Categoría: **Divulgación matemática**
Autor:
Simon Singh

Editorial:
Debate (también en Círculo de Lectores)

Año de publicación:
2000

Nº de hojas:
407

ISBN:
84-8306-278-X

El autor: Simon Singh es Ph.D. en Física de Partículas por la Universidad de Cambridge. Su principal campo de investigación ha sido el top quark. Ha trabajado en el Departamento de Ciencia de la BBC donde ha coproducido y dirigido un documental sobre «El último teorema de Fermat» para la serie Horizon (emitido también por la serie Nova de la EPS norteamericana) al que se le concedió el prestigioso premio Bafta. Tras dicha experiencia publicó su primer libro de divulgación: «Fermat,s Enigma» (1997) traducido para Planeta en 2000.

El libro: El libro presenta no sólo una historia de la criptografía (ciencia de la ocultación del contenido de un mensaje) y, por lo tanto, del criptoanálisis (método para recuperarlo) sino una descripción de su evolución desde la primeras codificaciones conocidas hasta los albores de la criptografía cuántica y sus perspectivas.

La elaboración de un mensaje entre dos seres tiene una componente de comunicación y una, no menos importante, de privacidad. Desde el mensaje entre dos enamorados hasta la comunicación entre dos unidades militares amigas separadas en el campo de batalla (o dos brockers en plena orgía bolsística), se nos pueden ocurrir millones de razones para que un mensaje sea sólo conocido por emisor y receptor, y para que multitud de ajenos deseen descifrarlo. Dos indios navajos pueden, en un zoco, diseñar en voz alta una estrategia de regateo que el vendedor árabe no tendrá tiempo de contraatacar.

La historia de este proceso iniciado en lo político y militar en la guerra de las Galias de César (citado en un tratado de Valerio Probo) con las llamadas cifras de sustitución es una historia dialéctica: se descubre un cifrado que es útil hasta que se descubre el método de descifrado

correspondiente que, a su vez, genera un cifrado mejor y así sucesivamente. Singh nos habla de la cifra de Vignole, la máquina Enigma y su impresionante entramado de espionaje y contraespionaje en la segunda guerra mundial, la interpretación del Lineal B por Ventris y Chadwick como griego antiguo y el actual enigma del Lineal A, la clave RSA y las comunicaciones bancarias y de la red de redes...

Se trata de un libro de divulgación, para no especialistas, pero no trivial. A veces directamente, a veces con apéndices, el sustrato matemático queda patente y por encima de todo una idea que ojalá haya trascendido tras el irregular Año Mundial de las Matemáticas: en muchos momentos de la historia el matemático es el científico adecuado para resolver el problema. Los servicios secretos ingleses se aperciben que lo que los lingüistas y los psicólogos son incapaces de resolver lo hacen los matemáticos con su lenguaje (las matemáticas como lenguaje de la ciencia). Turing es un ejemplo.

No olvida Singh las cuestiones éticas y legales del tema y aporta un buen número de lecturas adicionales e incluso páginas web donde el lector inquieto podrá saciar su sed de saber; con un pero: el quid de la cuestión es el secreto. Lo que se descubra hoy no se podrá conocer públicamente hasta que sea anecdótico su conocimiento y fuera de toda actualidad. ¿Se puede uno imaginar a un colega que descubra un resultado determinante en su disciplina y que lejos de correr a publicarlo tenga que morderse la, lengua y contentarse con saber que quizás esté siendo aplicado?

(Reseña aparecida en la revista En Breve vol. 1, no. 1, 2001)

- **Materias:** Criptografía, codificación, lenguaje
- **Autor de la reseña:** Rafael Crespo (Universitat de Valencia)