DOCUMENTA & INSTRUMENTA, 4 (2006), PP. 47-59

PRINCIPIOS BASICOS DE LA CRIPTOLOGÍA: EL MANUSCRITO18657 DE LA BIBLIOTECA NACIONAL

BASIC CONCEPTS OF THE CRYPTOLOGY: THE MANUSCRIPT OF THE BIBLIOTECA NACIONAL

JUAN CARLOS GALENDE DÍAZ
Universidad Complutense de Madrid

Resumen: Conjunto de directrices y normas prácticas para el criptoanálisis de textos cifrados, principalmente de carácter histórico.
Palabras clave: Criptografía, Documento, Escritura cifrada, Paleografía.

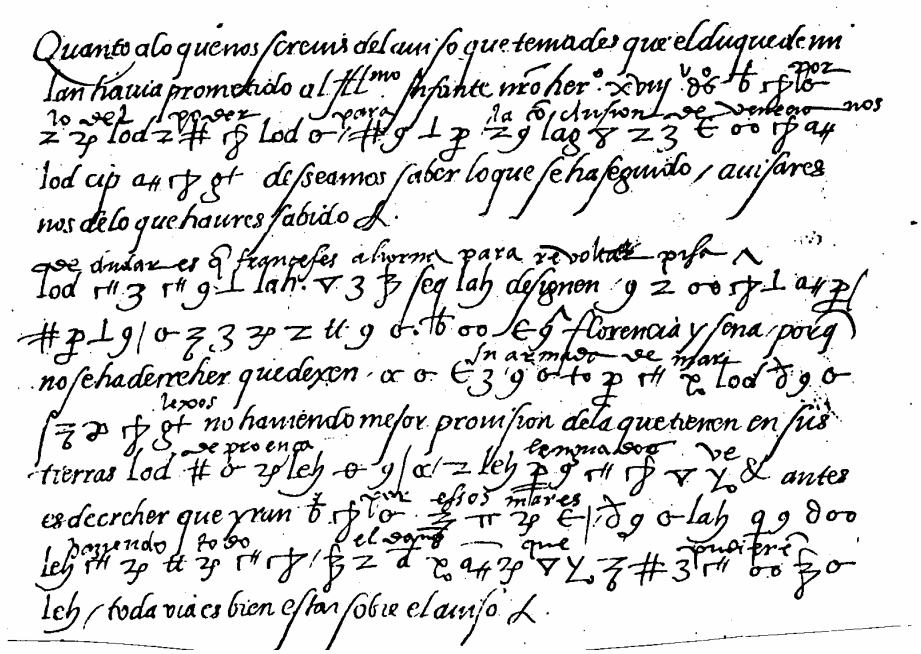
Abstract: Set of directives and practical procedure for the crytanalysis of ciphered texts, mainly of historical caracter.
Keywords: Criptogaphy, Document, Ciphered writing, Paleography.

Una de las actuaciones más dificultosas y enrevesadas que tiene que realizar el criptógrafo, quizás la mayor, es perlustrar o descriptar, ya que de ambas maneras se puede denominar la labor consistente en descifrar criptogramas desconociendo la clave[1]. No se puede olvidar que para efectuar esta tarea se requieren una serie de requisitos imprescindibles, por ejemplo: conocer la lengua en que esté escrito el texto codificado, determinar el sistema y el método empleado en su configuración, buscar la frecuencia en la aparición de las letras, establecer los signos anulantes, inertes, repetidos, nulos, etc; es decir, toda una serie de trabas que dificultan la labor criptológica (acepción, ésta última, también válida para la función apuntada anteriormente[2]). La finalidad de un criptograma, se quiera o no reconocer, es ocultar a terceras personas su contenido, siempre y cuando no sean parte de la denominada "red de cifra". Como en su momento sentenció Francis Bacon, *"una cifra perfecta no debe ser trabajosa de escribir ni de leer, debe ser imposible de*

[1] Sobre el tema del desciframiento, destacan las obras citadas a continuación: A. FIGL, *Systeme des chiffrierens*, Graz, 1926; H. F. GAINES, *Cryptanalysis*, Dover, 1956; J. IRIGOI, *Dechiffier les ecritures effacees*, Paris, 1988; D. KAHN, *The codebreakers*, Macmillam, 1967; D. MILLIKIN, *Elementary Cryptography*, New York, 1943; P. SERRANO GARCÍA, *Criptografía y perlustración*, Madrid, 1953; A. SINKOV, *Elementary cryptanalysis*, Random House, 1968; y J. WOLFE, *A first course in cryptanalysis*, Brooklyn, 1943.

[2] Un breve vocabulario técnico relativo a esta temática puede consultarse en el estudio de J. C. GALENDE DÍAZ: *Criptografía. Historia de la escritura cifrada*, Madrid, 1995, pp. 120-123.

descifrar". El triunfo del criptógrafo constituye el fracaso del criptoanalista, y viceversa[3].



Fragmento de misiva cifrada enviada por Carlos V al embajador Lope de Soria en 1523. BRAH, 9/1951

Es por este motivo, que el perlustrador tiene que echar mano de una serie de herramientas que le permitan efectuar el descriptado[4]. Entre ellas, sin duda, sobresale el conocimiento de las frecuencias, materia a tratar en las próximas líneas, ya que su comprensión resulta fundamental para el quehacer criptoanalítico, en especial para romper sistemas cifrados simétricos[5].

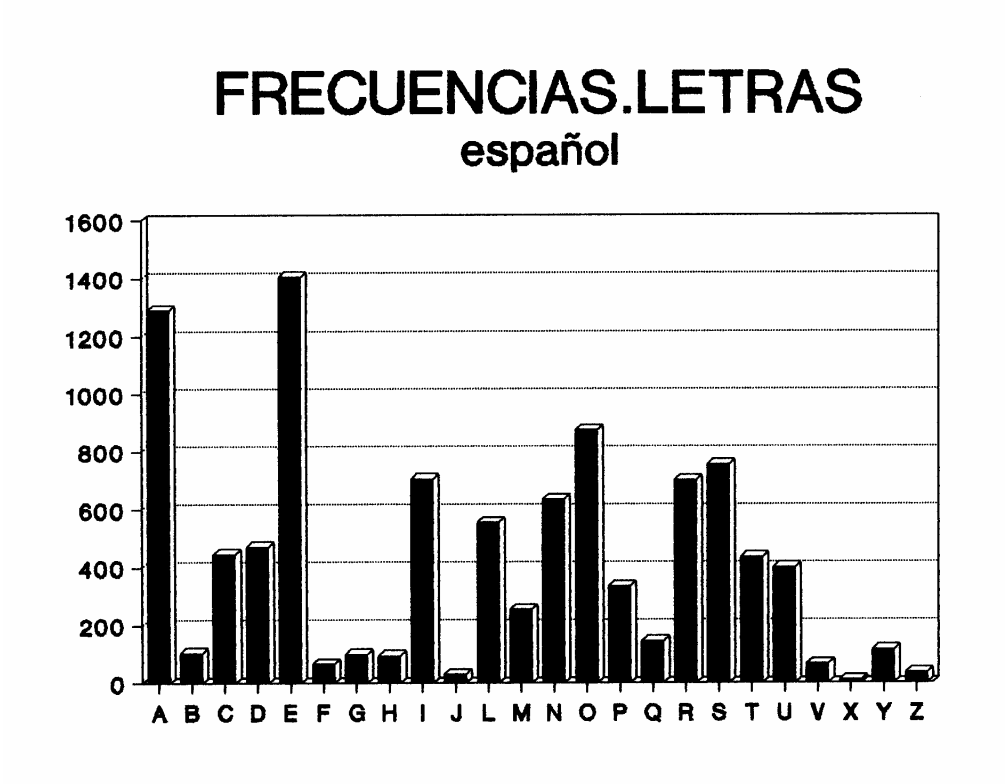
De esta manera, se puede comprobar que en los principales idiomas (italiano, francés, portugués, español, inglés y alemán), genéricamente, es la vocal *E* la que con mayor asiduidad aparece, seguida de las vocales *A* y *O*, y las consonantes

[3] Básicamente se puede conceptuar la criptografía, también denominada poligrafía y pasigrafía, como todo el conjunto de normas, técnicas, métodos y procedimientos que incumben tanto al cifrado como al descifrado de la información. J. C. GALENDE DÍAZ, "Recorrido histórico por la criptografía militar", *Revista de Historia Militar*, 88 (2000), pp. 11-12.

[4] El prelustrado general de los sistemas de sustitución se realiza, sobre todo, por dos métodos: procedimiento de la *palabra probable* –se fundamenta en el supuesto de conocer alguno de los vocablos contenidos en el mensaje- y procedimiento de los *bigramas de gran frecuencia* –basado en la apreciación de aquellos grupos de dos o más letras cuya formación es habitual y mediante la observación de las letras obligadas-.

[5] La descripción más antigua que se conoce de la perlustración mediante análisis de frecuencia se encuentra en la obra árabe del siglo IX titulada *Sobre el desciframiento de mensajes criptográficos*, cuyo autor es Abu Yusef Yaqoub ibn Ishaq Al-Kindi, padre de la filosofía islámica.

R, S, L, y N[6]. Por su parte, en la península Ibérica, la frecuencia de las letras es como sigue: *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, Ñ, W*, sin valor). Para comprobar mejor las diferencias en la repetición de las grafías, véase el siguiente diagrama:



En consecuencia, es fácilmente comprensible que sean aquellos bigramas conformados por las letras más frecuentes los predominantes: *ES, DE, EN, LA, OS, EL, AR, UE, RA, QU, RE, AS, ER, ON, ST, AD, AL, AN, AC, TE, IA, CI, NO, EC, TA, SE, DO, CO, IN, LO, IO, ND, PO, TO* y *NE*; por su parte, los trigramas más comunes son: *QUE, EST, ARA, ADO, DEL, CIO, NTE, OSA, EDE, PER, IST, NEI, HAN, RES, SDE, ESP, DES, ENC, ENT, CIA, ONS, LAS, END, ESE, ERE, DEN,*

[6] Particularizando en cada uno de los idiomas foráneos, se puede apuntar que en el alemán el orden en la reiteración de las letras es el siguiente: *E, N, R, I, S, T, U, D, A, H, L, C, G, O, M, Z, B, W, F, K, V, J* (*Q, X, Y*, sin valorar); en el francés: *E, N, R, S, A, I, T, O, U, L, D, C, M, P, V, F, Q, G, X, H, J, Y, Z* (*K, W*, sin contabilizar); en el inglés: *E, T, O, A, N, I, R, S, H, D, L, C, U, F, M, P, Y, W, G, B, V, K, X, J, Q, Z*; en el italiano: *E, I, A, O, R, L, N, T, S, C, D, P, U, M, G, V, H, B, Z, F, Q* (*J, K, W, X, Y*, sin valor); y, finalmente, en el portugués: *E, O, A, S, I, D, R, N, U, M, T, P, C, L, V, Q, H, F, B, G, J, Z, X* (*K, W, Y*, sin evaluar).

DOR y *ADO*; mientras que los tetragramas más asiduos son: *ADOS, IDOS* y *ENTE*; finalmente, los dos pentagramas más corrientes son: *ISIMO* Y *TRANS*[7].

Profundizando en el análisis de las frecuencias y de las letras obligadas en el idioma español[8], con el fin de facilitar la tarea del descriptador, hemos elaborado el siguiente decálogo[9]:

[7] Estudios complementarios a nuestra exposición, son los siguientes: H, F. GAINES, *Cryptanalysis*, Dover, 1956; J. GARCÍA CARMONA, *Tratado de Criptografía, con aplicación especial al ejército*, Madrid, 1894, pp. 203-229; K. JAMSA, *Códigos y claves secretas: criptografía en Basic*, Madrid, 1985; I. PARISI, "La correspondencia cifrada entre el rey Fernando el Católico y el embajador Joan Escriva de Romaní i Ram", *Pedralbes*, 24 (2004), pp. 55-115; P. SERRANO GARCÍA, *Criptografía y perlustración*, pp. 128-137; y M. ZANOTTI, *Crittografia. Le scritture segrete*, Milan, 1928, pp. 89-106. Es importante significar que en estas frecuencias y porcentajes influye, de manera considerable, la naturaleza del lenguaje habitual que se emplee en cada escrito: policial, militar, administrativo, literario, histórico, etc.; por esta razón no es recomendable servirse de las tablas construidas por otros criptólogos, sino que cada perlustrador ha de obtener las suyas, rectificando las posibles influencias que en las mismas hayan podido ejercer criptogramas de lenguaje peculiar.

[8] Son numerosas las páginas web de la red que abordan esta temática, entre ellas se pueden destacar las siguientes, las cuales, a su vez, tienen varios enlaces a otras de similar contenido:

www.matematicas.net/paraiso/cripto.php?id=frecuen;
www.rinconquevedo.iespana.es/rinconquevedo/criptografia/frecuencia.htm;
www.ubu.es/investig/aulavirtual/trabajos_04/Criptografia.pdf;
www.leo.worldonline.es/jlquijad/histo.htm;
www.es.tldp.org/Presentaciones/200203jornadassalamanca/jadebustos/conferencia-criptografia.pdf;
www.webs.ono.com/usr005/jsuarez/tabfrec.html;
www.criptored.upm.es/investigacion/informe.htm;
www.epsilones.com/paginas/p-laboratorio1.html;
www.giq.ifae.es/EducationalMaterial/Cripto.pdf;
www.cs.auckland.ac.nz/~pgut001/links.html;
www.ugr.es/~aquiran/cripto/cripto.htm;
www.ieee.udistrital.edu.co/concurso/ciencia_tecnologia_info_3/introduccion.html;
www.htmlweb.net/seguridad/cripto_p/cripto_princ_1.html;
www.uam.es/otros/fcmatematicas/Trabajos/Bartolome/Breve_Historia_de_la_Criptografia_Clasica.pdf;
www.textoscientificos.com/criptografia/playfair;
www.trincoll.edu/depts/cpsc/cryptography;
www.williamstallings.com/Extras/Security-Notes/lectures/classical.html;
www.ridex.co.uk/cryptology/;
www.mathcircle.berkeley.edu/BMC3/crypto.pdf;
www.cam.qubit.org/articles/crypto/intro.php;
www.cryptography.com/;
www.vectorsite.net/ttcode.html;
www.exploratorium.edu/ronh/secret/secret.html;
www.cypher.com.au/crypto_history.htm;
www.en.wikibooks.org/wiki/Cryptography:Classical_Cryptography;
www.es.wikipedia.org/wiki/Criptograf%C3%Ada;
www.uv.es/~montanan/redes/trabajos/criptografia.doc;
www.faculty.ncwc.edu/toconnor/426/426lect11.htm;
www.user.it.uu.se/~elenaf/Teaching/Krypto2003/vigenere.html;
www.cse.stanford.edu/classes/sophomore-college/projects-97/cryptography/history.html;
www.numaboa.com.br/criptologia/index.php.

1.- Los monogramas más habituales a lo largo de su historia han sido las vocales *E* (14%) y *A* (12'85%), seguidas en orden de frecuencia por la *O* (8'7%), *S* (7'55%), *I* (7%), *R* (7%), *N* (6'35%) y *L* (5'55%); a continuación, en un porcentaje inferior, aparecen la *D* (4'7%), *C* (4,45), *T* (4'35%), *U* (3'95%), *P* (3'35%) y *M* (2'55%); luego, la *Q* (1'45%), *Y* (1,15%), *B* (1'05%) y *G* (1%); en un tanto por ciento minúsculo la *H* (0'95%), *F* (0'65%), *V* (0'65%), *Z* (0'35%), *J* (0'3%) y *X* (0'1%); y prácticamente nulas la *K, Ñ* y *W*. A tenor de lo expuesto, y de los cálculos que hemos efectuado, el porcentaje entre vocales y consonantes sería 53'50% sobre 46'50% a favor de las segundas. La representación gráfica de estos datos es como sigue:

2.- Probablemente, las palabras de una única letra serán: *A, O, Y*; menos factible: *E, U, I*.

3.- La palabra de dos letras más usual es *DE*, seguida por: *LA, EL* y *EN*; además, en esta relación se pueden incluir: *ES, NO, SI, SE, LO* y *LE*.

4.- La palabra de tres letras más habitual es *QUE*, y luego: *CON, LAS, LOS* y *DEL*; asimismo, se pueden añadir los trigramas: *POR, NOS, SUS, MAS, TUS,*

[9] Para efectuarlo hemos tenido en cuenta el presentado por Martin GARDNER en su obra *El idioma de los espías* (Madrid, 1991, pp. 35-39), pero sus reglas son válidas para la escritura contemporánea, mientras que nosotros hemos adaptado las normas a épocas anteriores, es decir, para la que solemos denominar "criptografía histórica", Andrea Sgarro califica "de lápiz y papel" y David Juher, "clásica" (D. JUHER BARROT, *Introducció a la criptografia*, Gerona, 2000 y *L'Art de la comunicació secreta, : el llenguatge de la criptografia*, Barcelona, 2004

VOS, SIN y *LES*. Como se puede comprobar, normalmente, están formados por dos consonantes con una vocal intercalada.

5.- Las palabras de cuatro letras más frecuentes son: *ELLA, PARA* y *PERO*; también son ordinarias: *SUYO, SUYA, OTRA, OTRO, COMO, ESTE, ESTA, ELLO* y *TODO*.

6.- La letra más común al final de una palabra es la *O*. Luego habría que citar la *A* y la *S* (obsérvese que las tres expuestas son las utilizadas para configurar el masculino, femenino y plural), y en menor porcentaje: *E, N, R, D, L, I, Z* y *T*, en orden de frecuencia. Por su parte, las terminaciones más corrientes, con el posible margen de error que ello conlleva, son: *ADO, IDO, CION, ENTE, EMOS* e *ISIMO*.

7.- Por el contrario, la letra más reiterada al comienzo de una palabra es la *C*, seguida en orden decreciente por: *A, P, M* y *S*.

8.- Las letras que, generalmente, suelen ir dobles son: *LL, RR* y *CC*; menos frecuente: *NN, EE* y *OO*; excepcionalmente la *FF, II* y la *SS* también pueden aparecer repetidas o duplicadas, e incluso la *AA, BB, MM, PP* y *TT*.

9.- Es regla obligatoria que después de una *Q* haya una *U*, y detrás de esta vocal, muy probablemente, aparecerá una *E* o *I*, y más extrañamente una *A*. Asimismo, después de una *H, J* y *Z* siempre hay una vocal. Del mismo modo, se puede considerar como norma forzosa que la *X* vaya precedida por la vocal *E*, y así configurar la partícula *EX*.

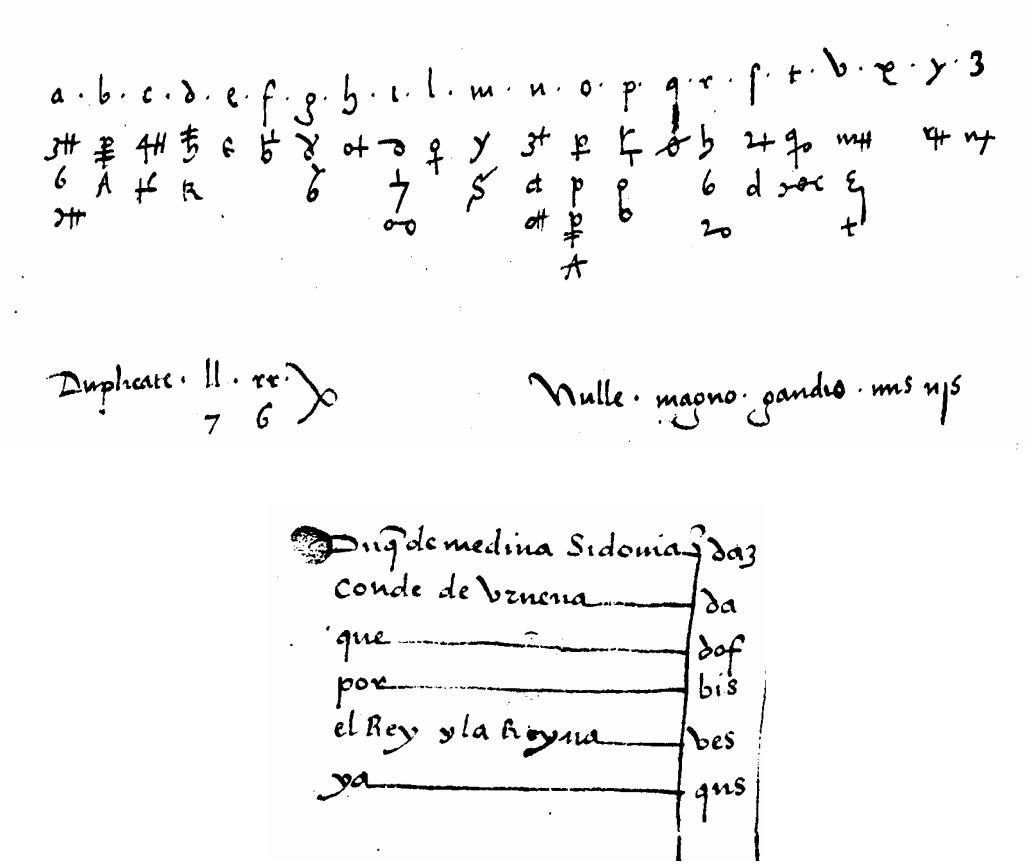
10.- Finalmente, en este último punto, expondremos diversas normas que se deben tener en cuenta a la hora de descriptar un criptograma: detrás de una *E*, la letra más probable es la *S*, al igual que después de una *O*. La letra más frecuente que sigue a la *A* es la *R*; a la *S*, la *T* y la *E*; a la *R*, la *E* y la *A*; a la *N*, la *O*; después de la *D*, la *E*; tras la *T*, la *E* y la *A*; a la *C*, la *O* y la *I*; a la *Ñ*, la *A* o la *O*; a la *X*, la *I, P* o *T*; a la *Z*, la *O* y la *A*; y por fin, a la *G*, la *A, E, R, I* o *U*.

Resulta fácil comprender la importancia que adquiere el cálculo de las frecuencias de las letras que aparecen en el criptograma con el fin de tener pistas muy valiosas para su desciframiento. Por este motivo, ya desde épocas antiguas se dedicaron obras al análisis criptográfico, siendo las primeras conocidas en occidente los tratados de Cicco Simonetta y Leon Battista Alberti, del siglo XV[10].

Para evitar este análisis estadístico de los textos cifrados, en ocasiones se han utilizado diversas artimañas, como las cuñas y los homófonos. Las primeras, conocidas también por el nombre de nulas, consisten en una serie de letras o signos carentes de significado, que no interfieren en su comprensión, pero sí dificultan

[10] Nos estamos refiriendo a las obras *Liber zifrorum* y *Modus scribendi in ziferas*, de Cicco Simonetta -secretario de la cancillería de los Sforza en Milán- y de Leon Battista Alberti -secretario de claves de la curia vaticana-, respectivamente.

considerablemente la labor descriptadora al insertarse en el texto codificado[11]. Por su parte, se denominan homófonos a aquellos símbolos que siendo diferentes representan una misma grafía[12]; estas representaciones son comunes en los nomenclatores -método preferido durante la época moderna, en detrimento de rejillas, tablas, regletas, etc.-, constituidos por un cifrario homofónico y un código de símbolos especiales secretos que corresponden al conjunto de términos o frases convenientes al uso que se destinen.



Nomenclátor seguido entre don Juan Manuel y el Marqués de Villena. BRAH, 9/15, fol. 19, fol. 19

Sin embargo, el código, como método de cifrado, tiene una serie de inconvenientes: sólo es posible transmitir aquellas palabras que tengan su correspondencia cifrada;

[11] Quizá, sea en las partes más estereotipadas de los mensajes (dirección y salutación) donde resulte más fácil identificar los elementos nulos. Todo aquello previsible es peligroso en criptografía, por lo que en ocasiones puede ser recomendable tergiversar el texto, como por ejemplo introducir errores de ortografía o utilizar términos arcaizantes.

[12] El primer cifrario homofónico del que se tiene noticia es el empleado en el año 1401 en la correspondencia cruzada entre Simeón de Crema y la corte mantuana.

el receptor debe poseer la clave completa para poder descifrarlas; en caso de modificar el código, es dificultoso y costoso cambiar el implemento; y su criptoanálisis se puede fundamentar en el estudio de las frecuencias. Por el contrario, constituye una ventaja de este método la interpretación de la información, siempre que las equivalencias codificadas sean más breves que las acepciones originales[13]. Una recomendación: un buen cifrario no debería ser demasiado complejo, ya que, de serlo, el criptólogo corre el riesgo de cometer errores, comprometiendo de esta forma la seguridad de todo el sistema de cifrado.

Sobre este último aspecto, creemos oportuno recoger los axiomas enunciados por Auguste Kerckhoffs von Nieuwenfof en su obra *La cryptographie militaire*, publicada en París el año 1883, y que transmite Andrea Sgarro[14]. Estos razonamientos se pueden agrupar en el siguiente hexálogo:

a)- El sistema de cifrado debe ser impenetrable, si no en teoría, al menos en la práctica.

b)- En caso de que el sistema se vea comprometido, los corresponsales deben quedar resguardados de cualquier sospecha.

c)- La clave debe ser sencilla de memorizar y, a la vez, fácil de sustituir.

d)- Tanto el instrumento o utensilio cifrador como los documentos necesarios para el codificado deben ser manejables para su transporte.

e)- Es necesario y recomendable que la operación de cifrado la pueda realizar una sola persona.

f)- El sistema debe ser comprensible, por lo que no se debe basar en el conocimiento de largas listas de normas ni requerir esfuerzos mentales excesivos.

No obstante, para el análisis de los sistemas criptográficos es necesario conocer su estructura, pudiéndose obtener los siguientes ataques[15]:

1. *Ataque sólo con texto cifrado*. Situación complicada y comprometida para el criptoanalista, puesto que surge cuando sólo tiene conocimiento del criptograma.

2. *Ataque con texto original conocido*. Consiste en acceder a una correspondencia de texto inicial y cifrado.

3. *Ataque con texto original escogido*. Se presenta cuando el enemigo puede conseguir, no sólo el criptograma a descifrar, sino también el cifrado de cualquier texto que él escoja; se entiende que él ya lo obtiene codificado, no que él deba criptografiarlo.

[13] P. CABALLERO GIL, *Introducción a la criptografía*,2ª ed., Madrid, 2002, pp. 9-10.
[14] A. SGARRO, *Códigos secretos*, Madrid, 1989, pp. 74-75.
[15] P.CABALLERO GIL, *Introducción a la criptografía*, pp. 8-9.

4. *Ataque con texto cifrado escogido*. Aparece en el supuesto de que el enemigo pueda obtener el texto original correspondiente a específicos textos cifrados de su preferencia.

Asimismo, conviene recordar otras directrices a tener en cuenta a la hora de componer documentos cifrados. En este caso fueron formuladas por Joaquín García Carmona, y se reducen a los siguientes principios:

. Es conveniente cifrar todo el contenido del criptograma, incluso los signos de puntuación –en caso de que el método lo admita-, desechando la costumbre de dejar algunos fragmentos en claro, con la finalidad de abreviar la operación de cifrado.

. Además de la dirección, que debe ponerse en lenguaje claro, también lo debe estar la data tópica y cronológica.

. La firma debe criptografiarse siempre.

. Un criptograma no debe remitirse nunca a su destino, salvo necesidad, sin haberlo descifrado por sí mismo o, mejor aún, por una persona de confianza, para cerciorarse de que no incluye errores.

. Se debe escribir con caracteres muy legibles y separar bien los grupos de letras o guarismos.

. Todo el material empleado para cifrar o descifrar un despacho, incluyendo los criptogramas recibidos después de descifrados, debe destruirse una vez finalizadas las tareas para que desaparezca todo rastro[16].

En conjunto, se puede mencionar que los medios utilizados para las operaciones de cifrar y descifrar la información se denominan "medios de cifra", los cuales pueden ser manuales, mecánicos, eléctricos y electrónicos, que son los más modernos, destacando entre ellos los secráfonos electrónicos para teléfonos por cable o para radio-teléfonos, 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[17].

Pero, antes de concluir, quisiéramos hacer referencia a un estudio concordante con el tema tratado. Nos estamos refiriendo a una obra, apenas conocida, que se atesora en la Biblioteca Nacional[18]: *Reglas que debe considerar quien quisiere probar a descifrar sin contrazifra, en lengua española*. Se trata de un texto anónimo, en 17 hojas de papel -tamaño cuartilla-, las cuales tienen como

[16] J. GARCÍA CARMONA, *Tratado de Criptografía*, pp. 158-159.
[17] *Reglamento, enlace y transmisiones*, Madrid, 1980, pp. 78-80.
[18] Biblioteca Nacional, mss. 18657/20.

peculiaridad que han sido arrancadas de un ejemplar a modo de "membra disiecta", puesto que se encuentran sueltas y las huellas que tienen en el lomo indican, sin lugar a dudas, que han estado encuadernadas en otros volúmenes (ahora están insertas en una carpetilla para su mejor conservación). Estos folios están numerados, con caracteres arábigos en su extremo superior derecho, desde el guarismo 344 al 361, estando todos manuscritos de forma opistógrafa hasta el 360 con tinta de color negro básicamente, ya que existen algunos fragmentos en tono sepia. De la misma manera, tampoco posee indicación alguna de fecha ni de lugar, aunque lo más probable, una vez realizado su análisis documental y examinado el lenguaje empleado, es que se hayan redactado entrado el siglo XVI, siendo el tipo de letra utilizado en su trazado la humanística cursiva corriente de esta época, de módulo mediano y bastante cuidada.

En este estudio, el anónimo autor examina de forma exhaustiva el tema de las frecuencias en el idioma español, dictando una serie de normas y reglas para la perlustración de un texto cifrado y efectuando un análisis de las probabilidades que existen en la configuración de bigramas, trigramas, etc. A modo ilustrativo, se ha creído conveniente transcribir los primeros párrafos de esta interesantísima obra:

> *"(Cruz). Reglas de descifrar.*
>
> *Quien oviere de aplicarse a negocio tan arduo ultra de la subtileza de yngenio de que a de ser dotado para con barias pruebas hallar la raíz, fundamento de su deseo deve buscar naturales principios en que fundar su yntención y estos se ofrecen con tanta copia a los que naturalmente nacieron para este ministerio, que no se pueden escrivir porque en un instante se representan en la ymaginación diversas ymágines y figuras y unos ciertos ocultos argumentos con que se biene a dar en la verdad, y quien no tubiere tal yngenio, qualquier diligencia le ara mas confuso el buscar naturales principios es que considere como abla, escrive o lee que si berdaderamente lo contempla allara en ello todas las reglas que en este particular se pueden ymaginar discurriendo por el orden y consonancia de su propia lengua el officio y disposición de cada letra el uso frequente o tardio de vocales y consonantes el fin de las letras de qualquiera dicción, el laço o desvio de una dicción con otra porque esto forzosamente a de concurrir en aquellos caracteres que se representan a los ojos con differente traxe de lo que hordinariamente se husa.*

Deve tener gran constancia en resistir a los motibos que terna de descomfianza y esperar que ha de salir con ello tiniendo en si por firme que debaxo aquel velo i tiniebla ay negocio calificado de que resultara gran gusto o honor porque en efeto con este pensamiento suben a la ymaginativa espíritus calidos que le dan el punto y temperamento necesario para decifrar, esto es lo que dixo Cicerón omnes ascendimur ad studia gloria*, y lo que se ve claramente en los poetas que sin un cierto calor no haçen buenos versos de quien dixo Obidio* est Deus in novis certo que incalescimo igne*, y sin llegar a este punto necesario de calor las obras de ymaginativa quedan ymperfectas y diminutas, y el verdadero medio de llegar a el es la consideración que digo, esta a sido bastante en cierta persona para alcançar a entender çiffras desesperadas del mismo, y propuniendole otras que en su comparación eran muy fáciles no acertarlas persuadiéndose que eran estas de poca importancia y por solo prueba a que no se podía aplicar con el fervor y consideración necesaria.*

De la regla pasada se saca que aunque un día ni otro no acierte, deve ingeniarse diversas veces sin cansar la imaginación que fatigada no obra y es necesario divertirse y recrearla por no haver estudio que mas fatigue en quantas profeçiones ay, sin dar de si fructo con que se deleite el ingenio en todo el discurso de la prueba hasta descifrarse.

Deven pasar por la fantasía varias cosas considerando la disposición de cada carácter en particular y de todos juntos y hazer entre si pruebas que podría ser este u aquel afirmándose en siete u ocho letras juntas de una dicción viendo como suenan y confforman entre si y después berlas en otra parte divididas como se juntan con otras, contar quantos caracteres diferentes tiene la cifra (...)"[19].

Tras el prólogo, se ofrecen numerosos consejos y normas a tener en cuenta en la perlustración, v. gr. los siguientes:

[19] Biblioteca Nacional, mss. 18657/20, fols. 344-346.

"(...) Si fueren mas de 22 caracteres la tal cifra tiene nullas o duplicas, o cada uno de los que sobran significa mas de una letra.

Si bieses quatro charactheres juntos de una misma forma, estas si no son nullas debes crer que es cifra de vagos o es cifra de contraposición de las 22 a beces.

En cifra de muchos charactheres si hay una raríssima, deves considerar que la antecedente no es una de estas: b, c, f, g, h, m, p, q, t*, sino de las restantes.*

Si entre dos figuras raras, o rarísimas, vieres una figura frequentíssima entiende que es vocal y no consonante porque serie haver tres consonantes.

Si una figura raríssima concurre entre dos frequentíssimas, será una de las dos vocal o ambas.

Dos charactheres diferentes siempre juntos, sospechar que son ch*; ultra de la consideración que se deve tener en la* qu*.*

Ymporta saver la persona que escrive la cifra porque mas fácilmente descubrirá por congeturas lo que ay considerando la materia que se trata y el conocimiento della, pues cada negocio tiene sus vocablos comunes.

Combiene que sea escripta la cifra por el propio que la entiende, y no copiada o recitada (...)"[20].

Finalmente, hay que significar que en la carrera diplomática siempre han existido y existen hábiles funcionarios en descifrar toda clase de criptogramas -baste recordar el Cabinet Noir de París o la Geheime Kabinets Kanzlei de Viena[21], así como las figuras de Partemio, Giovanni Soro, Philibert Babou, Mateo Argenti, Walsingham, François Viete, John Wallis, Edward Willes, Augusto de Brunswick, Antoine Rossignol, Auguste Kerckhoffs, Friedrich Kasiski y Etienne Bazeries, entre otras[22]-, por lo que puede afirmarse que, en la actualidad, es casi imposible

[20] Curiosas son también las instrucciones y disposiciones dirigidas al secretario de Felipe II, Pérez Almazán, recomendándole diversos métodos para cifrar la correspondencia. Tampoco tienen fecha ni el nombre del remitente, aunque por el lenguaje utilizado se puede pensar que se trata de un italiano o de alguien residente en Italia. Archivo General de Simancas, Patronato Real (capitulaciones con Inglaterra), leg. 2, fol. 9.

[21] Sobre el funcionamiento de estos departamentos de criptoanálisis puede consultarse el estudio de S. SING, *Los códigos secretos*, Madrid, 2000, pp. 69-70.

[22] En España, hasta que la capitalidad se traslada a Madrid en 1561, la criptografía oficialista se centralizaba en la Secretaría de Despacho Universal. Luego, este departamento se estableció en el Alcázar madrileño, bajo la dirección de Gonzalo Pérez, por entonces secretario del Exterior. J.

encontrar un escrito criptográfico al que aplicando cualquiera de los múltiples métodos perlustrativos, no pueda al fin ser descifrado[23], reflexión anticipada por Edgar Allan Poe cuando manifestó que "es dudoso que el género humano logre crear un enigma que el mismo ingenio humano no sea capaz de resolver". Por este motivo, se reconoce que la mejor manera de evitar que un criptograma sea interpretado por un extraño, a pesar de sus carencias, es utilizar en su formación el método del diccionario o tabla cifradora, cuyas claves convenidas son conocidas únicamente por los corresponsales.

C. GALENDE DÍAZ, "La correspondencia diplomática: Criptografía hispánica durante la Edad Moderna", en *La correspondencia en la historia. Modelos y prácticas de la escritura epistolar*, vol. I, Madrid, 2002, p. 154.

[23] En relación a este punto, es importante apuntar que en la criptografía contemporánea se diferencia la "estratégica" y la "táctica". Así, la criptografía estratégica consiste en garantizar el secreto de los mensajes cifrados por un largo período de tiempo, a poder ser para siempre, mientras que la criptografía táctica se conforma con una duración menor, la necesaria para llevar a buen fin el proyecto deseado, por lo que es menos ambiciosa.