Estudios de Historia Moderna y Contemporánea de México
ISSN: 0185-2620
moderna@unam.mx
Universidad Nacional Autónoma de México
México

Narváez, Roberto
Una carta cifrada atribuible a José Mariano Michelena (1824)
Estudios de Historia Moderna y Contemporánea de México, núm. 41, enero-junio, 2011, pp. 119-133
Universidad Nacional Autónoma de México
Distrito Federal, México

ESTUDIOS DE HISTORIA MODERNA Y CONTEMPORÁNEA DE MÉXICO/ISSN 0185-2620, n. 41, enero-junio 2011

UNA CARTA CIFRADA ATRIBUIBLE A JOSÉ MARIANO MICHELENA (1824)

An encoded letter attributable to José Mariano Michelena (1824)

ROBERTO NARVÁEZ

Resumen: En este trabajo se ofrece una serie de análisis y comparaciones entre documentos de archivo y argumentos de índole criptológica e histórica para fortalecer, especialmente con ayuda del criptoanálisis técnico y el razonamiento por analogía, la conclusión probabilística de que José Mariano Michelena fue autor de una carta cifrada remitida desde Inglaterra en octubre de 1824, como lo sostuvieron acertadamente los preparadores del catálogo tradicionalmente conocido como *A calendar of the Juan E. Hernández y Dávalos manuscript collection* (1954).

Palabras clave: José Mariano Michelena, carta cifrada, criptología, criptografía, criptoanálisis, historia diplomática, México, Inglaterra.

Abstract: This article offers a series of analysis and comparisons between archive documents and cryptological and historical documents to strengthen, particularly with the help of technical cryptoanalysis and reasoning by analogy, the probable conclusion that José Mariano Michelena was the author of a coded letter sent from England in October of 1824, as correctly believed by the compilers of the catalogue traditionally known as *A calendar of the Juan E. Hernández y Dávalos manuscript collection* (1954).

Key words: José Mariano Michelena, coded letter, cryptology, cryptography, cryptoanalysis, diplomatic history, Mexico, England.

Entre la colección de manuscritos Hernández y Dávalos que se resguarda en la biblioteca de la Universidad de Texas (Austin), como parte de la Nettie Lee Benson Latin American Collection, se cuenta una serie de documentos fechados en los días 5 y 6 de octubre de 1824, todos los cuales fueron atribuidos al diplomático mexicano José Mariano Michelena, quien en marzo de aquel año había recibido el nombramiento oficial del Congreso como agente confidencial del

Roberto Narváez, mexicano, es maestro en Historia por la Facultad de Filosofía y Letras de la UNAM. Labora en el Instituto Cultural Helénico y en la Facultad de Arquitectura de la UNAM. Sus principales áreas de estudio son lógica de la investigación histórica, historia de la criptología general y mexicana, e historia de las ciencias. Entre sus publicaciones recientes destacan: "El 'Diario reservado no. 18' de José Anastasio Torrens (1829)", *Estudios de Historia Moderna y Contemporánea de México*, 38, julio-diciembre 2009; "Los despachos codificados de Pablo Obregón desde Washington en 1825. Análisis y dos decodificaciones", *Historia Mexicana*, v. LVIII, n. 3 (231), enero-marzo 2009, y "La criptografía diplomática mexicana en la primera mitad del siglo XIX. Tres ejemplos", *Documenta & Instrumenta*, n. 6, 2008. Su correo electrónico es: gogmagog501@yahoo.com.mx.

Estudios de Historia Moderna y Contemporánea de México, n. 41, enero-junio 2011, p. 119-133.

gobierno mexicano en Inglaterra. En el catálogo de dicha colección, tradicionalmente conocido por su subtítulo *A calendar of the Juan E. Hernández y Dávalos manuscript collection*, se define que se trata de cinco cartas distribuidas en los fólders 2280 a 2284, relacionadas con negocios de cuyo seguimiento y resolución debía ocuparse Michelena mientras perseguía su objetivo fundamental: conseguir el reconocimiento británico a la independencia mexicana. Ahora bien, la descripción del ítem HD 17-5.4132, fólder 2284, que está completamente cifrado, incluye una indicación gráfica reveladora de que los catalogadores no pudieron o no supieron eliminar del todo una duda respecto a la justeza de atribuirlo al mismo individuo:

> [_____?] [Carta remitida en cifra al ministro de Relaciones sobre el estado de negocios con Francia, Inglaterra, y España.] Copy. October 6, 1824. 1 l. 21 × 31 cm.
>
> Reference to: Arrival of Samuel; reports of small; increase in French Navy; troops embarked at Ferrol; funds expected via the Tigre for work in Spain; favorable attitude of Holland.[1]

La indicación gráfica en cuestión es, por supuesto, el signo de interrogación al final de la pleca. La falta de una firma en el manuscrito lo justifica, y su función es, lógicamente, advertir que por semejante cualidad material sería precipitado responsabilizar de su creación a cualquier persona sin ulteriores investigaciones.

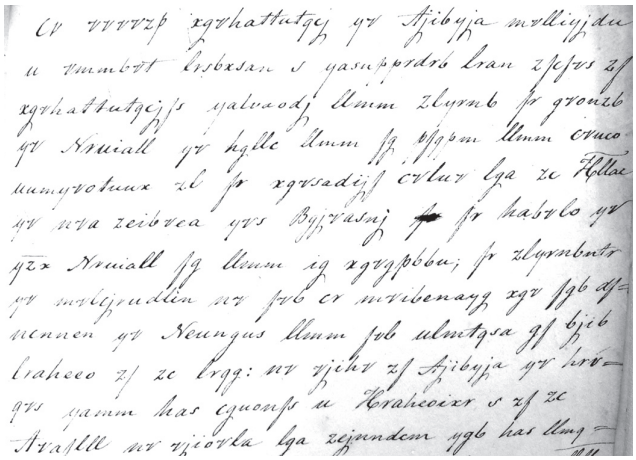
Los preparadores de *A calendar*, de acuerdo con las directrices de su particular metodología,[2] infirieron a partir de "evidencia interna" que Michelena puede ser nombrado, provisionalmente, como su autor. Es claro que por "evidencia interna" se refieren a piezas de información críticamente seleccionadas de entre los enunciados en el texto. Pero ¿cómo pudieron discernir los datos interesantes cuando el documento es un criptograma, siendo por tanto imposible su lectura automática sin descifrarlo previamente? (véase la figura 1). De algún modo, sin duda, tuvieron acceso a lo que en criptología se denomina el texto plano, es decir, inmediatamente

[1] *Independent Mexico in documents: Independence, Empire, and Republic. A calendar of the Juan E. Hernández y Dávalos manuscript collection. The University of Texas Library*, preparado por Carlos Eduardo Castañeda y Jack Autrey Dabbs, México, Jus, 1954, p. 345. La ficha citada también se puede consultar en el sitio de Internet http://www.lib.utexas.edu/taro/utlac/00067/lac—00067p7.html.

[2] Véase *A calendar…*, *op. cit.*, p. XI.

legible del mensaje críptico, pudiendo entonces realizar su ensayo de atribución. Pero no fueron ellos quienes lo descifraron, pues, de haberlo hecho, en el propio catálogo constaría la exposición criptológica del problema y la descripción técnica del procedimiento utilizado, manifestando por esa vía su compromiso con la responsabilidad intelectual en el ejercicio serio, minucioso, comprensivo y consecuente —desde la perspectiva lógico-científica— de la crítica textual, compromiso que seguramente tenían, vista la calidad general de su trabajo en este caso.

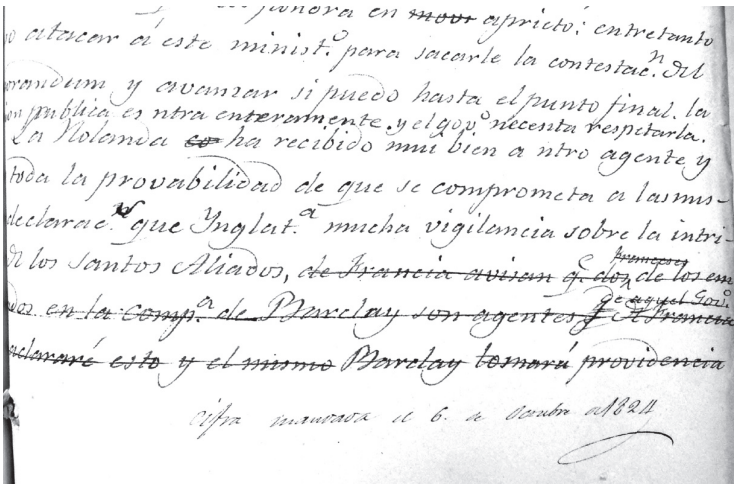
Entonces ¿quién descifró la carta? ¿Un experto en criptología contratado para el efecto? Habría sido la solución práctica ideal, pero si jamás tuvo lugar sólo queda una explicación probable: debe haber una versión en texto plano de la misma carta que no surgió de su descifrado, la cual representa un original compuesto a satisfacción del autor, transformado a cifra sólo posteriormente —en tanto a sus contenidos convenía la reserva— con la meta de garantizar su seguridad durante la transmisión (objetivo real y definido de toda criptografía). Ahora, esa versión, de hecho, existe, y se la puede consultar en el Acervo Histórico Diplomático de la Secretaría de Relaciones Exteriores de México (en adelante, AHDSREM) dentro del legajo 40-11-3, carente de numeración por fojas y titulado "Claves para la correspondencia de la Legación de México en Inglate-



1. Detalle de la carta cifrada de 6 de octubre de 1824, atribuida a José Mariano Michelena. AHDSREM, leg. 40-11-3, s/f

rra. Su uso y explicaciones sobre las mismas" (véase la figura 2). La precede un pliego con el preciso criptograma descrito en *A calendar*, y que constituye la versión críptica de aquel mismo mensaje original en texto plano, según lo argumentaré. Se trata de una vinculación criptológica e historiográfica cuyo estudio sugiere dos hipótesis también mutuamente relacionadas: (a) el texto plano del primero no surgió al descifrar el criptograma del segundo, y (b) ambos materiales son obra de Michelena. La importancia de (b) es fundamental para este escrito, pues de alcanzarse un máximo de certidumbre a su favor —mediando las observaciones, las críticas y los argumentos pertinentes— contaríamos con elementos de juicio mucho más amplios (de índole histórica, lógica y criptológica, y no sólo de crítica textual) de los que reunieron los preparadores de *A calendar* para asumir la corrección inicial de atribuir a Michelena la misiva cifrada del 6 de noviembre de 1824.

En resumen, parece improbable que los catalogadores descifraran la carta (según el argumento expuesto más arriba), debiendo entonces extraer su información de una copia de la versión original en texto plano (lo es en hipótesis) que se conserva en el AHDSREM. Es verdad que en *A calendar* nunca se alude a un ejemplar parecido,



2. Detalle del documento en texto plano que Michelena probablemente cifró y remitió a México el 6 de octubre de 1824. AHDSREM, leg. 40-11-3, s/f

luego es lícito dudar de su constancia en la Colección Nettie Lee Benson. Sin embargo, viendo la naturaleza del problema resulta igualmente lícito conjeturar que el ejemplar debe existir de cualquier forma, por lo que se impondría la necesidad de viajar a Texas para revisar los manuscritos hasta asegurarse. Con todo, provisto que mi propósito actual es demostrar con especial rigor científico y técnico la justeza de atribuir a Michelena un texto determinado, realmente no es imperativo tomar el siguiente vuelo a Texas. Apruebo, entiéndase, la postura crítica de los catalogadores en torno a su duda de atribución, y creo que su forma de acallar parcialmente la duda es apropiada y razonable. No obstante, mientras estemos obligados a medir el alcance de su interés crítico en este asunto por lo que ellos mismos declaran en su libro, esto es, prácticamente nada, enfrentaremos una disyuntiva: o descifraron la carta, o tuvieron a la vista una versión del mensaje original inmediatamente legible con cuyo auxilio penetraron en sus contenidos. La alternativa postrera, insisto, será siempre la más elegible. Podemos inclinarnos por la opción primera por un determinado motivo apreciable, pero aun si lo hiciéramos por una razón de algún modo adecuada, seguiría siendo censurable o, cuando menos, digna de lamentación la total ausencia en *A calendar* de una notificación o aviso en torno a las bases teóricas y el método utilizado para "romper" —como se dice en el argot criptológico— la cifra en la carta considerada, por cuanto ello representa un despropósito lógico-científico inadmisible en un ejercicio que se pretende serio, consecuente, en una palabra, comprensivo, de crítica textual.[3]

Explicaré cómo se "rompe" la cifra en esta carta y todo lo que se puede conjeturar y suponer a partir de una observación criptológica cuidadosa de sus contenidos, mediando una comparación con el texto claro adjunto en el legajo del AHDSREM, hasta configurar los argumentos necesarios para validar las hipótesis (a) y (b) formuladas más arriba. El procedimiento se centró en los ejemplares del AHDSREM, como no podía ser de otra manera según la estrategia de análisis general y mis propósitos de fondo, más ambiciosos que los asumidos por los autores de *A calendar*. Y si bien no he podido

[3] Como lo habría sido una exégesis rigurosa, que comenzaría por mostrar cómo en este caso Michelena recurrió a un método criptográfico reconocido y no a la taquigrafía u otro sistema de escritura que, si bien opera con signos auxiliares o símbolos para evitar la lectura inmediata de un texto, no califica técnicamente como una variedad criptológica.

revisar la copia de la carta relacionada en ese libro, mis inferencias y explicaciones acerca de la carta que tuve a mi disposición deberán ser asimismo válidas para la de la Colección Nettie Lee Benson, pues ambas pueden considerarse, en última instancia, como intercambiables desde la perspectiva historiográfica y criptológica.

1. Es difícil detectar algo en el despacho cifrado del AHDSREM que nos permita calificarlo, en términos cancillerescos, como un "principal" o una copia. Sin embargo, esta cuestión es irrelevante. Ahora bien, el documento adjunto no cifrado exhibe al calce las palabras "cifra mandada el 6. de Octubre 1824", enunciado de interpretación ambigua en tanto ignoramos si es hológrafo de Michelena. De serlo, como yo lo creo, se derivan consecuencias interesantes, comenzando por la de que constituye el original en texto plano tal y como lo habría redactado nuestro agente, pasándolo después a cifra él mismo o un subalterno. Tenemos un indicio a favor de esta posibilidad en los dos y medio renglones tachados al final, acto que se explica suponiéndolo resultado de una deliberación del autor directo, quien por ciertos motivos decide que tales líneas son inútiles, y no como efecto de la intervención de algún secretario encargado de descifrar despachos en la Primera Secretaría de Estado del Despacho de Relaciones Exteriores e Interiores de México. De este modo, la frase "cifra mandada el 6. de Octubre 1824" podría interpretarse como la expresión elíptica con la que Michelena se recordaría a sí mismo "cifré y remití por correo esta carta en esta fecha".

2. Un análisis grafológico sería valioso, quizá, para incrementar el alcance de la predicción virtualmente implícita en el supuesto hipotético anterior, pero carece de interés inmediato cuando el criptoanálisis[4] basta para demostrar que, al comparar el contenido de la carta descifrada con el de la versión legible, el mensaje termina en el primero justo antes de empezar las líneas eliminadas en el segundo, fuerte sugerencia de que dichas líneas debieron redactarse antes del criptograma, siendo eliminadas al cabo por alguna circunstancia. De no admitir esto nos queda suponer, de nuevo, que un secretario en la cancillería, luego de recibir y descifrar la misiva, las

[4] Por este término podemos entender el análisis comprensivo de las clases, las características técnicas y matemáticas y la ubicación histórica de los códigos y cifras que se han utilizado con diversos fines comunicativos a través del tiempo.

compuso por su cuenta y más tarde prefirió tacharlas conforme a su arbitrio, gesto cuya sola representación es demasiado absurda para disponernos a buscarle una explicación sensata. En definitiva, pues, la mejor hipótesis es que Michelena redactó un solo mensaje para facturar dos textos: uno sin cifrar, donde plasmó lo que deseaba comunicar exactamente, y la versión cifrada del mismo para el correo, si bien reducida ligeramente en extensión.

3. Es tiempo de examinar el criptograma, también denominado criptotexto, en sí mismo. Lo transcribiré según fui capaz de interpretarlo en el legajo del AHDSREM, numerando cada renglón sin alterar su longitud original y situando entre corchetes las fracciones ininteligibles y las letras o palabras conjeturadas a partir del contexto:

1	Cv vvvvzp xgvhattutqcj yv Ajibya mvlliyjdu
2	u vmmbvt lrsbxsan s yasnpprdrb lran zfcfvs zf
3	xgvhattutqcj fs yaluaodj llmm zlyrnb fr gvonzb
4	yv Nruiall yv hgllc llmm fg pfqpm llmm cvuco
5	uumyvotuux zl fr xqvsadijf cvluv lga zc H[p]llac
6	yv uva zeibvea yvs Bgjvasnj fr habvlo yv
7	yzx N[r]uiall fg llmm ig xgvgpbbu; fr zlyrnbntr
8	yv mvlijrudlin nv fvb cr mvibenayg xgv fgb df=
9	ncnnen yv Neungus llmm fvb ulmtqsa gf bjib
10	lraheeo zf zc lrqg: nv vjihv zf Ajibyia yv hrv=
11	qvz yamm has cguonfs u Hrahe(c)oixr s zf zc
12	Avajlll nv vjiovla lga zejnndcm ygb has llmq=
13	bejnvgb cguonfs zf ygb ajitvuan; zle[c]c xguc llllx=
14	hvllvpf Zlynjb llmmqvsa ajdgpbdj na xgv fg
15	qvvvzb yvs vva[t]votdf vaofa vvvtl ucoijbs
16	Mvtinto[v] lran agurjuam pfi zoyqedijn
17	y[u] egb xgrgheuuxaxbrllen llmm egb lgvzsa zf
18	uharano: zfcfauafc[c] uaebop ullipvsa a zlcr Ha=
19	uvouemax, lran nrlnnlle fr xgvhattutqcj yvs
20	hvucnbnymu s unibubr na lm[m]ql crbhr zc lmc=
21	hl aavng.
22	Fr Cgsnjea cr mvlvxjdj hmg
23	vamb u immgpso uymbpf s crg oglln ljxov=
24	cifallnz yv llmm nv xoudnpmzlli u frb
25	habavt yvlyvsaxaxbat llmm stoyvuemji; hmbi[…]
26	gaovgbnxai ngjfa fr dfcfeha yv fgb nrvhe[…]
27	ucqnzps.
	Octubre 6. a 1824

Para desarrollar el análisis me representó una ventaja poseer dos conocimientos antecedentes: 1) este despacho integra una serie con otros de clase similar que intercambiaron Michelena y sus superiores en México durante 1824 —notablemente Lucas Alamán mientras éste tuvo la cartera de Relaciones Interiores y Exteriores—, y 2) los detalles del criptosistema que emplearon para cifrar su mutua correspondencia.[5]

En efecto, Michelena remitió un total de seis despachos en cifra durante 1824: 4 en julio, 1 en octubre y 1 en noviembre. En varios casos[6] aplicó un criptosistema del que también se sirvió Lucas Alamán cuando redactó una misiva con fecha 12 de julio para instruir a su agente sobre las estrategias a seguir —de preferencia en un frente común con los representantes diplomáticos de otros países americanos, especialmente Argentina, Colombia y Chile— en relación con un proyecto inglés de firmar un tratado a propósito del reconocimiento de las independencias americanas.[7] Advertí esto tras comparar esta misiva y un despacho remitido por Michelena el 6 de noviembre siguiente;[8] también pude comprobar entonces que ambos hacían funcionar el sistema guiándose por la misma palabra clave, "Firmeza" (si bien Alamán se plegó a la lección "Firmesa" por motivos criptológicos que no viene al caso mencionar).[9]

Ahora, no he localizado descripciones y detalles técnicos de este preciso criptosistema ni en documentos de archivo ni en libros, pero conseguí deducirlos luego de que por ensayo y error supe identificar el modo preciso de operar con la clave citada en una *tabula recta*.[10] Por su clase general, cuenta entre los de sustitución polialfabética, reproduciendo en lo particular el modelo tradicionalmente conocido como de Vigenère (si bien lo justo es ceder la paternidad a Giovan Battista Belaso), un clásico de la criptografía manual que se aprende a reconocer por su dependencia técnica en una matriz o

[5] Véase Roberto Narváez, "La criptografía diplomática mexicana en la primera mitad del siglo XIX. Tres ejemplos", *Documenta & Instrumenta*, n. 6, 2008, p. 30-42.

[6] Uso esta restricción porque la inspección de registros archivísticos me ha convencido de que Michelena también utilizó cifras distintas a las polialfabéticas, notablemente una de diccionario. Planeo comentar esta evidencia en un trabajo de próxima aparición.

[7] Roberto Narváez, "La criptografía diplomática…", *op. cit.*, p. 39-41.

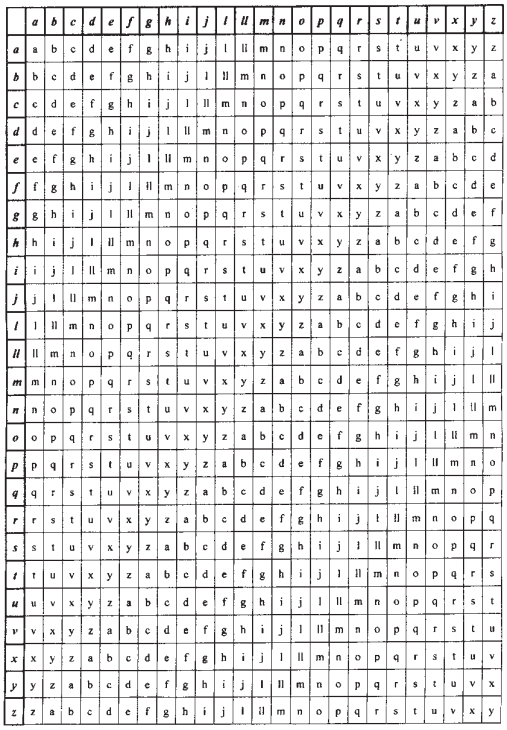
[8] En *A calendar…* se lo describe como el ítem HD17-6.4196, fólder 2334, sin dudas de atribución.

[9] Roberto Narváez, "La criptografía diplomática…", *op. cit.*, p. 41.

[10] Inspirado por dos *tabulas rectas* de clase parecida que se encuentran en el mismo legajo 40-11-3 del AHDSREM sobre las claves de la Legamex en Inglaterra durante 1824.

tabula recta, artilugio de típica evocación renacentista entre cuyas variaciones más familiares destacan las de Giambattista della Porta y el abad Tritemio.[11]

¿Por cuánto tiempo aplicó Michelena este criptosistema y la clave convenida? Siendo un hecho, a juzgar por la evidencia, que tanto él como sus jefes en México aparentemente no vieron razones para modificar o cancelar el criptosistema en el periodo julio a noviembre de 1824, se impone pensar que también debieron usarlo en octubre. Y Michelena lo hizo, sin duda, como pude comprobarlo tras aplicar "Firmeza" para descifrar la carta del 6 de octubre, guiándome por la misma matriz de 25 x 25 que diseñé durante la investigación del despacho del 6 de noviembre;[12] la reproduzco para facilitar la misma comprobación a mi lector:



[11] Información sobre estos criptógrafos puede hallarse en cualquier enciclopedia o manual respetable de criptografía.

[12] Roberto Narváez, "La criptografía diplomática…", *op. cit.*

Se procede colocando en pares los elementos de la clave con los del texto cifrado para fijar las direcciones que han de seguirse desde los dos alfabetos, el de definición o del texto plano (renglón inicial de la matriz) y el de cifrado (primera columna de la izquierda), hacia el interior del mapa formado por los alfabetos deslizados recíprocamente un lugar a la izquierda (prescripción tendiente a reducir los promedios de frecuencia en la aparición de cada letra sustituta en la cifra), hasta localizar, en sucesivas intersecciones, las letras formadoras de cada palabra en el texto plano original.

Como ilustración del procedimiento, en el gráfico se simula en orden descendente la articulación de cada ruta sucesiva en pos de la intersección donde se ubica la palabra en texto plano, usando como ejemplo el renglón 1 de la carta que nos ocupa:

Clave	*F*	*i*		*F*	*i*	*r*	*m*	*e*	*z*		*F*	*i*	*r*	*m*	*e*	*z*	*a*	*F*	*i*	*r*	*m*	*e*
Cifra	C	v		v	v	v	v	z	p		x	g	v	h	a	t	t	u	t	q	c	j
Texto plano	H	e		q	e	n	i	d	o		c	o	n	t	e	s	t	a	c	i	o	n

Clave	*F*	*i*		*F*	*i*	*r*	*m*	*e*	*z*	*a*		*F*	*i*	*r*	*m*	*e*	*z*	*a*	*f*
Cifra	y	v		A	j	i	b	y	j	a		m	v	ll	i	y	j	d	u
Texto plano	d	e		F	r	a	n	c	i	a		r	e	d	u	c	i	d	a

En el texto plano resultante, "He qenido contestacion de Francia reducida", se observa un error en la segunda palabra, de lo que podemos inferir un par de supuestos muy probables: (i) Michelena lo cometió mientras aplicaba la clave con el auxilio de la matriz; en verdad, no es raro equivocarse y tomar una letra por otra cuando se aplica manualmente un sistema de sustitución polialfabética, especialmente uno basado en el modelo Belaso-Vigenère, de configuración tan barrocamente densa, si se permite la expresión;[13] (ii) Michelena debió redactar el manuscrito inmediatamente legible, en el que tachó las líneas finales, antes de cifrarlo, siendo el error comentado antes el principal indicio a favor de esta posibilidad; en efecto, sólo pudo deberse a fallas durante su operación criptográfica la incorrecta transformación a cifra de aquel vocablo,

[13] Para el siglo XX se puede citar como ejemplo flagrante de error por esta causa un espécimen criptográfico destinado a Madero, véase mi artículo "La criptografía de los maderistas (1910-1911). Análisis pormenorizado de un caso especial: el criptosistema de Gabriel Leyva Solano y Francisco I. Madero (1910)", de próxima aparición en *Memorias de la Academia Mexicana de la Historia*.

mismo que en el original se lee "tenido" sin contratiempos. Por otra parte, no se debe pensar que la braquigrafía en términos como "contestaci.n" y muchos otros de la versión clara cumplía una función para modelar en algún sentido el cifrado posterior; en éste como en muchos casos análogos, tales abreviaturas revelan tan sólo que Michelena tenía el afán de terminar la composición cuanto antes, debido a que lo importante era ponerlo completo en cifra para su remisión a México.[14] Además, este criptosistema carece de dispositivos para encriptar signos de puntuación, como es fácil reconocerlo por una simple inspección de la *tabula recta*.

4. Sería precipitado conjeturar que la persona encargada de "traducir" claves en la cancillería mexicana, una vez recibida la carta de Michelena, corrigió las faltas en la cifra mientras recuperaba el texto plano, a fin de garantizar al secretario del Despacho una lectura sin tropiezos del mismo, supuesto que cometía un despropósito si le entregaba el descifrado directo y el secretario, ciertamente, no estaba para confundirse a causa de las confusiones criptográficas que por cualquier malaventura hubieran podido sufrir sus agentes y ministros previamente. Esta posibilidad, sin embargo, es inadmisible porque deja sin explicar la braquigrafía en "contestaci.n" y más de seis otras palabras en el documento (pueden ubicarse revisando la figura 2), porque no se antoja verosímil responsabilizar de las abreviaturas a nuestro hipotético descifrador, a menos que tuviese la instrucción de formularlas por ciertos motivos. Mas ¿cuáles podrían ser esos motivos? A nosotros, en todo caso, nos falta siquiera uno para imaginar al canciller ocupándose de buena gana en evaluar el ingenio braquigráfico de sus empleados. Estas reflexiones, como se puede ver, tienden a cimentar la idea de que Michelena redactó el texto plano primigenio de esta carta.

5. Veamos ahora el peculiar estilo de nuestro agente al usar la clave. Como se aprecia en el gráfico más arriba, "Firmeza" no siempre cumple su ciclo de repetición en toda la extensión de su espacio

[14] El recurso a las abreviaturas con este fin era muy común entre los diplomáticos mexicanos del XIX, siendo un caso extremo el de José A. Torrens en Colombia, véase mi artículo "El 'Diario reservado no. 18' de José Anastasio Torrens (1829)", *Estudios de Historia Moderna y Contemporánea de México*, 38, julio-diciembre 2009, p. 139-163. Por otra parte, las líneas que coronan a dos palabras en la cifra de Michelena que estoy comentando, una en el renglón 5 y la otra en el 7, probablemente funcionan como indicadores braquigráficos o de división silábica, aunque para averiguar esto con seguridad se necesita recuperar más información en los archivos.

(para decirlo en términos técnicos). Esto significa que en cada caso inicia y termina en una extensión determinada por la cantidad de letras en la palabra que se encripta. El espacio de "Firmeza" es 7, medida de las veces que deberían rotar los alfabetos en la matriz para potenciar el efecto de la polialfabeticidad: nivelar las frecuencias relativas de los caracteres sustitutos. Ahora, mide 8 la serie conjugada de los elementos en "He tenido"; sin embargo, como lo ilustra el gráfico, la clave no se repite completa para regular el cifrado de esos ocho elementos, esto es, no hace rotar en ciclos completos hasta comprender a todos los alfabetos, pero acaba y reinicia con un ritmo sincopado, digamos, marcado por los espacios entre las palabras. La clave se contrae a dos elementos cuando el término a cifrar es igualmente tan largo, caso de "He"; luego "Fi" hace cifrar "He" con "Cv" (rotación alfabética de dos); viene la pausa del carácter en blanco y toca el turno de velar "tenido"; la clave reinicia desde el principio, pero se agota en "Firmez" y con ello genera "vvvvzp" (rotación de 6) como sustitución de "tenido" (marginando el detalle del error en el ejemplar). Con el siguiente vocablo, "comunicación", la clave se queda corta, y es entonces cuando se repite en estricto ciclo "FirmezaFirme" hasta abarcar todo el espacio, rotando los alfabetos hasta 12 veces. Lo más interesante, a mi juicio, para la historia de la criptología mexicana y general, es apreciar cómo Michelena descuida la prescripción de Belaso, el diseñador del criptosistema, y prefiere ceñirse al estilo recomendado por Girolamo Cardano para un criptosistema similar.[15] En cambio, Lucas Alamán se atuvo a la ortodoxia belasiana en tanto se sirvió del mismo método para corresponder a su agente (si bien modificando la clave a "Firmesa"), rotando invariablemente los alfabetos hasta siete veces.[16]

6. En cuanto a sus dispositivos generales de seguridad, este criptotexto es muy vulnerable. Ante todo, su longitud es desmesurada, hecho inaceptable cuando se trata de imposibilitar en el más alto grado su decriptación, es decir, la penetración de su significado por un sujeto no autorizado para leerlo —un espía, vamos— a fuerza de ingenio y paciencia, en tanto ignora las reglas de transformación criptográfica que convinieron seguir los autores del despacho inter-

[15] *Cfr*. David Kahn, *The codebreakers. The story of secret writing*, Nueva York, Macmillan, *c*. 1967, p. 144.

[16] Roberto Narváez, "La criptografía diplomática…", *op. cit*., p. 41.

ceptado. En efecto, cualquier espía sagaz que inspeccionara la muestra con atención podría observar una serie de datos valiosos —por ejemplo, la puntuación y el número de letras en el alfabeto de definición— para orientar sus ensayos prometedoramente hacia la restitución de sus contenidos. Cuanto más extensa es una cifra, mayor es la probabilidad de que sus elementos presenten rasgos uniformes de frecuente aparición. La observación de esta frecuencia relativa sugiere la idea de que unas reglas criptográficas se aplicaron en un patrón invariable. Por ello, medir los intervalos de aparición de ciertos conjuntos crípticos constituye un índice para deducir la clase general del criptotexto analizado. Mientras más amplios son los intervalos, mayor es la probabilidad de que el criptosistema usado dependiese de una clave, y reconocer esto implica suponer que el criptotexto es de sustitución y no de transposición, y que la sustitución, en lo específico, es polialfabética y no monoalfabética. En la misiva de Michelena, por ejemplo, se cuentan cinco espacios entre los grupos "yj" del renglón 1 y los grupos "zf" del renglón 2, y siete espacios entre la doble aparición del trigrama "llmm" en el renglón 4. Y en tanto se comprueba que los caracteres de separación, incluyendo a los blancos entre los términos de otros grupos crípticos en el ejemplar, nunca son superiores a 7 ni menores a 5, se deduce que la extensión de la clave debe promediar entre estos dos guarismos. Al admitir esta posibilidad, un espía podría inferir la clave "Firmeza" tras múltiples ensayos, culminando así con éxito lo que se denomina "ataque por palabra probable". Además, la detección de repeticiones de grupos completos, como la muy ostentosa de "xgvhattutqcj" en los renglones 1, 3 y 19; el hecho de que se mantienen los signos de puntuación, las mayúsculas como capitales iniciales o de sustantivos propios (función acusada por la puntuación), y —lo más grave desde el punto de vista criptoanalítico— los espacios o caracteres blancos entre las palabras le servirían como indicios preciosos para averiguar el ritmo singular de aplicación de la clave.

Lo anterior demuestra que Michelena fue ingenuo al dotar a su cifra de la misma fisonomía de corrección compositiva, digamos, que infundió al texto plano en donde vertió su mensaje original, llegando al extremo de reproducir incluso las sangrías. Esto hace sospechar que su intelección del propósito fundamental de la criptografía; garantizar la seguridad en las comunicaciones reservadas, era notablemente defectuosa. (Lo mismo se puede decir de sus corresponsales,

comenzando por Alamán). Su error fundamental, en esta misiva como en la del 6 de noviembre, fue cifrar el mensaje completo, porque si bien la polialfabeticidad cumple, en principio, su cometido de nivelar las frecuencias relativas, la nivelación se quiebra conforme la cifra crece, dando así lugar a repeticiones y otras fallas que pueden aprovecharse para decriptar el texto. Un descuido similar es imperdonable para todo criptógrafo, mas el evitarlo nunca se convirtió en un hábito dentro del ámbito de las comunicaciones diplomáticas y políticas en México durante los siglos XIX y XX, a juzgar por ciertos registros de archivo.[17] Ciertamente, al meditar sobre esa tendencia debemos interrogarnos por la causa de que la cancillería consintiera en usar unas mismas "claves" —como genéricamente las llamaban entonces— por lapsos prolongados, a menudo más de seis meses, como lo evidencian las cifras de Michelena. Una conjetura elemental, desde el punto de vista teórico, es que los despachos o cartas de ese tipo nunca eran interceptados, y si lo eran, el enemigo era incapaz de restablecer su sentido claro, para fortuna del gobierno mexicano. Otra explicación posible se deriva del estudio inductivo de series criptográficas en varios archivos, la resumo de esta forma: los usuarios dependían de las cifras y sistemas codificadores inventados en otros países (particularmente europeos) y no solían estar al pendiente de los modelos cada vez más complejos y seguros —al menos en teoría— que se producían, sobre todo a partir de la segunda mitad del XIX. Además podemos inferir que si una dependencia similar era la norma, se echaba entonces de menos la preparación técnica y matemática requerida para disponer a la imaginación hacia el diseño de criptosistemas autóctonos.[18]

En conclusión, los razonamientos y argumentos precedentes vuelven altamente probable que José Mariano Michelena escribiera la carta cifrada del 6 de octubre de 1824 y el documento modélico en texto plano que lo acompaña en el legajo del AHDSREM, hipotéticamente identificado como la versión definitiva del mensaje que deseaba transmitir a la cancillería de México en aquella fecha. La

[17] Fue una práctica regular entre 1824 y 1917, por lo menos, de acuerdo con evidencias cuyo análisis pondré a consideración del público próximamente.

[18] Este diagnóstico es inevitable cuando se considera la gran persistencia de los nomencladores y las cifras digráficas, de sustitución simple monoalfabética y de sustitución polialfabética estilo Belaso-Vigenère desde 1824 y hasta bien entrada la década de 1920, como lo trataré con pormenor técnico en un escrito futuro.

lectura coordinada de dicho documento modélico y el texto descifrado de la carta revelan una correspondencia exacta en el número de temas y la secuencia de su tratamiento, quedando así patente la relación criptológica entre ambos. Y al examinar este hallazgo a la luz del sumario temático del ítem correspondiente en *A calendar de la Colección Hernández y Dávalos*, se deduce que éste y el del AHDSREM son idénticos, luego ambos admiten las críticas y los análisis aquí vertidos a propósito del segundo.

Apéndice

A continuación transcribo no el texto plano que resultó de mi ejercicio de descifrado, sino el del documento original escrito muy probablemente por el mismo Michelena, manteniendo la ortografía, la acentuación, la puntuación y la braquigrafía, y poniendo entre corchetes las palabras ilegibles o de lectura conjetural (dejo fuera las palabras tachadas, el interesado puede tratar de interpretarlas consultando el original o la figura 2 de este trabajo).

> He tenido contestac.n de Francia reducida a buenas palabras dilatorias para entrar en contestac.n diciendo que espera la llegada de M.r Samuel de modo que lo unico que hemos adelantado es la confesion hecha por el Mtro de ser emanada [del] Gov.o la mision de [dho] Samuel lo que no constaba, la [venganza] de reconquista se les ha reanimado con los informes de Smáll [*sic*] que les asegura un gran part. o en el país: se trata en Francia de mandar diez mil hombres a Martinica y en Ferrol se trabaja por embarcar 2500 homb.s en dos fragatas [que] tienen nuevas. Asi esto como [gto] medite España quedará frustrado si con la venida del bergant.n tigre o alg. recursos para fomentar una expedición los constituc. que los pondrá en aprieto: entretanto [pien]so atacar á este minist.o para sacarle la contestac.n del memorandum y avanzar si puedo hasta el punto final. La [opinión] publica es ntra enteramente y el gov.o necesita respetarla.
>
> La Holanda ha recibido mui bien a ntro agente y [hay] toda la provabilidad de que se comprometa a las mis[mas] declarac.es que Ynglat.a mucha vigilancia sobre la intriga de los Santos Aliados.
>
> Cifra mandada a 6. de Octubre a 1824