

HISTORIA MEXICANA

Historia Mexicana

ISSN: 0185-0172

histomex@colmex.mx

El Colegio de México, A.C.

México

Narváez, Roberto

LOS DESPACHOS CODIFICADOS DE PABLO OBREGÓN DESDE WASHINGTON EN 1825.

ANÁLISIS Y DOS DECODIFICACIONES

Historia Mexicana, vol. LVIII, núm. 3, enero-marzo, 2009, pp. 1093-1153

El Colegio de México, A.C.

Distrito Federal, México

Disponible en: <http://www.redalyc.org/articulo.oa?id=60012798004>

- ▶ Cómo citar el artículo
- ▶ Número completo
- ▶ Más información del artículo
- ▶ Página de la revista en redalyc.org



Sistema de Información Científica

Red de Revistas Científicas de América Latina, el Caribe, España y Portugal
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

ARCHIVOS Y DOCUMENTOS

LOS DESPACHOS CODIFICADOS DE PABLO OBREGÓN DESDE WASHINGTON EN 1825. ANÁLISIS Y DOS DECODIFICACIONES

Roberto Narváez

Universidad Nacional Autónoma de México

INTRODUCCIÓN

En esta contribución ofrezco parte de los resultados que me ha deparado una investigación más amplia sobre el recurso a la criptología, o ciencia de los principios y los métodos de las escrituras secretas, por parte de individuos mexicanos —en especial diplomáticos y militares— desde la época colonial hasta promediar la década de 1920. Asimismo ya en artículos anteriores he procurado satisfacer un anhelo cuya persistencia motivó la redacción de estas páginas: mostrar la importancia del estudio de la criptografía y la práctica del criptoanálisis (ambos, la criptografía y el criptoanálisis, son los terrenos fundamentales de la aplicación criptológica) para fomentar la reflexión comprensiva, seria y consistente sobre los genuinos alcances de la inducción, la deducción, el razonamiento analógico y la hipótesis en la investigación histórica. En atención a tal objetivo, deberá entenderse que juzgo suficiente una concepción básica, marcada claramente por un afán propedéutico, de la historia de la criptología co-

mo fuente valiosa de ilustraciones sobre cómo un historiador puede utilizar la lógica científica en el análisis de los más diversos tipos de evidencia, pero en especial las evidencias de la clase que forman los criptogramas, esto es, textos en cifra o codificados.

Ahora, con el fin supremo de proporcionar evidencias, análisis e ideas para impulsar el desarrollo de la historia de la criptología en México, he dedicado este estudio, concretamente, a revisar una pequeña muestra de textos codificados enviados por el ministro Pablo Obregón al gobierno de México desde Washington en 1825. Pero también confío en que los frutos de mi labor podrían ser útiles para complementar las historias generales de la criptología con el capítulo que típicamente falta en ellas. En efecto, los autores de aquellas historias generales, en su mayoría originarios de o situados en países anglosajones, no se han tomado la molestia de incursionar en los archivos de México para localizar y estudiar documentos útiles para colmar la supuesta ambición de sus proyectos. Carece de importancia especular sobre sus motivos de fondo. El único hecho cierto es que las evidencias del recurso secular a la criptología en nuestro país existen y su cantidad es respetable. Si los historiadores foráneos las pasan por alto, nada nos obliga a seguir su ejemplo.

Ahora bien, la declaración de propósitos complementarios que acabo de hacer está libre de ambigüedad, sin embargo, no faltarán lectores a quienes les resulte difícil entenderla a cabalidad o, por alguna razón probablemente digna de nota —desde el punto de vista lógico-científico—, consideren en última instancia baladí la investigación histórica de la criptología mexicana. En relación con posturas parecidas, comento que si bien una investigación similar podría considerarse

inútil en algún sentido justificado, en todo caso es innegable el valor del criptoanálisis, o cuando menos de la imaginación analítica sustentada en los principios de la criptología, para la investigación de muchas clases de objetos, fenómenos y sucesos históricos. Sea, por ejemplo, la clase de objetos, fenómenos y sucesos de que se ocupa la historia diplomática. Esta historia se cultiva mucho en nuestro país, no obstante, a menudo la documentación total disponible para informarla con la máxima riqueza no se aprovecha plenamente. La explicación reside en que los historiadores de la diplomacia, con una frecuencia lo bastante elevada como para tomarla por una actitud excepcional, deliberadamente pasan sin leer legajos a los que con facilidad pudieron acceder en el archivo. Por este acceso sin trabas me refiero —y es preciso atender con cuidado a esto— al hecho de que tan pronto solicitan al archivista un documento dado, lo reciben. Pero más tarde, conforme avanzan en su lectura, se topan de manera inesperada con pasmosas dificultades para lograr un segundo y, naturalmente, más importante acceso a la información contenida en el documento. Esto se debe a que las líneas o párrafos en el soporte ante sus ojos están en cifra o codificados, y ellos ignoran cómo lidiar con cifras o códigos. Ahora, tras revisar un conjunto selecto de monografías, artículos y libros acerca de la historia diplomática mexicana, he terminado por convencerme de que la decisión normal de los investigadores puestos en semejante situación es dejar a un lado el material problemático y limitarse a escrutar los textos legibles. Deliberadamente, pues aunque sin una sola razón válida desde la perspectiva científica, esos autores eliminan de sus preocupaciones instrumentales a cualquier técnica derivada de o relacionada con la criptología (y la

lógica, por implicación) y, lo que es peor, abandonan una posible fuente de datos sin haberla sometido previamente a ninguna especie de crítica. Ni siquiera se esfuerzan, por lo visto, en consultar a profesionales de la criptología, la lógica, la lingüística o las matemáticas para salir del atolladero y proseguir su actividad inquisitiva según corresponde al historiador imaginativo, serio, intelectualmente responsable.

Es urgente poner manos a la obra para que ese modo inaceptable de actuar quede sin vigencia. Por mi parte, desde hace tiempo he localizado textos en cifra o código en varios archivos de México, y tras aplicar con paciencia el criptanálisis (o bien alguna técnica o estilo de inferir basado en el razonamiento lógico-matemático) conseguí descifrarlos o decodificarlos. De hecho, casi un cuarto del presente escrito está formado por la decodificación de dos despachos remitidos por el ya mencionado Pablo Obregón desde Washington en 1825, de manera que cualquier estudioso interesado podrá leerlos sin apuros, al fin, después de casi 185 años. Se trata de los números reservados tres (fechado el 23 de marzo) y 14 (fechado el 1º de noviembre).¹ Así, el valor de este artículo puede limitarse al de constituir un aporte documental, suponiendo que por algún motivo razonable se decida negarle uno más extenso.

Antes de presentar las dos decodificaciones mencionadas, repasaré con brevedad algunos aspectos de la gestión diplomática de Obregón en Estados Unidos durante 1825 y presentaré en orden una serie de consideraciones, argumentos y explicaciones técnicas y metodológicas referentes tanto al

¹ AHDSREM, leg. encuadrado L-E-1333, “Independencia de Cuba”, ff. 15-30bis y 10-12.

proceso de mi investigación como a las características peculiares del sistema codificador o “libro de códigos” —el cual mostraré asimismo, restituido en su virtual totalidad— utilizado por nuestro ministro en aquel año, con el objetivo último de propiciar una intelección eficaz de las ventajas que supone el conocimiento criptológico para potenciar los descubrimientos y alentar los análisis comparativos en los estudios históricos generales.

CUMPLIR INSTRUCCIONES CON EL APOYO DE UN CÓDIGO:
LAS ACCIONES DIPLOMÁTICAS DE PABLO OBREGÓN
EN WASHINGTON DURANTE 1825

El 4 de agosto de 1824, Pablo Obregón —ex oficial insurgen-
te de distinguida familia y diputado al primer Congreso— fue
nombrado enviado extraordinario y ministro plenipoten-
ciario ante el gobierno de Estados Unidos por el Supremo
Poder Ejecutivo de la primera República Federal mexicana.²
Obregón desembarcó en Nueva York el 21 de octubre de
ese año, y a finales del siguiente mes sustituyó oficialmente
en el cargo al coronel José Anastasio Torrens.³ Cumplida
su misión en 1828, cierta desventura personal le quitó los
ánimos de regresar a México y, más aún, de vivir: se suicidó
en Filadelfia. Era de maneras distinguidas y proceder cor-
tés, devoto en el servicio a su país y dotado de importantes

² ALAMÁN, *Historia*, t. II, p. 230 y t. V, p. 289. SALADO ÁLVAREZ, *Méjico en tierra yanqui*, p. 26. FLORES, “Apuntes para una historia”, p. 46.

³ FLORES, “Apuntes para una historia”, p. 47. TORRENS, *Primera misión*, pp. 86-87.

cualidades para ejecutar debidamente los encargos de la Primera Secretaría de Estado y del Despacho de Relaciones Interiores y Exteriores.⁴ Además, a juzgar por su precisión al describir un estado de cosas y la puntualidad de sus observaciones y opiniones en torno de cada asunto tratado, es claro el denuedo con el que trató de satisfacer por completo las instrucciones que Lucas Alamán le entregó en dos pliegos fechados el 30 de agosto de 1824.⁵ También es indudable que comprendía la importancia de las escrituras veladas en el ámbito diplomático, como lo pone de manifiesto el número ingente de notas o despachos que redactó en código durante 1825 y después, aunque en este escrito no mencionaré evidencias correspondientes al periodo complementario de su misión.⁶ Una vez decodificados, tales mensajes permitían al canciller Alamán enterarse de las actividades de Obregón tendientes a cumplir, entre otras, las siguientes instrucciones oficiales (tanto abiertas como reservadas): fomentar las relaciones armónicas entre México y Estados Unidos; penetrar la conducta política que seguiría el gobierno de este país en caso de que la Santa Alianza decidiera combinarse con España en un proyecto de reconquista; estar atento a las miras estadounidenses sobre los territorios de Nuevo México, California y Texas; establecer contactos en Cuba para fortalecer al partido que se inclinaba por unir políticamente a dicha isla con la República Mexicana tras librirla del yugo español, y no discutir la cuestión de límites con Estados Unidos hasta estar

⁴ FLORES, “Apuntes para una historia”, p. 51.

⁵ FLORES, “Apuntes para una historia”, pp. 47-49. CHÁVEZ OROZCO, *Un esfuerzo de México*, p. xxiv y n. 2. SALADO ÁLVAREZ, *Méjico en tierra yanqui*, pp. 29-30.

⁶ Véase la nota 26.

en mejor situación, formalizando, si era necesario, las justas reclamaciones con base en el tratado signado por Estados Unidos y España en 1819.⁷

Ahora bien, la serie documental formada con los envíos de Obregón constituye un pródigo surtidor de datos para investigar muchos aspectos de la diplomacia mexicana en los primeros años que siguieron a la independencia, así como la política exterior de múltiples potencias en relación con varios procesos nacionales latinoamericanos durante el primer tercio del siglo XIX. Los datos recurrentes en mayor porcentaje se relacionan con las políticas interna y externa de Estados Unidos; en el número tres reservado de 1825, por ejemplo —así lo comprobará quien lea la primera decodificación, más adelante—, nuestro ministro relata prolíjamente la situación que se vivía en ese país la víspera de las elecciones presidenciales de ese año, las conversaciones personales que sostuvo con políticos de renombre y sus esfuerzos para familiarizar hondamente al gobierno de Washington con los propósitos ulteriores del Plan de Iguala. Por tanto, no extraña que en obras de historia diplomática firmadas por mexicanos, españoles, colombianos, cubanos y estadounidenses, entre otros, abunden las inferencias históricas a partir de éstos y otros detalles legados por Obregón. Es una propiedad que acusan con especial insistencia las monografías y artículos donde se tratan los movimientos tempranos en favor de la independencia de Cuba y la importancia de tal fenómeno a los ojos de España, Estados Unidos, Colombia y México. El hecho

⁷ FLORES, “Apuntes para una historia”, pp. 48-49. Sobre el proceso de cumplimiento de las instrucciones para Obregón en torno de la independencia cubana, véase Rojas, *Cuba mexicana*, pp. 114-120, y DELGADO, *España y México*, vol. 1, pp. 249-250.

es comprensible, ya que Obregón situó entre sus prioridades a la, digamos, “cuestión cubana”.⁸ En sus mensajes claros o codificados virtió muchas declaraciones oportunas para el gobierno mexicano acerca de los intereses, las preocupaciones, las exigencias políticas o diplomáticas y los proyectos militares de cada país interesado en asegurarse los máximos beneficios —comerciales y militares, primordialmente— cuando las tensiones internacionales a propósito de la más grande isla caribeña llegaran a su fin, suponiendo que ese fin llegaría en un plazo razonablemente corto (un supuesto que, como se sabe, probó ser ilusorio). Lo cierto es que del significado, los pormenores y el resultado preliminar de estas inquietudes diplomáticas los historiadores han aprendido mucho gracias a los escritos ministrados por Obregón. Un servicio análogo han prestado los reportes de los espías y agentes secretos que laboraban para diferentes gobiernos o servicios consulares y diplomáticos.⁹ El mismo Obregón se sirvió de las noticias que le proporcionaban los contactos que estableció con independentistas en Cuba y patriotas cubanos refugiados en Filadelfia y Nueva York. Asistido por esta red de inteligencia logró introducir a Cuba copias de la Constitución Mexicana de 1824 y obtener impresos políticos cubanos para mantener al tanto de las opiniones contenidas en ellos a sus superiores en México.¹⁰

⁸ FLORES, “Apuntes para una historia”, p. 52.

⁹ Estos espías y agentes operaban desde ciudades-puerto como Nueva Orleáns, La Habana, Cayo Hueso, Kingston y Charleston, y para mantener secreta su identidad usaban pseudónimos y codificaban o cifraban sus reportes. MUÑOZ, *En el interés de la nación*, pp. 88-89.

¹⁰ FLORES, “Apuntes para una historia”, p. 52.

A propósito del uso historiográfico que se puede hacer de las cartas, despachos o notas cursadas por diplomáticos, espías y agentes secretos, muchos investigadores, recordando sus experiencias personales en los archivos, no vacilarían en suscribir una declaración como la siguiente, en especial su segunda parte:

La actividad abierta puede seguirse, con las debidas reservas, por los testimonios preservados en la documentación oficial, mientras que la secreta, por su mismo carácter y aunque también está registrada en buena medida en la correspondencia, no permite conocer a todos los personajes involucrados ni ofrece un panorama completo de las actividades llevadas a cabo.¹¹

Por “actividad abierta” la autora de estas líneas se refiere a la que llevaron a cabo los diplomáticos, espías y agentes secretos de 1821-1830 en la zona del Caribe. Ahora, lo que he interpretado como segunda parte de la cita es el comentario en torno de la, por así decir, opacidad característica de la “documentación secreta”. Impera en el mismo un tono de fatalidad que es necesario someter a crítica. Para empezar, me parece indudable que la expresión “documentación secreta” es un modo de aludir a textos codificados o cifrados. Por tanto, el mensaje final del pasaje transcrita debe ser que las fuentes secretas son tales porque su lectura inmediata es imposible. Constituye un error admitir una interpretación similar, básicamente por cuanto en ella domina la creencia en que la meta de la criptografía es restar total o parcialmente la legibilidad a un texto. Esto es un equívoco, tanto como lo

¹¹ Muñoz, *En el interés de la nación*, p. 86.

sería pensar que una llamada telefónica inicia y termina con la digitación del número en el teclado, dispensando de toda función al conmutador, la línea, y los demás elementos que integran al teléfono; en realidad, los pasos de cifrado o codificación forman parte de una serie de pasos más abarcadora tendiente a consumar el designio verdadero de la criptografía: brindar seguridad a la comunicación que un sujeto identificado, el emisor, quiere hacer llegar a otro identificado, el receptor.¹² La criptología es una rama de las matemáticas, pero la modalidad específica de su funcionamiento y, en rigor, su carácter científico se aprecia mejor cuando se la comprende en una teoría general de las comunicaciones.¹³ El hecho de generar un criptograma, esto es, volver ilegible a una pieza de texto plano¹⁴ escrito en cualquier idioma, implica una operación de ciertas funciones matemáticas. A todo criptograma —ya sea una cifra o un código— subyace una operación matemática (en la criptografía clásica o manual, de la cual los códigos de Obregón son ejemplares, lo regular es que tal operación sea de clase aritmética)¹⁵ que provoca en un idioma el desorden u ocultamiento de los caracteres a determinado nivel lingüístico (de la sintaxis o la semántica).

¹² DIFFIE y HELLMAN, “New Directions”, p. 645. BAUER, *Decrypted Secrets*, pp. 25-26.

¹³ Véase SARUKKAI, “Mathematics, nature and cryptography”, especialmente pp. 1690-1691.

¹⁴ Técnicamente se denomina texto plano al mensaje que se va a transmitir en cifra o código. Se formula como un vocabulario criptográfico constituido por un conjunto de caracteres (generalmente letras) relacionado con un vocabulario correspondiente al género de criptograma (de ordinario una cifra o criptotexto) que se va a generar. BAUER, *Decrypted Secrets*, pp. 31 y 38.

¹⁵ MOLLIN, *An Introduction*, pp. 1-2.

En rigor, esto lo caracteriza, y no su circunstancial aspecto enigmático. Transformar un documento en cifra o código responde, sin más, al deseo de asegurarla contra el escrutinio de cualquier potencial tercer sujeto (un espía, digamos) no autorizado para leerlo. Y devolver la claridad a un texto en cifra o código demanda revertir el procedimiento criptológico (en principio, matemático) que se utilizó en su cifrado o codificación particular, y nada más. Semejante reversión, técnicamente, se denomina criptoanálisis.¹⁶ Un historiador puede aplicarlo a “documentos secretos” y, si lo hace bien, tendrá el júbilo de ver desplegarse ante sí “panoramas completos” o cualquier otra cosa que se digne asomar.

Concentrando nuevamente la atención en los despachos codificados de Pablo Obregón, muchos de ellos fueron aclarados o “traducidos” (como solía decirse antaño) por empleados de la Primera Secretaría de Estado y del Despacho de Relaciones Interiores y Exteriores tan pronto como los recibieron. Las versiones aclaradas han sido compulsadas hasta la saciedad por los investigadores. Sin embargo, varios de esos despachos, por alguna razón que ameritaría una indagación cuidadosa, terminaron en los archivos oficiales sin decodificar.¹⁷ Así ocurrió con un par de los que envió en 1825, actualmente conservados en el Acervo Histórico de la

¹⁶ BAUER, *Decrypted Secrets*, p. 31. LUCIANO y PRICHETT, “Cryptography”, p. 3.

¹⁷ Véase el documento “Año de 1825. Correspondencia reservada del Sr. Obregón de este año”, en AHDSREM, L-E-1333, ff. 31-32, donde aparece registrado cada número recibido con su correspondiente fecha y se apunta si el principal y el duplicado estaban en “cifra” y habían sido o no ya “traducidos” —como se decía entonces. También se relacionan los apellidos de las personas que los entregaban y/o traducían.

Secretaría de Relaciones Exteriores de México (en adelante AHDSREM). Se trata de los ya referidos números 3 y 14 reservados, justo los que decodifiqué. Específicamente se hallan disponibles en el legajo encuadrado L-E-1333 rotulado “Independencia de Cuba”. Es de advertir, sin embargo, un hecho muy significativo para los fines de este escrito: los historiadores comúnmente consultan los materiales ya decodificados de ese legajo según la forma que asumieron al ser publicados en libros. Los especialistas en la independencia cubana, por ejemplo, típicamente los estudian o bien en la recopilación *Un esfuerzo de México por la independencia de Cuba* (1930), prologada por Luis Chávez Orozco, o bien en el tomo I de la obra *México y Cuba. Dos pueblos unidos en la historia* (1982). A las transcripciones se agrega, incluso, la nota “Traducción” o “Traducción íntegra” que originalmente puso el decodificador en la parte superior de la primera foja. Pero es en *Un esfuerzo de México...* donde sólo en una ocasión se hace constar que la parte impresa en cursivas del reservado número 4 de Obregón (3 de marzo de 1825) estaba “cifrado” en el original. Es una comprobación muy interesante para la historia criptológica, revela que los editores de ese volumen tomaban sin más a una cifra por un código —lo cual es hasta cierto grado censurable, ya que Obregón usaba códigos y no cifras, como lo explicaré puntualmente—; además, mueve a extrañeza porque en los originales de por lo menos cinco documentos editados junto al recién mencionado descuellan las evidencias de que originalmente fueron códigos —y si por costumbre o confusión se los puede llamar cifras, el caso es que se trataba de criptogramas—. Por tanto, resulta difícil explicar que cuando una misma característica incide en el aspecto de seis

objetos de clase idéntica, los editores la hayan observado en uno solo de ellos.

Además, he comprobado que los prologistas o presentadores de los libros mencionados no dedican siquiera una mínima digresión analítica —como sería lo apropiado en una crítica textual consecuente— sobre la calidad de la evidencia tal y como fue recogida. Jamás anotan el número exacto de los documentos que yacen decodificados o aún codificados en el legajo, y en relación con los del último tipo descuidan informar a todo lector potencial —erudito, lego, quien sea— de que su ausencia en el libro se debe a que su decodificación, al momento de realizar la edición, había sido impracticable por alguna circunstancia de clase bien definida. Porque tales decodificaciones, conforme a lo que argumentaré más adelante, no estaban disponibles ni en 1930 ni en 1982. En ambos momentos hubiera sido lo justo apuntar los motivos de que fuera tan difícil volver legibles los textos en cuestión. Este acto, de haberlo consumado los escritores aludidos, bien merecería nuestro aprecio como una vigorosa manifestación de responsabilidades intelectual, editorial e historiográfica.

Como sea, es evidente que no lo consumaron. A mi juicio, esto sólo admite la explicación siguiente: los editores de los volúmenes considerados nunca se esforzaron en criptoanalizar los despachos de Pablo Obregón que encontraron sin “traducir”. Porque es obvio: si fracasaban en su criptoanálisis, las razones de su fracaso —supuesto que todo análisis, por la sola consistencia semántica de su definición, implica una operación fundamentalmente discriminadora— deberían mostrarse ante sus ojos con tanta nitidez como lo permitiera la crítica racional de su propio método, de suerte que una exposición posterior de los resultados de esa crítica fluyera

sin el peligro de caer en contratiempos analíticos imprevisibles. Por otra parte, esa exposición la habrían podido aprovechar los prologuistas o presentadores para optimizar la eficiencia introductoria de sus respectivas contribuciones. Pero este suceso, de acuerdo con la evidencia disponible, no se verificó. Ahora bien, una hipótesis formulada sobre la premisa *ad hoc* de que los editores criptoanalizaron con éxito los documentos en cuestión, suscita una inferencia muy interesante, mucho más significativa para dejar de preguntarse por la razón de que los prologuistas o presentadores omitieran cualquier comentario a las cualidades criptológicas de los despachos de Obregón y proponer, en cambio, una explicación sólida de que las ediciones acabaran por no incluir los textos aún codificados. En efecto: si los editores decodificaban los manuscritos, no forzosamente debía seguirse que los editaran, pues como se comprenderá, la ya posible lectura inmediata podía revelar que las noticias u opiniones de Obregón nada tenían que ver con la independencia de Cuba. Pero como de dicha lectura sí emergen copiosas noticias, detalles y opiniones en relación con acciones primigenias en favor de la independencia cubana, según lo juzgará patente quien lea las dos decodificaciones *infra*, resulta lógico concluir que ni los editores de *Un esfuerzo de México...* ni los de *Méjico y Cuba...* gozaron de ella; esto equivale a decir que no criptoanalizaron ninguno de los dos manuscritos en cuestión, por tanto, seleccionaron las piezas que se editarían de una provisión total que mutilaron sin el menor escrupulo científico.

Me parece improbable que en el corto plazo algún crítico se hallará en la posición de oponer objeciones de peso, criptológicas o de otra índole, a mi argumento; por lo pronto,

una estimación atenta de su validez impone la conclusión de que hasta hoy se careció de las decodificaciones tratadas.

EL MÉTODO CODIFICADOR UTILIZADO
POR OBREGÓN EN 1825

En las figuras 1 y 2 puede observarse el aspecto que asumían los despachos reservados de Obregón cuando éste los redactaba en código.

Ambas figuras muestran los resultados de un método de transformación criptográfica sobre cuyas características técnicas fundamentales, los elementos básicos que determinan su clasificación, y su aprovechamiento frecuente mediante la historia, lo indispensable que se debe decir (incluso para fines comparativos) es lo siguiente:

1. Se trata de una transformación a código y no a cifra. Siempre conviene distinguir entre cifras y códigos cuando se investigan ejemplares criptológicos. Mi lector se habrá percatado de la invariabilidad con la que desde un inicio he calificado de códigos a los despachos inmediatamente ilegibles de Obregón. Mis razones para expresarme de tal modo son de orden técnico, derivan de consideraciones lingüísticas y matemáticas y el deseo de utilizar un vocabulario preciso, apto para la elaboración de hipótesis tendientes a explicar todos los hechos relativos a evidencias del género representado por un objeto científicamente definido, como es el caso de un criptograma. Un código es un criptograma de una clase, una cifra es un criptograma de otra clase. Difieren entre sí por cuanto el primero se forma de acuerdo con un procedimiento inaplicable para originar a la segunda. Cifrar implica

Figura 1

UNA PLANA CODIFICADA DEL RESERVADO NÚMERO 3

(23 DE MARZO DE 1825)

42. 11. 25. 58. 42. 12. 21. 12. 67. 11. 44. 16. 11. 22. 43. 32. 116. 22. 61. 22. 1.
32. 212. 413. 214. 19. 415. 617. 12. 412. 23. 125. 421. 622. 23. 12. 613. 31. 212. 21.
23. 616. 63. 614. 69. 614. 49. 45. 312. 69. 42. 9. 112. 422. 12. 52. 113. 121.
314. 621. 121. 614. 311. 42. 12. 32. 416. 422. 43. 116. 63. 12. 324. 416.
422. 321. 22. 121. 62. 212. 24. 613. 23. 616. 32. 112. 221. 121. 222. 214. 22.
618. 12. 412. 23. 614. 12. 46. 12. 214. 36. 23. 22. 112. 619. 11. 321. 214. 416.
26. 121. 422. 32. 321. 22. 619. 14. 212. 27. 11. 126. 221. 422. 121. 26. 33. 11.
321. 322. 218. 217. 42. 113. 212. 24. 14. 11. 32. 221. 12. 512. 414. 34. 412. 34.
212. 121. 616. 32. 221. 421. 23. 34. 321. 32. 212. 32. 33. 11. 126. 212.
414. 121. 42. 222. 314. 418. 118. 12. 212. 32. 121. 122. 62. 13. 33. 614.
612. 13. 11. 20. 616. 21. 117. 32. 112. 614. 216. 12. 619. 11. 43. 42. 121. 422.
43. 11. 32. 11. 412. 19. 613. 22. 17. 22. 43. 11. 615. 11. 212. 17. 22. 11. 41.
121. 222. 114. 23. 11. 34. 112. 12. 22. 422. 112. 512. 32. 121. 222. 12. 312.
421. 414. 314. 422. 37. 34. 22. 112. 32. 112. 42. 34. 116. 314. 212. 121.
118. 42. 12. 116. 32. 221. 312. 43. 616. 22. 412. 32. 23. 612. 12.
212. 67. 212. 121. 27. 22. 23. 19. 415. 32. 416. 22. 116. 32. 414. 32.
422. 42. 66. 117. 24. 314. 114. 422. 612. 14. 213. 32. 121. 60. 116. 32. 215.
227. 62. 612. 121. 32. 121. 616. 416. 212. 121. 32. 614. 32. 116. 32. 212. 612.
612. 213. 212. 121. 32. 212. 121. 612. 14. 11. 616. 612. 14. 616. 32. 212. 612.
32. 215. 412. 121. 314. 14. 421. 126. 414. 612. 101. 612. 16. 321. 221. 10.
612. 32. 34. 117. 22. 214. 12. 212. 22. 118. 32. 23. 324. 12.

Figura 2

PRIMERA FOJA DEL RESERVADO NÚMERO 14

(1 DE NOVIEMBRE DE 1825)

5714. P.

5715 411 615 311 520 572 22 320 324 120 224 54 44 67 15 11
 124 15 619 15 516 321 28 42 11 122 220 415 121 418 220 54 215
 123 19 212 320 521 612 43 516 34 212 27 214 220 24 320 418
 320 221 45 222 115 320 121 521 12 220 515 20 321 24 120 W.
 112 521 412 42 622 14 24 112 221 516 120 118 220 421 34 115
 222 215 220 221 20 120 122 520 218 121 34 112 322 120
 420 520 420 117 24 212 520 618 12 412 22 52 115 312
 52 310 522 24 11 63 412 220 212 415 24 218 115 34
 116 42 11 24 212 126 123 212 34 62 22 214 121 11 212 118
 220 221 115 322 52 120 320 212 515 422 43 11 315 122
 220 512 121 28 224 515 520 121 514 44 220 54 121 126
 522 220 113 218 120 521 216 124 34 621 43 120 62 513
 24 63 215 522 28 218 224 54 215 221 322 245 57 42 114
 220 46 420 715 54 221 11 512 121 619 15 24 221 322 246
 422 66 520 515 11 221 11 43 64 24 324 222 620 514 120
 515 215 24 44 121 114 615 420 11 212 221 418 420 622
 618 12 412 52 24 212 126 122 212 218 520 121 221 420 11
 59 114 82 415 515 222 515 28 33 120 52 115 46 715 227 34
 218 120 521 215 121 222 115 415 44 221 23 320 222 121 24
 116 513 120 221 67 220 218 522 318 44 43 515 52 514 220 522

transformar un texto a nivel de los caracteres —incluyendo, a veces, los espacios en blanco— y las letras, codificar implica transformar un texto a nivel de las sílabas y las palabras.¹⁸

2. Una cifra se puede concebir como un conjunto matemático en donde los elementos se ocultan mediante una encriptación o método de cifrado al que corresponde un proceso de descifrado.¹⁹ El llamado texto plano se esconde por la encriptación y se vuelve un criptotexto. El criptotexto puede consistir en números, letras de un alfabeto conocido o inventado, o símbolos (tampoco necesariamente conocidos). Lo convencional es que los caracteres tanto del criptotexto como del texto plano sean del mismo tipo, formando así para ambos un mismo alfabeto de definición (entendido como un conjunto finito).²⁰ Se puede representar al mensaje claro a cifrar, M , por una cadena finita de caracteres del alfabeto finito Σ . Usamos $e(M)$ para denotar “cifrado de M ”; sea d la función de desciframiento y con ello podemos satisfacer la relación fundamental $d(e(M))=M$ para todos los mensajes M . En la práctica, e puede tomarse como la función o algoritmo con una colección de parámetros. Cada parámetro es lo que se denomina la clave del criptosistema, denotada usualmente por K . En la criptografía clásica fue la norma echar mano de claves, pero se debe saber que muchos criptosistemas no las incorporan. Cuando lo hacen, la cadena de encriptación $C=e(M, K)$ es la cifra o criptotexto, mientras que el desciframiento obedece a $d(C, K)=M$, donde M representa al texto plano.²¹

¹⁸ MOLLIN, *An Introduction*, p. 8.

¹⁹ BAUER, *Decrypted Secrets*, p. 33.

²⁰ MOLLIN, *An Introduction*, p. 76.

²¹ WELSH, *Codes and Cryptography*, pp. 105-106.

3. Ahora bien, el código también consiste en procedimientos transformadores del texto plano, dado su efecto de conversión de piezas legibles a secretas. En un sentido, por tanto, es un criptosistema. Sin embargo, la codificación no se confunde con el proceso total básico del cifrado al estar prácticamente libre de sujeción a cualquier algoritmo funcionalmente generado. En una palabra, es lo normal que en la descripción de los códigos, particularmente los diseñados durante la era clásica de la criptología, rara vez participen las nomenclaturas originadas en diversas áreas de las matemáticas —en especial la aritmética modular— y la lógica de conjuntos. Esto se explica, ante todo, por el hecho de que la creación y operación de un sistema codificador no se controlan por medio de claves. Así, un sistema parecido no permite variaciones deliberadas en la encriptación, razón fundamental para distinguirlo del criptosistema basado radicalmente en procesos de cifrado. Veamos este punto con más detenimiento. Una clave permite al criptógrafo cambiar con periodicidad los pasos de encriptación de acuerdo con reglas simples fijadas previamente, si se estima que así lo requiere la seguridad del criptosistema. La complejidad combinatoria de cada método de cifrado se determina por el número de claves disponibles.²² Quien constantemente se sirve de una misma clave para cifrar pone a su sistema en riesgo de ser “penetrado” o “roto” —para decirlo en el argot del criptoanálisis— por un eventual espía, pues lo constriñe a funcionar con un sólo elemento. Por esta razón, la mayoría de los criptógrafos profesionales, en todas las épocas, han evitado las encriptaciones fijas. La situación cambia al

²² BAUER, *Decrypted Secrets*, p. 40.

tratarse de códigos, dado que funcionan por el ocultamiento de letras agrupadas o palabras completas y no de caracteres individuales. Esto significa que la codificación es eminentemente multigráfica y demanda ceñirse a rutinas técnicas de sustitución especiales. En efecto, una clave participa en un algoritmo matemático cuya función es remplazar una letra por otra letra o por un símbolo, signo o carácter especial, pero es inútil cuando se trata de ocultar los monogramas (esto es, cada una de las letras del alfabeto claro) y, sobre todo, los multigramas de diferente extensión en que se puede dividir una palabra por lo menos bisílaba. Es posible, sin duda, establecer bigramas (grupos de dos letras), trigramas (grupos de tres letras), tetragramas y conjuntos aún mayores por algún método de cifrado, mas ello equivaldría tan sólo a yuxtaponer elementos individuales cifrados por separado y con eso formar lo que se denomina un libro de códigos. Pero este sistema podría generar, entre otras, la magna dificultad de manejar un libro de códigos muy voluminoso, tanto como para reunir montos enormes de caracteres cifrados y sus respectivos equivalentes uno por uno. Para prevenirse contra una incomodidad así, lo ideal es formular y enlistar las partes de un código completo con el menor número de elementos, en definitiva, aplicar un sistema de sustitución alternativo al del cifrado mecanizado por funciones matemáticas —como lo consiguió magníficamente Pablo Obregón, según lo explicaré. Semejante alternativa es la codificación, que permite encriptar decenas, centenas o miles de los multigramas más frecuentes y ordenarlos en un cúmulo razonablemente disminuido de páginas. Un código puede graficarse como C cuando su determinación lingüística proviene de las letras del alfabeto, las sílabas, los diptongos, triptongos, prefijos y

sufijos, las frases hechas y demás componentes propios de cada idioma, que constituyen los elementos planos que se han de esconder. Estos elementos se inscriben en una columna paralela a la de los equivalentes, fijándose de tal modo la relación transformadora de uno a uno. Así se confecciona, en rigor, un libro de códigos. Los equivalentes asumen típicamente la forma de letras-código, palabras-código, o números-código.²³ La asignación de cada equivalente puede responder al capricho personal o reproducir sistemas comunes de ordenamiento lexicográfico o matemático, aunque el nivel de vulnerabilidad a que se verá expuesto el código íntegro podría verse afectado por la elección final. Si marginamos un momento la importancia fundamental de este detalle, se torna lícito decir, con el propósito de aclarar a fondo el concepto de código por una comparación elementalmente técnica con el de cifra o criptosistema, que en los códigos el alfabeto de definición es demasiado grande, tanto como para volver improbable una hipótesis criptoanalítica en el sentido de que fue la letra sola, y no el multigrama, lo que funcionó como unidad básica del texto plano.²⁴

4. Pero los códigos, como he dicho, son encriptaciones fijas. Por esta razón es relativamente fácil ubicar grietas en sus dispositivos de protección. Sin embargo, las especificaciones propias de su peculiar sistema de formación determinan de tal modo sus cualidades criptográficas, que normalmente resisten los ataques criptoanalíticos con un vigor superior al de las cifras. Esto se confirma especialmente por la inves-

²³ BAUER, *Decrypted Secrets*, p. 66. Para un análisis de un caso similar en el ambiente político y diplomático español durante el reinado de Fernando VI, véase LORENZO CADARSO, “Los documentos cifrados”, p. 375.

²⁴ KAHN, *The Codebreakers*, p. XIV.

tigación histórica del recurso a la criptología en el ámbito diplomático; en efecto, hay evidencia de que muchos embajadores, cónsules, ministros extraordinarios y espías llegaron a utilizar durante meses o años un mismo libro de códigos en su intento de preservar la seguridad de su correspondencia secreta.²⁵ El examen atento de los aspectos formales, pero sobre todo, cronológico en sus despachos codificados, indica que Obregón procedió justo de esta manera.²⁶

5. En la evolución de la criptología occidental destacan dos tipos principales de códigos, los de una parte y los de dos partes. Un código de una parte consiste en la sustitución de cada elemento del texto plano, regularmente al nivel de las letras, con un carácter existente o inventado. Es un caso de la denominada sustitución monoalfabética, libre del control de cualquier clave y basada en el empleo de símbolos diferentes entre sí, pero que representan una misma letra del texto plano, técnicamente denominados homófonos,²⁷ como equivalentes de código. Se lo denomina “de una parte” porque su función está limitada a relacionar cada letra con su correspondiente homófono —símbolo, letra, o número, por unidad o agrupados—, respetando las habituales ordenaciones lexicográfica y matemática. Pero el sistema también podía efectuar un similar ejercicio de mapeo con multigramas,

²⁵ BAUER, *Decrypted Secrets*, p. 40.

²⁶ Tengo evidencias de que Obregón utilizó por lo menos una vez este código en 1826. Se trata de un documento parcialmente codificado cuyo texto plano he recuperado. Lo daré a conocer en un escrito posterior.

²⁷ GALENDE, “Principios básicos”, p. 53. Para definirlo en contraste con el fenómeno de la polifonía (véase nota 38), un homófono es cualquier palabra del vocabulario del criptotexto asignada a una misma palabra del vocabulario del texto plano, en la relación de encriptación descrita en la nota 14. Véase BAUER, *Decrypted Secrets*, p. 32.

por ejemplo, términos coloquiales o técnicos de uso muy repetido. El denominado *nomenclator* o nomenclador es una especie de criptosistema híbrido donde se mezclan cifras y los productos de un sistema codificador de una parte.²⁸ Su utilización fue preponderante en Europa y muchas latitudes americanas desde el siglo XIV hasta las primeras décadas del XX.²⁹ Sin embargo, adolece de una desventaja grave: dado que los elementos de código, agrupados o por unidad, reproducen las condiciones de aparición discursiva normal de los caracteres que se han de ocultar, la frecuencia de ambos en el mensaje oculto es lógicamente la misma; si con ese criptosistema, por ejemplo, se sustituye la e con, digamos, el signo &, entonces, dado el hecho lingüístico que esa vocal es una de las más frecuentes en idiomas como el español, es apropiado establecer la hipótesis criptoanalítica de que & equivale a e en el código (mejor dicho, y para expresarlo genéricamente, en el criptotexto).³⁰ Basta, así, un análisis de frecuencias para configurar hipótesis valiosas —hipótesis y

²⁸ Si bien esto es admisible con algunas reservas técnicas para determinados ejemplares. El nombre de este sistema se adoptó por referencia al oficial que, en los palacios regios, tenía la función de anunciar a los dignatarios visitantes enfatizando sus títulos. La voz *nomenclator* (también *nomenclador*) proviene del latín *nomenclātor*, *nomenclātoris*, compuesto con la raíz del arcaico *calare*, “llamar”. COROMINAS, *Diccionario crítico*, 1976, vol. III, p. 520. Sobre la trayectoria histórica del nomenclator véase KAHN, *The Codebreakers*, p. xv.

²⁹ Durante la revolución mexicana y por lo menos hasta 1930, varios personajes destacados de la política y el periodismo se auxiliaron de *nomenclators* para salvaguardar sus mensajes confidenciales. Un caso que he podido revisar con atención envuelve a los hermanos Flores Magón.

³⁰ Lo cual es válido, sobre todo, al tratar de *nomenclators*. Sobre la frecuencia de las vocales específicamente en el idioma castellano véase GALENDE, “Principios básicos”, pp. 48-49.

no meras conjeturas, dado que las premisas dispuestas por el conocimiento lingüístico y matemático faculta la predicción a comprobar deductivamente —acerca del valor de cada incógnita en la pieza escrutada.³¹ De este modo procedió el escritor Francisco Monterde García Icazbalceta en 1925 para romper las cifras generadas con unas tablas de *nomenclator* en una carta de Hernán Cortés.³² Es un hecho pues, que si una estimación estadística nos permite descubrir el equivalente en texto plano de un código o un grupo de códigos con un elevado nivel de certidumbre, podemos lógicamente inferir que todos los códigos del libro ubicados debajo equivaldrán, muy probablemente, a las restantes porciones del texto plano situadas en igual orden decreciente en el diccionario de la lengua o, si es el caso, en la serie de todos los números naturales. De este modo se funda una regla para predecir la estructura general y el sistema de funcionamiento del código analizado, predicción que regularmente se verifica.³³ Cuando en 1914 fue capturado el crucero Magdeburg de la Kaiserliche Marine alemana, en su interior se halló un *Signalbuch* cuya decrptación (éste tuvo que ser el procedimiento, pues se carecía de las correspondencias)³⁴ permitió reordenar los elementos

³¹ SINKOV, *Elementary Cryptanalysis*, pp. 16-20.

³² Sin embargo de que Monterde no supo explicar técnicamente su procedimiento cuando tuvo la oportunidad, además, ni siquiera intentó formular alguna hipótesis tendiente a dar cuenta de los códigos en la carta cortesiana. Véase NARVÁEZ, “Historia y criptología”, pp. 31-36.

³³ BAUER, *Decrypted Secrets*, p. 69.

³⁴ Se habla de decriptar una cifra o código cuando se desconocen las reglas de transformación o el criptosistema que se siguió en su creación. En caso contrario se habla de descifrar o decodificar, según el caso. A la decriptación, en el ámbito hispanoamericano, también se la conoce como “perlustración”, véase GALENDE, “Sistemas criptográficos”, p. 58.

claros y codificados, lo que reveló una secuencia paralela numérica y lexicográfica entre los códigos y los elementos del texto plano. Por ejemplo, el grupo 63940 tenía el equivalente claro “Ohnmacht, -ig”; 63941 equivalía a “Ohr, Ohren-”, 63942, “Okkupation, Okkupations, -ieren”, y así.³⁵

Se habla, en cambio, de un código de “dos partes” cuando su estructura surge de entreverar códigos numéricos o literales. El objetivo primario de este método es dificultar el análisis de frecuencias. Aquí es lícito reproducir el ordenamiento lexicográfico o matemático, sin embargo, la multiplicación de los códigos vuelve difícil el proceso autorizado de decodificación porque a cada elemento del texto plano le corresponden dos, tres o más equivalentes, y ya no sólo uno. El procedimiento aún califica como de sustitución, la cual se puede realizar con homófonos o grupos numéricos, excepto que ahora cada monograma o multigramma se puede sustituir con múltiples homófonos, grupos de dígitos, o una mezcla de homófonos y de grupos numéricos.³⁶ Lo mismo sucede cuando la sustitución es eminentemente poligráfica, esto es, definiendo a los bigramas, trigramas o multigramas de mayor longitud como las unidades básicas de sustitución. En la práctica se inicia colocando las listas de códigos y sus respectivos equivalentes en dos columnas lado a lado; una lista es para codificar, la otra para decodificar. Se obtiene como ventaja principal que el decodificador puede acelerar su labor. Todo esto, en fin, pone de manifiesto una similitud formal y de sentido práctico entre los códigos de dos partes y los diccionarios bilingües.³⁷

³⁵ BAUER, *Decrypted Secrets*, p. 70.

³⁶ BAUER, *Decrypted Secrets*, p. 69.

³⁷ Merced al desarrollo de un expediente similar, hacia 1630 Antoine Rossignol impulsó un adelanto vital en los sistemas usuales de formación de

6. En el siglo XVIII, cuando los *nomenclator* podían tener hasta tres mil entradas, los criptógrafos comenzaron a diseñar libros de códigos basados en propósitos y condiciones técnicas relativamente novedosas. En ocasiones acusaban todavía algunas características del *nomenclator* típico, por ejemplo, sustituir nombres propios con un solo grupo de códigos y demandar un vasto espacio para su redacción manuscrita y eventual impresión —sobre todo si junto a los homófonos empleaban la sustitución polifónica—,³⁸ sin

nomenclators. En colaboración con su hijo, Bonaventure, diseñó un código de 587 elementos que repelió las embestidas criptoanalíticas durante más de cuatro siglos y medio. BAUER, *Decrypted Secrets*, p. 70. Es interesante recordar que varios pensadores europeos del siglo XVII, interesados en fundar un lenguaje universal, articularon a menudo sus análisis del valor didáctico y mnemotécnico de la lexicografía con una reflexión sistemática sobre las propiedades de los textos en cifra o código, y las ventajas que puede conllevar su utilización. Destacan casos como el de John Wallis (él mismo un criptógrafo eminente); Seth Ward y John Wilkins entre los miembros de la Royal Society of London, y Leibniz y Athanasius Kircher entre los filósofos de la Europa continental que con mayor avidez procuraron fijar un “carácter universal”. Pero es entre la clase de códigos que venimos revisando y la propuesta del inglés Cave Beck hacia el idioma universal donde resaltan con singular brío las analogías formales, teóricas y técnicas; en *The Universal Character* (1657) Beck estableció como caracteres los números arábigos del 0 al 9; ordenó sus combinaciones —cada una expresaba los términos primitivos de cada lengua— progresivamente del 1 al 10 000 (número que para él bastaba para expresar todos los términos de uso general); a cada número correspondía un término de cada lengua; de este modo produjo un diccionario cuyos términos se organizan alfabéticamente de acuerdo con las diferentes lenguas; cada diccionario resultante funciona, entonces, como “clave” del otro. ROSSI, *Clavis universalis*, pp. 186-188 y 196-197. Véanse también SINGER, “Hyeroglyphs”, p. 57, y COHEN, “On the Project”, p. 53.

³⁸ Para definirla por contraste con la sustitución homofónica (véase la nota 27), la sustitución polifónica se realiza por asignación de palabras del texto plano a una misma palabra del criptotexto. BAUER, *Decrypted Secrets*, p. 35.

embargo, a diferencia del *nomenclator* su capacidad de almacenamiento podía colmarse a satisfacción con decenas o, a lo sumo, centenas de códigos.³⁹ Es apropiado describir el sistema de formación de estos artilugios como una mera colección de palabras, sílabas y letras arregladas y numeradas arbitrariamente.⁴⁰ Pero de aquí se sigue como una fundamental consecuencia impedir la reproducción del convencional ordenamiento numérico o lexicográfico. Durante la revolución de independencia de Estados Unidos fueron profusamente utilizados. Los delegados de Virginia al Congreso de 1782 se sirvieron de uno con 846 códigos-número en su correspondencia secreta oficial.⁴¹ Lo propio hizo Thomas Jefferson, ese genial y prolífico creador de sistemas criptográficos, para intercambiar epístolas con señeros “padres fundadores” como James Madison y James Monroe.⁴² Tampoco fue parco en su empleo de la codificación para mantenerse en contacto con su secretario William Short mientras éste cumplía una misión diplomática en Francia (1790-1792). Al aparejar su libro de códigos, Jefferson y Short convinieron, por ejemplo, en que el pronombre *I* se sustituiría con los dígitos 294; *you* con 1184 (*your* con 1593); la conjunción *and* con 890; *the* con 224, y *to* con 426. Los nombres propios y los títulos terminaron codificados al estilo de un nomenclator clásico (*President* tenía el equivalente individual 68, *England* el 263, *Federal Government* la serie 755.190.1149, y *Franklin* la serie 601.1124.646). Los números se sustituían con partidas de hasta cuatro dígitos (1=1286; 3=1393; 7=1489; 9=1351).

³⁹ BAUER, *Decrypted Secrets*, p. 71.

⁴⁰ BURNETT, “Ciphers”, p. 330.

⁴¹ BURNETT, “Ciphers”, p. 332.

⁴² BURNETT, “Ciphers”, pp. 332-333. BAUER, *Decrypted Secrets*, pp. 60-70.

Veamos como ilustración de su funcionamiento el siguiente fragmento de una misiva firmada por Jefferson el 28 de enero de 1792 en Filadelfia:

294.496.994.153.264.534.1479.168.306.1298.1165.712.218.1460.
1564.467.1340.224.318.1460.751.1559.755.230.307.

Al decodificarlo se aclara la cadena sintagmática “I have unalterable fixed for retiring from my office at the close of our first federal cycle”.⁴³

Ahora bien, considerando su sistema concreto de formación —en especial la figura y la extensión de los equivalentes y la falta de códigos unitarios para sustituir los nombres propios—, la estructura del código que usó Pablo Obregón en 1825 es apenas confundible con la del nomenclátor canónico y la de los códigos numéricos de dos partes. Con miras a clasificarlo con precisión es fácil reconocerlo, ante todo, por las siguientes cualidades específicas:

⁴³ JEFFERSON, “Letters”, p. 112. Todavía en 1790 seguían usando el mismo diccionario, como lo prueba una carta de Jefferson desde Nueva York del 6 de abril de ese año, véase JEFFERSON, “Letters”, pp. 294-296. Sobre la labor diplomática de Short en relación con Jefferson véase BOYCE, “The Diplomatic Career”. Al promediar el siglo XVIII, políticos y diplomáticos españoles apelaron intensamente a sistemas codificadores numéricos organizados de forma muy similar al libro de códigos que usaron Jefferson y Short, distinguiéndose sin embargo por cuanto los grupos numéricos normalmente se indizaban de menor a mayor comenzando por 0, explicándose así el predominio de los conjuntos que se inician por 0 y 1 en los de cuatro números, aumentando progresivamente en los de tres, dos y uno. Véase LORENZO CADARSO, “Los documentos cifrados”, pp. 364 y 371.

a) Lo constituye una función de correspondencias de uno a uno; es, pues, “de una parte” y está organizado según el modelo del diccionario de la lengua.

b) Los elementos del texto plano reproducen los ordenamientos lexicográfico y matemático normales (de manera prácticamente idéntica a la del *Signalbuch* hallado en el crucero Magdeburg en 1914).

c) La transformación se realiza por sustituciones numéricas.

d) Los códigos agrupan un mínimo de dos dígitos y un máximo de tres.

e) Los elementos que se toman como unidades del texto plano son monogramas y bigramas.

Sin embargo de los condicionamientos técnicos recién apuntados, una característica francamente admirable del código de Obregón es que sus entradas no superan las dos centenas. Un poco de paciencia, de imaginación distributiva —valga esta expresión— y una caligrafía o tipografía de tamaño apropiado (esto es, disminuida sin sobrepasar el grado de lo legible) bastarían para hacerlo caber en dos planas o cuartillas, manuscritas o impresas. Mas esta suposición es irrelevante, lo que viene al caso es explicar esa parvedad —hablando comparativamente— de elementos totales en el libro. Y la explicaré, al cabo del siguiente apartado; puedo adelantar que es elegante, sutil, una táctica magistral cuyo diseño, sin duda, respondió al deseo primordial de economizar en medios de expresión para agilizar la codificación y la decodificación —ya que para nada propende a cimentar un baluarte contra el análisis de frecuencias.

CÓMO RESTITUÍ EL LIBRO DE CÓDIGOS
UTILIZADO POR PABLO OBREGÓN EN 1825

Ignoro si el original de este libro existe todavía. De hacerlo —en México, tal vez, o en algún archivo estadounidense, donde lo habrían puesto junto con los demás papeles de nuestro ministro, recogidos cuando éste se quitó la vida en Filadelfia—, espero que no pase demasiado tiempo antes de recibir la noticia de su hallazgo. Por mi parte, lo confieso, nunca procuré localizarlo. De hecho, preferí darlo por absolutamente perdido y, en consecuencia, verme obligado a restituirlo, cuando tempranamente durante mi investigación advertí que un análisis inmanente de los documentos decodificados en el ya citado legajo L-E-1333 del AHSREM bien podía bastar para exhumar todos los componentes del sistema codificador (esto es, tanto los códigos como sus equivalentes en texto plano) en su virtual totalidad —así por fuerza, dado que la reproducción de un original sólo puede ser aproximada— y, en consecuencia, devolver la claridad a los reservados 3 y 14 de 1825.

Me explicaré con detenimiento. En este caso, el análisis inmanente procedió bajo el gobierno fundamental de un razonamiento analógico promovido por una observación realmente de sentido común, a saber, que los documentos ya “traducidos” en el legajo contienen —como no podía ser de otra manera, desde un punto de vista criptológico— un monto preciso de grupos de códigos con sus equivalencias correspondientes; mi lector puede repetir esta observación en las figuras 3 y 4.

Ahora bien, la mayoría de tales grupos de códigos aparecen sin la menor modificación en el par de manuscritos que por

Figura 3

PÁGINA DEL RESERVADO NÚMERO 4
(30 DE MARZO DE 1825), DONDE SE APRECIA EL TRABAJO
ORIGINAL DE DECODIFICACIÓN

Handwritten musical score for a single page of music. The score consists of two systems of music, each with two staves. The notation includes various note heads (solid black, hollow black, solid white, hollow white), stems, beams, and rests. The first system starts with a treble clef, a common time signature, and a key signature of one sharp. The second system starts with a bass clef, a common time signature, and a key signature of one sharp. The vocal parts are labeled 'Voc' and 'Voc' above the staves. The piano part is labeled 'Pno' below the staves. The score is written in ink on a light-colored background.

Washington March 1^o 1825

Pablo Oregón

Figura 4

EL RESERVADO NÚMERO 8 (8 DE JULIO DE 1825)
CON LA DECODIFICACIÓN ORIGINAL ENTRE LÍNEAS

FUENTE: AHDSREM, leg. encuadrado L-E-1333, "Independencia de Cuba", f. 69.

algún motivo se dejaron sin “traducir”; el significado criptológico de esta analogía formal es evidente, indica más de lo requerido para estimar como muy probable a la hipótesis de que, en los ejemplares analizados de manera comparativa, unos mismos códigos representan invariablemente a unos mismos elementos de texto plano; de acuerdo con esto, el razonamiento hacia la “hipótesis restitutiva” —valga esgrimir una expresión semejante— debe proceder como sigue: si el conjunto 16 representa a la vocal E en los documentos decodificados del legajo, esa misma relación continuará observándose en los dos manuscritos aún codificados. Como paso inicial rumbo a la confirmación de esta hipótesis anoté en dos columnas paralelas todos los códigos con sus respectivas equivalencias que me daban a conocer los materiales decodificados. A continuación asigné las equivalencias conocidas a los correspondientes códigos en los reservados 3 y 14 de Obregón, comprobando en seguida que el 16, efectivamente, representa a la “E”, el 118 a la “P”, el 43⁴⁴ al bigrama “ci”, el vínculo 619⁴⁵ 19, de repetición muy elevada, a “que”, y así con otros grupos, hasta aclarar palabras y frases. La hipótesis inicial, por tanto, se confirmaba en gran medida, y lo mejor era que este solo esfuerzo naturalmente me redituaba un beneficio doble, pues al tiempo de decodificar los mensajes recuperaban también la estructura del libro de códigos en un porcentaje importante. Además, la especie de los resultados obtenidos hacía evidente que Obregón había utilizado un código “de una parte” ordenado lexicográfica y matemáticamente, siendo la regla que cada grupo de dígitos

⁴⁴ Subrayado así en los originales. Más adelante explico el motivo técnico.

⁴⁵ Lo mismo que en la nota anterior.

y su correspondiente multigrama claro están ordenados en ascenso: cada multigrama finaliza en alguna vocal o consonante del alfabeto latino, y mientras más alto es el número terminal de cada serie de dígitos, el multigrama correspondiente termina invariablemente con una vocal o consonante situadas hacia abajo en la secuencia alfabética normal.⁴⁶

Esta información sobre la clase de código a la que pertenece el de Obregón, y cuya valoración analítica especial debí, en una medida enorme, a mis conocimientos de la historia criptológica general, me permitió acelerar la faena decodificadora, pues al establecer un criterio criptológico seguro para interpretar el valor de los dígitos agrupados, podía ya fácilmente deducir la sílaba o el multigrama siguiente a uno previamente conocido —en virtud de la identificación por el razonamiento analógico descrito— sin temor a incurrir en fallas lógicamente impredecibles. Hablando de fallas, una cantidad de ellas que mi procedimiento, desde luego, no era capaz de predecir aunque sí, dada su justificación teórica, logró detectar y explicar, fue acumulada por Obregón —o un amanuense o secretario suyo, aunque a mis fines para nada interesa saber con exactitud quién inscribía los códigos en el papel—⁴⁷ mientras componía los despachos 3 y 14; en

⁴⁶ También interesa notar que Obregón no sometió su código a lo que se llama un “sobrecifrado”; el suyo no fue, por tanto, un código cifrado o encriptado, sino un código plano, véase KAHN, *The Codebreakers*, p. xv.

⁴⁷ Con todo, me parece oportuno indicar que no deberá sorprendernos el eventual descubrimiento de que era un secretario quien tenía el encargo especial de codificar los mensajes de Obregón. Tenemos entendido que partió a su misión acompañado de varios jóvenes destinados a entrenarse para el servicio diplomático. (Véase FLORES, “Apuntes para una historia”, p. 51); acaso uno de ellos fungió como ese posible secretario de codificación (o de “cifrado”, para expresarlo con el vocablo

efecto, cuando la deducción hacía predecible (por necesidad lógica) la subsecuente aparición de una sílaba determinada y la verificación fallaba, lo justo era explicar el hecho como el resultado de una confusión, omisión inconsciente o distracción al codificar.⁴⁸ No es excepcional que suceda esto, sobre todo cuando la comunicación secreta resultante es tan exageradamente larga como el despacho número 3 reservado (31 fojas); ciertamente, el solo plan de codificar una tan enorme cantidad de texto es un error criptológico de primer orden, pues la seguridad del sistema se torna vulnerable por obvias razones ligadas a la definición y el propósito del análisis de frecuencias.

Quien pondere con calma la exposición técnica precedente acordará conmigo, espero, en que acerté al seleccionar un método razonable, apto sin lugar a dudas para dilucidar positivamente los enigmas en la evidencia tratada, por tanto, restituir el sistema codificador y decodificar los reservados 3 y 14. Así, no puedo imaginar ninguna objeción científicamente calificada que pudiera oponerse a mi gesto de añadir de manera automática al libro de códigos las equivalencias

más usual en aquella época). Valdría la pena considerar esta posibilidad en una investigación comparativa con los protocolos usuales en cancillerías y servicios diplomáticos o consulares de otros países. En España, por ejemplo, hay pruebas de que hubo subalternos especializados en penetrar mensajes abstrusos desde la época de Felipe II hasta la de Fernando VI, por lo menos, véase CARLOS MORALES, “El poder de los secretarios reales: Francisco de Eraso”, en MARTÍNEZ MILLÁN (dir.), *La corte de Felipe II*, pp. 107-148, y LORENZO CADARSO, “Los documentos cifrados”, p. 367.

⁴⁸ Para un análisis particular de las causas más normales de cometer errores al cifrar o codificar un documento véase LORENZO CADARSO, “Los documentos cifrados”, p. 372.

deducidas. Por lo demás, debe admitirse que este ejercicio, en buena medida y conforme a las clases específicas de información extraída de las evidencias, halló su límite criptológico en disponer a los elementos “traducidos” que en primer lugar ubiqué en los documentos decodificados para su ordenamiento sistemático. Pero es innegable que el concurso operativo de esa misma limitación fue positivo, guiándome a la postre para decodificar los reservados 3 y 14.

Considerando, en fin, las circunstancias particulares de su realización, el proceso total de esta operación analítica es equiparable más a la decodificación que a la decriptación, pues si bien de inicio se careció del libro de códigos original, bastó un poco de ingenio para generar de manera oportuna un duplicado —prácticamente exacto— del mismo; y con esto a la mano la “traducción” automática fluyó, por así decir, como de oficio.

Muchas personas tienen el hábito de imaginar que para “romper” un ejemplar criptográfico se necesita poseer, o bien una potencia intelectual sublime, o bien las inefables dotes del adivino. Lo más común es que identifiquen al criptoanálisis con un acto de magia. En realidad, sin embargo, nada tiene de portentoso. La concepción y el tratamiento de sus objetos implican y recomienda explícitamente la formulación matemática. Se trata de asignar los valores adecuados a todas las incógnitas en cada miembro de una ecuación. La meta final es probar, mediando un análisis formal basado de manera primordial en el razonamiento deductivo, que el funcionamiento de un algoritmo necesariamente produce un criptograma de cierta clase. En virtud de esta comprobación se vuelve lógico prever que una reversión de la misma operación funcional aclarará los caracteres ocultados por el

método analizado de manera formal.⁴⁹ Existen, por cierto, varios estándares o patrones de inspección matemática, establecidos por criptólogos profesionales, que aceleran la recuperación de claves, reglas de transformación, o porciones estructurales de muchos criptosistemas o códigos (la velocidad aumenta, por supuesto, si uno aplica el patrón elegido con el auxilio de una computadora).⁵⁰ Sin embargo, la práctica del razonamiento estrictamente matemático no es una condición indispensable para el éxito criptoanalítico. En ocasiones, pero en especial cuando el investigador está familiarizado con la historia general de la criptología, basta observar a fondo toda la evidencia disponible —tanto de índole histórica como técnica— relativa al ejemplar criptológico que se tenga entre manos —lo cual implica un análisis comparativo—, razonar al modo impuesto por la naturaleza de sus contenidos, y, si es pertinente, adaptar para el uso

⁴⁹ La obra del matemático y criptógrafo francés François Viète (1540-1603) reveló de manera crucial los paralelos entre el criptoanálisis y el álgebra. Introductor a la matemática de la notación simbólica para incógnitas y coeficientes, Viète propuso un sistema de cálculo simbólico donde la cifra era remplazada por el símbolo algebraico (la incógnita) y el texto plano por el valor implícito del símbolo. Convencido de que los antiguos habían ocultado deliberadamente un arte analítico en sus matemáticas sintéticas (calidad exhibida en las pruebas teoremativas de los geómetras), sirviéndose de un código para escribir sus proposiciones, decidió exhumar dicho arte y, para ello, concibió la noción de signo o especie; ahora, el signo es una cifra en esencia, su función es dotar del carácter general de número (la especie) a números particulares que satisfacen estipulaciones dadas; por tanto, si una ecuación algebraica es como un texto cifrado, la solución algebraica es análoga a la resolución de una cifra. Véase PESIC, “Secrets”, pp. 683-684.

⁵⁰ PESIC, “Secrets”, p. 678 y n. 11. GUILLEN, “Automated Cryptography”, pp. 188-189.

propio los métodos desarrollados por investigadores de otras ciencias. Al tomar su curso el proceso inquisitivo, y en especial tratándose de una cifra o código cuyas reglas de formación desconocemos, la observación —hablo de una observación de la lógica en el razonamiento y no de esa vagamente entendida “observación indirecta” que los profesores de universidad, influidos por ciertos escritores populares (en especial franceses) del siglo xx, suelen admitir como la observación “propiamente” histórica— cumple su parte permitiendo el reconocimiento del fenómeno como un suceso común, para nada sorpresivo en la perspectiva del saber histórico general (no sólo de la criptología) dado que contamos con innumerables indicios del recurso a la criptografía en todas las épocas, y la caracterización de la evidencia por sus aspectos cuantitativos, anticipando con ello la obtención final de conclusiones deductivas, o sea, necesarias.

De acuerdo con lo que anuncié al terminar el apartado previo, me resta exponer las propiedades técnicas en cuya virtud dicho libro es comparativamente corto. Como se aprecia en las figuras 1, 2, 3 y 4, unos mismos grupos de códigos aparecen a veces subrayados, a veces coronados por una raya. Sean, por ejemplo, los grupos 319 y 922; en este caso, el primero equivale al bigrama ne y el segundo, al bigrama to; en cambio, cuando es el caso que 319 y 922, el primer conjunto equivale a en y el segundo a ot. De tal modo se manifiesta cuál fue la estrategia: indicar la permutación de la vocal y la consonante en un mismo bigrama por la posición de la raya. Esta convención, según lo declaré líneas antes, acusa en el individuo responsable de crearla (sería interesante, por supuesto, averiguar de quién se trató) un ingenio dispuesto a no sacrificar la elegancia gráfica para garantizar, dotando

de una doble función transformadora a casi todos los dígitos agrupados (transformación de pares de letras claras en uno de dos posibles sentidos, por así decir, hacia la vocal o hacia la consonante, de acuerdo con una señal inequívoca), un beneficio práctico de indudable atractivo para todos los usuarios eventualmente implicados: agilizar tanto la codificación como la decodificación autorizadas.

He dicho, sin embargo, que casi todos los dígitos agrupados tienen una doble función transformadora; carecen de ella los sustitutos de los caracteres claros sencillos, o sea, cada una de las letras del alfabeto (como se puede apreciar de inmediato sólo en las figuras 3 y 4, por supuesto).

Es el momento de mostrar el libro de códigos virtualmente restituido (figura 5). He puesto en cursivas los caracteres o grupos de caracteres cuyos equivalentes obtuve por deducción, provisto que no aparecen inscritos en ninguno de los documentos (decodificados o no) del legajo L-E-1333 del AHDSREM. El lector deberá reparar sin sobresalto en varias duplicaciones, caso del 212 y el 252 que representan al bigrama “la”, pues la mejor forma de explicarlas es como una estratagema tendiente a dificultar el análisis de frecuencias.⁵¹ Pero necesito efectuar una última breve advertencia sobre otro aspecto que el lector también, sin duda, apreciará fácilmente: en muchas listas de los números-código sobreviene un, por así decir, salto inesperado en la secuencia natural ascendente de las decenas; apuntaré dos ejemplos: en los bigramas que empiezan con b al 42 sigue el 92 en lugar del 52

⁵¹ Un análisis muy interesante de duplicaciones en una esquela oficial española de 1750 se puede ver en LORENZO CADARSO, “Los documentos cifrados”, p. 371.

Figura 5

EL LIBRO DE CÓDIGOS DE PABLO OBREGÓN

—como sería de esperar—, y en los que empiezan con f al 46 sigue el 96 y no el 56. En la actualidad no estoy del todo preparado para explicar este fenómeno, aunque poseo evidencias cuyo análisis preliminar me ha sugerido el siguiente bosquejo de hipótesis: el libro de códigos utilizado por Obregón era o bien una versión modificada, en ciertos rasgos medulares, de un original que habría utilizado su predecesor inmediato en el cargo, José Anastasio Torrens, o bien sucedió a la inversa y fue Torrens quien aprovechó un sistema codificador formado a partir del libro de Obregón cuando lo destinaron a Colombia —donde permaneció de 1825-1829— para cumplir encargos diplomáticos. Refinaré mi hipótesis, la criticaré y probaré sucesivamente hasta configurar la que con el más alto grado de probabilidad explique este hecho, tanto desde la perspectiva lógica como desde la historiográfica. Después la comunicaré al público por un medio adecuado.⁵²

LOS NÚMEROS 3 Y 14 RESERVADOS DE 1825, DECODIFICADOS

Advertencia preliminar: con el propósito de facilitar la lectura, insribí estas decodificaciones atendiendo a las normas que siguen:

a) Dejé inalterada la ortografía original; no podía ser de otro modo, puesto que una decodificación efectiva consiste en restituir el texto plano a la letra; sólo me permití añadir las tildes a la vocales que lo requerían (esto se comprende

⁵² He vertido ya, sin embargo, algunas conjjeturas acerca del origen y la estructuración del código que usó Torrens, más una decodificación precaria de un manuscrito presuntamente suyo, en mi artículo “Dos criptosistemas”.

por la razón criptológica de que las tildes, como tales, no se pueden codificar o cifrar, por tanto, en casos como el actual es conveniente —aunque no estrictamente necesario— que el decodificador las agregue).

b) Suplí todos los signos de puntuación, en consecuencia, pude fijar los lugares en que cada párrafo debe separarse del anterior.⁵³ Era el modo natural de resolver dos dificultades creadas por los métodos criptográficos más comunes: 1) los puntos y otros signos análogos no suelen cifrarse o codificarse,⁵⁴ y 2) el criptógrafo, en su afán por dotar a su mensaje de una seguridad máxima, normalmente no mantiene los espacios entre las palabras del texto plano que transforma en cifras o códigos (es justo lo que hizo nuestro ministro, como se delata en las figuras 1, 2, 3 y 4).

c) Corregí sin más todos los errores cometidos al codificar. La mayoría de tales errores se debió a que Obregón trazó la raya encima del código cuando debía ir debajo y viceversa.

d) Todas las frases, bigramas y letras que restituí por conjectura aparecen entre corchetes.

e) Las partes ilegibles en el manuscrito están indicadas por tres puntos entre corchetes.

⁵³ Acaso más de un lector juzgará que mis criterios no fueron siempre adecuados.

⁵⁴ En tanto que el método utilizado lo permita, sin embargo, lo más conveniente es codificar o cifrar absolutamente todos los caracteres del mensaje, incluyendo puntos, comas, blancos entre las palabras y hasta la firma del remitente o sujeto finalmente responsable del contenido de la emisión. Véase GALENDE, “Principios básicos”, p. 55. (Hasta el momento, por cierto, no he visto un solo documento codificado de Obregón que no vaya claramente signado al calce por éste; quizá esta evidencia podría entenderse como índice favorable al hecho de que fuera él y no un subalterno quien codificaba sus despachos.)

1. Despacho número 3 reservado

[Desde mi arribo a este país he dedicado la mayor atención a conocer la opinión que se había formado del estado político de la república; que auc[s] ilios se le prestarían en caso de una imbasión o intervención]⁵⁵ estrangera en su guerra de independencia; si coperarían o han coperado de algún modo estos estados para el reconocimiento de la misma por las potencias europeas; cómo pensaban sobre las fronteras limítrofes de ellos y los de Mégico; cuál es su opinión en cuanto a la suerte futura de la ysla de Cuba, y cuál la consideración de Mégico respecto de las otras naciones del continente americano y con relación a Europa, puntos todos de la mayor importancia a la república y sobre algunos de los cuales se me hizo encargo particular de observar y conocer. Para su consecución, he atendido a las operaciones del gobierno, opinión pública manifestada por los medios comunes y rectificada o comprobada por el conocimiento del mayor número de personas del país que tienen más relaciones e influjo en sus negocios, y que he podido tratar los frecuentes transtornos políticos y conbulciones ocurridas después de conseguida la independencia; las pocas relaciones comerciales, el espíritu de monopolio de los que les dirigían y el no ser casi conosida la rebelión si no desde la reacción del plan de Yguala, había hecho forjar una idea poco ventajosa de la opinión pública y situación de la nación —como comunicó el coronel Torrens en sus números veinticinco y veintiséis—, pero la adopción del sistema republicano y forma federal que se manifestó

⁵⁵ Hasta aquí decodificado —entre líneas— en el manuscrito original.
Queda por investigar las razones de la interrupción.

desear, que alaga y satisface a este país con la idea de ser el modelo de las nuevas sociedades de América y, al mismo tiempo, por la destrucción que a causado del monárquico, visto con zelo y de sab [...] redo a una la gran distancia del Brasil; el restablecimiento general del orden en las provincias; el conocimiento de que algunas agitaciones no han tenido otro fundamento que la desconfianza de los españoles residentes en el país, y de las que aunque no se aprueban los medios y modos que se han querido tomar para precaverse de los males temidos, sí se consideran éstos como causa bastante para tales sucesos vistos por lo mismo como necesarios en el estado presente de cosas.

Las rápidas fortunas o ventajoso comercio que han hecho los primeros especuladores y la verdadera mejora del país han aumentado (*sic*) los concurrentes y destruido casi del todo la barrera que oponían aquellos con sus ecsa[ge]radas noticias para conservar el monopolio, siendo todo esto la base del [to]tal cambio de la opinión, causado, sin embargo, generalmente con la ejecución del señor Yturbide y con la promulgación y práctica de la constitución que se ha dado la república. Los Estados Unidos, de acuerdo con la Ynglaterra, o a lo menos en tal concepto su gobierno se había desidido desde el reconocimiento de la independencia a no permitir en dicho asunto la intervención de otra potencia que la España misma, empleando en último caso todo el poder y fuerza de la nación, resolución que manifestó públicamente el presidente en su mensage del año de mil ochocientos veintitrés y que reiteró o tocó en el mismo sentido este punto en el de mil ochocientos veinticuatro. Tal resolución está apoyada en la opinión general de toda la unión y con cuyo auxilio en el referido caso se puede contar; los Estados Unidos de América se in-

teresarán en la cuestión de independencia desde que la guerra se manifestó de un modo capaz a conoscer el espíritu que la animaba, haciendo saber el gobierno por medio de sus agentes en Ynglaterra y Francia que a su política no podía ser indiferente la lucha de [las] colonias españolas con la metrópoli, como igualmente el que se mesclaré en este negocio ninguna otra potencia a las mismas.

Dos naciones solicitaron de los Estados Unidos mandase un ministro al congreso de Aix-la-Chapelle para tratar de los asuntos de América, a lo que se negó el gobierno contestando que no se mesclaría en ellos del modo como se le proponía y que únicamente mandaría un ministro cuando se dispusiesen las potencias europeas a tratar del reconocimiento de la independencia, a lo que se dijo por la Francia e Ynglaterra en aquella fecha que no estaban dispuestas a hacerlo, pero que habían deseado saber su opinión en el particular por juzgarlo interesante, desde el momento en que se supo la formación de gobiernos en las nuevas sociedades de América y que presentaban ya estabilidad o fuerza. En cuanto a la independencia, la reconocieron participándolo a la Ynglaterra, de que en se habían creído haría lo mismo y la que por una política obscura o poco franca no correspondió a lo esperado. Después de esta época encargó el gobierno a todos sus agentes en Europa promoviesen el reconocimiento, encontrando poca disposición en Francia, alguna en Rucia y la Ynglaterra, embarcada [*sic*] únicamente por la forma de gobierno; la opinión de que los límites entre las dos repúblicas sean los demarcados en el último tratado echo con la [Es]paña el año de mil ochocientos diez y nueve es general en ésta, y aún el gobierno me ha manifestado tácita o indirectamente en su respuesta a la cámara de representantes sobre la

materia, que he comunicado en mi número treinta y ciete, la que se funda en el conocimiento que tienen de las grandes ventajas sacadas por ella de aquel tratado, y la que indicó igualmente el secretario de estado en la referida contestación con las palabras de que parecía estar Mégico conforme con la demarcación señalada por él, pero sin embargo de lo cual este pueblo se halla poseído de un espíritu de engrandecimiento por la adquisición de puntos de que tiene ideas muy favorables. La antigua provincia de Tejas es uno de los comprendidos en este caso, y que cre le perteneserá con el tiempo, para lo cual por ahora no se empleará otro medio que proteger la emigración a ella de estos habitantes y aprosimar sus poblaciones. El Nuevo Mégico llama al presente su atención con motivo de las grandes ventajas que sacó la última caravana de comercio dirigida a este territorio, con el que esperan fomentar los estados del oeste —principalmente del Missouri— y el establecimiento proyectado en la desembocadura del río Columbia (en mi número treinta y tres he comunicado los pormenores de dicha expedición y de la protección solicitada en favor de este tráfico). Todos los periódicos de la Unión, con pretesto de las piraterías que en efecto se ejecutan por los españoles en la isla de Cuba, toleradas o no podidas evitar de [sus] autoridades, manifiestan claramente los deceos de esta nación por [la] adquisición. La proposición de hacer en [el] senado su resultado y término, ni la cámara de representantes —de que he dado cuenta en mis números treinta y cuatro, cincuenta y dos y cincuenta y seis— no indican otra cosa. Con este motivo he hablado (*sic*) yo en la cámara de proteger el espíritu de independencia como único término de los males que su estado presente causa al comercio de la Unión.

Se comienza a crer que Mégico, además de dever acabar la guerra con los españoles en aquella ysla, sus intereses venideros lo [oc]cupan de una expedición a ella y en la que puede presentar sus tropas bajo aquel aspecto, protegiendo al mismo tiempo la opinión de independencia, que ya se considera fuerte y aun generalizada. De Colombia se dise lo mismo en cuanto a expediciones, pero [in]duse más bien que ésta lo verifique causando ya estas dos naciones en el particular algún zelo a los Estados Unidos, los que si no fuera por la oposición que e[n]contrarán en Ynglaterra, Francia y otras potencias europeas si ocuparan la ysla o favoreciesen su separación contra pas (*sic*), único caso en que se espera la pronunsiacion general en ella, no darían tiempo, a mi entender, a que obrasen las dichas dos potencias, pues que conosen deve seguir la suerte del continente y que al presente necesita de protección.

Dos son los aspectos bajo [los] que se concidera a Mégico: uno con relación a todo el continente y el otro con sólo a las nuevas sociedades; en el primero se le jusga la segunda potencia de América que la rivaliza y se aprocsima a la importancia de estos Estados; en el segundo se da a los megicanos un carácter más dulce, menos inclinado a la guerra que los colombianos, por lo cual se espera que ésta y esa república se dirigirán juntamente por unos mismos principios a su auemento y prosperidad. La población con que cuenta Mégico desde su independencia, su situación, climas y producciones —entre las cuales la gran cantidad de plata que se estraе de sus minas deslumbra a unas persunas (*sic*) que no son bulgares—, haciendo formar una idea muy ventajosa de la riqueza actual y de la que puede tener con el tiempo; el no ser casi conocida la rebolución de independencia [si]no

desde la reacción de Yguala, y en no suceder lo mismo en Colombia (tal vez por su situación física, que proporciona más acceso a los extranjeros y por la brillante conducta del general Bolívar), son las causas de dicha opinión. Las otras sociedades americanas son menos conocidas, y del Perú no se tienen las menores ideas en cuanto a su general opinión de independencia, el juicio formado de la república y el de el grande interés de la Europa en estender su comercio a las nuevas sociedades del otro continente le dan una importancia muy ventajosa en cuanto a la facilidad o medios que tiene para hacerse reconocer, ya sea obrando por sí o de acuerdo con las otras. La admisión o no a su comercio es el agente que se considera podría emplearse para dicho fin; este [ya] es juicio, pues, que he formado de [lo]s diferentes objetos que como interesantes me he propuesto presentar a V. E., y de los que manifestaré enseguida los datos que [he] tenido para que, impuesto de ellos, pueda V. E. considerar hasta que punto de[va] apreciárseles las causas de la mala opinión que tenía la república y el cambio actual; siendo hechos conocidos y sus principios bastantes, no hay necesidad de atender a otra cosa para percibir la variación efectuada que a todos los periódicos en donde se anuncia constantemente el buen aspecto que presenta hoy Mégico, a pesar de lo secreto con motivo de la cuestión de ciudad federal y cumplimiento de las leyes en el estado de Yucatán, pues que publicado aque[l] siempre se ha juzgado terminería (*sic*) todo felizmente y sería sugeto a la boluntad de la nación y al aumento de especuladores que de todos los estados me piden noticias para poder dirigir sus empresas con buen ecsito.

El no ser conocida la rebolución sino vagamente ha sido motivo para crerse que la opinión de independencia y

sistema republicano no heran generales, ni que éstas se formaran progresivamente en todo el tiempo de la guerra, que con la reacción de Yguala no se hizo otra cosa que conciliar los partidos para conseguir el fin sin los males anteriores, atribuyendo el felis pronto resultado de dicho plan a una ecsaltación repentina pero a la que no se le consedía el apoyo de la constancia ni la formación de su causa en el sufrimiento y desgracias de once años, por cuya razón he tratado de hacer conocer la revolución de la república cuanto he podido en sus acontecimientos más notables, dando todo (*sic*) la fuerza que le conosco al espíritu público sobre independencia y forma de gobierno establecida, y la relación de la conducta tenida por los Estados Unidos en la cuestión de independencia me ha sido comunicada por el ecspresidente Monroe antes de salir de este cargo y de que se supiera el reconocimiento de Ynglaterra. A dicho sugeto es deudora la república de distinciones particulares, pues habiendo yo manifestado un deseo de saber si en aquella época se interesava esta nación de algún modo en Europa por el reconocimiento de la independencia, dicho señor, en la primera ocación que después le ablé, me dijo lo fuese a visitar sin etiqueta y amistosamente, [que] me impondría de todo su manejo en cuanto a nuestros intereses porque creía necesario a la causa de América estubiera mi gobierno impuesto de la situación presente, conducta anterior y de lo que se devía esperar de la Europa. Me aseguró, además de lo que tengo referido, que aunque la Ynglaterra faltase a lo manifestado públicamente y en lo que estaban de acuerdo de no permitir la intervención de las potencias europeas en la guerra de independencia, los Estados Unidos siempre obrarían conforme a lo dicho por él en sus dos últimos mensages; que la Ynglaterra, luego

que conociera que la opinión en la forma de gobierno era tan sólida como la independencia, le reconocería; que creía seguiría la Rucia este ejemplo, pues el emperador había manifestado aprovar la conducta de los Estados Unidos y hera el que se había encontrado más inclinado por los agentes americanos para el reconocimiento; que la Francia siempre había aparentado desbío en el asunto, pero dado el paso por las otras dos no tardaría en imitarlas; que con respecto a la situación de la república y las relaciones de amistad con ésta, serían todos los días más estrechos, haciéndose [...] ri [...] con placer el cambio de sistema en la forma de gobierno a pesar de que respetaron el anterior, y, por último, con motibo de haberle impuesto de las precauciones tomadas por el gobierno para sostener la independencia, que él aprecia muy numeroso el ejército cuyo pago no permitiría progresar a la nación, jusgándolo además innecesario por la impotencia de la España; que con respecto a otros enemigos me asegurava y repetía lo anteriormente dicho de que los Estados Unidos emplearían sus fuerzas en unión de las de las otras potencias del continente para oponerse al enemigo común; en cuanto a límites he guardado la reserva o encargo de mis instrucciones para no tocas (*sic*) este punto sino hasta mejor ocación, pero, sin embargo, no he podido escusarme de tratar de él en combersaciones particulares, en las que generalmente he encontrado las ideas insinuadas. Se cre que el gobierno no be con mucho abandono a Tejas y Nuevo Mégico, que se encuentran como independientes de echo (según comuniqué en mi número treinta y tres) y que les agradaría la protección de estos Estados; la posibilidad y los medios de su reunión son tan difíciles como conose V. E. a todos los datos del modo de pensar de este gobierno en

el particular (*sic*) participación en mi número treinta y ciete; agregaré únicamente que el presidente Monroe, cuatro días antes de dejar de serlo, con motivo de tratar sobre la buena armonía de las dos repúblicas, me insinuó que no habiendo motivo de celos ni pretensiones sobre comercio y límites en ninguna de las dos, pronto nos arreglaríamos o fijaríamos definitivamente por medio de tratados; que él por delicadeza no había nombrado el ministro para Mégico, pero que su sucesor sería una de las primeras cosas que haría.

La opinión y miras de este pueblo sobre la isla de Cuba son públicas, manifestadas del modo que he participado en mis números treinta y cuatro y cincuenta y dos, y si su existencia o bienestar no dependiese de la paz tal vez más que otra nación alguna, seguramente no habría terminado este asunto como he impuesto a V. E.

La idea de la riqueza presente y futura de Mégico es general, la de el carácter suave y no inclinado a la guerra comparado con el de los colombianos, además de las causas ya indicadas, hay otra, y es la de considerarse a éstos como con pretensiones desde su nacimiento a influir en los negocios de las otras potencias; se dice que sus ministros en todas partes han demostrado tales deseos; se juzga o da el poder a las nuevas sociedades para hacerse reconocer de las naciones europeas en consideración al espíritu de independencia, orden y estabilidad que en la actualidad presentan y la (*sic*) gran interés de éstas en su comercio, pues que no creyendo posible la intervención de otra potencia que la España, nadie espera ya tenga suceso en sus pretensiones y de conciente (*sic*) está asegurada la existencia política, por lo que se cre sacará más ventajas de las relaciones comerciales respecto de otras. La nación que primero las establezca y conozca las

necesidades del país, y de cuyo fin alejaría a cualesquiera una [...], he manifestado a V. E. los datos que he tenido, en parte com (*sic*) seguras y en otras como el resultado de la observación, por [el] conocimiento del mayor número de personas interesadas o que entienden los negocios públicos reunidos en esta ciudad con motivo de la última legislatura y elección de presidente; antes de ahora habrálo di (*sic*) do (*sic*) informa ya a V. E. de varios de estos puntos con relación a lo que he sabido por el señor Monroe, pero la expectativa de una nueva administración de la que aunque confiara no se separaría de los principios y opiniones de este pueblo en cuanto a los intereses de la América, sin embargo, los candidatos que se presentarán a la presidencia, según la opinión general de sus cualidades, deberían interesar de diferente modo a la república, y cuyo resultado he esperado. La elección, estando ya echada, no trataré de los individuos que la compitieron sino en cuanto tenga relación con mi deseo de manifestar el aspecto que es de esperar tomarán los negocios públicos que interesan a Méjico. Se objetó a M. Adams para su elección de presidente el que hera amigo del sistema aristocrático, dañoso en sí para ese país y el continente todo; que no hera afecto a la independencia de las nuevas sociedades, pues que se opuso cuanto pudo a su reconocimiento, por lo que si se le ponía al frente de la unión en la época de que la Santa Alianza aún no abandona la pretención de intervenir en los negocios de América, se aventurará mucho ésta o a lo menos no hera la persona a propósito para las circunstancias, las que exigían un hombre firme, resuelto, que no contemporizase con los europeos y cuyas cualidades se presentaran unidas en el general Jackson, que gosa de gran popularidad por su conducta militar y política tenida en la Nueva Orleans en

la última guerra con los yngleses, y aun M. Crauvford, el tercero de los candidatos que entraron en la elección de la cámara que en (*sic*) por sus enfermedades no tubo más partido, hera presentado sin embargo con mejor aspecto que M. Adams para la causa de América, pero la mayoría de personas que dirigían y devían resolber este negocio, entre las que tenía gran influjo M. Clay —o fue el que lo decidió uniéndose con todo su partido al de M. Adams—, no tenían en él un hombre que pudiese causar recelos a la nación en quanto (*sic*) a sus instituciones ni que desconociese los intereses de la causa de América, sino que su carácter personal, serio o adusto; la upinión (*sic*) formada de su padre —que hera ya una prevención en su contra— con la resistencia u uposición (*sic*) que manifestó al reconocimiento de la independencia, lo hacían ser presentado desventajosamente a la nación.

El desear concluir el último tratado de límites con España, o algunas pretensiones o reclamos pendientes que tenían con ella los Estados Unidos, fue la causa de la resistencia de M. Adams al reconocimiento de la independencia, aunque se le atribuye además un principio de neutralidad tal que no conviene a los intereses del continente, pero lo que más decidió en su favor la elección fue el espíritu que hay en el país contra un jefe militar para confiarle la pirimera (*sic*) magistratura, no conceder bastantes talentos políticos al referido general Jackson y el temer cimprometiese (*sic*) la nación y la enfermedad de M. Crauvford, únicas dos personas que en el cavo podían ya ser nombradas desde que se decidió la elección.

Se creyó que el nuebo presidente trataría por todos los medios posibles de dirigir su administración conforme a la opinión pública en los puntos que no se le considerava acorde, y lo que ha comeenzado (*sic*) a verificar con los nombramien-

tos de M. Clay para secretario de estado, sugeto que además de por sus talentos gosa de gran opinión como partidario y promobedor del reconocimiento de la independencia, de los intereses del continente y de la libertad en general a pesar de lo que se ha dicho de él con motibo a su conducta en la elección de presidente y de M. Barbour para secretario de la guerra, igualmente acreditado este indibiduo (es el que promobió en el senado con motibo de los piratas el bloqueo de la ysla de Cuba). Tales personas y otras semejantes, colocadas en los primeros puestos; la opinión general de la Unión y ningún motibo en contra de conveniencia, aseguran que el nuevo presidente seguirá en cuanto a la causa del continente de América la misma conducta que su antecesor, y que obrará cual manifestó aquél en caso de que se mescle en dicha cuestión otra potencia europea que no sea la España.

La paz es el principio fundamental de la ecsistencia de este pueblo, como dijo el presidente en su discurso de inauguración en el cuatro del corriente, y que he remitido a V. E. Todo él asegura lo referido anteriormente, además, semejante conducta de la que es de esperar no se separará M. Adams no le permitirá pretención alguna directa sobre la ysla de Cuba lo mismo que sobre límites de esa y esta república, lo que no hubiera sucedido así si el general Jackson estubiera en su puesto pues que sostubo con ardor en el senado el que se adoptasen las medidas propuestas y que se dirigían a la ocupación de dicha ysla, igualmente, que su modo de pensar sobre la provincia de Tejas —que ya es conocido de V. E.— y en la que el expresado general obraría con toda la fuerza que da la opinión.

Tal es el estado en que concidero los puntos que he indicado a V. E., y lo que aún no me atrevería a hacer por

temor de inducir en algún error si los acontecimientos que varían todos los días a favor de la república no me obligasen a manifestar al gobierno mi juicio en el particular, para que examinado en unión de los que ministren sus otros agentes pueda servir a la política y dirección de los intereses de la nación en los diferentes objetos que he tocado, cuya marcha no se puede suspender y en los que es preciso obrar según los conocimientos presentes.

Mis dos anteriores comunicaciones en cifra de veintiocho de diciembre y catorce de enero últimos, en que comunicué la salida de buques con víveres de Baltimore para el castillo de San Juan de Ulúa, no estando comprendidas en la numeración ordinaria de mi correspondencia, me ha parecido conveniente formar de ellas ésta, y de las que en lo subsecivo ocurrieren del mismo carácter, otra reservada y la que llevará su numeración particular, por cuyas razones señalo esta nota con el numero tres, y lo que me dirá V. E. si es de su aprobación. Vvashington, Marzo 23 de 1825.
[Rúbrica]

2. Despacho número 14 reservado

En mi número once reservado digue a V. E. que no se había transpirado aquí la resolución de la cámara de representantes sobre no acceder a la solicitud del señor presidente para sacar tropas del territorio de la república con el objeto de auxiliar a la independencia de la isla de Cuba, mas a la presente corre la noticia entre los habaneros emigrados y otras personas de su círculo de cuanto ha pasado en este negocio, refiriéndose a los que de este país fueron a esa ciudad. Este rumor en nada disminuirá el espíritu público de la isla, pero sí sería

combeniente no hacer confianza de personas tan indiscretas dan por segura la expedición como resolución sabida por la boca del mismo presidente.

He remitido a V. E. dos paquetes del papel que ha escrito el doctor Varela y de que ablé en mi citado numero once; no desempeñó bien ni del todo su promesa; después he conocido la causa, y es de que esta producción fue dirigida por sus ideas, las del ministro de Colombia y las mías, que sin embargo de estar absolutamente acordes, Colombia tiene zelos de la preponderancia de Mégico, y he llegado a crer que ha admitido desde muy temprano en su política el principio europeo del equilibrio de las naciones, lo que me induxe a esperar que habrá convenido, si se le ha hecho, en la invitacion del señor presidente para auxiliar a Cuba con fuerzas reunidas de ambas repúblicas, pues que es un medio de evitar o disminuir la opinión por la reunión a Mégico. Su ministro ha guardado conmigo la mayor reserva y a tratado de saber de mí el juicio o pretenciones del gobierno en caso de que se le haga independiente. En este país, antes de la elección del actual presidente, M. Clay y otros sujetos que ni fluyen en los asuntos políticos heran de opinión de favoreser la independencia de Cuba y de que quedase bajo la protección de las tres repúblicas de los Estados Unidos, Colombia y Mégico, pero M Adams los cambió a la suya —que he comunicado en mi número diez reservado—, conociendo que en semejante cuestión no podían tomar parte los Estados Unidos, que de ningún modo les sería más esclusivo y ventajoso su comercio que perteneciendo a España, y que lo más probable en caso de independencia hera que se reuniese a Mégico. No dudo que tal proyecto tubiese por objeto principal el prevenir o evitar dicha incorporación.

La negociación proyectada para el reconocimiento del continente manifiesta el móvil y deseos de este gobierno, y si no tiene el efecto de embarazar la expedición de Cuba creo se adoptará y emprenderá el plan de la protección de las tres repúblicas, en cuyo caso será apoyado por Colombia.

La opinión de reunión a Mégico es de consideración y el no pretenderla será lo que tal vez la haga verificar, pero será también necesario no dejar obrar en contra a las otras dos potencias, ecsigiendo quede a la libre boluntad de los habitantes de la ysla el decidir de su suerte.

Vvashington, Noviembre 1.o de 1825. [Rúbrica]

SIGLAS Y REFERENCIAS

AHDSREM Accervo Histórico Diplomático de la Secretaría de Relaciones Exteriores de México, México, D. F.

AA. VV.

México y Cuba. Dos pueblos unidos en la historia, México, Centro de Investigación Científica Jorge L. Tamayo, A. C., 1982, t. I.

ALAMÁN, Lucas

Historia de Méjico. Desde los primeros movimientos que prepararon su independencia en el año de 1808 hasta la época presente, México, Libros del Bachiller Sansón Carrasco, 1985-1986, ts. II y V.

BAUER, F. L.

Decrypted Secrets. Methods and Maxims of Cryptology, Berlín, Springer, 2002.

BOYCE, Myrna

“The Diplomatic Career of William Short”, en *The Journal of Modern History*, xv:2 (jun. 1943), pp. 97-119.

BURNETT, Edmund C.

“Ciphers of the Revolutionary Period”, en *The Hispanic American Historical Review*, 22:2 (ene. 1917), pp. 329-334.

CARLOS MORALES, Carlos Javier de

“El poder de los secretarios reales: Francisco de Eraso”, en MARTÍNEZ MILLÁN, 1994, pp. 107-148.

COHEN, Jonathan

“On the Project of a Universal Character”, en *Mind* (nueva serie), 63:249 (1954), pp. 49-63.

COROMINAS, Joan

Diccionario crítico etimológico de la lengua castellana, Madrid, Gredos, 1976 (3a. impresión de la 1a. edición 1955-1957), vol. III.

CHÁVEZ OROZCO, Luis

Un esfuerzo de México por la independencia de Cuba, México, Secretaría de Relaciones Exteriores, «Archivo Histórico Diplomático Mexicano, 32», 1930.

DELGADO, Jaime

España y México en el siglo XIX, vol. I, 1820-1830, prólogo de C. Pérez Bustamante, Madrid, Consejo Superior de Investigación Científica, Instituto Gonzalo Fernández de Oviedo, 1950.

DIFFIE, Whitfield y Martin E. HELLMAN

“New Directions in Cryptography”, en *IEEE Transactions on Information Theory*, IT-22:6 (1976), pp. 644-654.

FLORES D., Jorge

“Apuntes para una historia de la diplomacia mexicana. La obra prima, 1810-1824”, en *Estudios de Historia Moderna y Contemporánea de México*, 4 (1972), pp. 9-62.

GALENDE, Juan Carlos

“Principios básicos de la criptografía: el manuscrito 18657 de la Biblioteca Nacional”, en *Documenta & Instrumenta*, 4 (2006), pp. 47-51.

“Sistemas criptográficos empleados en Hispanoamérica”, en *Revista complutense de historia de América*, 26 (2000), pp. 57-71.

GUILLEN, Michael

“Automated Cryptography”, en *Science News*, 110:12 (1976), pp. 188-190.

JEFFERSON, Thomas

“Letters of Thomas Jefferson to William Short”, en *William and Mary College Quarterly Historical Magazine*, 2a. Series, 13:2 (abr. 1933), pp. 98-116.

“The Letters of Thomas Jefferson to William Short”, en *William and Mary College Quarterly Historical Magazine*, 2a. Series, 12:4 (oct. 1932), pp. 287-304.

KAHN, David

The Codebreakers. The Story of Secret Writing, Nueva York, Macmillan Publishing Co., Inc., 1967.

LORENZO CADARSO, Pedro Luis

“Los documentos cifrados en la Corte de Fernando VI (1746-1759)”, en *Espacio, Tiempo y Forma*, Serie iv, H.^a Moderna, 11 (1998), pp. 359-379.

LUCIANO, Dennis y Gordon PRICHETT

“Cryptology: From Caesar Ciphers to Public-key Cryptosystems”, en *The College Mathematics Journal*, 18:1 (1987), pp. 2-17.

MARTÍNEZ MILLÁN, José (dir.)

La corte de Felipe II, Madrid, Alianza Editorial, 1994.

MUÑOZ, Laura

En el interés de la nación. Mexicanos y estadounidenses en el Golfo-Caribe, 1821-1830, México, Instituto de Investigaciones Dr. José María Luis Mora, «Historia internacional», 2004.

NARVÁEZ, Roberto

“Historia y criptología: reflexiones a propósito de dos cartas cortesianas”, en *Estudios de historia novohispana*, 36 (ene.-jun. 2007), pp 17-62.

“Dos criptosistemas empleados por el coronel José Anastasio Torrens en Colombia (1825-1826). Una contribución a la historia de la criptología mexicana”, en *Memorias de la Academia Mexicana de la Historia*, XLIX (2007-2008), pp. 7-43.

NAVARRO GARCÍA, Luis

La independencia de Cuba, Madrid, Mapfre, «Independencia de Iberoamérica», 1992.

PESIC, Peter

“Secrets, Symbols, and Systems. Parallels between Cryptanalysis and Algebra, 1580-1700”, en *Isis*, 88 (1997), pp. 674-692.

ROJAS, Rafael

Cuba mexicana. Historia de una anexión imposible, México, Secretaría de Relaciones Exteriores, 2001.

Rossi, Paolo

Clavis universalis. El arte de la memoria y la lógica combinatoria de Lulio a Leibniz, México, Fondo de Cultura Económica, 1989.

SALADO ÁLVAREZ, Victoriano

Méjico en tierra yanqui, introducción y selección de Álvaro Maturé, México, Universidad Nacional Autónoma de México «BEU, 112», 1990.

SARUKKAI, Sundar

“Mathematics, Nature and Cryptography: Insights from Philosophy of Information”, en *Current Science*, 92:12 (2007), pp. 1690-1696.

SINGER, Thomas C.

“Hieroglyphs, Real Characters, and the Idea of Natural Language in English Seventeenth-Century Thought”, en *Journal of the History of Ideas*, 50:1 (1989), pp. 49-70.

SINKOV, Abraham

Elementary Cryptanalysis. A Mathematical Approach, Arizona, Arizona State University, The Mathematical Association of America, «22», 1966.

TORRENS, José Anastasio

Primera misión de México en los Estados Unidos de Norte América, 1823-1824 (segundo período), México, Secretaría de Relaciones Exteriores, 1912.

WELSH, Dominic

Codes and Cryptography, Oxford, Oxford University Press, 1989.