Felipe II, el diablo y las matemáticas

Por Antonio Córdoba

Antonio Córdoba *(Murcia, 1949) es matemático. Ha publicado artículos de investigación en Análisis Armónico, Teoría de los Números, Ecuaciones Diferenciales y Física Matemática. Doctor por la Universidad de Chicago y catedrático de la Universidad Autónoma de Madrid, ha sido profesor de la Universidad de Princeton y miembro del Institute for Advanced Study. Fundó la* Revista Matemática Iberoamericana.

Felipe II fue paladín de la causa católica, pero también demonio del mediodía para muchos de sus súbditos holandeses. Como rey de España, que era la gran potencia del siglo XVI, ejerció un poder inmenso. Ahora, en estos comienzos del XXI, se han celebrado exposiciones tanto del reinado de su padre, el emperador Carlos V, como del suyo propio, y se han realizado estudios y publicado ensayos y monografías en torno a ambas figuras históricas.

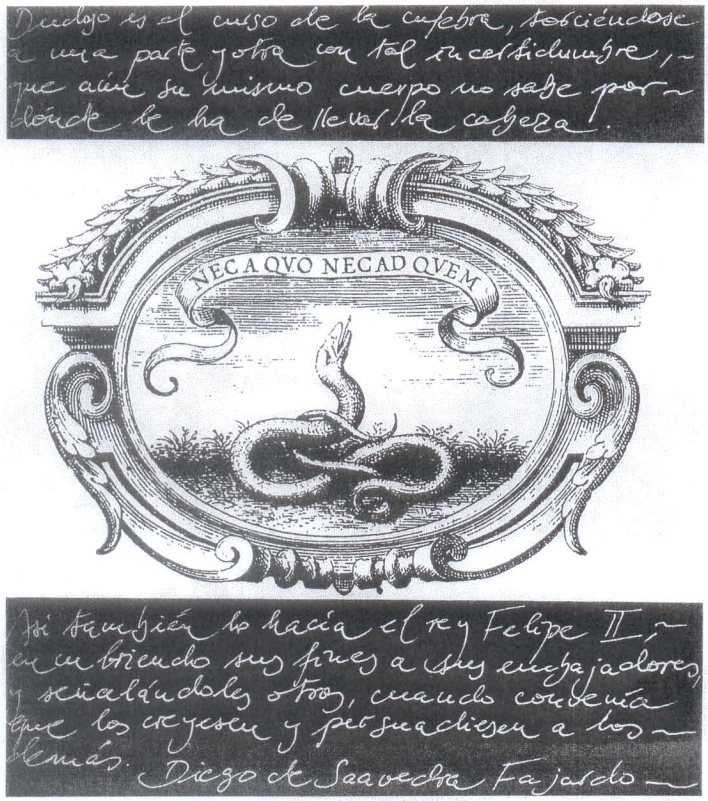
Hay un episodio del reinado de Felipe II que no ha sido suficientemente resaltado y que, sin embargo, ilustra de manera fehaciente sobre las limitaciones de su manera de gobernar. Seguramente el gran rey contaba entre sus asesores con avezados políticos, militares, hombres de iglesia, incluso artistas, y también, cómo no, se vería rodeado de intrigantes de la más diversa condición. Pero no parece que entre ellos hubiera nadie que estuviese al tanto de los avances científicos de su tiempo.

Antes de entrar de lleno en la descripción de ese episodio, conviene que presentemos a otro de sus protagonistas. Se trata de François Viéte (1540-1603), o Franciscus Vieta si nos atenemos a la versión latina, un hombre de leyes que ejerció un cargo de cierta relevancia en el tribunal de apelaciones de París durante el reinado de Carlos IX, pero que luego fue asesor real en los turbulentos años de los reinados de Henri III y de Enrique de Navarra (Henri IV).

Sin embargo, Vieta debe su notoriedad a las matemáticas. Está considerado como el padre del Álgebra, por ser el primer autor que introdujo el cálculo simbólico, operando con letras y con números, en sus esfuerzos por sistematizar el estudio de las ecuaciones de tercer y cuarto grado, cuyas soluciones habían sido obtenidas por los italianos del Ferro, Tartaglia, Cardano y Ferrari. Vieta estudiaba matemáticas por afición, en sus ratos libres, exactamente igual que hizo su paisano Pierre de Fermat, también con notable éxito, medio siglo más tarde.

Durante la guerra franco-española de 1589-90, Vieta descifró para Enrique de Navarra varias cartas del rey Felipe II, codificadas en un «complicado» sistema homofónico que usaba dos símbolos distintos para las consonantes y tres para las vocales. Además de otros específicos para términos habituales, tales como: España (leu), Francia (pe), armada (om), capitán (ne), Génova (tura), o Cataluña (ti). Las cartas estaban dirigidas al duque de Alba, a don Juan de Austria y a otros personajes importantes. Contenían información muy valiosa, por lo que al caer en manos de Enrique IV, del Papa, o de sir Francis Walsingham, ministro de la reina de Inglaterra, contribuyeron grandemente a desbaratar los planes de su cristianísima majestad.

Cuando Felipe II supo que había sido descubierto el sistema de codificación que su corte creía segurísimo, se dirigió al Papa acusando a los franceses de haber utilizado magia negra y de tener un pacto con el diablo, pues de otra forma no podía explicarse el asunto. Pero el Papa, que también era un rival de la corona española, tenía su propio especialista en descifrar mensajes, Giovanni Batista Argenti, y conocía la existencia y las habilidades de Vieta. Por lo que se ocupó en dar publicidad a las



STELLA WITTENBERG

ridículas conjeturas de Felipe II, provocando la hilaridad entre sus numerosos enemigos europeos.

Huelga decir que este asunto tiene bastante más miga. Podríamos añadir otros nombres, así como precisar fechas y detalles. Sin ir más lejos, mientras escribo estas líneas, tengo a la vista cientos de fotocopias de los archivos de Simancas que contienen diferentes métodos de cifrado que fueron usados durante el reinado de Felipe II. Letras, números y símbolos ingeniosos, pero con un sistema de sustitución que no era difícil de desvelar para los expertos del siglo XVI. Resulta patético observar cómo el hombre más poderoso de la Tierra, en cuyo reino no se ponía el sol, señor de grandes ejércitos y campeón de la contrarreforma, que planeó operaciones tan complicadas como la invasión de Inglaterra, no contaba entre sus asesores, políticos, militares y hombres de iglesia, con alguien dotado de los conocimientos necesarios para asegurar el secreto de su correspondencia.

Los códigos secretos

Esa anécdota del reinado de Felipe II está narrada en el libro que nos proponemos comentar: *Los códigos secretos* de Simon Singh, cuyo subtítulo reza: «El arte y la ciencia de la criptografía, desde el antiguo Egipto a la era de Internet». También recoge otras historias no menos jugosas, como la que atañe a María Estuardo, reina de Escocia, cuya correspondencia fue interceptada y descifrada por el poderoso Walsingham. Hecho que fue crucial en el desarrollo del juicio en el que fue condenada a muerte por el tribunal de la reina Isabel I de Inglaterra. Según se expone en el libro de Singh, el nacimiento de las claves secretas se remonta a los tiempos de Julio César. Los códigos de sustitución son versiones más o menos sofisticadas del sencillo método del emperador, consistente en efectuar una permutación de las letras del alfabeto. Empero, la debilidad de todos ellos radica en la diferente frecuencia con que las diversas letras aparecen en un texto. El autor, Simon Singh, aunque no es un experto en criptografía, muestra una sólida formación científica y domina el arte de divulgar, como muy bien demostró con su documental sobre *El último teorema de Fermat*. El libro está escrito en un estilo ameno, que resulta asequible para un lector sin especial formación matemática. La traducción al castellano es, en general, correcta, aunque no exenta de sobresaltos, tales como: «...doceava letra del alfabeto hebreo, que es reemplazada por kaph, la doceava empezando por el final» (¡Ay, los ordinales!).

En un nivel algo más serio existe la obra monumental de David Kahn *The Codebreakers* (Scribner, Nueva York), de la que ha aparecido recientemente una nueva edición, y que recomiendo con entusiasmo a quienes se interesen por estos temas.

Un giro importante en la evolución de la criptografía tuvo lugar en torno al año 1918, cuando el ingeniero Arthur Scherbius creó la máquina cifradora Enigma, que fue utilizada por el ejército alemán durante la II Guerra Mundial. Dotada de un sistema de rodillos, cada uno con una permutación distinta del alfabeto, forzados a rotar después de cada pulsación, y de un clavijero, la máquina Enigma resultaba invulnerable a los análisis de frecuencia, debido a la cantidad inmensa de las permutaciones involucradas que iban cambiándose con cada símbolo escrito. No obstante, el ejército de Polonia reunió un grupo de matemáticos, entre los que destaca Marian Rejewski, que fue capaz de encontrar el punto débil de Enigma y leer sus mensajes. Los trabajos de este grupo fueron comunicados al servicio secreto británico, creándose una unidad dirigida por Alan Turing, que logró descifrar las versiones más sofisticadas de Enigma mediante ingeniosas estrategias matemáticas y potentes métodos de cálculo. Este episodio es narrado también en el libro que comentamos, y representó un punto de inflexión en el estilo de la criptografía y en sus personajes: de un oficio de diletantes versados en lenguas pasó a ser una parte de las matemáticas que hace uso de métodos sofisticados de álgebra, teoría de los números, combinatoria, probabilidad y, por supuesto, de poderosas máquinas calculadoras.

Las dos culturas: Ravelstein

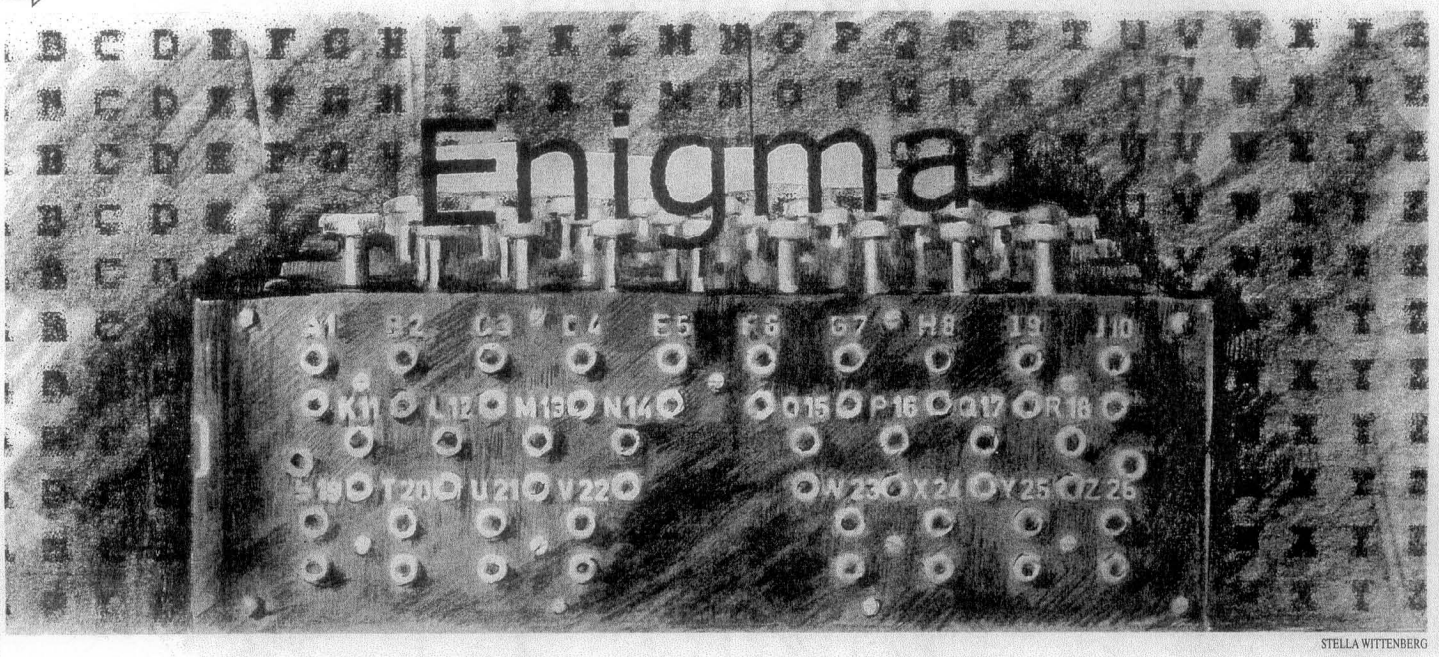
En la última novela del premio Nobel Saul Bellow, el personaje Ravelstein sostiene que «entre los científicos son escasos los ejemplos de grandes personalidades. Filósofos, pintores, estadistas, abogados, de gran categoría si los había. Pero grandes espíritus, hombres o mujeres, en el campo de la ciencia, son extremadamente raros». «Lo grande es su ciencia, no las personas», apostilla Chick, trasunto del autor, que en la novela refiere los pormenores de su vida matrimonial con Vela, una física del caos de la que se había divorciado. Casi como el propio Bellow, que lo hizo de una especialista en análisis matemático.

No es el único caso de espléndido narrador que ve en los científicos a seres un tanto anodinos, pero tampoco es mi intención combatir esa imagen con otra de características más favorables. Por el contrario, más bien conozco suficientes ejemplos para creer que entre los científicos, como en todo colectivo amplio, se dan los cultos y los ignorantes fuera de su área, los divertidos y los aburridos, los sagaces, los estúpidos y los mediopensionistas, en proporciones arbitrarias y, con frecuencia, bastante sorprendentes. Además, en un país tan invertebrado científicamente como España, no son siempre los más brillantes en sus campos quienes son escuchados por la feliz gobernación, en las pocas ocasiones en las que esa situación se presenta. Incluso en un mundo tan austero como es el de la ciencia, puede aplicarse el comentario de Francis Bacon de que «la fama es como un río que lleva a la superficie los cuerpos ligeros e hinchados y sumerge a los pesados y sólidos».

Bellow ha sido profesor de literatura en las universidades de Princeton y de Chicago, que son dos instituciones favoritas de todo matemático. El primero es un pequeño pueblo del estado de New Jersey, situado a una hora escasa de Nueva York, conocido por su universidad y por el Instituto de Estudio Avanzado (IAS), que es el lugar donde ejercieron Albert Einstein, Kurt Gödel y John von Neumann, quien, entre otras muchas razones, es famoso por haber diseñado y construido el primer ordenador moderno. Es también uno de los creadores de la teoría de juegos, aplicada a la guerra y a los modelos económicos. Cuando yo era allí un joven profesor, don Vicente Llorens estaba a punto de jubilarse de su cátedra en el departamento de literatura española. Tuve, no obstante, la oportunidad de tratarle y de participar en algunas de las tertulias que se organizaban en el club de profesores en torno a su persona. Recuerdo aún sus palabras en la reunión que, espontáneamente, se congregó en mi casa aquel día de otoño del 75, y que expresaban su emoción por haber sobrevivido al principal causante de tanta desgracia. En Princeton fue también profesor don Américo Castro, pero eso ocurrió mucho antes de mi llegada. Me parece interesante señalar que en esa famosa universidad americana enseñaron dos intelectuales españoles exiliados de la talla de don Américo y don Vicente. No obstante, con todo mi afecto y mi respeto por dos figuras tan señeras de nuestra cultura, creo que sería una muestra de sórdido narcisismo pensar que los hispanis-

➡

Viene de la página anterior



STELLA WITTENBERG

tas son una parte muy importante de la grandeza intelectual de aquel sitio. Princeton es uno de los pocos lugares del mundo en el que los matemáticos, y los físicos, representan el canon intelectual. Eso se nota hasta en el callejero, la arquitectura, y en la influencia ejercida en el complejo económico, político y de seguridad de Estados Unidos.

Durante el año 1976 el director del IAS quiso «fichar» a un sociólogo, que era catedrático en una universidad de prestigio. Los matemáticos del Instituto, capitaneados por André Weil, se opusieron rotundamente y protagonizaron un agrio debate público. En retrospectiva, podríamos achacarles, con cierta justicia, haber tenido un interés corporativo, por cuanto ese fichaje implicaba el aumento de las escuelas del IAS, con la consiguiente pérdida de poder específico para el grupo de físicos y matemáticos. En cualquier caso, al final se impuso la decisión del director. Pero las armas intelectuales que se esgrimieron fueron poderosas y el análisis de los trabajos del eminente sociólogo, a la luz de los criterios de los matemáticos, resultó demoledora: libros pletóricos de lugares comunes, afirmaciones sin demostrar o con demostraciones falsas, y páginas y páginas que podían ser resumidas en una simple frase. Constituyó una exhibición de lo peligroso que resulta usar el criterio de una disciplina tan austera, como son las matemáticas, para juzgar a las demás. Claro que en la vida diaria tenemos a menudo suficientes muestras de valoraciones que propugnan todo lo contrario. Por cierto, el mencionado André Weil, fallecido hace apenas unos años, fue uno de los matemáticos más brillantes del siglo XX. Pero en España es más conocida su hermana, Simone Weil, cuya pintoresca y apasionada vida de monja progresista aparece, con cierta frecuencia, comentada en la prensa por nuestros intelectuales. Este episodio del IAS inspiró a A. Sokal (que era entonces estudiante de doctorado en Princeton) y a J. Bricmont la escritura, algunos años después, de su celebrado *Imposturas intelectuales* (Ediciones Paidós Ibérica, 1999, ISBN: 84-493-0531-4).

En la primavera de 1989, el embajador de España vino desde Washington a Princeton para condecorar al ilustre hispanista John Elliot con la gran cruz de Alfonso X el Sabio. Entre los asistentes al acto nos encontrábamos los miembros españoles del IAS, pero también estaban algunos distinguidos matemáticos del lugar que habían tenido, y seguían teniendo, una prolongada relación científica con España, a través de alumnos, colaboradores y múltiples publicaciones conjuntas. Pues bien, en nuestra embajada se desconocía la existencia de esos lazos estrechos de colaboración con científicos relevantes. No se trata, entiéndase bien, de cuestionar la justicia, o la oportunidad, de la condecoración otorgada a Elliot, autor de una espléndida obra y que une a su indudable categoría de historiador una gran simpatía personal, que podemos muy bien certificar quienes hemos disfrutado de su hospitalidad. Lo que quisiera subrayar es que nuestra diplomacia, y en general nuestra feliz gobernación, mira casi siempre en una única dirección. Como es natural, tengo una idea muy somera de las tareas que lleva a cabo nuestro servicio exterior. Pero entiendo que una de ellas será la de establecer contactos y tender puentes hacia personalidades relevantes y de prestigio que ejercen, por lo tanto, una influencia natural en la vida de su país. ¿Ha considerado alguna vez nuestra diplomacia las posibilidades que se podrían abrir a través de los contactos entre científicos?

Ciencia, potencia y violencia

Los logros del equipo de Alan Turing fueron un factor decisivo para la victoria aliada. En el mejor de los escenarios, la guerra se hubiera prolongado algunos años más de no haber podido leerse los mensajes cifrados de Enigma. Fue también necesario hacer creer al alto mando alemán que su sistema de codificación seguía siendo invulnerable. Lo que dio lugar a decisiones dramáticas, que han sido llevadas al cine y a la literatura, por cuanto evitar el bombardeo anunciado de una ciudad podía dar pistas a los alemanes de la fragilidad de Enigma. Después de la guerra las proezas de Turing se mantuvieron en secreto. De hecho, Inglaterra había capturado miles de máquinas Enigma y las distribuyó entre sus antiguas colonias, cuyos gobiernos creían que eran tan seguras como les habían parecido a los alemanes. De esta manera los británicos descifraron las comunicaciones secretas de esos países durante años. En cuanto a Turing, en vez de ser aclamado como un héroe, fue perseguido por su homosexualidad. Sufrió una gran depresión y en 1954, con solo 52 años, se suicidó. Antes, no obstante, había desarrollado la importante noción de máquina universal de Turing. Fue uno de los grandes lógico-matemáticos del siglo XX y junto a L. Church, de la Universidad de Princeton, está considerado como el fundador de la teoría moderna de la computabilidad.

El arte de cifrar cambió radicalmente cuando a finales de los setenta se descubrieron los sistemas de clave pública: el cifrado puede ser realizado por cualquiera. Pero el descifrado sólo puede llevarlo a cabo quien posea una información privilegiada. El fundamento de estos sistemas radica en la existencia de unas funciones trampa. Es decir, funciones f tales que sea fácil calcular $f(x)$, pero muy difícil, prácticamente imposible si no se está en el secreto, calcular la inversa $f^{-1}(y)$. Un ejemplo notable es el llamado sistema RSA, por las iniciales de sus creadores. Está basado en la función multiplicación $(p, q) \rightarrow n=pq$, aplicada a pares de números primos. La función inversa es el famoso problema de la factorización. Se calcula que al ordenador más potente del momento le llevaría miles de años factorizar un entero típico de trescientas cifras. El sistema RSA involucra a un teorema de Fermat-Euler, de hace unos tres siglos, junto con el uso sistemático de los modernos ordenadores, y está en la base de la seguridad de las comunicaciones, desde los ejércitos a Internet. Además del libro que comentamos, recientemente han aparecido las siguientes monografías que recomiendo al lector interesado: J. A. Buchmann, *Introduction to Cryptography* (Springer-Verlag, 2001, ISBN 0-387-9534-6); y Joseph Kirtland, *Identification Numbers and Check Digit Schemes* (Mathematical Association of America, 2001, ISBN 0-88385-719-7).

En 1990 tuve la oportunidad de conocer personalmente a Ernest Lluch durante su visita a la «joven» escuela de sociología del IAS. Lluch había entablado amistad con un matemático distinguido y profesor del Instituto, que era también mi colaborador y amigo. Enseguida hicimos planes para crear, dentro de la Universidad Menéndez Pelayo, una escuela internacional de Matemáticas codirigida por varios profesores del IAS y de la Universidad Autónoma de Madrid. El proyecto se convirtió en una realidad que funcionó divinamente: cursos de Ecuaciones Diferenciales, Mecánica de Fluidos, Teoría de Números y Criptografía, en los que participaron los mejores especialistas del mundo y se dotaron becas para estudiantes españoles y extranjeros. Para el rector de la UIMP esta escuela internacional de Matemáticas era un modelo del tipo de cursos que deseaba propiciar en la universidad de verano.

Cuando se ha perdido a un amigo, y mucho más cuando lo ha sido de forma tan injusta, es difícil evitar una rabia y tristeza profundas. Pero siempre queda el consuelo de recordar lo que hizo. En ese sentido hemos podido leer las semblanzas realizadas por personas que le fueron muy cercanas y que atestiguan de su entrañable humanidad y de su gran cultura. Por mi parte puedo añadir su demostrado interés para que las Matemáticas tuviesen un lugar destacado en la programación de la UIMP; y la añoranza de aquellas deliciosas veladas santanderinas en las que, socarrón, nos contaba historias tan divertidas como la estimulación, plumero en mano, del toro Sultán, que había sido adquirido por la administración cántabra para mejorar la cabaña. Pero, tras su vil asesinato, han proliferado en los medios de comunicación artículos y declaraciones de intelectuales y analistas políticos. La mayoría repitiendo los mismos lugares comunes y diluyéndose en tópicos, palabras y más palabras, que parecen lanzadas con la esperanza de encontrar algo que decir. Salvo en algunos pocos casos, decepciona la falta de claridad de los análisis, tanto en la determinación de los protagonistas, cuanto en la descripción de los escenarios, de los intereses, de las implicaciones y de las cuentas económicas. En general, se echa en falta la exigencia de que los argumentos esgrimidos sean adecuados, las premisas ciertas y las conclusiones pertinentes.

De vez en cuando, las autoridades nos informan acerca de los sofisticados métodos informáticos, de propaganda y de manejo de los fondos económicos, que utilizan las diversas organizaciones mafiosas y terroristas. Por encima de los comandos constituidos por individuos fanatizados, parecen dominar unos cuadros bien preparados y competentes en la administración lucrativa del terror. Solo cabe esperar, y desear, que los responsables políticos de nuestras democracias cuenten con los medios y con las personas preparadas para analizar los escenarios posibles y asesorarles en la toma de decisiones. ¿O acaso les ocurre como a Felipe II, rodeado de aficionados incompetentes, mientras Vieta trabajaba para su demonio? □

RESUMEN

A Antonio Córdoba, la lectura del libro que comenta sobre «los códigos secretos» y la importancia de la criptografía en los avatares históricos, y que recoge una significativa anécdota de Felipe II, un rey rodeado de todo tipo de asesores, pero no de científicos, le lleva a reflexionar sobre el papel que tienen que desempeñar los científicos en las sociedades modernas y cómo frecuentemente los políticos y gobernantes miran más hacia otro lado, en la vieja controversia entre las dos culturas, la científica y la humanística. La reflexión no le aparta, sin embargo, del núcleo de su artículo, que es el de la aportación de los matemáticos al lenguaje cifrado utilizado por los gobiernos y la diplomacia a lo largo de la historia.

Simon Singh

Los códigos secretos

Debate, Madrid, 2000.407 páginas. 17,50 euros. ISBN: 84-8306-278-x