BATALLON

CLAVE VIOLETA

(1) A.B.C.D.E.F.G.H.I.J.K.L.M.N.O.P.Q.R.S.T.

(2) x.d.u.t.r.a.h.s.c.b.d.e.f.y.m.G.i.l.j.b.

(1) U.V.X.Y.Z.

(2) o.f.q.g.n.s.

Nota: Esta clave de régimen interior se crea para uso de los comandos de importancia entre las Compañías y el mando del Batallón.
Las cifras necesariamente deberán ser consignadas en letras.-Las columnas señaladas con el signo(1) corresponden al alfabeto.-Las columnas señaladas con el signo (2) corresponde en su equivalencia en clave.-

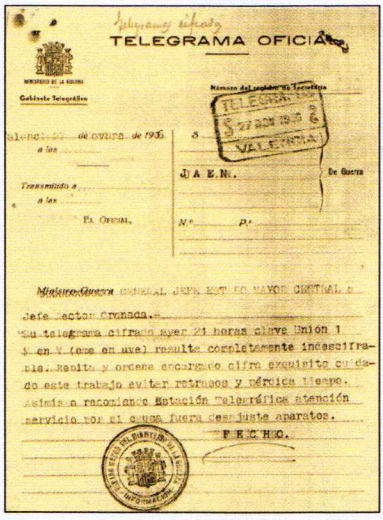
Hay un sello en tinta al costado derecho en forma de triangulo que dice.-Brigada Mixta 104.-Batallón 415.Dentro del triangulo.Mayoría.-

Clave Violeta usada por el 415 batallón, 104 Brigada republicana, y capturada por el bando nacional: «Las cifras necesariamente deberán ser consignadas en letras. Las columnas señaladas con el signo (1) corresponden al alfabeto. Las columnas señaladas con el signo (2) corresponden a su equivalencia en clave».

Una vez completado este proceso, el primer modificador llevaba a cabo una rotación que lo situaba en la siguiente de sus 26 posiciones posibles. La nueva posición del modificador traía consigo un nuevo cifrado de los caracteres, y el emisor introducía entonces la segunda letra, y así sucesivamente. Para descodificar el mensaje, bastaba con introducir los caracteres cifrados en otra máquina Enigma con la condición de que los parámetros de salida de esta última fueran iguales a los de la máquina con la que se había llevado a cabo la encriptación.

En el dibujo siguiente se esquematiza, de forma muy simplificada, el mecanismo de encriptación de los rotores, con un alfabeto de sólo tres letras y un rotor, por tanto, con sólo tres posiciones posibles.

Para las comunicaciones de mayor nivel, el bando nacional, liderado por el general Franco, disponía de otra arma: treinta máquinas de las denominadas Enigma, suministradas por el Reich. Se trata del primer uso militar intensivo del ingenio de cifrado que emplearía Alemania en la Segunda Guerra Mundial. Los británicos intentaron durante el conflicto romper el cifrado, sin éxito.



TELEGRAMA OFICIAL

Gobierno Telegráfico

J A E.M.

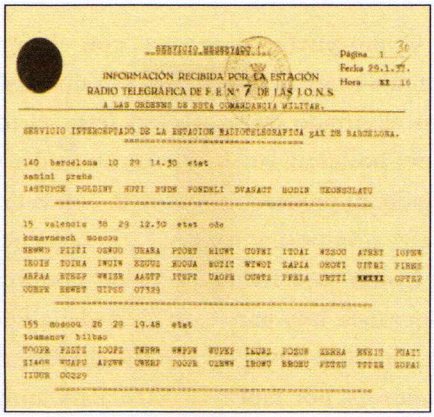
De Guerra

Jefe sector Granada.-

"Su telegrama cifrado ayer 21 horas clave Unión 1 1 en V (ene en uve) resulta completamente indescifrable. Repito y ordene encargado cifre exquisito cuidado este trabajo evitar retrasos y pérdida tiempo. Asimismo reconocimiento Rotación Telegráficas atención servicio por si alguna fuera mas justo aparatos.

F.R.C.H.O.

27 Octubre 1936. Al jefe del Sector Granada (republicano): «Su telegrama cifrado ayer... resulta indescifrable».

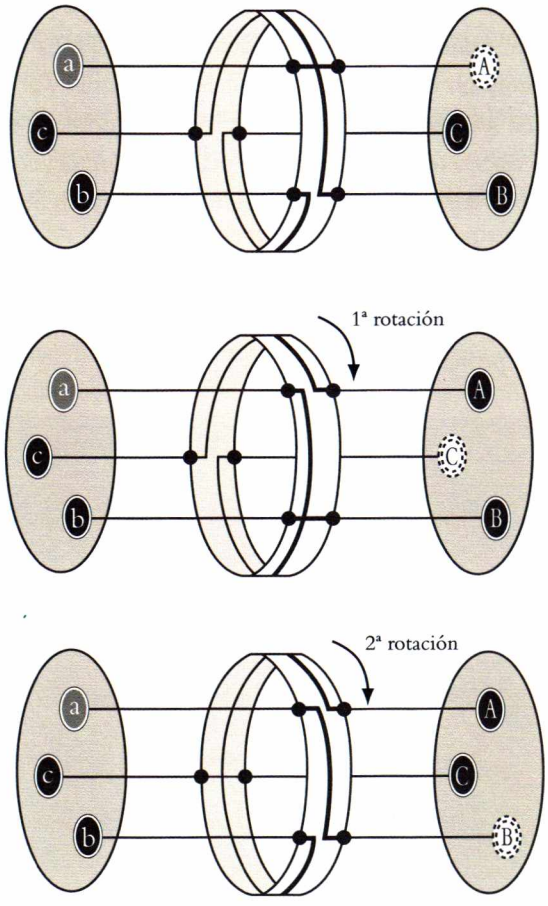


INFORMACIÓN RECIBIDA POR LA ESTACIÓN RADIO TELEGRÁFICA DE F.E.J.N.S. 7 DE LAS J.O.N.S.

A LAS ORDENES DE ESTA COMANDANCIA MILITAR.

SERVICIO INTERCEPTADO DE LA ESTACION RADIOTELEGRAFICA EAX DE BARCELONA.

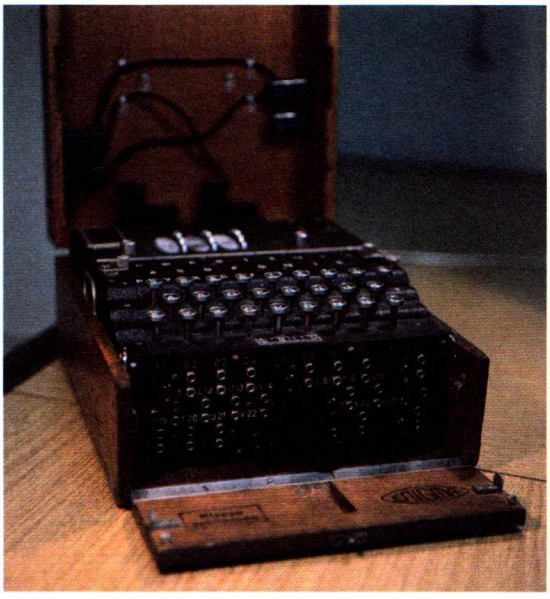
29 Enero 1936. Mensajes republicanos interceptados por Falange Española de las JONS en Canarias.



Como puede observarse, con el rotor en la posición inicial, cada letra del mensaje original se sustituye por una distinta, excepto la A, que queda inalterada. Tras el cifrado de la primera letra, el rotor se desplaza 1/3 de vuelta. En esta nueva posición, las letras son sustituidas ahora por otras distintas a las del primer cifrado. El proceso se completa con la tercera letra, momento en el cual el rotor vuelve a su posición inicial y la secuencia de cifrado volvería a repetirse.

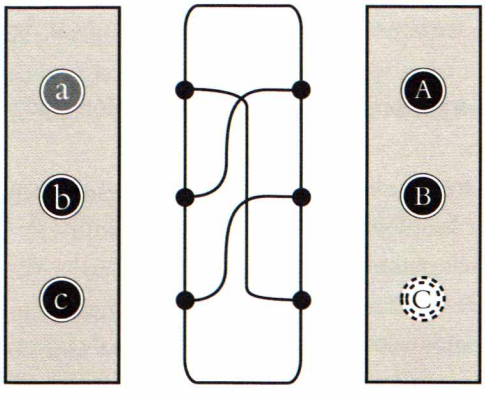
Como ya se ha indicado, los modificadores de la Enigma estándar tenían 26 posiciones, una para cada letra del alfabeto. En consecuencia, un modificador era capaz de llevar a cabo 26 cifrados distintos. La posición inicial del modificador es, por tanto, la clave. Para aumentar el número de claves posibles, el diseño de Enigma incorporaba hasta tres rotores, conectados de forma mecánica

uno con otro. Así, cuando el primer rotor completaba una vuelta, el siguiente iniciaba otra, y así hasta completar las rotaciones completas de los tres rotores para un total de $26 \times 26 \times 26 = 17.576$ posibles cifrados. Adicionalmente, el diseño de Scherbius permitía intercambiar el orden de los modificadores, aumentando todavía más el número de claves, como veremos más adelante.

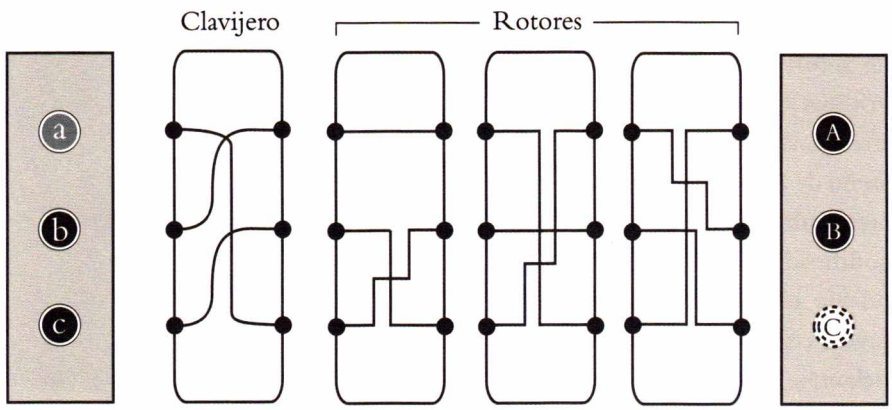


Máquina Enigma en la que puede observarse el clavijero.

En adición a los tres modificadores, Enigma disponía también de un clavijero situado entre el primero de ellos y el teclado. Este clavijero permitía intercambiar entre sí pares de letras antes de su conexión con el modificador, y añadía de este modo un número considerable de claves adicionales al cifrado. El diseño estándar de la máquina Enigma poseía seis cables, con los que se podían intercambiar hasta seis pares de letras. En el siguiente gráfico se muestra el funcionamiento del clavijero intercambiador, de nuevo con una estructura simplificada de tan sólo tres letras y tres cables.



De este modo, la A se intercambiaba con la C, la B con la A y la C con la B. Con el añadido del clavijero, una máquina Enigma simplificada de 3 letras quedaría de la siguiente manera:



¿Qué número de claves adicionales proporcionaba el clavijero, un añadido aparentemente trivial? Hay que considerar el número de maneras de conectar seis pares de letras escogidas entre un grupo de 26. En general, el número de posibles transformaciones de n pares de letras de un alfabeto de N caracteres viene determinado por la fórmula siguiente:

$$\frac{N!}{(N-2n)!\cdot n!\cdot 2^n}.$$

En nuestro ejemplo $N = 26$ y $n = 6$, de lo que resultan la friolera de 100.391.791.500 combinaciones.

En consecuencia, el número total de claves posibles que ofrece la máquina Enigma de tres rotores de 26 letras y un clavijero de seis cables es la siguiente:

1) En lo tocante a las rotaciones de los modificadores, $26^3 = 26 \cdot 26 \cdot 26 = 17.576$ combinaciones.
2) Asimismo, los tres modificadores (1, 2, 3) podían intercambiarse entre sí, pudiendo ocupar las posiciones 1-2-3, 1-3-2, 2-1-3, 2-3-1, 3-1-2, 3-2-1; con ello se tienen seis combinaciones posibles adicionales vinculadas, en este caso, con el orden de los modificadores.
3) Finalmente, hemos calculado que la disposición de los seis cables del clavijero inicial añadían por su parte 100.391.791.500 cifrados adicionales.

El número total de claves se obtiene del producto de las diferentes combinaciones especificadas, $6 \cdot 17.576 \cdot 100.391.791.500 = 10.586.916.764.424.000$. Por tanto, las máquinas Enigma podían cifrar un texto utilizando más de diez mil billones de combinaciones diferentes. El Reich descansaba tranquilo, instalado en la seguridad de que sus comunicaciones de más alto rango se encontraban perfectamente a salvo. Craso error.

Descifrar el código Enigma

Una clave cualquiera de Enigma especificaba la posición del clavijero para cada uno de los seis intercambios de letras posibles (por ejemplo, B/Z, F/Y, R/C, T/H, E/O y L/J para indicar que el primer cable intercambiaba las letras B y Z, y así sucesivamente), el orden de los rotores (como 2-3-1) y su orientación de partida (como R, V, B para indicar qué letra quedaba situada en la parte más alta). Estas indicaciones se recogían en libros de claves que a su vez eran transmitidos de forma encriptada, y podían cambiar día a día o en función de otras circunstancias, como la naturaleza del mensaje.

Para evitar repetir una misma clave a lo largo de todo un día –durante el cual podían llegar a enviarse miles de mensajes–, los operadores de Enigma recurrían a ingeniosos trucos para transmitir nuevas claves alternativas de uso restringido sin necesidad de alterar el libro de claves comunes. Así, el emisor codificaba, de acuerdo con la clave diaria pertinente, un mensaje de seis letras que indicaba, en realidad, una nueva disposición de los rotores, por ejemplo T-Y-J (para mayor seguridad, el emisor codificaba las tres indicaciones dos veces, de ahí las seis letras). A continuación, codificaba el mensaje real de acuerdo a esa nueva disposición. El receptor recibía un mensaje que no podía descifrar de acuerdo con la clave del día, pero sabía que los seis primeros caracteres de aquél eran en realidad instrucciones para disponer los rotores en otra posición. El receptor así lo hacía, manteniendo clavijero y orden de los rotores inalterados, y podía ahora desencriptar el mensaje de forma correcta.

Los aliados obtuvieron la primera información de valor relativa a Enigma en 1931 de mano de un espía alemán, Hans-Thilo Schmidt, y consistía en varios manuales para el uso práctico de la máquina. El contacto con Schmidt había sido establecido por la inteligencia polaca, que en esos años sentía ya a sus espaldas el resuello de una Alemania cada vez más belicosa. El departamento de criptoanálisis polaco, conocido como Byuro Szyfrów, se puso a trabajar con los documentos de

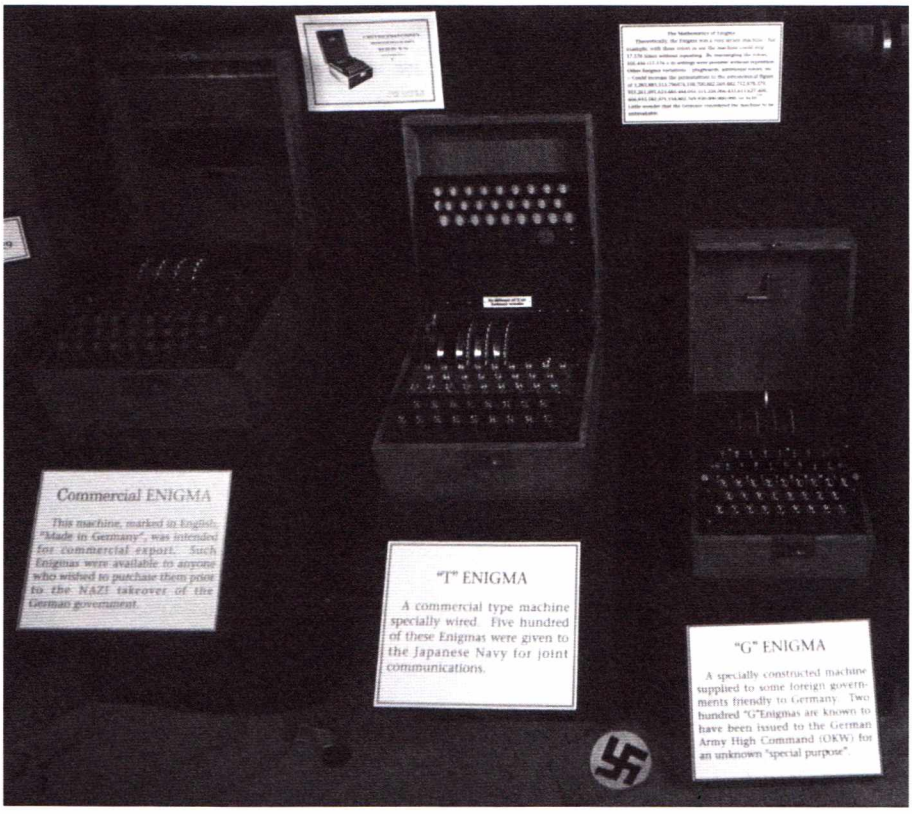
Schmidt y se agenció para ello varios ejemplares de máquinas Enigma sustraídas a los alemanes.

Como medida novedosa por aquella época, decidió incorporar al equipo de analistas un número considerable de matemáticos. Entre ellos se encontraba un talentoso joven de 23 años, introspectivo y tímido, llamado Marian Rejewski. Éste se puso a trabajar de inmediato y concentró sus esfuerzos, precisamente, en la clave de mensaje de seis letras que antecedía a muchos de los mensajes diarios que se intercambiaban los alemanes. Rejewski sabía que las segundas tres letras de la clave eran un nuevo cifrado de las tres primeras, y sabía, por tanto, que la cuarta, quinta y sexta letra podían dar pistas sobre la rotación de los modificadores.

De esta constatación, por ínfima que parezca, Rejewski edificó una extraordinaria red de deducciones que iba a permitir romper el código Enigma. El detalle de este proceso es muy complejo y no se va exponer aquí, pero el hecho es que, al cabo de unos meses, Rejewski había conseguido reducir el número de claves posibles que se debían desentrañar de los diez mil billones iniciales a los «escasos» 105.456 que resultaban de las diferentes combinaciones del orden de los modificadores y sus diferentes rotaciones. Para ello, Rejewski tuvo que construir un artefacto de funcionamiento similar a Enigma, conocido como *Bomba*, capaz de cotejar cualquiera de las posibles posiciones de los tres rotores en busca de la clave diaria. En fechas tan tempranas como 1934, el Byuro Szyfrów había conseguido romper Enigma y era capaz de descifrar cualquier mensaje en un plazo de 24 horas.

Aunque los alemanes desconocían que los polacos habían penetrado la seguridad de Enigma, no por ello dejaron de incorporar mejoras a un sistema que, al cabo, llevaba ya más de una década funcionando. En 1938, los operadores de Enigma recibieron dos rotores más que añadir a las tres ubicaciones estándar y, poco después, se distribuyeron nuevos modelos de máquina con clavijeros de diez cables.

El número de claves posibles aumentó de golpe a cerca de 159 trillones. Sólo la incorporación de dos rotores más a la rotación de modificadores aumentó de 6 a 60 las posibles combinaciones en su orden; es decir, uno cualquiera de los cinco rotores dispuestos en primer lugar (5 opciones) x uno cualquiera de los cuatro rotores restantes en la segunda posición (4 opciones) x uno cualquiera de los tres rotores en la tercera posición (3 opciones) $= 5 \times 4 \times 3 = 60$. Aunque sabía cómo descifrar el código, el Byuro Szyfrów carecía de los medios necesarios para analizar secuencialmente un número 10 veces mayor de nuevas configuraciones de los rotores.



Diferentes modelos de la máquina Enigma.

Los británicos toman el relevo

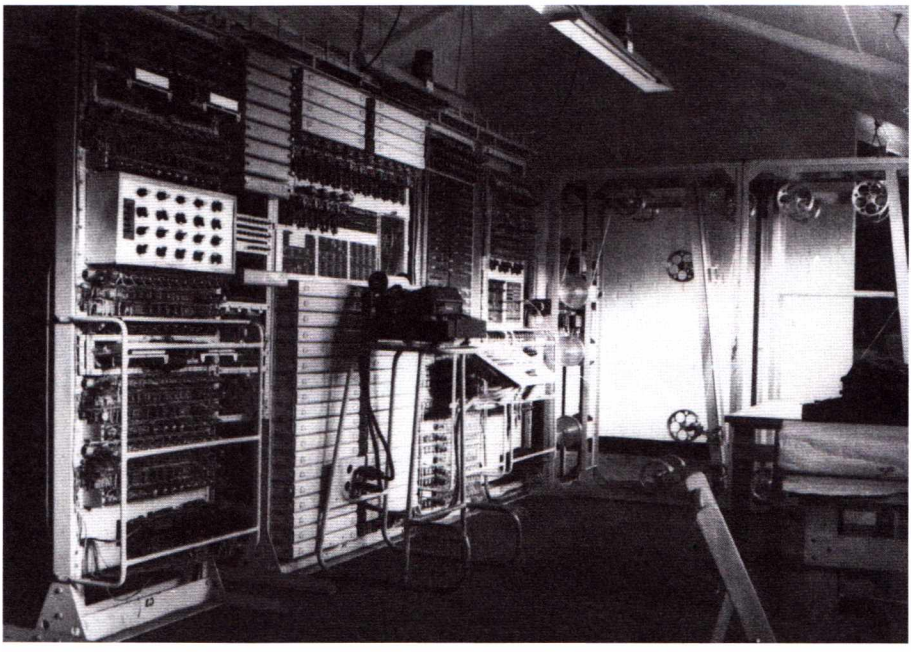
La mejora de Enigma no fue casual: Alemania había iniciado ya su agresiva expansión por Europa con la anexión de Checoslovaquia y Austria, y planeaba la invasión de Polonia. En 1939, con el conflicto ya desatado en el corazón de Europa y su país conquistado, los polacos remitieron sus máquinas Enigma y toda su información a sus aliados británicos, que en agosto de ese año decidieron concentrar y reubicar a sus dispersas unidades de criptoanálisis. El lugar escogido fue una casa señorial situada en las afueras de Londres, en una hacienda llamada Bletchley Park. Uno de los más brillantes criptoanalistas que el gobierno había incorporado al equipo de Bletchley Park era un joven matemático llamado Alan Turing. Turing era una autoridad mundial en el ámbito de la computación, por aquel entonces un campo todavía virgen y presto a nuevos y revolucionarios desarrollos. Estos conocimientos fueron clave a la hora de descifrar la mejorada Enigma.

Dependencias de Bletchley Park en las que trabajaban los expertos que descifraron el código Enigma.

Los expertos de Bletchley Park se centraron en fragmentos cortos de texto cifrado sobre los cuales tenían fundadas sospechas de cuál era su correspondencia con textos llanos. Por ejemplo, merced al trabajo de sus espías sobre el terreno, se sabía que los alemanes tenían la costumbre de transmitir un mensaje codificado acerca de las condiciones meteorológicas en varias posiciones del frente alrededor de las 6 de la tarde de todos los días. Por tanto, estaban razonablemente seguros de que un mensaje interceptado pocos minutos después de esa hora contenía la versión cifrada de textos llanos como «clima» o «lluvia». Turing ideó un sistema eléctrico que permitía reproducir todas y cada una de las 1.054.650 combinaciones posibles de orden y posición de los tres rotores en un tiempo inferior a las 5 horas. Este sistema era alimentado con las palabras cifradas que, por la longitud de los caracteres y otras pistas, se sospechaba que correspondían con fragmentos de texto llano como, por ejemplo, las anteriormente citadas «clima» o «lluvia».

Supongamos que se sospechaba que el texto cifrado FGRTY fuera la versión encriptada de «clima». Se introducía la cifra en la máquina y si existía una combinación de rotores que devolvía como resultado la palabra «clima», los criptoanalistas sabían que habían hallado, de las claves, la correspondiente a la configuración de los modificadores. A continuación, el operario introducía el texto cifrado en una máquina Enigma real con los rotores dispuestos según la clave. Si la máquina mostraba el

texto descifrado CIMLA, por ejemplo, era evidente que la parte de la clave relativa a la posición de los cables incluía la trasposición entre las letras I y L. De este modo, se obtenía la clave en su totalidad. Los secretos de Enigma salían definitivamente a la luz. En el proceso de desarrollo y refinamiento de las máquinas analíticas mencionadas, el equipo de Bletchley Park acabó desarrollando el primer prototipo de ordenador moderno de la historia, bautizado como *Colossus*.



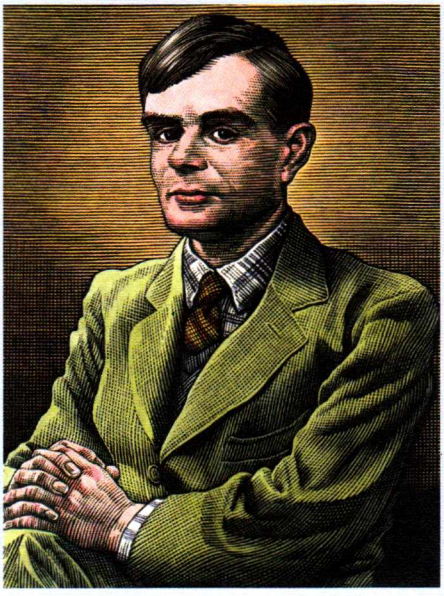
El Colossus, *prototipo del ordenador moderno, realizado en Bletchley Park. La fotografía, tomada en 1943, muestra el panel de control del complejo aparato.*

Otros códigos de la Segunda Guerra Mundial

Japón desarrolló dos sistemas propios de codificación: el Púrpura y el JN-25. El primero de ellos era utilizado para las comunicaciones diplomáticas y el segundo, para mandar mensajes de carácter militar. Ambos cifrados se implementaban mediante artefactos mecánicos. El JN-25, por ejemplo, consistía en un algoritmo de sustitución que traducía los ideogramas propios del idioma japonés (con una limitación de 30.000) a sucesiones de números según indicaban tablas aleatorias de cinco elementos. A pesar de las precauciones tomadas por los japoneses, británicos y norteamericanos descifraron el Púrpura y el JN-25 a tiempo de decidir

las primeras y cruciales batallas del Pacífico, en especial las del Mar del Coral y Midway, ambas en 1942, y de adoptar medidas trascendentales como la intercepción y asesinato del almirante Yamamoto el año siguiente. El material obtenido merced a las intercepciones de los cifrados Púrpura y JN-25 recibía el nombre de Magic.

UNA AUTÉNTICA «MENTE MARAVILLOSA»



Alan Turing nació en Inglaterra en 1912. Alumno atípico, mostró desde muy joven gran facilidad para las matemáticas y la física. En 1931 ingresó en Cambridge, donde se interesó por las aportaciones del lógico Kurt Gödel al problema general de la *indecibilidad* inherente a todo sistema lógico. Tres años antes había publicado un estudio sobre la posibilidad teórica de construir máquinas que fueran capaces de computar diversos algoritmos, tales como la suma, la multiplicación, etc. Espoleado por los trabajos de Gödel, en 1937 llevó sus ideas más allá y estableció los principios de una «máquina universal» capaz de computar toda clase de algoritmo. Nacía así uno de los pilares del edificio teórico de la informática moderna. Dos años antes de su revolucionaria aportación, Turing trabó contacto con el gran matemático húngaro John von Neumann, por aquel entonces exiliado en Estados Unidos. Von Neumann, a quien se considera «el otro padre» de la computación, ofreció a Turing un puesto en Princeton, trabajo bien remunerado y de mucho prestigio. Sin embargo, Turing prefirió el ambiente bohemio de Cambridge y declinó la oferta. En 1939 se incorporó al departamento británico de análisis criptográfico ubicado en Bletchley Park. Aunque por sus trabajos durante la guerra Turing mereció la Orden del Imperio Británico, su homosexualidad le expuso al rechazo del entorno académico. Afectado por una profunda depresión, Alan Turing se suicidó el 8 de junio de 1954 por ingesta de cianuro potásico. Tenía 42 años.

Los «hablantes en código» navajos

Una de las herramientas más sorprendentes de las implementadas durante el conflicto para ocultar información al enemigo fue la empleada por los norteamericanos en el teatro de operaciones del Pacífico. Los oficiales de inteligencia estadounidenses optaron en esta ocasión por varios códigos en el sentido estricto expuesto al principio del volumen; es decir, por unos algoritmos de encriptación que operaban directamente sobre la naturaleza de las palabras. Estos códigos –el Choctaw, el Comanche, el Meskwaki y, sobre todo, el Navajo– no estaban explicitados en farragosos manuales ni eran el resultado de la planificación de un sesudo departamento de criptógrafos: se trataba de idiomas amerindios reales.

El ejército estadounidense dispuso operadores de radio de dichas culturas étnicas en diversas unidades distribuidas en el frente, y les puso al cargo de transmitir los mensajes en sus respectivas lenguas, desconocidas no sólo para los japoneses sino incluso para el resto de sus compatriotas. A los mensajes así codificados se les superponía un libro de códigos básico para impedir que un soldado capturado pudiera traducirlos. Estos *code talkers* (en inglés, «hablantes en código») sirvieron en diversas unidades hasta la guerra de Corea.

Dos code talkers *(hablantes en código) navajo durante la batalla de Bougainville de 1943.*

Vías de innovación: el cifrado de Hill

Los cifrados expuestos hasta el momento, en los que se sustituye un carácter por otro de forma preestablecida, son, como se ha visto, susceptibles de criptoanálisis.

En 1929, el matemático estadounidense Lester S. Hill ideó, patentó y puso a la venta, sin éxito, un nuevo sistema de cifrado que se servía de una combinación de aritmética modular y álgebra lineal.

Como veremos a continuación, una matriz puede ser una herramienta muy útil para cifrar un mensaje, descomponiendo el texto en pares de letras y asociando a cada letra un valor numérico del alfabeto.

Para cifrar un mensaje, empleamos una matriz

$$A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

con la restricción de que su *determinante* sea 1; es decir, que $ad\text{-}bc = 1$. Para descifrar emplearemos la matriz inversa

$$A^{-1}=\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

UNA PINCELADA DE ÁLGEBRA LINEAL

Una *matriz* se puede caracterizar como una tabla dispuesta en filas y columnas. Por ejemplo, una matriz de 2×2 es de la forma

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

y una matriz de 1×2 es de la forma

$$\begin{pmatrix} x \\ y \end{pmatrix}.$$

Del producto de ambas matrices se obtiene una nueva matriz 1×2, llamada *vector columna*:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}=\begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}.$$

Para el caso de la matriz de 2×2, el valor $ad-bc$ se denomina *determinante* de la matriz.

La restricción en el valor del determinante viene obligada por la necesidad de disponer de esta matriz inversa para garantizar así el descifrado. Por regla general, para un alfabeto de n caracteres es necesario que mcd (determinante de A, n) = 1. En caso contrario no podría garantizarse la existencia de inverso en aritmética modular.

Siguiendo con el ejemplo, se toma un alfabeto de 27 letras con un carácter «espacio en blanco» que denominamos, a efectos del ejemplo, @. Se asigna a cada letra un valor numérico tal y como se indica en la tabla siguiente:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	@
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

Para poder obtener valores entre 0 y 27 se trabajará en módulo 28.

El proceso de cifrado y descifrado del texto es como sigue: en primer lugar, determinamos una matriz de cifrado A de determinante 1.

Por ejemplo, $A = \begin{pmatrix} 1 & 3 \\ 2 & 7 \end{pmatrix}$.

La matriz de descifrado será la matriz inversa $A^{-1} = \begin{pmatrix} 7 & -3 \\ -2 & 1 \end{pmatrix}$.

Por tanto, A será la clave de cifrado, y A^{-1} la de descifrado.

A continuación se establece el mensaje, por ejemplo «HOY». Se agrupan los caracteres del mensaje en pares: HOY@. Sus correspondencias numéricas según la tabla son los pares de cifras (7,15) y (25, 27).

Seguidamente se multiplica la matriz A por cada par de cifras:

$$\text{Cifrado «HO»} = \begin{pmatrix} 1 & 3 \\ 2 & 7 \end{pmatrix}\begin{pmatrix} 7 \\ 15 \end{pmatrix} = \begin{pmatrix} 52 \\ 119 \end{pmatrix} \equiv \begin{pmatrix} 24 \\ 7 \end{pmatrix} \text{ (mód. 28)},$$

que corresponde, según la tabla de equivalencias, a los caracteres (X, H).

$$\text{Cifrado «Y@»} = \begin{pmatrix} 1 & 3 \\ 2 & 7 \end{pmatrix}\begin{pmatrix} 25 \\ 27 \end{pmatrix} = \begin{pmatrix} 106 \\ 239 \end{pmatrix} \equiv \begin{pmatrix} 22 \\ 15 \end{pmatrix} \text{ (mód. 28)},$$

que corresponde a los caracteres (V, O).

El mensaje «HOY» queda cifrado como «XHVO».

Para el descifrado se lleva a cabo la operación inversa utilizando la matriz

$$A^{-1} = \begin{pmatrix} 7 & -3 \\ -2 & 1 \end{pmatrix}.$$

Se toma el par de caracteres (X, H) y se busca su equivalencia numérica: (24,7). A continuación, se multiplica por A^{-1}, obteniéndose:

$$\begin{pmatrix} 7 & -3 \\ -2 & 1 \end{pmatrix}\begin{pmatrix} 24 \\ 7 \end{pmatrix} = \begin{pmatrix} 147 \\ -41 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 15 \end{pmatrix} \text{ (mód. 28), equivalente a (H, O).}$$

Se hace lo propio con el par (V, O) y su correspondencia (22,15) y se obtiene:

$$\begin{pmatrix} 7 & -3 \\ -2 & 1 \end{pmatrix}\begin{pmatrix} 22 \\ 15 \end{pmatrix} = \begin{pmatrix} 109 \\ -29 \end{pmatrix} \equiv \begin{pmatrix} 25 \\ 27 \end{pmatrix} \text{ (mód. 28), equivalente a (Y,@).}$$

Se comprueba que el descifrado es correcto.

Para el ejemplo se han considerado pares de dos caracteres. Mayor seguridad se obtendría agrupando los caracteres en tríos o incluso de cuatro en cuatro. En esos casos lo cálculos se harían con matrices de 3×3 y 4×4, respectivamente, lo que resulta laborioso si se lleva a cabo manualmente. Con los ordenadores actuales, sin embargo, es posible trabajar con matrices de orden inmenso, y sus inversas respectivas.

El cifrado de Hill adolece de una importante debilidad: en caso de que el receptor disponga de un fragmento pequeño del texto llano, es factible descifrar el mensaje en su totalidad. La búsqueda del cifrado perfecto estaba lejos de concluir.

Capítulo 4

Dialogar con ceros y unos

El descifrado de Enigma y la invención del *Colossus* nos dejaba a las puertas de la mayor revolución de las comunicaciones que ha conocido la humanidad: la computación moderna. Este gigantesco salto adelante se apoyó en buena parte en el desarrollo de un sistema de codificado que permitió establecer comunicaciones eficaces y rápidas entre una vasta red articulada alrededor de dos agentes fundamentales: los ordenadores y sus usuarios, es decir, nosotros. Ya no hablamos aquí sólo de seguridad en el sentido criptográfico, sino en un sentido más amplio que abarca también nociones de fiabilidad y eficiencia.

En la base de esta revolución tecnológica se encuentra el sistema binario. Este sencillísimo código formado por dos caracteres, el 0 y el 1, es el más usado en informática por su capacidad de expresar funciones lógicas mediante las que interaccionar con los circuitos electrónicos de ordenadores y otros aparatos. Cada 0 y cada 1 se denomina *bit* (término derivado del inglés *binary digit*, es decir, «dígito binario»). Una buena analogía sería decir que el sistema binario es la lengua vernácula de los ordenadores.

El código ASCII

Una de las muchas aplicaciones del sistema binario es una familia particular de caracteres diseñados de tal forma que cada caracter tenga una longitud de 8 bits (1 *byte*).

Estos caracteres, denominados *alfanuméricos*, son el conjunto de signos básicos empleados en la comunicación convencional, y se le denomina código *ASCII* (siglas de *American Standard Code for Information Interchange* o «Código Estándar Americano

MEMORY BYTES

La *memoria* o capacidad de almacenamiento de un ordenador y, en general, de toda máquina se mide en múltiplos de bytes.

Kilobyte (KB): 1.024 bytes

Megabyte (MB): 1.048.576 bytes

Gigabyte (GB): 1.073.741.824 bytes

Terabyte (TB): 10.99.511.627.776 bytes

para Intercambio de Información»). El número de caracteres del código ASCII es 256, cifra que resulta de todas las formas posibles de ordenar de modo diferente un conjunto de 8 ceros o unos, es decir: $2^8 = 256$.

El código ASCII es el que permite la comunicación textual entre el usuario y el ordenador. Cuando se teclea un carácter alfanumérico, el ordenador lo traduce a bytes, es decir, a una cadena de ocho bits. Así, por ejemplo, al escribir la letra A, el ordenador entiende 0100 0001.

La relación entre valores binarios y decimales de los caracteres ASCII más comúnmente empleados en las tareas diarias (26 letras mayúsculas, 26 minúsculas, 10 dígitos numéricos, 7 signos de puntuación y algunos caracteres especiales) se muestra en la tabla siguiente:

TABLA ASCII								
Carácter	Binario	Dec.	Carácter	Binario	Dec.	Carácter	Binario	Dec.
	0010 0000	32	@	0100 0000	64	`	0110 0000	96
!	0010 0001	33	A	0100 0001	65	a	0110 0001	97
"	0010 0010	34	B	0100 0010	66	b	0110 0010	98
#	0010 0011	35	C	0100 0011	67	c	0110 0011	99
$	0010 0100	36	D	0100 0100	68	d	0110 0100	100
%	0010 0101	37	E	0100 0101	69	e	0110 0101	101
&	0010 0110	38	F	0100 0110	70	f	0110 0110	102
'	0010 0111	39	G	0100 0111	71	g	0110 0111	103
(	0010 1000	40	H	0100 1000	72	h	0110 1000	104
)	0010 1001	41	I	0100 1001	73	i	0110 1001	105
*	0010 1010	42	J	0100 1010	74	j	0110 1010	106
+	0010 1011	43	K	0100 1011	75	k	0110 1011	107
,	0010 1100	44	L	0100 1100	76	l	0110 1100	108
-	0010 1101	45	M	0100 1101	77	m	0110 1101	109
.	0010 1110	46	N	0100 1110	78	n	0110 1110	110
/	0010 1111	47	O	0100 1111	79	o	0110 1111	111
0	0011 0000	48	P	0101 0000	80	p	0111 0000	112
1	0011 0001	49	Q	0101 0001	81	q	0111 0001	113
2	0011 0010	50	R	0101 0010	82	r	0111 0010	114
3	0011 0011	51	S	0101 0011	83	s	0111 0011	115
4	0011 0100	52	T	0101 0100	84	t	0111 0100	116
5	0011 0101	53	U	0101 0101	85	u	0111 0101	117
6	0011 0110	54	V	0101 0110	86	v	0111 0110	118
7	0011 0111	55	W	0101 0111	87	w	0111 0111	119
8	0011 1000	56	X	0101 1000	88	x	0111 1000	120
9	0011 1001	57	Y	0101 1001	89	y	0111 1001	121

Carácter	Binario	Dec.	Carácter	Binario	Dec.	Carácter	Binario	Dec.
:	0011 1010	58	Z	0101 1010	90	z	0111 1010	122
;	0011 1011	59	[	0101 1011	91	{	0111 1011	123
<	0011 1100	60	\	0101 1100	92	|	0111 1100	124
=	0011 1101	61	]	0101 1101	93	}	0111 1101	125
>	0011 1110	62	^	0101 1110	94	~	0111 1110	126
?	0011 1111	63	-	0101 1111	95			

En el caso de teclear un texto como «GOTO 2», muy típico de la programación básica, el ordenador traducirá los caracteres a la secuencia binaria correspondiente:

Palabra tecleada	G	O	T	O	Espacio en blanco	2
Traducción al lenguaje del ordenador	01000111	01001111	01010100	01001111	0010 0000	00110010

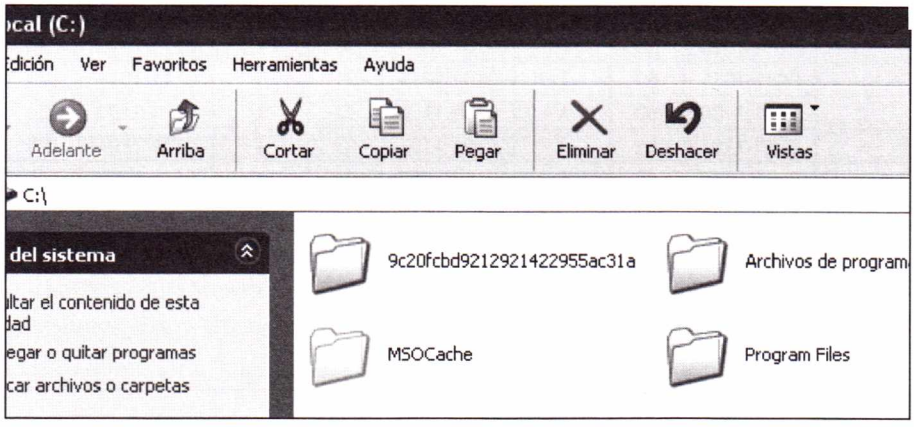
El ordenador implementará, pues, la secuencia

01000111010011110101010001001111001 0 000000110010.

El sistema hexadecimal

El sistema hexadecimal es un segundo código de notable importancia en el ámbito de los ordenadores. Se trata de un sistema de numeración que trabaja con dieciséis dígitos únicos (de ahí «hexadecimal»), a diferencia del habitual, que trabaja con diez («decimal»). El sistema hexadecimal, podría decirse, es el «segundo idioma» del ordenador después del binario. ¿Por qué? Recordemos que la unidad básica de memoria de los ordenadores, el byte, está compuesto por ocho bits, lo que arroja hasta $2^8 = 256$ combinaciones diferentes de ceros y unos. Obsérvese que $2^8 = 2^4 \times 2^4 = 16 \times 16$. Es decir, que la combinación de dos caracteres hexadecimales equivale a 1 byte. Los dieciséis dígitos del sistema hexadecimal son los tradicionales 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, y seis más establecidos por convenio: A, B, C, D, E, F. Para contar en sistema hexadecimal se procede de modo siguiente:

Del 0 al 15: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.
Del 16 al 31: 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 1A, 1B, 1C, 1D, 1E, 1F.
Del 32 en adelante: 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 2A, 2B, 2C...



La carpeta del extremo superior izquierdo la ha generado el ordenador de manera automática. Su extraño nombre es un número hexadecimal.

A diferencia del código binario, el hexadecimal no distingue entre mayúsculas y minúsculas. La correspondencia entre binario y hexadecimal de los 16 dígitos únicos de este segundo sistéma es la siguiente:

Binario	Hexadecimal
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

Para el paso de binario a hexadecimal se agrupan los bits de 4 en 4 desde la derecha y se completa la conversión según la tabla superior. Si el número de dígitos binarios no es múltiplo de 4 se completa la diferencia con ceros a la izquierda. Para el paso de hexadecimal a binario se convierte cada dígito hexadecimal a su equivalente en binario como en el ejemplo siguiente.

$9F2_{16}$ es la notación formal de un número hexadecimal (se indica así mediante el subíndice 16).

Tengamos en cuenta la correspondencia:

9	F	2
1001	1111	0010

así, $9F2_{16} = 100111110010_2$ (nótese el subíndice 2, que indica que el número está expresado en sistema binario).

Hagamos ahora el proceso contrario: 1110100110_2 tiene 10 dígitos. Por tanto, completaremos el número con dos ceros a la izquierda para así contar con 12 dígitos y poderlos agrupar de 4 en 4.

Convertimos:

$$1110100110_2 = 0011\ \ 1010\ \ 0110_2 = 3A6_{16}.$$

¿Cuál es la equivalencia entre caracteres hexagecimales y ASCII? Cada carácter ASCII contiene 8 bits de información (= 1 byte), luego 5 caracteres ASCII contendrán 40 bits (5 bytes) y, como un carácter hexadecimal contiene 4 bits, tendremos que 5 caracteres ASCII son 10 caracteres hexadecimales.

Veamos un ejemplo de codificación de una frase en código hexadecimal; para el caso, la frase «Ediciones RBA».

1) Traducimos «Ediciones RBA» a su versión binaria mediante el estándar ASCII.
2) Agrupamos los dígitos de 4 en 4 (si la longitud no es múltiplo de 4, se añaden ceros a la izquierda).
3) Se consulta la tabla de conversión de binario a hexadecimal y se procede a traducirlo.

Mensaje	E	d	i	c	i	o	n	e	s	
Equivalencia binaria según ASCII	01000101	01100100	01101001	01100011	01101001	01101111	01101110	01100101	01110011	00100000
Traducción a hexadecimal	45	64	69	63	69	6F	6E	65	73	20

Mensaje (cont.)	R	B	A
Equivalencia binaria según ASCII	01010010	01000010	01000001
Traducción a hexadecimal	52	42	41

La frase «Ediciones RBA» se codifica en hexadecimal, ahora ya sin mayúsculas ni minúsculas, como:

45 64 69 63 69 6F 6E 65 73 20 52 42 41.

Sistemas de numeración y cambios de base

De un sistema numérico de n dígitos se dice también que está en base n. Las manos humanas poseen diez dedos, y es ésa probablemente la razón de por qué se inventó el sistema numérico decimal: el conteo se realizaba con ellos. Un número decimal, como el 7392, representa una cantidad igual a 7 millares más 3 centenas más 9 decenas más 2 unidades. Millares, centenas, decenas y unidades son potencias de la base del sistema numérico; en este caso, de 10. El número 7392, por tanto, podría expresarse como:

$$7392 = 7 \cdot 10^3 + 3 \cdot 10^2 + 9 \cdot 10^1 + 2 \cdot 10^0.$$

Por convenio, se escriben únicamente los coeficientes. Además del sistema decimal existen muchos otros sistemas de numeración (de hecho, su número es potencialmente infinito). En este volumen hemos prestado especial atención a dos: el binario, de base 2, y el hexadecimal, de base 16. En un sistema binario de numeración los coeficientes sólo tienen dos valores posibles: 0 y 1. Los dígitos de los números binarios son coeficientes de potencias de 2. Así, el número 11011_2 puede escribirse también como

$$11011_2 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0.$$

Si operamos la expresión a la derecha de la igualdad obtenemos 27, que es la forma decimal del número binario considerado. Para el proceso inverso se divide sucesivamente el número decimal entre 2 (la base del binario) y se anotan los restos hasta obtener un cociente 0. El número binario tendrá el último cociente como primer dígito y le seguirán los restos a partir del último obtenido. Con el fin de visualizar el proceso escribiremos el número 76 en binario.

76 dividido entre 2 tiene cociente 38 y resto **0**.
38 dividido entre 2 tiene cociente 19 y resto **0**.
19 dividido entre 2 tiene cociente 9 y resto **1**.
9 dividido entre 2 tiene cociente 4 y resto **1**.
4 dividido entre 2 tiene cociente 2 y resto **0**.
2 dividido entre 2 tiene cociente 1 y resto **0**.

En consecuencia el número 76 escrito en sistema binario será 1001100_2.Este resultado puede comprobarse en la tabla ASCII anterior (téngase en cuenta que en la casilla correspondiente se visualiza un 0 de más al principio como resultado de la adición de ceros a la izquierda mencionada con anterioridad). La conversión de una cantidad expresada en un sistema de numeración a otro se conoce como «cambio de base» de la cantidad en cuestión.

Códigos contra la pérdida de información

Los distintos códigos antes señalados tienen por objetivo habilitar comunicaciones seguras y efectivas entre ordenadores y programas, por un lado, y los usuarios, por otro. Pero este lenguaje debe apoyarse en una teoría general de la información que siente las bases del proceso de comunicación mismo. El primer paso para una teoría de este tipo es tan básico que seguramente ni siquiera se nos ocurriría: cómo medir la información.

Una frase del estilo «el adjunto pesa 2 Kb» concentra una larga serie de geniales intuiciones cuyo arranque es un artículo en dos partes publicado en 1948 por el ingeniero norteamericano Claude E. Shannon y titulado «Una teoría matemática de la comunicación». En este artículo seminal, Shannon propuso una unidad de medida para la cantidad de información que bautizó como *bit*. El problema general que originó el trabajo de Shannon era uno que a los lectores de este volumen ya debe resultarles familiar: ¿Cuál es el mejor modo de codificar un mensaje para evitar

el deterioro de la información durante la transmisión? Shannon concluyó que era imposible definir una codificación que impidiera en todos los casos la pérdida de información; es decir, que esta última se deteriora de forma irremediable. Esta aleccionadora conclusión no detuvo los esfuerzos por definir estándares de codificación que si bien no pueden impedir dicho deterioro, aseguren al menos los máximos niveles posibles de fiabilidad e integridad.

En una transmisión digital de información, el mensaje, una vez generado por el emisor (que bien puede ser un agente no humano, es decir, una computadora u otro dispositivo), se codifica en sistema binario y entra en un canal de comunicación, el cual estará integrado por los ordenadores de emisor y receptor y el canal propiamente dicho, físico (cable) o incorpóreo (ondas, luz...). El viaje por el canal es el proceso más delicado, puesto que el mensaje se puede ver sometido a toda clase de interferencias: por cruzamiento de señales, por cambios de temperatura en los soportes físicos, bajadas de tensión que afectan a estos mismos soportes, etc. Estas interferencias se denominan técnicamente *ruidos*.

Para minimizar el impacto de los ruidos no sólo hay que proteger el canal, sino que es preciso establecer metodologías de detección y corrección de los errores que invariablemente se van a producir.

Una de esas metodologías es la *redundancia*. La redundancia consiste en repetir, bajo determinados criterios, ciertas características del mensaje. Mostraremos un ejemplo que ayudará a entender el proceso. Supongamos un alfabeto tal que cada palabra se construya con 4 bits, para un total de 16 palabras ($2^4 = 16$), cada una de ellas del tipo $a_1a_2a_3a_4$, siendo a_1, a_2, a_3 y a_4 los valores de los bits de la palabra. Antes de enviar un mensaje añadimos a la palabra 3 caracteres adicionales $c_1c_2c_3$, de forma que el mensaje codificado tal y como circula por el canal será de la forma $a_1a_2a_3a_4c_1c_2c_3$. Los elementos $c_1c_2c_3$ serán los garantes de la seguridad del mensaje –se les denomina *códigos de paridad*– y se generan del siguiente modo:

$$c_1 = \begin{cases} 0 \text{ si } a_1 + a_2 + a_3 \text{ es par} \\ 1 \text{ si } a_1 + a_2 + a_3 \text{ es impar} \end{cases}$$

$$c_2 = \begin{cases} 0 \text{ si } a_1 + a_2 + a_4 \text{ es par} \\ 1 \text{ si } a_1 + a_2 + a_4 \text{ es impar} \end{cases}$$

$$c_3 = \begin{cases} 0 \text{ si } a_2 + a_3 + a_4 \text{ es par} \\ 1 \text{ si } a_2 + a_3 + a_4 \text{ es impar} \end{cases}$$

A un mensaje como 0111 se le asignarán los siguientes códigos de paridad:

Como $0+1+1=2$ par, el dígito $c_1 = 0$

Como $0+1+1=2$ par, el dígito $c_2 = 0$

Como $1+1+1=3$ impar, el dígito $c_3 = 1$.

En consecuencia, el mensaje 0111 se enviará en la forma 0111001. Para las 16 «palabras» siguientes resulta la tabla:

Mensaje original	Mensaje enviado
0000	0000000
0001	0001011
0010	0010111
0100	0100101
1000	1000110
1100	1100011
1010	1010001
1001	1001101
0110	0110010
0101	0101110
0011	0011100
1110	1110100
1101	1101000
1011	1011010
0111	0111001
1111	1111111

GENIO SIN PREMIO

Claude Elwood Shannon (1916-2001) es una de las mayores figuras de la ciencia del siglo xx. Ingeniero técnico por la Universidad de Michigan y doctor por el Massachusetts Institute of Technology, trabajó como matemático en los Laboratorios Bell realizando investigaciones en criptografía y teoría de la comunicación. Sus aportaciones a la teoría de la información bastan para situarle en el panteón de los más grandes, pero al estar su trabajo a caballo entre la matemática y la informática, no recibió nunca el galardón más codiciado por todo científico: el Nobel.

Supongamos que al final del trayecto el sistema receptor recibe el mensaje 1010110. Nótese que esta combinación de ceros y unos no se encuentra entre los mensajes posibles y, por tanto, debe tratarse de un error de transmisión. Para intentar corregir el error, el sistema compara cada dígito con el conjunto de dígitos de posibles mensajes para buscar la alternativa más probable. Para ello examinará la cantidad de dígitos distintos para cada posición de la palabra errónea, tal y como se muestra a continuación.

Mensaje posible	0000000	0001011	0010111	0100101	1000110
Mensaje recibido	1010110	1010110	1010110	1010110	1010110
Número de dígitos distintos en cada posición	4	5	2	5	1

Mensaje posible	1100011	1010001	1001101	0110010	0101110
Mensaje recibido	1010110	1010110	1010110	1010110	1010110
Número de dígitos distintos en cada posición	4	3	4	3	4

Mensaje posible	0011100	1110100	1101000	1011010	0111001	1111111
Mensaje recibido	1010110	1010110	1010110	1010110	1010110	1010110
Número de dígitos distintos en cada posición	3	2	5	2	6	3

La palabra errónea (10**1**0110) difiere en un solo dígito de otra: 10**0**0110. Como la diferencia es muy escasa, el sistema ofrecerá al receptor este segundo mensaje. El principio es análogo al del corrector ortográfico de un procesador de texto cuando detecta un término que no consta en su diccionario interno y propone una serie de alternativas próximas. Al número de posiciones en que un mensaje, entendido en tanto que una secuencia de caracteres, difiere de otro se conoce como *distancia entre dos secuencias*. Este mecanismo concreto de detección y corrección de errores fue propuesto por el norteamericano Richard W. Hamming (n. 1915), contemporáneo de Shannon.

En información, como en cualquier otro ámbito, una cosa es detectar los posibles errores y otra muy distinta corregirlos. En codificaciones como la ejemplificada, si sólo hay un candidato de distancia mínima el problema es trivial. Si se llama t al número mínimo de «unos» que hay en las secuencias (exceptuando la secuencia cuyos dígitos son todos ceros) entonces se verifica que:

Si t es impar, se podrán corregir $\frac{t-1}{2}$ errores.

Si t es par, se podrán corregir $\frac{t-2}{2}$ errores.

Si sólo interesa detectar los errores, el número máximo que se podrá detectar será $t-1$.

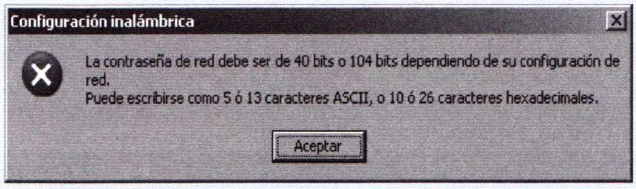
En el idioma de 16 caracteres expuesto más arriba, $t=3$, de lo que se obtiene que el dispositivo es capaz de detectar $3-1=2$ errores y de corregir $(3-1):2=1$ error.

ENCUENTROS CRIPTOGRÁFICOS EN LA TERCERA FASE

En 1997 se introdujo un *protocolo* para la transmisión segura de información entre redes inalámbricas denominado WEP (acrónimo del inglés *Wired Equivalent Privacy*, «Privacidad equiparable a la transmisión por hilo»). Este protocolo incluye un algoritmo de encriptación denominado RC4, con dos tipos de claves de 5 y de 13 caracteres ASCII, respectivamente. Se trata, en consecuencia, de claves de 40 o 104 bits o, alternativamente, de 10 o 26 caracteres hexadecimales:

5 letras alfanuméricas = 40 bits = 10 caracteres hexadecimales
13 letras alfanuméricas = 104 bits =26 caracteres hexadecimales

Las claves las proporciona el proveedor de la conexión, aunque el usuario suele poder cambiarlas. Antes de establecer la conexión, el ordenador solicita la clave. En la captura siguiente se puede observar un mensaje de petición de clave WEP donde se explicita su longitud en bits, caracteres ASCII y caracteres hexadecimales.



En realidad, las claves reales son de mayor longitud. A partir de las que el usuario le proporciona, el algoritmo RC4 genera una clave nueva de más bits, que es la que se emplea para cifrar la transmisión. Este tipo de criptografía se denomina de llave pública y se explicará con más detalle en el capítulo 5. Un usuario que quiera cambiar su clave hará bien en recordar que es más segura una clave de diez caracteres hexadecimales que otra de cinco caracteres alfanuméricos, aunque su tamaño en bits sea el mismo. Aunque también es cierto que «jaime» es más fácil de recordar que su equivalencia hexadecimal,«6A61696D65».

Los «otros» códigos: los estándares de la industria y el comercio

Aunque con menos *glamour* que los criptográficos o los binarios, y a menudo invisibles a nuestros ojos a pesar de su ubicuidad, los códigos estandarizados de bancos, mayoristas y otros grandes sectores de la actividad económica son uno de los pilares sobre los que se sustenta la sociedad moderna. Para el caso de estos códigos, la prioridad es asegurar la identificación única y correcta de los productos, ya sean éstos cuentas bancarias, libros o manzanas. Vamos a examinar en detalle la naturaleza y el funcionamiento de algunos de ellos y de los procesos mediante los cuales se cifran y supervisan.

Las tarjetas de crédito

Las tarjetas de crédito y débito que ofrecen entidades bancarias y grandes superficies se identifican esencialmente por los mismos grupos de dígitos y por un mismo algoritmo de cálculo y comprobación, basado precisamente en nuestra «vieja amiga» la aritmética modular. La mayoría de las tarjetas poseen 16 dígitos cuyo valor puede ser cualquiera entre 0 y 9, agrupados en grupos de 4 dígitos para su mejor visualización, a los cuales denotaremos:

ABCD EFGH IJKL MNOP

Cada grupo de dígitos codifica una información u otra: los cuatro primeros (A, B, C, D) corresponden al identificativo del banco o entidad que cede la tarjeta. Cada banco tiene un número diferente que puede variar según el continente, y que además está relacionado con la marca de tarjeta. Por ejemplo, para el caso de VISA y de algunos bancos destacados son las siguientes.

A B C D	Entidad
4940	Citibank
4024	Bank of America
4128	Citibank (EE.UU.)
4302	HSBC

El quinto dígito (E) corresponde al tipo de tarjeta e indica qué entidad financiera gestiona esa tarjeta.

Tipo	Entidad
3	American Express
4, 0, 2	Visa
5, 0	Master Card
6	Discover

Como se ve no es una norma rígida.

Los diez dígitos siguientes (FGH IJKL MNO) identifican al usuario de forma única. En esta identificación no sólo se proporciona un número de serie a cada cliente, sino que este número se relaciona también con el límite de crédito del grupo al que pertenece la tarjeta (clásica, oro, platino) y su fecha de caducidad.

Finalmente, se emplea un dígito de control (P) que se relaciona con los anteriores por el *algoritmo de Luhn*, llamado así en honor del ingeniero que lo desarrolló, el alemán Hans Peter Luhn.

El funcionamiento de este algoritmo para una tarjeta numerada con 16 dígitos es como sigue:

1) Para cada dígito de las posiciones impares, empezando por la izquierda, se calcula un dígito nuevo que es el que se tenía anteriormente multiplicado por dos. Si el resultado de esta multiplicación es mayor de 9 se suman las dos cifras del número obtenido (o hacemos la operación equivalente de restarle 9). Por ejemplo, si obtenemos 17 tomaremos $1+7=8$ o bien $17-9=8$.
2) A continuación, se suman los números así calculados y los dígitos situados en las posiciones pares (incluido el de control).
3) Si el resultado es múltiplo de 10 (es decir, vale 0 en módulo 10) la numeración de la tarjeta es correcta. Nótese que el dígito de control es el que hace que la suma total sea múltiplo de 10.

CLUB DE COMIDAS

Una de las primeras tarjetas de crédito en adquirir un importante volumen de aceptación fue la del Diner's Club, literalmente «Club de Comidas». Su impulsor fue el norteamericano Frank McNamara, quien logró que varios restaurantes aceptaran el pago a crédito tras la entrega de una tarjeta personalizada que McNamara repartía entre sus mejores clientes. De hecho, el uso más habitual de las tarjetas de crédito en sus primeras décadas de existencia era el pago de comidas y cenas por parte de los vendedores ambulantes.

Por ejemplo, y para el caso de una tarjeta numerada del siguiente modo:

$$1234\ 5678\ 9012\ 3452,$$

por el algoritmo de Luhn:

$$1\cdot 2 = 2$$
$$3\cdot 2 = 6$$
$$5\cdot 2 = 10 \Rightarrow 1+0 = 1$$
$$7\cdot 2 = 14 \Rightarrow 1+4 = 5 \text{ (o bien } 14-9=5)$$
$$9\cdot 2 = 18 \Rightarrow 1+8 = 9$$
$$1\cdot 2 = 2$$
$$3\cdot 2 = 6$$
$$5\cdot 2 = 10 \Rightarrow 1+0 = 1$$
$$2+6+1+5+9+2+6+1 = 32$$
$$2+4+6+8+0+2+4+2 = 28$$
$$32+28 = 60$$

El resultado es 60; múltiplo de 10. Por tanto el código de la tarjeta es un código correcto.

Otro modo de implementar el algoritmo de Luhn es el que sigue. Un número de tarjeta ABCD EFGH IJKL MNOP es correcto si el doble de la suma de los dígitos que ocupan un lugar impar más la suma de los dígitos que ocupan un valor par más el número de dígitos en posición impar mayores de 4 es múltiplo de 10. Es decir, $2(A+C+E+G+I+K+M+O)+(B+D+F+H+J+L+N+P)+$ número de dígitos en posición impar mayores que $4 \equiv 0$ (mód. 10).

Aplicando esta segunda versión del algoritmo al ejemplo anterior:

$$1234\ 5678\ 9012\ 3452$$

$$2\cdot(1+3+5+7+9+1+3+5)+(2+4+6+8+0+2+4+2)+4 =$$
$$= 100 \equiv 0 \text{ (mód. 10)}.$$

De nuevo se constata que el número es un número de tarjeta correcto. Hemos visto que los códigos de las tarjetas de crédito siguen un patrón matemático muy estricto.

APLICATIVO EXCEL PARA EL CÁLCULO DEL DÍGITO DE CONTROL DE UNA TARJETA DE CRÉDITO

El número asociado a una tarjeta de crédito consta de 15 dígitos más un código de control, agrupados en cuatro series de cuatro dígitos cada serie. El dígito de control se calcula según el algoritmo que queda reflejado en la tabla siguiente.

															D.C.
Nº. Tarjeta	5	5	2	1	4	5	7	2	6	1	6	2	3	6	2	4	
dígitos utilizados	**5**	**2**	**1**		**4**	**5**	**7**	**2**	**6**	**1**	**6**	**2**	**3**	**6**	**2**		
dígitos posición par		2				4		7		6		6		3		2	
Suma dígitos posición par																	30
Número de dígitos de lugar par mayores que 4																	3
Suma de las dos cantidades anteriores																	33
Dígitos posición impar	**5**		**1**			**5**		**2**		**1**		**2**		**6**			
Suma dígitos posición impar																	22
Sumar los dos resultados anteriores más 1																	56
Resto de dividir el resultado anterior por 10																	6
El D.C. es 0 si el resultado anterior es 0 en caso contrario es 10 menos el resultado anterior																	**4**

¿Sería posible recuperar un dígito perdido? Sí, siempre que se trate de un número de tarjeta válido. Averigüemos el valor de X en el número 4539 4512 03X8 7356.

Se empieza por multiplicar por 2 los números de las posiciones impares (4-3-4-1-0-X-7-5) y dejándolos con un solo dígito.

$$4 \cdot 2 = 8$$
$$3 \cdot 2 = 6$$
$$4 \cdot 2 = 8$$
$$1 \cdot 2 = 2$$
$$0 \cdot 2 = 0$$
$$X2 = 2X$$
$$7 \cdot 2 = 14,\ 14 - 9 = 5$$
$$5 \cdot 2 = 10,\ 10 - 9 = 1.$$

Sumamos los dígitos de las posiciones pares y los nuevos de las posiciones impares y se obtiene:

$$30+41+2X=71+2X$$

71+2X, que sabemos que debe ser múltiplo de 10.

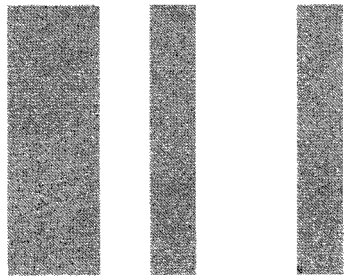
Si el valor de X fuera mayor de 4 (e inferior a 10) tendríamos que 2X estaría comprendido entre 10 y 18. El valor de 2X reducido a un solo dígito es $2X-9$, con lo que la suma anterior sería $71+2X-9$. El único valor de X que hace de la expresión múltiplo de 10 es 9. Si, por el contrario, X fuera inferior o igual a 4, se oberva que no hay ningún valor que verifique que $71+2X$ sea múltiplo de 10.

En consecuencia, el dígito perdido es el 9 y el número completo de la tarjeta de crédito, 4539 4512 0398 7356.

Los códigos de barras

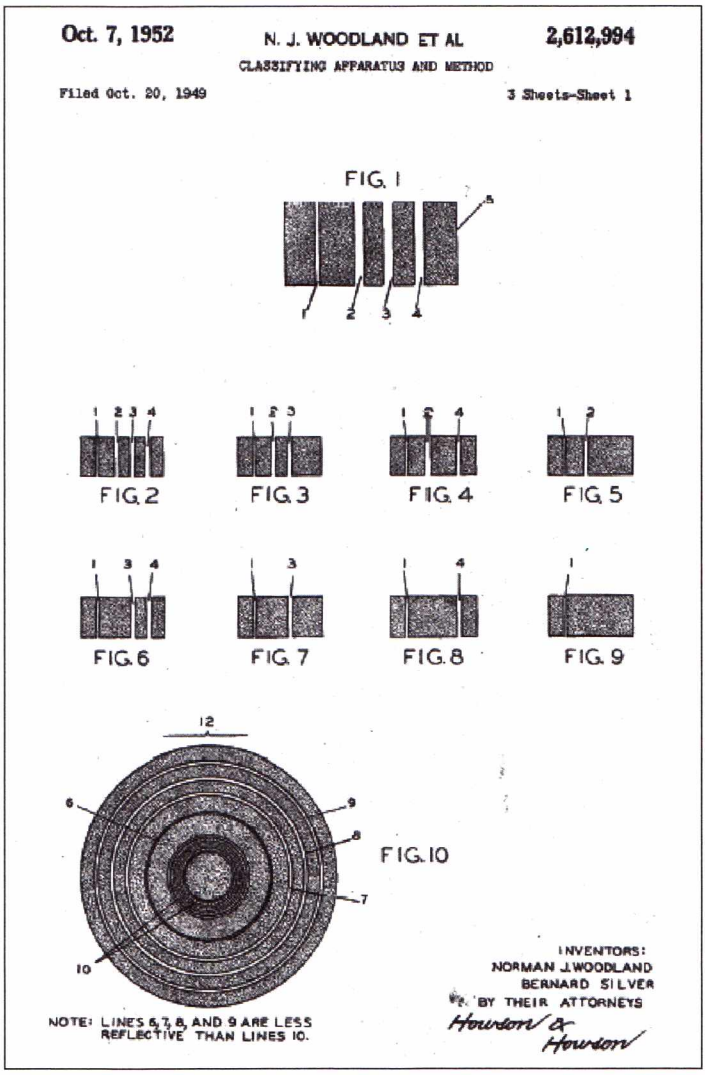
El primer sistema de código de barras fue patentado el 7 de octubre de 1952 por los norteamericanos Norman Woodland y Bernard Silver. Aunque el principio era el mismo, su aspecto no: en lugar de las familiares barras, Woodland y Silver pensaron en círculos concéntricos. El primer uso oficial de un código de barras en un comercio se dio en 1974, en un establecimiento de Troy, Ohio.

El código de barras moderno consiste en una serie de barras negras (que se codifican en sistema binario como unos) y los espacios en blanco que quedan entre ellas (que lo hacen como ceros), de diferentes anchos ambos, y que identifican artículos físicos. Los códigos suelen imprimirse en etiquetas y se leen mediante un dispositivo óptico. Este dispositivo, parecido a un escáner, mide la luz reflejada y deriva de ella la clave alfanumérica, que a continuación transmite a un ordenador. Existen numerosos estándar de códigos de



Correspondencia entre el grosor de las barras y el del espacio que quede entre ellas y los dígitos binarios.

barras, entre ellos: Code 128, Código 39, Codabar, EAN (apareció en 1976 en versiones de 8 y 13 dígitos) o UPC (código universal de producto, usado principalmente en Estados Unidos y disponible en versiones de 12 y 8 dígitos). El código más habitual es el EAN en su versión de 13 dígitos, y es el que se examinará aquí. A pesar de esta variedad de normas, el código de barras permite que todo producto pueda ser identificado en cualquier parte del mundo, de manera ágil y sin demasiado margen para el error.



La patente del sistema de anillos concéntricos de Woodland y Silver que prefigura los modernos códigos de barras.

APLICATIVO EXCEL PARA EL CÁLCULO DEL DÍGITO DE CONTROL DE CÓDIGO EAN-13

Un código de barras del tipo EAN-13 es un número formado por 12 dígitos más un decimotercero llamado código de control.

Los 12 dígitos se distribuyen en cuatro grupos:

País		Empresa					Producto					D.C.
8	4	1	1	3	4	9	0	4	5	1	2	6

El algoritmo de cálculo consta de los siguientes pasos:

	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
3	País			Empresa						Producto						D.C.
4	3	4		1	0	3	5	9		1	2	5	9	2		2
5																
6	Suma de los dígitos de lugar impar															27
7	Suma de los dígitos de lugar par y el resultado multiplicado por 3															51
8	Suma de los dos resultados anteriores															78
9	Resto de dividir por 10 el resultado anterior															8
10	El D.C es 0 o 10 menos el resultado anterior															2

Usando el entorno Excel este algoritmo se escribiría de la manera siguiente:

	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
3	País			Empresa						Producto						D.C.
4	3	4		1	0	3	5	9		1	2	5	9	2		=R10
5																
6	Suma de los dígitos de lugar impar															=C4+F4+H4+J4+M4+O4
7	Suma de los dígitos de lugar par y el resultado multiplicado por 3															=(D4+G4+I4+L4+N4+P4)*3
8	Suma de los dos resultados anteriores															=R6+R7
9	Resto de dividir por 10 el resultado anterior															=RESIDUO(R8;10)
10	El D.C es 0 o 10 menos el resultado anterior															=SI(R9=0;0;10-R9)

El código EAN-13

El término EAN procede de las siglas *European Article Number* («Número Europeo de Artículo») y su creación se remonta al año 1976. En la actualidad constituye uno de los estándares de mayor implantación a lo largo y ancho del globo. Los códigos EAN constan, habitualmente, de 13 dígitos representados mediante barras negras y espacios blancos que, de manera conjunta, determinan un código binario de fácil lectura. El EAN-13 representa esos 13 dígitos por medio de 30 barras. Los dígitos se encuentran distribuidos en tres partes: la primera, que consta de 2 o 3 números, indica el código del país; la segunda, que tiene 9 o 10 números, identifica la empresa y el producto; la tercera, de tan sólo un dígito, actúa como código de control. Para un código ABCDEFGHIJKLM estas partes se descomponen del modo siguiente:

- Los dos primeros (AB) forman el código del país de origen del producto. A España le corresponde el código 84, mientras que para Francia, por ejemplo, es el 83.
- Los cinco siguientes (CDEFG) identifican a la empresa productora.
- Los otros cinco (HIJKL) indican el código del producto que ha sido asignado por la empresa.
- El último (M) es el dígito de control. Para calcularlo se tienen que sumar los dígitos situados en posición impar, empezando por la izquierda y sin contar el de control. Al valor resultante se le añade tres veces la suma de los dígitos situados en las posiciones pares. El dígito de control es el valor que hace de la suma hallada anteriormente un múltiplo de 10. Como puede verse, el sistema de control recuerda enormemente al empleado para el caso de las tarjetas de crédito.

Verifiquemos si el código siguiente es correcto.

8413871003049

$$8+1+8+1+0+0+3(4+3+7+0+3+4)=18+3(21)=18+63=81.$$

El dígito de control ¿correcto? debería ser $90-81=9$.

El modelo matemático del algoritmo se fundamenta en aritmética modular módulo 10, de la siguiente forma.

ABCDEFGHIJKLM, se llama N al valor de la expresión:

$$A+C+E+G+I+K+3(B+D+F+H+J+L)=N$$

y n al valor de N en módulo 10. El dígito de control M viene determinado como $M=10-n$.

En el ejemplo mostrado tenemos que $81\equiv 1$ (mód. 10), luego el dígito de control será, efectivamente, $10-1=9$.

El algoritmo anterior puede enunciarse de manera equivalente utilizando el dígito de control en los cálculos. Puede verificarse así la corrección del código de control sin calcularlo previamente, según el algoritmo siguiente.

$$A+C+E+G+I+K+3(B+D+F+H+J+L)+M\equiv 0 \text{ (mód. 10)}.$$

Por ejemplo, y para el código

5701263900544

$$5+0+2+3+0+5+3(7+1+6+9+0+4)+4=100.$$

$$100\equiv 0 \text{ (mód. 10)}.$$

El código es correcto.

A título de curiosidad, vamos a intentar determinar el valor de un dígito perdido de un código de barras. En concreto, el representado por X en el código siguiente:

401332003X497

Componemos los dígitos según el algoritmo y llamamos X al dígito que desconocemos.

$$4+1+3+0+3+4(0+3+2+0+X+9)+7=64+3X\equiv 0 \text{ (mód. 10)}.$$

En módulo 10 tenemos la igualdad

$$4+3X\equiv 0 \text{ (mód. 10)}.$$

$$3X\equiv -4+0\equiv -4+10\cdot 1=6 \text{ (mód. 10)}.$$

Nótese que 3 tiene inverso ya que $\text{mcd}\,(3,10)=1$.

Se observa que X debe ser 2. Luego el código correcto es

$$4013320032497.$$

LOS CÓDIGOS QR

En 1994, la empresa japonesa Denso-Wave desarrolló un sistema gráfico de codificación para identificar las partes de los coches en una cadena de montaje. El sistema, llamado QR por la rapidez con la que podía ser leído por ingenios diseñados para tal fin (el nombre QR corresponde a las siglas del inglés *quick response*, «respuesta rápida»), acabó por extenderse más allá de las fábricas de coches y, a los pocos años, la mayoría de los teléfonos móviles de Japón era capaz de leer la información contenida en él al instante. El QR es un código de tipo matricial, formado por un número variable de cuadrados de color blanco o negro que, a su vez, se disponen en forma de un cuadrado de mayor tamaño. Los cuadrados representan un valor binario, 0 o 1, y por tanto, su funcionamiento se semeja mucho al de los códigos de barras, aunque los códigos bidimensionales de este tipo, en razón de su diseño, tienen una mayor capacidad de almacenamiento.

Un código QR de la universidad japonesa de Osaka de 37 filas.

Capítulo 5

Un secreto a voces: la criptografía de llave pública

La criptografía no escapó a la irrupción y posterior desarrollo de la computación. Emplear un ordenador para el cifrado de un mensaje es un proceso sustancialmente idéntico al del cifrado sin él, con tres diferencias básicas. La primera es que un ordenador puede programarse para simular el trabajo de una máquina convencional de cifrado de, por ejemplo, 1.000 rotores sin necesidad de construirla físicamente. En segundo lugar, un ordenador trabaja sólo con números binarios y, por tanto, todo cifrado se hará a ese nivel (aunque posteriormente la información numérica se descodifique de nuevo a texto). En tercer y último lugar, las computadoras poseen una enorme velocidad de cómputo y cálculo.

En la década de los años 70 se desarrollaron los primeros cifrados diseñados para aprovechar el potencial de los ordenadores, como, por ejemplo, *Lucifer*, un cifrado que dividía el texto en bloques de 64 bits y encriptaba parte de ellos mediante una compleja sustitución para luego reunirlos en un nuevo bloque cifrado de bits e ir repitiendo el proceso. El sistema necesitaba un ordenador con el programa de encriptado y una clave numérica para el emisor y el receptor. Una versión de 56 bits de *Lucifer* llamada DES fue introducida en Estados Unidos en 1976 y, a fecha de 2009, constituye todavía uno de los estándares de encriptación de dicho país.

La encriptación sin duda sacó partido de la capacidad de cómputo de los ordenadores, pero, al igual que sus antecesores milenarios, seguían expuestos al peligro de que un receptor no deseado se hiciera con las claves y, conocido el algoritmo de encriptación, lograra descifrar el mensaje. Esta debilidad básica de todo sistema «clásico» de criptografía es conocida como *el problema de la distribución de la clave.*

El problema de la distribución de la clave

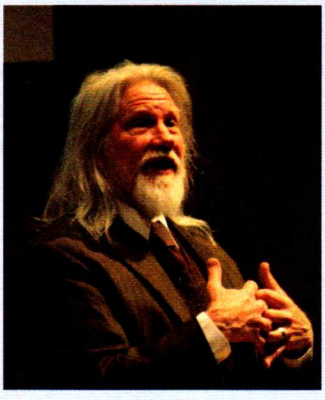
Desde que la comunidad criptográfica acordó que la protección de las claves, más que la del algoritmo, era el elemento fundamental que debía garantizarse para asegurar la seguridad del criptosistema, la implantación de cualquiera de estos

últimos debía enfrentarse al problema de cómo distribuir sus claves de forma segura. En el menor de los casos ello ocasionaba auténticos problemas logísticos, como por ejemplo a la hora de repartir los miles de libros de claves generados por un ejército de grandes dimensiones, o el hacerlo a centros de comunicaciones móviles que operan en circunstancias extremas como la tripulación de los submarinos o las unidades en el frente de batalla. No importa lo sofisticado que sea un sistema de encriptación «clásico»: todos ellos son vulnerables a la intercepción de sus claves respectivas.

El algoritmo de Diffie-Hellman

La noción de un intercambio seguro de claves puede parecer una contradicción: la transmisión misma de la clave es de por sí un mensaje, así que también debe encriptarse, y con una clave que debe haberse intercambiado previamente. Sin embargo, si el intercambio se plantea como un proceso comunicativo en varias fases, puede idearse una solución al problema, al menos en el plano teórico.

Supongamos qúe un emisor cualquiera llamado Jaime encripta un mensaje con una clave propia y lo remite a un receptor, Pedro. Éste encripta de nuevo el mensaje cifrado con otra clave propia y lo devuelve al emisor. Jaime descifra el mensaje con su clave y envía este nuevo mensaje, que ahora sólo está cifrado con la clave de Pedro, que procede a descifrarlo. El milenario problema del intercambio seguro de claves ha sido resuelto. ¿Es así en realidad? Pues no. De hecho, en todo algoritmo de cifrado complejo el orden en que se aplique la clave es fundamental, y hemos visto



LOS HOMBRES DETRÁS DEL ALGORITMO

Bailey Whitfield Diffie (en la ilustración) nació en 1944 en Estados Unidos. Matemático por el Massachusetts Institute of Technology (MIT), desde 2002 es director de seguridad y vicepresidente de Sun Microsystems, con sede en California. Por su parte, Monte Hellman, ingeniero, nació en 1945 y desempeñó su carrera profesional en IBM y en el MIT, donde conoció a Diffie.

que en nuestro ejemplo teórico Jaime tiene que descifrar un mensaje ya cifrado con otra clave. El resultado de invertir el orden de los cifrados resultaría un galimatías. La teoría no nos sirve en este caso, pero iluminó el camino que se debía seguir. En 1976 dos jóvenes científicos estadounidenses, Whitfield Diffie y Monte Hellman, dieron con un modo de que dos individuos intercambiaran mensajes cifrados sin tener por ello que intercambiar clave alguna. Este método se sirve de la aritmética modular, así como de las propiedades de los números primos de las operaciones que los implican. La idea es la siguiente:

1) Jaime elige un número cualquiera, que mantiene secreto. Llamaremos a este número N_{J1}.
2) Pedro elige otro número cualquiera, que también mantiene secreto. Llamaremos a este número N_{P1}.
3) A continuación, tanto Jaime como Pedro aplican sobre sus respectivos números una función del tipo $f(x) = a^x$ mód. p, siendo p un número primo conocido.
   - Jaime obtiene de dicha operación un nuevo número, N_{J2}, que esta vez sí envía a Pedro.
   - Pedro obtiene de dicha operación un nuevo número, N_{P2}, que envía a Jaime.
4) Jaime resuelve una ecuación del tipo $N_{P2}^{N_{J1}}$ (mód. p), y obtiene como resultado un nuevo número, C_J.
5) Pedro resuelve una ecuación del tipo $N_{J2}^{N_{P1}}$ (mód. p), y obtiene como resultado un nuevo número, C_P.

Aunque parezca asombroso, C_J y C_P serán iguales. Y ya se tiene la clave. Nótese que el único momento en el que tanto Jaime como Pedro se han intercambiado información ha sido al acordar la función $f(x) = a^x$ mód. p, y al enviarse N_{J2} y N_{P2}, que no son la clave y cuya eventual intercepción, por tanto, no compromete la seguridad del criptosistema. La clave de este sistema tendrá la forma general

$$a^{N_{J1} \cdot N_{P1}} \text{ en módulo } p.$$

Es también importante tener en cuenta que la función original tiene la particularidad de no ser reversible, es decir, conociendo tanto la función como el resultado de aplicarla a una variable x, resulta imposible (o muy difícil) obtener la variable x original.

A continuación, y para «fijar ideas», repetiremos el proceso con funciones y números concretos. La función escogida es, por ejemplo,

$$f(x) = 7^x \text{ (mód. 11)}.$$

1) Jaime escoge un número, N_{J1}, por ejemplo el 3, y calcula $f(x) = 7^x$ (mód. 11) obteniendo $f(3) = 7^3 \equiv 2$ (mód. 11).
2) Pedro escoge un número N_{P1}, por ejemplo el 6, y calcula $f(x) = 7^x$ (mód. 11) obteniendo $f(6) = 7^6 \equiv 4$ (mód. 11).
3) Jaime envía a Pedro su resultado, 2, y Pedro hace lo propio con el suyo, 4.
4) Jaime calcula $4^3 \equiv 9$ (mód. 11).
5) Pedro calcula $2^6 \equiv 9$ (mód. 11).

Este valor, 9, será la clave del sistema.

Jaime y Pedro han intercambiado tanto la función $f(x)$ como los números 2 y 4. ¿Qué información real aportan ambos datos a un posible espía? Supongamos que nuestro receptor inesperado conoce tanto la función como los números. Su problema es ahora resolver $7^{N_{J1}} = 2$ y $7^{N_{P1}} = 4$ en módulo 11, siendo N_{J1} y N_{P1} los números que tanto Jaime como Pedro mantienen en secreto. Si consigue averiguarlos, dispondrá de la clave sólo con resolver $a^{N_{J1}N_{P1}}$ en módulo p. La solución a este problema, por cierto, se denomina en matemáticas un *logaritmo discreto*. Por ejemplo, en el caso

$$f(x) = 3^x \text{ (mód. 17)}$$

se observa que $3^x = 15$ (mód 17) y, probando diferentes valores de x, se obtiene que $x = 6$ se verifica la relación $3^x = 15$.

Los algoritmos de esta tipología y el problema del logaritmo discreto no recibieron especial atención hasta el comienzo de la década de los años 90, y ha sido en estos últimos años cuando más se han desarrollado. En este ejemplo, se dice que 6 es el logaritmo discreto de 15 en base 3 con módulo 17.

La particularidad de este tipo de ecuaciones es, como se ha mencionado antes, que son difícilmente reversibles (o también, que son *asimétricas*). Para valores de p de más de 300 cifras y de a de más de 100, la solución –y, por tanto, la ruptura de la clave– se torna dificilísima.

VIRUS Y «PUERTAS TRASERAS»

Hasta el más seguro de los cifrados de clave pública depende de que la clave privada se guarde en secreto. En consecuencia, un virus que se instale en el sistema de un emisor, localice y transmita esa clave privada echa al traste el criptosistema.

En 1998 se supo que una empresa suiza líder en la elaboración y venta de productos criptográficos había incluido en ellos «puertas traseras» que detectaban las claves privadas de los usuarios y las enviaban de vuelta a la empresa. Parte de esa información se entregó al gobierno estadounidense, que a todos los efectos podía de esta manera monitorizar las comunicaciones entre los ordenadores infectados.

Este algoritmo es uno de los pilares de la criptografía moderna. Diffie y Hellman expusieron su idea en un Congreso Nacional de Informática, durante un seminario que sólo cabe calificar de histórico. El trabajo completo puede consultarse en su totalidad en www.cs.berkeley.edu/~christos/classics/diffiehellman.pdf, donde aparece bajo el título de *New Directions in Cryptography* («Nuevas direcciones en criptografía»).

El algoritmo de Diffie-Hellman demostró teóricamente la posibilidad de crear un método criptográfico que no necesitara un intercambio de claves, pero, paradójicamente, contaba con la comunicación pública de parte del proceso (el par de números iniciales que sirven para determinar la clave).

Dicho de otro modo, se había demostrado la viabilidad de un criptosistema cuyos emisores y receptores no tenían que encontrarse para establecer las claves. Pero todavía quedaban en pie ciertos inconvenientes: si Jaime desea enviar un mensaje a Pedro mientras éste está durmiendo, por ejemplo, deberá esperar a que el otro se despierte para llevar a cabo el proceso de generar la clave.

En el proceso de descubrir nuevos algoritmos de mayor eficacia, Diffie teorizó acerca de un criptosistema en el cual la clave de cifrado fuera distinta de la de descifrado y que, obviamente, una no pudiera derivarse nunca de la otra. En este criptosistema teórico, el emisor dispondría de dos claves: la de encriptación y la de desencriptación. De las dos, haría *pública* tan sólo la primera, para que todo aquel que quisiera enviarle un mensaje pudiera encriptarlo. Una vez recibido el mensaje, el emisor procedería a descifrarlo con la clave de desencriptación, que, obviamente, habría permanecido secreta. Ahora bien, ¿cómo se conseguía implementar este sistema?

Los primos acuden al rescate: el algoritmo RSA

En agosto de 1977 el conocido divulgador científico estadounidense Martin Gardner publicó en su columna de recreaciones matemáticas de la revista *Scientific American* un artículo titulado «Un nuevo tipo de cifrado que costaría millones de años descifrar». Tras explicar detalladamente los fundamentos del sistema de clave pública, hizo constar el mensaje cifrado así como la clave pública N empleada para ello:

$$N = 114.381.625.757.888.867.669.235.779.976.146.$$
$$612.010.218.296.721.242.362.562.561.842.935.706.935.245.733.$$
$$897.830.597.123.563.958.705.058.989.075.147.599.290.026.879.$$
$$543.541.$$

Gardner planteó a sus lectores el reto de descifrar el mensaje a partir de la información dada, e indicó como pista que la solución requeriría de factorizar N en sus componentes primos p y q. Como remate, Gardner prometió un premio de 100 dólares (cifra muy suculenta en la época) a quien fuera el primero en responder correctamente. Todo aquel que deseara más información acerca del cifrado en cuestión, escribió Gardner, podía enviar una petición al respecto al Laboratorio de Informática del MIT a la atención de sus creadores Ron Rivest, Adi Shamir y Len Adelman.

La respuesta correcta no se recibió hasta 17 años más tarde, y para hallarla se necesitó de la colaboración de más de 600 personas. Las claves resultaron ser $p = 32.769.132.993.266.709.549.961.988.190.834.461.413.177.642.967.992.942.539.798.288.533$ y $q = 3.490.529.510.847.650.949.147.849.619.903.898.133.417.764.638.493.387.843.990.820.577$, y el mensaje cifrado, «*the magic words are squeamish ossifrage*» («las palabras mágicas son un quebrantahuesos impresionable»).

El algoritmo presentado por Gardner se conoce como RSA, acrónimo de los apellidos Rivest, Shamir y Adelman. Se trata de la primera implementación práctica del modelo de clave pública planteado por Diffie y se emplea asiduamente hoy en día. La seguridad que ofrece es extrema por cuanto el proceso de descifrado es increíblemente laborioso aunque, como se verá más adelante, no imposible. A continuación se ofrecen los fundamentos del sistema de manera básica, sin entrar en excesivos tecnicismos.

El algoritmo RSA, en detalle

El algoritmo RSA se fundamenta en ciertas propiedades de los números primos, que los lectores interesados podrán consultar en los anexos del presente volumen. Aquí nos limitaremos a exponer las asunciones básicas que lo fundamentan.

- El conjunto de números menores que n que son asimismo primos con n se denomina *función de Euler* y se expresa como $\varphi(n)$.
- Si $n = pq$ siendo p y q dos números primos, entonces $\varphi(n) = (p-1)(q-1)$.
- Por el «pequeño teorema de Fermat», se sabe que si p es un número primo y a es un entero coprimo con p" (es decir, si $mcd(a,p)=1$) entonces se cumple la ecuación $a^{p-1} \equiv 1$ (mód. p).
- Por el teorma de Euler, si $mcd(n,a)=1$, entonces $a^{\varphi(n)} \equiv 1$ (mód.1).

Tal y como se ha mencionado, el sistema se denomina de clave pública por el hecho de que la clave de encriptación se pone en conocimiento de los emisores interesados en enviar mensajes. Cada receptor posee una clave pública propia. Se parte de la base de que los mensajes se transmitirán traducidos a números, ya sea mediante un código ASCII o de cualquier otro modo que se desee.

En primer lugar, Jaime genera un valor n como producto de dos números primos p y q ($n = p \cdot q$) y se escoge un valor e de manera que el mcd $(\varphi(n), e) = 1$. Recordemos que $\varphi(n) = (p-1)(q-1)$. Los datos que se hacen públicos son el valor de n y el valor de e (en ninguna circunstancia proporcionaremos los valores p y q). El par (n,e) es la clave pública del sistema, y los valores p y q se conocen como *números RSA*. En paralelo, Jaime calcula el único valor d en módulo $\varphi(n)$ que verifica $d \cdot e = 1$, es decir, el inverso de e en módulo $\varphi(n)$. Se sabe que este inverso existe porque mcd $(\varphi(n), e) = 1$. Este valor d es la clave privada del sistema. Por su parte, Pedro emplea la clave pública (n,e) para encriptar el mensaje m mediante la función $M = m^e$ (mód. n). Recibido el mensaje encriptado M, Jaime realiza la operación $M^d = (m^e)^d$ (mód. n), Esta expresión equivale a $M^d = (m^e)^d = m$ (mód. n), lo que demuestra que el mensaje puede descifrarse.

Vamos ahora a aplicar el procedimiento expuesto con valores numéricos concretos.

- Sea $p = 3$ y $q = 11$, se tiene que $n = 33$. $\varphi(33) = (3-1) \cdot (11-1) = 20$. Jaime escoge e de manera que no tenga divisores comunes con 20, por ejemplo $e = 7$. La clave pública de Jaime es (33,7).

- Entre tanto, Jaime ha calculado una clave privada d que será el inverso de 7 módulo 20, es decir, $7 \cdot 3 \equiv 1$ (mód. 20), y con ello $d = 3$.
- Pedro se hace con la clave pública y desea enviarnos el mensaje «9», o sea, $m = 9$. Para cifrarlo hace uso de la clave pública de Jaime y resuelve:

$$9^7 = 4.782.969 \equiv 15 \text{ (mód. 33)}.$$

El mensaje cifrado es «15». Pedro nos envía el mensaje.
Jaime recibe el mensaje «$M = 15$», y lo descifra operando:

$$15^3 = 3.375 \equiv 9 \text{ (mód. 33)}.$$

El mensaje ha sido descifrado correctamente.

A medida que se escogen primos p, q de mayor tamaño, la dificultad de implementar el algoritmo RSA aumenta, hasta el punto que se hace necesario el uso del ordenador para el cálculo de las congruencias. Por ejemplo, sean $p = 23$ y $q = 17$, se tiene que $n = 391$. La clave pública resultante para $e = 3$ es (391,3). En consecuencia, $d = 235$. Para un mensaje llano como «34», la operación de descifrado es:

$$204^{235} \equiv 34 \text{ (mód. 391)}.$$

Obsérvese el grado de la potencia y piénsese en la gigantesca capacidad de cálculo necesaria para hallar la congruencia.

¿Por qué deberíamos confiar en el algoritmo RSA?

Un eventual espía conoce los valores de n y de e por el hecho de que son públicos. Para descifrar el mensaje necesita, además, del valor de d, la clave privada. Como se ha mostrado en el ejemplo anterior, el valor d se genera a partir de n y de e. ¿Dónde radica la seguridad? Recordemos que para construir d es preciso conocer $\varphi(n) = (p-1)(q-1)$, en particular, p y q. Para ello «basta» con descomponer n como producto de dos números primos p y q. El problema para el espía es que factorizar un número grande como producto de dos números primos estriba en un proceso lento y laborioso. Si n es lo suficientemente «grande» (del orden de más de 100 dígitos), no hay manera conocida de

encontrar p y q en un período de tiempo razonable. En la actualidad, los primos empleados en el cifrado de mensajes de mayor confidencialidad superan los 200 dígitos.

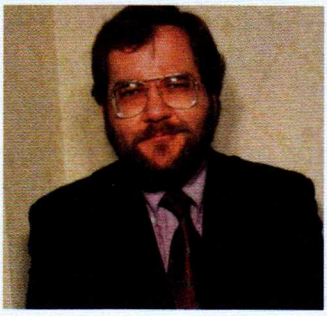
Una privacidad razonable

El algoritmo RSA consume mucho tiempo de computación y ordenadores de gran capacidad. Hasta los años 80 sólo los gobiernos, el ejército y las grandes empresas tenían ordenadores suficientemente potentes para trabajar con RSA y, en consecuencia, disfrutaban de un monopolio de facto sobre la encriptación de máximo nivel. En el verano de 1991 Phil Zimmermann, físico estadounidense y activista en pro de la privacidad, ofreció de forma gratuita el sistema PGP (siglas del inglés *Pretty Good Privacy*, «Privacidad razonable»), un algoritmo de encriptación capaz de funcionar en ordenadores domésticos. El PGP emplea la codificación simétrica clásica –factor que le confiere mayor rapidez– pero cifra las claves con un encriptado asimétrico RSA.

Zimmermann explicó las razones de su medida en una carta abierta que merece ser citada, al menos parcialmente, por la relevancia de sus reflexiones en el contexto del mundo que nos rodea:

> «Es personal. Es privado. Y sólo a ti te importa. Puedes estar organizando una campaña electoral, hablando de tus impuestos, o teniendo una aventura. O puede que estés haciendo algo que piensas que no debería ser ilegal, pero lo es. Por todo esto, no quieres que tu correo electrónico privado o tus documentos confidenciales sean leídos por nadie más. No hay nada de malo en mantener tu privacidad. La privacidad es uno de los derechos que establece la Constitución [de Estados Unidos] (...) Nos movemos hacia un futuro en el que la nación [Estados Unidos] será atravesada por redes de datos compuestas por cable de fibra óptica de alta capacidad, uniendo conjuntamente todos nuestros, cada vez más, omnipresentes ordenadores personales. El correo electrónico será lo normal, no la novedad como lo es hoy en día. El gobierno protegerá nuestros correos electrónicos con protocolos de encriptación designados por él mismo. Probablemente la mayoría de la gente esté de acuerdo con esto. Pero quizás algunos preferirán sus propias medidas de protección. (...) Si la privacidad está fuera de la ley, sólo los que están fuera de la ley tendrán privacidad. Las agencias de inteligencia

SEGURIDAD PARA TODOS



Phil Zimmermann, nacido en 1954, es un físico e informático estadounidense que ha protagonizado una lucha política en pro de la extensión de la criptografía moderna al ámbito privado. Además del sistema PGP, en 2006 creó Zfone, un programa de comunicación por voz por Internet y es presidente de la Open PGP Alliance, un *lobby* a favor del *software* de código abierto.

tienen acceso a una buena tecnología criptográfica. Así como los grandes traficantes de armas y de drogas. También los contratistas de defensa, las compañías petrolíferas y otras corporaciones gigantes. Pero la mayoría de la gente corriente, y de las organizaciones políticas de la oposición, no tenían acceso a tecnología criptográfica militar de clave pública. Hasta ahora.

PGP permite a la gente tener su privacidad en sus propias manos. Hay una creciente necesidad social de privacidad. Por eso lo escribí.»

De las reflexiones de Zimmerman se desprende que el precio a pagar por vivir en la era de la información es ver amenazadas nuestras tradicionales nociones de privacidad. En consecuencia, una adecuada comprensión de los mecanismos de codificación y encriptación que nos rodean no sólo nos hace más sabios, sino que pueden acabar resultando de enorme utilidad a la hora de proteger un bien tan preciado.

El uso de PGP se ha ido extendiendo desde su creación y que constituye la más importante herramienta criptográfica privada disponible a principios del siglo XXI.

Autenticación de mensajes y claves

Los diferentes sistemas de encriptación de clave pública –o mixtos de clave pública y privada, como el PGP– aseguran un alto grado de confidencialidad en la transmisión de información. Sin embargo, la seguridad de un sistema de comunicaciones complejo como Internet no reside únicamente en la confidencialidad.

Con anterioridad a la llegada de las modernas tecnologías de la comunicación, la gran mayoría de los mensajes procedían de fuentes conocidas, tales como la familia, los amigos o un puñado de relaciones profesionales. Hoy en día, sin embargo, cada

individuo se ve sometido a un auténtico alud de comunicaciones procedente de una miríada de fuentes. La autenticidad de estas comunicaciones es muy a menudo imposible de determinar, con todos los problemas que se derivan de ello. ¿Cómo evitar, por ejemplo, que alguien falsifique la dirección de origen de un correo electrónico?

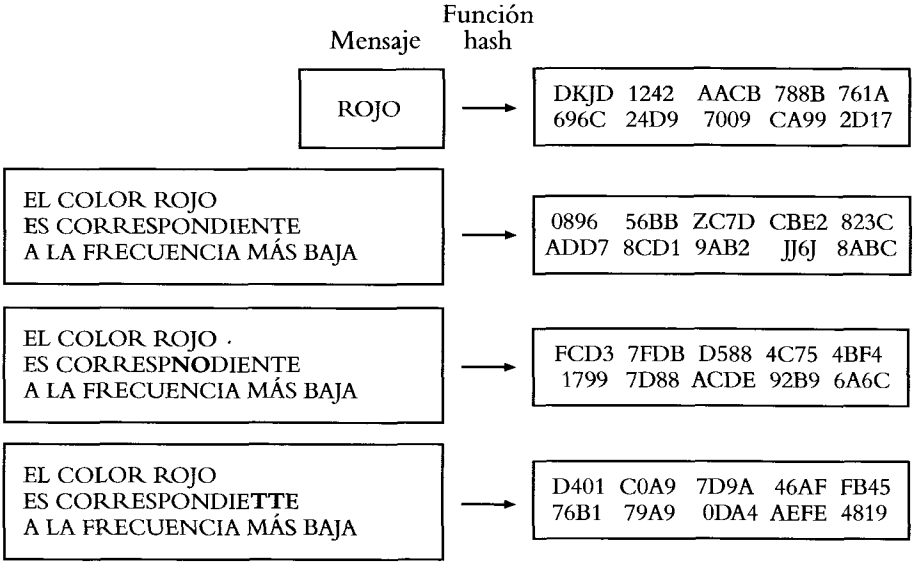
Los propios Diffie y Hellman propusieron un modo muy ingenioso de emplear la encriptación de clave pública para acreditar el origen de un mensaje. En un criptosistema de este tipo, el emisor cifra el mensaje con la clave pública del receptor, quien a continuación emplea su propia clave privada para descifrar aquél. Diffie y Hellman se percataron de que el algoritmo RSA y otros similares exhibía una interesante simetría: la clave privada podía emplearse también para cifrar un mensaje, y la pública, para descifrarlo. Esta operación no provee de seguridad alguna –la clave pública está al alcance de todos–, pero sí asegura al receptor que el mensaje proviene de un emisor en concreto: el propietario de la clave privada. Para autenticar al emisor de un mensaje es suficiente, en teoría, con que al proceso de encriptación normal se le añada otro del modo siguiente:

1) El emisor encripta un mensaje con la clave pública del receptor. Este primer paso asegura la confidencialidad.
2) El emisor encripta de nuevo el mensaje, esta vez con su clave privada. De este modo, el mensaje queda autenticado o *firmado*.
3) El receptor utiliza la clave pública del emisor para deshacer la encriptación del paso 2. El origen del mensaje queda así *verificado*.
4) El receptor emplea ahora su clave privada para deshacer la encriptación del paso 1.

Las funciones *hash*

Uno de los problemas de este esquema teórico es que la encriptación de clave pública requiere una capacidad de computación considerable, y repetir el proceso con el fin de firmar y verificar los mensajes resultaría muy costoso. Es por ello que, a la práctica, la firma de un mensaje se lleva a cabo mediante recursos matemáticos conocidos como *funciones* o *algoritmos* hash. Estos algoritmos generan, a partir del mensaje original, una cadena sencilla de bits (de ordinario, 160) llamada *hash*, y tienen la interesante propiedad de hacerlo de forma que la probabilidad de que a distintos mensajes se les asocie un mismo *hash* sea prácticamente nula. Asimismo, es prácticamente imposible deshacer el proceso y obtener el mensaje original a

partir de su *hash*. El *hash* de un mensaje cualquiera lo encripta el emisor con su clave privada y se envía junto con el mensaje cifrado de manera convencional. El receptor desencripta el mensaje que contiene el *hash* con la clave pública del emisor. A continuación, y dado que conoce la función *hash* empleada por aquél, aplica sobre el mensaje dicha función y coteja ambos *hash*. Si coinciden, la identidad del emisor queda verificada, y además está seguro de que nadie ha manipulado el mensaje original.



Pequeñísimos cambios en el contenido del mensaje genera «hashes» totalmente distintos. De este modo, el receptor puede estar seguro de que el texto no ha sido manipulado.

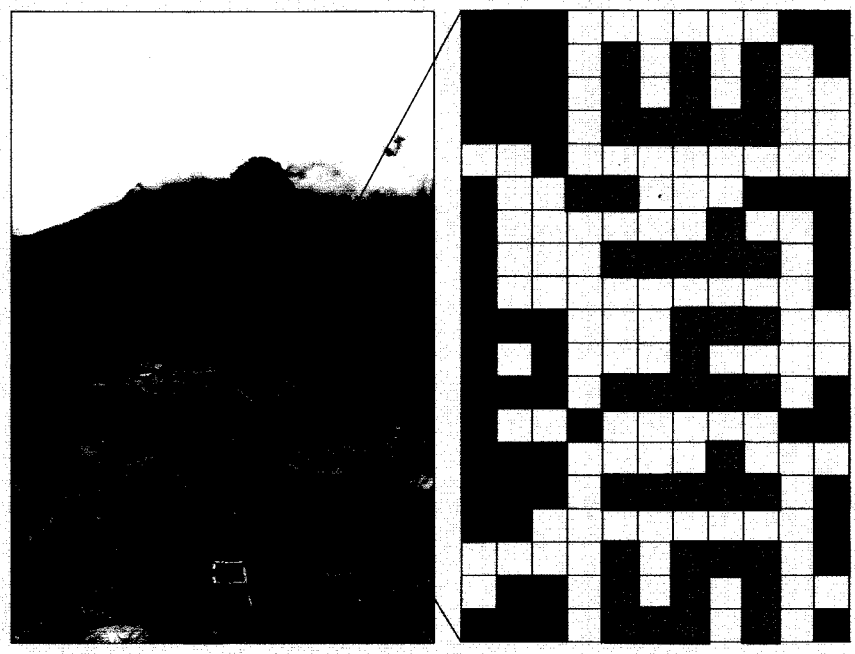
Los certificados de clave pública

Sin embargo, el problema más importante al que se enfrenta un criptosistema de clave pública reside no en la autenticación de los mensajes, sino en la de las claves públicas mismas.¿Cómo saben emisor y receptor que las claves públicas del otro son, en efecto, las correctas? Supongamos que un espía engaña al emisor dándole su propia clave pública, haciéndole creer que se trata de la del receptor. Si el espía logra interceptar un mensaje puede emplear ahora su clave privada para desencriptarlo. Para evitar ser detectado, el espía emplea la clave pública del receptor para encriptar nuevamente el mensaje y enviarlo a su destinatario original.

Es por ello que existen instituciones, tanto públicas como privadas, dedicadas a la certificación independiente de claves públicas. Un certificado de este tipo contiene, aparte de la clave correspondiente, información sobre el receptor y una fecha de caducidad. Los detentores de este tipo de claves hacen públicos sus certificados a las partes, que pueden ahora emplearlas e intercambiarlas con un cierto grado de seguridad.

ESTEGANOGRAFÍA DIGITAL

Aunque resulte en apariencia paradójico, el desarrollo de las nuevas tecnologías ha generado un auténtico *revival* de la esteganografía. Un archivo convencional de audio consiste en fragmentos de 16 bits reproducidos a una ratio de 44.100 por segundo. Resulta muy sencillo emplear alguno de esos bits para transmitir un mensaje secreto sin que un oyente perciba diferencia acústica alguna. Otro tipo de archivos que también permite este ingenioso sistema de transmisión son los de imagen.



Un ejemplo de esteganografía digital: el número pi hasta su cuarto decimal está escondido en un pequeño fragmento de la imagen. A la izquierda, la foto, aparentemente normal, y a la derecha, los píxeles de un fragmento que esconden la cifra 3,1415.

Pero ¿es seguro comprar en Internet?

La mayoría de espías o *hackers* tienen poco interés en los mensajes que la gente ordinaria se intercambia, con una notable excepción: el número de sus tarjetas de crédito. El criptosistema que rige la transmisión de tan delicado fragmento de información (o «capa», en la jerga informática) se conoce como TLS (del inglés *Transport Layer Security*, o «Seguro de transporte de capa») y fue desarrollado por la empresa de *software* Netscape en 1994 y adoptado como estándar dos años después.

El protocolo TLS combina clave pública y simétrica en un proceso bastante complejo que se ofrece aquí de forma resumida. En primer lugar, el navegador de Internet del comprador comprueba que el vendedor *online* dispone de un certificado de clave pública válido. Si es el caso, emplea esta clave pública para encriptar una segunda clave, esta vez simétrica, que remite al vendedor. Éste emplea su clave privada para desencriptar el mensaje y hacerse con la clave simétrica, que será la empleada para cifrar todo el proceso de intercambio de información. En consecuencia, para hacerse con el número de tarjeta de crédito en una transacción *online* cualquiera, un espía deberá penetrar no uno, sino dos criptosistemas.

Capítulo 6

Un futuro cuántico

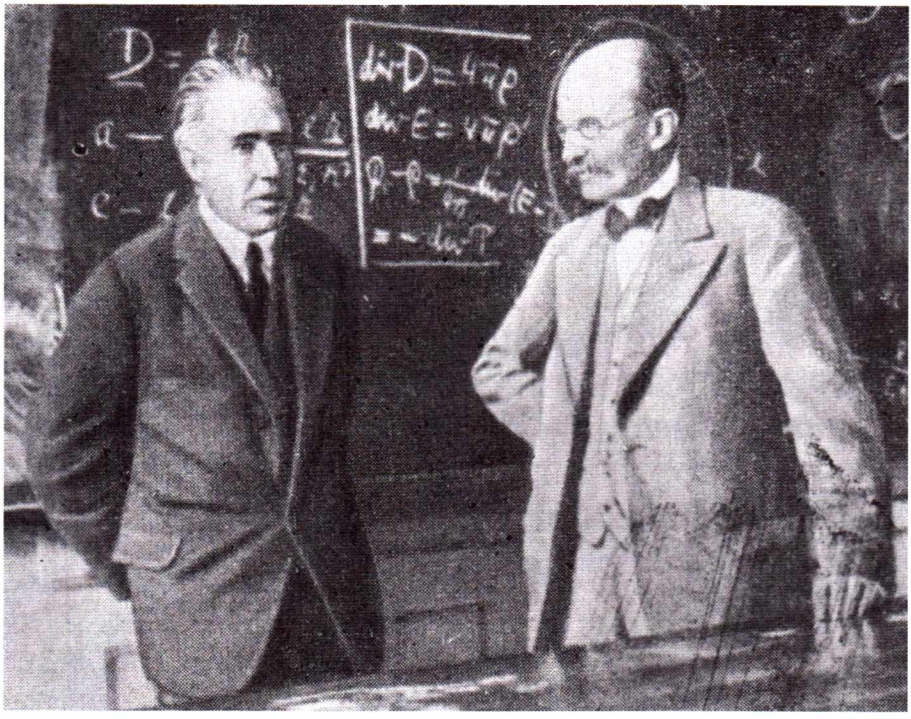
Según palabras de Phil Zimmermann, citadas en *Los códigos secretos* del divulgador Simon Singh, «en la criptografía moderna es posible crear cifras que están realmente fuera del alcance de todas las formas conocidas de criptoanálisis». Como ya se ha comentado, tratar de romper por fuerza bruta los algoritmos de encriptación como RSA o DES e incluso sistemas mixtos como el PGP está más allá de la capacidad de cómputo del más rápido de los ordenadores actuales. ¿Cabe pensar en algún tipo de atajo matemático que permita a los espías del futuro reducir la complejidad del criptoanálisis? Aunque esta posibilidad no puede descartarse, nadie la considera demasiado probable. ¿Tendrá Zimmermann razón? ¿Se ha resuelto, por fin, el conflicto milenario entre criptógrafos y criptoanalistas?

La computación cuántica

La respuesta es que «no exactamente». En las últimas décadas del siglo pasado, la *computación cuántica*, una nueva y revolucionaria forma de diseñar y operar con ordenadores, todavía circunscrita al ámbito teórico, amenaza con aumentar hasta tal punto la potencia de cálculo de las máquinas que descifrar por prueba y error los algoritmos actuales de encriptación se convertiría en un juego de niños.

Esta revolución tecnológica se apoya en la *mecánica cuántica*, el edificio teórico levantado a principios del siglo pasado por científicos como el danés Niels Bohr (1885-1962), los alemanes Max Planck (1858-1947) y Werner Heisenberg (1901-1976), y el austríaco Erwin Schrödinger (1887-1961), entre otros. La visión del universo que postula la mecánica cuántica resulta tan profundamente contraintuitiva que Albert Einstein se vio impelido a alzar su voz en contra de ella con una frase que se ha hecho célebre: «Dios no juega a los dados». A pesar de los reparos de Einstein, la mecánica cuántica es una teoría física que ha sido puesta a prueba con éxito en infinidad de ocasiones y cuya validez está fuera de toda duda: la comunidad científica en pleno asume que, en el ámbito macroscópico –es decir, el universo de las estrellas, las casas– nuestro entorno sigue las reglas de la física clásica tradicional, pero en el microscópico –el reino de las partículas subatómicas

como los quarks, los fotones, los electrones, etc.– quien manda es la mecánica cuántica y sus asombrosas paradojas. Sin las herramientas de esta teoría no habrían reactores nucleares ni lectores láser; no habría manera de explicar ni el brillo del Sol ni el funcionamiento del ADN.

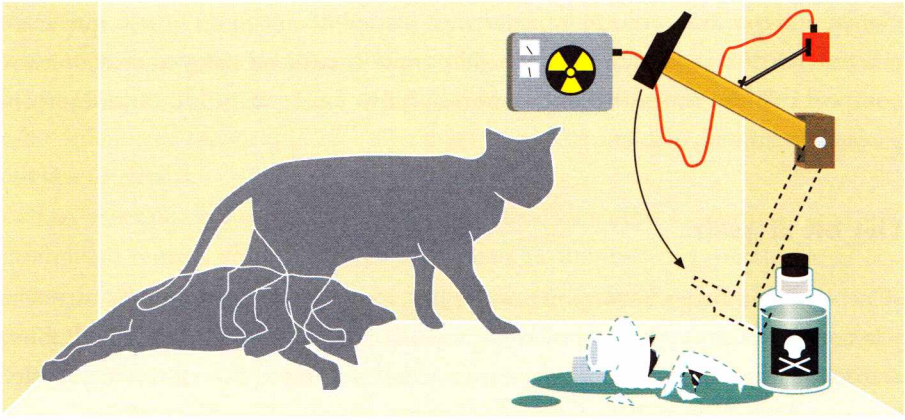


Niels Bohr (a la izquierda) junto a Max Planck, padres de la física cuántica, en una fotografía realizada en 1930.

El gato que no estaba ni vivo ni muerto

En un seminario de física cuántica celebrado en 1958, Bohr llegó a opinar sobre la propuesta de uno de los ponentes del modo siguiente: «Todos estamos de acuerdo en que su teoría es de locos. Lo que nos mantiene divididos al respecto es si es lo bastante de locos como para que pueda ser verdadera». ¿Cuán «de locos» es, en realidad, la mecánica cuántica? Consideremos, por ejemplo, el concepto de superposición de estados. Se dice que una partícula presenta una *superposición de estados* cuando ocupa, *a la vez*, más de una posición, o posee, *simultáneamente*, cantidades distintas de energía. Cuando un observador mide alguna de estas variables, *y no*

antes, la partícula *decide*, de un modo misterioso, adoptar una posición u otra o poseer una cantidad de energía u otra. El propio Schrödinger ideó un experimento imaginario, el del «gato de Schrödinger», que ilustra esta noción en apariencia extravagante. Imagínese un felino del tipo mencionado depositado en una caja sellada y opaca. En el interior de la caja se coloca un recipiente de gas venenoso conectado por un dispositivo a una partícula radiactiva de modo que, si ésta se desintegra, el gas escapa del recipiente y el gato muere envenenado. La partícula en cuestión tiene un 50% de probabilidades de desintegrarse durante un período de tiempo determinado. La totalidad del sistema, al depender del comportamiento de una única partícula, está sometido a las leyes de la física cuántica.



El gato de Schrödinger es un experimento imaginario que ilustra con gran claridad el concepto físico de superposición de estados.

Supóngase ahora que ya se ha cumplido dicho período de tiempo. La pregunta es: ¿Está el gato vivo o muerto? O, en la jerga de la mecánica cuántica, ¿cuál es el estado del sistema caja-gato-mecanismo? Pues bien, la respuesta a la pregunta es que, hasta que un observador no abra la caja y «mida» el valor del sistema, la partícula no «decidirá» si se ha desintegrado o no y, por tanto, el sistema se encuentra en una superposición de estados: el gato no está, estrictamente, ni vivo ni muerto, sino las dos cosas a la vez.

Para todos aquellos que consideren la superposición de estados como una hipótesis difícil de creer, es de rigor hacer constar interpretaciones alternativas que sostienen algunos físicos respetados, como por ejemplo la conocida como *interpretación de los mundos posibles*. Dicha interpretación alternativa a la superposición de

estados sostiene que esta última se trata de una tesis insostenible y que lo que ocurre en realidad es que, *para cada uno* de los posibles estados en que se encuentra una partícula, es decir, posición, cantidad de energía, etc., existe un *universo alternativo* donde la partícula adopta un estado u otro. Es decir, que en un universo el gato de la caja está vivo y, en el otro, muerto. Cuando el observador abre la caja y comprueba que nuestro felino está en efecto vivo, lo está haciendo como parte integrante de sólo uno de los universos posibles. En otro universo paralelo –y completo, con sus estrellas, planetas, estaciones de metro y demás–, ese mismo observador mira dentro de la caja y, comprueba, imaginamos que con cierto pesar, que el gato ha muerto envenenado. Los partidarios de la interpretación de los mundos posibles todavía no han aclarado de qué modo estos universos interaccionan entre sí. Sea como fuere, queremos insistir de nuevo en que lo que acaso está en cuestión es la interpretación de porqué la realidad física microscópica se comporta de ese modo, no el comportamiento en sí, ratificado en numerosos y concluyentes experimentos.

Del bit al *qubit*

¿Cuál es, sin embargo, la relación entre la superposición de estados de las partículas y la computación (y no digamos la criptografía)? Hasta 1984 a nadie se le hubiera ocurrido siquiera plantear una relación entre ambos campos. Por esas fechas, el físico británico David Deutsch empezó a barajar una idea revolucionaria: ¿Cómo serían los ordenadores que, en lugar de plegarse a las leyes de la física clásica, obedecieran a las de la mecánica cuántica? ¿De qué modo podría la computación sacar partido de la superposición de estados de las partículas?

Recuérdese que los ordenadores convencionales manejan unidades mínimas de información denominadas bits, capaces de tomar dos valores opuestos: cero o uno. Un ordenador cuántico, en cambio, podría tomar como unidad mínima de información una partícula que presente dos estados posibles; por ejemplo, el espín de un electrón, que sólo puede estar en dos posiciones, «arriba» o «abajo». Esta partícula tendría la fantástica propiedad de representar el valor cero (espín «abajo»), el uno (espín «arriba»), y la superposición de estados espín «arriba»-espín «abajo», es decir, podría representar los dos valores simultáneamente. A esta nueva unidad de información se la denomina *qubit*, acrónimo de *quantum bit* (en inglés, «bit cuántico»), y su manipulación abre las puertas a un mundo insospechado de ordenadores ultrapotentes.

Un ordenador convencional lleva a cabo sus cálculos secuencialmente. Tomemos como ejemplo la información numérica contenida en 32 bits. Con este número de bits pueden codificarse los números del 1 hasta el 4.292.967.296. Si un ordenador convencional tuviera que encontrar un número concreto incluido en dicho conjunto, tendría que hacerlo bit por bit. Sin embargo, un ordenador cuántico podría llevar a cabo la tarea de un modo infinitamente más rápido. Si tomamos 32 electrones, los disponemos en una «caja opaca» y a continuación los hacemos entrar en una superposición de estados (por ejemplo, por medio de un impulso eléctrico lo bastante fuerte como para hacer cambiar el espín del electrón de «arriba» a «abajo»), estos 32 electrones –los *qubits* de nuestro ordenador cuántico- estarían representando todas las combinaciones posibles de espín «arriba» (uno) y espín «abajo» (cero) de manera *simultánea*. De este modo, la búsqueda del número deseado se haría *de una sola vez* sobre todos y cada una de las opciones posibles. Si aumentamos la cantidad de *qubits* a, por ejemplo, 250, la cantidad de operaciones simultáneas que podrían llevarse a cabo serían nada menos que 10^{75}, algo más que el número de átomos que contiene nuestro universo.

Los trabajos de Deutsch probaron que los ordenadores cuánticos eran una posibilidad teórica. Que algún día sean también una realidad práctica es el objetivo de instituciones y grupos de investigadores de todo el mundo, los cuales, sin embargo, todavía no han sido capaces de superar las dificultades técnicas de construir un ordenador cuántico viable. Algunos expertos consideran que todavía se tardarán entre 15 y 25 años en lograrlo; otros, sin embargo, dudan de que sea incluso posible.

UN GRAN HERMANO PARA EL SIGLO XXI

Las consecuencias de la construcción de un ordenador cuántico viable no sólo se restringirían al desplome de la criptografía tal y como la conocemos. Tamaña potencia de cálculo puesta al servicio de cualquier interés, ya sea público o privado, decantaría la balanza del poder mundial del lado de quien lo poseyera. La lucha por ser el primer país en desarrollar una tecnología semejante podría muy bien acabar emulando a las carreras de armamentos del pasado reciente. No resulta extravagante pensar que decisivos avances en este sentido puedan quererse mantener en secreto por razones de seguridad nacional. ¿Habrá en algún lugar del globo, en un subterráneo refrigerado, un primer ordenador cuántico a la espera de ser puesto en pleno funcionamiento y cambiar nuestras vidas para siempre?

ADIÓS, DES, ADIÓS

Dos años después de que Shor demostrara que un ordenador cuántico podría demoler el cifrado RSA, otro estadounidense, Lov Grover, hizo lo propio con otro puntal de la criptografía moderna, el algoritmo DES. Grover diseñó un programa que permite a un ordenador cuántico encontrar el valor numérico correcto de una lista de valores posibles en un tiempo que es la raíz cuadrada del que necesitaría un ordenador convencional. Otro algoritmo de uso común que se vería afectado por esta innovación es el RC5, el estándar empleado por los navegadores de Microsoft.

¿El fin de la criptografía?

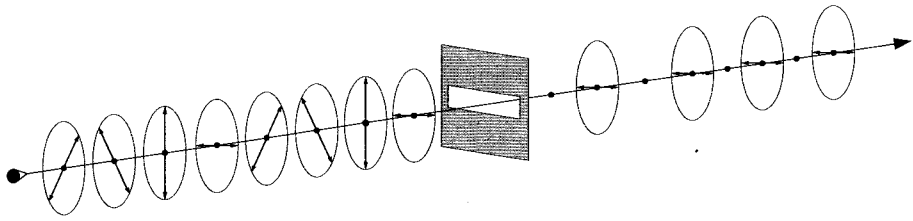
La computación cuántica traería consigo el derrumbe de la criptografía tal y como la conocemos. Tomemos como ejemplo a la estrella de los algoritmos modernos de encriptación, el RSA. Como se recordará, cualquiera que intente romper una clave RSA por fuerza bruta necesitará factorizar con éxito el producto de dos números primos de enorme tamaño. Está operación es extraordinariamente laboriosa y no se ha encontrado todavía ningún tipo de atajo matemático para abordarla con mayor facilidad. ¿Podría un ordenador cuántico afrontar el reto de factorizar un número primo del tamaño de los que manejan las claves RSA? La respuesta, afirmativa, la dio el informático estadounidense Peter Shor en 1994. Shor diseñó un algoritmo, susceptible de ser ejecutado por un ordenador cuántico, capaz de descomponer números enormes en un tiempo infinitamente menor que el del ordenador convencional más potente.

Si finalmente se construyera este asombroso artilugio, el algoritmo de Shor demolería, pieza a pieza, el poderoso edificio criptográfico construido alrededor de RSA y, de la noche a la mañana, las comunicaciones más delicadas del planeta se verían expuestas a la luz del día. El resto de criptosistemas contemporáneos seguirían un mismo camino. Parafraseando a Mark Twain, se diría que el anuncio de la muerte del criptoanálisis había sido «un tanto prematura».

Lo que la mecánica cuántica quita, la mecánica cuántica lo da

Uno de los pilares de la mecánica cuántica es el denominado *principio de indeterminación*, enunciado por Werner Heisenberg en 1927. Aunque su formulación exacta es muy técnica, su propio creador se atrevió a resumirlo del modo siguiente: «Por

principio, no podemos conocer el presente en todos sus detalles». Más en concreto, resulta imposible determinar con precisión ciertas propiedades complementarias de una partícula en un momento cualquiera. Tomemos, por ejemplo, el caso de las partículas lumínicas o *fotones*. Una de sus características fundamentales es la *polarización*, un término técnico que se refiere a la oscilación o vibración de un campo eléctrico. [Aunque los fotones vibran en todas direcciones, a efectos de esta breve exposición asumiremos que lo hace en cuatro: vertical (↕), horizontal (↔), diagonal izquierdo (↖↘) y diagonal derecho (↙↗).] Pues bien, el principio de Heisenberg afirma que la única forma de averiguar algo acerca de la polarización de un fotón cualquiera es haciéndolo pasar por un filtro o «rendija», que a su vez es del tipo horizontal, vertical, diagonal izquierdo o diagonal derecho. Los fotones polarizados horizontalmente atravesarán intactos un filtro vertical, mientras que los polarizados de forma vertical rebotarán. En cuanto a los fotones polarizados diagonalmente, la mitad de ellos atravesará el filtro, con su polarización cambiada a horizontal, y la otra mitad rebotará, *totalmente al azar*. En consecuencia, una vez emitido un fotón no es posible saber con certeza cuál era la polarización original.



Si se hace pasar una serie de fotones de distinta polarización por un filtro horizontal se observa que la mitad de los orientados diagonalmente atravesarán el filtro con la polarización cambiada a horizontal.

¿Qué relación existe entre la polarización de los fotones y la criptografía? Mucha, como veremos a continuación. Para empezar, asumamos el papel de un investigador que desea saber cuál es la polarización de una serie de fotones. Para ello no tiene otra opción que escoger un filtro de una determinada orientación; por ejemplo, la horizontal. Supongamos que el fotón supera el filtro. ¿Qué información obtiene de ello el investigador? Desde luego, puede descartar que la polarización original del fotón fuera vertical. ¿Puede hacer alguna otra suposición? Ninguna. En un principio se podría pensar que hay más probabilidades de que el fotón original estuviera orientado horizontal que diagonalmente, puesto que la mitad de estos segundos no

pasarían el filtro; el número de fotones orientado diagonalmente, sin embargo, es también el doble. Es importante recalcar que esta dificultad a la hora de detectar la polarización de un fotón no es fruto de alguna carencia tecnológica o teórica, susceptible de subsanarse en el futuro: es una consecuencia de la naturaleza misma de la realidad física subatómica. Aprovechada del modo adecuado, esta particularidad puede utilizarse para construir un criptosistema total y absolutamente irrompible; el Santo Grial de la criptografía.

La cifra indescifrable

En 1984, el estadounidense Charles Bennett y el canadiense Gilles Brassard idearon un criptosistema basado en la transmisión de fotones polarizados. El primer paso consiste en que emisor y receptor acuerden un método para asignar un cero o un uno a una polarización u otra. En el ejemplo que sigue, la asignación de ceros y unos estará en función de dos esquemas o bases de polarización: la primera base, denominada *recta* y representada por el signo +, hace corresponder el 1 a la polarización ↕ y el 0 a la polarización ↔; la segunda base, denominado *diagonal* y representada por el signo X, asigna el 1 a la polarización ↙↗ y el 0 a la ↖↘. Por ejemplo, el mensaje 0100101001 se podría transmitir del modo siguiente:

Mensaje	0	1	0	0	1	0	1	0	1	1
Base	×	+	+	×	+	×	×	+	×	+
Transmisión	↖↘	↕	↔	↖↘	↕	↖↘	↙↗	↔	↙↗	↕

Si un espía interceptara la transmisión, debería para ello emplear un filtro de una orientación concreta, pongamos ×:

Mensaje original	↖↘	↕	↕	↖↘	↕	↖↘	↙↗	↕	↙↗	↕
Filtro	×									
Polarización detectada	↖↘	↖↘ o ↙↗	↖↘ o ↙↗	↖↘	↖↘ o ↙↗	↖↘	↙↗	↖↘ o ↙↗	↙↗	↖↘ o ↙↗
Mensaje posible	↖↘ ↕ ↔	↖↘ o ↙↗, ↕ ↕	↖↘ o ↙↗, ↕ ↔	↖↘ ↕ ↔	↖↘ o ↙↗, ↕ ↔	↖↘ ↕ ↕	↙↗ ↕ ↕	↖↘ o ↙↗, ↕ ↕	↙↗ ↕ ↕	↖↘ o ↙↗, ↕ ↕

Como puede verse, al desconocer la base original, el espía es incapaz de averiguar información relevante alguna a partir de la polarización detectada. Aún sabiendo el esquema de asignación de ceros y unos empleado por emisor y receptor, si el primero alterna las bases de manera aleatoria, el espía se equivocará aproximadamente un tercio de las veces (en la tabla puede observarse un desglose de todas las combinaciones de emisión y recepción posibles bajo las condiciones descritas). El problema obvio en este escenario es que el receptor no se encuentra en mejor posición que el espía.

Llegados a este punto, emisor y receptor podrían sortear el problema enviándose la secuencia de bases empleadas por algún medio seguro; por ejemplo, cifrándola mediante RSA. Pero entonces la seguridad de la cifra estaría al albur de que los ordenadores cuánticos fueran todavía una quimera. Para superar este último obstáculo, Brassard y Bennett tuvieron que añadir una sutileza más a su método.

Si el lector hace memoria, el talón de Aquiles de los cifrados polialfabéticos de la familia del cuadrado de De Vigenère era que el uso de claves cortas y repetidas generaba regularidades en el cifrado que abrían una pequeña pero significativa rendija para el criptoanalista. ¿Qué ocurriría, sin embargo, si la clave empleada fuera una ristra aleatoria de caracteres de una longitud mayor que la del mensaje? ¿Y si, para mayor seguridad, cada mensaje, por insignificante que fuera, se cifrara con una clave distinta? La respuesta es que se dispondría de un cifrado irrompible. El primero en sugerir el uso del cifrado polialfabético de clave única, poco después de la Primera Guerra Mundial, fue Joseph Mauborgne, a la sazón investigador jefe del servicio criptográfico estadounidense. Mauborgne imaginó un cuaderno de claves compuesto por series aleatorias de más de un centenar de caracteres cada una, que se entregarían a emisor y receptor con las instrucciones de destruir la clave empleada en cada ocasión y pasar a la siguiente. Este sistema, conocido como la *cifra del cuaderno de uso único* es, como se ha dicho, irrompible, y así puede demostrarse matemáticamente. De hecho, las comunicaciones de alto secreto entre algunos jefes de Estado se llevan a cabo mediante este método.

Si la cifra del cuaderno de uso único es tan segura, ¿por qué no se ha extendido su uso? ¿Qué sentido tiene preocuparse por el advenimiento de los ordenadores cuánticos y, para decirlo vulgarmente, andar manipulando fotones?

Dejando de lado las dificultades logísticas derivadas de generar miles y miles de claves aleatorias de un único uso para cifrar un mismo número de mensajes, la cifra del cuaderno de uso único presenta la misma debilidad que el resto de algoritmos clásicos de encriptación: la distribución de la clave, precisamente el obstáculo que la criptografía moderna tanto se ha preocupado por resolver.

Base del emisor	Bit del emisor	El emisor envía	Detector del receptor	¿Es correcto el detector?	El receptor detecta	Bit del receptor	¿Es correcto el bit del receptor?
DIAGONAL	1	↗	+	No	↕	1	Sí
					↔	0	No
			×	Sí	↗	1	Sí
	0	↖	+	No	↕	1	No
					↔	0	Sí
			×	Sí	↖	0	Sí
RECTO	1	↕	+	Sí	↕	1	Sí
			×	No	↖	0	No
					↗	1	Sí
	0	↔	+	Sí	↔	0	Sí
			×	No	↗	1	No
					↖	0	Sí

Sin embargo, la transmisión de información por medio de fotones polarizados es el canal idóneo por medio del cual transmitir sin peligro una clave única. Para ello, son necesarios tres pasos previos a la transmisión del mensaje:

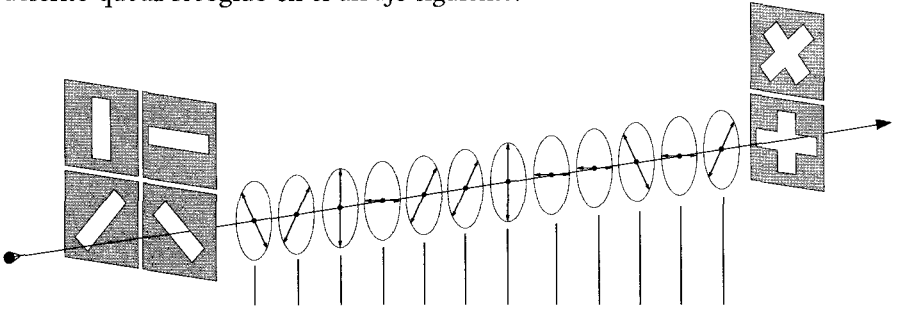
1) En primer lugar, el emisor envía al receptor una secuencia aleatoria de unos y ceros empleando para ello, también aleatoriamente, diferentes filtros de polarización vertical (↕), horizontal (↔) y diagonal (↗, ↖).
2) El receptor procede a medir la polarización de los fotones recibidos mediante la alternancia aleatoria de bases rectas (+) y diagonales (×). Comoquiera que desconoce la secuencia de filtros empleados por el emisor, buena parte de la secuencia de ceros y unos será también errónea.
3) Por último, emisor y receptor se ponen en contacto del modo que prefieran, sin importarles si se trata de un canal inseguro, y se intercambian la información siguiente: en primer lugar, el emisor explica qué base, la recta o la diagonal, debe emplearse para leer correctamente cada fotón, pero sin revelar su polarización

EL MENSAJE DE BABEL

El escritor argentino Jorge Luis Borges imaginó en el relato *La biblioteca de Babel* una biblioteca tan vasta que contuviera en sus anaqueles todos y cada uno de los libros posibles: cada novela, poema y tesis; y las refutaciones de estas tesis y las refutaciones de las refutaciones, así hasta el infinito. Un criptoanalista que intentara descifrar por prueba y error un mensaje cifrado con una cifra de cuaderno de uso único se encontraría en un caso semejante. Como la cifra es totalmente aleatoria, los posibles descifrados contendrán todos los textos posibles de igual longitud: el mensaje real, y una (breve) refutación del mensaje, y el mismo mensaje con todos los nombres propios cambiados por otros de igual longitud, y así hasta el infinito.

(es decir, el filtro empleado). Por su parte, el receptor le comenta en qué casos ha acertado en la elección de la base. Como puede comprobarse en la tabla anterior, si un emisor y un receptor aciertan en las respectivas bases, puede asegurarse que la transmisión del cero o del uno se ha completado de forma correcta. Por último, ya en privado, ambos desechan los bits correspondientes a los fotones que el receptor detectó con la base equivocada.

El resultado de este proceso es que emisor y receptor ahora comparten una secuencia de unos y ceros generada de un modo totalmente aleatorio: la elección de los filtros de polarización empleados por el emisor es aleatoria, al igual que la elección de bases usada por el receptor. Un modesto ejemplo de doce bits del proceso arriba descrito queda recogido en el dibujo siguiente:



Bits del emisor	0	1	1	0	1	1	1	0	0	0	0	1
Detector del receptor	+	×	×	+	×	+	×	+	+	×	+	×
El receptor detecta	1	1	1	0	1	0	1	0	0	0	0	1
Bits retenidos	–	1	–	0	1	–	–	0	0	0	0	1

Obsérvese que, de los bits finalmente retenidos, algunos de ellos se descartan aunque hayan sido interpretados de forma correcta. Ello se hace así porque el receptor no puede estar seguro de haberlos detectado correctamente, al haber empleado para ello bases erróneas. Si la transmisión inicial está compuesta por un número suficiente de fotones, la secuencia de unos y ceros será lo bastante larga como para constituir una clave de cuaderno de uso único capaz de cifrar mensajes de la longitud que deseemos.

Pongámonos ahora en el papel de un espía que ha interceptado tanto los fotones enviados como las conversaciones públicas de emisor y receptor. Ya hemos visto que, sin saber exactamente qué filtro de polarización ha empleado el emisor del mensaje, es imposible determinar en qué casos se ha detectado la polarización correcta. La información que intercambian emisor y receptor tampoco le sirve de ayuda, porque en ningún caso se transmiten información alguna acerca de las polarizaciones concretas.

Y lo que resulta todavía más fastidioso para el espía: en el caso de no haber acertado con la base correcta, y por tanto haber alterado la polarización del fotón, su intromisión quedará al descubierto sin que pueda hacer nada por evitarlo. En efecto, basta con que emisor y receptor verifiquen una parte lo bastante extensa de la clave para detectar cualquier manipulación de la polarización de los fotones.

Para ello, emisor y receptor acuerdan un protocolo de verificación muy sencillo: completadas las tres fases preliminares especificadas más arriba, y con un número suficiente de bits retenidos, el emisor se pone en contacto con el receptor, de nuevo por un medio convencional, y entre los dos revisan un subconjunto de bits escogido al azar del total; pongamos 100 bits. Si coinciden los 100 tanto emisor como receptor pueden estar del todo seguros de que ningún espía ha fisgoneado la transmisión, y pueden dar por buena la secuencia como clave de cuaderno de uso único. En caso contrario, emisor y receptor deben empezar de nuevo todo el proceso.

32 centímetros de secreto absoluto

El método de Brassard y Bennett es impecable desde un punto de vista teórico, pero su eventual puesta en práctica fue recibida en su día con mucho escepticismo. En 1989, y tras más de un año de arduos trabajos, Bennett puso a punto un sistema formado por dos ordenadores separados por una distancia de 32 centímetros, uno de los cuales iba a hacer las veces de emisor y, el otro, de receptor. Tras varias

horas de pruebas y ajustes, el experimento se vio coronado por el éxito: emisor y receptor completaron todas las fases del proceso e incluso fueron capaces de verificar sus claves respectivas. La criptografía cuántica era posible.

El histórico experimento de Bennett tenía el obvio inconveniente de la distancia. Sin embargo, en años sucesivos, otros equipos de investigación fueron ampliado el alcance de la transmisión: en 1995, investigadores de la Universidad de Ginebra llegaron a 23 km por medio de un cable de fibra óptica; en 2006, un equipo de Laboratorio Nacional de Los Alamos, de Estados Unidos, a 107 km por el mismo procedimiento. Aunque no son todavía distancias suficientes como para que sean útiles en el ámbito de la comunicación convencional, sí pueden serlo para el caso de áreas de comunicación restringida, como edificios gubernamentales, sedes de empresa o similares.

Dejando al margen consideraciones relativas a la seguridad física de la transmisión –es decir, a la posibilidad de que la transmisión se vea impedida por medidas de sabotaje que también pueden ser de naturaleza cuántica–, el criptosistema cuántico aquí esbozado representa el triunfo final del secreto sobre la indiscreción, de la criptografía sobre el criptoanálisis. Ahora sólo queda preocuparse –y no es un tema menor, si se ha de hacer caso a las reflexiones de Zimmermann– de cómo se aplica esta herramienta, y a quién beneficia.

Anexo

Varios cifrados clásicos (y un tesoro escondido)

A continuación expondremos varios cifrados de criptografía clásica mencionados en el texto pero no desarrollados en profundidad en su momento. Todos ellos revisten un gran interés en tanto que son representativos del proceder criptográfico de distintas épocas, o bien como simple divertimento. Se completa la selección con un descifrado ficcional obra del narrador estadounidense Edgar Allan Poe que ilustra a la perfección el criptoanálisis por el método de las frecuencias.

El cifrado de Polibio

Este cifrado, uno de los más antiguos de los que se dispone de información detallada, se basa en escoger 5 letras de un alfabeto y distribuir el resto de los caracteres en una tabla de 5 filas y 5 columnas. El cifrado consiste en hacer corresponder a cada letra el par de letras que indican la fila y la columna del tablero. Originariamente se usaba el alfabeto griego. Para ejemplificar este cifrado se escogen como letras «base» los caracteres A, B, C, D y E. A continuación, se colocan las letras del alfabeto en las casillas de la tabla con un orden acordado entre el emisor y receptor. Podemos pues considerar la tabla siguiente:

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I-J	K
C	L	M	N-Ñ	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Nótese que el alfabeto cifrado tiene que pasar obligatoriamente a ser de 25 letras (5×5). También es posible organizar el alfabeto cifrado a partir de valores numéricos (por ejemplo, las cifras 1, 2, 3, 4 y 5); de ello resultaría la tabla:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I-J	K
3	L	M	N-Ñ	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Veamos un ejemplo de cifrado Polibio usando las dos versiones. El mensaje llano es «GRECIA». De la primera tabla resulta que:

G será sustituida por el par BB.
R será sustituida por el par DB.
E será sustituida por AE.
C será sustituida por AC.
I será sustituida por BD.
A será sustituida por AA.

El mensaje cifrado es «BBDBAEACBDAA». Si se emplea la versión numérica se obtiene, por un proceso análogo: 224215132411.

El cifrado de Gronsfeld

Este cifrado, ideado por el neerlandés Josse Maximilaan Bronckhorst, primer conde de Gronsfeld, fue empleado en la Europa del siglo XVII. Se trata de un cifrado polialfabético, análogo al cuadrado de DeVigenère pero de menor dificultad (y seguridad). Para encriptar un mensaje se parte de la tabla siguiente.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0:	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
1:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
2:	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
3:	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
4:	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
5:	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
6:	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
7:	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
8:	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
9:	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

A continuación se escoge un número aleatorio que tenga el mismo número de cifras que caracteres tiene el mensaje que se desea cifrar. Si el mensaje llano es «MATEMATICAS», se escogerá un número aleatorio de 11 cifras, por ejemplo, 12345678912. Este número será la palabra clave del cifrado. A continuación se sustituye cada letra del mensaje por la letra correspondiente al número en la tabla de referencia.

Mensaje	M	A	T	E	M	A	T	I	C	A	S
Clave	1	2	3	4	5	6	7	8	9	1	2
Mensaje cifrado	P	F	A	P	Z	R	M	F	E	D	X

Al par (M,1) le corresponde la P, y así sucesivamente. El mensaje queda cifrado como «PFAPZRMFEDX». Nótese que la letra A del mensaje original se cifra de maneras distintas; F, R y D. Como en el caso general de los cifrados polialfabéticos, este criptosistema es resistente tanto a la fuerza bruta como al análisis de frecuencia. El número de claves de un cifrado de Gronsfeld para un alfabeto de 27 letras es de $27! \times 10! = 3,9514 \times 10^{34}$ claves.

La cifra Playfair

Los creadores de esta cifra, el barón Lyon Playfair y Sir Charles Wheatstone, este último pionero del telégrafo eléctrico, eran vecinos y amigos y tenían la criptografía como afición común. El método recuerda a un ilustre antecesor, el cifrado de Polibio, y como aquél emplea una tabla de 5 filas y 5 columnas. En un primer paso, se sustituye cada carácter del mensaje llano por un par de letras según una clave de 5 letras distintas. En nuestro ejemplo, la clave será JAMES. Para el caso de un alfabeto de 27 caracteres se genera la tabla de cifrado siguiente.

J	A	M	E	S
B	C	D	F	G
H	I-K	L	N-Ñ	O
P	Q	R	T	U
V	W	X	Y	Z

A continuación, el mensaje llano se divide en pares de letras o *dígrafos*. Las dos letras de todos los dígrafos deben ser diferentes, y para evitar posibles coincidencias

se emplea el carácter X. También se emplea este carácter para completar un dígrafo en caso de que la letra final quede sola. Por ejemplo, para el mensaje llano «PERRO», la división en dígrafos sería:

PE Rx RO.

La palabra «HOY» se desglosa:

HO Yx.

Una vez se tiene el mensaje llano en forma de dígrafos ya puede empezarse la codificación. Para ello hay que tener en cuenta tres casos:

a) Que las dos letras del dígrafo están en la misma fila.
b) Que las dos letras del dígrafo están en la misma columna.
c) Ninguno de los casos anteriores.

En el caso (a) los caracteres del dígrafo se reemplazan por la letra situada a la derecha de cada uno de ellos (la «siguiente» en el orden natural de la tabla). De esta forma el par JE, se codifica como AS:

J	A	M	E	S

En el caso (b) los caracteres del dígrafo se reemplazan por la letra que se encuentra en la posición inmediatamente inferior de la tabla. Por ejemplo, el dígrafo ET se codifica como FY y el TY como YE:

E
F
N-Ñ
T
Y

En el caso (c), para codificar la primera letra del dígrafo se mira su fila hasta llegar a la columna que contiene la segunda letra; el cifrado de la letra llana es la que se encuentra en la intersección. Para codificar la segunda letra, se mira su fila hasta

llegar a la columna que contiene a la primera letra; el cifrado de la letra llana es, de nuevo, la que se encuentra en la intersección.

Por ejemplo, del dígrafo CO, la C se codifica como G y la O se codificaría como una I o bien una K.

J	A	M	E	S
B	**C**	D	F	G
H	*I-K*	L	N-Ñ	**O**
P	Q	R	T	U
V	W	X	Y	Z

Para cifrar el mensaje «RBA» con la clave JAMES se procede del siguiente modo.

- Se expresa en dígrafos: RB Ax.
- La R se cifra con una P.
- La B como una D.
- La A como una M.
- La X como una W.

El mensaje cifrado es «PDMW».

El criptograma de *El escarabajo de oro*

William Legrand, el protagonista de *El escarabajo de oro* (1843), de Edgar Allan Poe, descubre el lugar donde reside un fabuloso tesoro tras descifrar un criptograma escrito sobre un pergamino. El procedimiento utilizado por Legrand es un método estadístico basado en la frecuencia de aparición de las letras que componen un texto inglés. El mensaje cifrado es el siguiente:

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)8¶8*;4069285);)6†8)4‡
‡;1(‡9;48081;8:8‡1;48†85; 4)485†528806*81(
‡9;48;(88;4(‡?34;48)4‡;161;:188;‡?;

Legrand parte del supuesto de que el texto original estaba escrito en idioma inglés. La letra que se encuentra con mayor frecuencia en dicho idioma es la *e*. A continuación, y ordenadas de mayor a menor frecuencia de aparición, se cuentan las letras: *a, o, i, d, h, n, r, s, t, u, y, c, f, g, l, m, w, b, k, p, q, x, z*.

Nuestro héroe obtiene del criptograma la siguiente tabla, en la cual aparecen en la primera fila los caracteres presentes en el mensaje codificado y en la segunda, su frecuencia de aparición.

8	;	4	‡	)	*	5	6	(	+	1	0	9	2	:	3	?	¶	_
33	26	19	16	16	13	12	11	10	8	8	6	5	5	4	4	3	2	1

Luego, el 8 muy probablemente sea la letra *e*. A continuación, busca apariciones del trío de caracteres *the* (en castellano, los artículos «el» o «la»), también muy común, lo que le permite traducir así los caracteres «;48».

La aparición del término «(88», ahora que sabe significa «t(ee» le permite colegir que el término que le falta, «(», sólo puede ser una «r» dado que *tree* («árbol») es la única posibilidad del diccionario. Finalmente, por medio de otros ingeniosos recursos de criptoanálisis parecidos y con mucha paciencia, llega al alfabeto de cifrado siguiente:

5	+	8	3	4	6	*	‡	(	;	?
A	d	e	g	H	i	n	o	R	T	U

El texto resultante en inglés es:

«A good glass in the bishop's hostel in the devil's seat –forty one degrees and thirteen minutes– northeast and by north –main branch seventh limb east side– shoot from the left eye of the death's-head– a beeline from the tree through the shot fifty feet out.»

La traducción aproximada en castellano es:

«Un buen vaso en la hostería del obispo en la silla del diablo –cuarenta y un grados y trece minutos– Nordeste cuarto de Norte –principal rama séptimo vástago lado Este– soltar desde el ojo izquierdo de la cabeza de muerto –una línea recta desde el árbol a través de la bala cincuenta pies hacia fuera.»

Los números primos y su valor en criptografía

Las matemáticas de verdad no tienen efecto alguno en las guerras.
Nadie ha descubierto todavía ninguna aplicación bélica de, por ejemplo,
la teoría de números.
Godfrey H. Hardy, *Apología de un matemático* (1940)

Para el adecuado descifrado de un mensaje se revela de vital importancia que el cifrado posea inverso. Como ya se observó en el estudio de los códigos afines, un modo de asegurar este punto es trabajar con módulo número primo. Además, el producto de primos constituye una función no reversible, es decir, una vez realizado el producto resulta muy laborioso averiguar el valor de los factores originales.

Dicha propiedad hace de esta operación una herramienta muy útil para aquellos sistemas basados en claves asimétricas, como el algoritmo RSA, que a su vez constituyen la base de la criptografía de clave pública. Procederemos, pues, a estudiar más en detalle la imbricación entre los números primos y la criptografía, y ejemplificaremos lo aprendido mediante la exposición formal del funcionamiento del RSA en su dimensión matemática.

Los números primos y el «otro» teorema de Fermat

El conjunto de los números primos es un subconjunto de los números naturales que engloba a todos los elementos de éste mayores que 1 que son divisibles únicamente por sí mismos y por la unidad. El teorema fundamental de la aritmética establece que cualquier número natural mayor que 1 siempre puede representarse como un producto de potencias de números primos, y esta representación (factorización) es única, por ejemplo en:

$$20 = 2^2 \cdot 5$$
$$63 = 3^2 \cdot 7$$
$$1.050 = 2 \cdot 3 \cdot 5^2 \cdot 7.$$

Todos los números primos, excepto el 2, son impares. Los únicos dos números primos consecutivos son el 2 y el 3. Los números primos impares consecutivos, es decir, aquellos que se hallan a una distancia numérica de 2 (por ejemplo, el

17 y el 19), se llaman *números primos gemelos*. Son de especial interés los números primos *de Mersenne* y los *de Fermat*.

Un número primo es primo de Mersenne si al sumarle 1 el resultado es una potencia de 2. Por ejemplo, 7 es un número primo de Mersenne al cumplirse $(7+1=8=2^3)$. Los ocho primeros números primos de Mersenne son, en consecuencia:

$$3, 7, 31, 127, 8.191, 131.071, 524.287, 2.147.483.647.$$

En la actualidad se conocen apenas una cuarentena de números primos de Mersenne. Se trata de números gigantescos, como el $2^{43.112.609}-1$, descubierto en 2008. A título de comparación, el número estimado de partículas elementales de todo el universo es inferior a 2^{300}. Por su parte, un número primo de Fermat es un número primo de la forma:

$$F_n = 2^{2^n}+1, \text{ siendo } n \text{ un número natural.}$$

Sólo se conocen cinco primos de Fermat: 3 $(n=0)$, 5 $(n=1)$, 17 $(n=2)$, 257 $(n=3)$ y 65.537 $(n=4)$.

Los primos de Fermat llevan el nombre del ilustre jurista y matemático francés que los descubrió, Pierre de Fermat (1601-1665). El francés llevó a cabo numerosos e importantes descubrimientos adicionales relativos a los números primos, de entre los cuales destaca el conocido como *pequeño teorema de Fermat*, el cual establece que:

> Si p es un número primo entonces para cualquier entero a obtenemos que $a^p = a$ en módulo p.

Este resultado es de gran importancia en criptografía moderna, como se verá a continuación.

De Euler a RSA

Otro resultado de gran interés en aritmética modular es la conocida como *identidad de Bézout*. La identidad establece que si a y b son números enteros positivos, la igualdad $\text{mcd}\,(a,b)=k$ equivale a que existen dos números enteros p, q que verifican

$$pa+qb=k.$$

En el caso particular de que $\text{mcd}(a,b)=1$ tenemos que existen p y q enteros tales que

$$pa+qb=1.$$

Si trabajamos en módulo n podemos establecer que si $\text{mcd}(a,n)=1$ entonces existen, necesariamente, enteros p y q de manera que $pa+qn=1$. Por la suposición de módulo n se tiene que $qn=0$, con lo cual se concluye que existe un p de forma que $pa=1$, es decir, el inverso de a en módulo n existe y es p.

El número de elementos con inverso en módulo n será pues el número de naturales a menores que n que cumplen $\text{mcd}(a,n)=1$. Este conjunto de números se conoce como *función de Euler* y se denota como $\varphi(n)$.

Si la descomposición de n en factores primos es $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$, entonces:

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)...\left(1+\frac{1}{p_k}\right).$$

Si, por ejemplo, $n=1.600=2^6 5^2$ tendremos que:

$$\varphi(1.600)=1.600\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=640.$$

Y afinando todavía más, si la situación es que n es primo se obtiene que para cualquier valor de a el $\text{mcd}(a,n)=1$ y, en consecuencia, cualquier valor de a tendrá inverso módulo n y, por consiguiente, $\varphi(n)=n-1$.

Hagamos un aparte y recordemos las conclusiones más importantes a las que se ha llegado hasta ahora:

1) $\varphi(n)$ se denomina función de Euler e indica la cantidad de números menores que n que son primos con n.
2) Si $n=pq$ siendo p y q dos números primos, entonces

$$\varphi(n)=(p-1)(q-1).$$

3) Por el pequeño teorema de Fermat se sabe que si p es un número primo y a es un número coprimo con p se tendrá la relación $a^p \equiv a$ (mód. p), que equivale a afirmar que $a^{p-1} \equiv 1$ (mód. p).

Sólo falta añadir la puntilla final, que nos la proporciona el teorema de Euler. Éste afirma que:

4) Si $\text{mcd}(a,n)=1$, entonces se verifica la igualdad $a^{\varphi(n)} \equiv 1$ (mód. n).

¿Por qué funciona el algoritmo RSA?

Armados con los conocimientos expuestos anteriormente, se está en disposición de mostrar los argumentos matemáticos que subyacen al proceso de cifrado del algoritmo RSA.

El algoritmo en cuestión encripta una correspondencia numérica m de un mensaje cualquiera sean p y q dos números primos y $n=p\cdot q$. Se denomina e a un valor cualquiera que verifique que $\text{mcd}(e,\varphi(n))=1$ y se llama d al inverso de n en módulo $\varphi(n)$ [que se sabe que existe, ya que $\text{mcd}(e,\varphi(n))=1$]. Así:

$$d\cdot e=1 \text{ mód.}\varphi(n).$$

El mensaje cifrado, M, se cifra según $M=m^e$ (mód. n). El algoritmo presupone que el mensaje original m se obtiene por $m=M^d=(m^e)^d$ (mód. n). Verificar esta igualdad equivale a demostrar la validez de RSA. Para ello se combinan el teorema de Fermat y el teorema de Euler.

Considérense dos casos:

1) Si $\text{mcd}(m,n)=1$ por el teorema de Euler $m^{\varphi(n)} \equiv 1$ (mód. n).

Partimos de la relación la cual es equivalente a $e\cdot d-1\equiv 0$ (mód. $\varphi(n)$), es decir, existe un valor k, entero, de manera que $e\cdot d-1=k\cdot\varphi(n)$, es decir, $e\cdot d-1=k\cdot\varphi(n)+1$. Con ello tenemos, aplicando el teorema de Euler, la igualdad:

$$(m^e)^d=m^{e\cdot d}=m^{k\cdot\varphi(n)+1}=m^{k\cdot\varphi(n)}\cdot m=(m^{\varphi(n)})^k\cdot m\equiv 1^k\cdot m \text{ (mód. } n)=$$
$$=m \text{ (mód. } n).$$

Es decir, el resultado que se buscaba.

2) Si $\text{mcd}(m,n)\neq 1$, como que $n=p\cdot q$, m contendrá como factor únicamente a p, únicamente a q, o a ambos a la vez. En el primer caso,

a) m será múltiplo de p, es decir, existe un entero r de manera que $m = r \cdot p$. Con lo cual se tiene que y en consecuencia $m^{de} \equiv 0$ (mód. p), y finalmente: $m^{de} \equiv m$ (mód. p), es decir, existe un valor A de manera que:

$$m^{de} - m = A\,p. \qquad (1)$$

En el segundo caso,

b) se tiene que

$$(m^e)^d = m^{e \cdot d} = m^{k \cdot \varphi(n)+1} = m^{k \cdot \varphi(n)} \cdot m = (m^{\varphi(n)})^k \cdot m \equiv$$
$$\equiv (m^{(q-1)})^{k(p-1)} \cdot m \text{ (mód. } n) = m.$$

Como $\text{mcd}(m,n) = p$ el $\text{mcd}(m,q) = 1$ y por el teorema de Fermat $m^{(q-1)} = 1$ (mód. q).

Aplicado a la igualdad de partida:

$$(m^e)^d = m^{e \cdot d} = m^{k \cdot \varphi(n)+1} = m^{k \cdot \varphi(n)} \cdot m = (m^{\varphi(n)})^k \cdot m \equiv$$
$$\equiv (m^{(q-1)})^{k(p-1)} \cdot m \text{ (mód. } n) = 1^{k(p-1)} m = m \text{ (mód. } q),$$

con lo que se determina que existe un valor B de manera que

$$m^{de} - m = Bq. \qquad (2)$$

De las expresiones (1) y (2) se puede afirmar que $p \cdot q = n$ divide a $m^{de} - m$, luego $m^{de} - m \equiv 0$ (mód. n).

El proceso es análogo para el caso de considerar q.
En el caso de que m sea múltiplo de p y q simultáneamente, el resultado es trivial.
En consecuencia,

$$(m^e)^d \equiv m \text{ (mód. } n).$$

Y el cifrado del algoritmo RSA queda demostrado.

Bibliografía

FERNÁNDEZ, S., *La criptografía clásica*, Revista *Sigma* nº 24, abril 2004.

GARFUNKEL, S., *Las matemáticas en la vida cotidiana*, Madrid, COMAP. Addison-Wesley, UAM, 1998.

GÓMEZ, J., *De la enseñanza al aprendizaje de las matemáticas*, Barcelona, Paidós, 2002.

KAHN, D., *The Codebreakers: The Story of Secret Writing* [=Los rompedores de códigos: Historia de la escritura secreta], Nueva York, Scribner, 1996.

SINGH, S., *Los códigos secretos*, Madrid, Editorial Debate, 2000.

TOCCI, R., *Sistemas digitales. Principios y aplicaciones*, Prentice Hall, 2003.

Índice analítico

NATIONAL GEOGRAPHIC

Matemáticos, espías y piratas informáticos

La integridad y confidencialidad de las comunicaciones dependen de complejos códigos diseñados gracias a la matemática. Este libro propone un estimulante viaje a la aritmética de la seguridad y el secreto, con paradas, entre otras, en los cifrados que han decidido el destino de las naciones y en el lenguaje con que se comunican los ordenadores.

FL
FreeLibros

El mundo es matemático