LA CIFRA EN LA CORRESPONDENCIA DEL CONDE DE GONDOMAR

El epistolario del conde de Gondomar contiene un conjunto de cartas y otros tipos documentales que muestran aspectos importantes de la práctica criptográfica de la España moderna. En primer lugar, desde la perspectiva de la producción y recepción de los textos cifrados, se conservan al menos dos nomenclátores, es decir, dos claves que constituyen el instrumento imprescindible para encriptar y desencriptar un mensaje. Por otra parte, existe un conjunto de cartas que describe el protocolo seguido para el intercambio de esas claves. Y, finalmente, como resultado de esta práctica, se conservan un buen número de misivas cifradas, bien en su totalidad, bien parcialmente, que ocultan los asuntos críticos en los que se hallan inmersos sus autores, en su mayor parte representantes de la monarquía en el exterior. Afortunadamente, en la mayoría de los casos, obra del secretario de lenguas del destinatario de las misivas, se conserva la puesta en claro de la cifra, como anotación marginal, cuando se trata de fragmentos breves, o en folios contiguos, cuando el cifrado del mensaje es completo.

Louis Morin, *L'infant prodigue*. Paris: Delagrave, 1898 [RB INF/3144]

Técnicamente, los nomenclátores conservados nada aportan a los mecanismos de ocultación del texto habituales en la época: se trata de la técnica criptográfica en vigor durante al menos los reinados de Felipe III y Felipe IV, es decir, la de sustitución homofónica, en virtud de la cual para la sustitución de una determinada letra del texto plano están disponibles uno o más signos de la cifra, de ahí que los signos se consideren homofónicos.

El alfabeto, que da cuenta de esta correspondencia entre las letras del texto plano y las correspondientes a la cifra, que pueden ser, también, símbolos o números, se expone en el primer bloque del nomenclátor. La finalidad de evitar la correspondencia biunívoca, de uno a uno entre la letra y su cifra correspondiente, es impedir el análisis de frecuencias como método eficaz de criptoanálisis, es decir, de intento de ruptura de la cifra. En efecto, ya en la época es bien conocida la frecuencia relativa de las letras en las distintas lenguas. En este sentido, en el nomenclátor que se va a utilizar como modelo, que corresponde a la cifra general de 1625, y del que se conserva un ejemplar en el fondo Gondomar (II/1850, doc. 17), se observa que las vocales cuentan con cuatro cifras candidatas para su sustitución, frente a las consonantes, que disponen todas ellas de dos opciones (fig. 1).

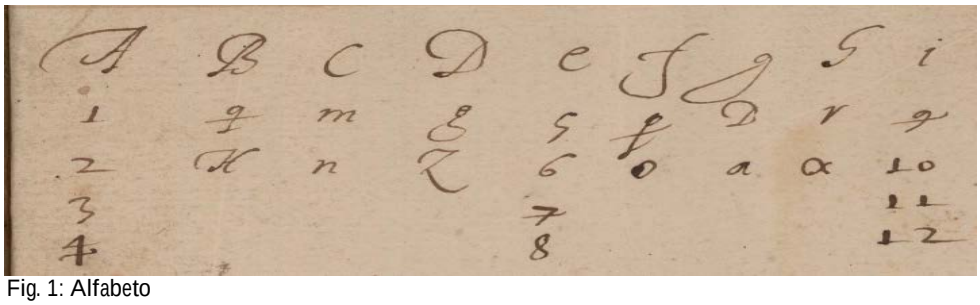

Fig. 1: Alfabeto

Pero, por si la homofonía no fuera un recurso suficiente para reforzar la cifra, existen otros mecanismos, agrupados en un segundo bloque del nomenclátor, que vienen en su ayuda para frustrar casi definitivamente la tarea del criptoanalista. El primero de ellos es la correspondencia entre grupos silábicos de dos o tres letras con un símbolo, un carácter o un grupo de caracteres de la cifra, ajenos a la sustitución letra a letra siguiendo la tabla alfabética que encabeza el nomenclátor. Así, a modo de ejemplo, dígrafos como 'la', 'le', 'li', se cifran, respectivamente, con 'fur', 'for', 'fer', o trígrafos como 'cha', 'che', 'chi', son cifrados con los números '100', '101' y '102', respectivamente (fig. 2).

Un tercer mecanismo que contribuye a la robustez de este sistema criptográfico lo constituyen las denominadas «nullas», «dúplices» y «finales de vocales». Las «nullas», como su nombre indica, constituyen una marca que invalida el símbolo al que acompañan: suele ser una cruz, a modo de diacrítico sobrepuesto, o dos puntos debajo, y es frecuente que haya varias opciones de nulidad dentro de un mismo nomenclátor. Incluso este procedimiento puede servir para eliminar renglones enteros, como se desprende del nomenclátor conservado en Simancas (AGS Leg 1/1/1, 28) que, a modo de adición al final, declara que «nullas serán también todos los renglones que comen-

NIPO: 046-19-007-9 · DEPÓSITO LEGAL:M-1496-1996

çaren con estas señales…».

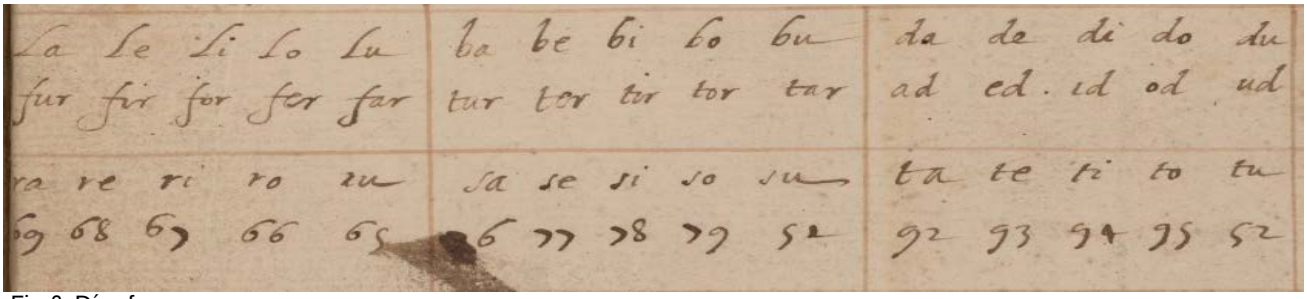

Fig. 2: Dígrafos

Las dúplices se utilizan para codificar las geminadas, como la 'll' o la 'nn'. El objetivo de este encubrimiento es impedir que el criptoanalista detecte dos símbolos iguales contiguos que, dada la escasez de este tipo de combinaciones, podría desencriptar fácilmente (fig. 3). Los números, por su parte, para ser identificados como tales, suelen llevar una marca superpuesta. Por último, las «finales de vocales» permiten en muchos casos asignar el género a un sustantivo. Por ejemplo, la cifra 'no', que representa al posesivo 'nuestro', seguida de la marca ':', que es final de vocal 'na', debe resolverse en 'nuestra'.

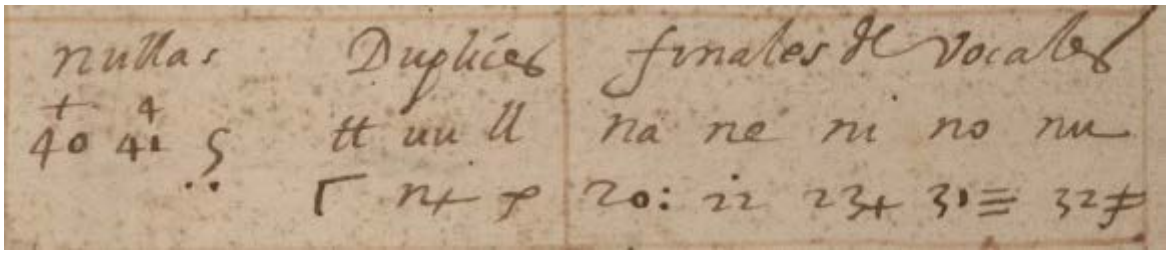

Fig. 3: Nulas, dúplices y finales de vocales

El denominado «diccionario» constituye un bloque aparte, el más extenso, dentro del nomenclátor, y está formado por la tabla de correspondencias entre palabras de uso frecuente o de ocurrencia esperable y el símbolo o grupo de símbolos de sustitución. Su orden es alfabético, por la palabra en lenguaje plano; y está organizado en columnas, haciendo corresponder a cada una de ellas un patrón concreto de caracteres para su cifra. Abundan las personas, referenciadas por su título nobiliario o su cargo, tales como los archiduques Alberto, Maximiliano, Leopoldo o Fernando, los duques de Baviera, Sajonia, Florencia, Osuna o Saboya, los reyes de Francia, Inglaterra, Dinamarca o España; nombres de lugares, como Flandes, Ferrara, Barcelona, Florencia, Argel, Inglaterra o Piamonte, que acotan la amplia geografía de la monarquía española; palabras comunes del lenguaje militar, como artillería, armada, fortificación, paz, capitán, castillo, caballería; palabras que delatan la presencia de la religión, como hereje o fe o sede apostólica o doctrina. En fin, una muestra representativa del repertorio léxico de una época histórica, con sus personajes, su pensamiento y su lucha (fig. 4).

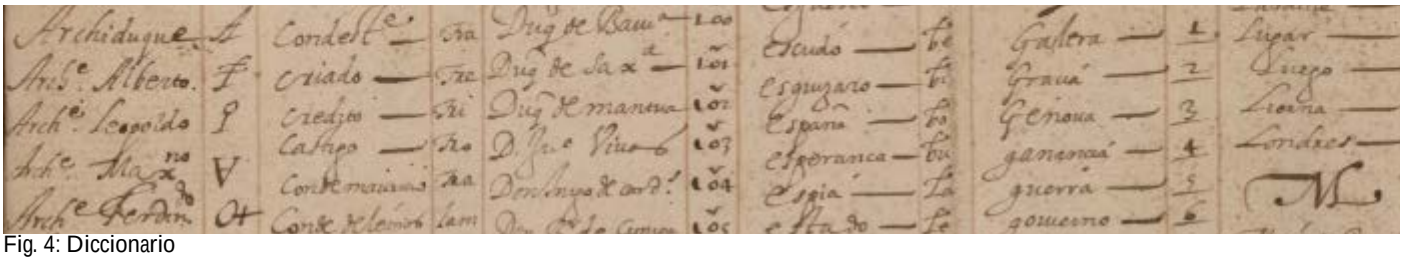

Fig. 4: Diccionario

En lo que se refiere a las noticias sobre la práctica criptográfica contenidas en este fondo, es posible comprobar los sucesivos procesos de cambio de cifra y los protocolos que se siguen para llevarlos a cabo. El primer cambio del que tenemos testimonio es el que se produce en 1615, que corresponde a la primera embajada de Gondomar en Inglaterra: Luis Gaitán, por carta desde Pavía fechada el 15 de marzo de ese año, solicita confirmación a su remitente, el conde de Gondomar, de que ha recibido también la nueva cifra:

> Lo que ahora ocurre es aver reçivido entre otros despachos de su Magd. la nueva cifra con orden que, antes de usar della, sepa V.S. y de todos los que de ordinario la tienen, si a llegado a su poder (II/2169, doc. 22).

Como ejemplo de notificación oficial de la entrada en vigor de una nueva cifra, se muestra la misiva que Juan de Ciriza, secretario de Estado, envía en 1618 a don Diego, que añade, además, advertencias sobre la vulnerabilidad de la precedente, señala el modo en el que recibirá la nueva y el protocolo a seguir antes de empezar a «corresponder» con ella:

> Por aver tiempo que se usa de la cifra general en que al presente se escribe y indicios que obligan a mudarla se ha hecho de nuevo la que va con esta. Valdreysos della para los partes y de la misma manera que de la que havéys tenido hasta agora, y avisadme luego del recibo y si la dicha cifra llega a vuestras manos cerrada y con las señas que os advertirá el secretario Juan de Ciriça, enviándole la cubierta para satisfacción de que en el camino no se ha tocado a ella, y también avisaréys a mis ministros... para que tengan entendido que está en vuestro poder la dicha nueba cifra y hecho esto y no antes os corresponderéis en ella conmigo y con ellos. (II/2541, fol. 14r).

De 31 de marzo de ese año de 1618, se conserva la carta que acompaña la propia cifra, y que describe con precisión el sistema de protección para garantizar la confidencialidad de la entrega, también firmada por Ciriza:

> Su Majestad ha mandado que se mude la cifra general que hasta agora se ha tenido y que en su lugar se husse de aquí adelante la que va con este despacho, debajo de dos cubiertas, la primera sellada con tres sellos míos con lacre, que son como el que va a

la margen de esta carta, y la otra cubierta va cerrada con un sello de Su Majestad, también con lacre, y el sobreescrito diçe: papel para guardar rubricado de mi mano. Avisolo a V.S. en conformidad de lo que contiene la carta de Su Majestad, para que se execute lo que en ella se apunta. (II/2174, doc. 18).

Respecto a la remisión de las cubiertas al remitente para verificar la integridad del envío, de acuerdo con el protocolo de seguridad, se trae a colación un testimonio de noviembre de 1623. Su responsable es Carlos Coloma, sucesor del conde de Gondomar en la embajada de Inglaterra:

Dos cartas me trujo Rivas de V.M. con las buenas nuevas de su salud, que yo deseava y desearé siempre. La una remitiéndome la nueva cifra, que llegó sana y salva, cuyas cubiertas ban aquí como V.M. me lo manda… (II/2590, fol. 43r).

En los mismos términos se expresa Pedro de Arce, secretario ya de Felipe IV, en su envío de una nueva cifra en julio de 1640, esta vez a Antonio Sarmiento de Acuña, hijo de don Diego, conde de Gondomar (II/2208, doc. 46). Aclara, a mayores, que «convendrá también que V.S. avisse a los demás ministros de Italia, Flandes, Alemania y Inglaterra como está en poder de V.S. esta nueva cifra". Y solo cuando se haya efectuado esta comunicación podrá «corresponderse» con la nueva cifra.

El arco cronológico de esta colección criptográfica se extiende desde 1568 hasta 1642. De la primera fecha se conservan tan solo dos cartas dirigidas al duque de Alba por Guerau Espés en 1568, evidentemente ajenas a la biografía del conde de Gondomar, pero custodiadas en su archivo (II/2196, docs. 145, 148). En el otro extremo, 1639 y 1642, se encuentran las cartas dirigidas a Antonio Sarmiento de Acuña, primogénito de don Diego, que asumiría, al igual que su padre, un papel importante en la diplomacia española en distintos territorios de la Monarquía, tales como Italia, Flandes o el Franco Condado.

Sin embargo, el núcleo principal de las cartas en cifra del fondo Gondomar está formado por dos bloques que, cronológica y temáticamente, se corresponden con la primera y la segunda embajada del conde de Gondomar en Inglaterra. Los temas abordados en las cartas cifradas circunscritas a esos dos periodos están siendo objeto de estudio por parte de la Real Biblioteca y se espera dar a conocer en breve los resultados.

Para finalizar, y a modo de avance del estudio mencionado, se ofrecen a continuación dos testimonios de uno de los temas, tal vez el más predecible, correspondiente a la segunda embajada, que se desarrolla entre los años de 1620-1623: las negociaciones para el fallido intento de matrimonio de María Ana de Austria, hija menor de Felipe III, con Carlos, hijo y heredero de Jacobo I, rey de Inglaterra y Escocia. Por las consecuencias que se derivarían de este enlace para los destinos de ambas monarquías y por los intereses contrarios de Francia, es fundamental garantizar la confidencialidad de la negociación a través la comunicación cifrada.

El primer testimonio, datado en 1619, procedente del dominico Diego de la Fuente, confesor de Gondomar, refleja la necesidad de la cifra para proteger la información sensible sobre esta negociación y exponer su preocupación por las informaciones que por diversas vías le están llegando a Jacobo I, adversas a la concertación del matrimonio:

Quiero decir a V.S., en carta a parte y en cifra, el daño que han hecho algunos papeles que han llegado a manos de este rey [Jacobo I] de personas que están en España, en Madrid, en que dicen que tienen certeça de que al rey nuestro señor no le pasa por pensamiento concluir el casamiento con este príncipe sino en Alemania, que se verá bien presto que es así. He sabido esto de buena parte y bien cierto y que algunos papeles (que an sido muchos los que ha visto este rey y todos conformes) son de religiosos y de otras personas de quien cierto cavallero muestra hacer mucha confianza y que el entender esto el rey, me dicen, le ha metido en desesperación (II/551, fol. 103v).

El asunto es controvertido y no parece conveniente que el rey inglés desconfíe del propósito firme del español para llevar a cabo el casamiento. En este segundo testimonio, en cifra y dirigido al conde de Gondomar, se comprueba que las exigencias que debe aceptar el rey inglés, al menos en lo tocante a religión, son lo suficientemente severas para que nada estorbe la negociación. Bajo el encabezamiento «Lo que se ha de dezir al señor embaxador de Inglaterra y pedir respuesta», se enumeran doce condiciones, entre las que constan, al margen de otras, la educación católica de los futuros infantes, su bautizo según el rito de la iglesia romana, la necesidad de que todos los miembros de la casa que lleve la infanta sean católicos, incluidos los criados de los criados y las amas de cría, o que cuenten con una iglesia pública para la administración de los sacramentos. Todo ello al margen de «la tolerancia de nuestra religión en Inglaterra, por ser cosa ya ofrezida».

En definitiva, la correspondencia del embajador de Felipe III en Inglaterra brinda el contexto idóneo para la práctica criptográfica, y su examen permite extraer datos suficientes para ilustrar los aspectos puramente técnicos del proceso de cifrado, así como seguir las pautas del protocolo del cambio y remisión de las nuevas cifras, y el análisis de la información crítica objeto de este tipo de comunicación.