ARTÍCULOS

Documenta & Instrumenta
ISSN-e: 1697-3798

http://dx.doi.org/10.5209/docu.75474

EDICIONES COMPLUTENSE

Cuestiones criptológicas en tres obras poco conocidas de recreación matemática y teoría de la diplomacia

Roberto R. Narváez[1]

Recibido: 26 de mayo de 2020 / Aceptado: 15 de julio de 2020

Resumen. Descripciones bibliográficas y análisis técnicos e históricos de los contenidos sobre criptografía y criptoanálisis en tres obras del dominio público, que fueron impresas entre los siglos XVII y XIX y cuyo tema general de fondo son las recreaciones matemáticas y la teoría de la diplomacia.
Palabras clave. Historia de la criptología; criptografía; esteganografía; recreaciones matemáticas; diplomacia; William Leybourn; William Hooper; conde Guillaume de Garden.

[en] Cryptologic issues in three little known works of mathematical recreations and the theory of diplomacy

Abstract. Bibliographic descriptions and some technical and historical analyses of the cryptological contents in three little known books published between the 17th and 19th centuries. These works are concerned with mathematical recreations and the theory of diplomacy.
Keywords. History of cryptology; cryptography; steganography; mathematical recreations; diplomacy; William Leybourn; William Hooper; Guillaume comte de Garden.

Cómo citar. R. R. Narváez, "Cuestiones criptológicas en tres obras poco conocidas de recreación matemática y teoría de la diplomacia", *Documenta & Instrumenta*, 19 (2021), pp. 169-187.

[1] Instituto Cultural Helénico (México)
E-mail: rsrn74@gmail.com

1. Introducción

Además de los manuales, memorias, ensayos y tratados específicamente dedicados al "arte de cifrar y descifrar" que se han publicado en los últimos cinco siglos, entre los cuales destacan clásicos familiares para quienes se interesan en la bibliografía histórica de la criptología (obras como las de Alberti, Porta, Falconer, Bacon, Vigenère, Bazeries, Kirkchoff, García Carmona, Gaines y Friedman), también han visto la luz muchísimas obras en diferentes idiomas que, aunque en el fondo versan sobre asuntos no estrictamente criptológicos, incluyen varias páginas notables donde se tratan las "escrituras secretas". No me estoy refiriendo a enciclopedias, diccionarios o piezas de diseño y función similar, sino a compilaciones y monografías didácticas cuya temática definida justifica el abordaje de aspectos relativos a la seguridad de las comunicaciones entre individuos o corporaciones, así como, por implicación técnica, la descripción y análisis de artificios tendientes a garantizar aquella seguridad. En décadas recientes se ha facilitado al investigador de la criptología histórica la detección rápida de análogos contenidos, insertos en los títulos más dispares (a menudo, también, inesperados), gracias a los instrumentos de búsqueda automatizada que ofrecen bibliotecas, acervos y otros repositorios en línea, siendo casos muy notables Internet Archive y Hathitrust.

He podido comprobar esto en repetidas ocasiones durante el último lustro, formando por añadidura un catálogo de escritos misceláneos —digitalizados desde soportes impresos en su mayoría— donde se habla de códigos, cifras, el hoy denominado criptoanálisis y otros asuntos relativos a la criptología técnica, en los tonos y conforme a los motivos más variados. Bien sé que otros han invertido tiempo y esfuerzo en idéntica faena, ubicando entre sus hallazgos algunos no mencionados en ciertos listados populares (al menos entre los especialistas), por ejemplo, la *Historical and Analytical Bibliography of the Literature of Cryptology* (1945) de Joseph S. Galland, o la no tan célebre pero sí colosal *Bibliography of the Literature of Cryptography*, de Henry E. Langen[2]. Claro que no todos los correspondientes bibliógrafos-anticuarios estarán de acuerdo sobre los criterios para decidir cuáles redacciones aportan algo de genuino interés a los *connoissieurs* de la literatura criptológica. Sea de esto lo que fuere, cuanto sobre las "escrituras secretas" llegaron a expresar los ingleses William Leybourn y William Hooper, y el francés Guillaume de Garden, en los volúmenes cuya breve descripción y comentario se sucederán en los tres apartados siguientes de este artículo, no suelen figurar en las historias, los catálogos, manuales o diccionarios de más frecuente consulta por los estudiosos profesionales o aficionados de la "criptohistoria". Al incursionar en ellos, lo último que he deseado es evaluar si se trata o no de "rarezas"; el mero intento de discutirlo sería ridículo, pues ni son tan antiguos ni, como he dicho, es ya difícil acceder a ellos de manera tan libre como virtualmente inmediata (perteneciendo además todos, por elementales razones cronológicas, al dominio público). Como sea, estoy convencido de que no es baladí examinarlos con la meta última de fomentar la investigación histórica de la teoría y la tecnología criptológica. Podrá

[2] Manuscrito inédito (fechado el 31 de diciembre de 1956) que reúne más de 850 entradas en total. Para datos bibliográficos y sinopsis puede verse la relación parcial publicada por John F. Dooley en su sitio web johnfdooley.com.

ser una contribución modesta, pero si, a juicio de los lectores, también resulta sustancial, mi designio se habrá cumplido.

2. El caso de William Leybourn

Durante el siglo XVII se forjó en Europa una vigorosa tendencia a publicar libros dedicados a plantear, comentar y resolver "problemas recreativos" de aritmética, geometría, mecánica, óptica, acústica, y ciertas cuestiones de lo que entonces se denominaba "filosofía natural" (hoy el conjunto de las ciencias físicas). El impulso inicial se debió a Bachet de Méziriac, Jean Leurechon, Claude Mydorge y otros autores franceses que laboraron entre 1620 y 1660[3]. La fiebre se extendió hasta sobrepasar los límites del continente, y así en 1694 William Leybourn, profesor de matemáticas y agrimensor profesional establecido en Londres, dio a las prensas *Pleasure with Profit: Consisting of Recreations of Divers Kinds, viz, Numerical, Geometrical, Mechanical, Statical, Astronomical, Horometrical, Criptographical, Magnetical, Automatical, Chymical, and Historical* [*Placer con provecho. Consiste en recreaciones de diversas clases, esto es, numéricas, geométricas, mecánicas, estadísticas, astronómicas, horométricas, criptográficas, magnéticas, automáticas, químicas e históricas*]. La obra estaba dirigida a los jóvenes con un solo propósito, anunciado en la portada del volumen: recrear sus ingeniosos espíritus e inducirlos "a prolongar el escrutinio de aquellas ciencias sublimes [esto es, la geometría, mecánica, astronomía, etc.] y otras parecidas", con el fin de "persuadirlos a no rendirse a los vicios que tanto atraen a la juventud de esta época"[4]. Se trataba, pues, de sustituir un placer por otro: el que rendían o, al menos, prometían los "vicios del siglo", por el de aplicar el intelecto a resolver *puzzles* eminentemente numéricos[5].

Los lexicógrafos suponen generalmente que Leybourn (1626-1716) inició su carrera como impresor y librero. Autor prolífico, se le debe el primer libro jamás escrito en inglés sobre astronomía, *Urania Practica* (1648; según la portada, lo escribió en sociedad con Vincent Wing). También firmó manuales y libros de texto sobre geografía, matemáticas y agrimensura, así como tablas de logaritmos y de cálculos (*ready reckoners*) para mercaderes, negociantes, banqueros y quienes tenían el encargo de tramitar hipotecas, rentas, pensiones y análogos ítems de contabilidad. Entre sus obras más resistentes al olvido cuenta *The Compleat Surveyor*, de la que Leybourn admitió ser autor hasta 1653, cuando se reeditó con agregados,

---

3 Véase el art. "Number games and other mathematical recreations", *The New Encyclopædia Britannica*, vol. 25, 1991, 15th ed., p. 2. Sobre Bachet véase W. W. ROUSE BALL, *A Short Account of the History of Mathematics*, London, 1912, 4th ed., pp. 305-306, y *passim* en la obra del mismo autor *Mathematical Recreations and Essays*, London, 1926, 10th ed.

4 Mi traducción es muy libre. Véase W. LEYBOURN, *Pleasure with profit*..., London, 1694. El nombre del autor aparece como "William Leybourn, Philomathes". Esta edición incluye como "Anexo" un "A Tratise of Algebra" por R. SAULT, "Master of the Mathematick School in Adam's-Court, in Broadstreet, near the Royal Exchange, London". (Disponible desde Internet en el sitio archive.org). A. DE MORGAN lo menciona, con alguna glosa más humorística que crítica, en *Arithmetical Books from the invention of printing to the present time, being brief notices of a large number of Works drawn up from actual inspection*, London, 1847, p. 54. Véase también R. P. AGARWAL y S. K. SEN, *Creators of Mathematical and Computational Sciences*, Heidelberg, New York, Dordrecht, London, 2014, p. 158-59.

5 B. WARDHAUGH, *Poor Robin's Prophecies: A Curious Almanac, and the Everyday Mathematics of Georgian Britain*, Oxford, 2012, p. 130.

pero que en un primer momento (1650) había visto la luz con el título *Planometria, or the Whole Art of Surveying of Land* y firmado por "Oliver Wallinby"[6]. Ahora, este nombre, como ya lo habrá notado más de un lector, es un anagrama de "William Leybourn", agregando la V y excluyendo la M y la U. He aquí un indicio de que nuestro personaje, cuatro décadas antes de producir *Pleasure with profit...*, estaba ya familiarizado con ciertos métodos de criptografía básica.

En *Pleasure with profit...* Leybourn dedica el tratado VII a las "Recreaciones criptográficas". Este Arte, dice, "es de gran utilidad en muchos respectos, pero principalmente en la Guerra".

> Y si consideramos las grandes necesidades en que se vieron grandes príncipes y potentados para comunicar sus decisiones o intenciones a sus corresponsales, antes del perfeccionamiento de este Arte, cualquier hombre de entendimiento razonable se admirará. Por lo cual le ofreceré aquí un recuento muy breve de algunos [medios de este Arte], y después mostraré algunos otros, más artificiosos y absolutos, que propician una comunicación tanto secreta como rápida (p. 1).

A este preliminar lo siguen cuatro secciones de repaso, descripción y lineamientos prácticos de varios criptosistemas más o menos arcaicos. En la sección I se enumeran algunas formas de transmisión comunicativa segura que los persas, lacedemonios, milesios, romanos, entre otros pueblos de la antigüedad, pusieron en marcha sin recurrir, propiamente hablando, a sistemas criptográficos. Así Harpago, por ejemplo, estimando que el rey persa Ciro debía apresurar su invasión a Media, le hizo llegar su consejo en una carta remetida en las entrañas de una liebre. Cita igualmente la memorable *scytala* de los espartanos. Pero éstos, en rigor, son artilugios que dependen básicamente de tecnologías y sistemas postales en donde no participa ningún método para volver ilegible o indetectable un texto, ya por la transformación ostensiva, ya por el encubrimiento esteganográfico. Ahora, es de tales métodos, "más artificiosos y absolutos" (p. 1), que Leybourn se ocupa en el resto del capítulo.

Uno consiste en disponer las "24 letras comunes del alfabeto" en un paralelogramo rectangular o un cuadrado de madera, o algún otro material no demasiado duro[7], que incorpore cualquier número de guarismos e intervalos o letras superfluas entre cada letra significativa, "a fin de que tu corresponsal pueda leer tu escritura" o por columnas o por líneas horizontales, en forma bidireccional; por supuesto, para evitar confusiones se debe establecer en cada ocasión si el procedimiento será de columnas o líneas. En el primer caso hay cuatro posibilidades: 1) descender con cuatro intervalos, 2) ascender con tres intervalos, 3) descender y ascender alternativamente, con dos intervalos, y 4) ascender o descender alternativamente, con tres intervalos. También son cuatro las posibilidades en el sistema de las líneas o renglones: 1) vía directa, con siete intervalos, 2) vía retrógrada, con cinco intervalos,

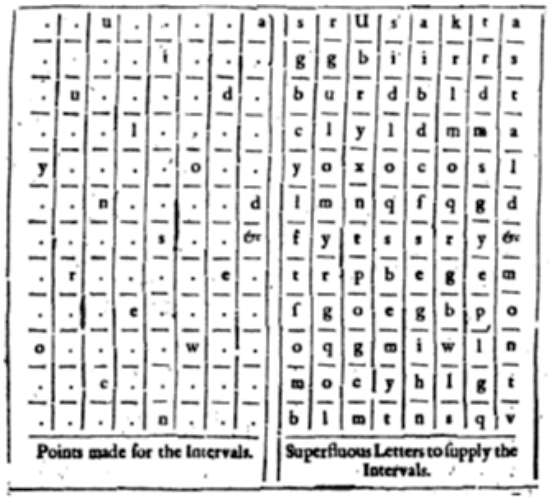
---

6 A. M. ROOS, "William Leybourn", en C. BAKER (ed.), *Absolutism and the Sicentific Revolution, 1600-1720*..., London, 2002, pp. 228-229. S. LEE (ed.), *Dictionary of National Biography*, New York, 1893, pp. 208-209.

7 Leybourn no especifica, pero que conviene sea suave o poroso, como ciertos tipos de madera, se comprenderá por las descripciones siguientes.

3) alternando la directa y la retrógrada, con dos intervalos, y 3) alternando la retrógrada y la directa, con tres intervalos (pp. 2-5).

Veamos un ejemplo de operación. Deseo informar a mi corresponsal *Your Uncle is now Dead* ("Tu tío está ahora muerto"). Escribo en las columnas descendiendo (por previo acuerdo) con cuatro intervalos. Por tanto, en el paralelogramo realizo *cuatro pinchazos*, uno debajo del otro, y *a continuación* pongo la primera letra de mi mensaje, Y, seguida de *otros cuatro pinchazos*, tras los cuales inscribiré mi siguiente letra, O; pongo luego *dos pinchazos más* en esa columna y se termina el espacio, entonces abro los *dos restantes* en la cima de la siguiente. Debajo de estas marcas inscribo la U, tercera letra de mi texto plano, y continúo en el mismo estilo hasta terminar (pp. 2-3). El gráfico a continuación, que proviene de la edición facsimilar disponible en Internet[8], muestra, a la izquierda, el paralelogramo con la inscripción y los pinchazos intercalados, y a la derecha la versión final a transmitir, con "letras superfluas" en lugar de los pinchazos.



Leybourn da ejemplos y gráficos para ilustrar cada una de las opciones conforme a las posibles rutas indicadas (pp. 3-7). En la segunda sección se describe la clásica cifra de transposición asociada a C. Julio César y C. Octavio Augusto. Cada letra del alfabeto único se sustituirá criptográficamente por la limitante al contar tres a la derecha desde su sitio aritmético, esto es, A por D, B por E, C por F, y así. Una peculiaridad es el arreglo de las transposiciones en una *Clavis*, como la denomina Leybourn, donde se aprecia con mayor facilidad la correspondencia entre las letras del texto plano y las del criptotexto. Se organiza entonces la encriptación en columnas de lectura ascendente, directa, diagonal, retrógrada, etc., al estilo del criptosistema descrito en la sección anterior. El criptotexto siempre asumirá la forma de una matriz cuadrada. Leybourn comenta que este artificio es "muy susceptible de ser descubierto" porque "no hay más letras que las requeridas para formar las Palabras buscadas [de un criptotexto dado]" (p. 8). En tales términos alude a la natural incapacidad de los alfabetos únicos para rotar de cualquier manera y, por

[8] En el sitio web archive.org.

consiguiente, multiplicar los equivalentes crípticos asignables a cada carácter de texto plano, en particular los de mayor frecuencia relativa.

Un modo de paliar esto, nos dice Leybourn, consiste en elegir sustitutos que representen a las 24 letras del alfabeto[9]. Esto es tanto como recomendar la formación de una lista de homófonos que serán signos o símbolos, "no inventados al arbitrio [...] como hacen los estenógrafos y taquígrafos", sino seleccionados de los reinos astronómico, planetario, y "de los Aspectos": 12 signos, 7 planetas y 5 aspectos, en suma, 24.

Los 5 aspectos representan a las 5 vocales, los 7 planetas a los caracteres iniciales del alfabeto y los 12 signos zodiacales a las grafías alfabéticas de cierre. Para agilizar el procedimiento, Leybourne construye una tabla de correspondencias que denomina *Clavis astronomica*. Los corresponsales deben acordar claves para indicar si el criptotexto se articulará en cuadrados, rectángulos, triángulos o cualquier otra figura geométrica. Se usarán los numerales del 1 al 9 inclusive como términos nulos que se insertarán a capricho entre las letras con significado, y al concluir se colocará siempre una cruz dentro de un círculo. Así, por ejemplo, el mensaje *I have escaped out of the Castle in Disguise, and do lodge at the Ball in the High Street, by the name of Mary Grice* ["He escapado del castillo disfrazada, y me estoy hospedando en el Ball en High Street, bajo el nombre de Mary Grice"] se cifrará como sigue[10]:

Este criptosistema no es del todo original, pero Leybourn lo estima sólido contra el análisis de frecuencias (pp. 8-9).

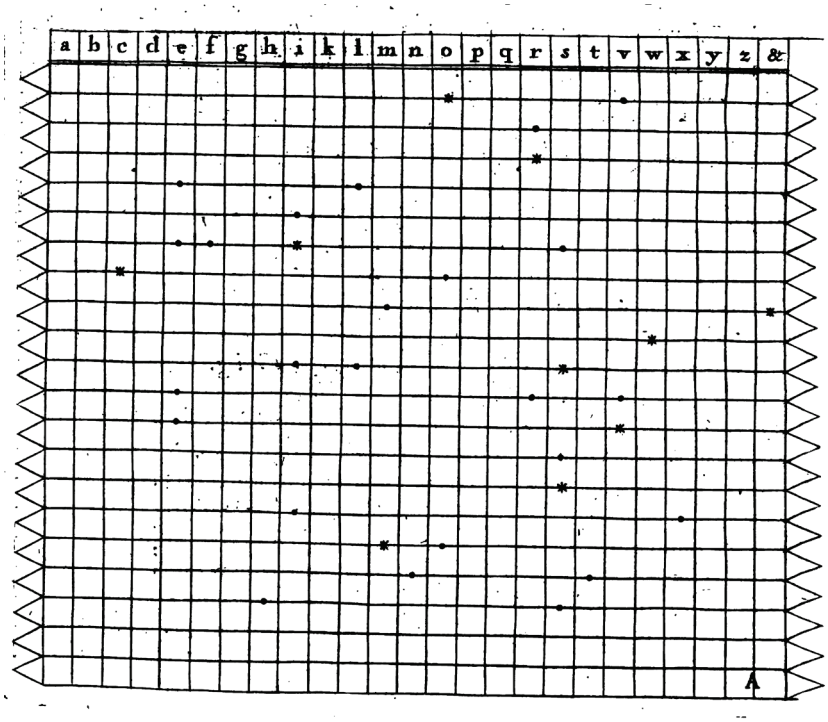
En la cuarta parte se describe (pp. 9-10) un mecanismo de alfabeto único que también John Wilkins, en su *Mercury*, juzgó como una opción señera[11]. Se fabrica un paralelogramo de cobre u otro material flexible. Acto seguido se inscriben las 24 letras de la A a la Z, en su orden regular, más el *ampersand*. Los nudos se harán con un hilo o cordón cuidadosamente seleccionado. Se agregarán ganchos en la parte posterior de la tabla para fijar en ellos el hilo y, desde ahí, pasarlo por unas

9 Entiéndase, para el alfabeto básico de extensión W=24 que él utiliza en todo este tratado.

10 Este ejemplo se complementa con un curioso criptotexto en francés integrado como un romboide, para leerse en sentido diagonal alternado de arriba abajo y a la inversa (p. 9).

11 J. WILKINS, *Mercury, or The Secret and Swift Messenger*, London, 1694, pp. 44-47.

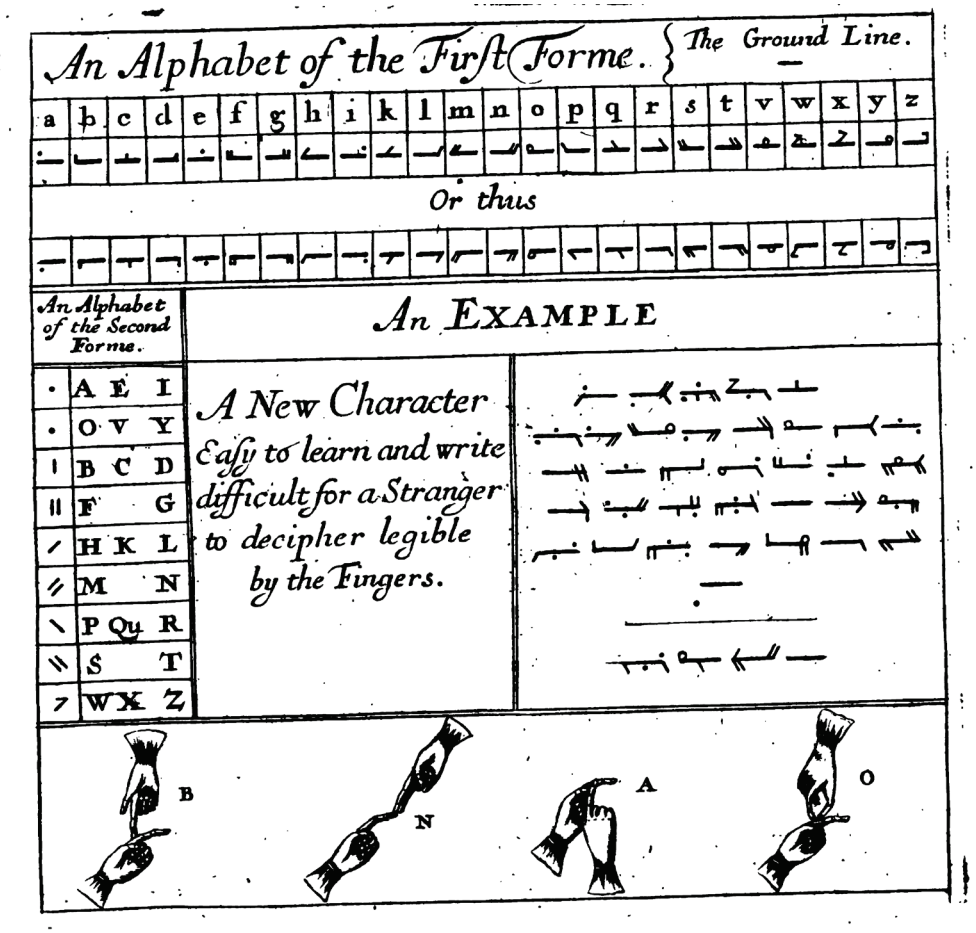
muescas practicadas en ambos bordes. El hilo se traslada de izquierda a derecha hasta quedar tenso, y se ata cada nudo en el punto requerido para alinearse, por así decir, con su grafía equivalente en la franja superior.



Los nudos quedan separados entre sí a distancias cuyas medidas dependerán del lugar ocupado por cada uno. Emisor y receptor deben tener ejemplares idénticos de la tabla, y es legítimo pensar que también convendría especificar la longitud del hilo —detalle éste que Leybourn no comenta en absoluto[12]. Sin duda que la medida se fijaría como estándar, en tanto las dimensiones de la matriz no son variables. Abundar en esto importa porque, al final, el hilo funciona como vehículo del criptotexto; se remite enrollado o como se prefiera, pero sus nudos delatan su cometido criptográfico sólo cuando generan relieves aislados, de separación calculada, en sitios diversos de la tabla, curiosa suerte de bordado que sólo apreciará por su sentido último quien, avisado, sepa ver al tablero como la clave del sistema íntegro. En buena medida representa, vistos los pormenores técnicos de operación y construcción, una variación de la *scytala* espartana. Nuestro autor ensalza la resistencia superior de este método, entre todos los de transposición, para resistir los ataques criptoanalíticos.

[12] WILKINS (*Mercury*, *op. cit.*, p. 47) contempló, de algún modo, este detalle, al preguntarse qué se debe hacer cuando el mensaje resulta demasiado largo. Propone dos opciones: (a) suplir la parte final del criptotexto mediante un segundo cordón, y (b) "empezar de nuevo" usando el cabo sobrante del mismo cordón —suponiendo que lo haya. Con esto a la vista, lo ideal sólo puede ser, desde luego, preparar criptogramas tan breves como sea posible.

Leybourn cierra el tratado proponiendo "Un nuevo carácter fácil de aprender y escribir, difícil de descifrar [...], legible por el movimiento de los dedos, en donde cada línea de escritura contendrá dos líneas de sentido" (pp. 11-12). Los componentes y ejemplos básicos de funcionamiento se muestran en el siguiente gráfico.



Leybourn explica:

> Cada letra de este alfabeto se construye sobre una línea breve, como esta (—), la cual, para fines de distinción, podrá llamarse la *Línea Base*. Las letras se forman por la adición de algunas marcas o puntos pequeños, los cuales representan [letras precisas], según se pongan al *inicio*, la *mitad*, o el *final de la Línea Base*.
> Muestro al alfabeto en dos formas. La primera, tan sencilla como para ser entendida; la segunda, tan sencilla como para ser recordada. En la cima del segundo alfabeto tienes un punto, o mota, y las letras A E I, que denotan que el *punto* al *inicio* de la *Línea Base* (ya por encima, ya por debajo de ella) representa la A, primera de las tres letras. Si el punto está encima (o debajo) de la *mitad* de la *Línea Base*, es E, la letra media; y si está encima (o debajo) del *final*, es I, la terce-

> ra letra a mano derecha. Ahora, en el rango de en medio aparece (′) H K L, mostrando que esta marca [...] puesta al *inicio* de la *Línea Base*, es H; a la *mitad* K, y al *final* L; y así para el resto (pp. 11-12).

Siguen otras especificaciones y consejos de aplicación, concluyendo con una adaptación de lo mismo para el uso de ambas manos. El dedo índice de la mano izquierda representará la "Línea Base" y las "letras varias" se formarán "poniendo los *dedos* de la *mano derecha* sobe esta *base*, cada *dedo* de tal manera, que habrá de representar a [cada] *Letra*". En el gráfico queda patente la manera estilizada de formar cuatro letras. Uno se pregunta cuánto tiempo de práctica sería necesario para dominar este sutil artificio, en tanto fue diseñado —como es obvio— para utilizarse en ocasiones extremadamente delicadas, cuando no cabe reflexionar pausadamente sobre otros medios de transmitir con discreción. Como sea, más allá de su pintoresquismo no dejará de interesar a quien estudie los sistemas de comunicación no verbal en general[13].

3. El caso de William Hooper

Las proposiciones criptológicas de Hooper que trataré aquí se coleccionaron en el libro *Recreaciones racionales en las que se elucidan clara y copiosamente los principios de los números y la filosofía natural, por una serie de experimentos fáciles y entretenidos, entre los cuales se hallan los que comúnmente se ejecutan con naipes*, 2 vols. Examiné la cuarta edición, corregida y publicada en Londres, 1794, por B. Law and Son[14]. De este autor apenas se han ocupado los lexicógrafos, enciclopedistas e historiadores de las matemáticas[15]. Su nombre en la portada del volumen I de *Recreaciones...* va seguido de las siglas "M.D.", sin duda convencionales para indicar un grado académico. Lo único cierto es que las matemáticas, las disciplinas experimentales y la "filosofía natural" (el paralelo, a este respecto, con Leybourn y otra miríada de autores de su tiempo no deberá sorprender) eran su objetivo de interés fundamental. Si fue profesor, nada entre los preliminares al aludido volumen permite conjeturar en dónde enseñó, tampoco su lugar de residencia mientras componía la pieza. Con todo, hay indicios de que esta obra fue leída

---

[13] Una cifra generada por este medio resultaría similar a las que formaban una "relación" que el arbitrista José de Orozco y Gamarra envió desde el Callao a las autoridades imperiales de la Metrópoli en 1604, véase G. LOHMANN VILLENA, "Cifras y claves indianas. Capítulos provisionales para un estudio sobre criptografía indiana", *Anuario de Estudios Americanos*, t. XI, 1954, pp. 323-325 y lámina 9. Lo mismo valdría decir a propósito de las "cifras de Basingstoke" (llamadas así en honor al monje inglés John of Basingstoke, m. 1252), dado el sistema para trazar grupos de tres numerales usando una sola línea vertical como "base", véase D. A. KING, *The ciphers of the monks*, Stuttgart, 2001, pp. 33-37.

[14] *Rational Recreations in which the principles of numbers and natural philosophy are clearly and copiously elucidated, by a series of easy, entertaining, interesting experiments, among which are all those commonly performed with the cards*, 2 vols. Se publicó originalmente en 1774, en 4 volúmenes. Ya en la segunda edición (1782-83) se había reducido a dos volúmenes. Cf. la información bibliográfica de la Royal Collection Trust, en su sitio web www.rct.uk. S. DURING en su libro *Modern Enchantments. The Cultural Powers of Secular Magic*, Cambridge and London, 2002, p. 87, dice que este libro constituye, básicamente, una traducción de *Nouvelles Récréations* (1769), de Edme-Gilles Guyot (1706-1786).

[15] Véase art. "Number games and other mathematical recreations", *The New Encyclopædia Britannica*, vol. 25, 1991, p. 2. S. WERRETT, *Fireworks: Pyrotechnic Arts and Sciences in European History*, Chicago and London, 2010, p. 206.

por experimentalistas e inventores durante el siglo XIX; así Daguerre, por ejemplo, bien pudo haber atendido a lo dicho por Hooper sobre el uso de sales de plata en papel para crear imágenes sombreadas y tintas invisibles[16]. De estas tintas, como se sabe, han hablado con frecuencia los historiadores o tratadistas de la criptografía, pero Hooper las examina en un volumen posterior, por tanto, aparte del estricto tema criptográfico[17]. Destinó, en fin, la Recreación XLVII para escribir sus ideas acerca de los "Diferentes métodos de escribir en cifra".

Después de una brevísima introducción donde se mencionan las consabidas prácticas criptográficas de los lacedemonios, nuestro autor describe un sistema de "comunicar inteligencia mediante un mazo de naipes de piquet"[18]. Tras barajar los naipes, el emisor escribe las primeras 32 letras de su mensaje una en cada naipe. Vuelve a barajar y escribe las siguientes 32 letras, de nuevo una por carta. Repite la acción hasta agotarse el texto plano. Veamos este ejemplo, *I am in full march to relieve you; within threedays I shall be with you. If the enemy in the mean time should make an assault, remember what you owe to your country, to your family and yourself. Live with honour or die with glory*[19]. Siguiendo la prescripción técnica, resulta una clasificación de los naipes por palo y número (según el estándar francés) en el orden de los caracteres de texto plano que se les terminó asociando.

As de espadas	*i a d u y i*
Diez de diamantes	*a l e u l*
Ocho de corazones	*m l m o i u*
Rey de espadas	*i s u m l*
Nueve de tréboles	*n h l e o*
Siete de diamantes	*f b m r i*
Nueve de diamantes	*u e a c t n*
As de tréboles	*l w k r y i*
Sota de corazones	*l s e e a e*
...	

El receptor ordena los naipes de acuerdo con un esquema convenido (toma 3 de arriba y encima les pone 2 de abajo, etc.) y apunta en un papel la primera letra de cada carta, encontrando así, como se muestra en el listado parcial *supra*, que el mensaje adquiere gradualmente sentido cuando se lee de arriba abajo: "I am in full...". Después barajará de nuevo el paquete para definir las grafías de la siguiente columna, que leerá de manera descendente. Repetirá la operación hasta inscribir el mensaje completo (pp. 143-147).

---

16 R. WATSON y H. RAPPAPORT, *Capturing the Light. The Birth of Photography, a True Story of Genius and Rivalry*, New York, 2013, p. 57.

17 En el vol. IV, "Recreación LVIII", pp. 183-189.

18 No se conoce con plena seguridad el origen del juego de piquet, pero es tradicional afirmar que cobró popularidad en Francia entre los siglos 15 y 16 (la palabra *piquet* es francesa, puede traducirse como "estaca" o "piqueta"). Para detalles sobre las formas de jugar y apostar véase R. P. CARLISLE (ed.), *Encyclopedia of Play in Today's Society*, SAGE Publications, 2009, vol. I, p. 484.

19 En español se puede verter así: "Estoy en marcha para relevarte; dentro de tres días estaré contigo. Si, mientras tanto, el enemigo te ataca, recuerda lo que debes a tu país, a tu familia y a ti mismo. Vive con honor, o muere con gloria".

Hooper sugiere tácticas especiales de barajeo para prevenir el riesgo de que un interceptor del grupo de naipes logre adivinar el mecanismo de transformación críptica monoalfabética, pero advierte: "[...] si bien todas las cifras dependen de la combinación de letras, apenas hay alguna que no pueda ser descifrada con tiempo y tesón" (p. 147). Y termina esta sección aseverando que "las mejores cifras son las que, por naturaleza, están libres de la sospecha de ser cifras" (p. 147), en una palabra, su convicción es que los principios y métodos de la esteganografía, en punto a garantía de seguridad, superan a los de la criptografía. En tal sentido recomienda, volviendo a su sistema de barajas, escribir las letras con tinta invisible, singular artimaña de "sobre esteganografía" con cuyo auxilio el paquete podrá evadir más confiadamente los embates del espionaje o la censura postal.

En la "Recreación XLVIII" Hooper describe un "Disco místico" que se basa directamente en el clásico disco albertiano para potenciar sustituciones múltiples polialfabéticas. En una superficie cuadrangular se instalan dos discos, uno como base, que va fijo, y en su interior otro, más pequeño y móvil. En el fijo, o, como lo estipuló Leon Battista Alberti en su panfleto *De Cifris* (o *De Componendis Cifris*)[20], el *Stabilis*, estarán inscritos el alfabeto y los números 1 2 3 4. El disco móvil o *Mobilis* (en la nomenclatura de Alberti) presenta en minúsculas un alfabeto mezclado (excluyendo la J, U y W) más el signo &, y se consolida en el tablero con una aguja, su eje de rotación. Los guarismos 1-4 del *Stabilis*, por otra parte, funcionan para sobrecodificar el criptotexto con base en una lista de 336 frases a las que se asigna un valor numérico. Ahora, en la propuesta de Hooper el *Mobilis* muestra en exclusiva las letras del alfabeto A-Z, mientras que el *Stabilis* hace lo mismo, pero en desorden. No se agregan signos auxiliares de clase alguna. Sin embargo, el funcionamiento elemental es el mismo: los corresponsales acuerdan una clave de rotación del disco móvil para potenciar las sustituciones polialfabéticas, por ejemplo, *Ma*; esto significa que la *a* del *Mobilis* deberá alinearse con la *M* del *Stabilis*, y así, nos dice Hooper, al cifrar las palabras "If you" tendremos "Un juc" (pp. 147-148). Y de manera interesante ofrece una alternativa tecnológica al disco para conseguir un efecto relativamente similar. Se colocan dos reglas una encima de la otra; la superior estará fija y llevará inscrito el alfabeto en el orden regular, la inferior será deslizable y ostentará, en sucesión inmediata horizontal, dos alfabetos normalmente ordenados. Esta pareja corresponde a la cifra, de modo que se debe alinearlos con letras del alfabeto en la regla superior, a definir con una clave, para generar la sustitución. He aquí la variación de otro modelo clásico, el de Saint-Cyr[21], aunque previsiblemente menos efectiva, ya que no se recurre al desorden alfabético en ningún momento.

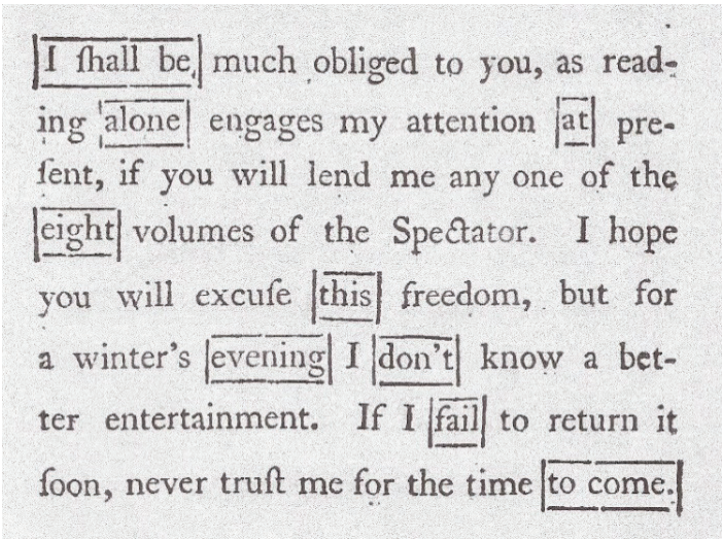
La "Recreación XLIX" describe el sistema de "Los espacios correspondientes". No es otra cosa que la vieja "rejilla" fruto del ingenio esteganográfico de Gerolamo (o Girolamo, o Geronimo) Cardano (1501-1576), propuesto hacia 1550[22]. Hooper ilustró su empleo con la siguiente composición ideal (p. 150):

---

[20] Apareció por primera vez en italiano en 1568 (Venecia), como parte de los *Opuscoli Morali* de Alberti. Se dispone de una versión inglesa: *A Treatise of Ciphers*, Torino, 1997 (texto latino establecido por Augusto Buonfalace).

[21] Una buena ilustración de este método en H. F. GAINES, *Cryptanalisis: A Study of Ciphers and Their Solutions*, New York, 1956, pp. 110-111.

[22] J. F. DOOLEY, *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms*, Springer, 2018, p. 17.


I ſhall be much obliged to you, as reading alone engages my attention at preſent, if you will lend me any one of the eight volumes of the Spectator. I hope you will excuſe this freedom, but for a winter's evening I don't know a better entertainment. If I fail to return it ſoon, never truſt me for the time to come.

El único texto significativo que se debe interpretar es el formado por las palabras en los recuadros, *I shall be alone at eight this evening don't fail to come* ["Estaré solo esta noche, a las ocho, preséntate sin falta"]. Los recuadros son aperturas practicadas en un trozo de cartulina u otro material similar de tamaño igual al de los folios en que se ha de redactar el texto completo; cuanto se apunta en ellos configura el único mensaje significativo a transmitir. La cartulina o placa representa, como es obvio, la "clave" del esteganograma. Constituyó una de las más vigorosas estrategias técnicas durante la época de la criptografía manual. Con todo, Hooper acierta al señalar que no es opción primaria cuando se trata de velar mensajes demasiado breves (pp. 150-151).

Tras describir una ingeniosa variación operativa del "Disco místico" con base en los signos de notación musical[23], cuyo tratamiento en este artículo resultaría ya muy prolijo, Hooper despliega una lista de doce preceptos en torno al "arte de descifrar". La preceptiva al punto varía con cada idioma, pero tratándose de una cifra en inglés debemos tener en cuenta, primero, las letras o caracteres de ocurrencia más frecuente y adjuntarlas a las "vocales fijas", incluyendo la Y; de esas vocales las más frecuente será la E, la menos frecuente la U. Las vocales conjuntadas de mayor aparición son EA y OU. La consonante más común al final de las palabras es S, seguida por la R y la T. Cuarta regla: cuando en una cifra aparecen juntos dos caracteres similares, ambos serán muy probablemente las consonantes F, L o S, o las vocales E u O. Por último, la letra que precede o sigue a dos caracteres similares es o una vocal o las consonantes L, M, N o R. La serie final de observaciones asienta las tácticas para lidiar con multigramas (pp. 153-156).

Para terminar esta "Recreación", Hooper ofrece dos criptogramas, uno formado por signos arbitrarios y otro por letras, como ejercicios prácticos para el lector (pp. 156-160).

[23] "Recreación L", pp. 151-153.

4. El caso de Guillaume de Garden

Como sucede con Leybourn y Hooper, son escasos los datos biográficos que poseemos del conde Guillaume de Garden (1796-1872), diplomático y escritor francés. A juzgar por enciclopedias y diccionarios referentes a la teoría del derecho y de las relaciones internacionales, su *Traité complet de Diplomatie* [*Tratado completo de diplomacia*] (1833)[24] es de ordinario preterido ante aportes de la temprana modernidad tan clásicos como los de un Wicquefort, un Calliéres o un Rayneval, por citar tan sólo a tres magnos autores de entre sus compatriotas. En la portada de su libro recién citado leemos que fue "chambelán de Su Majestad el Rey de Baviera, antiguo ministro residente, y comandante y caballero de varias órdenes nobiliarias". Editado originalmente en tres tomos en París (Librairie de Treuttel et Würtz, Rue de Lille, no. 17; Strasbourg, Grand'Rue, No. 15), ese texto lleva el subtítulo *Théorie Générale des relations extérieures des puissances de l'Europe* [*Teoría general de las relaciones exteriores de las potencias de Europa*]. Es un estudio sistemático de prácticamente todos los elementos que configuran y marcan los aspectos fundamentales de la diplomacia, con una vasta provisión de ejemplos, reflexiones, anécdotas y comparaciones de interés para los estudiosos del origen de ciertos cánones modernos acerca del modo de pensar y actuar, o pensar y dejar a los otros actuar o no hacerlo, en las relaciones internacionales. Cada tomo se subdivide en libros, y cada libro en secciones o apartados. La sección XVII del tomo 2 se titula "De la cifra", y en ella Garden hace dos cosas: (1) pasa revista a una serie de principios y métodos en torno a las "escrituras secretas", y (2) propone un "criptosistema original" que juzga prácticamente invulnerable contra los "descifradores".

Garden define a las cifras como caracteres ignotos ya por ir "disfrazados" o ya por ser "variados". Quien carece de su "llave" (*clef*), o clave, no puede interpretarlos. La esteganografía es aquel arte de mimetizar, por decirlo así, un mensaje en otro mensaje, de modo tal que su mera existencia resulta insospechable a primera vista. La criptografía depende de estipular un significado particular para símbolos o caracteres elegidos a capricho de diferentes ámbitos científicos o artísticos, por ejemplo, la aritmética, la química y la notación musical. Para Garden todo cifrado depende o de codificar piezas lingüísticas de diferentes tamaños o de sustituir grafías con base en algoritmos, en particular cuando esto exige operar con alfabetos únicos (pp. 123-124). Declara que "todos los gabinetes de Europa tienen cifras diferentes", y cuando un ministro parte a misión extranjera se le remiten, de ordinario, tres cifras: 1) la "cifra cifradora", 2) la "cifra descifradora", y 3) la "cifra común". La primera es el nomenclátor clásico en el que los equivalentes pueden ser numerales, caracteres extraños, etc. Propone un ejemplo en el que cada ítem en la lista se sustituye hasta por cinco dígitos simples o agrupados. "Se tiene cuidado de poner por orden alfabético los nombres sustantivos, los verbos y las frases según sus letras iniciales, para la comodidad de quien está cifrando", y esta persona puede seleccionar los grupos numerales a voluntad[25]. Ahora, por "cifra descifradora"

[24] Disponible desde Internet en el sitio hathitrust.org.

[25] El modelo que ofrece como caso típico recuerda a las cifras españolas oficiales en tiempos de los Reyes Católicos, que con tan inusitada pericia, en la década de 1850, decriptó Gustav Bergenroth en el antiguo ar-

Garden se refiere a lo que en el ámbito hispanoamericano se solía llamar "contracifra", y forma una imagen contrapuesta, elemento por elemento, del sistema original, útil para agilizar la traducción de los criptotextos. Como puntualiza Garden:

> Cuando se quiere descifrar algún pliego, se busca en la cifra descifradora la significación de cada número [...] y se escribe debajo, entre las líneas, las cuales a este efecto deben estar espaciadas convenientemente, y los números separados unos de otros a una justa distancia. Se puede asimismo descifrar sobre una hoja de papel separada, pero la obra es más larga y penosa, aunque en general sea menos difícil descifrar que cifrar (p. 126).

A este propósito abunda en torno a la necesidad de ejecutar el trabajo manual con esmero, so pena de ocasionar ambigüedades de lectura tras el descifrado (p. 130). Estos apuntes evocan las peculiaridades normales que se detectan, merced a la investigación histórica, en los estilos de concebir el trabajo criptográfico en las representaciones diplomáticas durante la época en que Garden escribió, y que constan en las instrucciones reservadas que se entregaban a los ministros o agentes, así como también, por supuesto, los escritos de todo tipo (despachos, memoriales, notas, etc.) que se generaban en estricta reserva y con el anhelo de protegerlos al máximo durante la transmisión.

Cifras como las recién descritas, nos dice Garden, parten de un "tronco común", aunque la práctica tradicional ha sido facturar ejemplares individualizados para cada legación en su respectivo destino. Sin embargo, cuando es conveniente o preciso que los operadores diplomáticos compartan información delicada entre ellos, emplean una "cifra común", la cual se diseña y realiza sobre el modelo de las otras dos cifras mencionadas, o, valdría decir, de la cifra original y su correspondiente contracifra (pp. 127-128).

Garden refiere asimismo la que llama "cifra anulante", una providencia impuesta por el reconocimiento de que hay gente incapaz de rechazar el soborno de espías o agentes del enemigo (p. 127). Pero si todo traidor es un engañador, valga entonces, para salvaguardar la causa propia, hundirlo y, por implicación, confundir a sus empleadores mediante engaños, del siguiente modo: la Corte escribe a su ministro lo contrario de sus verdaderas instrucciones, o bien el ministro remite a su Corte lo contrario de sus verdaderos avances y las noticias que desea comunicar, poniendo "una señal, una marca, un carácter, una palabra o una frase en que se ha convenido [...], la cual anula no solamente todo lo que se acaba de decir, sino que indica también que se lo debe entender en el sentido opuesto" (p. 127). Otro medio para prevenir la corrupción en las embajadas o consulados —eventualidad no infrecuente, por cierto, según lo muestran las historias diplomáticas— era enviar por medios regulares una cifra falsa para instaurar el desconcierto, mientras que por otra vía (no sólo el correo regular, por supuesto, pues esto implicaba el riesgo de la censura o captura por espionaje) se remitían los criptosistemas reales a utilizar. Y es que, dice Garden, "la industria de los hombres, estimulada por el interés y la necesidad,

chivo de Simancas. Véase W. C. CARTWRIGHT (ed.), *Gustav Bergenroth: A Memorial Sketch*, Edinburgh, 1870.

ha inventado y aun inventa todos los días cifras y reglas para descifrarlas[26], lazos para coger en ellos al enemigo, y medios para garantizarse uno mismo" (p. 127).

En cuanto al "arte de descifrar", que se refiere propiamente a lo que hoy llamamos decriptación, Garden considera que en realidad no puede enseñarse; las reglas o sugerencias para conjeturar significados probables que ofrecen los manuales no tienden realmente a formar "descifradores" expertos. Cuando un despacho, digamos, es penetrado ilegalmente, lo único que vale asumir es que el criptograma no resistió por negligencia de su creador[27]. Esto es afirmar que, en principio, los criptosistemas deben concebirse como dispositivos totalmente aptos para otorgar seguridad a las comunicaciones. Por otra parte, Garden estima que "adivinar" los posibles contenidos de un mensaje velado es prácticamente imposible sin tener alguna información o pista previa en relación a sus contenidos efectivos, o bien algún otro "socorro preliminar", esto es, datos filtrados por algún traidor o espía (p. 128)[28]. Esto explica el espacio que concede a la cuestión de la deslealtad siempre posible por codicia o cualquier otra motivación, así como su dictamen de que quienes pretenden romper una cifra o código sin tener algún antecedente de contenido son puros charlatanes.

En consonancia con lo anterior, Garden asevera que un "descifrador" requiere pocos datos para adivinar una cifra monoalfabética de sustitución simple, o de "llave simple", como la denomina, mientras que la dificultad se incrementa cuando el ejemplar es de sustitución polialfabética, o de "doble llave". Pero, mucho mayor será la complejidad al tratarse de una clave de libro, cuya "llave" consiste en tres "cifras" (en realidad, se trataría de índices): la de la página del libro, la de una línea en esa página y, por último, la palabra a usar como equivalente en dicha línea. El máximo desafío para el intruso en este caso es "adivinar" no sólo el título del libro, sino la edición utilizada por los corresponsales autorizados; además, está el detalle de que una misma palabra puede aparecer encriptada de diferente manera, en tanto siempre es posible renovar la indicación de página, línea, etc (pp. 129-130)[29].

Para terminar, Garden describe formalmente un "nuevo sistema" (*nouveau système*). Esta propuesta, sin embargo, es tan sólo una variación del clásico modelo de cifrado polialfabético asociado a Blaise de Vigenère y Giovan Battista Belaso (o Bellaso). Ante todo, se coloca a la serie de alfabetos mutuamente deslizables en una matriz cuadrangular para facilitar la localización de los equivalentes de sustitución al cifrar y descifrar. La matriz reúne 73 caracteres en total: letras, tildes, signos auxiliares, signos de puntuación y numerales, tantos como se consideran útiles para incrementar la variabilidad de promedios de aparición de cada sustituto posi-

---

[26] Hay aquí un eco de François de CALLIÈRES, *De la maniere de negocier avec les souverains*, Amsterdam, 1716, p. 206 —dentro del cap. XX "De lettres en chiffre".

[27] Idéntico pensamiento en CALLIÈRES, *op. cit.*, pp. 206-207.

[28] Como lo había señalado ya Abraham de WICQUEFORT en *L'Ambassador et ses fonctions* (1716) en cuanto se conoce el "tenor de un asunto y la corte donde se lo negocia", no hay dificultad para identificar a las personas referidas en un determinado despacho interceptado. Cito por los extractos en inglés que D. P. HEATLEY incorporó a su libro *Diplomacy and the study of international relations*, Oxford, 1919, pp. 245-246, donde también incluyó, por cierto, observaciones sobre la criptografía en la diplomacia de Callières, Martens, y Juan Antonio de Vera y Figueroa.

[29] El modelo clásico de este sistema lo propuso Pierre-Resard Wouves D'Arges al conde de Floridablanca en 1787, durante unas reuniones en San Ildefonso con vistas a definir la misión del primero como agente de la monarquía española en la región del Mississippi, en Estados Unidos de América. LOHMANN VILLENA, "Cifras y claves indianas...", pp. 362-363.

ble a elegir[30]. En cuanto a la forma de operación específica, lo primero es escoger una "llave" que puede ser un término de uso real o inventado para la ocasión, o una cantidad expresada con guarismos, o un "conjunto arbitrario de signos elegidos en la primera columna vertical" del cuadro de referencia. Es preciso evitar, subraya Garden, que la "llave" incluya caracteres repetidos, buena previsión con vistas a nivelar las frecuencias relativas en el criptograma resultante (pp. 132-133).

Acto seguido se escribe la llave debajo del texto plano a velar y transmitir; a este conjunto de sintagmas Garden lo llama "tema". Al rotar la clave para encriptar, debe cuidarse que cada grafía, numeral u otra línea cualquiera se encuentre debajo de una grafía, numeral o cualquier otro signo del tema. Garden prescribe que al repetir cíclicamente la clave se la escriba completa en toda ocasión, hasta agotarse el tema (Belaso asentó idéntica regla en su sistema). La clave en rotación debe cubrir incluso a los "blancos del tema", esto es, la separación entre palabras, incluyendo al blanco después de todo punto y seguido. Lo mismo debe ocurrir con respecto a signos de puntuación y otros auxiliares de la escritura (p. 133).

Para ilustrar con un ejemplo, Garden elige la clave CABINET y el tema *La guerre est déclarée* ["La guerra está declarada"]. Iniciamos, pues —y como es típico en todos los artilugios de esta clase canónica—, pareando la clave con los elementos del texto plano.

L a g u e r r e e s t d e c l a r è e
C A B I N E T C A B I N E T C A B I N E T C

La L del "tema" se ubica en la primera fila horizontal, o sea, del alfabeto del texto plano, y se combina con la C inicial de la clave, haciendo que ambas converjan a través del mapa alfabético que constituye la matriz, hasta llegar al punto de sustitución, con la P como el primer elemento del criptotexto. Repitiendo estos pasos con los demás pares en el gráfico anterior, tenemos que la a del tema con A de la clave resulta en À, luego el primer blanco del tema combinado con B da Ä, G con I = T, U con N = C, E con E = Î, y así se prosigue hasta generar la encriptación pàätcî:üèäôvzsfèèxoxig (pp. 133-135).

Para exaltar las virtudes de las técnicas polialfabéticas por encima de las monoalfabéticas, Garden ofrece la siguiente reflexión: "Si se adopta por llave la colección de los 73 signos [...] en la tabla, en cualquier orden absolutamente arbitrario que se les combinase tendríamos igualmente hasta 73 signos diferentes para traducir cada uno de los signos o blancos del tema, lo que en los métodos ordinarios exigiría 5329 signos" (p. 135). Todo lo anterior se verifica sólo en tanto la llave se cambie periódicamente, y que ésta no contenga caracteres repetidos, pero en última instancia equivale a decir que la única alternativa a un similar esquema polialfabético sólo podrá ser un esquema de tipo nomenclátor, o bien alguna especie de código de una o dos partes, en donde para cada carácter se tendría que formar un grupo de 73 sustitutos posibles, o sea, 73 grupos independientes de 73 elementos, luego "5329 signos" en total. Esta evaluación es muy discutible, además, impone suponer

[30] En la versión digital del tomo revisado esta tabla aparece doblada en cuatro partes, entre las pp. 140 y 141. Pero lo que de ella se muestra legible es apenas un fragmento que no basta para ilustrar la riqueza de su composición general. Por tal motivo, decidí no insertarlo como imagen.

como corriente la necesidad de encriptar montos de texto muy grandes, aunque esto no implique necesariamente transformar al documento por entero. Como sea, el ejemplo aducido revela que la E, "tan frecuente en el discurso francés" (así como en el de tantos idiomas romances), está presente seis veces, pero acaba encriptada cada vez por un signo diferente. Lo mismo sucede a propósito de las tres R, las dos L y las dos A en la misma frase. El signo *é*, repetido en la frase, tiene dos significaciones diferentes (pp. 135-136).

Para descifrar, dice Garden, la llave debe escribirse bajo el criptograma "de la misma manera absoluta que ha debido estarlo bajo el tema", según lo hiciera el criptógrafo original. Luego se procede, por así decir, en reversa, hasta recuperar cada elemento del texto plano. Con este método es posible cifrar y descifrar muy aprisa y evitar errores con el auxilio de "dos reglas planas" que se hacen correr juntas, como escuadra, entre el mapa de los sustitutos. Ahora, no es preciso cifrar el despacho completo; en el caso de las partículas y "otras palabras de uso frecuente", tales como artículos, pronombres, preposiciones, adverbios y conjunciones (que "nada enseñan" salvo por su combinación con términos menos particularizados), es innecesario asignarles signos especiales, "como se acostumbra [...] en la mayor parte de los métodos conocidos". Lo único urgente, subraya, es que "el pliego cifrado sea impenetrable", y el sistema recién propuesto puede conseguir tal efecto, pues quien carece de la llave en vano la buscará, ello sería como tratar de asir "un grano de arena particular en el fondo del océano" (pp. 136-137)[31].

Por otra parte, si un número expresado con letras o signos aritméticos debe ser tomado en el sentido ordinal, una cruz o cualquier otro signo convencional puesto debajo de la traducción lo anunciará. Para nombrar individuos, objetos o instituciones de las que los corresponsales tratan continuamente, lo ideal es asignarles equivalentes fijos (términos código). Para variar las llaves periódicamente convendrá definir tácticas o contraseñas tales, que la indicación gráfica del cambio será imposible de percibir por cualquier sujeto ajeno a esta red de cifra (p. 139).

En fin, este método, visto en conjunto, proporciona según Garden ventajas inigualables, ya que ofrece una "variabilidad indefinida, dependiente únicamente de la voluntad del que la emplea" (p. 140).

Una última consideración histórica y bibliográfica. Hasta el momento sólo he sabido de una traducción de este *Traité* a otra lengua, me refiero a la castellana que debemos a Vicente García Torres (1811-1894)[32]. Bajo el título *Tratado completo de diplomacia, ó teoría general de las relaciones exteriores de las potencias de Europa, conforme a las más célebres autoridades, por un antiguo ministro*, la imprimió en 1838 Miguel González ("tercera calle Real n. 3"), en tres tomos, y en las páginas 108-123 del segundo se sigue hallando lo referente a criptografía, notándose aquí, sin embargo, que el ejemplo de aplicación se deja sin traducir y no está incluida la matriz de alfabetos. Con todo, en otro lugar he mostrado que esta sec-

[31] Garden refuerza su postura añadiendo una tabla con las permutaciones de los primeros 16 números naturales: cada uno, a partir del 2, se multiplica por el producto del número inmediatamente precedente, de modo que 2 por 1 es igual a 2 permutaciones, 3 por 2 a 6, 4 por 6 a 24, y así siguiendo tenemos que al 16 le tocan casi cuatro mil millones de posibles permutaciones, resultando la cantidad de combinaciones posibles del número 73, o sea, el de signos en el cuadrángulo de alfabetos múltiples (p. 138).

[32] Periodista mexicano, recordado especialmente por haber fundado *El Monitor republicano*, un importante órgano informativo de las corrientes políticas liberales en México durante el siglo XIX.

ción fue leída y, de hecho, utilizada prácticamente por miembros de la diplomacia mexicana —sobre todo en Estados Unidos— entre 1849 y 1851[33].

5. Bibliografía

AGARWAL, Ravi P. y Syamal K. SEN, *Creators of Mathematical and Computational Sciences*, Heidelberg, New York, Dordrecht, London, Springer, 2014.

ALBERTI, Leon Battista, *A Treatise of Ciphers*, Torino, Galimberti, 1997.

BAKER, Christopher (ed.), *Absolutism and the Scientific Revolution, 1600-1720: A Biographical Dictionary*, Westport, Conn., London, Greenwood Press, 2002.

CALLIÈRES, François de, *De la maniere de negocier avec les souverains*, Amsterdam, 1716.

CARLISLE, Rodney P. (ed.), *Encyclopedia of Play in Today's Society*, vol. I, SAGE Publications, 2009.

CARTWRIGHT, W. C. (ed.), *Gustav Bergenroth: A Memorial Sketch*, Edinburgh, Edmonston and Douglas, 1870.

DE MORGAN, Augustus, *Arithmetical Books from the invention of printing to the present time, being brief notices of a large number of Works drawn up from actual inspection*, London, Taylor and Walton, 1847.

DOOLEY, John F., *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms*, Springer, 2018.

DURING, Simon, *Modern Enchantments. The Cultural Powers of Secular Magic*, Cambridge and London, Harvard University Press, 2002.

GAINES, Helen F., *Cryptanalisis: A Study of Ciphers and Their Solutions*, New York, Dover, 1956.

GARDEN, Guillaume, comte de, *Traité complet de Diplomatie. Théorie Générale des relations extérieures des puissances de l'Europe*, París, Librairie de Treuttel et Würtz, Rue de Lille, no. 17; Strasbourg, Grand'Rue, No. 15, 1833.

HEATLEY, D. P., *Diplomacy and the study of international relations*, Oxford, Clarendon Press, 1919.

HOOPER, William, *Rational Recreations in which the principles of numbers and natural philosophy are clearly and copiously elucidated, by a series of easy, entertaining, interesting experiments, among which are all those commonly performed with the cards*, 2 vols., London, B. Law and Son, 1794, 4a ed.

KING, David A., *The ciphers of the monks. A forgotten number-notation of the middle ages*, Stuttgart, Steiner, 2001

LEE, Sydney (ed.), *Dictionary of National Biography*, New York, Macmillan and Co./London: Smith, Elder, & Co., 1893.

LEYBOURN, William, *Pleasure with Profit: Consisting of Recreations of Divers Kinds, viz, Numerical, Geometrical, Mechanical, Statical, Astronomical, Horometrical, Criptographical, Magnetical, Automatical, Chymical, and Historical,* London, Printed for Baldwin and Dunton; near the Oxford-Arms in Warwick-Lane: And at the Raven in the Puoltry, 1694.

[33] R. R. NARVÁEZ, *Criptografía diplomática, política y militar en México, 1813-1926*, México, 2019, cap. 5.

LOHMANN VILLENA, Guillermo, "Cifras y claves indianas. Capítulos provisionales para un estudio sobre criptografía indiana", en *Anuario de Estudios Americanos*, t. XI, 1954, pp. 287-380 + láminas.

NARVÁEZ, Roberto R., *Criptografía diplomática, política y militar en México, 1813-1926*, México, SRE-Acervo Histórico Diplomático, 2019.

"Number games and other mathematical recreations", en *The New Encyclopædia Britannica*, vol. 25, Macropædia, Chicago, Encyclopædia Britannica, Inc., 1991, 15th ed.

ROOS, Anna Marie, "William Leybourn", en C. BAKER (ed.), pp. 228-229.

ROUSE BALL, *Mathematical Recreations and Essays*, London, Macmillan and Co., Ltd., 1926, 10th ed.

— *A Short Account of the History of Mathematics*, London, Macmillan and Co., Ltd., 1912, 4th ed.

WARDHAUGH, Benjamin, *Poor Robin's Prophecies: A Curious Almanac, and the Everyday Mathematics of Georgian Britain*, Oxford, Oxford University Press, 2012.

WATSON, Roger y Helen RAPPAPORT, *Capturing the Light. The Birth of Photography, a True Story of Genius and Rivalry*, New York, St. Martin's Press, 2013.

WERRETT, Simon, *Fireworks: Pyrotechnic Arts and Sciences in European History*, Chicago and London, The University of Chicago Press, 2010.

WILKINS, John, *Mercury, or The Secret and Swift Messenger*, London, printed for Rich, Baldwin, near the Oxford-Arms in Warwick-Lane, 1694.

Sitios web:

hathitrust.org
internetarchive.org
johnfdooley.com
rct.uk