RECORRIDO HISTÓRICO POR LA CRIPTOGRAFÍA MILITAR*

Juan Carlos GALENDE DÍAZ
Doctor en Historia
Universidad Complutense de Madrid

INTRODUCCIÓN

LA finalidad de la criptografía, cuyo étimo significa *ciencia que estudia la escritura oculta*, es enmascarar 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[1]. Así lo insinúa también el profesor Rufino Blanco cuando manifiesta que esta ciencia consiste en *comunicar por medio de letras, signos o números, las informaciones conseguidas para el espionaje, dispuestas de tal manera que el enemigo no consiga descubrir su significado*[2], es decir, se puede entender como el arte

* En homenaje y recuerdo del coronel don Longinos Criado Martínez, profundo conocedor y erudito de esta materia, de quien recibí lecciones magistrales y a quien debo que cultivase en mí la afición por la misma.

Deseo expresar, igualmente, mi agradecimiento al coronel don Eduardo Bravo Garrido por las explicaciones, orientaciones y sugerencias que me ha ofrecido y formulado, fundamentalmente en lo relativo a la criptografía militar contemporánea.

[1] En lenguaje estrictamente militar se denomina *red de cifra* al conjunto de corresponsales que pueden transmitirse entre sí mensajes cifrados, los cuales requieren, al menos, una clave común de trabajo y una de reserva. El número de componentes está en función del medio empleado para la cifra y del tráfico a cursar.

[2] BLANCO, R.: *Estudios paleográficos.* Sao Paulo, 1987, p. 110.

de escribir en un lenguaje convenido mediante el uso de claves o cifras. En consecuencia, esta disciplina enseña a diseñar cifrarios o códigos secretos. La labor inversa es *criptoanalizar*: interpretar mediante análisis los cifrarios construidos por los criptógrafos.

Por su parte, la operación de transformar un texto cifrado en el mensaje claro, si se conoce la clave, se denomina *descifrar* o *decodificar*, mientras que si se ignora es más adecuado llamarla *perlustrar* o *descriptar*. Por consiguiente, la *criptología*, *perlustración* o *descriptación* es la actividad que tiene por objeto el descifrado de criptogramas desconociendo la clave[3].

Por todo lo mencionado, se puede deducir que para criptoanalizar un documento cifrado hay que saber la clave o el significado de los símbolos que lo configuran. La formación de una clave no es complicado, puesto que no se sujeta a reglas fijas y sólo depende de la pericia en la combinación de signos. Lo difícil es el descifrado del criptograma cuando falta el código.

Descriptar o perlustrar es tarea penosa y dificilísima[4]. No sólo requiere saber la lengua, determinar el sistema empleado y buscar la frecuencia en la aparición de las letras[5], sino también reconocer las letras y signos repetidos, inertes o anulantes[6], etc.

A lo largo de la historia se han empleado diferentes sistemas criptográficos, siendo los tres principales el de *transposición*, el de *sustitución* y el de *ocultación.*

---

[3] De todas las maneras, y con un carácter más genérico, se puede conceptuar la criptografía como todo el conjunto de normas, técnicas, métodos y procedimientos que competen tanto al cifrado como al descifrado de la información.

[4] KAHN, D.: *The Codebreakers.* Macmillan, 1967. Esta obra es una de las más precisas y completas que se han escrito hasta la actualidad sobre este tema. Otras recomendables son: FIGL, A.: *Systeme des chiffrierens.* Graz, 1926; GAINES, H.F.: *Cryptanalysys.* Dover, 1956; IRIGOIN, J.: *Dechiffier les ecritures effacees.* París, 1988; MILLIKIN, D.: *Elementary cryptography.* New York, 1943; SERRANO, P.: *Criptografía y perlustración.* Madrid, 1953; SINKOV, A.: *Elementary cryptanalysis.* Random House, 1968 y WOLFE, J.M.: *A first course in cryptanalysis.* Brooklyn, 1943.

[5] En las principales lenguas (española, italiana, francesa, inglesa, portuguesa y alemana) es la vocal E la que con mayor asiduidad aparece, seguida de las vocales A y O, y las consonantes R, S, L y N. En la península Ibérica, en orden decreciente, la sucesión de las letras según su frecuencia es la siguiente: E, A, O, S, I, R, N, L, D, C, T, U, P, M, Q, Y, B, G, H, F, V, Z, J, X, K. Según lo expuesto, es fácilmente deducible que sean los bigramas conformados por alguna de estas letras los más frecuentes: ES, DE, EN, LA, OS, EL, AR, etc; por su parte, los trigramas más comunes son: QUE, EST, ARA, ADO, DEL, CIO, NTE, OSA, EDE, PER...; mientras que los tetragramas más asiduos son ADOS, IDOS y ENTE; finalmente, los dos pentagramas más corrientes son ISIMO y TRANS. Es recomendable servirse de las tablas construidas por uno mismo y no de las confeccionadas por otros criptólogos, ya que en estas frecuencias influye de forma considerable la naturaleza del lenguaje habitual que se emplee en cada escrito: policial, literario, militar, etc.

[6] Biblioteca Nacional (BN): *Regla que debe considerar quien quisiere probar a descifrar sin contracifra, en lengua española,* mss. 18657/20. Es una interesante obra anónima, supuestamente del siglo XVI.

»22,94,79,96,58,33,76,24,91,79,75,33,80,58,71,es necesario por lo tanto
e a l t e r a r e l o r . e n
»que V. E.,11,44,18,22,60,33,91,46,11,25,14,55,10,59,24,58,80,75,26,79,58,46,74,
e s t e p r e . e n i d o . r e . o b l e . i
»28,93,79,94,50,66,14,16,evitando en lo posible que de ella se,52,60,22,33,66,
. i l a n c i a a p e r c
»14,87,52,91,34,48,62,39,85.93,66,95,convendría mientras duren,58,44,18,76,44,
i . a e l p u . . i c o e s t a s
»29,93,78,82,40,25,65,96,52,71,29,74,52,57,83,30,91,34,75,57,41,22,69,58,65,se se-
c i r c u n s t a n c i a s . . e l o s . e . e s
»paren,34,10,47,58,25,95,44,48,10,57,93,26,79,91,13,11,44,62,18,24,95,60,16,y que
l o m e n o s p o s i b l e d e s u t r o p a
»permanezcan cerca de ella el mayor número de,75,43,14,29,54,16,79,58,65,
o f i c i a l e s
»así como que V. E. se halle,44,14,58,36,60,33,58,22,50,29,75,90,18,76,82,96,10,
s i e m p r e e n c o n t a c t o
»66,95,71,22,45,10,57,para la rápida,18,24,16,44,36,74,57,93,10,50,15,22,99,58,66,
c o n e . o s t r a s m i s i o n y e . e c
»40,29,93,75,90,13,22,79,94,65,10,33,55,91,50,22,44,que en un momento,80,94,
u c i o n d e l a s o r d e n e s . a
»13,10,37,62,23,14,91,33,76,25,66,95,50,46,58,71,93,78,para,44,10,43,75,66,94,33,
d o . u . i e r a n c o n . e n i r s o f o c a r
»78,52,60,93,55,94,15,44,91,31,22,33,16,72,58,25,96,11,la menor,14,50,18,22,25,
r a p i d a y s e v e r a m e n t e i n t e n
»96,10,71,94,quedando V. E. autorizado para,44,30,17,33,14,36,54,78,10,70,16,
t o n a s . . r i m i r o . a
»33,74,52,33,79,94,57,81,12,76,24,55,93,76,57,13,58,44,18,76,29,16,47,22,25,18,10,
r i a r l a s . . a r d i a s d e s t a c a m e n t o
»44,75,37,12,11,57,18,75,65,que creyera innecesarios,95,36,52,34,57,54,96,30,16,
s o . . e s t o s o m a l s i t . a
»13,10,65,y pudieran utilizarse más ventajosamente,29,10,50,43,54,75,para
d o s c o n f i o
»todo en su acreditado,29,11,34,10,37,24,30,13,22,25,66,14,94,15,58,25,91,33,19,
c e l o . r . d e n c i a y e n e r .
»14,94,recomendándole me participe,18,75,55,16,50,95,46,91,13,16,80,15,68,76,
i a t o d a n o . e d a . y . a
»47,94,50,80,10,72,11,76,34,52,60,94,33,52,18,95,53,91,34,11,19,33,16,89,54,29,10,
m a n . o m e a l a p a r a t o . e l e . r a . i c o
»si el caso lo merece. Á los Gobernadores de los fuertes y Comandantes mi-

»litares de los cantones dependientes de su autoridad,79,91,44,53,24,16,57,29,
l e s . r a s c
»33,14,26,93,78,52,11,65,18,94.57,74,25,65,53,78,30,29,66,14,10,50.11,44,59,34,16,
r i b i r a e s t a s i n s . r . c c i o n e s . l a
»57,55,22,47,16,57,que V. E. crea conveniente comunicarles. Lo,13,14,28,10,
s d e m a s d i . o

Fragmento de parte cifrado

El primero consiste en colocar un fragmento cifrado en un lugar previamente conocido por el destinatario, 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, telégrafo, tabla, enrejado, Richelieu*, etc. Este sistema puede ser *simple* o *sencillo* -cuando el orden de las letras que componen el escrito no experimenta más que una sola alteración- y *doble* o *múltiple* -que supone una segunda alteración del texto ya modificado por una primera transposición-.

El sistema de sustitución o perturbación consiste en reemplazar alguna letra del alfabeto por uno o varios signos convenidos de antemano por los corresponsales, incluyendo los métodos basados en sustituir los elementos del texto claro o normal por una representación distinta a la original, v. gr.: *Julio César, masónico, plancheta de Eneas, criptógrafo de Alberti, benedictino, criptógrafo de Porta, tabla de Tritemio, criptógrafo de la Curia Papal, criptógrafo de Fleissner, lord Bacon, Frederici, criptógrafo de cinta, criptógrafo de disco*, etc. Este sistema, como el de transposición, puede ser *sencillo* o *simple* -en el que cada letra del mensaje es sustituida por otra letra, cifra o signo- y *doble, múltiple* o *de varias claves* -en el que cada letra del texto claro puede ser reemplazado por diversas letras, cifras o signos-. De este modo, si la sustitución se realiza por medio de letras, suele denominarse *literal*, si por números, *numérica*, y si por signos, *esteganográfica* o *figurativa*.

El descriptado general de los sistemas de sustitución se efectúa, fundamentalmente, por dos métodos: 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-.

Los métodos que participan de las características de los sistemas criptográficos anteriores están comprendidos en el sistema *mixto*. Es decir, aquéllos en los que el texto claro es primeramente sustituido y luego transpuesto, o viceversa. Un ejemplo de este sistema lo constituye el *criptógrafo de Bazeries*.

El sistema de 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.

Además de los citados, existen otros métodos que, si bien encajan perfectamente dentro del sistema de sustitución, pueden considerarse agrupados de manera independiente. Entre ellos, por ser los principales, sobresalen los

siguientes: método de los *impresos, lenguaje convenido, diccionarios cifradores, tablas* o *códigos cifradores*[7] y *máquinas cifradoras.*

Por último, cabe mencionar que los medios que se utilizan para las operaciones de cifrar y descifrar la información se denominan *medios de cifra.* Estos, exceptuando el codificado a mano y los *códigos* o *diccionarios,* pueden ser: *manuales*, constituidos por rejillas, discos, regletas o materiales similares, que, aunque económicos y sencillos de construir, suelen ser premiosos y sujetos a errores; *mecánicos*, que con criptógrafos -relativamente seguros-, cuyo movimiento puede efectuarse de forma manual o mediante el ensamblaje de un motor eléctrico, que proporcionan un criptograma, bien por lectura directa, bien por impresión sobre una cinta u hoja de papel; *eléctricos,* compuestos por máquinas, actualmente caducas y en desuso, que realizan las labores de criptografiado y decodificado mediante circuitos eléctricos; y *electrónicos*, que son los medios más modernos, destacando entre ellos los secráfonos electrónicos para teléfonos por cable o para radioteléfonos, los criptógrafos para textos escritos y mezcladores para teletipos, los equipos de cifrado de imágenes o datos y, finalmente, los equipos de multicifrado, los cuales, empleando la técnica digital o de código de impulsos, verifican el cifrado y descifrado de la información procedente de un múltiplex o multicanal[8].

Los *medios de cifra*, anteriormente expuestos, se pueden emplear *fuera de circuito* y *en circuito.* En el primero de los casos, la información codificada es preparada independientemente del circuito de telecomunicación, y cuando esta labor se ha verificado se procede a su transmisión por un terminal cualquiera; el terminal receptor, por su parte, recibe la información enigmática, la cual, cuando es registrada, es pasada por medio de cifra, efectuándose su decodificado.

Los *medios* que permiten su utilización *en circuito*, también llamados *telecifrantes,* son aquéllos que en los terminales de transmisión se inserta y se recibe el comunicado en claro, pero en determinados lugares del circuito están montados los equipos de criptografiar que realizan las operaciones de cifrado y descifrado, comúnmente adosados a los terminales; muchos de ellos permiten no sólo el trabajo *en circuito*, sino también *fuera* de él[9].

---

[7] También llamados *nomenclatores*, y que desde el siglo XVI hasta la primera mitad del siglo pasado fue el método de cifrado más utilizado en la correspondencia diplomática.

[8] *Reglamento, enlace y transmisiones.* Madrid, 1980, pp. 78-80.

[9] Ibídem, p. 80.

EVOLUCIÓN HISTÓRICA

Etapa antigua

Entendida en sentido amplio, la criptografía se usa desde la más remota antigüedad, pues indios, chinos, persas, asirios, babilonios y egipcios poseían ya signos convencionales, equivalentes a las letras de sus alfabetos, con los que comunicaban órdenes secretas a sus emisarios, especialmente en tiempo de guerra, y a los que daban en ocasiones, además de este valor práctico, unos atributos mágicos y religiosos.

Desde tiempos pretéritos se emplearon ya ciertas señales que consistían en luminarias sobre determinadas alturas, agrupadas o esparcidas de un modo convenido, para avisar de la presencia del enemigo u otro acontecimiento previsto de antemano. Después se utilizaron antorchas encendidas o estandartes desde torres construidas al efecto, con los cuales se entendían haciéndolos aparecer y desaparecer[10].

Asimismo, desde que el hombre dispuso de la escritura como vehículo de comunicación mostró un empeño especial en impedir la lectura de información particular. Al principio, los sistemas más sencillos empleados para enviar mensajes privados consistían en guardarlos en receptáculos cerrados, pero bastaba con capturar al portador para obtener la información. Por esta causa se hizo necesario escribir de alguna manera el contenido del mensaje para que su localización no conllevara su interpretación. Entre los medios más antiguos utilizados para este fin se conoce el empleado en el siglo VI a. C. por Damarato, quien, para informar a los lacedemonios del proyecto de Jerjes de invadir Grecia, escribió un mensaje inciso en una tablilla y la recubrió después de cera.

En el siglo siguiente, el general espartano Lisandro para comunicarse con otros generales empleó unos rodillos o bastones de madera sobre los que enrollaba unas correas de cuero y escribía el mensaje a lo largo de ellos. Luego retiraba la cinta y la enviaba al destinatario, que tenía en su poder una copia idéntica de la vara. Cuando éste colocaba la correa correctamente de nuevo podía leer el mensaje, ya que hasta ese momento las letras no tenían relación aparente entre sí. Se trata del método conocido con el nom-

[10] CARMONA, J. C.: *Tratado de criptografía con aplicación especial al ejército*. Madrid, 1894, p. 155. Es conocido, por ejemplo, que los romanos emplearon la telegrafía óptica, cuyas torres se ven todavía entre los vestigios que quedan de los llamados campos romanos.

bre de *escítalo* que, en esta ocasión histórica, como expone A. Rodríguez Prieto, sirvió para salvar un imperio y un general[11].

Otro ejemplo de carácter criptográfico empleado en esta época es el utilizado por el griego Histiaeus, quien, pensando enviar un mensaje a su yerno Aristágoras para que capitaneara una revuelta, afeitó la cabeza de un esclavo que ejercería las funciones de mensajero. Posteriormente escribió el aviso con caracteres endebles sobre su cuero cabelludo y, cuando le creció el pelo, fue enviado al campamento de destino, en donde se le rasuró otra vez la cabeza, y de esta manera el receptor pudo entonces leer el texto[12].

En el siglo II a. C., el historiador griego Polibio ideó una sencilla tabla alfanumérica, conocida con el nombre de *damero*, en la que cada letra era sustituida por un grupo de dos números, correspondientes a las coordenadas de la misma.

A lo largo del período romano se tiene noticia de la utilización de un método para transmitir información con carácter secreto, consistente en efectuar la comunicación sustituyendo unos símbolos por otros en el conjunto de los que componían el mensaje, obedeciendo a cierta regla fija. Así, Julio César utilizaba un cifrario basado en sustituir cada letra del alfabeto latino por otra colocada tres puestas después y, posteriormente, Augusto hacía corresponder cada letra por la que la seguía[13].

Etapa medieval

Durante la Edad Media, hasta el siglo XIII, no se tiene mucho conocimiento de la evolución de la criptografía, aunque es presumible que se utilizase, fundamentalmente, con ocasión de guerras o embajadas.

Fue corriente entre los criptógrafos emplear sencillos sistemas de sustitución, reemplazando diferentes letras del alfabeto, casi siempre las vocales, por otras letras o símbolos[14]. Asimismo, se usaron otros procedimientos

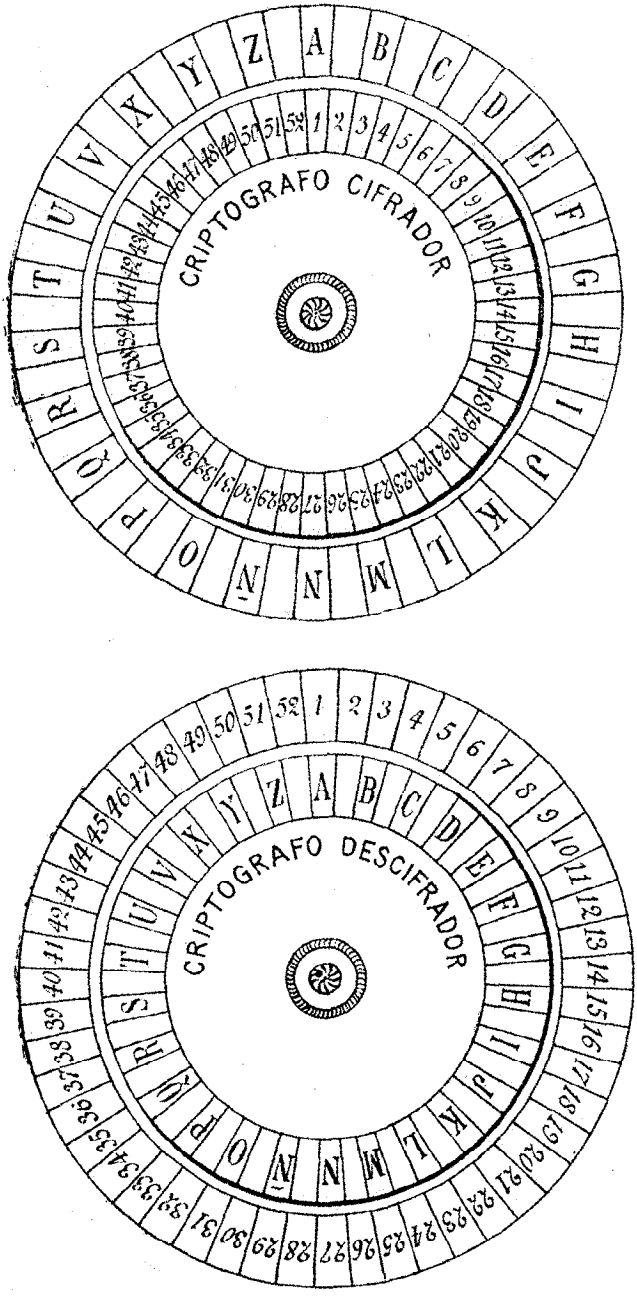
---

[11] RODRÍGUEZ, A.: *Protección de la información: diseño de criptosistemas informáticos.* Madrid, 1986, p. 13.

[12] GARCÍA ORGA, V.: *Criptografía: la ocultación de mensajes y el ordenador*, Madrid, 1986, p. 8.

[13] Basado también en el sistema de sustitución, en épocas antiguas, fue empleado el cifrario denominado *atbash hebreo*. Este método consistía en escribir las letras que componen el alfabeto hebreo en dos líneas: en la primera las grafías se sucedían de manera sinistrorsa y en la segunda de forma dextrorsa. Luego, se permutaban las letras originales de cada renglón por las que ocuparan su mismo lugar en el antagónico.

[14] Por ejemplo, Carlomagno utilizó un sistema de sustitución consistente en representar cada letra del alfabeto por un símbolo de carácter esteganográfico. También fue habitual entre los criptógrafos los alfabetos pictóricos, siendo uno de los más populares el *alfabeto zodiacal*, en donde los signos representativos de los cuerpos celestes más conocidos: Venus, Luna, Géminis, Sol, Libra, Acuario, Neptuno, etc., tenían su correspondencia con las diferentes letras que componen el alfabeto.



Criptógrafo de Grivel

criptográficos, v. gr. anagramas, alteración de las letras de una palabra, fuga de vocales, etc., sin que faltase la inclusión de signos nulos o sin valor. Siempre la misma finalidad: dificultar la labor descriptadora, y es que *una cifra perfecta no debe ser trabajosa de escribir ni de leer, sino que debe ser imposible de descifrar*, como sentenció Francis Bacon.

Más tarde, la escritura oculta continuó practicándose en la cancillería carolingia e irlandesa, y además se empezó a aplicar en la curia pontificia y en algunos estados italianos, como en Venecia. Estas repúblicas descubrieron un sistema fácil para evitar el análisis de frecuencias: la sustitución de una misma letra por varios signos diferentes, añadiendo varios nulos o inertes para los espacios entre palabras.

En esta etapa destacan como principales autores de obras sobre temática criptográfica los siguientes: el franciscano Roger Bacon; Gabriel de Lavinde, secretario de las comunicaciones secretas del Papa Urbano VI y autor de la obra más antigua conocida, *Liber Zifrorum* (publicada en Roma entre 1375 y 1385); el secretario pontificio de la corte romana Leon Bautista Alberti, autor del célebre *Trattati in cifra*, publicado en Roma en 1470; y Cicco Simoneta, consejero y secretario de los duques de Sforza, que en 1474 escribe en Milán su *Regule ad extrahendum litteras ziferatas sine exemplo*.

A finales del siglo XV, como curiosidad, se puede recordar que Leonardo da Vinci usaba con intención enigmática un procedimiento ingenioso, consistente en trazar su escritura de tal forma que sólo se podía leer reflejando el texto en un espejo[15].

Etapa moderna

El establecimiento con carácter permanente de embajadas y secretarías de Estado, el incremento de las relaciones internacionales y la necesidad de asegurar el secreto de la correspondencia, motivada por las circunstancias antes reseñadas, son las causas que provocaron el auge de la criptografía en la Edad Moderna, al tiempo que se procede a complicar los métodos empleados, lo que redunda en mayor dificultad a la hora de perlustrar.

De esta época sobresalen como tratadistas: el historiador y religioso benedictino alemán Tritemio, que en 1499 publicó en seis volúmenes su obra

[15] LAFFIN, J.: *Códigos y cifras. Los mensajes secretos y su historia.* La Coruña, 1976; GARDNER, M.: *El idioma de los espías.* Madrid, 1991.En estas obras encontramos anécdotas históricas relacionadas con la criptografía.

Poligraphiae[16] y en 1531 editó en *Lyon Steganografía o arte de escribir en cifra*; Juan Bautista Belasso, autor en 1533 de la obra *El auténtico modo para escribir en cifra*; Gerolamo Cardano, inventor del sistema de rejilla y autor de la obra *De rerum varietate*, editada en Basilea en 1557; Juan Bautista Porta, a quien la historia le ha concedido el título de *padre de la moderna criptografía*, que en 1563 publica en Nápoles un tratado titulado *De furtivis litterarum notis vulgo de ziferis*; el noble francés Blaise de Vigènere, que publicó en París en 1586 la *obra Traicté des chiffres ou secrétes manieres d'écrire*; y el filósofo y político inglés Francis Bacon, vizconde de St. Albans y lord canciller de Inglaterra.

A partir de la centuria decimosexta lo más destacado es la investigación criptoanalista en el hallazgo de claves y desciframiento de correspondencia, sin grandes progresos en la aparición de nuevos métodos. En este sentido, John Wallis está considerado como el primer gran criptoanalista, debiéndosele el revelado de los criptogramas de Carlos I. Luego destacan Edward Willes, autor de la obra *Opera miscellanea* -publicada en Oxford en 1699- y Antoine Rossignol, jefe de la correspondencia del servicio secreto con Richelieu y Luis XIV, quien descubrió, entre otras cosas, las claves de los hugonotes[17]. Otros grandes perlustradores fueron Partemio, Mateo Argenti, Walsingham y François Viète[18], y es que era costumbre tener en cada corte un especialista en cifra.

Entre los más famosos departamentos de criptoanálisis descuellan el Cabinet Noir de París y la Geheime Kabinets Kanzlei de Viena, tan eficientes que, al leer la historia de la criptografía de esta época, se tiene la sensación de que el intercambio de criptogramas sólo era un pasatiempo social, puesto que se interceptaban y resolvían con demasiada frecuencia.

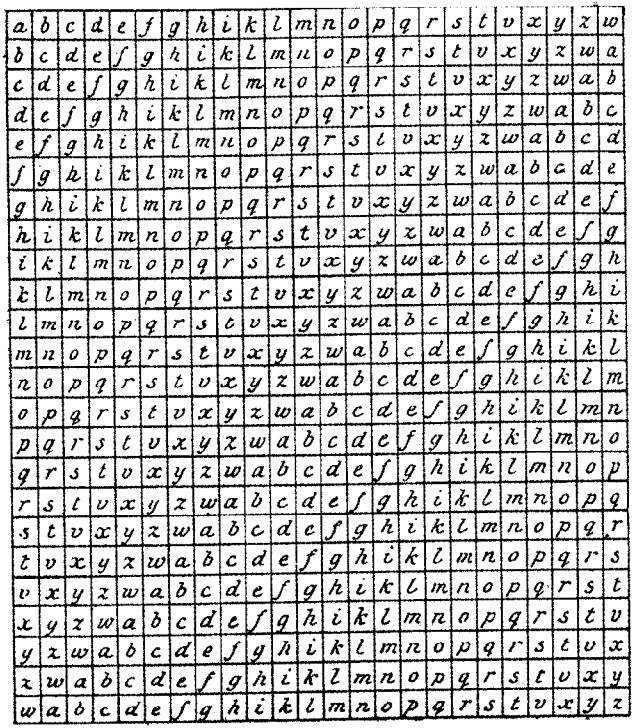
En España, la edad de oro de la escritura cifrada se produce durante el reinado de Felipe II. En carta dirigida el día 24 de mayo de 1556 a su tío el emperador de Alemania Fernando I, le reveló la resolución de variar la cifra que empleaba su padre Carlos V para comunicarse con sus ministros y embajadores en otros países. Para tomar esta medida no sólo argumenta que

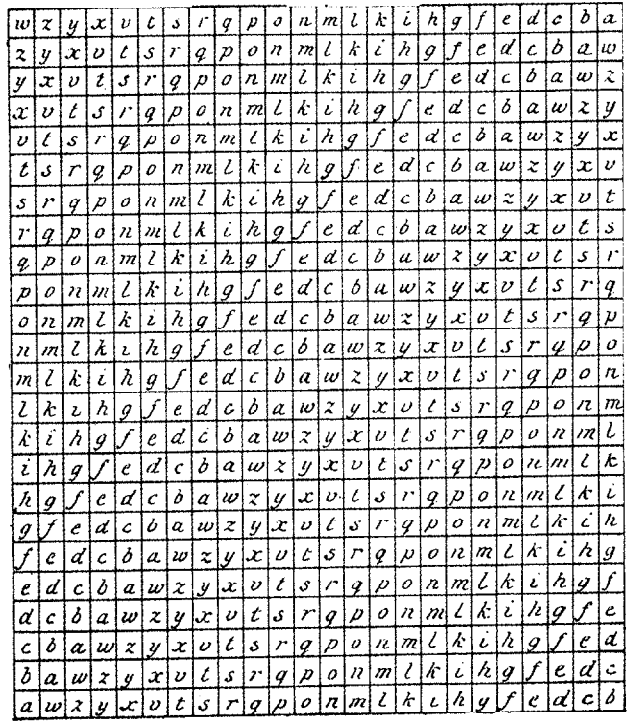
---

[16] Uno de los volúmenes, el tercero concretamente, no ha sido descriptado hasta 1996, labor que llevó a efecto Thomas Ernst, profesor de la Universidad de Pittsburgh.

[17] El duque Augusto de Brunswick, con el seudónimo de *Selenus*, compuso una extensa obra titulada *Criptomentycis et cryptographiae Libri IX*, publicada en Luneburgo en 1624.

[18] Este último criptoanalista, François Viète, perlustró los escritos secretos cambiados entre la corte española y los jefes de la Liga. Ante esta situación Felipe II, dejándose llevar de las corrientes de la época, supuso que en la corte francesa tenían al diablo a su servicio y acusó a Viète de nigromancia y sortilegio ante el Tribunal Eclesiástico de Roma, pero por fortuna el galo no tuvo que realizar grandes esfuerzos para sincerarse, y la ridiculez de la acusación fue notoria.





Polygraphia del abad Juan Tritemio

la cifra era antigua y habían fallecido muchos de sus ministros y mudado otros de destino, sino también que se hallaba divulgada, por lo que no convenía al buen éxito de los negocios. De él se conocen ocho códigos generales y varios particulares, como los seguidos con el duque de Alba, el conde de Monteagudo, don Francés de Alba, don Gueran d'Espes, etc.[19].

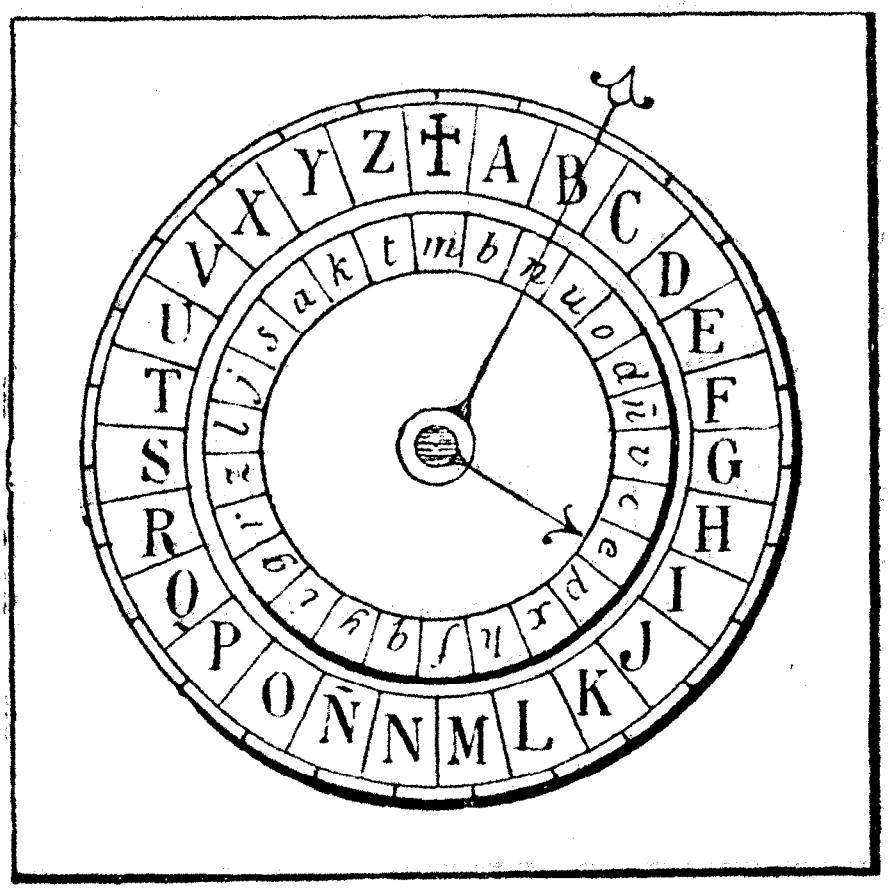
A partir del siglo XVIII decae el empleo de la escritura secreta, desapareciendo la elegancia, la uniformidad y la belleza antes empleada en la construcción de documentos cifrados, en los cuales se utilizan con valor de elementos criptográficos tanto signos anulantes, inertes, repetidos, obligados y nulos, como letras, números y signos convencionales de difícil interpretación[20].

Etapa contemporánea

Durante el siglo XIX se produce la consolidación del sistema de transposición. Destacan las figuras del científico británico Charles Wheaststone, el almirante inglés Francis Beaufort, Friedrich Kasiski -oficial prusiano que publicó en 1863 en Berlín *Las escrituras secretas y el criptoanálisis*-, Félix Marie Delastelle, el marqués Gaetan de Viaris, Etienne Bazeries -conocido criptógrafo que desentrañó diferentes nomenclatores confeccionados por personajes históricos, como Francisco I, Francisco II, Enrique IV, Mirabeau y Napoleón[21], Auguste Kerckhoffs -autor de un libro esencial publicado

[19] FERNÁNDEZ DE PALENCIA, Diego: *Historia del Perú*. Sevilla, 1571. En nuestro país, este es el primer estudio sobre materia criptográfica. En el capítulo 52 describe la composición de diferentes tintas simpáticas, analiza varios sistemas y explica diversos métodos empleados en la composición de textos cifrados. Más tarde encontramos a TAMAYO DE VARGAS, Tomás: *Cifra, contracifra antigua y moderna,* 1612; RODRÍGUEZ, Cristóbal: *Biblioteca Universal de la Poligrafía Española*. Madrid, 1738 (el tema de la criptografía está tratado de forma exigua; TORRUBIA, José: *Centinela contra francs-massones, discurso sobre su origen, instituto, secreto y juramento; descúbrese la cifra con que se escriben*. Madrid, 1752 (es una obra muy temprana sobre el método masónico); MARCOS BURRIEL, Andrés: *Paleografía española.* Madrid, 1758; OLOD, Luis de: *Tratado del origen y arte de escribir bien.* Barcelona, 1768; MÁRTIR ANGLÉS, Pedro: *Prontuario orthologi-graphico*. Barcelona, 1742; MARTÍ, Francisco de Paula: *Poligrafía o arte de escribir en cifra en diferentes modos.* Madrid, 1808.
Archivo de la Real Sociedad Económica Matritense (ARSEM), leg. 436/24. En el año 1854, a petición de Francisco Val, se intentó establecer una cátedra de poligrafía dependiente de la Sociedad Económica Matritense de Amigos del País, pero el dictamen final de la comisión encargada de debatir el tema es contrario a la solicitud formulada.

[20] LOHMANN, G.: "Cifras y claves indianas. Claves provisionales de un estudio sobre criptografía indiana", en *Anuario de Estudios Americanos*, XI (1954), pp. 285-380 y "Documentos cifrados indianos", en *Revista de Indias*, 15 (1955), pp. 255-282).Los métodos empleados en tierras americanas difieren poco de los utilizados en la Península, y es que la génesis de la criptografía indiana hay que localizar la en suelo hispano. Fue necesario tomar una serie de precauciones para evi-



Criptógrafo Wheatstone

en 1883, *La cryptographie militaire*, y de un tratado de volapuk, una lengua artificial, del tipo del esperanto, que ya ha caído en el olvido pero que en aquellos años logró un gran éxito-, y el coronel austriaco Fleissner.

El período de mayor esplendor en la historia de la criptografía americana se produjo durante la etapa de la emancipación, en la que los principales métodos empleados fueron: la escritura invisible por empleo de tintas simpáticas, cifrado mediante el sistema de diccionario y de nomenclátor, procedimiento de transposición -fundamentalmente el método de rejilla simple- y claves de sustitución simple a un solo alfabeto[22]. Resulta interesante comprobar que el empleo de los sistemas criptográficos estaba bastante difundido, aunque eran arcaicos y elementales, tanto en el bando realista como en el de patriotas americanos; características, en cierto modo, similares a las adquiridas por los métodos utilizados en la Península[23].

A continuación, el impulso decisivo a la criptografía fue proporcionado por las dos Guerras Mundiales, al igual que a las técnicas criptoanalíticas, acuciados los gobiernos por los grandes intereses en juego. En ellas, además de los escritos, se utilizaron entre otros métodos: la radio para cifrar avisos, la ocultación de informes bajo inocentes diseños y la traducción del mensaje a un lenguaje o idioma poco habitual antes de criptografiarlo[24]. No se puede

---

tar que ciertos despachos importantes cayeran en manos de corsarios o de enemigos. De ahí, que la documentación, en múltiples ocasiones, estuviese confeccionada mediante claves, pues no era suficiente enviarla por triplicado o cuadruplicado, si no iba cifrada. Hay claves usadas por los virreyes y otras altas jerarquías de la Corona, y otras utilizadas por las órdenes religiosas o simples particulares para comunicarse entre sí desde distintos lugares de las Indias o bien de la Península. Entre ellas son conocidas las utilizadas por Colón, Hernán Cortés, Luis de Velasco, Ruiz de Apodaca, Francisco de Toledo, Juan de Tejada, etc.

[21] Napoleón fue muy aficionado a las cifras. Utilizó diversos sistemas basados en el método de Richelieu y también en la asignación de símbolos numéricos a grupos de una o más letras.

[22] BAKULA, J.M.: *Apuntes de historia, criptografía y diplomacia de la emancipación.* Lima, 1949. Aquí se analizan las claves empleadas por figuras tan conocidas como Sucre, San Martín, Bolívar, O'Higgins, Santander, Carrera y Ricafort.
En relación a la independencia de Filipinas respecto a España (año 1898) es interesante la colección de legajos conservados en el Instituto de Historia y Cultura Militar (antiguo Servicio Histórico Militar). Concretamente resulta notable toda la correspondencia mantenida entre el Gobernador General de Filipinas y el Ministro de Ultramar del Gobierno español entre 1893 y 1898 (sección Ultramar, signs. 5.321.10, 5.322.06, 5.332.08, 5.322.12, 5.324.23 y 5.324.56).

[23] En el Archivo del Palacio Real de Madrid se conserva una relevante y destacada colección de documentos cifrados relativos a los reinados de Alfonso XII (fondo: Alfonso XII, claves y cifras, cajón 18/2) y Alfonso XIII (fondo: Registros, signs. 6062-6078, inclusive). Por ejemplo, en este último fondo se pueden localizar tanto criptogramas y cifras mantenidos entre la reina María Cristina y su hijo Alfonso XIII, como cifras particulares sostenidas entre la Reina Regente con su madre Isabel o con diversos ministros y embajadores.

[24] En la I Guerra Mundial se utilizaron en Europa indios navajos norteamericanos en las líneas telefónicas de campaña, lo mismo que en el Pacífico durante la II Guerra Mundial. Hay que advertir que sólo hablan el navajo unas decenas de miles de personas que viven en el altiplano del Colora-

olvidar toda la serie de claves y códigos empleados en el espionaje y contraespionaje y así, por ejemplo, durante la II Guerra Mundial en Gran Bretaña había más de treinta mil personas asignadas a la tarea de cifrar y perlustrar.

Un importante avance de la criptografía lo supone la invención de máquinas con dispositivos ex profeso para cifrar y descifrar automáticamente toda clase de mensajes, v. gr.: la *Hagelin C-48*, ideada en 1940; la *Enigma*, construida por los alemanes durante la II Guerra Mundial; la *Colossus,* inventada por los ingleses en 1943 y considerada como precursora de los ordenadores electrónicos modernos; y la *Magic*, creada por los norteamericanos para descifrar el código *púrpura* japonés. Es el paso de la criptografía *manual* o *de lápiz y papel*, según la define Andrea Sgarro[25], a la *mecánica.*

A comienzo de los años 50 se produce un cambio fundamental en la práctica de la criptografía. La comercialización de los primeros ordenadores y la potencia de cálculo que aportaron hizo surgir métodos de cifrado que se basan en la dificultad computacional de su vulneración. El ordenador ha revolucionado las técnicas criptográficas en razón de su enorme capacidad y de la gran rapidez con que trata la información. De este modo, se puede recurrir a claves de complejidad ilimitada, creándose infinitos criptosistemas.

Sin embargo, conviene recordar que entre los materiales empleados para este menester han tenido una enorme importancia los teletipos con mezclador por cinta perforada, con serie aleatoria, es decir, configurada por una gama de signos elegidos al azar. De este modo, producen el combinado o mescolanza entre las letras en claro y los símbolos de la cinta aleatoria, proporcionando un codificado que sirve tanto para perforar una cinta como para remitir directamente al circuito. El grado de fiabilidad criptográfica que confieren es bastante elevado, aunque, en contrapartida, se necesita que los corresponsales dispongan de la misma cinta y que ésta no se utilice más que en una sola ocasión, cifrando cada mensaje con un tramo distinto de la misma[26].

En este siglo la criptografía ha avanzado con pasos de gigante. Utiliza ya instrumentos matemáticos de enorme sofisticación, considerándose como el padre de la criptografía teórica moderna a Claude Shannon, quien en 1949

---

do, siendo incluso muy difícil de pronunciar para cualquiera que no sea un indígena. Luego, en 1960, las tropas irlandesas que formaban parte de una expedición de Naciones Unidas a Africa tuvieron una idea muy parecida: emplearon el irlandés para comunicarse.

[25] SGARRO, A.: *Códigos secretos.* Madrid, 1989, p. 83.

[26] *Reglamento, enlace y transmisiones*, 1980, pp. 80-81.

publicó un interesante artículo científico, *Communication theory of secrecy systems*. En vista de que las matemáticas han hecho su entrada triunfal en la criptografía, no debe sorprendernos que, al igual que existen teoremas de álgebra o de geometría, existan también teoremas de criptología, por ejemplo: si se emplea un cifrario con clave no reutilizable, la secuencia de las letras o de las cifras que componen el criptograma será totalmente casual y, por sí mismo, y a falta de la clave, no ofrece información alguna sobre el contenido del mensaje de origen[27].

Tampoco se puede olvidar el sistema de la *criptofonía*[28], consistente en proteger las conversaciones telefónicas ocultando o enmascarando las voces de los interlocutores. Una máquina de cifrar, el *mezclador* o *modulador*, transforma las señales de origen convirtiéndolas en un sonido ininteligible e incoherente. Luego, otra máquina, el *demodulador*, se encarga de rectificarlas en salida, donde se encuentra el receptor autorizado. Ahora bien, es frecuente que los mezcladores sean rígidos, es decir, que no dispongan de clave, con lo que cada sonido *claro* se transforma siempre de la misma manera. Esto significa, por consiguiente, que el cifrario utilizado es degenerativo. Sin embargo, estos mezcladores pueden resultar muy útiles en algunas circunstancias de tipo *táctico*, pero si unos perlustradores profesionales pudieran apoderarse de cintas con la grabación de dichas conversaciones y pudieran analizarlas, el cifrario terminaría siendo descubierto; a largo plazo los mezcladores de clave fija no son recomendables. Una protección prolongada de una línea telefónica requiere de un cifrario *estratégico*, con un elevado número de claves.

Consideraciones finales

Hasta bien entrado el siglo XIX la criptografía militar se limitó, básicamente, al empleo de comunicaciones enviadas por correo o por emisarios especiales, y no era tan fácil sorprender o interceptar los criptogramas como en tiempos posteriores que se transmitieron, en su mayor parte, por líneas telegráficas, y luego telefónicas. Además, al tener que intervenir mayor número de personas con este motivo, el enemigo podía establecer una derivación y enterarse de los partes que circulaban, y aun expedir criptogramas

---

[27] CABALLERO, P.: *Introducción a la criptografía*, Madrid, 1996. En este estudio el autor aporta, además, una abundante bibliografía.

[28] Los medios utilizados para cifrar la voz o el sonido, en general, se denominan *criptófonos* o *secrá-fonos*, mientras que los empleados en textos escritos se llaman *criptógrafos*.

falsos si el método elegido no ofrecía suficientes garantías de seguridad, como se realizó en la Guerra de Secesión norteamericana[29]. Por consiguiente, la criptografía militar adquirió una importancia capital debido a la misma facilidad de las comunicaciones, que llevaba consigo mayores probabilidades de que el enemigo se apoderase o interceptase los despachos. Eso sí, tampoco era conveniente abusar de ella hasta el extremo de desterrar el lenguaje claro, porque en muchas ocasiones era más conveniente emplearlo en campaña con preferencia. Había que tener en cuenta que no sólo la prontitud con que debía circular una orden y la falta de práctica en los telegrafistas militares, sino también la aglomeración de partes en las estaciones y otras circunstancias de índole análoga, aconsejaban el empleo del texto normal a pesar de correr el riesgo de su divulgación. Un parte cifrado que no llega a tiempo o no pueda ser descifrado por el destinatario, es igual que si no se hubiese recibido.

En atención a lo expuesto, Auguste Kerckhoffs formuló, en su obra *La cryptographie militaire*[30], una serie de axiomas a tener en cuenta en la confección de cifrarios: el sistema de cifrado debe ser impenetrable, sino en teoría, al menos en la práctica; la clave debe ser fácil de memorizar y, a la vez, fácil de sustituir; es recomendable que la operación de cifrado la realice una sóla persona; tanto el utensilio que se emplee para cifrar como los documentos necesarios para el codificado deben ser manejables para su transporte; el sistema debe ser sencillo, por lo que no se debe basar en el conocimiento de largas listas de normas ni requerir esfuerzos mentales excesivos; y en caso de que el sistema se vea comprometido, los corresponsales deben quedar resguardados de cualquier sospecha, algo esencial. Además añade que los criptogramas deben ser idóneos para su transmisión por telégrafo; lógicamente hay que actualizar este último principio y sustituir el telégrafo por los ordenadores electrónicos. Un buen cifrario no debería ser demasiado complejo, ya que de serlo, el criptólogo corre el riesgo de cometer errores, comprometiendo de este modo la seguridad de todo el sistema de cifrado. Claridad y concesión serían las dos principales cualidades que debe poseer la redacción de un buen criptograma.

Otras normas, útiles y prácticas, en la composición de los documentos cifrados son ofrecidas por J. C. Carmona[31], las cuales se reducen a los

---

[29] CARMONA, 1894, p. 159.

[30] SGARRO, 1989, p. 74. Esta obra constituye la piedra miliar de la que se puede denominar *criptografía de la época del telégrafo*. Kerckhoffs ilustra claramente la diferencia existente entre los sistemas de tipo táctico y los de tipo estratégico.

[31] CARMONA, 1894, pp. 158-159.

siguientes principios: conviene cifrar todo el contenido del criptograma, incluso los signos de puntuación -si el método lo admite-, desechando la costumbre de dejar algunos fragmentos en claro, con objeto de abreviar la operación de ciframiento; además de la dirección, que siempre ha de ponerse en lenguaje claro, también lo deben estar el lugar, la fecha y hasta la hora; la firma debe criptografiarse siempre; un criptograma no debe enviarse nunca a su destino, salvo necesidad, sin haberle descifrado por sí mismo o, mejor aún, por una segunda persona de confianza, para cerciorarse de que no incluye errores; se debe escribir con letra muy legible y separar perfectamente los grupos de letras o guarismos; y todo el material empleado para cifrar o descifrar un despacho, incluyendo los criptogramas recibidos después de descifrados, debe destruirse una vez concluidas las operaciones para que desaparezca todo rastro.

Por otra parte, la criptografía puede dividirse en estratégica y táctica. La primera consiste en garantizar el secreto de los mensajes cifrados por un largo período de tiempo, mientras que la segunda se conforma con una duración menor, la necesaria para llevar a feliz puerto una acción determinada. De ahí que en la criptografía estratégica hay que actuar con mucho cuidado y ser muy prudentes; en la táctica se pueden tomar las cosas más a la ligera, aunque todo es siempre relativo.

En la actualidad, al haber pasado del telégrafo a los ordenadores electrónicos, la criptografía estratégica ha desbordado el ámbito estrictamente militar, penetrando en los centros de cálculo, donde se custodian muchos datos reservados e incluso secretos[32]. De todas las maneras, en la carrera diplomática siempre han existido y existen hábiles funcionarios en descriptar toda clase de criptogramas, por lo que es poco menos que imposible hallar un escrito criptográfico al que, aplicando los métodos adecuados, no pueda al fin ser descifrado.

Eso sí, como se ha dejado entrever por todo lo expuesto con anterioridad, de estar en manos de militares y diplomáticos, en la sociedad moderna ha surgido la necesidad de la criptografía civil, debido al empleo de información diversa que se almacena en bancos de datos y se transmite a través de redes de ordenadores.

---

[32] *Reglamento, enlace y transmisiones,* pp. 81-85. El organigrama concerniente a la organización del Servicio de Cifra en nuestro país durante los años 80 -tanto en lo relativo a centros criptográficos y red de cifra como a las instrucciones- y al empleo de los medios de cifra puede consultarse en esta obra publicada por el Estado Mayor del Ejército.

BIBLIOGRAFÍA

AIRALDI, Gabriela: "Paleografia e criptografia nella storia genovese del Quatrocento", en *Studi e Documenti su Genova e l'Oltremare*. Génova, 1974.

ALCOCER, Mariano: "Criptografía española", *en Boletín de la Real Academia de la Historia*, CV (1934), pp. 337-460 y CVII (1935).

ARAGO, Antonio María: "Una clau criptográfica del segle XV", en *Cuadernos de Arqueología e Historia de la Ciudad*, 12 (1968).

BAKULA, Juan Miguel: *Apuntes de historia, criptografía y diplomacia de la emancipación*. Lima, Imprenta Torres Aguirre, 1949.

BARDIN, E. A.: *Dictionnaire de l'Armée de terre*, Saint-Cloud, Imp. Belin-Mandar, 1841.

BAZERIES, Etienne: *Chiffres de Napoleon*, Fontainebleau, 1896; *Etude sur la criptographie militaire*, París, 1900.

BEAUFORT, Francis: *Cryptography. A system of secret writing*, Londres, 1870.

BENDONIN, R.: *Elements de cryptographie*, París, 1946.

BLUM, A., "Les chiffres de Colomb", en *Studi Colombiani*, II.

BREMOND, Charles: *Les écritures secrètes et les encres mystérieuses dites symphathiques*. París, Albin Michel, 1919.

CABALLERO, Pino: *Introducción a la criptografía*. Madrid, Ra-Ma, 1996.

CANDELA, Rosario: *Chiffre militaire du commandant Bazeries*. New York, Cardanus Press, 1938.

CARMONA, J. C.: *Tratado de criptografía con aplicación especial al Ejército*. Madrid, Sucesores de Rivadeneyra, 1894.

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

COLLON, August: *Etude sur la cryptographie*. Bruxelles, 3 vols., 1899.

CONDE, Rafael: "Una clave criptográfica relacionada con la germanía valenciana", en *Saitabi*, XXVIII (1978).

CORTÉS, Josefa y PONS, Vicente: "Una clau criptográfica d'Alfons el Magnànim per a la guerra amb Castella (1429)", en *Saitabi*, XXXVI (1986).

COSTAMAGNA, Giorgio: *Tachigrafia notarile e scritture segreti medioevali in Italia*. Roma, 1968.

CRYPTO 83: *Advances in cryptology: proceedings of Cripto 83*. New York, Plenum Press, 1983.

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

DELASTELLE, Felix Marie: *Traité élémentaire du cryptographie.* París, 1921.

DEVOS, J. Paul: *Les chiffres du Philippe II (1555-1598 et du Despacho Universal durant le XVIe siécle.* Bruselas, Academie de l'Histoire de Belgique, 1950.

FEISTEL, H.: "Cryptography and computer privacy", en *Scientific American*, 228/5 (1973).

FIGL, Andreas: *Systeme des chiffrierens.* Graz, Mossers, 1926.

FLEISSNER, Eduard: *Handbuch der kryptographie.* Viena, E. W. Seidel, 1881.

FRIEDMAN, William F.: *Elements of criptanalysis.* Londres, 1924.

FRIEDMAN, William F. y FRIEDMAN, Elizabeth S.: *The Shakespearean ciphers examined.* Cambridge, Cambridge University Press, 1957.

GAINES, Helen Fouche: *Cryptanalysis.* Dover, 1956.

GALENDE, Juan Carlos: *Criptografía. Historia de la escritura cifrada*, Madrid, Complutense, 1995; "Criptografía moderna: curioso cifrario entre el obispo Diego de Muros y los Reyes Católicos", *en Boletín del Real Instituto de Estudios Asturianos*, 144 (1994); "Introducción a la criptografía histórica", en *Boletín de la Sociedad Castellonense de Cultura*, LXIX/4 (1993); "La correspondencia cifrada del embajador Lope de Soria", en *Hispania*, LII/181 (1992); "La escritura cifrada durante el reinado de los Reyes Católicos y Carlos V", en *Cuadernos de Estudios Medievales y Ciencias y Técnicas Historiográficas*, 18-19 (1993-94); "Un diplomático español en la Europa del siglo XVII: Diego de Saavedra Fajardo y su clave criptográfica con Felipe IV", en *Murgetana,* 89 (1994).

GALENDE, Juan Carlos y SALAMANCA, Manuel: "El arte de escribir cifrarios en tiempos del emperador Carlos V", en *Actas de las IX Jornadas Nacionales de Historia Militar.* Sevilla, 1999 (en prensa).

GARCIA ROURE, Jacobo: *Diccionario de frases militares para abreviar y cifrar las comunicaciones postales y telegráficas entre las autoridades del Ejército.* Madrid, Tip. Juan Pérez Torres, 1915.

GARDNER, Martin: *El idioma de los espías.* Madrid, Zugarto, 1991.

GIOPPI, Luigi: *La criptografía.* Milán, Hoepli, 1896.

GIVIERGE, Marcel: *Cours de cryptographie.* París, Berger et Levrault, 1925.

GÓMEZ DEL CAMPILLO, Miguel: "De cifras", en *Boletín de la Real Academia de la Historia.* 129 (1951), Madrid.

GREENWOOD, Gareth: *Códigos y claves secretas: criptografía en Basic.* Madrid, Anaya, 1986.

JAKUBOWICZ, Daniel y LEHNING, Herve: *Matemáticas para la información personal*. Barcelona, Masson, 1985.

HEUSCH, Waldor de: *Les opérations en campagne autrefois et aujourd'hui*. Bruselas, Imp. Tr. Rein, 1888.

HULME, F. Edward: *Cryptography; or the history, principles and practice of cipher-writing*. Londres, 1898.

IRIGOIN, J.: *Déchiffier les écritures effacées*. París, 1988.

JOSSE, Henry: *La cryptographie et ses applications à l'art militaire*, Revue Maritime et Coloniale. París, 1885.

KAHN, David: *The codebrakers*. New York, Macmillan, 1967 (reed. en 1996).

KASISKI, Friedrich: *Die Geheimschriften und die Dechiffrierkunst*. Berlín, 1863.

KERCKHOFFS, Auguste: *La cryptographie militaire ou deschiffres usites en temps de guerre*. París, Journal des Sciences Militaires, 1883.

KLUBER, Johann L.: *Kryptographik, lehrbuch der Geheimschreibekunst*. Tubingen, J. C. Gotta, 1809.

KONHEIM, Alan: *Cryptography: A primer*. New York, A Wiley-Inter Science Publication, 1981.

LACROIX, P.: *La Cryptographie ou l'art d'écrire en chiffres*. París, 1858.

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

LANGIE, Andre: *Cryptography*. Londres, Enoch Pratt Library, 1922.

LANGIE, Andre y SOUDART, A.: *Traité de cryptographie*. París, Alcan, 1925.

LAURENT, M. Hyacinthe: *Innocent VI (1352-1362). Lettres secrétes et curiales publiées*. París, E. de Boccard, 1959-60.

L'ESPRIT, Adolphe: *Elements de cryptographie*. París, 1889.

LOHMANN, Guillermo: "Cifras y claves indianas. Claves provisionales de un estudio sobre criptografía indiana", en *Anuario de Estudios Americanos*, XI (1954); "Documentos cifrados indianos", en *Revista de Indias*, 15 (1955); "Documentos cifrados relativos al Perú en la época del virreinato", en *Revista Histórica*, XII (1955-56).

LORENZO CADARSO, Pedro Luis: "Los documentos cifrados en la corte de Fernando VI (1746-1759), en *Espacio, Tiempo y Forma*, serie III, 1999 (en prensa).

LOSADA, Fernando: *Manual práctico de telegrafía militar*. Madrid, Librería de Hernando y C^{a}, 1886.

MACBETH, James: *Cryptography*. London, 1922.

MANSFIELD, Louis C.: *The solution of codes and ciphers.* Londres, A. Maclehose and CO, 1936.

MARTANS, H.: *Tratado de criptografía.* Lima, 1958.

MARTÍ, Francisco de Paula: *Poligrafía ó arte de escribir en cifra en diferentes modos.* Madrid, 1808 (reed. en Valencia, Librerías París-Valencia, 1993).

MARTÍNEZ ORGA, Vicente: *Criptografía: la ocultación de mensajes y el ordenador.* Madrid, Siglo Cultural, 1986.

MEISTER, Aloys: *Die Geheimschrift im Dienste der päpslichen Kurie von ihren Anfängen bis zum ende des XVI Jahrhunderts.* Paderborn, F. Schöningh, 1906; "Zur kenntnis des venetianischen chiffren wesen", en *Historische Jahrbuch,* XVII.

MIGNE, Jacques Paul: *Dictionnaire de paléographie, de cryptographie, de dactylogie.* París, 1854.

MILLIKIN, Donald: *Elementary cripography.* New York, University Bookstore, 1943.

MOREYRA, Carlos Alberto: *Los criptogramas de Santa Teresa.* Córdoba (Argentina), 1964.

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

OSBORNE, Herbert: *The American Black Chamber.* Bobbs-Merrill, 1931.

PERRET, P. M.: "Les règles de Cicco Simonetta pour le déchiffrement des écritures secrètes", en *Bibliothéque de l'Ecole des Chartes,* II (1890).

PRATT, Fletcher: *Histoire de la cryptographie.* París, Payot, 1940.

Recetario para tintas negras, de colores y simpáticas con un apéndice de un sistema de escritura cifrada por S. H. A., Palma, 1876.

RIOLS, J. de.: *La correspondence secrète devoilée.* París, 1881.

RICHARD, Jean, Cryptographie: *L'Histoire et ses méthodes.* XI (1961).

ROBLING, E. D.: *Cryptography and data security.* Massachusetts, Addison Wesley, 1982.

RODRÍGUEZ, Amador: *Protección de la información: diseño de criptosistemas informáticos.* Madrid, Paraninfo, 1986; "Cifrado de información para uso en modo no transparente", en *Novatica,* IX (1983).

RODRÍGUEZ VILLA, Antonio: "Escritura cifrada", en *Revista de Archivos, Bibliotecas y Museos,* 2 (1872).

ROMÁN, Ricardo: *A Paleografia e as fontes cifradas ou criptografia,* Memórias da I Semana de História, Franca, 1979.

ROSELL, Rebeca: *Las claves de Martí y el plan de alzamiento para Cuba.* La Habana, Cleveland Public Library, 1948.

SACCO, Luigi: *Manuale di crittografia.* Roma, 1925.

SARMIENTO, A.: "Servicios de escucha y cifra", en *Ejército*, Mayo-1941.

SECADURAS, José Antonio: *Sistema criptográfico "Seza"*, Madrid, 1977.

SECKEL, Emil: "Paläographie der juristischen Handschriften des 12. bis 15. und der juristischen Drucke des 15. und 16. Jahrhunderts", en *Zeitschrift der Savigny-Stiftung fur Rechtsgeschichte*, 45 (1925).

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

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

SHULMAN, David: *An annotated bibliography of cryptography.* New York-Londres, Garland Publishing, 1976.

SINKOV, Abraham: *Elementary cryptanalysis.* Nueva York, Random House, 1968.

SMITH, Lawrence Dwight: *Cryptography. The science of secret writing*, Nueva York, 1943.

TONNEAU, A.: "L'enigme des chiffres de Christophe Colomb", en *Studi Colombiani,* II.

TRASSELLI, Carmelo: "Cifrari italiani e spagnuoli del XVI secole", en *Archivi*, 8 (1941).

VALERIO, Paul: *De la cryptographie.* París, Libraire Militaire de L. Baudoin, 2 vols., 1893-1896.

VESIN, Charles François: *La cryptographie dévoilée; ou art de traduire ou de déchiffrer toutes les écritures.* Bruxelles, Libraire de Deprez-Parent, 1840.

VOLTS, James D.: *Bibliography of cryptography.* Cincinnati, 1938.

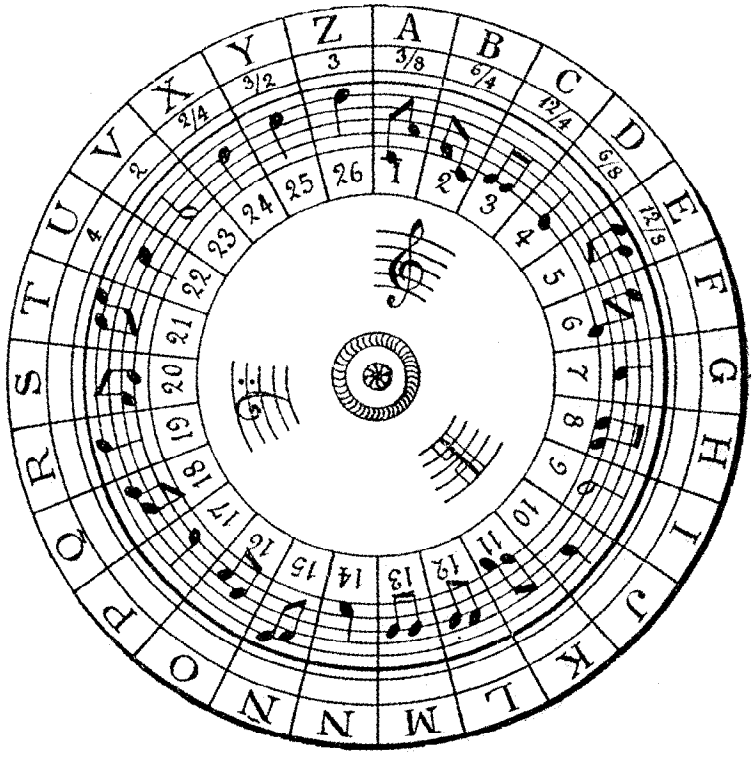
WAGNER, Fr.: "Estudien zur einer lehre der Geheimschrift", en *Archivalische Zeitschrift,* XI (1886); XII (1887) y XIII (1888).

WOLFE, Jack.: *A first course in criptanalysis.* Brooklyn, Brooklyn Collage Press, 1943.

WOLFE, James Raymond: *Secret writing*. McGraw-Hill, 1970.

YARDLEY, Herbert: *The American Black Chamber.* Indianapolis, Bobbs-Merrill, 1931.

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



Criptógrafo Guyot