Documenta & Instrumenta
ISSN-e: 1697-3798

http://dx.doi.org/10.5209/rev_DOCU.2018.v16.60242

EDICIONES COMPLUTENSE

Carlos TARANILLA DE LA VARGA, *Criptografía. Los lenguajes secretos a lo largo de la Historia*, Córdoba, Guadalmazán, 2018, 297 pp. ISBN: 978-84-94608-59-9.

José Ramón Soler y Francisco Javier López-Brea, en su monografía publicada a finales del año 2016 *Mensajes secretos. La historia de la criptografía española desde sus inicios hasta los años 50*, exponían que "la aparición de un libro dedicado a la criptografía ya no es noticia". Bien es verdad que hasta no hace mucho tiempo la mayoría de las publicaciones sobre esta disciplina científica versaban más sobre aspectos técnicos que sobre históricos. Sin embargo, aunque conviene precisar que todavía quedan considerables cuestiones y perspectivas que investigar desde la consideración de "criptografía de lápiz y papel", esta alternativa ha sido objeto de estudio en diversas publicaciones del presente siglo con una cierta frecuencia.

En esta ocasión, Carlos Javier Taranilla de la Varga se acerca a esta materia desde una visión divulgativa, sin obviar el cientifismo que siempre ha acompañado a sus obras. Desde un enfoque histórico realiza un repaso de la criptografía desde la antigüedad hasta nuestros días. El propio autor, en el preámbulo, revela que el lector, con este libro, tiene la ocasión de ejercitar su mente, *se irá asombrando de hasta dónde arribó el ingenio de nuestros antepasados para comunicarse "sin ser vistos u oídos", es decir, entendidos por terceras personas*.

Después de un capítulo introductorio, relativo al concepto, claves, códigos y sistemas de cifrado (trasposición y sustitución), siguiendo un criterio histórico-cronológico, analiza los principales procedimientos criptográficos.

De este modo, en el primer capítulo -centrado en la Edad Antigua-, analiza entre otros el método del escítalo, las cifras chinas y hebreas, el código de Polibio, la clave de Julio César, la escritura jeroglífica egipcia, la plancheta de Eneas o el cifrado del *Kamasutra*.

En el siguiente, que abarca el periodo medieval, destacan los análisis relativos a la tabla del abad Tritemio y a los alfabetos zodiacal, templario, benedictino y masón.

El Renacimiento y la Edad Moderna son los objetivos del tercero. En él estudia tanto sistemas sustitutivos (el disco de Alberti, los polífonos de Cardano, la tabla de Della Porta o las cifras de Yvry, Vigenère, Bellaso, Gronsfeld...) y esteganográficos (el alfabeto binario de Francis Bacon, la escritura especular de Leonardo da Vinci, la rejilla de Cardano o los alfabetos trífidos de Vigenére, Wikins y Friderici), como códigos (las cifras de Felipe II, Richelieu, María Antonieta o Rossignol).

Del mismo modo, son diversos los métodos y códigos analizados en el capítulo coincidente con la centuria decimonónica. Entre otros, cabe citar las cifras de

Chappe, Wheaststone, Auvray, Hirsch, Delastelle, Chase, Colon, Playfair, Slidefayr, Saint-Cyr, Beaufort, lord Wolseley, Beale, Bazeries, Morse, etc.

Con la misma sistematización que en los anteriores capítulos, en el quinto se centra en la criptografía durante el siglo XX. En esta ocasión, distribuye el examen de los principales procedimientos empleados durante esta centuria en cuatro períodos claramente diferenciados. Uno hasta el comienzo de la Primera Guerra Mundial, otro en referencia a este conflicto bélico, el tercero a la Segunda Guerra Mundial y el último a la década de los 60's. A lo largo de las páginas de esta sección desfilan métodos cifradores tales como el de Grandpré, Fleissner, Zimmerman, el Che Guevara, Vernan o el telegráfico de Sittler, sin olvidar los códigos navajo, euskera o de las máquinas *Enigma*, *Hageli*n o *Colussus*.

El penúltimo capítulo está dedicado a la criptografía coetánea, y más concretamente a su interrelación con la informática.

Por último, el *Manuscrito Voynich* es el tema central del capítulo final, "el mayor reto de la Criptografía actual", en palabras del profesor leonés. En su exposición alcanza hasta la propuesta de Nicholas Gibbs en septiembre de 2017, quien afirmó haberlo descriptado y que versaba sobre un tratado de buenos usos y costumbres ginecológicas para damas de la alta sociedad. Bien es verdad que, a comienzos de 2018, ha llegado la noticia de que un grupo de investigadores de la universidad canadiense de Alberta, dirigido por el profesor Greg Kondrak, han sometido este antiguo manuscrito a una inteligencia artificial, detectando que está escrito con alfagramas hebreos, por lo que su perlustración parece posible.

La monografía de Carlos Taranilla se completa con una somera bibliografía, un glosario de los términos más comunes en lenguaje poligráfico y dos anexos. En el primero plantea una serie de ejercicios criptoanalíticos con la finalidad de que el lector descifre los criptogramas presentados. En el segundo apéndice incluye una relación de diferentes sistemas y códigos que tienen como finalidad transmitir noticias, sin que necesariamente pretendan ocultar su contenido, por lo que no siempre son de naturaleza criptográfica: el alfabeto Braille, el lenguaje del abanico, el código de banderas, la dactilología, señales de buceo, de tráfico, de montaña, deportivas, etc.

Al igual que otras obras similares, en cuanto a su contenido, este libro supone una contribución al campo de esta disciplina, siendo de interés tanto para investigadores ya versados como para noveles y neófitos en la misma.

Juan Carlos Galende Díaz
Universidad Complutense de Madrid
jgalende@ucm.es