ISSN: 1139-0107 ISSN-E: 2254-6367

MEMORIA Y CIVILIZACIÓN

ANUARIO DE HISTORIA

19/2016

REVISTA DEL DEPARTAMENTO DE HISTORIA,
HISTORIA DEL ARTE Y GEOGRAFÍA
FACULTAD DE FILOSOFÍA Y LETRAS
UNIVERSIDAD DE NAVARRA

Simon Kroll

Evolución de los sistemas criptográficos desde la Edad Media a la Moderna

Evolution of Cryptographic Systems from Medieval to Early Modern Times

pp. 181-199

DOI: 10.15581/001.19.181-199

Universidad de Navarra

Evolución de los sistemas criptográficos desde la Edad Media a la Moderna*

Evolution of Cryptographic Systems from Medieval to Early Modern Times

SIMON KROLL
Universität Heidelberg
simon.kroll@gmail.com

RECIBIDO: OCTUBRE DE 2016
ACEPTADO: DICIEMBRE DE 2016

Resumen: Este artículo quiere trazar la historia de la criptología europea desde la Antigüedad hasta el comienzo de la Edad Moderna, enfocándose especialmente en el paso de sistemas monoalfabéticos a sistemas polialfabéticos. Se aducen tres causas principales para explicar el rápido auge de la criptología en la Edad Moderna europea: la introducción definitiva del papel, la aparición de servicios postales y el comienzo de la diplomacia moderna. Se termina el artículo con una observación sobre la curiosa discrepancia entre el uso real de cifras y la evolución de nuevas tecnologías criptológicas.

Palabras clave: Criptología. Cifras. Edad Moderna. Sistemas polialfabéticos

Abstract: This article tries to describe the history of cryptology from Ancient to Early Modern times, paying special attention to the emerging of polyalphabetic ciphers. The author discusses three main reasons for this fast evolution of ideas in Early Modern Europe: the final implementation of the paper, the appearance of postal services and the beginning of modern diplomacy. The text concludes with an observation concerning the curious discrepancy between the actual use of ciphers and the evolution of new cryptologic technologies.

Keywords: Cryptology. Ciphers. Early Modern Times. Polyalphabetic Ciphers.

* El presente trabajo forma parte del proyecto de investigación *Secrets and Secrecy in Calderón's Comedies and in Spanish Golden Age Culture* financiado por el «Austrian Science Fund FWF» (project number P24903-G23) y el «Anniversary Fund del Oesterreichische Nationalbank» (project number 14725). Agradezco sus aportaciones y críticas a Wolfram Aichinger y a Fernando Rodríguez-Gallego.

1. INTRODUCCIÓN: LOS COMIENZOS EUROPEOS

En la Antigüedad las cosas estaban muy claras. Solo el príncipe, el rey, césar, dictador, o llámese como se llame el mandatario en el poder, era capaz de mantener un sistema de mensajeros, recaderos o embajadores. Solo él o ella tenía los recursos necesarios con los que poder pagar a personas para que viajasen por Europa llevando mensajes para aliados, generales en el campo de batalla, o enemigos, muchas veces solo de manera oral, a veces también por escrito. Es importante resaltar este monopolio extraordinario de toda comunicación a distancia[1]. Tal dominio casi total del conocimiento no inhibió, sin embargo, la elaboración de métodos criptográficos básicos para todo avance científico en este terreno que se dio a caballo entre la Edad Media y la Edad Moderna. Así, el objetivo de este artículo, tras esbozar brevemente los métodos antiguos como base de los sistemas por venir, consiste en presentar el repentino desarrollo de estas técnicas de escrituras secretas a partir de finales del siglo XV, además de encontrar explicaciones a por qué se dan precisamente en estos años los avances mencionados.

Tanto los griegos como los romanos tenían técnicas criptográficas. Y dada la importancia de una comunicación segura en asuntos bélicos, no sorprende que los más beligerantes de todos, los espartanos, hayan dejado noticia de un sistema criptográfico bastante ingenioso. Me refiero a la *skytale*:

> It was the Spartans, the most warlike of the Greek, who established the first system of military cryptography. As early as the fifth century B.C., they employed a device called the 'skytale', the earliest apparatus used in cryptology and one of the few ever devised in the whole history of the science for transposition ciphers[2].

La escítala consiste en una vara octaédrica que se envuelve con una tira larga de pergamino. El mensaje se escribe sobre el pergamino a lo largo de la vara. Si a continuación quitamos la vara, la tira de pergamino cae y el orden de las letras, establecido por la vara, se pierde. El mensaje se vuelve ilegible. Solo cuando el destinatario del mensaje cifrado coge

[1] Beyrer, 1996, p. 11.
[2] Kahn, 1966, p. 82. Ver también la más reciente edición de 1996, en la que añade algunos capítulos sobre la criptografía en tiempos de internet.

un palo de exactamente las mismas medidas y enrolla la tira de nuevo alrededor del palo, podrá leerse el texto.

Ilustración 1. Escítala, Fuente: https://de.wikipedia.org/wiki/Skytale

También uno de los políticos y militares más importantes del Imperio Romano, Julio César, se servía de cifras, en particular para su correspondencia con otros senadores, como Cicerón[3]. Este dato se basa sobre todo en los escritos biográficos de Suetonio:

> si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui inuestigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet[4].
>
> (Si tenía que tratar algún tema muy confidencial, lo escribía en clave, es decir, disponiendo el orden de las letras de tal forma que no pudiera formarse palabra alguna. Y, en caso de que alguien quisiera descifrarlas y entenderlas, había de cambiar cada letra por la tercera siguiente del alfabeto; así, por ejemplo, la D en lugar de la A, y lo mismo para las restantes letras[5].)

El código de César es un cifrado por sustitución, es decir, se sustituyen las letras originales por otras de un alfabeto alterado. César desplazaba el alfabeto para el texto cifrado hacia la derecha por un determinado número de espacios, comúnmente tres:

[3] Kahn, 1966, p. 84. Ver también la edición de 1996 con un muy interesante capítulo sobre cifras en tiempos de internet.
[4] Suetonius, *De vita caesarum*, 78.
[5] Suetonio, Vida de los doce césares, cap. LVI.

Texto original: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Texto cifrado: DEFGHIJKLMNOPQRSTUVWXYZABC

Es un cifrado seguro en su momento histórico, ya que el criptoanálisis, la ciencia para penetrar sistemas criptográficos sin conocer las claves correspondientes, todavía desconocía métodos estadísticos. Es más, el criptoanálisis no existía todavía y sería invención de los árabes en el siglo IX. Volveremos sobre dicho aspecto. Es importante subrayar ahora algunas de las ventajas sustanciales del método de César. Por un lado, es relativamente practicable, pues no hace falta un libro lleno de signos fantásticos, inventados, para su utilización, y solo se necesita el conocimiento del alfabeto latino. Además, es un sistema variable y, aunque César solo utilizaba una posición desplazada, según Suetonio, es obvio que en un alfabeto con 23 letras hay 22 posiciones posibles para el alfabeto del texto cifrado, dependiendo de la cantidad de espacio con que se desplace dicho alfabeto a la derecha[6].

Sabemos que Augusto usaba una cifra parecida aunque bastante más simplificada. Solo reemplazaba cada letra del texto original con la que le sigue en el alfabeto. Es decir, cambiaba la «a» por una «b», la «b» por una «c», etc. Curiosamente se sigue utilizando este método de cifrar en la Antigüedad tardía y en la Edad Media europea. Así, Bernhard Bischoff anota una serie bastante grande de cifras presentes en documentos medievales. Son todas bastante sencillas y entre ellas se encuentra el sistema de Augusto, que aparece en varios documentos del Vaticano y de Oxford[7]. Incluso san Isidoro de Sevilla menciona el método de Augusto y pasa por alto el de César, a pesar de basarse en la misma fuente histórica que nosotros, los libros de Suetonio. ¿No reconoció que el método de César era mejor, entre otras cosas porque puede variarse? De todos modos, anota en el primer apartado de su obra monumental, «Acerca de la gramática»:

> Notas etiam litterarum inter se veteres faciebant, ut quidquid occulte invicem per scripturas significare vellent, mutue scriberent. Testis est Brutus, qui in his litteris ea quae acturus erat notabat, ignorantibus aliis quid aliis quid sibi vellent haec litterae[8].

[6] El alfabeto clásico del latín tenía solo 23 letras.
[7] Bischoff, 1954, p. 5.
[8] Isidoro de Sevilla, *Etimologías*, I, 25,1, p. 304.

> (También nuestros antepasados utilizaban notas secretas en su correspondencia para poder mantener oculto a un tercero cuanto mutuamente deseaban transmitirse por la escritura. De ejemplo nos sirve Bruto cuando escribía en clave lo que se proponía realizar, e ignoraban todos lo que aquellas letras querían decir)[9].

A continuación cita la obra de Suetonio, que también explica la cifra que utilizaba Augusto, y anota que «había otros que escribían con las letras al revés» («Quidam etiam versis verbis scribunt»)[10]. A pesar del inmenso valor intelectual que posee la obra de Isidoro, se hacen evidentes dos cosas en este breve apartado acerca de la criptografía: 1) la conciencia de la importancia de cifras y códigos sigue existiendo en la Antigüedad tardía y seguirá existiendo durante la Edad Media; 2) el empobrecimiento del conocimiento de los recursos técnicos en dicho periodo. Ambos aspectos caracterizan igualmente la Edad Media europea.

No fue este precisamente un tiempo muy productivo para la criptografía. Esto no quiere decir que no se soliesen cifrar de cuando en cuando textos, pero todos los sistemas son bastante simples y ninguna innovación del peso de la de César aparece en el Medievo europeo. El casi fundador de la investigación moderna sobre la criptografía y su historia, David Kahn, lo describe con estas palabras pintorescas:

> In the Europe of the Latin alphabet —from which modern cryptology would spring— cryptography flickered weakly. With the collapse of the Roman empire, Europe had plunged into the obscurity of the Dark Ages. Literacy had all but disappeared. Arts and sciences were forgotten, and cryptography was not excepted. Only during the Middle Ages occasional manuscripts, with an infrequent signature or gloss or «deo gratias» that a bored monk put into cipher to amuse himself, fitfully illuminate the cryptologic darkness, and, like a single candle guttering in a great medieval hall, their feeble flarings only emphasize the gloom […].
>
> For almost a thousand years, from before 500 to 1400, the cryptology of Western civilization stagnated[11].

En esta época empieza a florecer la cultura musulmana, y sería ella la que produciría los primeros testimonios de un acompañante significa-

[9] Isidoro de Sevilla, *Etimologías*, I, 25,1, p. 305.
[10] Isidoro de Sevilla, *Etimologías*, I, 25, 2, pp. 304-305.
[11] Kahn, 1966, p. 89.

tivo de la criptografía, el ya brevemente mencionado criptoanálisis[12]. Se trata del arte de descifrar un mensaje cifrado sin conocer la clave o el método con el que ha sido encriptado. Una parte fundamental del criptoanálisis es el método estadístico, sobre todo para métodos del tipo del de César, que son muy vulnerables frente a este ataque. Sin embargo, conviene repetir que el código de César otorgaba una seguridad inmensa mientras estos métodos estadísticos no habían sido elaborados. Se descubren estos en la famosa *Casa de la sabiduría*, en Bagdad. En ella el filósofo, matemático y también criptólogo Abu Yusuf al-Kindi (801-873) escribe un manuscrito que es el primer documento en el que se describen técnicas criptoanalíticas, en especial el uso de métodos estadísticos al respecto[13]. Dice en su *Manuscrito para descifrar mensajes criptográficos* en traducción inglesa:

> One way to solve an encrypted message, if we know its language, is to find a different plaintext of the same language long enough to fill one sheet or so, and then we count the occurrences of each letter. We call the most frequently occurring letter the «first», the next most occurring letter the «second», the following most occurring letter the «third», and so on, until we account for all different letters in the plaintext sample.
>
> Then we look at the ciphertext we want to solve and we also classify its symbols. We find the most occurring symbol and change it to the form of the «first» letter of the plaintext sample, the next most common symbol is changed to the form of the «second» letter, and the following most common symbol is changed to the form of the «third» letter, and so on, until we account for all symbols of the cryptogram we want to solve[14].

2. EDAD MODERNA

Las cosas cambiarían radicalmente al comienzo de la Edad Moderna. En un curioso movimiento inverso podemos detectar un olvido casi total del conocimiento criptológico en el mundo árabe[15] y un auge insólito de sistemas criptológicos en Europa, algunos de los cuales son todavía la base para nuestros métodos modernos de criptología. Este auge del conocimiento europeo de la ciencia de las escrituras secretas se describe

[12] Ver Al-Kadi, 1992.
[13] Ver Al-Kadi, 1992, p. 106.
[14] En Singh, 2000, p. 17.
[15] Kahn, 1966, p. 98.

en cada historia de la criptografía o en los manuales de dicho tema. Muy pocos investigadores de estas técnicas culturales han tratado de explicar por qué aparece esta innovación precisamente en estos años. El único argumento que se suele dar al respecto es la vuelta paulatina de una cultura de la escritura, opuesta a la oralidad medieval. Y parece lógico: si se apuntan más detalles sobre soportes materiales, como cartas, hay más necesidad de encriptar mensajes. Así, apunta también David Kahn: «it must be that as soon as a culture has reached a certain level, probably measured largely by its literacy, cryptography appears spontaneously —as its parents, language and writing, probably also did»[16].

No obstante, es un argumento demasiado vago para explicar una evolución de tal envergadura y me gustaría discutir a continuación algunas novedades que se produjeron en el cambio de la Edad Media a la Edad Moderna y que tienen una influencia directa en la evolución de la criptología: vamos a hablar de un nuevo medio, de un nuevo servicio, y de política.

2.1. Papel

Es cierto: el papel ya empieza a llegar a Europa antes del año 1000[17]. Sin embargo, necesitará algunos años, mejor dicho siglos, para convertirse en el nuevo medio de uso general, en vez del pergamino. Según Meyer y Sauer, habría que esperar hasta el siglo XIV para convertirse en el medio principal[18]. ¿Por qué es crucial la aparición del papel en Europa, cuando ya se podía anotar un mensaje cifrado perfectamente sobre un pergamino, papiro, piedras o incluso la piel humana[19]? La importancia no radica quizá tanto en la materialidad del soporte[20], sino más bien en las consecuencias que tendrá la implementación del nuevo medio.

En cuanto a las condiciones de producción, la diferencia entre el pergamino y el papel es abismal: una vez instalados los molinos de papel

[16] Kahn, 1966, p. 84.
[17] Meyer y Sauer, 2015, p. 360.
[18] Meyer y Sauer, 2015, p. 362.
[19] Hay una anécdota de la Antigüedad según la cual se supone que le afeitaron la cabeza a un esclavo, luego tatuaron el mensaje en su piel y esperaron a que su pelo volviese a crecer para que pasase desapercibido.
[20] Aunque se podría reflexionar sobre si la diferencia más importante entre pergamino y papel es de importancia para nuestro tema: un texto sobre un pergamino nunca es definitivo, puesto que es posible borrar una letra escrita sobre un pergamino, mientras que un papel, una vez manchado de tinta, siempre quedará manchado. Este carácter definitivo del texto escrito sobre papel incita quizá más a cifrarlo.

en Europa, producen papel de manera rápida y barata, siempre en comparación con el pergamino, claro está. El papel sigue siendo un recurso de elevado coste; sin embargo, su precio ya no es comparable al del pergamino. Conocemos perfectamente uno de los resultados de esta implementación del nuevo medio: la imprenta, que aparece poco después, a mediados del siglo XV. Pero hay otra consecuencia de importancia para nuestra pregunta: al tener un soporte más asequible, empieza a ser posible para más personas el escribirse cartas, por lo que aparecen los grandes gobiernos de papel en Europa, al igual que la correspondencia personal, en dimensiones mucho más grandes que durante la Edad Media. Todos ellos utilizaron cifras[21] porque era más que ingenuo suponer que una carta que se envía de una ciudad a otra, o de un país a otro, no iba a ser abierta y leída por otras personas, curiosas por descubrir los secretos que un papel doblado, probablemente metido en un sobre, podría guardar[22].

El papel es, por tanto, una de las razones por las que aparece un nuevo servicio que, tras una larga evolución, se encargará únicamente de llevar cartas y paquetes de un lado a otro. Hablemos, pues, del servicio postal.

2.2. El servicio postal

La Edad Moderna ve también la implementación de servicios postales monopolizados por el Estado. No es que la Edad Media no haya conocido mensajeros de todo tipo. El hombre y la mujer medievales podían usar el correo universitario, el de los monjes o el de los gremios de profesiones (como, por ejemplo, los de los diferentes mercaderes), que también en la Edad Media dependían de una comunicación a distancia[23]. Al comienzo de la Edad Moderna se empieza a establecer el monopolio estatal del servicio postal a través de una red de postas donde los empleados de correos podían cambiar los caballos[24]. De esta manera fue posible manejar una gran cantidad de envíos en un tiempo bastante razonable. En Austria la familia Taxis se encargaría de establecer este servicio postal con gran éxito[25]. A finales del siglo XV se empieza a crear un siste-

[21] Meister, 1902 y 1906; Jütte, 2011, p. 88-89.
[22] Täubrich, 1997, p. 49.
[23] Ver Rauscher, 1946, pp. 8-10.
[24] Ver Kalmus, 1937, p. 48, y también Kießkalt, 1938.
[25] Bauer, 1906.

ma de postas muy eficaz por cuyas manos pasaría pronto una parte considerable de la correspondencia europea. Sin embargo, no es el primer estado que trata de unificar los distintos servicios postales en un único monopolio. Francia ya había conseguido la creación de dicho servicio en 1464 bajo el reinado de Luis XI[26].

> Tandis […] que Louis XI avait institué une poste destinée exclusivement au service de l'État; qu'Henri III, par son édit de novembre 1576, avait définitivement créé le service des messageries; qu'Henri IV avait organisé la Poste aux chevaux, Richelieu mit définitivement le service des Poste à la disposition du public et créa vraiment la Poste moderne[27].

Cada carta que se envía a otra ciudad o país corre el peligro de ser abierta y leída por otra persona. De manera que también en la Edad Media se solían usar, aunque en menor medida que durante la Edad Moderna, cifras para asegurar la seguridad de una información[28]. No obstante, es también el monopolio estatal del servicio postal el que crea más necesidad de protegerse. La historia del servicio postal es también la del control por parte del Estado de toda la comunicación escrita. Buena parte de Europa solo consiguió el respeto por el secreto epistolar a finales del siglo XX[29]. La implementación de un servicio postal monopolizado le permite un control extraordinario al estado respectivo[30]. Sobre todo a partir del momento en el que los distintos servicios postales se encargan no solo de las cartas de su propio gobierno, sino también de cartas privadas y de las de diplomáticos y políticos de otros países, a veces enemistados, se hace palpable la necesidad de asegurar el contenido de las cartas mediante distintos códigos cifrados[31].

Resumiendo, podemos decir que la aparición de los servicios postales modernos crea una creciente demanda de métodos criptológicos para la comunicación a distancia. Pero me gustaría anotar una tercera innovación de la Edad Moderna que también habrá provocado más demanda en el ámbito criptológico. Me refiero a la investidura de embaja-

[26] Racevskis, 2001, p. 31; Laurent, 1922, p. 9.
[27] Laurent, 1922, p. 9. Ver también Le Roux, 2002.
[28] Bischoff, 1954.
[29] Que ese respeto es una ilusión tuvimos que aprenderlo poco después, al comienzo del siglo XXI.
[30] Hubatschke, 1975, pp. 1122 y 1130.
[31] Hubatschke, 1975, pp. 1123 y 1140-1141. Ver también Preto (2010, pp. 268-272) para el ejemplo de Venecia.

das y embajadores permanentes en las capitales de los distintos reinos europeos.

2.3. Diplomacia

La diplomacia moderna tal y como la conocemos, con embajadas permanentes y embajadores de turno, aparece en Europa en la transición de la Edad Media a la Edad Moderna. Desde Bizancio llega la diplomacia moderna a Europa. Los primeros estados en cultivarla fueron los del norte de Italia, como Venecia, Milán o Florencia[32]. La diplomacia necesita de secretos, como bien ha demostrado Seiz Rodrigo[33]. Y un enviado italiano en la corte de París, por poner un ejemplo, necesitará algún sistema para, por lo menos, tratar de comunicarse en secreto con su corte en Italia, puesto que él es prácticamente un espía, denominado «espía honrado» por los comentaristas de los siglos XVI y XVII[34]:

> Che l'ambasciatore abbia come compito primario la raccolta di notizie e il vero e proppio spionaggio è quasi ovvio sin dal tardo Medioevo e nei primi tempi dell'età moderna quando cominciano ad affermarsi le rappresentanze diplomatiche stabili[35].

El propio Maquiavelo recomienda el uso de cifras en estos casos, y la influencia de sus escritos en la política de su tiempo es bien conocida[36].

En el caso del siglo XVII español encontramos una muy influyente mención de la importancia de la cifra en el tratado *El embajador* de Juan Antonio de Vera. Especialmente en el discurso tercero subraya la necesidad de cifrar mensajes diplomáticos, narrando ejemplos de cartas interceptadas del siglo XVI[37]. Y escribe:

> Es en fin importante parte de la legacía la cifra, y a veces es el todo de una grande acción, y será en los tiempos presentes mal seguros culpable confianza o pereza, fiar negocio cuya publicidad puede traer inconveniente menos que a muy acreditada cifra[38].

[32] Nicolson, 1955, p. 36.
[33] Seiz Rodrigo, 2010, p. 78. Ver también Preto, 2010 y Kroll, 2012.
[34] Preto, 2010, p. 198.
[35] Preto, 2010, p. 198.
[36] Machiavelli, *The Art of War*, p. 198. Ver también Pesic, 1997, p. 675, y Jütte, 2011, p. 87.
[37] Vera, *El embajador*, III, fols. 18v-22.
[38] Vera, *El embajador*, III, fol. 19r.

Por varias razones es importante mencionar este tratado aquí. En primer lugar, es el primer tratado sobre diplomacia escrito en castellano y se convierte muy poco después de su publicación en un tratado básico para diplomáticos españoles. A partir de las años treinta del siglo XVII incluso se traduce al francés y al italiano por considerarse también fuera del ámbito hispanohablante un tratado importante que debe ser conocido por todos los embajadores[39]. Este libro aporta, además, otros indicios para las hipótesis de este trabajo. Cuando habla de las cifras, por ejemplo, siempre menciona el problema de la seguridad del servicio postal[40], respaldando una de las tesis principales de este artículo. El hecho de que su tratado sobre diplomacia verse además tan detenidamente sobre problemas de cifras subraya a su vez la influencia que tuvo para la evolución de la cifra.

A partir del siglo XV las cortes europeas buscan, por tanto, los mejores matemáticos y criptólogos para asegurar sus correspondencias[41], aunque es cierto que también personas privadas practicaban métodos criptológicos, como demuestra esta carta de un judío alemán del siglo XVII:

> Sonst, libe schwester, wis, das ich habe die *[Geheim-]sprache* verloren […] drum schik mir es mit imanten gewis wieder her die *[Geheim-]sprache*, den man kann nit also ales teisch iber feld schreiben[42].
>
> (Además, querida hija, debes saber que he perdido la cifra […] así que envíamela de todas maneras de vuelta, porque no se puede escribir simplemente todo en alemán lo que va a larga distancia).

Sin embargo, el comienzo de la diplomacia moderna es una de las causas por las que se genera una creciente demanda de métodos criptológicos.

2.4. La innovación

Hacia la mitad del siglo XV Leonardo Dato, secretario del papa, y su amigo Leon Battista Alberti tuvieron una conversación en los jardines

[39] Debo estos datos a la generosidad de Conchi Gutiérrez.
[40] Vera, *El embajador*, III, fol. 18v.
[41] Jütte, 2011, p. 90. Ver también el interesante capítulo sobre la *Scotografia* de Ambramo Colorni (a partir de p. 258). La fortuna del libro y de su autor son un buen ejemplo de los esfuerzos de las cortes europeas por conseguir los mejores criptólogos. Ver al respecto además Meister, 1902 y Meister 1906.
[42] Citado en Jütte, 2011, pp. 88-89 (la traducción es mía).

del Vaticano. Hablaron de la novedosa técnica de la imprenta y finalmente acabaron por hablar de cifras. Alberti cita algunas palabras del diálogo que tuvo con Dato, y decía este:

> Tu invero —disse guardandomi il Dati— da sempre impegnato a investigare le arti occulte e ad indagare nei misteri della natura, che pensi di questi, se possiamo chiamarli così, interpreti di cifre e rivelatori di segreti?[43].

Y un poco adelante dice Dato respondiendo a la pregunta de si en su trabajo de secretario del papa tenía que ver con ese tipo de problemas:

> È vero —rispose il Dati— e non mi spiacerebbe, in conformità del mio ruolo, potermela sbrigare da solo, senza dover ricorrere a un estraneo che sia espero di linguaggi cifrati. Succede che talvolta vengano intercettati dalle spie e giungano sulle nostre scrivanie dei messaggi in cifra che ci pare meritino una certa attenzione. Se quindi hai scoperto qualcosa al riguardo, te prego de farmene parte[44].

Alberti cita esta conversación en su obra *Dello scrivere in cifra*[45], que escribió a raíz de ella y que revolucionó la criptografía moderna. Y conviene citarla aquí, puesto que nos demuestra cómo la práctica diaria criptológica generó la demanda y la pasaría a las cabezas más brillantes de su siglo. Leon Battista Alberti fue una de ellas. En su obra criptológica describe el primer sistema sustitucional polialfabético que ha llegado a nuestro conocimiento. Es decir, se trata de un método en el que se sustituyen las letras del texto original con caracteres de diferentes alfabetos para conseguir el texto cifrado.

¿Cómo funcionaba el sistema de Alberti? Se basa en el uso de dos discos. Sobre el más pequeño, el interior, se colocan todas las letras del alfabeto, y sobre el más grande, el exterior, se anota una combinación de 20 letras y 4 números[46]. Ambos discos se sitúan sobre el mismo eje y pueden moverse. He aquí una ilustración para facilitar la comprensión:

[43] Alberti, *Dello scrivere in cifra*, p. 4.
[44] Alberti, *Dello scrivere in cifra*, p. 4.
[45] Para la compleja situación de su transmisión puede verse Mendelsohn (1940) y la magnífica edición (Alberti, *Dello scrivere in cifra*) de la que estoy citando. También conviene mirar la traducción al inglés preparada por los mismos editores (Alberti, *A Treatise on Ciphers*). Ambas ediciones contienen también el texto en latín.
[46] Ver también Galende Díaz, 1995, p. 78.

Ilustración 2. Disco de Alberti. *Fuente:* https://es.wikipedia.org/wiki/Cifrado_de_Alberti

Las letras del disco interior representan el texto original, no cifrado, mientras que las letras y números del disco exterior corresponden al texto cifrado. Para encriptar un texto se sustituyen las letras del texto original, pongamos como ejemplo «Roma», con los signos correspondientes del disco exterior, teniendo este en una posición determinada. Si tomamos la posición del disco de la ilustración, tendríamos que encriptar la palabra «Roma» con el siguiente código: «FQR2». El que quisiera descifrar el texto cifrado tendría que tener un aparato igual y usar la misma posición de los dos discos.

Si Alberti se hubiera detenido ahí, solo habría inventado un instrumento muy práctico para el uso del cifrado César que vimos al comienzo de este texto. La innovación que cambiaría la historia de la criptografía moderna la explica poco después:

> Quando avrò scritto tre o quattro parole muterò nella nostra *formula* la posizione dell'indice, ruotando il disco fino a che, ammettiamo, l'indice k si trovi sotto la R maiuscola. Allora nella missiva scriverò una R maiuscola e, da questo punto in poi, la k minuscola assumerà il significato non più della B, ma della R, e le lettere che seguiranno nel testo riceveranno nuovi significati dalle sovrastanti maiuscole del disco fisso[47].

Es decir, Alberti propone cambiar la posición de los dos discos después de que se hayan cifrado algunas palabras del texto original. Su

[47] Alberti, Dello scrivere in cifra, p. 20.

aparato se convierte de esta manera en una herramienta perfecta para una cifra sustitucional polialfabética. Este sistema es absolutamente inmune a los análisis estadísticos que por aquel entonces ya estaban llegando a Europa. El propio Alberti describe este método de criptoanálisis en su texto[48]. La seguridad del cifrado polialfabético era tal que pronto se creó el mito de su presunta invulnerabilidad absoluta[49]. Sin llegar a este extremo, sí es cierto que el criptoanálisis iba a necesitar 300 años para elaborar y describir un método para descifrar un cifrado polialfabético sin conocer la llave correspondiente[50].

La idea revolucionaria del italiano pronto se daría a conocer en toda Europa, aunque parece que algunos criptólogos llegaron a la misma idea sin conocer los trabajos de Alberti. Eruditos como Johannes Tritemio, Blaise de Vigenère o Giovanni Battista della Porta son los nombres más destacados y conocidos en la elaboración de distintos métodos para hacer más practicable el uso de cifrados polialfabéticos. No es el momento para describir cada uno independientemente, puesto que la idea principal polialfabética es igual en todos ellos. Me parece importante destacar al respecto la rápida aparición del mismo sistema en varios países europeos, lo que parece confirmar la idea principal de este artículo de que una creciente demanda a nivel europeo generó esta multiplicación de ideas innovadoras después de cientos de años de estancamiento.

Al menos en el caso de Tritemio, conviene apuntar, además, otra influencia para la elaboración de sus ideas criptológicas. Me refiero al descubrimiento de la cábala por las culturas cristianas de Europa en el siglo XV.

En la Edad Media aparece entre los judíos europeos en el sur de Francia y en el norte de España una tradición religiosa que elabora estrategias de lectura de un texto sagrado para interpretar dicho texto. Es la tradición de la cábala hebrea. Trata de leer el texto de la Torá con estrategias de lectura combinatorias para descubrir sentidos más profundos del texto sagrado. Así, se sirven del valor numérico de las letras hebreas, de anagramas y acrósticos para sus lecturas. Estos conceptos religiosos proporcionan al receptor no judío métodos combinatorios para el trabajo con

[48] Kahn, 1966, p. 127.
[49] Kahn, 1966, p. 150.
[50] Beutelspacher, 2002, pp. 31-33; Kroll, 2015, p. 16.

textos. Es muy probable que este fenómeno haya influenciado sobre todo al abad Tritemio[51]. Así, apunta la investigadora von Samsonow:

> Die liebende Umkreisung des göttlichen Namens in der hebräischen Kabbala schlägt nach ihrer Entdeckung für die Latinität und die europäischen Sprachen um in eine Attacke auf den Sinn […]. Die Steganographie […] wird zur Kabbala des europäischen Geistes[52].
>
> (El orbitar amoroso del nombre divino en la cábala hebrea se vuelve, después de su descubrimiento por la latinidad y los idiomas europeos, un ataque al sentido, que multiplica la cantidad de enigmas escritos. La esteganografía llega a ser la cábala del ingenio europeo[53].)

Pero la cultura del secreto del Barroco es más complicada de lo que a primera vista podría parecer[54] y de lo que sugieren muchos de los manuales de criptología que suelen concentrarse en los grandes avances de esta disciplina, sin tener en cuenta el uso práctico de las cifras en las distintas épocas. Tratemos, por tanto, de acercarnos a la cultura de la criptografía en los primeros siglos de la Edad Moderna y de esta manera contribuir al estudio de la cultura del secreto en dicha época.

3. La cultura de la criptografía en los primeros siglos de la Edad Moderna

Entre el avance revolucionario de la criptología y el uso práctico de cifras en el día a día de las correspondencias hay una diferencia muy curiosa. A pesar de que los avances de Alberti, Tritemio, Vigenère y muchos otros hayan sido conocidos por los secretarios de cifra[55] en las cortes europeas, se seguían utilizando cifras menos complejas y que en algunos casos incluso se parecen a las medievales. El uso de tintas invisibles que solo se hacían visibles con un tratamiento especial, sustituir los términos políticos por términos inocentes del mundo mercantil y otros modos sustitucionales eran los métodos más frecuentes[56].

[51] Ver también Jütte, 2011, pp. 91-92.
[52] Samsonow, 1997, p. 284.
[53] Traducción mía.
[54] Ver al respecto sobre todo Aichinger, 2011 y 2013; Aichinger y Kroll, 2013. Jütte, 2011, también le consagra el primer capítulo de su obra a dicho tema, tratado asimismo por Seiz Rodrigo 2010.
[55] Con la aparición de las embajadas también se suele dar la de los secretarios de cifra, que se ocupaban únicamente del manejo de las cifras.
[56] Preto, 2010, pp. 269-271; Kahn, 1966, pp. 150-151.

Para crear el texto cifrado se solían utilizar tablas cifradoras. Comentemos brevemente el ejemplo del insigne tratadista Diego de Saavedra Fajardo, que en su correspondencia con Felipe IV se servía de dichas tablas[57]. Estas ofrecían, por un lado, combinaciones de letras y números para encriptar las letras del alfabeto y una serie de números. Además, usaban una tabla para sustituir términos frecuentes como «secreto», «Viena», «infante» o «Italia» con signos acordados. Así, «nos» significaba «Viena», o «ler», «secreto»[58]. Este tipo de cifras en las que se sustituyen los significantes del texto original por otros cifrados según una tabla era el más usado durante los primeros siglos de la Edad Moderna. Paolo Preto, por ejemplo, describe cifras muy parecidas que solía usar el servicio secreto de Venecia[59]. Estos métodos ofrecen una seguridad relativamente alta; sin embargo, no llegan a procurar el grado de seguridad de los de Alberti o Tritemio. El tratado mencionado arriba, *El embajador*, también menciona este tipo de cifrados. De Vera no parece haber entendido mucho sobre la técnicas conretas de la criptografía, puesto que describe estas cifras como muy fiables y seguras[60].

¿A qué se debe esta curiosa contradicción entre el avance de la ciencia y el uso concreto de sistemas de cifrado? ¿Por qué apenas se aplican los métodos polialfabéticos cuando se sabía que eran más seguros? La respuesta más sencilla, obvia y probablemente más válida es la problemática practicabilidad de dichas técnicas. Cifrar toda una carta con el método de Alberti significaba hacerlo letra por letra, cambiar después de un número determinado el alfabeto del texto cifrado, acordar una clave con el destinatario para coordinar el cambio de los alfabetos y comunicar clave y carta cifrada por separado. El margen de error es, además, bastante grande, y un único error en la sustitución puede invalidar todo el mensaje; en el caso de que se haya enviado con una errata, se tendría que pedir que se vuelva a cifrar el mensaje. Todo ello significa una pérdida enorme de tiempo, y el aumento de seguridad al aplicar dichos métodos parece que no recompensa esta pérdida. Si se leen, por ejemplo, las cartas del emperador austríaco Leopoldo I, se nota que cifraba con la misma velocidad con la que escribía el texto no cifrado. Además, se hace eviden-

[57] Galende Díaz, 1994.
[58] Galende Díaz, 1994, pp. 61-62.
[59] Preto, 2010, p. 271.
[60] Vera, *El embajador*, III, fol. 19r.

te que solo cifraba los términos clave; el resto del texto lo escribía en su extraña mezcla de alemán, francés, latín y español. La razón para el escaso uso de métodos polialfabéticos radica, por tanto, en su poca practicabilidad. La respuesta de la ciencia a la creciente demanda de nuevos métodos criptológicos fue en un primer momento insuficiente. Solo el uso de máquinas en el proceso de la encriptación significaría el éxito absoluto de los métodos modernos.

A pesar de la plausibilidad de la explicación que acabamos de exponer, podría aventurarse otra que tiene más que ver con la cultura del Barroco mismo. Y es que en el Barroco parece haber tratado de forma muy diferente el tema del secreto. Hasta cierto punto estaban perfectamente al tanto de que gran parte de la correspondencia diplomática era leída por el enemigo, y aquí tenemos que hablar nuevamente de los servicios postales. Junto a su creación aparece el *cabinet noir*, por primera vez en Francia. En estas cámaras se trataba de abrir, copiar y, si era necesario, también descifrar toda la comunicación epistolar que circulaba por el servicio postal. Es decir, si el embajador español en Francia se servía del correo francés para su correspondencia, tenía que contar con que todo lo que quería comunicarle en secreto a su rey se leía en la corte francesa incluso antes de que la carta dejara la ciudad. En el *cabinet noir* procuraban hablar todas las lenguas habituales, dominar los métodos criptológicos más importantes y tener todos los tipos de sellos, papel y tinta posibles para poder duplicar perfectamente toda carta que llegase al *cabinet*. Se dice de algunos potentados del tiempo que nos ocupa que se quejaban de que leían su correspondencia solamente en copias, puesto que los *cabinets noirs* que pronto aparecerían en toda Europa controlaban el tráfico de las cartas a la perfección[61].

4. CONCLUSIONES

La cultura del secreto en la Edad Moderna está marcada por un debate continuo sobre las fronteras entre el secreto y lo público. No sorprende, pues, que los grandes avances de la criptografía se den precisamente en esta época. La creciente demanda de nuevos métodos criptológicos debida a la evolución de la diplomacia, los servicios postales y también la implementación del papel en Europa generó una respuesta

[61] Hubatschke, 1975, p. 1160.

por parte de los científicos más prolíficos de su época. No obstante, esta no cumplió con los requisitos del tiempo, que pedía cifras seguras pero también de uso fácil y practicable. Por tanto, se siguieron elaborando sistemas más sencillos pero más fáciles de usar. De esta manera se pudo garantizar una seguridad relativa aunque, debido a los *cabinets noirs*, era bastante probable que una parte considerable de la correspondencia llegase a las manos del enemigo. La cultura del secreto en este tiempo es, por tanto, un continuo «yo sé que tú sabes que yo sé», «yo no sé si tú sabes que yo sé que tú sabes», y las variedades que puede llegar a tener esta situación en la que continuamente se mueven los límites del secreto.

BIBLIOGRAFÍA

Aichinger, Wolfram, «Laute Geheimnisse. Verheimlichen, Chiffrieren und Enthüllen in Calderóns Komödie und der Kultur des Barock», en *Laute Geheimnisse. Calderón und die Chiffren des Barock*, ed. Wolfram Aichinger y Simon Kroll, Wien, Turia + Kant, 2011, pp. 31-68.

Aichinger, Wolfram, «Confesores, espías, secretarios: los agentes ocultos del poder y su representación en el teatro de Calderón», en *Teatro y poder en el Siglo de Oro*, ed. Mariela Insúa y Felix K. E. Schmelzer, Pamplona, Universidad de Navarra/Publicaciones Digitales del GRISO, 2013, pp. 9-21.

Aichinger, Wolfram, y Simon Kroll, «Secrets and Secrecy in Calderón's Comedies and in Spanish Golden Age Culture. Outline of a New Research Focus in Calderonian Studies», *Hipogrifo*, 1, 2, 2013, pp. 135–144.

Al-Kadi, Ibrahim A., «Origins of Cryptology: the Arab Contributions», *Cryptologia*, 16.2, 1992, pp. 97-126.

Alberti, Leon Battista, *A Treatise on Ciphers*, ed. Augusto Buonafalce, David Kahn, Torino, Galimberti, 1997.

Alberti, Leon Battista, *Dello scrivere in cifra*, ed. Augusto Buonafalce, David Kahn, Torino, Galimberti, 1994.

Bauer, Wilhelm, «Die Taxis'sche Post und die Beförderung der Briefe Karls V. in den Jahren 1523 bis 1525», *Mitteilungen des Instituts für österreichische Geschichtsforschung*, 27, 1906, pp. 436-459.

Beutelspacher, Albrecht, *Geheimsprachen. Geschichte und Techniken*, München, C. H. Beck, 2002.

Beyrer, Klaus, «Der alte Weg eines Briefes. Von der Botenpost zum Postboten», en *Der Brief. Eine Kulturgeschichte der Kommunikation*, ed. Klaus Beyrer y Hans-Christian Täubrich, Heidelberg, Museumsstiftung, Post und Telekommunikation, 1996, pp. 11-26.

Bischoff, Bernhard, «Übersicht über die nichtdiplomatischen Geheimschriften des Mittelalters», *Mitteilungen des Instituts für österreichische Geschichtsforschung*, 62, 1954, pp. 1-27.

Galende Díaz, Juan Carlos, «Un diplomático español en la Europa del siglo XVII: Diego de Saavedra Fajardo y su clave criptográfica con Felipe IV», *Murgetana*, 89, 1994, pp. 55–62.

Galende Díaz, Juan Carlos, *Criptografía: Historia de la escritura cifrada*, Madrid, Editorial Complutense, 1995.

Hubatschke, Harald, *Ferdinand Prantner (Pseudonym Leo Wolfram), 1817-1871: Die Anfänge des politischen Romans sowie die Geschichte der Briefspionage und des geheimen Chiffredienstes in Österreich*, vol. 5, Wien, Univ. Diss., 1975.

Isidoro de Sevilla, *Etimologías*, edición bilingüe de J. Oroz Reta y M.-A. Marcos Casquero, introd. de M. C. Díaz y Díaz, Madrid, Biblioteca de Autores Cristianos, 2009.

Jütte, Daniel, *Das Zeitalter des Geheimnisses. Juden, Christen und die Ökonomie des Geheimen (1400-1800)*, Göttingen, Vandenhoeck & Ruprecht, 2011.

Kahn, David, *The Codebreakers. The Story of Secret Writing*, Winsley, Weidenfeld and Nicolson, 1966.
Kahn, David, *The Codebreakers. The Comprehensive History of Secret Communication from Ancient Times to the Internet*, New York, Scribner, 1996.
Kalmus, Ludwig, *Weltgeschichte der Post, mit besonderer Berücksichtigung des deutschen Sprachgebietes*, Wien, Amon Franz Göth, 1937.
Kießkalt, Ernst, *Die Entstehung der Deutschen Post und ihre Entwicklung bis zum Jahre 1932*, Erlangen, Palm & Enke, 1938.
Kroll, Simon, «Cifras y sus secretarios. Un manuscrito desconocido de Tomás Tamayo de Vargas», *Estudios Hispánicos*, 20, 2012, pp. 59–66.
Kroll, Simon, «Kryptologie: Entwicklungen einer Wissenschaft der Geheimnisse», *Historische Sozialkunde, Geschichte – Fachdidaktik – Politische Bildung*, 3, 2015, pp. 11–19.
Laurent, Benoît, *Poste et postiers*, Paris, Doin, 1922.
Le Roux, Muriel (dir.), *Histoire de la poste: De l'administration á l'entreprise*, Paris, Éditions rue d'Ulm/Presses de l'École Normale Supérieure, 2002.
Machiavelli, Niccolò, *The Art of War [Dell'arte della guerra]*, ed. Neal Wood, New York, Da Capo, 1965.
Meister, Aloys, *Die Anfänge der modernen diplomatischen Geheimschrift. Beiträge zur Geschichte der italienischen Kryptographie des XV. Jahrhunderts*, Paderborn/Wien, Schöningh, 1902.
Meister, Aloys, *Die Geheimschrift im Dienste der päpstlichen Kurie: Von ihren Anfängen bis zum Ende des XVI. Jahrhunderts; mit fünf kryptographischen Schrifttafeln*, Paderborn/Wien, Schöningh, 1906.
Mendelsohn, Charles J., «Bibliographical Note on the *De Cifris* of Leone Battista Alberti», *Isis*, 32.1, 1940, pp. 48–51.
Meyer, Carla, y Rebecca Sauer, «Papier», en *Materiale Textkulturen: Konzepte – Materialien – Praktiken*, ed. Thomas Meier, Michael R. Ott y Rebecca Sauer, Berlin/München/Boston, de Gruyter, 2015, pp. 355-370.
Nicolson, Harold, *Kleine Geschichte der Diplomatie*, Frankfurt am Main, Scheffler, 1955.
Pesic, Peter, «Secrets, Symbols, and Systems. Parallels between Cyptanalysis and Algebra, 1580-1700», *Isis*, 88, 1997, pp. 674-692.
Preto, Paolo, *I servizi segreti di Venezia. Spionaggio e controspionaggio ai tempi della Serenissima*, Milano, Il Saggiatore, 2010.
Racevskis, Roland, «Time, Postal Practices, and Daily Life in Mme. de Sévigné's Letters», en *Studies in Early Modern France*, vol. 7, *Rethinking Cultural Studies 2: Exemplary Essays*, ed. David Lee Rubin y Julia W Douthwaite, Charlottesville, Rokkwood Press, 2001, pp. 29-47.
Rauscher, Rudolf, *Geschichte des Postwesens*, Wien, Verlag für philatelistische Wissensgebiete, [1946].
Samsonow, Elisabeth von, «Die Hehler des Sinns. Zum Verhältnis von Kabbala und Secret Service», en *Schleier und Schwelle. Geheimnis und Öffentlichkeit*, ed. Aleida Assmann y Jan Assmann, München, Fink, 1997, pp. 281-290.
Seiz Rodrigo, David, *La disimulación honesta. Los gastos secretos en el reinado de Felipe IV entre la razón de estado y la merced cortesana*, Madrid, Ediciones Endymion, 2010.
Singh, Simon, *The Code Book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, New York, Anchor Books, 2000.
Suetonio, Gayo, *De vita Caesarum / Lives of the Caesars*, ed. John C. Rolfe, Boston, Harvard University Press, 1994.
Suetonio, Gayo, *Vida de los doce césares*, ed. Alfonso Cuatrecasas, Barcelona, Espasa, 2012 (eBook).
Täubrich, Hans-Christian, «Wissen ist Macht. Der heimlich Griff nach Brief und Siegel», en *Der Brief. Eine Kulturgeschichte der Kommunikation*, ed. Klaus Beyrer y Hans-Christian Täubrich, Heidelberg, Museumsstiftung, Post und Telekommunikation, 1996, pp. 46-55.
Vera, Juan Antonio de, *El embajador*, Sevilla, Francisco de Lyra, 1620.