Revista Digital Universitaria
10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

ARTICULO

DIPLOMACIA CIFRADA HISPÁNICA DURANTE EL SIGLO XVI

Juan Carlos Galende Díaz
Doctor en Historia
jgalende@ghis.ucm.es

http://www.revista.unam.mx/vol.7/num7/art53/int53.htm

DIPLOMACIA CIFRADA HISPÁNICA DURANTE EL SIGLO XVI

Resumen

El reinado de Isabel y Fernando supone el inicio de una nueva etapa en el desarrollo de la criptografía hispánica. La sencillez, característica en la elaboración de los criptogramas durante el período medieval, dará paso a la complejidad, pues será fundamental, en ocasiones, mantener el secreto de los mensajes y de las comunicaciones en aras al éxito o fracaso de una negociación.

La intención del autor en este artículo es presentar una panorámica general de las técnicas y procedimientos de naturaleza cifrada empleados durante la centuria decimosexta en la conformación de la correspondencia diplomática.

Palabras clave: Criptografía, Documentación, Escritura, Edad Moderna, Historia.

DIPLOMACY ENCIPHERED HISPANIC OF THE XVI CENTURY

Abstract

The reign of Isabel and Fernando supposes the beginning of a new stage in the development of the cryptography. Simplicity, characteristic of the elaboration of cryptograms during the medieval period, will give way to complexity, as sometimes it will be fundamental to keep the secret of the messages and communications, in order to get the success in a negotiation.

The intention of the author in this article is to display a general panoramic of the techniques and procedures in code employed during the sixteenth century in the conformation of the diplomatic correspondence.

Keywords: Cryptography, Documentation, Write, Modern Age, History.

10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

INTRODUCCIÓN

Desde que el hombre dispuso de la escritura como vehículo comunicador mostró un empeño especial en impedir la lectura de información particular. Entendida en sentido amplio, la criptografía[1] se usa desde la más remota antigüedad, pues ya fue empleada por pueblos indios, chinos, persas, asirios, babilonios, egipcios, griegos, romanos... Su finalidad es clara: ocultar a terceras personas el contenido de textos que no les han sido destinados o que por su naturaleza e importancia sólo los deben conocer los interesados.

LA ESCRITURA CIFRADA EN LA PENÍNSULA IBÉRICA

Tradicionalmente, la cifra utilizada por los Reyes Católicos en la correspondencia mantenida con su embajador en tierras inglesas, el doctor Puebla, está considerada como la precursora del período moderno en relación a la península Ibérica. Tras la etapa medieval, en que los métodos criptográficos eran de sencilla confección, ahora van a complicarse y desarrollarse, debido a la necesidad de proteger el secreto de las comunicaciones, pues se asiste a un momento en el que se incrementan las relaciones internacionales y se establecen con carácter permanente las embajadas y las secretarías de Estado. Sin embargo, hay que precisar que esta documentación así elaborada es un procedimiento para desempeñar el poder político de una manera más competente, no significa un símbolo autoritario.

Además de la clave citada, elaborada por el consejero Miguel Pérez de Almazán[2], Isabel y Fernando también mantuvieron correspondencia cifrada con otras personalidades coetáneas suyas, como el obispo Diego de Muros, Gonzalo Fernández de Córdoba, Luis Despuig, Gracilazo de la Vega o fray Juan de Mauleón.

Esta misma práctica será seguida por el cardenal Cisneros, en sus misivas con Diego López de Ayala o con el Emperador, y por Carlos V, cuyos testimonios de esta naturaleza son múltiples: con la emperatriz María y su hijo Felipe, con Lope Hurtado de Mendoza, con Francisco I de Francia, con Fernando Dávalos, con el canciller Mercurino de Gattinara, con Andrea Doria, con el embajador Lope de Soria y con el abad Fernando Marín, entre otros[3].

Pero si ya estaba extendida la práctica criptográfica durante la primera mitad de la centuria decimosexta, más lo va a estar durante la segunda. Tanto es así que se puede considerar el reinado de Felipe II como un período áureo en el arte de la correspondencia diplomática. Pretextando que la cifra general empleada por su padre, Carlos V, para comunicarse con sus ministros y embajadores foráneos estaba difundida y, en consecuencia, no era conveniente para que los pactos internacionales llegasen a buen puerto, el Rey Prudente decide modificarla, y como tal se lo revela a su tío, el emperador Fernando, en una carta que le dirigió el día 24 de mayo de 1556. De Felipe II se conservan ocho códigos generales (fechados entre 1562 y 1582) y diversos particulares, como son los seguidos con su hermana la Princesa de Portugal, con el Duque de Alba, con el emperador Maximiliano, con Juan de Austria, con Luis de Requesens, con el cardenal Ganvela, etc.[4]

---

[1] Atendiendo a su étimo ("kryptos" y "graphein"), se entiende por tal la ciencia que estudia la escritura oculta. Hoy en día se puede conceptuar la criptografía como el arte de escribir en un lenguaje convenido mediante el empleo de claves o cifras, las cuales son las piezas maestras de todas las escrituras secretas.

[2] Archivo General de Simancas, Estado, leg. 2, fol. 1.

[3] Biblioteca de la Real Academia de la Historia, signs. 9/17 a 9/43 y 9/1951 a 9/1954. Archivo General de Simancas, Estado, legs. 59, 439, 442, 496 y 664.

[4] Archivo General de Simancas, Estado, legs. 514, 557, 590, 657, 658, 662, 664, 817, 820, 826 y 1060.

Puede ser que un episodio vivido por el rey austriaco unos años antes fuera determinante para que se aficionase por esta disciplina. Felipe II, dejándose llevar de las corrientes de la época, pensaba que en la corte gala tenían a Lucifer a su servicio y acusó a François Viète de sortílego y nigromante ante el Tribunal Eclesiástico Romano. La ridiculez de la censura fue obvia, ya que el francés inmediatamente descubrió el secreto, además de que el propio pontífice, Pío V, también contaba con un gabinete de criptoanalistas que habían perlustrado numerosas cifras españolas durante años.

El Siglo de Hierro supuso un decaimiento en el empleo de la escritura secreta, más acusado en el siguiente, en que desaparece la uniformidad y la elegancia utilizada en la construcción de criptogramas. Esto no es óbice para que los últimos monarcas Austracistas y los primeros Borbones continuaran usando esta práctica en sus comunicaciones con notables personalidades (Diego Sarmiento, el conde-duque de Olivares, el cardenal Albornoz, Rodrigo Ponce de León, Diego Saavedra Fajardo, Iñigo Vélez de Guevara, Ricardo Wall, Jorge Juan...)[5]. Luego, a partir de la centuria decimonónica, se asiste al triunfo de la técnica, olvidándose la denominada criptografía "histórica" o de "lápiz y papel", en beneficio de las máquinas cifradoras y, posteriormente, de las computadoras y ordenadores.

LA ESCRITURA CIFRADA EN HISPANOAMÉRICA

En relación a Hispanoamérica, los métodos de cifrado guardan un paralelismo manifiesto con los utilizados en la Península, y es que la génesis de la pasigrafía indiana, como es lógico, se encuentra en suelo hispano.

Con el fin de impedir que ciertos despachos importantes cayesen en manos enemigas se tomaron diversas prevenciones, y así, además de remitir el documento por triplicado o cuadruplicado, se codificaba. Es más, como afirma Guillermo Lohmann[6], la dificultad en la elaboración de las claves aumentaba si se quería encubrir información a potencias extranjeras, tal como noticias alarmantes sobre rebeliones indianas, indicios de problemas financieros concomitantes a la Monarquía o fechas de navegación en las que las flotas acarreaban riquezas ultramarinas. Periódicamente se fueron confeccionando claves "oficiales", para de este modo evitar su interceptación e interpretación, como fue el caso de las confeccionadas por la Casa de la Contratación o por el Consejo de Estado.

Pero no sólo emplearon este procedimiento los virreyes y otras altas jerarquías de la Corona, sino que también lo usaron miembros del estamento eclesiástico y simples particulares, tanto para comunicarse entre sí desde diferentes enclaves americanos como de la Península. Entre otros personajes, se tienen noticias de que emplearon métodos poligráficos Cristóbal Colón, Hernán Cortés, Pedro de Lagasca, el contador Rodrigo de Albornoz, Luis de Velasco, el almirante Antonio de Aguayo, Francisco de Toledo, fray Francisco de Santa Cruz, el capitán Pedro de Roelas, el gobernador de la isla de Cuba Juan de Tejada, el general de la flota Pedro Menéndez Márquez, etc. Eso sí, a diferencia de lo acontecido en la península Ibérica, en donde el período de mayor esplendor lo hemos datado durante el reinado de Felipe II, en tierras americanas será durante la etapa emancipadora cuando este arte alcance su edad de oro.

Cabe decir, asimismo, que es también de este período histórico el primer estudio de un autor hispano relativo a esta materia. Este honor ha correspondido a Diego Fernández de Palencia, quien el año 1571 publica en Sevilla su *Historia del Perú*, en la que dedica un capítulo –52°- a describir y analizar diversos métodos de cifrado.

[5] Archivo General de Simancas, Estado, legs. 1, 739, 1160, 2056, 2322, 2590, 2999 y 3010. Archivo Histórico Nacional, Osuna, legs. 3456 y 3551.

[6] LOHMANN, G. (1954) "Cifras y claves indianas. Capítulos provisionales de un estudio sobre criptografía indiana", *Anuario de Estudios Americanos*, XI (1954): 299-300.

10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

PRÁCTICAS CRIPTOGRÁFICAS

Retomando el tema de las claves utilizadas en España durante el siglo XVI, hay que significar que los elementos que prevalecen en su configuración son de carácter esteganográfico o figurativo y literal, imponiéndose estos últimos con el paso del tiempo[7].

El método predilecto empleado en la correspondencia diplomática moderna de índole confidente es el llamado "nomenclátor", compuesto por un alfabeto, casi siempre homofónico, y una serie de palabras o frases codificadas, representándose cada una de ellas por uno o más símbolos enigmáticos. Estas "tablas cifradoras" o "códigos", encuadrados en el sistema de sustitución[8], constituyen un método que ofrecía bastante seguridad, y cuyo origen se localiza en la corte mantuana a comienzos de la centuria decimoquinta. No obstante también tenían varios inconvenientes, v. gr. que el corresponsal que recibe el criptograma debe conocer la clave completa para poder interpretarlo, que sólo se pueden transmitir los testimonios que tengan su correspondencia cifrada, que puede ser problemático cambiar el implemento en caso de variar el código y que su criptoanálisis se puede basar en el examen de las frecuencias.

DIPLOMACIA VS. CRIPTOANÁLISIS

Expuesto lo anterior, hay que significar que, por una parte, la reaparición de las artes, la erudición y las ciencias durante el Renacimiento propició el avance de esta disciplina, y por otra, que la detonación de las maquinaciones políticas benefició el desarrollo de las comunicaciones secretas. En consecuencia, la diplomacia floreció; cada estado enviaba embajadores a la corte de los demás y, por lo general, se establecieron oficinas de cifras, a la vez que cada plenipotenciario tenía un secretario de cifras. Entre otros departamentos de criptoanálisis destacan el Cabinet Noir parisino y la Geheime Kabinets-Kanzlei vienesa. En España, hasta que en el año 1561 se traslada la capitalidad a Madrid, se centralizaba la criptografía "oficialista" en la Secretaría de Despacho Universal, emplazamiento desde el que era distribuida por los Correos a todos los lugares hispanos, europeos y americanos con los que se mantenían relaciones diplomáticas. Después, este Despacho se estableció en el Alcázar madrileño, siendo su director el Secretario del Exterior, por entonces Gonzalo Pérez.

También se comienza a asistir durante esta etapa histórica a un fenómeno advertido por el profesor Singh, consistente en que no sólo la escritura cifrada se estaba convirtiendo en un instrumento diplomático frecuente, sino que la técnica criptoanalítica empezaba a aparecer en Occidente[9].

---

[7] En la centuria siguiente se introducen los numéricos, que son los predominantes en el siglo XIX.

[8] El sistema de sustitución o perturbación consiste en reemplazar alguna letra del alfabeto por uno o más signos convenidos por los corresponsales, incluyendo aquellos métodos basados en sustituir los elementos del texto claro o normal por una representación diferente a la original: Julio César, masónico, tabla de Tritemio, Frederici, criptógrafo de Porta, lord Bacon, criptógrafo de Alberti, etc. El descriptado general de este procedimiento se efectúa, básicamente, por dos procedimientos: método de la palabra probable –se basa en el supuesto de conocer alguno de los vocablos contenidos en el mensaje- y método de los bigramas de gran frecuencia –se fundamenta en la apreciación de aquellos grupos de dos o más letras cuya formación es frecuente y mediante la observación de las letras obligadas-.
Además se ha empleado el sistema de transposición, que estriba en colocar un fragmento cifrado en un lugar previamente conocido por el otro corresponsal, comprendiendo los métodos que alteran el orden natural de las letras o palabras en un texto, trastrocándolas o formando anagramas con ellas, por ejemplo: escítalo, enrejado, tabla, Richelieu.
El tercer sistema, ocultación, encuadra todos los procedimientos en los que el remitente transmite las verdaderas letras del mensaje de forma oculta o disfrazada, siendo ejemplos las artimañas y tretas empleadas a lo largo de la historia para conseguir que un criptograma llegue a su lugar de destino y sea interpretado por el corresponsal receptor.

[9] SINGH, S. (2000), *Los códigos secretos*, Madrid: Debate, pp. 69-70.

Es decir, surgieron individuos que intentaban romper la protección que supuestamente procuraban los métodos criptográficos[10]. Esta es la razón por la que se introdujeron nuevos elementos con la finalidad de complicar la perlustración de las comunicaciones cifradas: inclusión de símbolos "nulos", intencional deletreo erróneo de algunas palabras antes de codificar el mensaje para evitar el análisis de frecuencias, implantación de los "codigos" en los nomenclatores, etc.

Comúnmente, los textos codificados son misivas que se adaptan a los estilos propios en la correspondencia privada o a las notas de oficio empleadas en la Administración. Sin embargo, para evitar su perlustrado, se eliden muchas veces los tratamientos protocolarios, los saludos, la intitulación, la dirección y la data, es decir aquellos elementos que se prestan mejor al descodificado. Misivas estas que podían estarlo en su totalidad con caracteres enigmáticos o en aquellos fragmentos que se considerasen convenientes por su contenido confidencial. En función de esta particularidad, su descifrado o texto claro, que solía correr a cargo de un oficial capacitado para tal labor, se podía presentar al corresponsal receptor en una hoja aparte o efectuar el descodificado en el propio papel remitido por el emisor, bien interlineado, bien marginal. Aunque también es verdad que muchas veces este ejercicio estaba supeditado a la forma de transmitir la información: por correo ordinario o de manera enmascarada.

En fin, que al leer la historia de la criptografía de esta época, casi se tiene la sensación de que el intercambio de criptogramas era un pasatiempo social, debido a su intercepción y resolución frecuente. Recuérdese aquel axioma que dice: "El triunfo del criptógrafo constituye el fracaso del criptoanalista, y viceversa"; en consecuencia, la poligrafía ha ido adquiriendo un lugar relevante y esencial en la actividad diplomática de los diferentes gobiernos y estados. Incluso, con el paso del tiempo, de estar en manos de militares y diplomáticos, en la sociedad contemporánea ha surgido la necesidad de una criptografía civil, cerrojo de la "era de la información".

[10] Son conocidos, entre otros, además de Viéte, los nombres de Philibert Babou (criptoanalista del rey francés Francisco I), Giovanni Soro y Partemio (al servicio de la republica veneciana durante el siglo XVI), Mateo Argenti (criptógrafo de la república romana) y Walsingham (afamado descriptador en la Inglaterra de Isabel I).

10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

CONCLUSIONES

En la evolución histórica de la criptografía hispánica se considera el reinado de los Reyes Católicos el inicio del período moderno, el cual alcanzará hasta la centuria decimonovena en la que, con el triunfo de la técnica, decae el empleo de la escritura secreta, desapareciendo la belleza y homogeneidad antes empleada en la configuración de criptogramas.

Asimismo, el asentamiento estable de secretarías de Estado y de legaciones provocará la necesidad de asegurar la confidencialidad de la correspondencia, lo que conllevará un auge de la criptografía, al tiempo que se complican los métodos cifradores empleados, lo que redunda en una mayor dificultad a la hora de perlustrar.

Si en Europa destacan tratadistas y criptógrafos de la talla del benedictino alemán Tritemio, del noble francés Blaise de Vigènere, del político inglés Francis Bacon y de los italianos Juan Bautista Belasso, Gerolamo Cardano y Juan Bautista Porta, en España se considera el reinado de Felipe II una de las etapas más esplendorosas en este arte poligráfico.

Pero no solamente el Rey Prudente, sino que también los soberanos anteriores y posteriores usaron esta práctica con profusión en sus comunicaciones diplomáticas, siendo el procedimiento preferido en la construcción de las mismas las denominadas "tablas cifradoras" o "nomenclátores", pues constituyen un método bastante seguro.

Asimismo, aunque el período áureo en la historia de la criptografía americana se produjo durante la etapa de la emancipación, desde la centuria decimosexta los sistemas cifradores estaban bastante difundidos, pues fueron empleados tanto por organismos estatales y virreyes, como por órdenes religiosas e individuos particulares.

Por último, hay que significar que la criptografía era una industria floreciente, un instrumento diplomático habitual, de tal modo que cuando todavía se estaba intentando familiarizar con las habilidades precisas para establecer comunicaciones protegidas, aparecieron perlustradores que ambicionaban destruir esa seguridad, circunstancia que ocasionó la pretensión de perfeccionar estos procedimientos aumentando la dificultad de los sistemas de cifrado.

BIBLIOGRAFÍA BÁSICA

CABALLERO GIL, Pino, *Introducción a la criptografía*, 2ª ed. Madrid: Ra-Ma, 2002.

CEILLIER, Rémi, *La cryptographie*, Paris: Presses Universitaires de France, 1945.

D'AGAPEYEFF, Alexander, *Codes and ciphers*, Oxford: Oxford University Press, 1932.

GAINES, Helen Fouche, *Cryptanalysis*, 2ª ed., New York: Dover Publications, 1989.

GALENDE DÍAZ, Juan Carlos, *Criptografía. Historia de la escritura cifrada*, Madrid: Complutense, 1995.

GALENDE DÍAZ, Juan Carlos, "La escritura cifrada durante el reinado de los Reyes Católicos y Carlos V", *Cuadernos de Estudios Medievales y Ciencias y Técnicas Historiográficas*, 18-19 (1993-1994), Granada,,, pp. 159-178.

GALENDE DÍAZ, Juan Carlos, "Recorrido histórico por la criptografía militar", *Revista de Historia Militar*, 88 (2000), Madrid, pp. 11-34.

GALENDE DÍAZ, Juan Carlos, "Sistemas criptográficos empleados en Hispanoamérica", *Revista Complutense de Historia de América*, 26 (2000), Madrid, pp.57-71.

JUHER, David, *L'art de la comunicació secreta: el llenguatge de la criptografía*, Barcelona: Llibres de l'Índex, 2004.

KAHN, David, *The codebreakers*, 2ª ed. .Nueva York: Scribner, 1996.

LAFFIN, John, *Códigos y cifras. Los mensajes secretos y su historia*, La Coruña: Adara, 1976.

LANGIE, Andre y SOUDART, A., *Traité de Cryptographie*, Paris: Alcan, 1925.

LOHMANN, Guillermo, "Cifras y claves indianas. Claves provisionales de un estudio sobre criptografía indiana", *Anuario de Estudios Americanos*, XI (1954), Sevilla, pp. 285-380.

LOHMANN, Guillermo, "Documentos cifrados indianos", *Revista de Indias*, 15 (1955), Madrid, pp. 255-282.

NEWTON, David E., *Encyclopedia of Cryptology*, Santa Bárbara: ABC-Clio, 1997.

MULLER, Andre, *Les écritures secrétes*. Le chiffre, Paris: Presses Universitaires de France, 1971.

PRATT, Fletcheer, *Histoire de la cryptographie*, Paris: Payot, 1940.

SERRANO GARCÍA, Pedro, *Criptografía y perlustración*, Madrid: La Xilográfica, 1953.

SGARRO, Andrea: *Códigos secretos*, Madrid, Pirámide, 1990.

SINGH, Simon, *Los códigos secretos*, Madrid: Debate. 2000.

SMITH, Lawrence Dwight: *Cryptography. The science of secret writing*, New York: Dover Publications, 1943.

10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

TRAPPE, Wade y WASHINGTON, Lawrence C., *Introduction to cryptography with coding theory*, New Jersey: Pearson Education, 2006.

VAUDENA, Serge, *A classical introduction to cryptography*, New York: Springer, 2006.

WELSH, Dominic, *Codes and cryptography*, Oxford: Clarendon Press, 2005.

ZANOTTI, Mario, *Crittografia. La scrittura segrete*, Milano: Ulrico Hoepli, 1928.