



CONSTRUCCIÓN, USO Y DESCIFRADO DE LOS LENGUAJES SECRETOS EN EL SIGLO XVI*

CONSTRUCTION, USE AND DECIPHERMENT
OF SECRET LANGUAGES IN THE 16th CENTURY

Júlia Benavent Benavent

Departament de Filologia Francesa i Italiana

Universitat de València

València (España)

Julia.Benavent@uv.es

<https://orcid.org/0000-0003-3809-6039>

Recepción: 21/05/2025 – Aceptación: 21/07/2025

Resumen

En este artículo se aborda la construcción, uso y descifrado de la correspondencia del siglo XVI en Europa. La necesidad de proteger la comunicación impulsó el desarrollo de los sistemas de encriptación ante los conflictos políticos, religiosos y bélicos. La interceptación de las cartas cifradas era temida por los monarcas y gobernantes, que debían cambiar apresuradamente el cifrario para evitar que la información fuera conocida por lectores no deseados. Los testimonios estudiados, en lengua española, pertenecen a los fondos del Archivo General de Simancas. El objetivo es conocer cómo se construye un lenguaje artificial, convenido entre pocos usuarios. La metodología agrupa la edición de textos y las técnicas de la criptografía histórica. Los resultados son interesantes para la Filología, la Historia y la Criptografía Histórica.

Palabras clave: Siglo XVI, criptografía, lenguaje cifrado, Europa

* Esta investigación es posible gracias al proyecto *Los códigos lingüísticos secretos de las mujeres de la Casa de Austria en tiempos de Carlos V.* (PID2021-126189NB-I00), dirigido por Júlia Benavent y María José Bertomeu. Universitat de València.

Abstract

This article addresses the construction, use and decipherment of 16th century correspondence in Europe. The need to protect communication drove the development of encryption systems in the face of political, religious and war conflicts. The interception of coded letters was feared by monarchs and rulers, who had to hastily change the cipher to prevent the information from becoming known to unwanted readers. The testimonies studied, in Spanish, belong to the funds of the General Archive of Simancas. The objective of the study is to know how an artificial language, agreed upon among a few users, is constructed. The methodology brings together text editing and the techniques of historical cryptography. The results are interesting for Philology, History and Historical Cryptography.

Keywords: 16th century, cryptography, cyphered language, Europe

PRESENTACIÓN

Los primeros testimonios de documentación cifrada en Europa se registran en el siglo x y en el siglo xii, y tras un largo periodo lagunar, retoma su fuerza en el siglo xv, pero se extiende de forma generalizada en el siglo xvi. En los archivos es muy fácil hallar documentos cifrados entre los fondos del siglo xvi. No es fácil dar una datación, ni siquiera aproximada del origen de la criptografía histórica. Ciertamente no pudo surgir de la nada, y es difícil la reconstrucción de los primeros pasos por su carácter aislado, los innumerables intervalos de interrupciones y las reapariciones sin conexión hasta que podemos hablar de un sistema. Se ha podido observar que en los inicios la escritura alfábética fue sustituida por los dígitos como medio más sencillo de cifrado. Al menos así se constata en los primeros testimonios italianos que pudieron tener un origen común oriental o griego (Meister, 1906), sin que se pueda afirmar con rotundidad ni su ascendencia ni su difusión. En dos códices, el Bodl. Barocc. 50 de la Bodleian Library de Oxford y el Laurentianus Badia 53 de 1331, se han podido ver rastros, pero no con la claridad suficiente. Se podría interpretar que ambos conservan restos de un uso más extenso.

Es indudable que en Italia el uso de la escritura cifrada está unida a la actividad de la Curia, y es anterior a la del resto de los Estados italianos, pero tampoco podemos decir cuándo tuvo su origen, aunque se sospecha que esta actividad no era regular ni habitual. Es posible que los primeros textos cifrados se escribieran en alguna circunstancia muy singular, cuando se requería una protección mayor por algún grave asunto.

Las primeras referencias son las llamadas *litterae formatae*, que se remontan al obispo Ático de Constantinopla y el Concilio de Nicea. El origen de las *litterae formatae* sería la *tessera hospitalis*, una acreditación de los cristianos para ser acogidos y hospedados en lugares donde no eran conocidos. La *tessera hospitalis* de los sacerdotes cristianos eran las *litterae formatae*. Otro rasgo podría ser la práctica retórica de usar imágenes y símiles, como forma de comunicación secreta, solo comprensible para quien conociera la clave. El método más sencillo es cambiar el nombre de personas y lugares.

De 1326 o 1327 es el cifrario más antiguo hallado en los archivos de los papas, usado en las batallas de güelfos y guibelinos entre Orvieto y Viterbo y por la codificación de los eclesiásticos es de suponer que era un sistema de cifra que pertenecía a la Curia.

El primitivo sistema de listas de sustitución de nombres y palabras recibe el nombre de nomenclátor. Con el fin de dotar al texto de una mayor dificultad, el listado de palabras simulaba que se dirigía a una congregación, por lo que el mensaje parecía referirse a un asunto de monasterios o eclesiástico.

El nomenclátor no tiene mucha capacidad de desarrollo, por lo que hubo de buscar otros sistemas, sin renunciar por completo a él.

Los testimonios, dispersos, pueden encontrarse en el siglo VI a. C., cuando se empleaba una sustitución de letras en los mensajes del emperador Octaviano. En las biografías de César y Augusto. En la actualidad el sistema de cifrar mediante la sustitución de una letra por otra, se llama “cifrado César”. Suetonio lo describe de la siguiente manera:

Quotiens autem per notas scribit, B pro A, C pro B ac deinceps eadem ratione sequentis litteras ponit; pro X autem duplex A Suetonio (*De vita Caesarum libri VIII*) Sobre Augusto, sección LXXXVIII.

Más tarde Teofilacto de Frascati, creado papa en 1033, escribía su nombre transponiendo las vocales por la consonante inmediatamente anterior o posterior: Así Theofilactus se convertía en Thfpfklbctxs. En este caso la transposición afecta solo a las vocales, pero sigue siendo alfabetico. Podría suceder, como también se ve en testimonios antiguos, que las vocales fueran sustituidas por la variación de las líneas de H.



La escritura se cifra mediante varios sistemas criptográficos, que se valen de métodos distintos. El más común es el llamado de sustitución, que consiste en representar cada letra del alfabeto con uno o más signos. Pero hay otros sistemas, como el de transposición, que consiste en alterar el orden de las letras, de las sílabas o de las palabras para formar anagramas. Puede ser más o menos complejo, según la dificultad que se quiera dar a la codificación. Hay otro sistema, que consiste en ocultar la información, como la tinta invisible, el tatuaje sobre el cuero cabelludo, oculto bajo el cabello, las palomas mensajeras, ocultar los mensajes en el interior de la fruta, en los zapatos, etc.

Los signos no alfabéticos y no numéricos se llaman esteganográficos. La definición sería: Técnica criptográfica que consiste en sustituir las letras de un texto por otros signos convencionales distintos de letras o números (Galende Díaz, 1995; 2006).

Fundamentalmente, esos son los tres modos más empleados: alfabético, numérico y esteganográfico. En el siglo XVI solían combinarse los tres en sistemas mixtos.

De finales del siglo XIV son los testimonios de los cifrados del epistolario de Petrus de Gratia, arzobispo de Nápoles. Para representar las vocales usa unos signos engañosos que consisten en modificar las letras con una diéresis, o un punto o una tilde, es decir, un elemento modificador. Leon Battista Alberti los llama signos *otiosos* o *nihil importantes*. El objetivo era engañar al lector no deseado, pues carecían de valor y se intercalaban al azar. El arzobispo los colocaba detrás de cada letra, o detrás de dos o tres caprichosamente, de forma aleatoria. Este epistolario del arzobispo también añadía otro rasgo nuevo, cifraba las consonantes más usadas en latín: *l, m, n, r, s*.

Las vocales siempre han sido las letras más protegidas en los cifrarios, ya que su aparición frecuente en un texto es una entrada para la decodificación y la descriptación. Veamos ahora un ejemplo de transposición:

Un secreto es tu debilidad.

Ahora escribimos en dos líneas las letras que la componen, alternando cada letra en una línea:

U s c e o e t d b l d
N e r t e s u e i i a

Y la frase “Un secreto es tu debilidad” queda transformada en:

U s c e o e t d b l d d n e r t e s u e i i a

Conocida la clave, se decodificaría fácilmente.

Hemos visto anteriormente un caso de cifrado por transposición. Veamos otro sistema de cifrado, llamado nomenclator o por sustitución, tomando la *m* como partida:

A b c d e f g h i l m n o p q r s t u v x y z
O p q r s t u v x y z m l i h g f e d c b a n

O totalmente aleatorio:

Z t b x a p s l m f c q n o e r i p u y g

Observemos que la primera convención es acordar cuántas serán las letras del alfabeto. En el ejemplo anterior faltan los grafemas *j*, *k*, *ñ*. Las letras *y*, *i*, *j* pueden compartir el mismo signo, así como las *u/v* o *b/v*.

En el opúsculo *Opera nova la quale insegnna scrivere e leggere invintisette modi di zifere et per homini excellenti desiosi di virtù* (*Opera nova*, 1546) se ofrecían hasta 27 modos de cifrar por sustitución. En la primera se decía que se había de sacar del alfabeto todas las vocales y colocarlas al final; se dejaba fuera la *k* y se usaría la *b* por la *a*:

A b c d e f g h i l m n o p q r s t u
b c d e f g h l m n q r s t a e i o u

LOS LENGUAJES CIFRADOS EN EL SIGLO XVI BAJO LA MONARQUÍA DE LOS AUSTRIAS

A finales del siglo xv, el uso de los lenguajes cifrados era común en Europa. Conocemos uno de los cifrarios de mayor vigencia durante el reinado de los Reyes Católicos, el de Rodrigo González de la Puebla, el llamado doctor Puebla. En el Archivo General de Simancas (Estado, Tratados con Inglaterra, Leg. 2, doc. 1) se conserva la clave de González de la Puebla, compuesta de 2.400 palabras. La correspondencia cifrada entre los reyes y las legaciones diplomáticas es muy abundante. El problema de los cifrarios extensos era que, al ser interceptados, se

necesitaba mucho tiempo para ser sustituidos y recompuestos de nuevo (Alcocer Martín, 1934, pp. 336-340 y 603-676). Poco a poco, los cifrarios fueron simplificándose.

En tiempos de Carlos V, el uso de los lenguajes cifrados creció y se extendió a todas las embajadas, pero la estructura cambió notablemente respecto de la que tenían los cifrarios de los Reyes Católicos. Cuando una carta cifrada era interceptada, la clave de cifra era sustituida inmediatamente por otra. A veces la impresión visual es que se trata de la misma, pero en realidad los signos han cambiado de significado.

El monarca enviaba la clave a los gobernadores, virreyes, regentes, embajadores y familiares para comunicarse con él y entre sí. La comunicación entre los embajadores era exigida para contrastar los avisos que se recibían: Si llegaban avisos o noticias sobre un hecho, los embajadores intercambiaban la información para asegurarse de que los distintos agentes que tenían a su servicio las corroboraban. Esas cifras compartidas eran llamadas generales. Si la clave era enviada para el uso de dos o tres personas, la cifra era considerada particular.

La minuta de la carta que se dictaba al secretario llevaba la indicación de qué partes tenían que ser cifradas, de lo que se ocupaba el secretario de cifra. Cuando la carta era recibida en su lugar de destino, el secretario de cifra que compartía la clave descifraba el texto que, según la extensión, podía ser de tres maneras: 1. El descifrado aparece entre líneas, cada letra sobre el signo que la cifra. 2. El descifrado se escribía en los márgenes izquierdo, superior e inferior, si era necesario. 3. Si el texto cifrado de la carta era íntegro o muy extenso, el descifrado se adjuntaba en un papel adjunto, bajo el epígrafe “claro”.

Hay textos íntegramente cifrados, cuyo contenido desconocemos. La mayoría de ellos llevan adjunto el claro, aunque no siempre es completo.

Los secretarios de los monarcas y dirigentes eran personas instruidas que, en algunas ocasiones, gustaron de debatir sobre la naturaleza de las cifras y escribieron algunos tratados que merecen nuestra atención.

LOS TRATADOS DE CIFRA Y LA COMPOSICIÓN DE UN CIFRARIO

En el siglo XVI no había tema, cuestión o debate que no contara con la publicación de un libro sobre su historia, un análisis erudito desde la Antigüedad, o un diálogo a través del que, mediante representantes de pensamientos antagónicos, se arrojara luz sobre él. Hay que tener presente que los conocimientos sobre argumentos nuevos eran también muy apreciados, y que la imprenta daba espacio

a todos ellos. Los lenguajes cifrados se pusieron de moda y fueron usados por amplios sectores de la sociedad, porque eran útiles en algunas circunstancias o se divertían con ellos.

Hay una serie de tratados de cifra que son un referente en el mundo de la criptología. Uno de los tratados más importantes es el de Leone Battista Alberti, destacado arquitecto (1404-1472). La obra *De componendis cifris* fue escrita alrededor de 1466. Empezaba con una alabanza al arte de la imprenta e introducía a continuación un debate sobre el uso de las letras en las cifras secretas. Proponía un sistema indescifrable basado en dos ruedas sobreuestas, una fija y la otra móvil (Alberti, 1906). El interés por el sistema de cifras era compartido por Luca Pacioli, huésped suyo. De esta obra, cuyos testimonios se hallan en la Archivo Apostolico Vaticano (*Varia Politica LXXX*, ff. 173-181), Biblioteca Apostolica Vaticana (*Chigi M II 49*, ff. 9-34) y en Venecia, Archivio di Stato (*Trattati in cifra*, busta VI, n° 1), Alois Meister cuidó una edición crítica que publicó en 1906 (Meister, 1906, pp. 125-141). La herramienta por la que Leon Battista Alberti es conocido en la criptografía es el conocido como Discos de Alberti, un cifrario de sustitución.

El disco de Alberti era dos en realidad; uno de ellos era fijo, con 24 casillas. En las primeras 20 se escriben las letras en mayúscula y en orden alfabetico (quedan excluidas la J, H, K, Y, W. En las restantes 4 casillas, se escriben los números 1, 2, 3, y 4.

El otro disco, interno, es móvil. Consta también de 24 casillas, donde se escriben 24 letras en minúscula, desordenadas, que son: b, a, c, e, g, k, l, n, p, r, t, v, z, &c, x, y, s, o, m, q, i, h, f, d.

El usuario de este modo de cifrar debía elegir una letra clave. Para cifrar había que mover el disco interno, situándolo en la letra clave. Al acabar de cifrar la primera palabra, se daba un giro de nuevo al disco interno para cambiar el alfabeto. Así, cada palabra tenía un alfabeto propio. Las que correspondían a los números no se usaban.

En 1518 se publicó el primer libro de criptografía, *Polygraphiae libri sex*, en alemán por Johannes Trithemius. El método era de sustitución.

Otro tratado de cifra es de Fedele Piccolomini, *Di una nuova inventione di cifra dell'eccellente messer Fedeli Piccolhomini*, impreso en Pesaro en 1560.

Veamos las recomendaciones que ofrecía en su breve tratado:

Con un solo caratere significar diverse lettere
 Usar carateri di niun significato
 Usar carateri per parte di voce o di sentenza

Usar diversi carateri e non naturali
 Usar più di tre alfabeti diversi in una cifra
 Non si obligar alla consequentia nelli alfabeti che usa
 Tralasciar l'una delle lettere doppie o per le due un solo caratere porre
 Sprezzar l'ortografia
 Con più carateri insieme significare una sola lettera
 Non separare le parole né usare gli spazi in bianco (Piccolomini, 1560)

Giovanni Battista Porta es autor de un tratado en latín, *De furtivis literarum notis vulgo de Ziferis, libri IIII* (Porta, 1563). Giovanni Battista Bellaso publicó un tratado breve en 1553, reimpresso en 1555 y en 1564, titulado *La cifra nuovamente da lui medesimo ridotta a grandissima brevità e perfettione*, en Venecia. En 1555 publicó *Nuovi e singolari modi di cifrare* en la tipografía de Giacomo Britannico en Brescia. Y en 1564, *Il vero modo di scrivere in cifra con facilità, prestezza et securezza di misser Giovan Battista Bellaso gentil 'huomo bresciano. Con le sue singolarissime qualità et novi precetti et regole, da esso nella bellissima et importantissima arte di cifrar ritrovate et in luce poste*, también en Brescia. Propuso muchos modos de cifrar, basados en alfabetos construidos a partir de un verso, como por ejemplo el *incipit* de la *Eneida*:

Arma virumque cano, Troiae qui primus ab oris

Y proponía los siguientes pasos:

1. Se sacan las consonantes del verso de Virgilio, sin tener en cuenta las duplicadas:

R M Q C N T P S B

2. A continuación se escriben las consonantes que faltan del alfabeto en orden

D F G H L X Y Z

3. Se escriben las vocales del verso de Virgilio, sin tener en cuenta las repetidas:

AUIEO

4. Luego se escribe, siguiendo el orden, una vocal cada tres consonantes:

R M Q A C N T U P S B I D F G E H L X O Y Z

5. A continuación se separan de la anterior serie las 11 primeras letras en vertical y se construye un alfabeto dividido en dos líneas y asociado a una referencia de palabras mayúsculas: en vertical con las consonantes del *incipit* de la Eneida más las vocales en este orden: AUIEO; la siguiente serie son en grupos de dos las consonantes no presentes en el *incipit* virgiliano. De esta manera se han formado 11 alfabetos. Para descifrar el usuario se vale de las claves.

R A	r m q a c n t u p s b
	i d f g e h l x o y z
M U	r m q a c n t u p s b
	z i d f g e h l x o y
Q I	r m q a c n t u p s b
	y z i d f g e h l x o
C E	r m q a c n t u p s b
	o y z i d f g e h l x
N O	r m q a c n t u p s b
	x o y z i d f g e h l
T P	r m q a c n t u p s b
	l x o y z i d f g e h
S B	r m q a c n t u p s b
	b l x o y z i d f g e
D F	r m q a c n t u p s b
	e h l x o y z i d f g
G H	r m q a c n t u p s b
	g e b l x o y z i d f
L X	r m q a c n t u p s b
	f g e b l x o y z i d
Y Z	r m q a e n t u p s b
	d f g e b l x o y z i

Las claves de uso eran:

L'armata turca
Chiare fresche

En 1565, Blaise de Vignère ideó un modo de cifrar, que era una versión perfeccionada del cifrario César.

En la Cancillería vaticana, los secretarios Giovan Battista Argenti y su sobrino Matteo Argenti eran responsables del cifrado de la Cancillería romana. Las noticias biográficas de ambos se hallan en la Biblioteca Apostólica Vaticana (Chigi M II 48). Matteo Argenti dejó manuscritos dos tratados para uso de los secretarios que habían de continuar su labor:

1. *Trattato che insegnă di formare cifre di varie sorti che s'appartiene a secretarii et a gran signori.* (BAV, Chigi M II, 49, f. 149; BAV Cod. Vat. Lat. 6532, ff. 142-178, Biblioteca Barberini LVII 67, f. 63; Biblioteca Casanatense X. IV. 46, nº 2084, ff. 1-35)
2. *Discorso et considerationi et congettture da levar senza contracifra et altri particolari cuncti a tal professione.* (BAV, Chigi M II 48, ff. 136-142)

En el fondo Chigi se conservan también otros testimonios muy interesantes para el estudio de las cifras de los Argenti, como cifras usadas (Chigi M II 49), los últimos cifrarios del papado de Gregorio XIII (Chigi M II 50) (Hinojosa, 1896).

Los tratados de cifra impresos estaban muy alejados de la práctica diaria de la escritura cifrada en las cancillerías, las embajadas y la actividad diaria de los secretarios y agentes. Los cifrarios secretos de las cancillerías, no impresos, eran compuestos siguiendo las reglas de la prudencia y de la variedad, proponían un alfabeto que pudiera ser utilizado con agilidad por hablantes de varias lenguas y eran sustituidos inmediatamente, si eran interceptados. El debate renacentista participó del interés por las escrituras cifradas, reflexionó sobre la composición de los alfabetos aleatorios, pero sus tratados no eran un manual manejable para un secretario de cifras. Hemos podido comprobar cómo la erudición humanista penetraba en los tratados con el *incipit* de la *Eneida* de Virgilio y el sintagma *Chiare fresche* de la canción CXXVI del *Rerum vulgarium fragmenta* de Francesco Petrarca

Venecia adquirió en la Europa del siglo XVI la fama de albergar a los mejores descifradores en la ciudad, pero los casos estudiados en las cartas que fueron descipladas constatan que la clave fue conocida por la traición de algún secretario de la embajada, probablemente disgustado por alguna razón. Uno de los episodios de interceptación de cartas cifradas más famoso ocurrió en 1556. Se dijo entonces que la carta había sido enviada a Venecia para ser descifrada, como así pasó. El códice Ottoboniano latino 2348 de la Biblioteca Apostólica Vaticana desvela lo que había ocurrido. Un secretario de la embajada de Felipe II en Venecia entregó la clave a los partidarios del papa Paolo IV. La depositó en el tronco de un árbol y de allí fue tomada por un agente del obispo de Toulon, Antonio Trivulzio, nuncio

en Venecia. A Girolamo Ruscelli se le entregó una buena cantidad de dinero para que afirmara que la había descifrado él, por lo que sumó a su fama de polígrafo la de experto perlustrador, por lo que nunca se supo quién había sido (Benavent, 2024).

El uso de los lenguajes cifrados está ligado a la actividad de los espías y agentes de los monarcas y a los secretos de sus estrategias.

LAS PARTES DE UN CIFRARIO

Las prácticas de cifrados en la Cancillería imperial eran frecuentes y en varias lenguas. Se mandaban textos cifrados desde los Países Bajos a Inglaterra, a España, a Italia, a Turquía y viceversa. La actividad era muy dinámica como podemos ver por las varias manos de los secretarios que usaban el mismo cifrario en distintas partes de Europa. La característica de estos lenguajes está marcada por ser una comunicación secreta, que excluye a destinatarios no deseados, por lo que la tarea de usar un cifrario vigente se limitaba a usuarios de absoluta confianza. Informadores a sueldo, agentes infiltrados y mercenarios eran también muy habituales. La información era muy apreciada en todas las cortes europeas y, sobre todo, muy bien recompensada.

La acción de transformar una lengua en otro lenguaje cifrado se llama cifrar o codificar. La tarea de devolver el texto cifrado a la lengua de la que partió se denomina describir o decodificar, en el caso de que la clave sea conocida. Si no es así, si se ignora la clave para descifrar, los especialistas denominan esta acción descriptar o perlustrar.

La sección fundamental de un cifrario es el abecedario, que comprende un número determinado de letras, según la lengua que se encripta. El alfabeto español consta de 27, pero no siempre ha sido así. En el cifrario del siglo xv, usado por los Reyes Católicos y el doctor Puebla, el número de letras era 22, de las que quedaban excluidas *j*, *k*, *ll*, *ñ*. La *w* no aparece en ningún cifrario. La *ll* era considerada una letra doble, como la *rr*, *ss*. La *ñ* se escribía como *nn*, cuya abreviatura, una sola *n* con una vírgula encima, dio lugar a la *ñ*. Los abecedarios de los cifrarios estudiados hasta el momento constan de 21 letras, por la exclusión de la *j* y la *ñ* que, sin embargo, aparecen aisladamente, fuera del abecedario, con un signo propio. La *ñ* aparece en algunos cifrarios, no todos. La *j* aparece, sacada del abecedario, entre los años 1530 y 1539; es decir, la razón por la que no aparece en todas las tablas de cifra es probablemente que el cifrario tenía que ser empleado por hablantes de lenguas distintas. En los mencionados se le asignaba un código

y, donde no consta, se usaba la *i* en su lugar o la *x*. Podemos hallar la palabra *señores* cifrada con una *n*.

A cada letra del alfabeto se asocia uno o más signos. Las vocales suelen tener siempre más de uno por ser las letras más repetidas. Se asignaba a cada consonante uno o dos signos. En el cifrario del doctor Puebla, las consonantes cuentan con cuatro signos diferentes para cada una; las vocales tienen cinco.

En los cifrarios que se han conservado completos hay dos para cada consonante y tres para las vocales. El motivo es muy fácil de comprender: se recomendaba a los secretarios de cifra que usaran indistintamente los signos propuestos para cada letra, con el fin de dificultar la perlustración del texto si era interceptado. La experiencia en el descifrado nos ha demostrado que era muy habitual que se usaran siempre los mismos signos para las letras, por comodidad probablemente.

Los signos del cifrado para el alfabeto suelen ser alfabéticos, numéricos, esteganográficos o mixtos.

Como hemos apuntado anteriormente, algunas letras eran cifradas separadamente del alfabeto, como la *ñ* y la *j*. Las letras dobles eran una categoría también separada del alfabeto por una razón sencilla: la repetición de dos signos iguales era una vía segura para romper la cifra que garantizaba la perlustración. Así pues, las letras dobles se cifran con un solo signo.

Con el fin de entorpecer la perlustración, se creaban signos nulos o *nihil importantes*, que se intercalaban entre los dotados de significado. Suelen asemejarse a los válidos, pero se modifican con algún punto, vírgula, número en exponente o cualquier otro elemento. También pueden constituir frases completas. Es frecuente hallar estos signos nulos en el principio y en el final de los textos cifrados.

Otra parte del cifrario era la formada por la codificación de las sílabas, bilíteras y triliteras. Por lo general la sílaba bilítera en los cifrarios imperiales está formada por la consonante + vocal. En los cifrarios del Vaticano el grupo de dos letras se realizaba al revés, vocal + consonante, por lo que era mucho más difícil la encriptación y la perlustración de un texto. En los cifrarios que hemos estudiado podemos observar que con mucha frecuencia se asocia un signo a la consonante que se repite en el silábico bilítero. Por ejemplo, si asignamos a la *b* un signo Φ , la sílaba *ba* será Φ , la *be* Φ , la *bi* Φ , *bo* Φ y *bu* Φ . Y lo mismo con el signo para la sílaba *c* + vocal. No es previsible, pero es una buena indicación para romper la cifra. Algunos cifrarios otorgan un signo para las sílabas triliteras: *fr* + vocal; *fl* + vocal; *gr* + vocal; *gl* + vocal; *pr* + vocal; *pl* + vocal; *tr* + vocal.

La tercera sección de un cifrario, no presente en todos, es el vocabulario de conceptos, un listado de las palabras o de los sintagmas más usados en la redacción de los textos, que reflejan el momento que justifica el encriptado del texto,

bien sea por los personajes mencionados, los movimientos bélicos o las acciones concretas que se desean encubrir. Entre los cifrarios completos conservados los términos del vocabulario oscilan entre los 74 y los 150, ordenados alfabéticamente y con lemas como *emperador, guerra, Perú, quant-, tant-*. Estos conceptos cifrados dificultan mucho la perlustración. El cifrario de los Reyes Católicos que compartían con el embajador doctor Puebla, el secretario Almazán y las infantas en el extranjero constaba de casi 700 términos.

Esta sección es más difícil de completar en los cifrarios reconstruidos, porque nunca se puede saber con seguridad si hemos tenido la suerte de identificarlos completamente. De hecho, entre unos 40 cifrarios reconstruidos que hemos estudiado, 19 no cuentan con vocabulario cifrado; los términos de los 21 restantes oscilan entre 2 y 39. La importancia de estos términos es fundamental para datarlos *ante quem* y *post quem*, cuando se encuentran entre los documentos de un legajo.

La última sección solo se halla en algunos de los cifrarios conservados. Se trata de las recomendaciones para el uso de la cifra:

Hase de escribir con cuidado, variando unas veces por los carateres que denotan las sílavas, otras veces por los números, que por eso se ponen dos órdenes y, para hacerlo más difícil, aunque sea más larga la escritura, se podrá escribir quando la cosa fuere de mucha importancia por entrabbas a dos líneas de la cifra, de suerte que sirvan por una sola de lo claro y para que se conozca al descifrar se ponga una B en la primera palabra.¹

A MODO DE CONCLUSIÓN

La criptografía era una práctica muy común para asegurar la comunicación y para ello se crearon sistemas de cifras que fueron muy usados desde la Antigüedad, aunque los testimonios que se han conservado no son suficientes para saber su composición, uso y vigencia. A partir de mediados del siglo xv los testimonios de escritura cifrada son cada vez más abundantes en los archivos. Sin embargo no es un campo de estudio extendido, por lo que no se ha explicado aún su complejidad que aúna conocimientos de Paleografía, Filología aplicadas a los hechos históricos y a la historia de la comunicación secreta y de la historia de los sistemas de inteligencia en Europa; es decir, encierran una reflexión interdisciplinar necesaria.

¹ Este fragmento pertenece a AGS Est. Leg. 1.1.1 doc. 44 y 49.

BIBLIOGRAFÍA

Manuscritos

Archivos

Simancas

- Archivo General de Simancas
Estado, Tratados con Inglaterra, Leg. 2, doc. 1
Estado, Leg. 1.1.1

Città del Vaticano

- Archivio Apostolico Vaticano
Varia Politica LXXX, ff.173-181

Venecia

- Archivio di Stato
Trattati in cifra, busta VI, nº 1

Bibliotecas

Città del Vaticano

- Biblioteca Apostolica Vaticana
Chigi M II 48, ff. 136-142
Chigi M II 49, ff.9-34
Chigi M II, 49, f. 149
Vat. Lat. 6532, ff. 142-178

Florencia

- Biblioteca Laurenziana
Laurentinus Badia 53

Roma

- Biblioteca Barberini LVII 67, f.63
Biblioteca Casanatense X.IV. 46, nº 2084, ff. 1-35

Reino Unido

- Oxford
Bodleian Library de Oxford
Bodl. Barocc. 50

Estudios

- Alberti, Leone Battista, 1906: "De componendis cifris (Der Chiffrentraktat des Leo Baptista Alberti)", en Alois Meister, *Die Geheimschrift im Dienste der Päpstlichen Kurie. Von ihren Anfängen bis zum Ende des XVI Jahrhunderts*. Paderborn, pp. 125-141.
- Alcocer Martín, Mariano, 1934-1935: "Criptografía española", en *Boletín de la Real Academia de la Historia*, nº CV y CVI.
- Benavent, Júlia, 2024: "Maestros de postas y cartas cifradas contra Paolo IV" en *Italia y España: una pasión intelectual*. Salamanca, pp. 849-864.
- Benavent, Júlia, 2025 (coord.), "La escritura secreta en la Europa del siglo xvi" *Estudios Románicos*, 34.
- Galende Díaz, Juan Carlos, 1995: *Criptografía. Historia de la escritura cifrada*, Madrid.
- , 2006: "Diplomacia cifrada hispánica durante el siglo xvi", *Revista Digital Universitaria*, 7 (7), pp. 1-9.
- , 1993: "La escritura cifrada en España". Actas del II Congreso de Jóvenes Historiadores y Geógrafos, Valencia, pp. 693-699.
- Hinojosa, Ricardo de, 1896: *Los despachos de la diplomacia pontificia en España*, Madrid.
- Kahn, David (1967): *The Codebreakers*, Mac-millan, Nueva York.
- Muñoz Benavent, María, 2025, "Estudio de un manual para descifrar textos españoles del siglo xvi". *Estudios Románicos*, 34.
- Meister, Alois, 1906: *Die Geheimschrift im Dienste der Päpstlichen Kurie. Von ihren Anfängen bis zum Ende des XVI Jahrhunderts*, Paderborn.
- Opera nova*, 1546: *Opera nova la quale inseagna scrivere e leggere invintisette modi di zifere et per homini excellenti desiosi di virtù*, Bressa.
- Parisi, Ivan, "La correspondencia cifrada entre el rey Fernando el Católico y el embajador Joan Escrivà de Romaní i Ram", *Pedralbes*, 24 (2024), pp. 55-116.
- Piccolomini, Fedele, 1560: *Di una nuova inventione di cifra dell'eccellente messer Fedele Fedeli Piccolhomini*, Pesaro.
- Porta, Giovanni Battista, 1563: *De furtivis literarum notis vulgo de Ziferis, libri III*, Nápoles.
- Sacco, Luigi (1925): *Manuale de Crittografia*. Roma.