HISTORIA Y CRIPTOLOGÍA: REFLEXIONES A PROPÓSITO DE DOS CARTAS CORTESIANAS

Roberto NARVÁEZ
Facultad de Arquitectura, UNAM
gogmagog@prodigy.net.mx

Introducción

Ocurre a veces que un historiador, ocupado en una investigación de archivo, fracasa en acceder al contenido de un documento por cuanto ni siquiera está seguro de poder interpretar a los caracteres o signos ante su mirada como grafemas de algún sistema de escritura común. En tales casos, los especialistas en paleografía, diplomática y disciplinas afines pueden revisar el texto en cuestión e iluminar aspectos como el agrupamiento, lugar de origen y la filiación de los tipos gráficos empleados en su composición, facilitando con ello la intelección de los términos.[1] Desde luego, siempre es probable que toda esta labor heurística termine por mostrarse inútil para garantizar la lectura. Sin embargo, desde una perspectiva científica el eventual incumplimiento de aquella probabilidad no es una razón para creer que la competencia del paleógrafo y el diplomatista, en la investigación de un fenómeno similar al considerado, ha llegado a su final. Recordemos que los métodos de la paleografía y la diplomática promueven la inferencia de hipótesis cuya meta suprema es explicar todos los aspectos problemáticos, formales y de otros tipos, en una muestra específica de escritura, y por ello, en efecto, califican de científicos.[2] Así, cuando un manuscrito es ilegible a primera vis-

[1] Luis Núñez de Contreras, *Manual de paleografía. Fundamentos e historia de la escritura latina hasta el siglo VIII*, Madrid, Cátedra (Historia. Serie Mayor), 1994, p. 50. María Belén Piqueras García, "Concepto, método, técnicas y fuentes de la Diplomática", en Ángel Rieseo Terrero (editor), *Introducción a la paleografía y la diplomática general*, Madrid, Editorial Síntesis (Letras Universitarias), 1999, p. 191-205 (198-199 especialmente).

[2] Sobre todo en tanto descubre relaciones analíticas normalmente ignoradas por la tradición normal y literaria. *Cf.* Núñez de Contreras, *op. cit.*, p. 22. Un paleógrafo debe la potencia *científica* de sus análisis al manejo lógicamente consecuente del razonamiento hipotético.

ta, diplomatistas y paleógrafos pueden juzgar probable la explicación de que su autor "así lo quiso"; y si este razonamiento prueba su validez en la solución de varios casos análogos, tiene sentido inferir un supuesto teórico general, a saber, que "el mensaje de un texto puede ocultarse por diferentes motivos y con el auxilio de diversos medios". Así, en definitiva, un paleógrafo, un diplomatista consecuente, diestro en el manejo de la lógica científica,[3] tal vez nunca será capaz de convertir un mensaje abstruso en una pieza textual fácilmente legible, pero siempre sabrá razonar hacia una explicación de que tal mensaje no sea fácilmente legible, y se trate, por tanto, de un criptograma, una cifra.

A pesar de las indicaciones precedentes, conviene entender que el asunto de la criptografía, esto es, de la escritura deliberadamente oculta,[4] supera los límites del método paleográfico por muchos y muy importantes motivos analíticos. Sería vano que un historiador, perplejo ante un criptograma, solicitase la técnica del desciframiento al paleógrafo. Éste no tiene por qué llevar su labor más allá de la identificación de sintagmas en cifra. El experto en criptogramas debe tomar el relevo en ese punto. Es un hecho, sin embargo, que a veces ni siquiera un experto conoce la técnica para penetrar o "romper" —como se dice en el argot criptoanalítico— una cifra determinada, pues hasta el momento sólo se conoce una parte de los sistemas

[3] Con esta expresión me refiero a la clase de lógica que estudia los diferentes modos de razonamiento (inducción, deducción, hipótesis, y las combinaciones de éstos) aplicados por un investigador a propósito de un fenómeno determinado. No se trata de una mera variación o desarrollo de la lógica formal o la de relativos, sino que constituye una denominación para todos los aspectos lógicos realmente discernibles en la metodología científica en general. Es una cuestión central en los debates actuales sobre la heurística, la justificación de la inducción, la naturaleza de las inferencias probabilísticas, el falibilismo epistemológico y las investigaciones del género de lógica que presumiblemente regula los descubrimientos científicos. En tales debates participan filósofos e historiadores de la ciencia, lógicos, psicólogos y especialistas en inteligencia artificial y ciencias cognitivas, principalmente; casi en todos ellos, por cierto, la fuente directa de inspiración ha sido la obra de lógicos como el estadounidense Charles S. Peirce (1839-1914). **Véase Atocha Aliseda, "Logics in Scientific Discovery", en** *Foundations of Science*, v. 9, 2004, p. 339-363; Thora Margareta Bertilsson, "The elementary forms of pragmatism: on different types of abduction", en *European Journal of Social Theory*, v. 7, 2004, p. 371-389; Jaako Hintikka, "What is abduction? The fundamental problem of contemporary epistemology", en *Transactions of the Charles S. Peirce Society*, v. 34, n. 3, 1998, p. 503-533; Ilkka Niiniluoto, "Defending Abduction", en *Philosophy of Science*, v. 66 (Supplement Proceedings of the 1998 Biennial Meeting of the Philosophy of Science Association. Part I: Contributed Papers), September 1999, p. S436-S451, y Nicholas Rescher, *Peirce's Philosophy of Science. Critical Studies in His Theory of Induction and Scientific Method*, Notre Dame (Indiana), University of Notre Dame Press, 1978.

[4] Los étimos de "criptografía" son griegos: *kryptos*, oculto, y *graphein*, escribir.

criptográficos que los hombres han empleado desde tiempos remotos. Más adelante comentaré los beneficios lógicos e historiográficos que reporta el saber esto, por lo pronto advertiré contra el despropósito clasificatorio de quienes definen a la criptografía como la ciencia exclusiva del ciframiento y desciframiento de textos (los manuales de paleografía normalmente difunden esta versión simplificadora). Propiamente, se llama criptología la ciencia que, englobando a las técnicas de la criptografía y el criptoanálisis, reconoce como su objeto a las escrituras inmediatamente ilegibles. El criptógrafo elimina provisionalmente la claridad del texto al cifrarlo, el conocedor de la clave (principalmente el destinatario del mensaje, aunque puede ser cualquier persona) se la devuelve al descifrarlo. El criptoanalista es quien, careciendo del acceso a la clave de una cifra, restituye o bien el mensaje, o bien la clave, en un proceso al que técnicamente se denomina decriptar.[5]

Indudablemente, una práctica sostenida puede fortalecer la competencia del historiador como diplomatista o paleógrafo. No veo ningún obstáculo a que por la sola constancia lograría desarrollar, igualmente, habilidades de criptólogo. La investigación histórica de la América Latina colonial ofrece numerosas oportunidades para ejercitar el desciframiento de textos. Varios autores han señalado el uso extensivo que se dio a los criptogramas en las comunicaciones de las Indias con España y viceversa. Por otra parte, disponemos de una ingente provisión de manuales e historias de la criptología que describen y enseñan a comprender los métodos de cifrado más frecuentemente utilizados desde el siglo XV hasta el XIX en muchos países europeos, africanos, asiáticos y americanos, aunque típicamente pasan por alto a los ejemplares de lo que Guillermo Lohmann Villena denominó "criptografía indiana". La clasificación de estos métodos está lejos de haberse agotado —inevitablemente

[5] En el ámbito hispanoamericano también se ha llamado a esta técnica "perlustrar", *cf.* Juan Carlos Galende, "Sistemas criptográficos empleados en Hispanoamérica", en *Revista complutense de historia de América*, n. 26, 2000, p. 58. Existen muchos manuales de historia y técnica de la criptología donde se explican detalladamente las diferencias entre descifrar y decriptar, así como la interrelación del criptoanálisis y la criptografía, por ejemplo, Simon Singh, *Los códigos secretos*, Madrid, Debate, 2000; David Kahn, *Codebreakers. The Story of Secret Writing*, New York, Scribner, 1996, revised edition; Joseph S. Galland, *An Historical and Analytical Bibliography of the Literature of Cryptology*, New York, AMS Press, 1970, y Helen Fouche Gaines, *Cryptanalysis. A Study of Ciphers and Their Solution*, New York, Dover, 1956. En la Internet se puede consultar una cantidad enorme de monografías, ensayos, glosarios y bibliografías muy útiles acerca de este tema.

crece cuando por lo menos un historiador o criptólogo profesional se dedica conscientemente a recolectarlas en los archivos—, no obstante, pienso que su estudio crítico y comparado suscita reflexiones interesantes en torno a: 1) los múltiples beneficios técnicos, heurísticos, metodológicos y conceptuales que los historiadores de la América colonial reciben cuando aprenden a identificar, distinguir y comparar los criptogramas y sistemas criptográficos representativos de la "criptografía indiana" —una división legítima de la "criptografía clásica"—,[6] así como valerse, cuando la ocasión lo amerite, de algunas estrategias criptoanalíticas básicas; 2) la forma en que un cierto manejo de la erudición, la imaginación científica y, sobre todo, el razonamiento lógico puede optimizar el aprovechamiento de un documento descifrado cuando la meta es explicar, a través de la historiografía, un acontecimiento del pasado con las mejores hipótesis, y 3) la pertinencia de renovar el proyecto de una historia de la "criptografía indiana" con dos objetivos fundamentales: primero, suplir a las historias generales de la criptología con el capítulo que normalmente falta en ellas, y segundo, enriquecer o refinar la metodología de investigación al uso para reconstruir la historia de México desde el siglo XV hasta la guerra de Independencia, cuando menos.

En las páginas restantes expongo los contenidos de mis propias reflexiones, análisis y prospectivas en relación con los tres puntos recién mencionados, partiendo de una evaluación historiográfica y criptológica de un *corpus* documental, historiográfico y hemerográfico referente a dos cartas escritas por Hernán Cortés a su procurador *ad litem* en la corte española, licenciado Francisco Núñez, una fechada el 25 de junio de 1532 y la otra el 20 de junio de 1533, ambas parcialmente cifradas.[7]

[6] Se entiende por "criptografía clásica" la que se practicó desde la Antigüedad hasta la invención y puesta en marcha de las máquinas de rotor y los sistemas automatizados de cómputo para ocultar información (por ejemplo, el DES —Data Encryption Standard— y el RSA —Rivest, Shamir, Adleman—, que se desarrollaron durante la década de 1970 para una variedad de aplicaciones militares, financieras, telefónicas, televisivas, etcétera). En criptografía, el algoritmo es la función matemática usada para la encriptación y decriptación de un mensaje. Si la seguridad de un algoritmo depende de mantener secreta la manera en que opera, el algoritmo en cuestión se califica de restringido (es el tipo de algoritmos normalmente utilizados en la criptografía clásica). Ahora bien, los criptólogos modernos enfatizan que la seguridad no debería depender de la secrecía de los métodos de cifrado o encriptación, esto es, del algoritmo, sino de la secrecía de las claves.

[7] Los originales obran en los autos seguidos en 1546 por Núñez contra el marqués del Valle, sobre un pago de devengados en concepto de gestión de negocios. Se localizan en el Archivo General de Indias, de acuerdo con Guillermo Lohmann Villena, "Cifras y claves india-

Sobre la organización y el desenlace de un concurso inusual en México

En los números correspondientes a abril y junio de 1925, los *Anales* del antiguo Museo Nacional de Arqueología, Historia y Etnografía incluyeron un ofrecimiento de 200 pesos "oro nacional" a quien consiguiera descifrar pasajes de la carta de Cortés firmada el 25 de junio de 1532 en Cuernavaca [figuras 1 y 2]. Las partes inmediatamente legibles de dicha carta habían visto ya la luz en 1915,[8] pero como los paleógrafos fallaban sin cesar en sus intentos de aclarar las restantes partes en cifra, Mariano Cuevas y Alfonso Toro —director del Museo Nacional en aquella época— juzgaron oportuno convocar a un concurso público de "descifración". [9]

El facsímil de la carta y los criptogramas que tratarían de resolver los concursantes también apareció en los *Anales*.[10] El plazo para remitir las propuestas cerraba el 11 de septiembre de 1925, pero debido a diversas circunstancias los organizadores concedieron una prórroga hasta el 31 de octubre,[11] permaneciendo inalteradas las bases de la convocatoria. Cuando el plazo se cumplió, el jurado había recibido un solo trabajo, firmado por el escritor mexicano Francisco Monterde García Icazbalceta. Los miembros del jurado eran Luis González Obregón, Nicolás Rangel y Pablo González Casanova; reunidos el 5 de noviembre en el Archivo General de la Nación, consignaron en acta oficial que Monterde merecía pública felicitación y le entregaron el premio.

En relación con los hechos que acabo de resumir sucintamente, quiero hacer varias observaciones:

1. Los paleógrafos nunca lograron penetrar "el sentido de los pasajes… en cifra" en la carta.[12] ¿Por qué? Para responder sería muy útil, quizá, contar con el relato de las dificultades insuperables que

nas. Capítulos provisionales de un estudio sobre criptografía indiana", en *Anuario de Estudios Americanos*, Sevilla, 1954, v. XI, p. 304, nota 41.

[8] Mariano Cuevas, *Cartas y otros documentos de Hernán Cortés*, Sevilla, Tipografía de F. Díaz, 1915, p. 67-77.

[9] "Convocatoria para un concurso del Museo Nacional", en *Anales del Museo Nacional de Arqueología, Historia y Etnografía*, abril a junio, época 5a., tomo I, n. 2, 1925, p. 208.

[10] Mismos tomo y número citados en la nota 9, pero en las p. 123-130.

[11] *Cf. Anales del Museo Nacional de Arqueología, Historia y Etnografía*, julio y agosto, 5a. época, tomo I, n. 3, 1925, p. 330.

[12] Véase "La carta cifrada de don Hernán Cortés", en *Anales del Museo Nacional de Arqueología, Historia y Etnografía*, julio y agosto, 5a. época, tomo I, n. 3, 1925, p. 436-443.

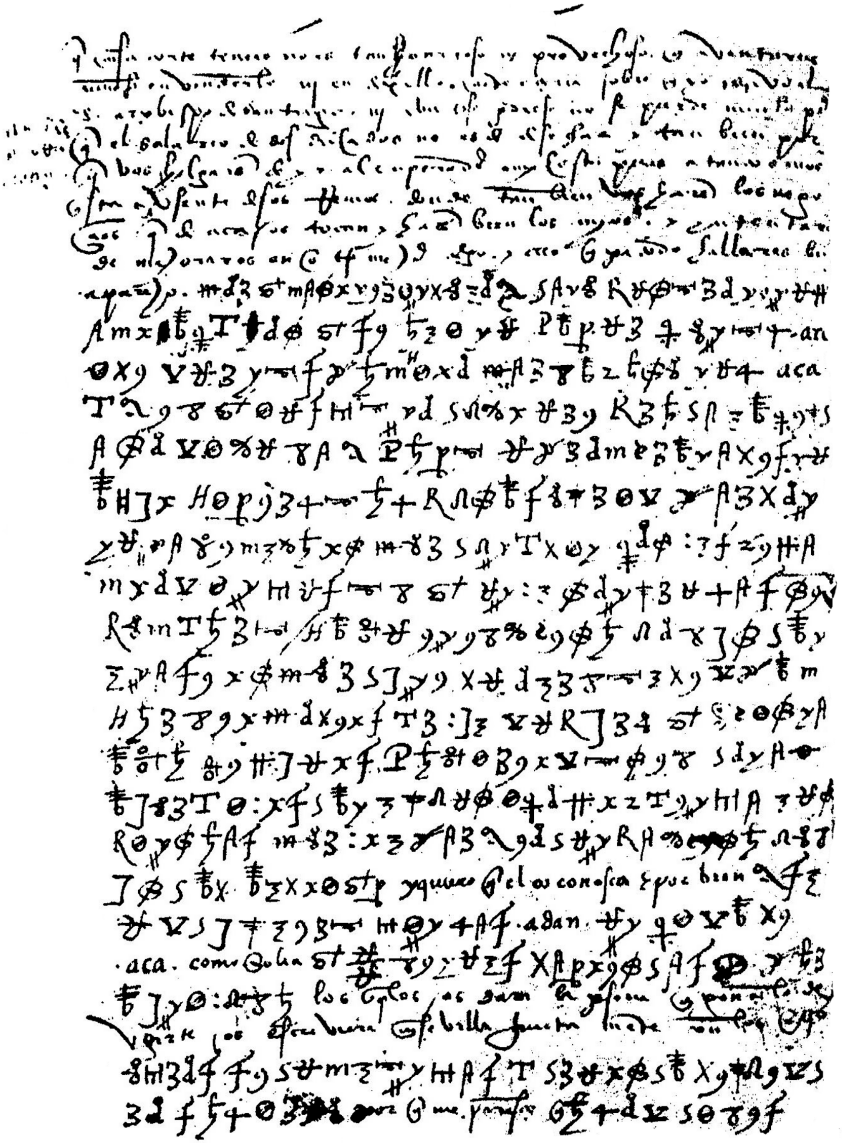

Figura 1. Detalles del facsímil 1 de la carta del 25 de junio de 1532. Fuente: "La carta cifrada de don Hernán Cortés", en *Anales del Museo Nacional de Arqueología, Historia Y Etnografía*, julio y agosto, 5a. época, t. 1, n. 3, 1925, p. 436-443

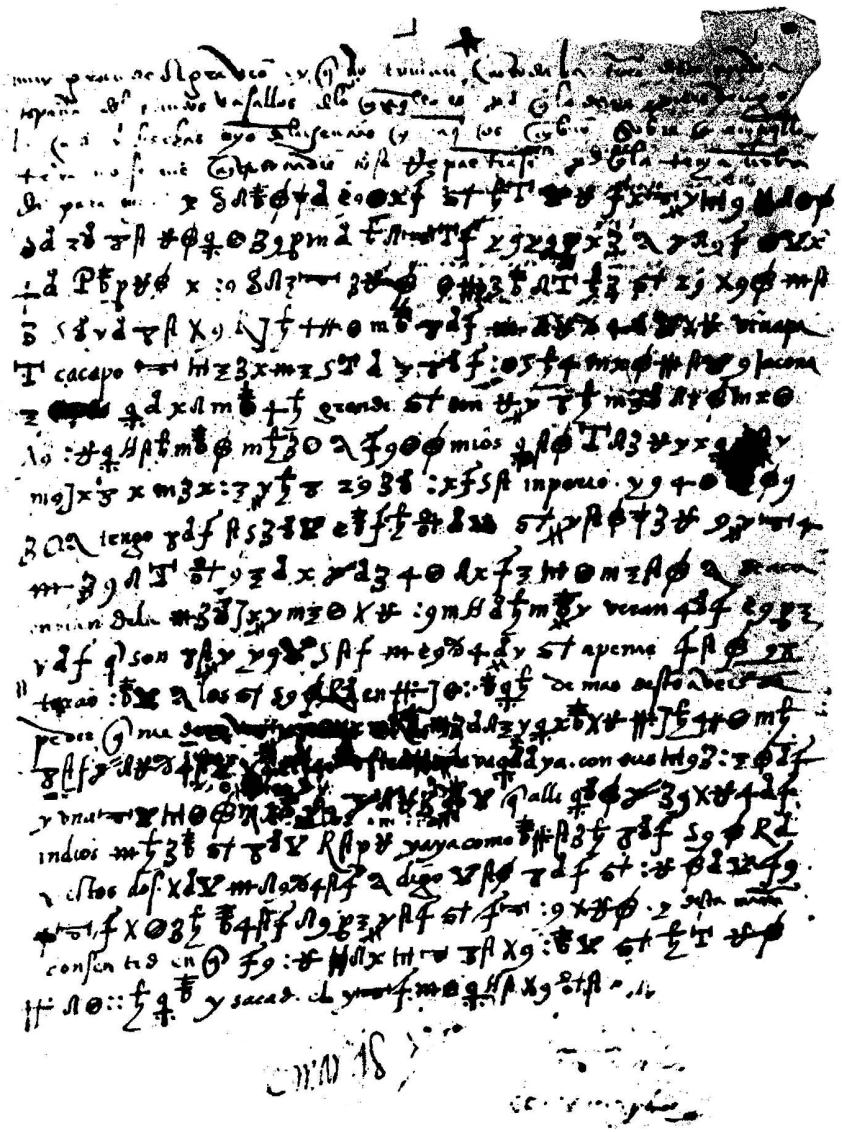

Figura 2. Detalles del facsímil 4 de la carta del 25 de junio de 1532. Fuente: "La carta cifrada de don Hernán Cortés", en *Anales del Museo Nacional de Arqueología, Historia y Etnografía*, julio y agosto, 5a. época, t. 1, n. 3, 1925, p. 436-443

abrumaron a todos los implicados; a reserva de localizarlo en algún archivo —suponiendo que existe—, podemos obtener una respuesta probable al admitir la siguiente hipótesis: esos paleógrafos no practicaron el criptoanálisis, por tanto, no supieron conjeturar que Cortés había empleado deliberadamente ciertos métodos para esconder el significado literal de los caracteres. Cortés, en efecto, se valió de un sistema criptográfico que mezcla cifras y códigos —líneas abajo explico esto con amplitud—, y para detectar siquiera esto las técnicas de la paleografía son insuficientes. He aquí una situación donde se marcan claramente, como ya señalé al introducir el presente escrito, los límites entre paleografía y criptología. Ahora, es verdad que los paleógrafos han reunido en sus clasificaciones varios signos de índole críptica. Se trata de signos complementarios o especiales de la escritura, función que asimismo cumplen los signos numerales, musicales y de puntuación, los membretes, logotipos, imagotipos y rúbricas, entre otros.[13] Un paleógrafo puede identificar sin mayores problemas cualquiera de estos caracteres en, digamos, un oficio del siglo XVI, y definirlo en atención a su operatividad en el texto; sin embargo, las cosas cambiarían radicalmente si el mismo documento estuviera compuesto en su totalidad por signos crípticos o especiales, o aún por signos todavía sin clasificar, formando un exasperante bloque de renglones en donde resulta imposible, para magnificar el embrollo, distinguir un solo espacio en blanco. El paleógrafo será capaz, entonces, de nombrar algunos caracteres, mas no de asignarles una función inequívoca en el texto. Pues el objeto de su escrutinio será una cifra, y en las cifras cada signo tiene un valor determinado de cifrado, más que una función de escritura. El valor de un signo en la cifra dependerá del método criptográfico empleado —el cual, dicho sea de paso, no siempre necesita basarse en un algoritmo para funcionar.[14] Hernán Cortés, por ejemplo, dotó

[13] Núñez de Contreras, *Manual de paleografía*, *op. cit.*, p. 159. Pedro Luis Lorenzo Cadarso, "Caracteres extrínsecos e intrínsecos del documento", en Ángel Rieseo Terrero (editor), *Introducción a la paleografía y la diplomática general*, Madrid, Editorial Síntesis (Letras Universitarias), 1999, p. 264.

[14] Es el caso de la esteganografía. Consiste en distribuir planificadamente cada letra del mensaje oculto entre las letras de un mensaje claro, de modo que la cifra ni siquiera permite sospechar su presencia en el texto (un ejemplo familiar es el acróstico). Johannes Trithemius en su *Steganographia* (escrita en 1518 pero impresa por primera vez en 1606) y Francis Bacon en su *Advancement of Learning* (1623) cuentan entre los tratadistas clásicos de la criptología que describieron este sistema, véase David Kahn, *op. cit.*, p. 132-135; Galland, *op. cit.*, p. 183, y Thomas Leary, "Cryptology in the 16th and 17th centuries", en *Cryptologia*, v. 20, n. 3, July 1996, p. 223-242.

a cada signo en su cifra de un valor por medio de la llamada sustitución homofónica, o alfabética —de la cual hablo por extenso más adelante. El paleógrafo bien puede saber que la criptografía medieval y renacentista se desarrollaron, básicamente, a partir de la sustitución de caracteres alfabéticos por otros, o por signos no alfabéticos,[15] pero ello jamás le bastará para reconocer y discernir ese género de cifras.

2. Considerando lo expresado al inicio del artículo "La carta cifrada de don Hernán Cortés",[16] la idea del concurso surgió directamente del fracaso de los paleógrafos. Francamente, ignoro si Cuevas, Toro y sus compañeros del Museo Nacional estimaron alguna vez que sería suficiente contratar un criptólogo profesional para despejar las incógnitas en la carta. En más de una embajada o secretaría de Estado pudieron haber hallado uno, justo como se podría hacer hoy. En fin, el hecho es que prefirieron la opción del concurso. Por supuesto, cuando llegó el momento de aplaudir a Monterde supusieron que habían elegido lo mejor. Pero, seamos honestos: a propósito de la organización misma del concurso "lo mejor" fue que sólo Monterde presentara un desciframiento al concluir el plazo de recepción. Y se trató de una casualidad estupenda, sin duda, pues de su verificación dependió que el concurso mantuviera los portes de un evento serio. En realidad, y para enunciarlo con un símil, Monterde ganó una carrera en la que hasta el último corredor en cruzar la meta merecía también las alabanzas y el trofeo. Me explicaré: las bases del concurso indican que se daría el dinero al "descifrador" del texto cortesiano, pero dejan absolutamente sin especificar las condi-

Guillermo Lohmann, sin embargo, invariablemente habla de esteganografía, o de "clave esteganográfica", cuando el método a describir es, en realidad, un nomenclator (del que hablaré más adelante en el texto); además, da por sentado que este sistema se basa en la "sustitución de primer grado", y que proceder con él implica utilizar unos "caracteres caprichosos" a manera de"signos esteganográficos" para la sustitución, todo lo cual es sumamente discutible. Véase Guillermo Lohmann Villena, "Cifras y claves indianas. Capítulos provisionales de un estudio sobre criptografía indiana", *loc. cit.*, p. 373 (a propósito del método criptográfico entregado por la corona española a los comisionados para la pacificación de América en 1820).

[15] Núñez de Contreras, *Manual de paleografía*, *op. cit.*, p. 180. Véase también la entrada "Criptografía" en Germán Bleiberg (director), *Diccionario de historia de España*, Madrid, Alianza Editorial, 1979, 2a. edición corregida y aumentada, 3 tomos, t. 1, p. 1022-1023. En Bizancio existió un sistema criptográfico en el que un numeral griego remplazaba una letra con la mitad del valor numérico por 2 (*iota*, 10, se vuelve *epsilon epsilon*, 5 y 5. Véase Alexander P. Kazhdan (editor in chief), *The Oxford Dictionary of Byzantium*, New York-Oxford, Oxford University Press, 1991, 3 v., v. 1, p. 561.

[16] Véase nota 12.

ciones de aceptación de los trabajos; ahora, estas condiciones, tomando en cuenta el objetivo de éste y todos los concursos de su clase, naturalmente se deben referir a los tiempos de entrega, no a determinados aspectos analíticos o formales de cada ensayo criptoanalítico. Por consiguiente, resulta curioso leer en la base 4: "El trabajo de descifración que apruebe el jurado…".[17] Cuando se rompe una cifra, la solución prueba su validez automáticamente si la clave exhumada —representante de tal solución— faculta la lectura de algo hasta entonces ilegible. No hace falta, por tanto, la aprobación de ningún juez. En todo caso, el único "juez" de que un criptograma es un algoritmo genuino y, por tanto, admite una solución dependiente del sistema de su formación, es el propio criptoanalista. Esto es obvio; la primera lectura de un documento descifrado, en efecto, siempre la realizará quien lo haya criptoanalizado, a menos que no lo haya criptoanalizado. Monterde supo que había encontrado "la" solución en cuanto juzgó evidente la coordinación semántica de los fragmentos descifrados con las partes inmediatamente legibles (más abajo comento detalladamente su estilo de criptoanálisis). Y es totalmente probable que otros individuos, enterados del concurso, criptoanalizaran la carta con tesón hasta lograr igualmente la solución, aunque demasiado tarde para poder "competir" contra Monterde.

La práctica del criptoanálisis reclama, normalmente, una concentración prolongada, pero tratar de hacerlo contra el reloj debe causar una gran ansiedad, en especial para quien no acostumbra lidiar con textos en cifra. Esto explica el que varios interesados en concursar solicitaran una prórroga (quizá entre ellos se encontró el propio Francisco Monterde). Sin embargo, conceder la prórroga no evitó que los jueces recibieran apenas un trabajo. Pero supongamos que hasta seis o siete individuos hubieran entablado una verdadera "competencia" al remitir sus trabajos dentro del plazo. Los jueces atienden los envíos por separado, luego los comparan mutuamente y, al final, se ven obligados a reconocer que la coherencia lingüística general del mensaje descifrado jamás varía, o, para expresar lo mismo en términos diferentes, que los concursantes restituyeron sin excepción la clave de la cifra cortesiana —es forzoso admitir como válida esta condición hipotética, pues de otro modo nos queda sos-

[17] Véase nota 9.

pechar que por lo menos uno fue plenamente incapaz de apreciar la calidad heurística del desafío. En tal situación, y recordando lo estipulado en la base 4 ¿a quién le otorgarían los jueces el premio? Mi lector acordará conmigo, espero, en que lo sensato es responder: a la persona cuyo ejercicio criptoanalítico llegó a sus gabinetes en primer lugar. Mas ¿cómo satisfarían, después, las reclamaciones legítimas de los demás contendientes? Pues cada uno de éstos, por excelentes razones algorítmicas, estaría totalmente convencido de que su solución a los criptogramas cortesianos es la solución.

Así, como dije, para los convocantes resultó una casualidad magnífica, sumamente oportuna, el que únicamente Monterde presentara la "descifración" (si bien lo que Monterde hizo fue, propiamente, decriptar la clave). Sin embargo, no hay motivos para dejar que la fortuna, en cualquier época y país, prodigue un desenlace apropiado a los concursos de criptografía; lo absolutamente necesario es comprender la primacía del factor tiempo: en efecto, toda cifra real creada por un humano es penetrable por cualquier individuo racional, observador y tenaz, aunque bien le podría tomar semanas, meses o años lograrlo. Por tanto, constituye una muestra de previsión criptológica el que los organizadores de un concurso de criptografía típicamente ofrezcan tres premios, cuando menos, para otorgar a los tres concursantes más rápidos en superar el desafío.[18]

3. Los miembros del jurado calificador "aprobaron" el trabajo de Monterde aplicando unos criterios cuya impertinencia es manifiesta cuando se trata de criptoanálisis. A este respecto ya expuse algunas consideraciones críticas en el subapartado precedente, pero es interesante comentar, desde una perspectiva historiográfica y ya no criptológica, otras consecuencias que derivan de lo mismo. Analizaré con ese fin el "Acta del jurado" leída el 5 de noviembre de 1925 en el Archivo General de la Nación.[19]

[18] En el siglo XXI, cuando casi todo lo referente a la criptología, incluso desde un punto de vista historiográfico, se hace y transmite a grandísimas velocidades por medios cibernéticos —especialmente vía Internet—, todavía se observa este fundamental detalle de organización. Así ocurre, por ejemplo, con el concurso al que anualmente convoca la Universidad de Southampton (véase Graham A. Niblo, "The University of Southampton National Cipher Challenge", en *Cryptologia*, v. 28, n. 3, July 2004, p. 277-286) y la compañía RSA Security, véase su sitio web http://www.rsasecurity.com. En ambos casos las soluciones deben enviarse por Internet, y los tres primeros en hacerlo reciben un premio.

[19] "La carta cifrada de don Hernán Cortés", *loc. cit.*, p. 437-439.

Después de las formalidades iniciales de rigor, dicho documento se compone de cinco puntos. En el segundo se declaran los criterios decisivos para galardonar a Monterde, y se compone, a su vez, de cinco incisos. El inciso *a* registra que la "descifración", "desde el punto de vista paleográfico como… criptográfico", era difícil por cuanto las partes en cifra de la carta cortesiana están escritas con "caracteres y signos del siglo dieciséis, y no haber, para la interpretación de estos últimos, claves especiales, ni manuscritas ni impresas".[20] Ahora bien, esto es totalmente falso, lo era ya en 1925, según argumentaré más adelante. Pasemos al inciso *b*; leemos que la dificultad crecía porque en la cifra "todas las palabras [están] aparentemente unidas entre sí, lo cual [requiere] una suma atención, a fin de no confundir la última parte de un vocablo con el principio del siguiente";[21] en la cifra de Cortés los signos, y todavía no las palabras, están evidentemente unidos entre sí; las palabras aparecen cada una con su inconfundible inicio y fin con posterioridad al criptoanálisis, momento en el cual, si se tiene precaución lexicográfica, no hace falta poner "suma atención" para marcar los espacios entre ellas.

Los incisos *c* y *d* son complementarios y se refieren a la dificultad ocasionada por haberse utilizado "cuarenta y nueve signos para representar distintamente una misma letra; así, la a está escrita de tres maneras diferentes; la b de dos, la c de dos, la d de dos", etcétera, agregándose la "promiscuidad de los signos empleados, pues indistintamente se usó de caracteres matemáticos o alfabéticos de las lenguas copta, griega y latina, cosa desusada en las claves modernas".[22] [figura 3] Para empezar, Cortés usó un alfabeto o tabla de homofonías de cincuenta signos, no cuarenta y nueve. En segundo lugar, la "promiscuidad" de que vale hablar se acusa mediando siempre una estimación de las frecuencias de repetición de todos los caracteres en el texto, los del alfabeto críptico y los del alfabeto latino claro, para lo cual es irrelevante de dónde procedan los signos de la cifra. De hecho, se debe entender que la efectividad de un método criptográfico como el que usó Cortés —muy socorrido en su época, según veremos— aumenta, o se espera que aumente, cuando el criptógrafo inventa los signos de sustitución.

[20] *Ibid.*, p. 438.
[21] *Ibid.*
[22] *Ibid.*

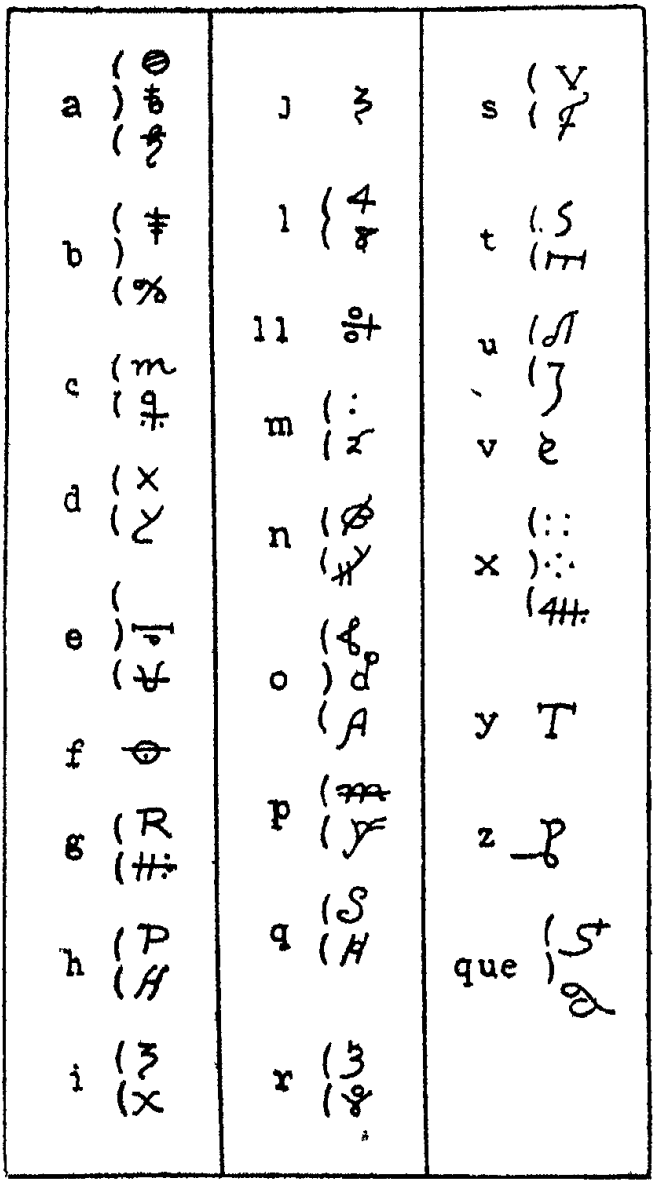

Figura 3. La tabla de correspondencias usada por Cortés, restituida por Francisco Monterde. Fuente: "La carta cifrada de don Hernán Cortés", en *Anales del Museo Nacional de Arqueología, Historia y Etnografía*, julio y agosto, 5a. época, t. 1, n. 3, 1925, p. 438

Por último, en el inciso *e* se reseñan los problemas para examinar la carta en la reproducción fotográfica que facilitó Mariano Cuevas.[23]

En el cuarto punto del Acta los jueces relatan que Monterde les expuso su procedimiento analítico de viva voz, y cómo ellos "comprobaron" el funcionamiento de la clave leyendo de nuevo "parte de la carta cuyo texto había consignado por escrito en su […] descifración". Trataban de decir que juzgaron positivamente descubierta la "clave" cuando notaron que a cada signo críptico restituido por Monterde corresponde una letra del alfabeto latino. Sin embargo, es fácil advertir la completa falta de sentido criptológico en una "comprobación" semejante (recordando, además, lo dicho en el subapartado 2 *supra*), dado que la clave restituida permite la lectura inmediata del texto antes velado; en otros términos, la clave perpetra su función evidentemente, por tanto, basta con ella misma para "juzgar" si merece una calificación aprobatoria en cualquier certamen de criptología.

Los jueces destinaron el quinto punto a consignar una pública felicitación a Monterde, alegando una doble motivación de fondo: "[…] por habernos revelado el texto misterioso de esta carta" y "[…] por haber formado la clave que sin duda servirá, en lo futuro, para descifrar muchos documentos de la misma índole, relacionados con nuestra historia y que deben existir en los archivos, casi abandonados por las dificultades que presenta su lectura". Como han contribuido a demostrarlo algunos historiadores de España y de la América Latina colonial, en especial Guillermo Lohmann, los archivos están llenos de documentos total o parcialmente cifrados que acusan un enorme parecido con la carta cortesiana de 1532 (y también con la del 20 de junio de 1533, según argumento *infra*). La explicación es que toda esa muestra documental fue cifrada con el mismo método general. En este sentido científico es apropiado decir que la carta de Cortés forma una clase junto a otros muchos textos "de la misma índole". Sin embargo, es precipitado aseverar que la "clave" de las cifras en aquella carta particular brindará el acceso a otros documentos de su clase. Tengamos en cuenta que los archivos históricos de Inglaterra, por ejemplo, también deparan continuamente a los investigadores el hallazgo de materiales criptográficos. Ahora, es un

[23] *Ibid.*

hecho que ninguna letra o palabra se presenta con la misma frecuencia en los idiomas inglés y español. Existen razones lingüísticas y filológicas que hacen vano esperar el funcionamiento de una clave diseñada para ocultar —por vía de la sustitución homofónica— textos españoles en el ocultamiento de textos ingleses. Como sea, limitándonos a cifras en español podemos negar validez al principio hipotético de que una clave inventada circunstancialmente por un individuo, en una época determinada, para hacer funcionar un método general de cifrado, permitirá vencer la resistencia de cifras inventadas en épocas y circunstancias diferentes por otros individuos con el mismo propósito. En el capítulo siguiente, donde reviso con pormenor el criptoanálisis de Monterde, abundaré sobre estos aspectos teóricos de la criptología.

En resumen, me parece que hubiera sido muy conveniente a Mariano Cuevas, Alfonso Toro y sus compañeros del Museo Nacional asesorarse por un criptólogo profesional, o bien informarse muy escrupulosamente sobre los propósitos, los usos, el estatuto científico y, sobre todo, la historia de la criptología, antes de organizar un concurso marcado por despropósitos e inconsistencias desde sus bases. En cuanto a los jurados, pienso que un conocimiento insuficiente de la criptología les impidió apreciar y exponer el genuino alcance de lo realizado por Monterde. Pero, veamos, a propósito de ese "genuino alcance" recién mencionado, ¿cuál era el grado de conocimiento del propio Francisco Monterde? El hecho de que decriptase las cifras no implica que fuera capaz de nombrarlas y caracterizarlas técnicamente. Es lícito suponer que no lo era, pues en el caso contrario lo hubiera dejado patente en sus exposiciones metodológicas ante el jurado, de las cuales, por cierto, habría debido inferir una buena razón para justificar el hecho de que su decriptación fuera incompleta —pues no consiguió interpretar el significado de los términos codificados en el texto.

El criptoanálisis de Francisco Monterde

Como ya lo he señalado, Hernán Cortés empleó un sistema criptográfico basado en la sustitución homofónica y en la codificación de nombres propios. Monterde triunfó al analizar la cifra por sustitución homofónica, si bien jamás mencionó a sus jueces esta definición

técnica. Y tampoco explicó técnicamente la intervención de un código en la carta. Esto implica que no estaba en posición de valorar un hecho fundamental desde las perspectivas histórica y criptológica, a saber, que Cortés eligió una de entre las múltiples estrategias a su disposición para obstruir la intelección automática de sus letras. Ahora bien, el conquistador de México no estaba satisfecho con la mera sustitución homofónica, ¿por qué decidió complementarla precisamente con un código? Como bien lo interpretaron Monterde y sus jueces, las palabras legibles pero no inmediatamente significativas en la parte cifrada de la carta (are, aca, adan, beril) son títulos arbitrarios para nombrar a ciertos individuos,[24] a los cuales nadie, salvo Cortés y su procurador *ad litem*, podría identificar mediando la correspondiente decodificación. Pero decodificar no es lo mismo que descifrar o decriptar; producir un código es un acto diferente al de formar una cifra; muchas consideraciones algorítmicas son dispensables cuando la elección es codificar palabras, o grupos de palabras, con otras palabras (inventadas o corrientes) en lugar de letras o signos. En definitiva, pues, Cortés decidió usar un método que combina la sustitución homofónica y la codificación por una razón criptológica elemental: dificultar lo más posible la lectura total de su mensaje a quienes pudieran interceptarlo. Su intención era repeler el "ataque criptoanalítico" —otra expresión de argot— blindando a su texto por cuenta doble. En 1925 Francisco Monterde abatió la coraza del cifrado, pero la del código fue lo bastante sólida para incitarlo a la rendición. Así, como dije, la decriptación de Monterde terminó siendo parcial.

En un apartado posterior sugiero que hay suficiente información historiográfica para formular hipótesis que permiten traducir los nombres propios codificados en la carta de 1532, por lo pronto comentaré el estilo de analizar frecuencias adoptado por Monterde.

Ante todo, conviene saber que el así denominado "análisis de frecuencias" es el auxiliar técnico fundamental en el estudio de cifras clásicas generadas por sustitución homofónica, o alfabética. La forma básica de instrumentarlo es la siguiente: contar la frecuencia de las letras en la cifra y después asociar a cada una, por adivinación o hipótesis cuidadosamente valoradas, la letra correspondiente del texto claro, esto es, no cifrado. Se sustenta en el principio teórico de que

[24] Véase "La carta cifrada de don Hernán Cortés", *loc. cit.*, p. 442.

ciertas letras y combinaciones de letras, en cualquier muestra de lenguaje escrito conocido, suelen repetirse con frecuencias variables. Las letras más repetidas en el idioma español son las vocales. Para comprobar esto basta revisar un fragmento de la primera novela en español que se tenga a la mano: pronto se observa que las letras e, a y o se distinguen en cada renglón más a menudo que la t, la w y la x, digamos. Y si extendemos la revisión a cien o ciento treinta novelas, detectaremos en casi todas aquella misma distribución relativa de las letras.[25] Otro tanto sucede con pares o tríos de letras comúnmente utilizados en nuestra lengua con diferentes funciones, por ejemplo, be, ca y que. En criptoanálisis, a los pares de letras más frecuentes se los llama bigramas, y a los tríos trigramas.[26]

Ahora bien, es posible criptografiar un texto de modo que las propiedades citadas del lenguaje, observadas en textos claros, se observen asimismo en el criptograma. Es evidente, sin embargo, que reproducir de tal manera el patrón de las frecuencias en el texto cifrado facilita el criptoanálisis. Para evitar esto, los criptógrafos de las épocas previas al advenimiento de las máquinas cifradoras, la cibernética y la informática se valieron de la homofonía, esto es, asignar a capricho un mayor número de signos para sustituir, o representar, a cada letra o grupo de letras (bigramas, trigramas, etcétera) de más frecuente aparición. Esto contribuye a nivelar la distribución de las frecuencias relativas, en detrimento de cualquier eventual ofensiva criptoanalítica.[27]

[25] Digo casi porque es posible escribir una novela completa sin utilizar alguna o varias vocales en absoluto. Se trata de un método para crear un tipo especial de texto, el denominado lipograma.

[26] La explicación registrada más antigua del análisis de frecuencias —quizá de cualquier forma de criptoanálisis— data del siglo XI, y fue obra del polígrafo árabe Abu Yusuf Yaqub ibn Is-haq ibn as Sabbah ibn 'omran ibn Ismail Al-Kindi. Sobre las contribuciones árabes al criptoanálisis y al establecimiento del vocabulario criptológico general (términos tales como algoritmo y cifra) a partir de sus desarrollos del álgebra y la teoría del número, véase Ibrahim A. al-Kadi, "Origins of Cryptology: The Arab Contributions", en *Cryptologia*, v. XVI, n. 2, April 1992, p. 97-127, y "Cryptography and Data Security: Cryptographic Properties of Arabic", en *Proceedings of the Third Saudi Engineering Conference*, Riyadh, Saudi Arabia, November 24-27, 1991, v. II, p. 910-921.

[27] Durante el Renacimiento muchos criptógrafos europeos desarrollaron esquemas para repeler el análisis de frecuencias, destacando, junto al uso de homofonías (o sustitución monoalfabética), la sustitución polialfabética —esto es, el uso de muchos alfabetos escogidos más o menos al azar— y la sustitución poligráfica (en la cual se trata a los bigramas y trigramas, en lugar de letras sencillas, como unidades de sustitución). Para una descripción del algoritmo que se forma por sustitución, véase Thomas Jakobsen, "A Fast Method for Cryptanalysis of Substitution Ciphers", en *Cryptologia*, v. XIX, n. 3, July 1995, p. 265-274.

Tal fue la táctica que siguió Cortés. Monterde ignoraba que anticipar esto es una función elemental del razonamiento estadístico para un criptoanalista, con todo, salió avante procediendo así:

> Primero conté el número de signos diferentes que figuran [en la cifra]. Son cuarenta y nueve.[28] Como el total de las letras del alfabeto no llega sino a menos de la mitad de ese número, supuse que habría letras representadas con dos signos y como éstos rara vez se repiten en el mismo orden, comprendí que una misma palabra podía escribirse de distintos modos.
>
> A continuación separé, aproximadamente, por medio de rayas verticales, los grupos de signos que forman palabras y observé cuáles signos figuran en todos esos grupos, para saber qué signos correspondían a las vocales. Obtuve doce. Había, pues, algunas vocales representadas con más de dos signos. Como, de éstas, las que se repiten con mayor frecuencia son la *e*, la *o* y la *a* —según el cálculo hecho por mí, sobre un total de cerca de quinientas (500) letras, en la parte paleografiada—, hice el mismo cálculo sobre un número igual de signos, y así averigüé cuales podrían corresponder a esas vocales.
>
> Sustituyendo los signos por vocales conocidas y el resto por puntos, fui descifrando las palabras cortas en que entran aquellas vocales, poniendo consonantes entre los huecos.
>
> Las primeras palabras que logré descifrar fueron *sean* y *tengo*. Estas me sirvieron de base para conocer nuevos signos, nuevas consonantes, que anoté en otras palabras, hasta completar la clave.

Como vemos, Monterde jamás consigna un solo término técnico de la criptología. Le bastó con observar, contar signos crípticos y letras, y conjeturar cada posible sustitución hasta voltear, por decirlo así, las cosas del revés al derecho. Y por más que haya procedido como un aficionado, su criptoanálisis es admirable. Con todo, su método de análisis exhibe aspectos realmente singulares, los cuales conviene revisar para darse cuenta de que los criptoanalistas, profesionales o no, conciben, desarrollan y justifican sus particulares "ataques" en estilos diferentes. Apuntaré brevemente los dos aspectos que más impacto causaron en mi atención:

1. Monterde percibió el recurso a las sustituciones tras observar que los signos de cifrado en la carta superan a las letras del alfabeto español en una proporción de 2 a 1, por lo menos. Esto lo forzó a suponer que hasta dos signos podían ocultar a cada grafema, en

[28] De hecho, son cincuenta. La misma tabla de correspondencias que ofreció Monterde lo revela, véase la figura 3.

consecuencia, que cada palabra (exceptuando los códigos) repetida en el texto una vez —cuando menos— admitía lógicamente un cifrado con signos alternativos (considerando estrictamente la proporción fijada de sustituciones potenciales) para esconder a cada una de sus letras. Así comprendió que "una misma palabra podía escribirse de distintos modos".[29] En esta altura de su análisis, lo más interesante es que tuviera por obvia la función cifradora positiva de todos los signos en el texto. Y es que Cortés, en efecto, no utilizó los denominados nulos,[30]es decir, signos inútiles al propósito del ocultamiento pero que se insertan en la cifra con dos objetivos básicos: darle una traza de colosal intrincación y, tanto más importante, frustrar con "ruido" el análisis de frecuencias. En relación con esto, sin duda resultó venturoso el que Monterde no estuviera entrenado técnicamente en criptoanálisis, pues el recelo contra los posibles nulos le hubiera generado, quizá, dudas ante sus iniciales hallazgos. A esto seguiría la desconfianza generalizada en su método y, cosa más grave, una pérdida de tiempo.

2. Monterde ubicó a las letras que más se repiten en el texto (las vocales *a*, *e* y *o*) tomando como muestra exclusiva del idioma español a las fracciones legibles en la carta de Cortés. Procedió justo a la inversa de como lo haría un criptoanalista profesional, quien siempre estima el principio general de la distribución relativa de las letras en el español para deducir que, en una muestra escrita de ese lenguaje, la misma distribución relativa se habrá de mantener (de acuerdo con lo ya explicado).[31] Al ignorar tal principio y, por tanto, no poder imaginar una razón analítica para manejarlo como una suerte de premisa mayor en una inferencia deductiva, Monterde gastó esfuerzo y tiempo en cálculos estadísticos, obteniendo una información válida para sentar el hecho descubierto (la distribución relativa de las letras en el español) por el análisis de la carta, como un caso del cual deducir una regla general.[32] Es verosímil atribuir a

[29] Si bien las combinaciones, por supuesto, son limitadas.

[30] Al menos es lo que observo en las reproducciones que se contienen en el artículo "La carta cifrada de don Hernán Cortés", *loc. cit.*

[31] Pero esto no siempre sucede con la misma flagrancia: los mensajes breves normalmente exhiben una variabilidad mayor.

[32] Para un análisis estadístico de las frecuencias relativas absolutas y por grupos de las letras en el español, realizado con base en un texto de 60 115 letras, véase Wayne G. Barker, *Cryptograms in Spanish*, Aegean Park Press, Laguna Hills, CA., 1986. Sobre la singular interpretación que el matemático inglés Charles Babbage (1792-1871) daba al fenómeno de las

esta circunstancia, por encima de cualesquiera otras, el que su criptoanálisis tuviera que prolongarse tres meses.

Nombre y caracterización técnica del método criptográfico de Cortés

Por su forma, organización y contenido, la carta cortesiana con cifras de 1532 puede suscitar el interés de historiadores, diplomatistas y criptólogos. En cuanto a su contenido, se disciernen tres designios primordiales de Cortés que regulan la pertinencia, la extensión y el sentido de cada mensaje incluido:

a) Explicar plenamente a Francisco Núñez (su primo, además de procurador)[33] los motivos por los cuales deberá seguir encargándose de todos sus asuntos jurídicos ante la corona.
b) Insistir a Núñez que viaje a donde sea preciso con el fin de mantenerse próximo al emperador y los asuntos de la corte y poder, así, mantenerlo informado sobre los altos personajes y los acontecimientos políticos de mayor trascendencia, en particular dentro del ámbito imperial de Carlos V. Por otra parte, Cortés fija las cantidades de dinero que se habrán de gastar en salarios —comenzando por el del mismo Núñez—, regalos para funcionarios influyentes y otras partidas.
c) Instruir jurídicamente a su procurador para obrar de modo que la Corte acepte compensarlo con cierto número de pueblos si, en un afán de "agraviarlo", decide reducir sus mercedes en Oaxaca separando de ellas la villa de Antequera, en la cual unos oidores habían puesto a vivir cristianos españoles con el franco propósito de afectar a Cortés —según lo que éste clamaba— en sus derechos señoriales.

La materia de los fragmentos criptografiados por extenso en la carta se distribuye bajo los rubros b y c. Ninguno de los nombres en código, por cierto, se mezcla con la cifra referente al tema de Ante-

frecuencias relativas de las letras en un idioma, considerándolo como una suerte de constante legalista, véase Ian Hacking, *La domesticación del azar*, Barcelona, Gedisa, 1991, p. 96-100. Babbage siempre mostró un interés muy vivo por la criptografía, y se acepta, en general, que los principios fundamentales del ordenador digital fueron establecidos por él.

[33] José Luis Martínez, *Hernán Cortés*, México, FCE/UNAM, 1993, p. 373.

quera.[34] Como haya sido, lo cierto es que Cortés —valga repetirlo— combinó el cifrado por sustitución homofónica y la codificación. En lo particular, eligió un sistema de correspondencias destinado a prevenir la reproducción de la misma distribución de frecuencias relativas que se observa en las letras de un texto claro y, por tanto, dificultar la penetración de la cifra con el análisis de frecuencias. Ahora bien, desde un punto de vista historiográfico (referente a los métodos de la investigación histórica, en especial) estoy convencido de que resulta muy ilustrativo aprender a nombrar y caracterizar técnicamente a ese sistema. Se trata de un *nomenclator*. Fue llamado así por el oficial encargado de anunciar, en los palacios regios, los títulos de los dignatarios visitantes.[35] Se construye con un diccionario de nombres en código y unas tablas donde se establece la correspondencia homofónica o alfabética de unos signos arbitrarios con cada letra o grupo de letras (bigramas, trigramas) del alfabeto claro.[36] La serie de correspondencias que Francisco Monterde restituyó no es, pues, hablando con rigor técnico, la "clave" de la cifra cortesiana, como repiten sus jueces, sino la tabla de sustituciones homofónicas con la que se guió Cortés —o la persona que propiamente inscribió al dictado los mensajes cortesianos con el cálamo—[37] para formar los criptogramas.

En Europa, el primer manual de criptografía vio la luz en 1379.[38] Contiene la descripción del sistema nomenclator clásico, mismo que

[34] Quizá una hipótesis adecuada para explicar esto es la siguiente: juzgando por la fecha de composición y el contenido de la carta misma, el asunto de Antequera se hallaba en una instancia jurídica más bien avanzada, cuando su solución favorable a Cortés ya dependía estrictamente de la capacidad litigante de Núñez; de poco le servía al conquistador, entonces, repartir dádivas a hombres poderosos para granjearse su intercesión. Una exposición sencilla de los pleitos de Cortés relativos al valle de Oaxaca se puede ver en José Luis Martínez, *Hernán Cortés*, *op. cit.*, p. 635-636.

[35] La voz *nomenclator* (en ocasiones *nomenclador*) proviene del latín *nomenclātor*, *nomenclatōris*, compuesto con la raíz del arcaico *calare*, "llamar". Joan Corominas, *Diccionario crítico etimológico de la lengua castellana*, Madrid, Gredos, 1976 (3a. impresión de la 1a. edición 1955-57), v. III, p. 520.

[36] David Kahn ofrece la siguiente definición: "[…] a system that was half a code and half a cipher […]. It usually had a separate cipher alphabet with homophones and a codelike list of names, words, and syllables", en *Codebreakers*, *op. cit.*, p. XV (pero también sugiero consultar las p. 107, 115-119, 150-151, 173-74, y 190-192).

[37] El cálamo, también conocido como peñola o pluma, es el instrumento que los escribanos utilizaron durante siglos en ambos lados del Atlántico. Normalmente lo fabricaban los mismos escribanos a partir de plumas de gallo o de oca. *Cf.* Vicenta Cortés Alonso, *La escritura y lo escrito. Paleografía y diplomática de España y América en los siglos XVI y XVII*, Madrid, Instituto de Cooperación Iberoamericana, 1986, p. 2.

[38] Es una colección de cifras concebidas por Gabriele de Lavinde, criptógrafo parmesano que sirvió al papa Clemente VII. *Cf.* David Kahn, *op. cit.*, p. 107.

sería utilizado por innumerables corresponsales europeos y americanos durante más de cuatro siglos.[39] El asunto general de la criptografía se volvió extremadamente popular durante los siglos XVI y XVII. De hecho, circulaban tantos libros al respecto que el duque de Brunswick-Lüneburg, en 1622, llegó a revisar y comentar casi doscientos.[40]

Los métodos criptográficos de Simeone de Crema nos permiten suponer que la Europa occidental tenía nociones claras del criptoanálisis a principios del siglo XV. De Crema fue un pionero (1401) en el uso de tablas homofónicas para ocultar a cada vocal del texto con más de un equivalente, muestra de previsión contra los ataques criptoanalíticos de la cual, según vimos, Hernán Cortés hizo gala más de cien años después.

A partir del último cuarto del siglo XV las técnicas de cifrado alcanzaron una complejidad extrema. Políticamente, la criptología se convirtió en un instrumento de comunicación a tal grado vital para los Estados europeos, que la mayoría de las cortes instauraron secretarías donde criptógrafos y criptoanalistas laboraban tiempo completo sobre cada despacho interceptado.[41]

En Francia, Antoine Rossignol mereció la vía libre a los secretos de la corte de Luis XIV gracias a sus excelsas dotes criptológicas. El sistema nomenclator le debe algunas innovaciones técnicas de gran valor, por ejemplo, la organización azarosa en dos tablas de las correspondencias entre las letras claras (ordenadas alfabéticamente) y los elementos del código. De esta manera, las dos partes del código recuerdan a un diccionario bilingüe. Con la colaboración de su hijo, Bonaventure, Rossignol diseñó un código formado de 587 elementos, conocido como la *Grand Chiffre* (Gran Cifra), que durante cuatrocientos años gozó la fama de ser impenetrable.[42]

[39] Kahn, *ibidem*.

[40] En su obra *Cryptomenytices et Cryptographiae Libri IX* (1624). *Cf*. Gerhard F. Strasser, "The Noblest Cryptologist: Duke August the Younger of Brunswick-Lüneburg (Gustavus Selenus) and His Cryptological Activities", en *Cryptologia*, v. 7, n. 3, 1983, p. 193-217.

[41] Kahn, *op. cit.*, p. 108-109.

[42] El comandante Étienne Bazeries la rompió hacia 1893, adivinando correctamente que una secuencia particular de números repetidos, 124-22-125-46-345, valía para la expresión *"les ennemis"* (los enemigos); esta información lo facultó para decriptar el resto. Otro criptógrafo francés de grandes dotes fue el matemático François Viète, seigneur de la Bigotiere (1540-1603). Simpatizante de los hugonotes durante las guerras religiosas entre Enrique de Navarra y la Liga, en 1589 consiguió penetrar una cifra de casi 500 signos que Felipe II estimaba como invulnerable. Cf. Kahn, *op. cit.*, p. 118 y 244.

En la historia de Inglaterra son famosos los criptogramas epistolares utilizados por María Estuardo, reina de los escoceses, en sus conspiraciones contra Isabel I para recuperar el trono de Inglaterra. Gilbert Curle, su secretario, era quien propiamente cifraba las misivas con el método nomenclator [figura 4]. Éstas eran sin falta interceptadas por un doble agente católico, Gilbert Gifford, empleado del secretario de Estado sir Francis Walsingham, y Thomas Phelippes, un experto en falsificaciones, las decriptaba invariablemente. Animado por amigos en el extranjero, Anthony Babington escribió el 6 de julio de 1586 a María solicitando aprobación y consejo para "despachar" a la "usurpadora" (Isabel). La respuesta, fechada el 17 de julio, selló el destino de María. Después de discernir el texto claro, Phelippes la hizo llegar a Babington acompañada de un breve *post scriptum* (falsificado por él) donde solicitaba los nombres de todos los cómplices en la maquinación [figura 5]. Arrestaron a María, la juzgaron y, declarada culpable, fue decapitada el 8 de febrero de 1587.[43]

El nomenclator fue muy socorrido en el medio diplomático español durante el siglo XVI.[44] El 11 de mayo de 1532 el embajador en Venecia, Rodrigo Niño, lo aplicó para sugerir al emperador unas medidas defensivas en previsión de que el Gran Turco intentase tomar la fortaleza de Klisa (en Dalmacia, cerca de Split, Croacia).[45] Casi veinticinco años después hizo lo propio el marqués de Mondéjar, virrey de Nápoles, para informar a Felipe II sobre la posible negociación de una tregua entre cristianos y turcos, lo que determinó una crisis del espionaje imperial en el Mediterráneo. La segunda

[43] Durante la década de 1570 Walsingham reclutó espías de Oxford y Cambridge para crear una escuela de espionaje en Londres, misma que se desarrolló hasta convertirse en la red de informantes europea más poderosa. **Cf. Stephen Budiansky,** *Her Majesty's Spymaster: Elizabeth I, Sir Francis Walsingham, and the Birth of Modern Espionage*, New York, Penguin, 2005. Véase también el sitio web http://www.nationalarchives.gov.uk/spies//ciphers.

[44] Horst Rabe y sus colaboradores han trabajado durante años en el ambicioso proyecto de publicar en línea la correspondencia política de Carlos V, formada por más de 120 000 cartas y otros documentos, de los cuales no pocos contienen criptogramas. Véase Horst Rabe y Heide Stratenwerth, "Carlos V en Internet. Sistema de gobierno y comunicación política del Emperador como tema de un proyecto de investigación realizado en la Universidad de Konstanz (Alemania)" (traducido por Publio Fernández Morán). Disponible desde Internet en: <http://www.cervantesvirtual.com/historia/CarlosV/recurso2.shtml> [con acceso el 22-09-2005].

[45] E. Sola, "Los venecianos y Klisa: el arte de fragmentar", en *Archivo de la frontera* [publicación en línea]. Disponible desde Internet en: <http://www.hazhistoria.com> [con acceso el 14-03-2006].

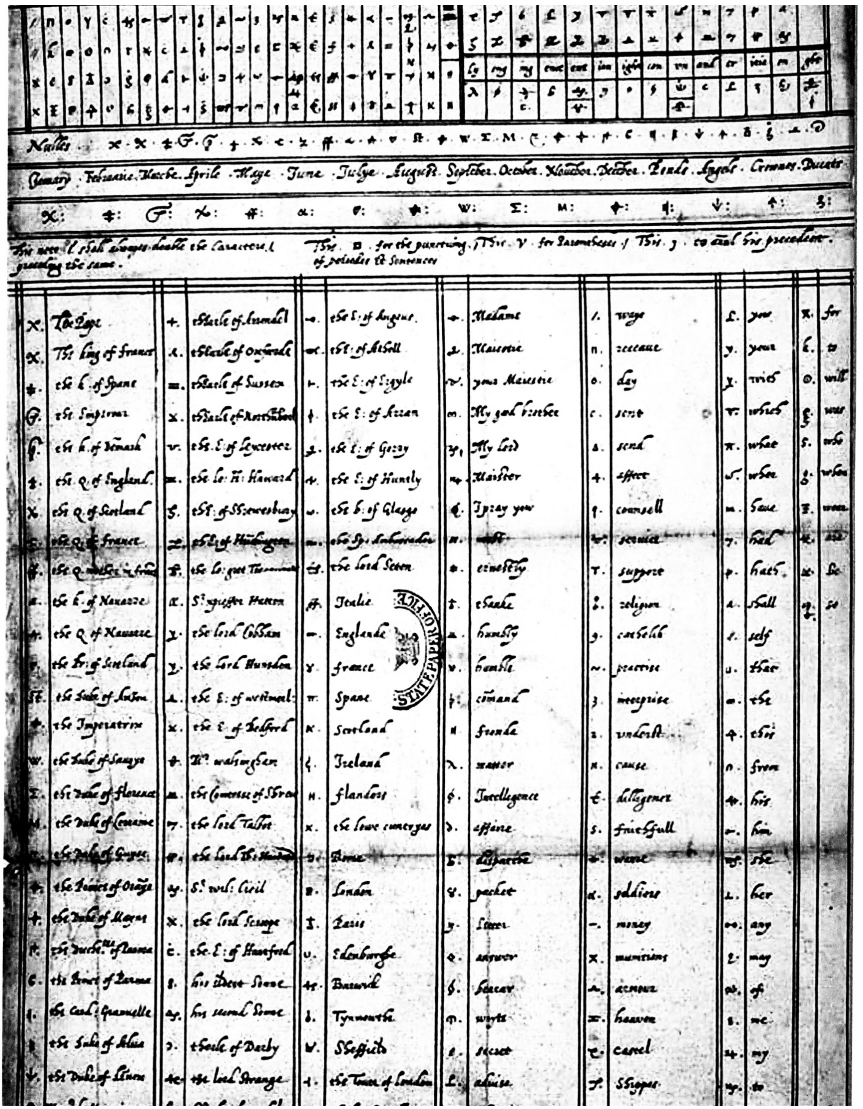

Figura 4. Sistema nomenclator empleado por María Estuardo. Como se puede ver, algunos signos prácticamente son idénticos a otros tantos que utilizó Cortés. Fuente: http://www.nationalarchives.gov.uk/spies//ciphers

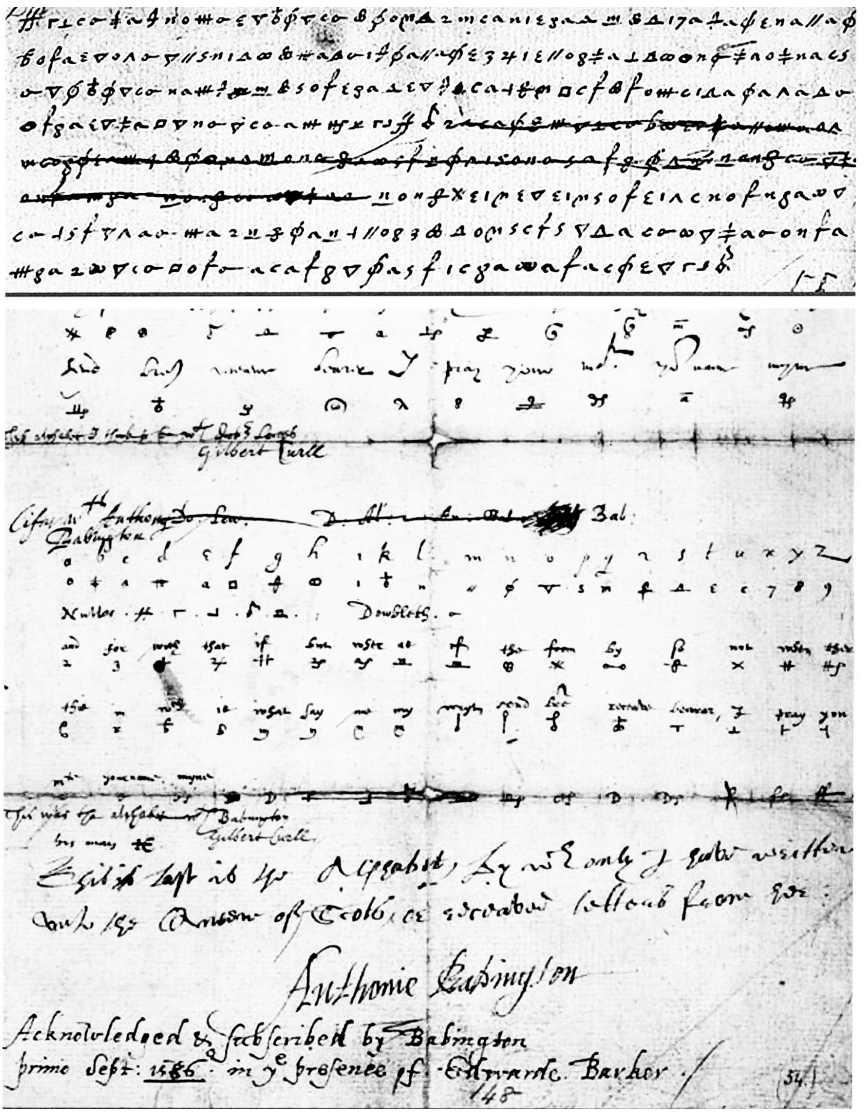

Figura 5. *El post scriptum* falsificado por Thomas Phelippes para destruir la conjura de Anthony Babington a favor de María Estuardo. Fuente: http://www.nationalarchives.gov.uk/spies//ciphers

de tres páginas que ocupa el texto está colmada de sustituciones homofónicas (con letras, números y símbolos diversos).[46]

Bernardino de Mendoza (1541-1604), diplomático y escritor, sobresalió por sus habilidades criptológicas. Inició su carrera diplomática en marzo de 1578 y mientras fungió como embajador de Felipe II ante la corte de Inglaterra participó en las conspiraciones de María Estuardo contra Isabel I. De 1584 a 1590 ocupó la embajada española en Francia, desde donde mantuvo una intensa correspondencia con los primos don Juan y don Martín de Idiaquez, ambos secretarios de Estado. En muchas de estas cartas aplicó un método de nomenclator donde destaca la sustitución de letras con números y el cifrado de bigramas (por ejemplo, BL = 23, BR = 24, y TR = 34).[47]

Como señaló Guillermo Lohmann Villena, historiador que de manera ejemplar decriptó por cuenta propia una cantidad importante de cifras en la serie de documentos que su "buena estrella" y un poco de "malicia" —para "intuir los filones" posiblemente fructíferos— le permitió rescatar del Archivo General de Indias, la "criptografía indiana" fue de aparición precoz, adelantándose incluso a las fundaciones de Nueva España y del virreinato peruano. Ya en 1500 el gobernador de Santo Domingo, Francisco de Bobadilla, interceptó una misiva de Cristóbal Colón a Diego Colón escrita con "caracteres ignotos".[48] Pero no sólo cifraban sus comunicaciones los virreyes y otros altos oficiales de la corona, también lo hacían las órdenes religiosas y los particulares. Típicamente apelaron a los métodos de la sustitución homofónica y del nomenclator, usanza que se mantuvo vigente aún durante las luchas por la independencia.[49]

[46] Kenneth L. Clewett, Aida Borrallo Leal y Carlos Muñoz Pozo, "El filtro de Nápoles. Carta del virrey Mondejar de Nápoles al rey Felipe II, 20 de noviembre, 1577", en *Archivo de la frontera* [publicación en línea]. Disponible desde Internet en: <http://www.hazhistoria.com> [con acceso el 10-04-2006]. (El documento sirve para inferir la causa de la "caída" de Aurelio de Santa Cruz, jefe de la red de espías de Felipe II en Estambul, así como la razón de la nueva fórmula de negociación empleada por la Corte.)

[47] A. Herrera Casado, "Bernardino de Mendoza", texto íntegro de la conferencia de clausura del curso 1988-1989 de la Real Sociedad Económica Matritense de Amigos del País. Disponible desde Internet en: <www.aache.com/docs/bernardino.htm> [con acceso el 21-05-2005].

[48] Guillermo Lohmann Villena, "Cifras y claves indianas. Capítulos provisionales de un estudio sobre criptografía indiana (primera adición)", en *Anuario de Estudios Americanos*, tomo XIV, 1957, p. 351-359, p. 352. Pedro Mártir de Anglería, *Décadas del Nuevo Mundo (1493-1525)*, México, Porrúa, 1964, traducción de Agustín Millares Carlo, estudio y apéndices de Edmundo O´Gorman, 2 v.; v. I, Primera Década, Libro VII, p. 177.

[49] Sobre los autores que han tratado la "criptografía independentista" —como valdría llamarla, quizá— en América Latina, véase Juan Carlos Galende, "Sistemas cripto-

En Perú, cuando transcurría la década de 1540, el licenciado Pedro de la Gasca empleó una tabla de sustitución y un puñado de términos codificados en su correspondencia oficial con el Consejo de Indias [figura 6].[50] El almirante Antonio de Aguayo, en agosto de 1563, aprovechó una tabla de sustitución elemental para cifrar un despacho en Nombre de Dios (istmo de Panamá) [figura 7].[51] Idéntica maniobra pusieron en marcha los almirantes Flores de Valdés (en 1567, también en Nombre de Dios) y Cristóbal de Eraso (para despachar un correo desde San Juan de Ulúa el 20 de febrero de 1568); ambos recibieron la convención criptográfica de la Casa de la Contratación.[52] Por su parte, Pedro Castillo del Salto, virrey del Perú, recibió —probablemente de Cristóbal Ramírez de Cartagena (Fiscal de la Audiencia de Lima)— una carta fechada el 19 de marzo de 1575, cifrada con un sistema nomenclator dotado de un conjunto de códigos mucho más nutrido que el diseñado por De la Gasca 35 años antes [figura 8].[53]

Es hasta la tercera década del XVII cuando se aprecia un aumento de complejidad en el diseño de un "nomenclator indiano". Un ejemplo son las tablas y el diccionario que el Consejo de Estado suministró a Luis Jerónimo Fernández de Cabrera y Bobadilla, conde de Chinchón, virrey del Perú de 1629 a 1639. Se trata de tres tablas con sustituciones numéricas y homofónicas para letras y bigramas, una lista de signos nulos, y un diccionario de 62 elementos en donde los nombres propios se sustituyen con cantidades numéricas (de hasta tres guarismos) o con bigramas o trigramas [figura 9]. Ahora bien, según lo ha narrado Lohmann Villena, circunstancias determinadas impidieron que los mensajes cifrados con aquellas tablas pudieran ser leídos en el Consejo de Indias. Debido a esto, el conde de Chinchón solicitó un sistema criptográfico que desbancase al anterior.[54] Desde una perspectiva historiográfica y criptológica, es manifiesto el interés de los refinamientos que se aplicaron al nuevo sistema: las letras se representan con dos núme-

gráficos empleados en Hispanoamérica", en *Revista complutense de historia de América*, n. 26, 2000, p. 65-68.

[50] Lohmann, "Cifras y claves indianas. Capítulos provisionales de un estudio sobre criptografía indiana", en *Anuario de Estudios Americanos*, Sevilla, 1954, v. XI, p. 307.

[51] *Ibid.*, p. 313-314.

[52] *Ibid.*, p. 315-317.

[53] *Ibid.* p. 317-319.

[54] *Ibid.*, p. 326-337.

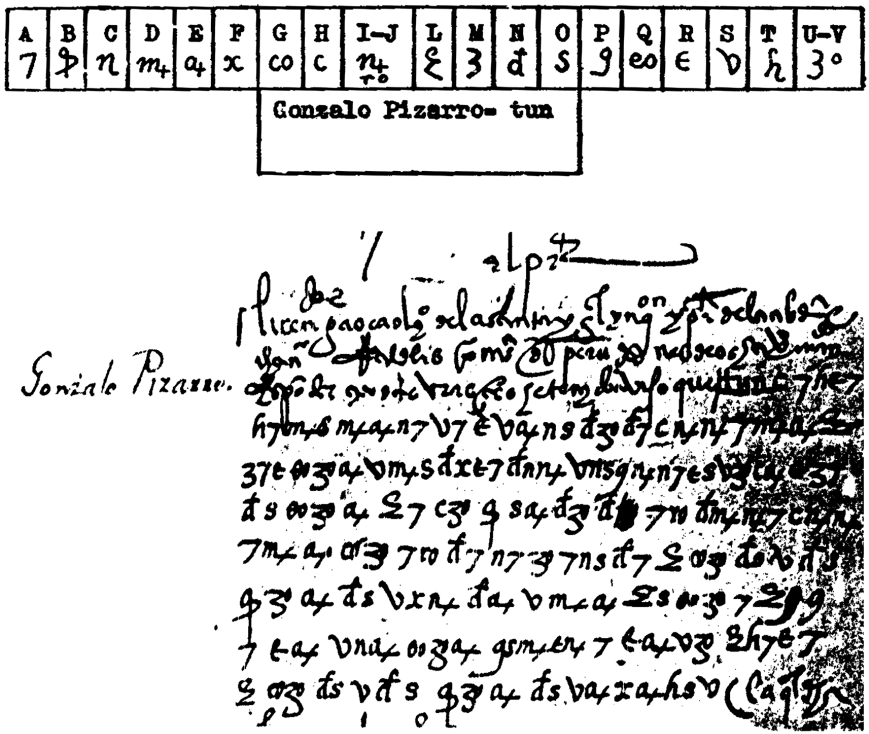

Figura 6. Sistema criptográfico y fragmento de una carta cifrada por Pedro de la Gasca. Fuente: Guillermo Lohmann Villena, "Cifras y claves indianas. Capítulos provisionales de un estudio sobre criptografía indiana", en *Anuario de Estudios Americanos*, Sevilla, 1954, v. XI, montaje realizado con la imagen de la página 307 y la lámina 3

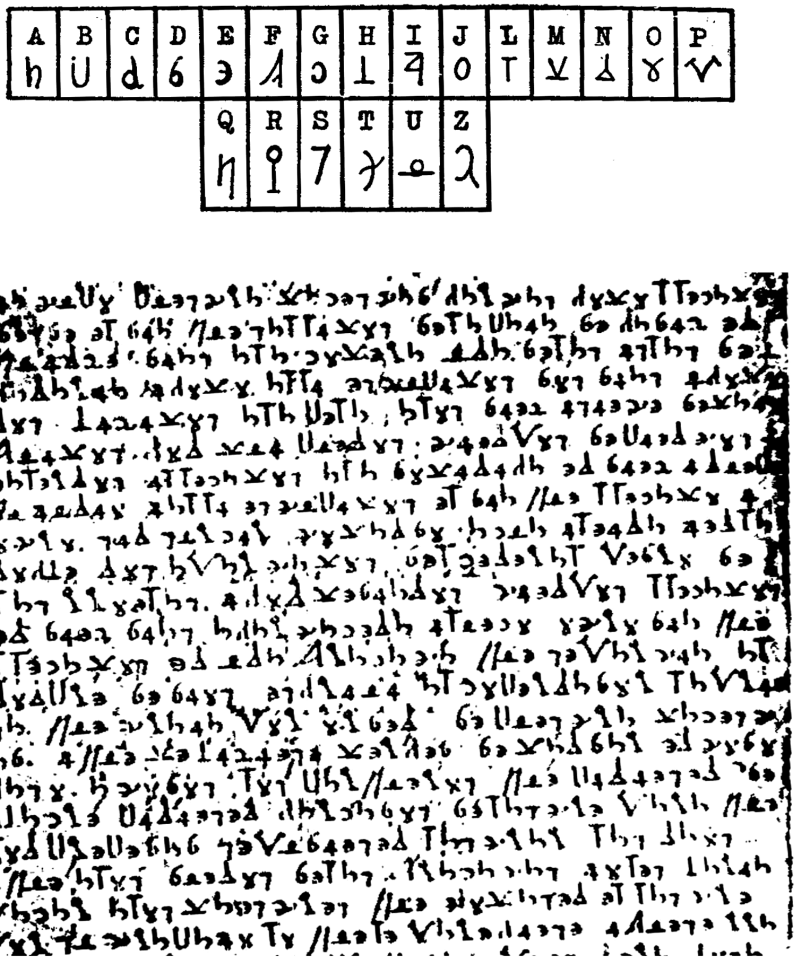

Figura 7. Sistema criptográfico y fragmento de un despacho cifrado por el almirante Aguayo. Fuente: Guillermo Lohmann Villena, "Cifras y claves indianas", *loc. cit.*, montaje realizado con imagen de página 314 y lámina 4-A

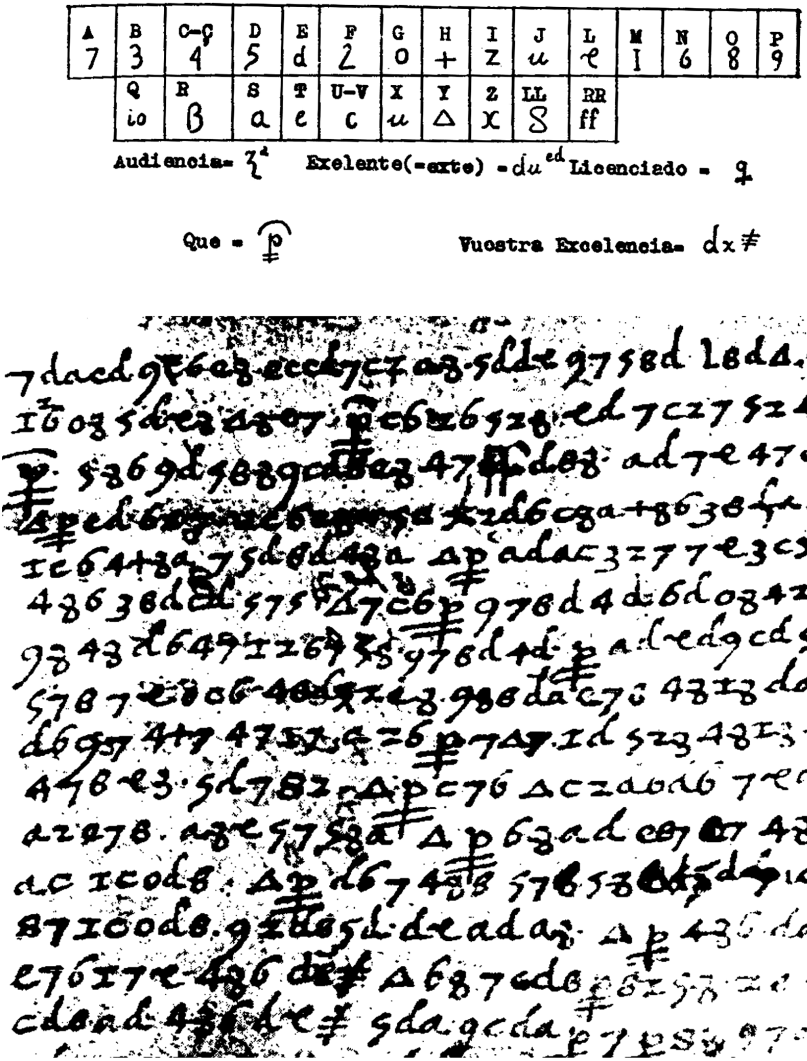

Figura 8. Fragmento de una carta cifrada con el sistema criptográfico del virrey Toledo. Fuente: Guillermo Lohmann Villena, "Cifras y claves indianas", *loc. cit.*, montaje realizado con imagen de página 319 y lámina 7

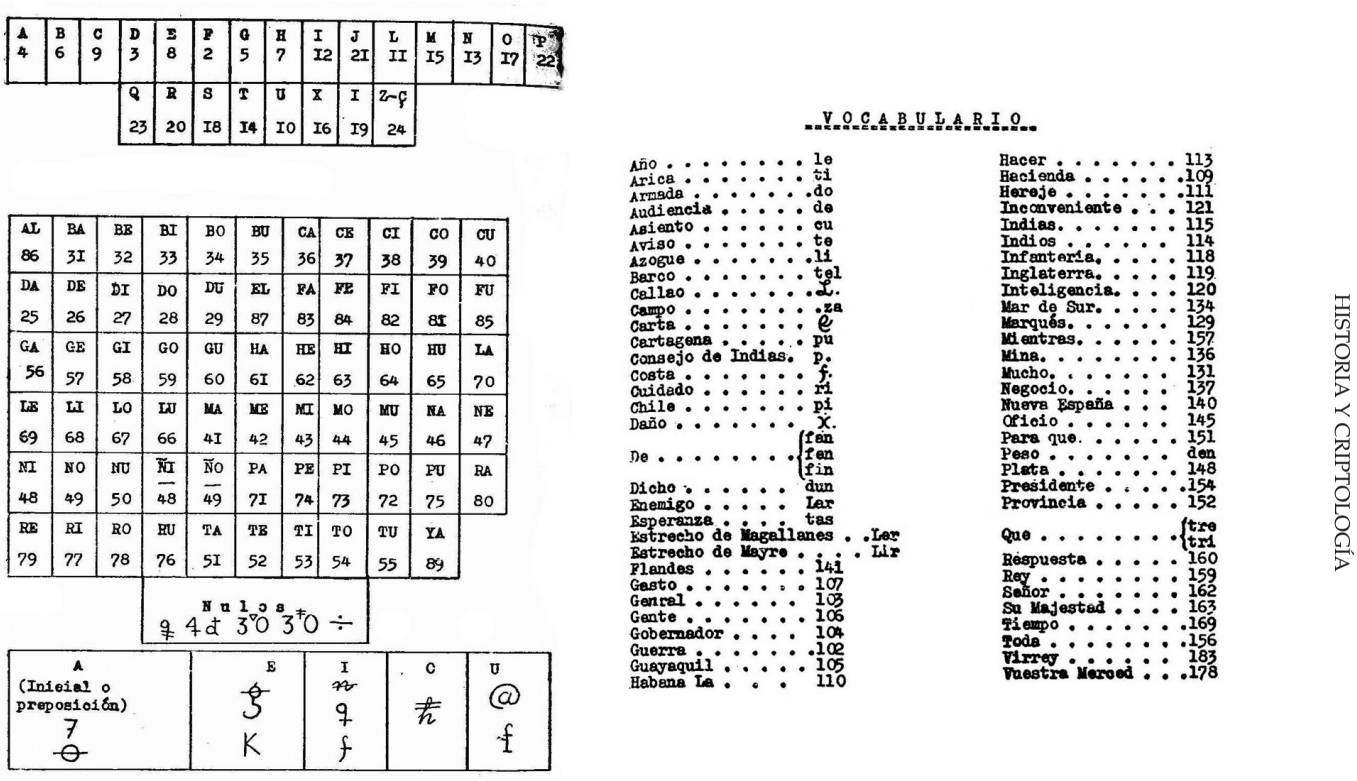

Figura 9. Primer sistema nomenclator del conde de Chinchón.
Fuente: Guillermo Lohmann Villena, "Cifras y claves indianas", *loc. cit.*, p. 330 y 331

ros (figurando con doble equivalencia algunas de ellas); los trigramas entran en juego para representar sílabas; varios números están coronados por una tilde, lo que evita confundirlos con los números de sustitución en el alfabeto simple (es decir, la sustitución de letras solas); los nulos, en fin, son más escasos, pero el diccionario se robustece ahora con casi 100 conceptos y algunos signos inéditos de correspondencia [figura 10].

En décadas posteriores no se multiplicaron estos adelantos técnicos, al contrario, hubo casos en que el interesado siguió unas pautas de ocultamiento realmente ingenuas. Ocurrió así, por ejemplo, con Juan Ruiz de Apodaca, virrey de la Nueva España, quien se sirvió en 1818 de una tabla de sustituciones numéricas para letras individuales, un signo nulo y un diccionario de apenas dos locuciones.[55]

Al comparar mutuamente los ejemplares criptográficos europeos e indianos que acabo de reseñar brevemente, y considerar su época de creación y uso, derivamos cuando menos un par de conclusiones irrebatibles: 1) el método nomenclator dominó lo que se podría denominar "criptografía occidental" desde el Renacimiento hasta los albores de la época moderna; no debe extrañar, por tanto, que Hernán Cortés se haya limitado a facturar una variación del mismo en la carta de 1532 —pero también en la del 20 de junio de 1533, como veremos—, y 2) el nomenclator de que se sirvió Cortés no constituye, en definitiva, una "clave" para descifrar documentos diferentes a la carta de 1532, o bien, hablando genéricamente, documentos en los cuales el cifrado y la codificación hayan dependido de tablas de sustitución y equivalencias diferentes a las estipuladas, en su momento y lugar, por el conquistador de Tenochtitlan y su procurador *ad litem* en España.

El código en la carta de Cortés

Los términos equivalentes en un diccionario de nomenclator se pueden graficar de varias maneras. En el diccionario del segundo sistema criptográfico que le proporcionaron al conde de Chinchón (véase la figura 10) las equivalencias están generalmente represen-

[55] *Ibid.*, p. 366. Su vulnerabilidad es obvia, pues cada vocal se sustituye con un complejo de cuatro guarismos y no hay mayor suministro de paridades terminológicas para fortificar el acertijo, lo que facilita el análisis de frecuencias.

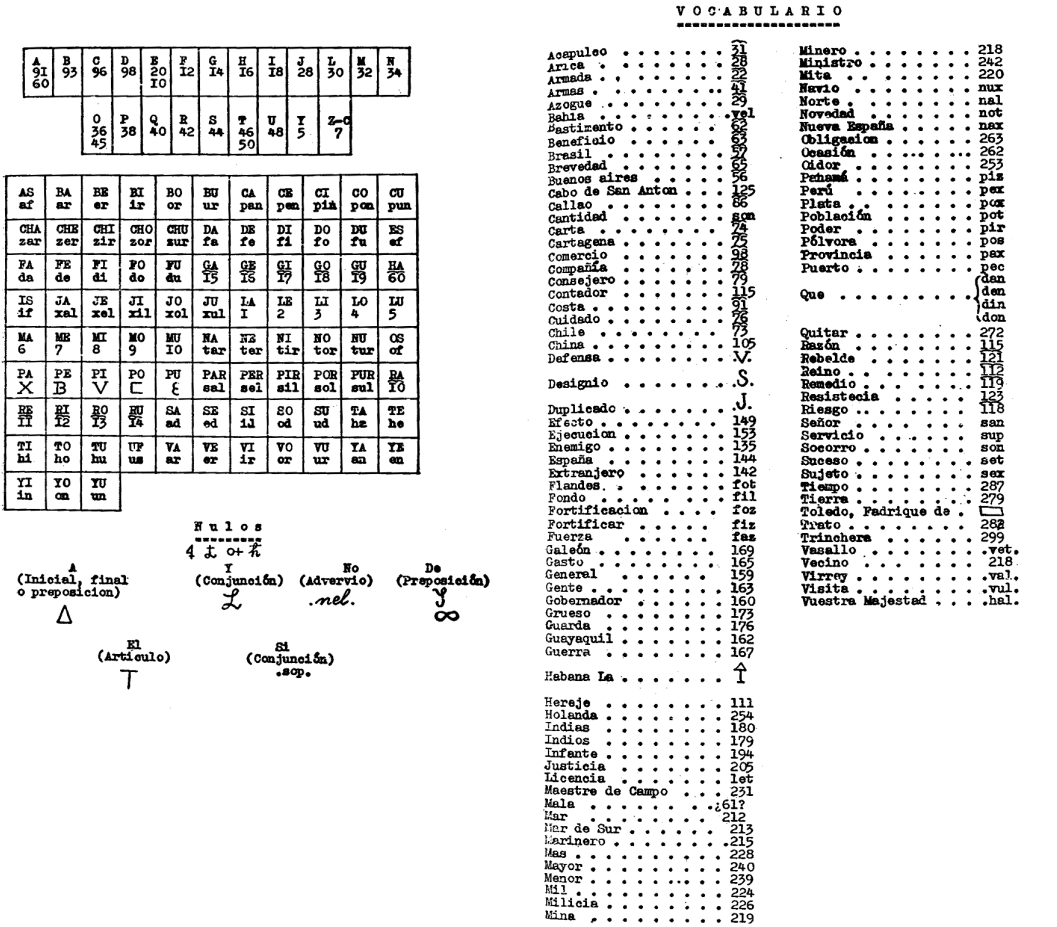

Figura 10. Segundo sistema nomenclator del conde de Chinchón.
Fuente: Guillermo Lohmann Villena, "Cifras y claves indianas", *loc. cit.*, p. 336 y 337

tadas por grupos de tres números arábigos o de tres letras minúsculas; en ocasiones los grupos numéricos están subrayados y los grupos literales van precedidos y seguidos de un punto. Estas eran convenciones tendientes a reproducir, con las modificaciones adecuadas a cada caso, el modelo de codificación predominante en la criptografía clásica.[56] Cortés, como ya señalé, preparó un breve diccionario que incluye cuatro grupos de hasta cinco letras —are, aca, beril y adan— para esconder nombres propios en su carta, aunque resulta complicado distinguir en los facsímiles si todos los grupos están realmente cercados por puntos en cada extremo. Asumiré, sin embargo, que tal fue la convención aplicada, pues ello no afecta en lo absoluto a mis intentos de inferir las equivalencias probables de dos elementos codificados en el texto.

He aquí el resultado de mis intentos. Los elementos sobre los cuales razoné son .are. y .aca. Guillermo Lohmann escribió que no es difícil vislumbrar su significado, aún careciendo del diccionario. Para comprobar si es así, repasemos el fragmento de la carta donde aparecen citados:

> [Después de repetir a Núñez los motivos por los cuales éste deberá ir en pos del emperador, prosigue Cortés en cifra:] porque considerando yo que todo género de negociación que se haya de hacer con el .are. ha de ser despachada por la mano de .aca., y que el que a éste no tuviere grato y acepto no sabe lo que hace, he procurado desde aquí hacerle algunas obras por donde no reciba importunidad con mis negocios, antes el que en mi nombre los negociare, halle en él buena voluntad y no se importune de oírle y despacharle; y podéis ir muy seguro que cuando allá lleguéis hallaréis en él todo favor y amistad y buen acogimiento…[57]

Si establecemos un contexto tomando en cuenta el texto claro que antecede inmediatamente a estas líneas cifradas,[58] me parece de sentido común y de lógico razonamiento inferir lo siguiente:

[56] Así, por ejemplo, la cifra española decriptada por François Viète (véase nota 42 *supra*) consistía de sustituciones alfabéticas y un código de 413 términos representados por grupos de dos o tres letras mayúsculas, o por dos números subrayados o punteados encima. Un grupo de dos dígitos coronado por una línea indicaba un signo nulo.

[57] "Carta de Hernán Cortés a su procurador *ad litem* Francisco Núñez acerca de sus negocios ante la corte (con pasajes cifrados)", en José Luis Martínez (editor), *Documentos cortesianos*, México, UNAM/FCE, tomo III, sección VI (primera parte), 1991, p. 315-316.

[58] *Ibid.*, p. 315.

1) La mejor hipótesis es que ".are." codifica uno de dos posibles términos: "Emperador" o "Rey", aludiendo a Carlos V. Para realizar esta inferencia basta interpretar en el sentido de un testimonio a las repetidas alusiones de Cortés al emperador como la contraparte última de sus negocios jurídicos ante la corte, y valorar a tal testimonio como lo que puede ser el hecho en la conclusión de este razonamiento hipotético. Como declaré al cabo de la Introducción, siempre será oportuno reflexionar sobre las ventajas que un historiador puede obtener si comprende y ejercita este modo de razonamiento.

2) A mi juicio, contamos con suficientes monografías bien informadas acerca de la política y la diplomacia durante los reinados de Carlos V y Felipe II cuyo análisis, tendiente a configurar una hipótesis del significado de .aca. en la carta cortesiana, nos permite inferir que ".aca." puede ser el nombre "Francisco de los Cobos" en código. Secretario real desde 1517 y de Indias desde 1518, Francisco de los Cobos (que obtuvo el título de Comendador Mayor de León en 1529) fue durante décadas uno de los principales consejeros del emperador español. Varios autores afirman que todos los asuntos de España, Italia y las Indias pasaban por sus manos antes de llegar a las del monarca.[59] Entonces, cuando Cortés, en 1532, apunta "[…] considerando yo que todo género de negociación que se haya de hacer con el .are. ha de ser despachada por la mano de .aca.…", parece correcto suponer, como cimiento de una hipótesis hacia la mejor explicación, que con ".aca." está diciendo, veladamente, "Francisco de los Cobos". Y tiene sentido, por cierto, imaginar a Cortés "haciendo algunas obras" a favor de tan influyente personaje, confiando en que así no encontraría "importuno" recibir al procurador Núñez en audiencia.

Estoy seguro de que la consulta de obras historiográficas pertinentes podrá inspirar a cualquiera las mejores inferencias —o, al menos, un esfuerzo de adivinación bien orientado— para modificar o corregir las hipótesis anteriores, o bien restituir los nombres

[59] De los Cobos tenía un grupo de auxiliares para tramitar sus despachos de todas las materias de gobierno que controlaba desde la corte, sobre todo las relacionadas con Castilla, Cámara, Hacienda, Guerra e Indias. De tales auxiliares cabe mencionar a Francisco de Eraso, un típico aprendiz y escribano que tenía entre sus deberes la decriptación de textos en cifra. *Cf*. Carlos Javier de Carlos Morales, "El poder de los secretarios reales: Francisco de Eraso", en José Martínez Millán (director), *La corte de Felipe II*, Madrid, Alianza Editorial, 1994, p. 107-148.

propios equivalentes a los dos términos codificados restantes, . adan. y .beril.

El procuradorFrancisco Núñez ¿recibió y leyó la carta?

José Luis Martínez ha juzgado como evidente que Núñez jamás despachó ni siquiera uno de los mandatos que le transmitió Cortés en la carta de 1532. Este juicio le parece válido por considerar posible que la carta fue interceptada, o recogida junto con los demás papeles del procurador, después de que éste murió, y resguardada en el Archivo General de Indias. En rigor, Martínez admite esa posibilidad para explicar el hecho —como lo quiere concebir él— de que Núñez no haya dejado "rastro" de haber atendido los encargos. Sin embargo, hay medios de inferir lógicamente, más que aducirla como posible, la existencia de un hecho, a saber, que Núñez sí dejó testimonio de haber actuado conforme a las instrucciones de su primo, lo cual obviamente implica que recibió y leyó la carta. Para lograr esto no hace falta consumar algún prodigio analítico, basta leer cuidadosamente un grupo documental referente a las labores jurídicas de Núñez y relacionar hipotéticamente su contenido textual con determinadas fracciones de la carta criptografiada de Cortés.

El grupo documental en cuestión está compuesto por un "memorial" acerca de los pleitos y negocios del conquistador y su complementaria lista de cédulas, provisiones y cartas ejecutorias despachadas por Núñez de 1522 a 1543 —piezas ambas que, por cierto, fueron compiladas por el mismo José Luis Martínez en sus *Documentos cortesianos*. El "memorial" debió su redacción, seguramente, al inicio de un procedimiento jurídico solicitado por Francisco Núñez para exigir a Cortés el pago completo por servirlo durante veintiún años.[60] Reúne 82 capítulos o "posiciones" numeradas con romanos que están dirigidas expresamente al marqués del Valle para su confirmación o rechazo. Las declaraciones sobre los despachos

[60] En España, durante el siglo XVI, los oficios, informes y cartas eran indistintamente llamados "memoriales". Sin embargo, hay motivos para clasificarlos por sus funciones, por ejemplo, la de iniciación de procedimientos a petición de parte o de oficio, y la transmisión de información y disposiciones de trámite. *Cf.* Pedro Luis Lorenzo Cadarso, "La correspondencia administrativa en el Estado absoluto castellano (siglos XVI-XVII)", *Tiempos Modernos. Revista electrónica de Historia Moderna*, Núm. 5, 2002 [publicación en línea]. Disponible desde Internet en: <http://www.tiemposmodernos.org> [con acceso el 02-03-2004].

realizados a partir de 1531 empiezan en el capítulo XXXI, dato que conviene tener en mente cuando se lee el XLVIII: "Ítem, despaché otra cédula para el dicho marqués porque se quejó que teniendo cédula y sobrecédula de Su Majestad para que los pueblos de indios que tenía encomendados no se le quitasen, las cuales no habían querido obedecer el presidente y oidores, mandando se le volver a restituir".[61] Si esto se llevó a efecto tal y como lo asentó el escribano, entonces parece probable que Núñez atendió el preciso asunto de pueblos en Oaxaca del que se quejó pormenorizadamente su primo en la carta de 1532, en los renglones inmediatamente previos a la última cifra: "En esta tierra", dice ahí Cortés, "es muy estimada la provincia de Guaxaca donde yo tengo alguna cantidad de pueblos que entran en los veintitrés mil vasallos [que se le entregaron por merced real el 6 de julio de 1529][62] y pretendo […] que un pueblo de cristianos españoles que allí está [y] se llama Antequera, es mío porque entra en el término de lo por mí nombrado en la dicha provincia; e oidores pasados lo hicieron poblar por repartir la tierra y que yo no lo hubiese", y agrega: "[…] creo que de aquel pueblo [Antequera] irá un regidor a esa Corte, el cual con otras personas que desta cibdad de México irán, han de poner mucha contradicción en que no se me dé […] y creo quel presidente e oidores lo escribirá (*sic*) y procurarán que los pueblos que allí tengo se me quiten. Habéis de resistirlo con mucha solicitud…".[63] Por supuesto, gracias a la decriptación de Francisco Monterde del subsecuente fragmento criptografiado sabemos que Cortés tenía una estrategia alternativa para salir de aquel asunto sin mayores pérdidas, aún si Antequera terminaba excluida del marquesado.[64] Todo esto indica que Núñez recibió y leyó la carta y procedió según lo exigido.[65]

[61] "Memorial del licenciado Francisco Núñez acerca de los pleitos y negocios de Hernán Cortés de 1522 a 1543", en José Luis Martínez (editor), *Documentos cortesianos*, México, UNAM/FCE, tomo IV, secciones VI (segunda parte) a VIII, p. 291-292.

[62] José Luis Martínez, *Hernán Cortés*, México, UNAM/FCE, 1993, p. 505-506.

[63] "Carta de Hernán Cortés a su procurador *ad litem* Francisco Núñez acerca de sus negocios ante la corte (con pasajes cifrados)", en José Luis Martínez, *Documentos cortesianos*, *op. cit.*, p. 317.

[64] *Ibid.*, p. 317-218 (pasajes entre corchetes descifrados).

[65] La Antequera española nunca terminó cercada dentro del perímetro del marquesado del Valle. Una exposición amplia de los motivos de Cortés para no juzgar conveniente a sus intereses señoriales el que Antequera estuviese habitada por españoles, así como del pleito por el establecimiento de los límites entre Antequera y la villa propiamente marquesana en Oaxaca, véase Bernardo García Martínez, *El Marquesado del Valle. Tres siglos de régimen señorial*

Veamos otro caso. En el capítulo LVIII Núñez dice: "Y viniendo a particularizar más por estenso, parece que juntamente con estos procesos que arriba digo [donde se deben incluir los que Cortés menciona en la carta]… vino una instrucción para mí de veinte e tantos pliegos, demás de ciento e veinte capítulos de los cuales se dieron peticiones e se despacharon veinte e seis cédulas […] tengo la dicha instrucción original firmada del señor marqués e con lo proveído en las márgenes".[66] Cortés, luego de consignar largamente sus razones para mantener a Núñez como procurador suyo en España, agrega: "[…] por tanto, yo os envío una istrución (*sic*) de negocios y pleitos en la cual se resumen todas las instruciones (*sic*) que allá os he enviado de negocios […] y porque en ella van todos asentados, y lo que habéis de decir a Su Majestad y al Consejo de Indias, y lo que sobre cada cosa habéis de suplicar […] en esta carta no hago minción (*sic*) de negocio ninguno pues allí van todos."[67] A reserva de localizar nuevas instancias de esta correspondencia, se impone inferir que la "instrucción" aludida por Núñez es la que describe Cortés en la cita, pues en la carta de 1533 (la otra que conocemos, también con cifras) nada se dice de instrucciones adjuntas.

Por último, considero patente que el capítulo final del "Memorial" se refiere a una exigencia muy repetida por Cortés en la mitad inicial de su carta de 1532.[68] Cada lector podrá comparar las palabras exactas del conquistador con la siguiente declaración de Núñez, y juzgar hasta qué punto tenemos la opción de inferir una solución lógicamente probable a la cuestión revisada en este apartado:

en Nueva España, México, El Colegio de México, 1969 (Centro de Estudios Históricos, Nueva serie, 5), p. 49, 61-63.

[66] "Memorial del licenciado Francisco Núñez acerca de los pleitos y negocios de Hernán Cortés de 1522 a 1543", en José Luis Martínez (editor), *Documentos cortesianos*, *op. cit.*, p. 292.

[67] "Carta de Hernán Cortés a su procurador *ad litem* Francisco Núñez acerca de sus negocios ante la corte (con pasajes cifrados)", *loc. cit.*, p. 313-314. En realidad Cortés, con éste y otros enunciados en la carta, está siguiendo una estrategia para desanimar a los espías potenciales del correo, pues es un hecho que sí menciona negocios a su procurador, aunque de manera criptográfica. Así, en previsión de que no podrá retener legalmente al pueblo de Antequera dentro de sus dominios, instruye a Núñez (p. 317-18) para exigir una importante cantidad de pueblos a cambio de la villa quitada.

[68] Y que se ubica bajo el rubro b) cuyo sentido describí en el apartado "Nombre y caracterización técnica del método de Cortés". Según mi interpretación, la primera mitad de esta carta en la edición de José Luis Martínez ocupa de la página 311 a los dos tercios iniciales de la página 315.

> Fuera destos procesos […] en la instrucción que dejó escripta de su mano e firmada de su nombre, entre otros capítulos me dijo uno por el cual me manda siempre tenga cuidado de le enviar todas las nuevas que hobiere en esta Corte y en la del emperador…, las cuales yo le envié tan copiosamente después que partió destos reinos que ninguna cosa se ofreció en España, Francia, Italia e Turquía, Inglaterra e Alemania de que no le envié copia [y] aunque otros negocios suyo no hobiese hecho, se me debe el salario porque muchos grandes señores destos reinos tienen solicitadores en esta Corte sin tener pleitos solamente para que les escriba nuevas.[69]

La segunda carta cifrada de Cortés

Está fechada el 20 de junio de 1533, Puerto de Santiago en la Mar del Sur. El original obra en los autos seguidos por Núñez contra Cortés en 1546.[70] También Mariano Cuevas tuvo la primicia de publicarla en 1915, pero en la edición de Cuevas el documento aparece mutilado; quiero decir que los dos breves párrafos donde se insertaron los criptogramas fueron separados del texto, uno parcialmente y otro completamente. Quizá Cuevas, como hizo con la carta de 1532, procuró vanamente dilucidar las escasas líneas con el apoyo de un paleógrafo, sin embargo, esta vez no consideró pertinente organizar ningún certamen público de "descifración". Ahora, si damos por un hecho que jamás pudo acceder a los breves mensajes disimulados en esta segunda carta, me parece interesante buscar una explicación a su decisión de suprimirlos. A mi juicio, es acertado responder lo siguiente: notando la magna desigualdad cuantitativa entre los signos crípticos de esta carta y los de la primera, supuso que no podían ocultar algo importante, y los extirpó sin más.[71]

Como haya sido, lo cierto es que la carta de 1533 se incluye mutilada en las colecciones de documentos cortesianos posteriores a la de Cuevas.[72] Ahora ¿cómo justificar esta tradición editorial? En úl-

[69] "Memorial del licenciado Francisco Núñez acerca de los pleitos y negocios de Hernán Cortés de 1522 a 1543", *op. cit.*, p. 292.

[70] Véase nota 7.

[71] Considero lícito sospechar que uno de los motivos fundamentales, o quizá el motivo fundamental de convocar al concurso de 1925, fue que Cuevas, Toro y los demás miembros del antiguo Museo Nacional pensaron que las cifras en la carta de 1532, dada su longitud, necesariamente ocultaban información digna de acopio.

[72] Lo hace el propio Martínez en sus *Documentos cortesianos*, México, UNAM/FCE, tomo IV, secciones VI (segunda parte) a VIII, p. 32-41. En la nota 1 al texto señala que sólo se conser-

tima instancia, por la regular falta de interés de los investigadores hispanoamericanos en la historia de la criptografía, en particular de la "criptografía indiana". Como sea, es tiempo de ponerse al día: Guillermo Lohmann reveló en 1954 la existencia de la carta de 1533, y en el año siguiente publicó su texto íntegro, ya sin criptogramas (como vemos, no se limitó a notificar el hallazgo, sino que examinó las cifras hasta restituir las correspondencias de cada sustitución homofónica).[73] Tenemos, pues, que desde 1955 las dos cartas cortesianas con cifras se pueden leer prácticamente completas —la de 1532 gracias a Francisco Monterde—, ya que en ambas persiste la incertidumbre respecto de los códigos.

Es probable que Lohmann haya descifrado la segunda carta valiéndose de las tablas de sustitución derivadas por Monterde para la primera carta.[74] Basta clasificar y comparar cada signo de sustitución en la cifra de 1533 con la de 1532 para inclinarse por esta hipótesis [figura 11],[75] pero creo que si las cifras en la carta de 1533 hubiesen superado su paciencia analítica, aún teniendo a mano las tablas de Monterde, Lohmann lo hubiera confesado. Al comentar esto no pretendo filtrar una opinión sobre la honestidad intelectual de aquel investigador, mi meta es argumentar que conviene saber criptología, así sea lo básico, para reconocer una cifra tan pronto se la ve y, si es el caso, entender las razones de que los esfuerzos para romperla fra-

van dos cartas entre las que se remitieron Cortés y Núñez, y que la de junio de 1532 es la única que contiene cifras. Ambas asunciones, desde luego, carecen de justificación. La misma versión incompleta de la carta de 1533 se incluye, por ejemplo, en la colección *Hernán Cortés. Cartas y documentos*, México, Porrúa, 1963 (introducción de Mario Hernández Sánchez-Barba), p. 514-523, siendo de notar que el introductor, en la nota 44 a su texto, menciona el criptoanálisis de Monterde sobre la epístola de 1532.

[73] Guillermo Lohmann Villena, "Documentos cifrados indianos", en *Revista de Indias*, 15, 1955, p. 255-282, p. 260-268 (Apéndice I). Las transcripciones de los textos descifrados en este material complementan al estudio que publicó en 1954, y las mismas, "aparte de su valor intrínseco como testimonios de orden criptográfico, suministran noticias de primera mano, ya que en su mayor parte son textos que han permanecido mudos desde la época de su redacción", p. 256. Lohmann publicó otras decriptaciones o desciframientos en su artículo "Documentos cifrados relativos al Perú en la época del Virreinato", en *Revista histórica*, XX, 1955-1956, p. 222-253.

[74] Como una muestra de responsabilidad intelectual, Guillermo Lohmann hizo constar en su estudio de 1954 tener conocimiento de la edición primigenia de Cuevas y todo lo referente a la decriptación de Monterde.

[75] Y sería muy interesante que resultara correcta, pues implicaría la lógica consecuencia de que Cortés y Núñez utilizaron las tablas y el diccionario de 1532 más de una vez, por tanto, su correspondencia normalmente sorteaba el espionaje, pero no es el momento de disertar sobre el mejor modo de probar esta hipótesis.

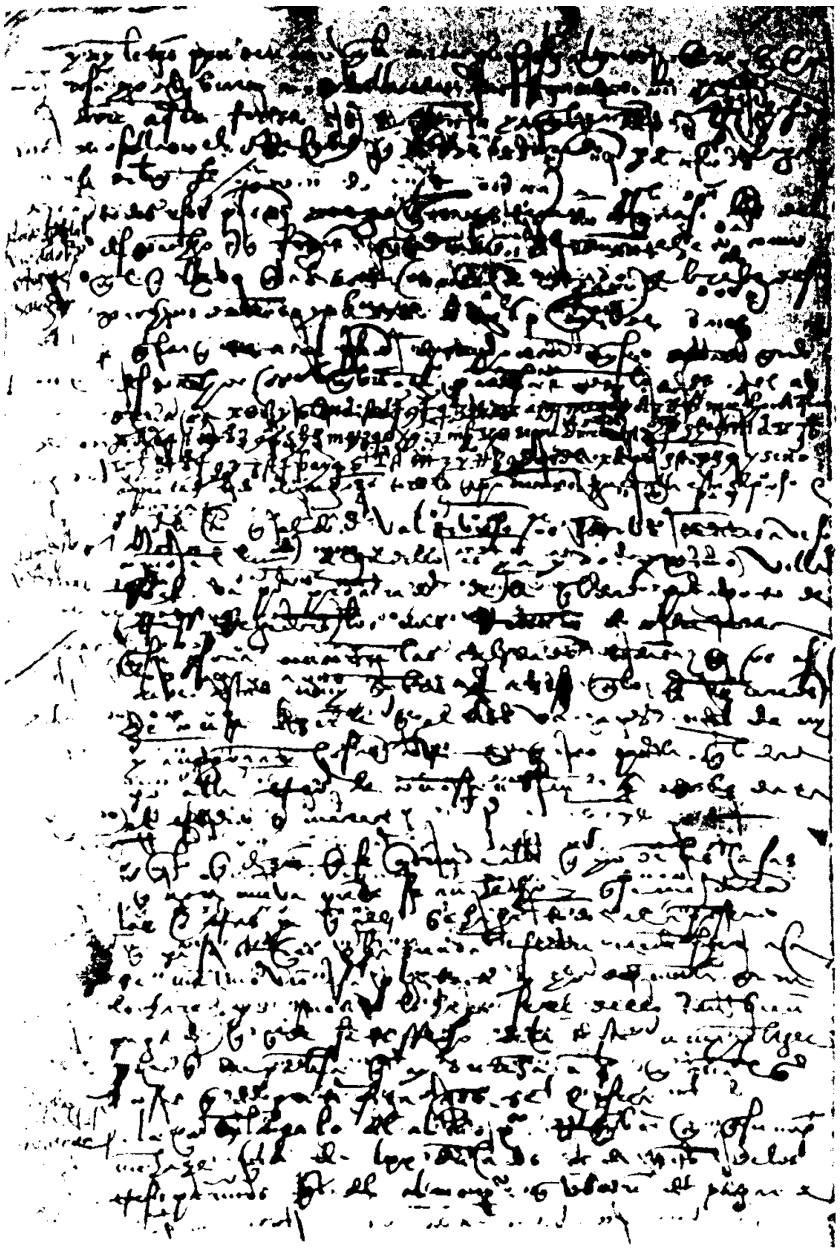

Figura 11. Página de la carta de Cortés a Francisco Núñez del 20 de junio de 1533, con cifras. Fuente: Guillermo Lohmann Villena, "Cifras y claves indianas", *loc. cit.*, lámina 1

casen. Como sea, el hecho es que Lohmann seguramente se esforzó para su mayor aprendizaje técnico al decriptar o descifrar las cifras mencionadas.[76] Y corresponde a los expertos en la vida de Cortés argumentar algo válido, bien fundamentado, sobre si la investigación historiográfica de su tema permanecería inalterada, para cualquier propósito, si la lectura tradicional del fragmento "En lo que toca al pleito de Cuyoacan, en estotro segundo despacho os enviaré el parecer de los señores del Audiencia y si no apretad todo el negocio todo lo que pudiéredes pues allá está el proceso e parecer",[77] se sustituye con la lectura facultada tras las restituciones de Lohmann (en cursivas): "En lo que toca al plito de Cuyoacán, en estotro segundo despacho os enbiaré el paresçer de los ss. del abdençia, *i aunque como os escreví*, a mí me *conuien[e]* mucho aquel *pu[e]blo por estar cerca de mi casa*, si me Dieren *trs* (*sic*) *tantos uasallos en los 'baya' que yo pidere* (*sic*), dezid que *io lo tomaré* y si no, apretad todo el negoçio todo lo q. pudiéredes, pues allá está el proceso e paresçer",[78] o si devolvieran a su lugar y repasaran el original párrafo antepenúltimo —separado totalmente por Cuevas— que dice: "Aquí enbío al señor Eleto una Carta: tened mucho cuydado de bisitarle y darle pte. de mys negoçios y aprobecharos de su fabor, [aun] *que bien sé que no fará nada en ellos*".[79]

Epílogo

En el año 2004 diversos medios de comunicación propagaron la noticia de que el historiador Marcello Simonetta, profesor de la Universidad de Wesleyan, había desvanecido el misterio en torno a la fa-

[76] Si un biografo de Cortés —para mantener el ejemplo— asumiera la actitud analítica recién descrita (y que es la propia del científico), cualquier lector potencial de su obra terminada podrá aprender más sobre el marqués del Valle —y, por supuesto, de la manera en que lógicamente opera un historiador consecuente— que si explora otra biografía cuyo autor improvisa unas especulaciones inútiles sobre las razones de Cortés para aplicar un sistema criptográfico en lugar de otro, y además considera de suyo la cuestión de las cifras y la criptografía como un mero asunto de "recreo". Esto es precisamente lo que hizo José Luis Martínez en su *Hernán Cortés*, *op. cit.*, p. 647-652, donde repite el contenido central de un fascículo suyo hecho circular en 1987 con el título "Homenaje a la hazaña de Francisco Monterde", *cf.* Héctor Azar, *Francisco Monterde (Discurso)*, México, UNAM, 1987, p. 19-22 (trátase de su discurso de ingreso a la Academia de la Lengua).

[77] Martínez, *Documentos cortesianos*, México, UNAM/FCE, tomo IV, secciones VI (segunda parte) a VIII, p. 39.

[78] Guillermo Lohmann Villena, "Documentos cifrados indianos", *loc. cit.*, p. 265.

[79] *Ibid.*, p. 267.

mosa conspiración de 1478 encabezada por miembros prominentes de la familia Pazzi en contra de los Medici, a la sazón gobernantes de Florencia. En rigor, la contribución de Simonetta fue descifrar una carta con criptogramas escrita por Federico da Montefeltro, duque de Urbino, unos dos meses antes del atentado mortal contra Giuliano de Medici.[80] El texto aclarado permite saber muchos detalles del plan y los nombres de los conjurados.

Sin duda, este aporte criptológico a la investigación histórica de un caso definido es digno de nota, pero es oportuno reparar en que Simonetta gozó de una ventaja importante para sobreponerse al desafío de la carta cifrada sin verse forzado a improvisar ningún "ataque criptoanalítico": un manual de criptoanálisis y desciframiento redactado en el siglo XVI por su ancestro, Cicco Simonetta.[81] A este respecto, debemos entender que la deducción de reglas para facilitar un criptoanálisis —y esto es lo que hizo Cicco Simonetta— nunca puede anteceder al diseño de los métodos criptográficos, pues aquella deducción está basada en el análisis algorítmico de tales métodos (considerando que normalmente se asume el conocimiento público de éstos y el carácter secreto de las claves). Esto equivale a decir que constantemente se inventan cifras cuyas propiedades algorítmicas, obviamente, no se hallarán descritas o analizadas en ningún manual disponible al momento de su aparición. Ahora bien, si la ocurrencia de este fenómeno se observa normalmente, nada nos impide predecir —con la lógica probabilística de las hipótesis— su ocurrencia en el futuro y el pasado. Así, no deberá extrañarnos el que algún día se llegue a tener noticia de una cifra compuesta en el siglo XVI que jamás haya sido registrada técnicamente

[80] Laura C. Perillo, "A Renaissance Murder Mystery. How a Family Heirloom Helped a Wesleyan Professor Solve the Famous Italian Pazzi Conspiracy". Disponible desde Internet en: <magazine.wesleyan.edu/magazine/mag_archives/wm_04spr_w+.html> [con acceso el 08-11-2005], y Felicia R. Lee, "1478 Assassination Solved. The Humanist Did It", en *The New York Times*, March 6, 2004, p. 11.

[81] Cicco Simonetta fue secretario en jefe de Francesco Sforza y cabeza de la cancillería ducal milanesa. En las fuentes que consulté se afirma que Marcello Simonetta utilizó un manual de criptografía redactado por Cicco, y que ha pertenecido a su familia durante generaciones, pero no se asienta el título. Quizá se trate de una versión manuscrita de la obra *Regulae ad extrahendum litteras zifferatas sine exemplo*, fechada en 1474, *cf*. Galland, *op. cit.*, p. 171. Como sea, es interesante saber que el secretario de Sforza dedicó muchas páginas al criptoanálisis, como lo muestran sus *Diari* (edición de 1962), los cuales, entre otras muchas anotaciones, reúnen algunas acerca de las mejores estrategias para romper cifras de sustitución monoalfabética, véase Vincent Ilardi, "The Visconti-Sforza Regime of Milan: Recent Published Sources", en *Renaissance Quarterly*, v. 31, n. 3, Autumn 1978, p. 335-336.

por tratadistas contemporáneos de la criptografía; será preciso, entonces, caracterizarla formalmente y revisar las clasificaciones para colocarla en el sitio adecuado (en atención al supuesto lógico de que una cifra distinta, pero de la misma clase, podría nuevamente sorprender a un investigador). Pero hacer esto, si bien robustece nuestro conocimiento de la criptología general, en lo absoluto basta para que la clasificación de todas las cifras posibles se agote. Al contrario, debemos mantener la hipótesis de que el descubrimiento de cifras inéditas continuará indefinidamente.

Se sigue de todo lo anterior que los manuales o reglas de apoyo sólo por excepción ofrecen un servicio a los historiadores enfrentados a una cifra, no constituyen, pues, una garantía de la victoria criptoanalítica.

Hay ocasiones, por supuesto, en que decididamente lo hacen. Así lo muestra el caso de Marcello Simonetta —considerando específicamente las circunstancias de su investigación. Sin embargo, es indiscutible que Simonetta pudo elegir una opción diferente a la del manual: contratar un criptoanalista profesional para acceder al texto claro en la carta del duque. Y todavía le quedaba un tercer camino: romper la cifra utilizando sus facultades de observación y razonamiento como instrumental exclusivo. Personalmente, juzgo merecedor de un sumo respeto y de aclamación al historiador —sea, por ejemplo, uno especializado en temas novohispanos— que, hallándose en una situación análoga a la de nuestro colega italiano, elige sin vacilar el último procedimiento citado; él sabe (supongamos) que podría ejecutar la faena con un grado de seguridad y una velocidad relativamente mayor si echa mano de un manual o se asesora por un experto en criptología, no obstante, prefiere deliberadamente confiar en sus poderes de observación y razonamiento, ejercitándolos hasta inferir las mejores hipótesis explicativas de la cifra.

Es mi convicción que cualquier historiador, si se dispone al análisis criptológico en esta guisa, se encuentra lógica y metodológicamente autorizado para creer que sus descubrimientos bien pueden justificar la revisión crítica de determinadas tesis historiográficas, así como fijar las pautas lógicas para predecir el hallazgo de nuevos documentos cuya inspección y comparación podrían renovar las interpretaciones tradicionales de un fenómeno histórico dado. Veamos un ejemplo interesante de las posibilidades a este respecto. Como sabemos, varias crónicas de Indias transmiten que en 1524 el

contador Rodrigo de Albornoz, oficial real, envió a la corte una serie de comunicaciones en cifra para imputar supuestos crímenes o calumniar a Hernán Cortés;[82] ahora bien, hasta donde sé nadie ha descubierto ninguna de esas comunicaciones; en el presente ignoramos, pues, cuál fue el sistema criptográfico empleado por Albornoz; no obstante, la historia de la criptología revela que el método de cifrado más comúnmente utilizado en el siglo XVI fue el nomenclator, y esto determina la probabilidad de que Albornoz haya recurrido a ese mismo método, o bien a un método alternativo pero igualmente basado en la sustitución homofónica (esta segunda expectativa resulta adecuada para flexibilizar los alcances de la hipótesis, ya que la sustitución homofónica es propiamente la técnica criptográfica cuyo manejo extensivo generó la clase de cifras a la que pertenece el nomenclator, sin menoscabo de que este sistema en particular incluya la codificación de ciertos términos). Si admitimos como válida esta especie de inferencia inductiva, podemos lógicamente predecir que cuando hallemos las referidas cartas del contador Albornoz identificaremos en ellas cifras de nomenclator. Por supuesto, sabremos también cómo decriptarlas, y al hacerlo pondremos a disposición de los especialistas el texto más o menos aclarado —dependiendo de que logremos restituir el significado de los términos en código. Por otro lado, nos hallaremos en la posición de colaborar en la redacción de una historia de la "criptografía indiana", conforme al proyecto que Guillermo Lohmann trabajó tanto para impulsar. Desde luego, esto no cambiaría si descubrimos que Albornoz, o cualquiera de sus contemporáneos en la Nueva España, solía emplear un método radicalmente distinto al del nomenclator cuando cifraba partes de su correspondencia; supongamos, incluso, que Albornoz se valía de un método no clasificado todavía; si este resultara ser el caso (lo que no habrá de parecernos extraño, según lo explicado arriba), deberíamos agradecer la sorpresa, pues nuestra ganancia como razonadores e historiadores se duplicaría. En efecto, a la par que aumentaríamos el repertorio de ejemplares para ilustrar la proyectada historia de la "criptografía indiana" —lo que por extensión implica suplementar y renovar los contenidos de la historia general de la criptología— forzaríamos la actualización de las téc-

[82] *Cf*., por ejemplo, Bernal Díaz del Castillo, *Historia verdadera de la conquista de la Nueva España* (edición, índices y prólogo de Carmelo Sáenz de Santa María), México, Alianza Editorial, 1991, p. 679-684 (capítulo CLXXII).

nicas criptoanalíticas.[83] Sin duda, un corolario de todo esto sería el enriquecimiento de la metodología de investigación al uso para reconstruir la historia de México desde el siglo XV hasta la guerra de Independencia, cuando menos.[84]

Quiero terminar subrayando un hecho —o, al menos, lo que me parece conveniente subrayar como tal desde una perspectiva didáctica—: la práctica del criptoanálisis por cuenta personal es relativamente sencilla mientras se tenga la habilidad de identificar las cifras por sus clases y discriminar entre ellas, y también, por supuesto, de jamás confundirlas con meros ejemplares paleográficos. Una vez cumplido este requisito mínimo, queda reunir tanta paciencia como sea necesaria y desplegar lo mejor de las propias capacidades de observación y razonamiento lógico. Me parece válido afirmar que, en general, no debe ser preciso conocer a fondo ni las técnicas ni la historia de la criptología para adquirir competencia en el reconocimiento y "ataque" de las cifras clásicas. Arriesgo esta proposición considerando el caso de Francisco Monterde García Icazbalceta, quien, de acuerdo con los argumentos y las hipótesis que formulé, ignoraba muchos aspectos técnicos e históricos de la criptología y sin embargo rompió la cifra en la carta cortesiana de 1532. Como historiadores debemos apreciar y, cuando tengamos la ocasión, reproducir esa lección de razonamiento, poder de observación y paciencia, especialmente si recordamos que Monterde se condujo como un aficionado, pero esto no significa, en lo absoluto, que debamos descuidar el estudio de la técnica y la historia de la criptología, al contrario, lo mejor será familiarizarnos hondamente con ambas para optimizar la calidad lógica de nuestras inferencias al razonar sobre un objeto eminentemente definido por sus características formales, caso de un criptograma. Además, gracias a esta propedéutica evitaremos desde un inicio confundir los problemas paleográficos con los criptográficos en un texto, agilizando de tal modo nuestro empeño criptoanalítico.

Artículo recibido el 9 de noviembre de 2006
y aprobado el 10 de enero de 2007

[83] Para lo cual sería irrelevante que la cifra fuera decriptada por un criptoanalista profesional y no por un historiador.

[84] De acuerdo con lo explicado al promediar el apartado "Nombre y caracterización técnica del método criptográfico de Cortés".