

TEMAS 36

INVESTIGACION y CIENCIA

Edición española de SCIENTIFIC AMERICAN

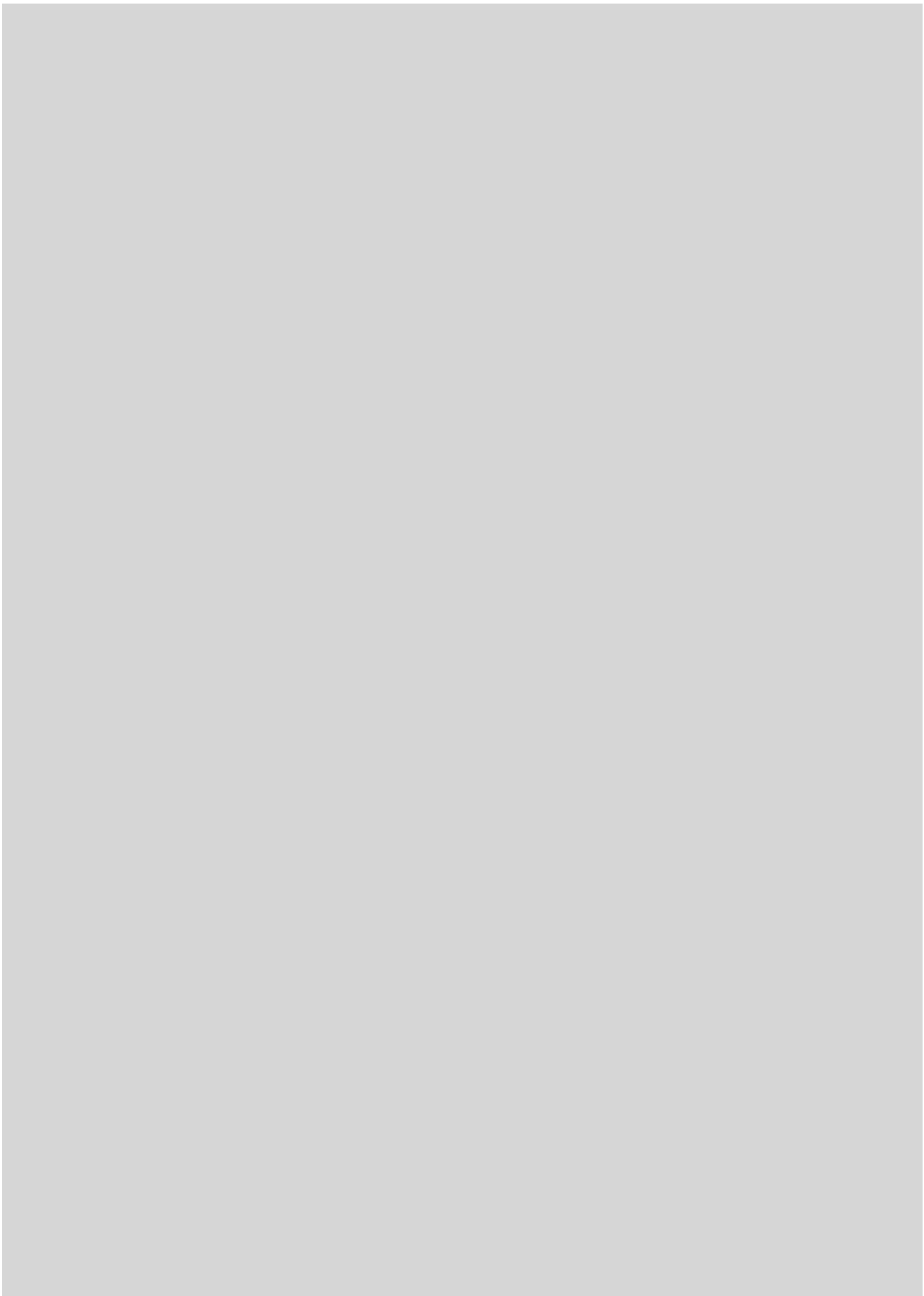
La información

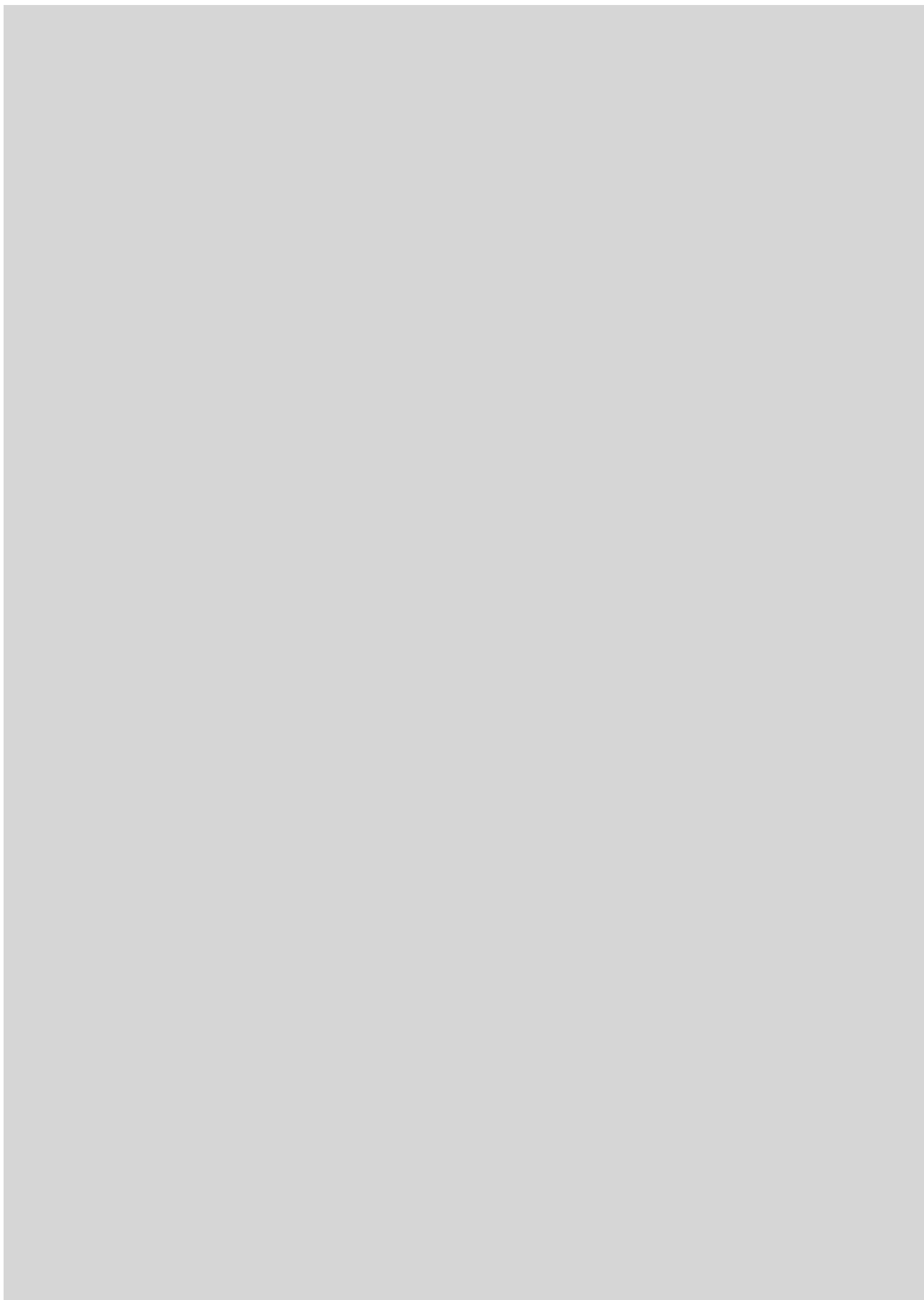


2º trimestre 2004



6,50 EURO





Sumario

CUANTIFICAR LA INFORMACION

4 Los orígenes del código binario

F. G. Heath

12 El geómetra de la información

Jérôme Segal

16 La información en el universo holográfico

Jacob D. Bekenstein

24 Un Alan Turing desconocido

B. Jack Copeland y Diane Proudfoot

ALMACENAR LA INFORMACION

32 Nanounidades de memoria

Peter Vettiger y Gerd Binnig

40 DVD

Alan D. Bell

46 El primer siglo de las memorias magnéticas

James D. Livingston

52 ¿Son perdurables los documentos digitales?

Jeff Rothenberg

58 La crisis de las memorias masivas

Jon William Toigo

TRANSMITIR LA INFORMACION

72 Criptografía para Internet

Philip R. Zimmermann

79 Láser en el kilómetro final

Anthony Acampora

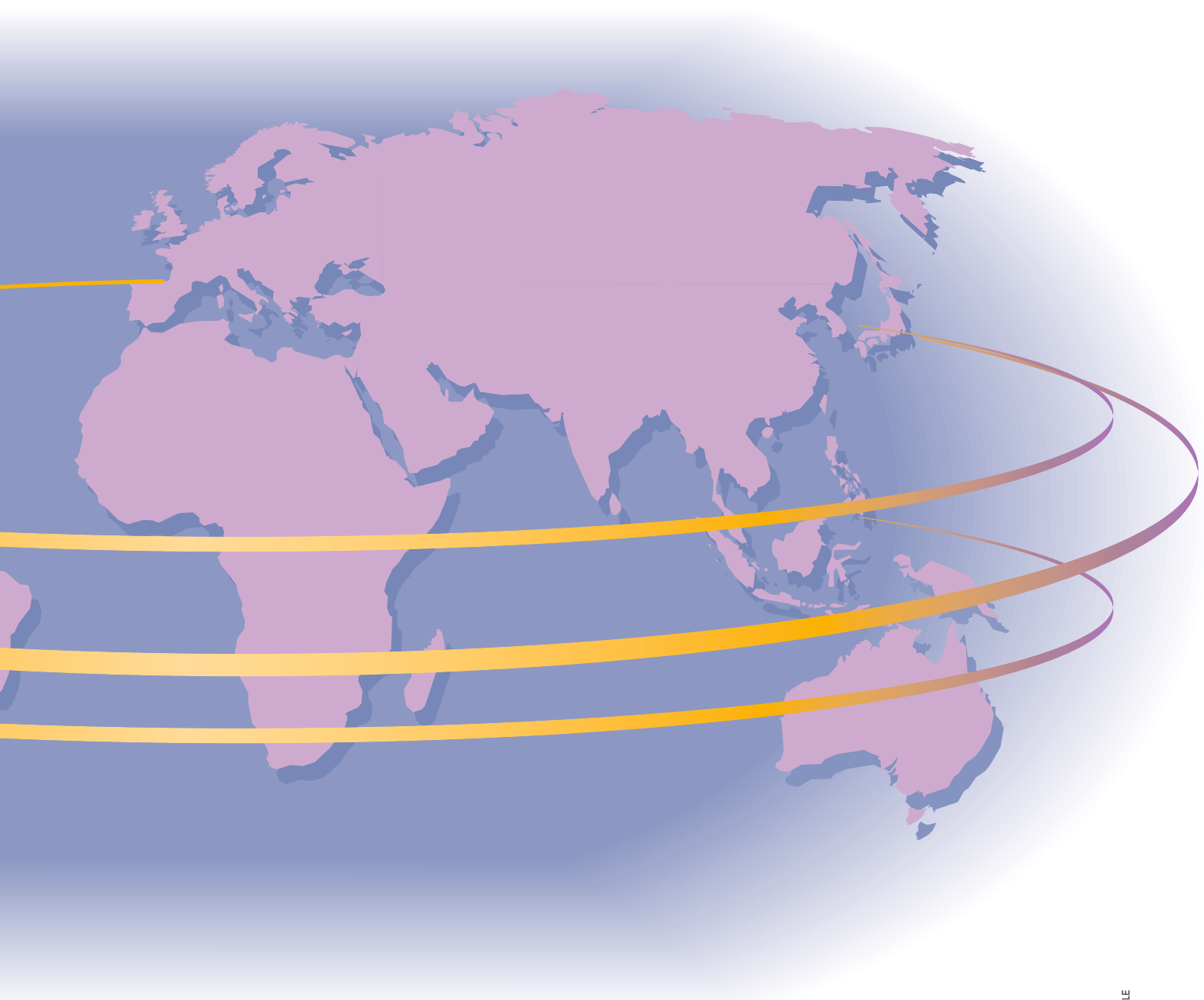
84 Informatización del hogar

W. Wayt Gibbs

90 Antenas adaptables

Martin Cooper

CUANTIFICAR LA INFORMACION



Los orígenes del código binario

Los antecedentes de este elemento clave para los sistemas de cómputo modernos se remontan hasta el siglo XVII. Francis Bacon se valió entonces de una treta tipográfica binaria para codificar sus mensajes secretos

F. G. Heath

El sistema binario de numeración se ha convertido en un elemento básico para la tecnología moderna. Sirve como medio de cómputo en los ordenadores digitales, así como de sistema de control en una infinidad de mecanismos. Sin embargo, pocos conocen la historia de este código o los personajes que protagonizaron los descubrimientos más importantes en este campo. Describiré en estas páginas cuatro de tales descubrimientos, las aportaciones de cuatro hombres que enfocaron la cuestión desde distintos ángulos. Fueron éstos Francis Bacon (1561-1626), cuyo código *omnia per omnia* para enviar mensajes secretos era en realidad binario; Joseph Marie Jacquard (1752-1834), quien diseñó un sistema para el control de telares basado en tarjetas perforadas, de código binario; George Boole (1815-1864), matemático inglés cuya álgebra proposicional constituye la base de la lógica computacional; y Emile Baudot (1845-1903), que tanto contribuyó a la telegrafía con su código de permutación cíclica.

El sistema binario de numeración solamente utiliza dos símbolos: 0 y 1. De ahí su nombre. El sistema decimal, que nos resulta más familiar, se basa en los números que van del 0 al 9. En el sistema binario, las diez unidades del sistema decimal se expresan como sigue:

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

El lector podrá observar que cada paso adelante en este sistema lleva al número inmediatamente mayor que podemos formar con las cifras 0 y 1. En la conversión (de decimal a binario) de un número un poco mayor como el 41, por ejemplo, la misma progresión produce 101001. Para convertirlo de nuevo en decimal debemos leer las cifras binarias de derecha a izquierda en forma de potencias crecientes de 2. Así, en este ejemplo concreto se comprueba que hay un 1, ningún 2, ningún 4, un 8, ningún 16 y un 32, por lo que tenemos $1 + 8 + 32 = 41$.

En el cálculo mental que usamos para resolver pequeñas operaciones, la codificación binaria no ha sido tan fructífera. Las largas ristas de ceros y unos ejercen un efecto hipnótico que dificulta su reconocimiento y manejo. Probablemente la única aplicación del sistema binario en la computación no mecanizada haya sido la “multiplicación del campesino ruso”: los dos números a multiplicar se escriben uno junto a otro (como, por ejemplo, en 10×12); el número de la izquierda se divide por 2 (sin tener en cuenta la parte fraccionaria del resultado) al tiempo que se duplica el número de la derecha; a continuación se tachan en la columna de la derecha todos los números situados frente a números pares en la izquierda; el cálculo termina sumando todos los números que aún queden a la derecha. En el ejemplo de 10×12 se procedería como sigue:

$$\begin{array}{r}
 10 \times 12 \\
 5 \quad 24 \\
 2 \quad 48 \\
 1 \quad 96 \\
 \hline
 120
 \end{array}$$

Aunque se opera en la notación

decimal, este método se vale de procesos binarios.

El sistema binario muestra su gran valor en operaciones de naturaleza binaria: encendido o apagado, abierto o cerrado, verdadero o falso, seguir o parar, y así sucesivamente. Un componente electrónico de un ordenador se encuentra activo o inactivo. La información que aporta el que esté en uno o en otro estado recibe el nombre de bit, palabra construida truncando la frase “binary digit” (“dígito binario” en inglés). Esa es la razón por la cual el sistema binario resulta tan eficaz para el cálculo computacional.

El alfabeto binario de Bacon

La aportación de Bacon no corresponde al cómputo sino a la codificación. Fue el primero en idear conscientemente un código binario y en describir sus propiedades. Se proponía desarrollar una clave para sus mensajes diplomáticos secretos. En primer lugar, estableció para cada una de las 24 letras del alfabeto inglés (que en aquella época no incluía las letras *v* y *j*) un código binario de cinco letras compuesto por diversas combinaciones de *a* y *b*: la letra *a* se traducía en *aaaaa*, la *b* en *aaaab*, y así sucesivamente hasta la *z*, sin repetir ningún grupo de cinco letras. (Bacon pudo asimismo haber hecho que los símbolos del código fueran 0 y 1.)

El segundo elemento de la clave de Bacon consistió en un “alfabeto biforme”. Se trataba de utilizar dos tipos de letra ligeramente distintos para imprimir un mensaje aparentemente inocente. Uno de los tipos representaba la *a* de su código binario; el otro denotaba la *b*. Por ejemplo, una *G* mayúscula de un cierto tipo de letra podría representar una *a*, la segunda *G* se tomaría de otro tipo de

letra y representaría una *b*; dos *g* minúsculas se diferenciarían de modo similar.

Para dar un ejemplo, el propio Bacon propuso la codificación del mensaje “fuge”, que en latín significa “huye”. Examinando las agrupaciones de cinco letras se comprueba que la *f* se traduce en *aabab*, *u* en *baabb*, *g* en *aabba* y *e* en *aabaa*. Ahora es preciso formular un mensaje “exterior” que abarque el mensaje “interior”; el mensaje exterior de Bacon fue “Manere te volo, doneo venero”. La *M* y la *a* habrían de ser impresas con el tipo de letra representativo de la *a*, la *n* se tomaría de la letra del tipo

b, la *e* del tipo *a* y la *r* del tipo *b*, lo que proporcionaría la letra *f* a quien dispusiera de la clave. Partiendo del mensaje exterior, uno acabaría con la siguiente secuencia: *aababb aabbaa bbaaa baa[aaa]*. Agrupando las letras en grupos de cinco, se obtendría la versión codificada de *fuge*.

Bacon hizo breve mención del código en 1605, en *Of the Advancement of Learning*. Lo describió por completo en *De augmentis scientiarum*. El objetivo fundamental y la naturaleza binaria del código fueron enunciados como sigue en un pasaje de esta última obra: “Estos caracteres-cifras no son nada baladíes: pues por este *arte* un

camino se abre, por cuya virtud puede un hombre expresar y dar significado a sus pensamientos a cualquier distancia, mediante objetos que puedan verse y oírse; suponiendo, únicamente, que éstos admitan sólo una doble condición. Para ello sirven campanas, trompetas, luces y antorchas, mosquetes y cualesquiera instrumentos de similar naturaleza”.

Si bien Bacon opinaba que la disposición binaria proporcionaba el código más efectivo, él mismo ideó y utilizó otros sistemas criptográficos. En uno de ellos, empleaba palabras clave para señalar párrafos de lugares sin relación que, ensamblados,



1. EL TELAR JACQUARD, desarrollado en Francia a principios del siglo XIX por Joseph Marie Jacquard, constituye la primera máquina de producción con control binario. Opera mediante tarjetas perforadas. Estas gobiernan el alzamiento de la urdimbre (hilos longitudinales) de forma que la lanzadera, que contiene la trama (hilos transversales), se entrecruce con la urdimbre tejiendo un determinado motivo. Las tarjetas pasan y se apoyan sobre un bloque cuadrangular de madera. Cada una de las caras del bloque tiene un conjunto de perforaciones enfrentadas a un ar-

reglo horizontal de agujas unidas a ganchos que alzan los hilos de la urdimbre. Cuando las agujas se dirigen hacia el bloque de madera, topan con una tarjeta. Las que encuentran una perforación, siguen su camino hasta penetrar en el orificio del bloque y alzan el hilo de urdimbre correspondiente. Las que no encuentran perforación, quedan bloqueadas; su gancho se desvía y el hilo de urdimbre no se alza. El número de tarjetas necesarias en cada caso es igual al número de hilos de la trama del motivo que se pretende tejer.

componían el mensaje secreto. Tal esquema aparece ahora en los ordenadores con el nombre de “descriptor” o “método de direccionamiento indirecto por palabras clave”.

El telar de Jacquard

De forma parecida, el telar de Jacquard constituye el ancestro de muchos de los aparatos digitales que se utilizan hoy en día. Aunque más reciente, la pianola representaría otro antepasado de la misma familia. Sin embargo, ninguno de estos artificios puede considerarse, estrictamente, un prototipo de los equipos modernos: sus mecanismos son binarios por naturaleza, mientras que las máquinas actuales requieren procesos más complejos. En un telar, cada hilo de la urdimbre concreto se levanta, o no, al pasar la lanzadera; en una pianola, se hace sonar, o no, una nota en un momento determinado. Con todo, el telar Jacquard fue la primera máquina de control binario que se utilizó extensamente.

El desarrollo del telar puede resumirse como sigue. Cuando la industria textil empezó a interesarse por la fabricación de telas con motivos tejidos (no estampados), recurrió en primera instancia a un sistema manual: un aprendiz se encargaba de ir levantando hilos de la urdimbre para que se pasasen entre ellos los de la trama (en un telar, los hilos de urdimbre se colocan en sentido longitudinal; los de trama, en el transversal). Durante el siglo XVII, se inventaron en Italia y en Francia mecanismos que subían y bajaban los lizos. Estos dispositivos reducían la mano de obra pero el telar seguía exigiendo un ope-

riario. En 1725, Basile Bouchon ideó un sistema en el cual los hilos de la urdimbre se controlaban mediante papel perforado y un conjunto de agujas. En 1728, Jean Falcon propuso utilizar una tarjeta para cada separación de la urdimbre en hilos levantados y no levantados. En 1745, Jacques de Vaucanson construyó un telar que incorporaba las ideas de Bouchon y de De Falcon.

En 1801 este telar se encontraba averiado. Jacquard, tras promocionar su maquinaria textil en una exposición, gozaba de una reputación de experto. Así que Napoleón le convocó a París para que trabajara en la máquina de De Vaucanson. Su contribución consistió en reemplazar el cilindro que portaba las tarjetas perforadas por un montaje prismático. Ello permitía colocar, en el orden adecuado, muchas más tarjetas en un mismo telar. Esta modificación estuvo respaldada por una ingeniería de alta precisión, lo que resultaba de vital importancia para un mecanismo que requiere tolerancias mecánicas estrictas (un concepto original en aquellos tiempos).

El telar perfeccionado se construyó en 1804. Hacia 1812 funcionaban en Francia unos 11.000 telares Jacquard. A pesar de las tensas relaciones entre ambos países, la innovación se propagó hasta Inglaterra. En 1834 había ya en Coventry 600 telares Jacquard. Muchos de ellos se instalaron en viviendas de los propios obreros. Funcionaban mediante ejes y correas accionados por máquinas de vapor.

Se ha dicho a veces que Jacquard, en realidad, no inventó nada. Tal acusación parece injusta. La modificación que introdujo, utilizar superfi-

cies planas en el portador de tarjetas, resultó decisiva. Además, el uso generalizado de telares fácilmente reprogramables, aptos para tejer cualquier motivo, puede considerarse también resultado directo de su trabajo.

Del telar Jacquard emanaron dos desarrollos importantes. Por un lado, Charles Babbage, quien concibió el primer ordenador digital en el siglo XIX, llegó a la conclusión de que el método óptimo para introducir datos en su máquina consistía en usar tarjetas perforadas, inspiradas en las de Jacquard. Ello suponía una aplicación genuina de la codificación binaria. Por otro lado, muchas de las subrutinas y los sistemas de corrección usados en los ordenadores modernos se concibieron en el siglo XIX con el objetivo de diseñar tarjetas perforadas para tejer motivos en la ropa. Transformar un dibujo en una secuencia binaria para tejerlo equivale a traducir un programa escrito en un lenguaje de alto nivel (Fortran, C++, etc.) a su código binario correspondiente, expresado en lenguaje máquina (apto para el ordenador). En efecto, la conexión entre tejer una tela y diseñar un sistema de cómputo es muy estrecha. Veán sino el parecido que muestran el cableado de un ordenador o la imagen ampliada de un circuito integrado complejo con los dibujos tejidos en la ropa.

El problema que resolvieron Jacquard y sus predecesores afecta hoy a otros sectores industriales. Consiguieron tejer motivos muy diferentes en un mismo telar, el cual podía cambiar rápidamente de un patrón a otro. Los fabricantes de aparatos electrónicos, por ejemplo, requieren proce-



2. LOS TEJIDOS Y LOS CIRCUITOS, vistos muy de cerca, presentan gran semejanza a causa de la conexión con los sistemas binarios. En un tejido, el elemento binario es el punto, que puede consistir en

un hilo horizontal sobre uno vertical o viceversa. En el circuito integrado, determina el carácter binario la conductividad eléctrica de cada región, que será metálica o aislante.