Javier Marcos Rivas

LA CRIPTOGRAFIA Y LOS SERVICIOS SECRETOS DE FELIPE II

javiermarcos.ies@gmail.com

Colección: Clásicos mínimos
Fecha de Publicación: 15/09/2014
Número de páginas: 8
I.S.B.N. 978-84-690-5859-6

Archivo de la Frontera: Banco de recursos históricos.
Más documentos disponibles en www.archivodelafrontera.com

El *Archivo de la Frontera* es un proyecto del **Centro Europeo para la Difusión de las Ciencias Sociales (CEDCS)**, bajo la dirección del Dr. Emilio Sola, con la colaboración tecnológica de **Alma Comunicación Creativa.**

www.cedcs.org
info@cedcs.org
contacta@archivodelafrontera.com

www.miramistrabajos.com

LA CRIPTOGRAFIA
Y LOS SERVICIOS SECRETOS
DE FELIPE II

La obtención de información por parte de los espías no tendría ningún sentido si no se hubieran desarrollado, desde los orígenes de los servicios de inteligencia, una serie de procedimientos y técnicas encaminadas a asegurar el secreto de la correspondencia. De esta labor se ha encargado la criptografía.

La **criptografía** es la disciplina que estudia la escritura oculta, el arte de escribir con un lenguaje convenido mediante el uso de claves o cifras. Enseña, por tanto, a confeccionar cifrarios. La labor de transformar un mensaje cifrado en el texto original, si se conoce la clave, se denomina descifrar o decodificar, mientras que, si se ignora el código secreto, es más exacto hablar de perlustrar o descriptar. Su finalidad es ocultar a terceras personas el contenido de un texto que no les ha sido destinado o que, por su naturaleza secreta, solo pueden conocer los interesados. Es, por consiguiente, **el lenguaje de los espías**.

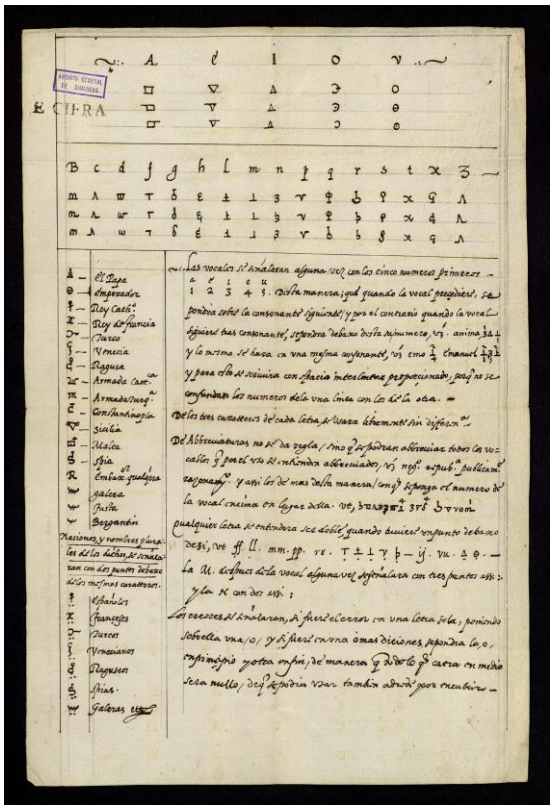
La criptografía es tan antigua como la escritura. De hecho, muchos especialistas superponen el estudio de las lenguas con el de la criptografía. Así, por ejemplo, un gran erudito como Champollion que descifró la Piedra Rosetta y nos legó el conocimiento de la escritura jeroglífica egipcia, se le considera un insigne criptoanalista. A lo largo de la historia se han creado diferentes **tipos de sistemas criptográficos** que a su vez han desarrollado infinidad de métodos.

El primer sistema es el de **sustitución**, inventado al final de la República romana, que consiste en reemplazar alguna letra del alfabeto por uno o varios signos convenidos de antemano por ambas partes. Este sistema comprende todos los métodos basados en sustituir letras, sílabas, palabras o frases de un texto por otras distintas, guarismos o signos, es decir, los elementos del escrito claro o normal son sustituidos por una representación distinta a la original. Este sistema puede ser simple o múltiple, si cada letra, signo o número es sustituida por una o varias letras, signos o números. De esta manera si la sustitución se hace por medio de letras se denomina literal, si por números, numérica y si es por signos, esteganográfica.

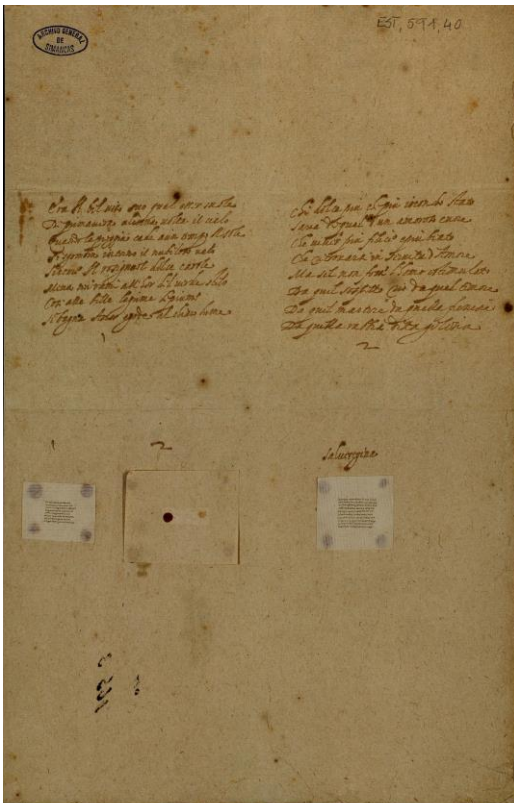
El sistema de **transposición**, de origen griego, consiste en colocar un fragmento cifrado en un lugar previamente conocido por el destinatario. Comprende todos los métodos que alteran el orden natural de letras, sílabas o palabras en un texto, trastocándolas o formando anagramas con ellas. También puede ser simple, si solo se produce una alteración o múltiple si se realiza un segundo cambio del texto ya modificado para dotar de mayor seguridad el cifrado de documentos.

El tercer sistema es el de **ocultación**, que incluye cualquier tipo de procedimiento en el que el remitente transmite las letras de forma oculta o disfrazada. Es el caso del método del esclavo, una práctica criptográfica muy poco recomendable, entre otras razones, por su lentitud, que consistía en afeitar la cabeza de un esclavo que ejercía las

funciones de mensajero y escribir el mensaje sobre su cuero cabelludo con caracteres endebles. Una vez crecido el pelo, era enviado al lugar de destino a cumplir su misión. Si conseguía llegar, se le afeitaba la cabeza por segunda vez y se leía el mensaje por la persona a la que iba dirigido. También pertenece a esta categoría el escribir mensajes en la piel, bajo la ropa, en los asedios a ciudades flamencas durante la guerra de los Países Bajos, como cuenta el militar y diplomático Bernardino de Mendoza en su obra *Teórica y práctica de la guerra.*



Cifra utilizada por el arzobispo de Ragusa. 1575. Ejemplo de sustitución triple esteganográfica. AGS Estado-1/66.



Ejemplo de sistema criptográfico de ocultación consistente en muestras de escritura microscópica realizadas por un italiano. AGS Estado-591/40.

Otro sistema criptográfico que suele estudiarse de forma independiente a la tipología anterior es el llamado método de los impresos que consiste en confeccionar un cifrado subrayando o marcando imperceptiblemente determinadas palabras o letras en un libro o en un documento determinado.

Aunque los mensajes cifrados surgieron con toda probabilidad de forma paralela a las primeras manifestaciones de la escritura, la evolución histórica de la criptografía se inicia en el siglo V a. C. en la guerra del Peloponeso entre Atenas y Esparta. A partir de este momento, las referencias griegas y romanas a códigos criptográficos, como han hecho constar autores como Polibio o Plutarco, son relativamente frecuentes. Este último describió el método del escítalo utilizado por el general Lisandro de Esparta que consiste en enviar un mensaje en una cinta con letras con una aparente falta de sentido.

Al ser enrollada la cinta en un rodillo de madera con unas características concretas, se podía leer el mensaje longitudinalmente.

Durante la Edad Media, hasta el siglo XIII no se tienen noticias fiables sobre la evolución de la criptografía, pero es probable que se utilizara en guerras y embajadas. Según David Kahn, uno de los mayores expertos en criptografía histórica y autor de "The codebreakers", uno de los documentos criptográficos más antiguos que se conoce y que se custodia en los Archivos Vaticanos es una pequeña lista de nombres con sus equivalencias en cifra elaborada a principios del siglo XIV y usada en el conflicto que enfrentó en Italia central a güelfos y gibelinos, dentro del enfrentamiento entre el Papado y el Imperio. Con frecuencia, los copistas de códices escondían sus nombres utilizando procedimientos criptográficos como anagramas, fuga de vocales o alterando letras de los mismos (Fusnular por Arnulfus, por ejemplo). También fueron frecuentes entre los criptólogos los alfabetos pictóricos. Uno de los más populares fue el "alfabeto zodiacal", en el que los signos astrológicos y sus correspondientes planetas tenían su equivalencia con las letras del abecedario.

La época moderna fue, sin duda, una auténtica "Edad de Oro de la criptografía", no solo porque surgieron figuras que se consideran los padres de la criptografía moderna como el monje benedictino alemán Johannes Heindelberg, conocido como Tritemio, León Battista Alberti o el napolitano Giovanni Battista Porta, sino porque se convirtió en un saber muy extendido en las cortes europeas, como conocimiento necesario para la correspondencia diplomática e incluso como entretenimiento.

Giovanni Battista Porta, el criptógrafo más famoso del Renacimiento.

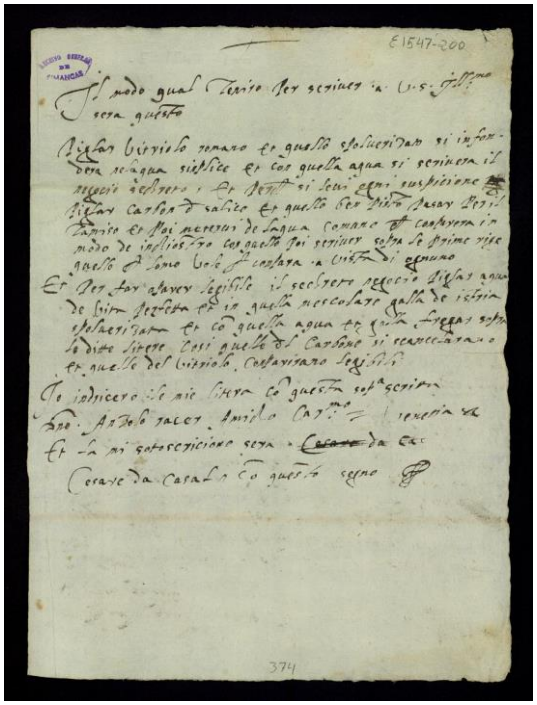
Disco para cifrar y descifrar de León Battista Alberti, famoso arquitecto y también importante criptógrafo.

La **organización de los servicios criptográficos de Felipe II** seguía, como es lógico, el mismo orden jerárquico que el resto del aparato de espionaje. Las decisiones sobre qué cifra utilizar y cómo hacerlo la tomaba la cúpula de los servicios secretos, es decir, el propio rey y el secretario de Estado. Existen pruebas documentales de que Felipe II llegó a descifrar personalmente y que secretarios de Estado como Antonio Pérez eran expertos criptógrafos, habilidad que, según Marañón, utilizó manipulando el contenido real de las cartas que D. Juan de Austria enviaba a su hermanastro el rey. Las cartas eran cifradas por el "secretario de la cifra" y se enviaban a su destinatario, representante de la monarquía en otros territorios del Imperio o en el exterior (virreyes,

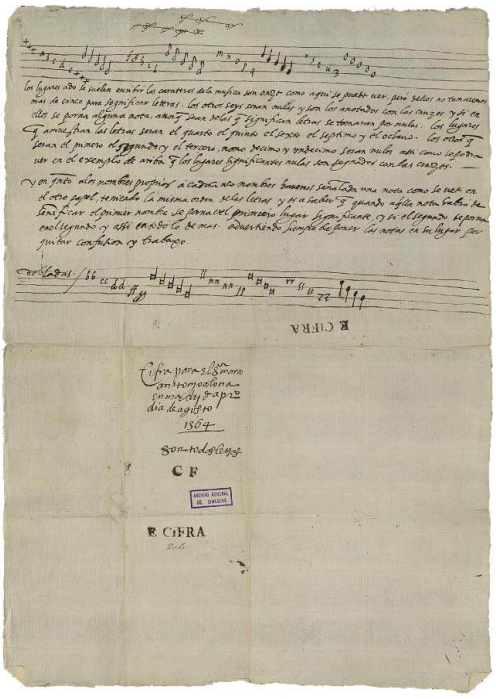
gobernadores generales y embajadores). Una vez en sus manos, los mensajes eran descifrados por el secretario, que era quien custodiaba la clave del código secreto.

Desde el punto de vista del destinatario, los servicios criptográficos de Felipe II contaban con dos grandes tipos de cifra.

La **cifra general** era el código que debía comunicar al rey y a la cúpula del espionaje con sus representantes en el exterior y éstos entre sí. Aunque las cambiantes circunstancias políticas y militares marcaron algunas diferencias en los destinatarios de la cifra general, ésta iba dirigida a los gobernadores generales de Flandes y Milán, virreyes de Nápoles y Sicilia, a los embajadores en Inglaterra, Francia, Roma, Génova, Venecia, Saboya y Corte Imperial en Praga y al Capitán General de las galeras del Mediterráneo, Juan Andrea Doria. Por razones de seguridad y de efectividad, se cambiaba cada cierto tiempo. Autores como Geoffrey Parker afirman que la cifra general se cambiaba cada cuatro o cinco años, lo que no coincide con la relación de cifras generales incluida por Devos en su obra sobre la cifra de Felipe II. Éstos y otros autores han intentado saber cuántas cifras generales estuvieron en vigor en los cuarenta y dos años de reinado de Felipe II y seguramente, son más de las mencionadas por ellos. Esta cuestión tiene, sin duda, una importancia relativa, lo realmente significativo es llegar a saber cuáles eran los criterios aplicados para efectuar estos cambios. Todo parece indicar que, sin excluir la periodicidad para salvaguardar la seguridad de las comunicaciones, se hacía antes de una gran empresa política o militar. La rebelión de Flandes, la batalla de Lepanto, el intento de invasión de Inglaterra o el inicio de las negociaciones que llevaron a la tregua hispano-turca empujaron a estos cambios sin someterse a una periodicidad determinada como el caso de la rebelión flamenca que en 1566 obligó a cuatro cambios de la cifra general en solo dos años.



Fórmula para elaborar tinta invisible. AGS Estado-1547/200.



Cifra particular de Marco Antonio Colonna a base de notas musicales. 1564. AGS. Estado-1/204.

La **cifra particular** cuya función era comunicarse el rey o el secretario de Estado con determinados personajes. También la tenían los virreyes y embajadores y solo se podía utilizar para comunicar noticias de especial gravedad y secreto, que no quedaría del todo protegido con un código compartido como la cifra general.

Durante mucho tiempo y debido al vacío historiográfico sobre el espionaje español en la Edad Moderna, historiadores extranjeros han dado una imagen muy pobre de la criptografía española incidiendo, sobre todo, en la debilidad de las cifras españolas y su facilidad para ser prelustradas. Así, en la lista de grandes descifradores del siglo XVI suelen aparecer personajes como Thomas Phelippes, descifrador inglés de Francis Walsingham, Francoise Viéte que trabajó para Enrique IV de Francia, el criptoanalista papal Mateo Argenti, Pietro Partenio y Agostino Armandi al servicio de los venecianos o el descifrador del líder de la revuelta flamenca Guillermo de Orange, Felipe Von Marnix…pero ninguno español. En la actualidad, las cosas han cambiado y conocemos algunos nombres de descifradores de los servicios secretos de Felipe II que, sin duda, estaban a la misma altura que sus homólogos europeos. Estos son algunos de los **principales criptoanalistas que trabajaron para los servicios de inteligencia de la Monarquía Hispánica** en la segunda mitad del siglo XVI y principios del XVII.

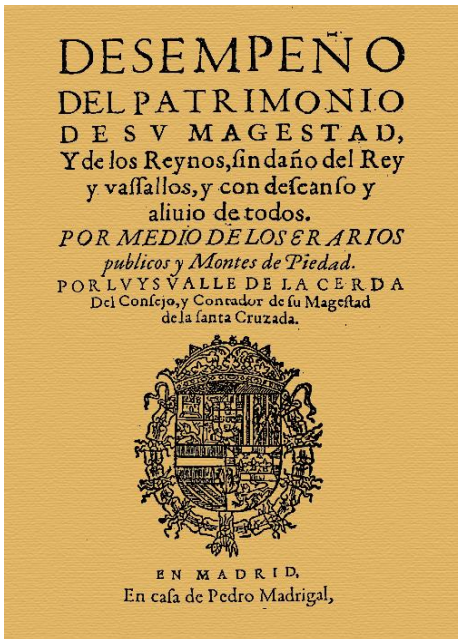
Felipe Von Marnix, descifrador de Guillermo de Orange.

Juan Vázquez de Zamora. Inició su carrera como descifrador del secretario de Estado Antonio Pérez. Viajó a Génova con Juan de Idiáquez cuando fue nombrado embajador en esta república. Tras la marcha de Idiáquez, permaneció en Génova, sin duda, uno de los "puntos calientes" del espionaje europeo y donde no le faltó trabajo como criptoanalista, llevando a cabo importantes servicios reconocidos por Idiáquez cuando accedió a la secretaría de Estado.

Gaspar de Soto empezó muy joven, a los catorce años, a familiarizarse con la criptografía en los escritorios de las secretarías de Estado y de Italia, con los secretarios Gaytán y Gabriel de Zayas, destacando por su labor en la invasión de Portugal.

Jerónimo González, descifrador del Duque de Alba en Flandes, cuyo secretario Francisco de Albornoz llegó a escribir de él que *"tiene tal habilidad para la cifra que las de S. M. tiene en la cabeza como el pater noster y las de estos herejes todas las ha sacado y tenemos la contracifra como si estuviéramos de acuerdo".*

Luis Valle de la Cerda fue, seguramente, uno de los mejores criptoanalistas españoles de los siglos XVI y XVII, aunque durante mucho tiempo esta actividad ha estado arrinconada por su faceta de arbitrista, autor de varios libros e introductor en España de los montes de piedad, siguiendo las ideas del flamenco Peter Van Oudegherste. Nacido en Cuenca hacia 1559, estudió en la universidad de Salamanca y pronto empezó su carrera como "secretario de cifras" en Italia y más tarde en Flandes llamado por el gobernador Alejandro Farnesio. Su fama de magnifico descifrador se fue acrecentando lo que le llevó a la corte, a la secretaría de Estado con Juan de Idiáquez. Regresó a Flandes y fue hecho prisionero de los ingleses, que no consiguieron averiguar su verdadera identidad, lo que le hubiese supuesto una muerte casi segura. De regreso a España, fue nombrado contador del consejo de Cruzada, pero siguió dedicándose a la criptografía hasta su muerte en 1606.



DESEMPEÑO
DEL PATRIMONIO
DE SV MAGESTAD,
Y de los Reynos, sin daño del Rey
y vassallos, y con descanso y
aliuio de todos.
POR MEDIO DE LOS ERARIOS
publicos y Montes de Piedad.
POR LVYS VALLE DE LA CERDA
Del Consejo, y Contador de su Magestad
de la santa Cruzada.

EN MADRID,
En casa de Pedro Madrigal,

Una de las obras de Luis Valle de la Cerda, más conocido como arbitrista que como criptógrafo.

Bernardino de Mendoza fue uno de los diplomáticos de Felipe II con más conocimiento e interés sobre criptografía.

La utilización de la escritura secreta no era garantía de inviolabilidad de la información. Los servicios secretos de Felipe II, al igual que sus homólogos europeos, tuvo que enfrentarse a **varios problemas derivados del uso de la criptografía.** El primero, relativamente frecuente era la falta de coordinación en el uso de códigos como

la cifra general. Esto es lo que le pasó al embajador en Praga Guillén de San Clemente que en 1590 dio la voz de alarma comunicando que la nueva cifra general, que acababa de entrar en uso, había sido descriptada por los franceses. Todo se debió a un error del embajador que confundió la cifra vieja por la nueva. La obsesión por la seguridad, por crear un código fácil de recordar pero a la vez muy difícil de prelustrar, preocupó a muchos ministros relacionados con el espionaje. Un ejemplo de esta inquietud compartida fue el envío de Bernardino de Mendoza a Juan de Idiáquez en 1587 de una nueva cifra que ahorraba tiempo al descifrar ya que no utilizaba rueda. Sin embargo, el mayor problema al que se enfrentaron los servicios de inteligencia de Felipe II, común al espionaje de todo los tiempos, fue el robo de códigos o la traición de algunos "funcionarios" que entregaron las cifras al enemigo. Se dieron, como es natural, varios casos. Uno relativamente conocido fue el robo de la cifra general por parte de un criado del embajador español en París Francés de Álava, Jean Fleurin, que fue detenido rápidamente. Otro, el de un tal Aguilón que entregó a los rebeldes flamencos una cifra española y huyó. Por último, el más controvertido y todavía sin aclarar fue la supuesta traición del oficial mayor de la secretaría de Estado de Gabriel de Zayas, Juan del Castillo, al que varios autores acusan de entregar información secreta y varias claves españolas a los flamencos a cambio de dinero. Según un historiador holandés P. Bor, esto permitió a Von Marnix descifrar durante diez años las cartas españolas interceptadas y afirma que Castillo fue ejecutado en 1581. Sin embargo, Luis Cabrera de Córdoba da una versión diametralmente opuesta. Según el cronista de Felipe II, la acusación contra Castillo era infundada y se debió a la denuncia de un enemigo personal. Estuvo encarcelado mientras se realizaba una investigación y al no poderse demostrar nada fue liberado, marchando a Nápoles junto al virrey duque de Osuna. Una vez muerto el prelado que le había denunciado, viajó a Flandes donde trabajó como contador hasta su muerte.