ISSN: 1697-4328

RECIBIDO: 7/07/10
EVALUADO: 15/06/11
ACEPTADO: 20/06/11

LA CRIPTOGRAFÍA MADERISTA EN LA REVOLUCIÓN MEXICANA (1910-1911). CRIPTOANÁLISIS DE UNA CARTA CIFRADA POR GABRIEL LEYVA SOLANO

THE CRYPTOGRAPHY OF THE "MADERISTAS" IN THE MEXICAN REVOLUTION (1910-1911). CRYPTANALYSIS OF A CIPHER LETTER BY GABRIEL LEYVA SOLANO

Roberto Narváez
Instituto Cultural Helénico, A. C. México, D. F.

Resumen: Este artículo se basa en el texto de una ponencia dictada por el autor en junio de 2010. Aborda temas relacionados con las comunicaciones secretas del movimiento revolucionario comandado por Francisco I. Madero a partir de 1910. Se compone de dos partes: la primera es una breve reseña crítica de ejemplos criptográficos del maderismo que fueron generados entre 1910 y 1911, la segunda describe paso a paso el criptoanálisis que aplicó el autor para decriptar una carta parcialmente cifrada de Gabriel Leyva Solano a Madero. El propósito general último es contribuir al conocimiento de la criptografía mexicana en el siglo XX. En lo particular se trata de poner a disposición de los estudiosos el contenido completo de la carta de Leyva Solano, por primera vez después de 100 años, y al mismo tiempo someter a la crítica técnica e histórica el procedimiento criptoanalítico puesto en operación para recuperar el texto plano.
Palabras clave: Criptografía, criptoanálisis, sustitución polialfabética, Francisco I. Madero, Gabriel Leyva Solano, maderismo, Revolución Mexicana.

Abstract: This article is based on the text of a lecture that was delivered by the author in June 2010. It addresses issues related to the secret communications of the revolutionary movement led by Francisco I. Madero in 1910. It consists of two parts: the first is a brief critical review of a few cryptographic examples of the "maderista" movement that were generated between 1910 and 1911; the second part describes every step of the cryptanalysis applied by the author to decrypt a partially encrypted letter written by Gabriel Leyva Solano and addressed to Madero in 1910. In the end, the general purpose of this paper is to contribute to the knowledge of Mexican cryptography in the 20th century. In particular it seeks to make available to scholars the full content of the letter by Leyva Solano, for the first time after 100 years, and at the same time submit to technical and historical criticism the sort of cryptanalysis put into operation to recover the plaintext.
Keywords: Cryptography, cryptanalysis, polyalphabetic substitution, Francisco I. Madero, Gabriel Leyva Solano, maderismo, Mexican Revolution.

PREÁMBULO[1]

Los métodos criptográficos, o criptosistemas, que Francisco I. Madero convino en utilizar con sus diferentes corresponsales en varios momentos de su actividad política son relativamente sencillos, perteneciendo todos, generalmente, a la clase de cifras por sustitución monoalfabética. Su análisis detenido permite caracterizarlos técnicamente desde el punto de vista criptológico y, por tanto, aprender a definirlos y estudiarlos por su clase, una ventaja mayor para el historiador interesado en ubicarlos cronológicamente y compararlos con métodos idénticos o análogos. Esto es lo que trataré de hacer a propósito de los ejemplares criptográficos legados por varios seguidores del movimiento revolucionario encabezado por Francisco I. Madero, destacando entre los mismos al sinaloense Gabriel Leyva Solano (1871-1910).

Las dos metas principales de este artículo son:

1. Contribuir a la historia de la criptología mexicana por medio de una breve reseña de la criptografía maderista entre 1910 y 1911, y muy especialmente a través del análisis, la descripción técnica y la presentación detallada del procedimiento aplicado para decriptar la cifra en una carta dirigida por Gabriel Leyva Solano a Francisco I. Madero, fechada en Sinaloa el 6 de junio de 1910.

2. Reflexionar sobre las ventajas de practicar el criptoanálisis para estimar la importancia del método lógico-crítico en la historiografía general, en tanto dicho método se regula en gran medida por la función del razonamiento inductivo, la hipótesis y la analogía en el tratamiento de los documentos.

ALGUNOS CRIPTOSISTEMAS COMUNES A LOS MADERISTAS (1910-1911)

Entre la documentación que se resguarda en el "Fondo Histórico Francisco I. Madero", con sede en el Palacio Nacional de México, es posible localizar y revisar una serie de textos de varias clases en cuya composición original participó, total o parcialmente, algún sistema de codificación o cifrado. En su mayoría, tal documentación está formada por telegramas y cartas, y su observación atenta permite identificar la clase de las cifras o códigos que contienen. En ciertos casos basta una inspección somera para reconocer el género preciso de los criptosistemas utilizados por maderistas ubicados en diferentes ciudades en los albores de la lucha revolucionaria. Esto es tanto más fácil cuando el folio bajo escrutinio constituye la descripción formal y técnica del sistema transformador a cifra o código; sucede así, por ejemplo, con el folio 23517,[2] donde apa-

[1] *Este artículo se basa en el texto de una conferencia que dictó el autor el 10 de junio de 2010 en la ciudad de Culiacán, Sinaloa (México), dentro de las actividades relativas a la conmemoración del bicentenario de la Independencia y el centenario de la Revolución de la actual nación mexicana, pero también como parte de los eventos realizados en Sinaloa in memoriam de Gabriel Leyva Solano (1871-1910), "protomártir" de la revolución maderista y autor de la carta parcialmente cifrada cuya solución se ofrece en estas páginas. El autor ha realizado algunas variaciones de composición en un intento de simplificar los análisis técnicos del documento y el proceso criptoanalítico. Eliminó asimismo referencias y alusiones que resultaban de interés tan sólo en el contexto de la conferencia dictada en Culiacán.*

[2] Secretaría de Hacienda y Crédito Público. Oficialía Mayor. Dirección General de Promoción Cultural, Obra

rece trazada una matriz de sustitución simple numérica en la que se pretende lograr el efecto del polialfabetismo por el recurso al ordenamiento irregular de las letras del alfabeto (30 en total, por la inclusión de la CH y la W, cosa extraña para un criptosistema en español de cualquier época) en las primeras tres filas. Además, queda patente la intención de fortalecer la seguridad del sistema —que constituye básicamente una cifra y no un código— por la adición de características propias de un sistema codificador basado en la distribución de sílabas (hasta de cuatro elementos), artículos, preposiciones, sufijos y palabras completas, como "Presidente", "Conspiración" y "Gobernador", términos que, si bien son claramente miembros de un código, estaban destinados al cifrado por el mismo método que se seguiría con las letras alfabéticas.

Todo esto, sin embargo, no resta valor histórico al hecho de que la inserción de dichos términos-código determine la incorporación de funciones propias del clásico nomenclátor a un sistema que de otra manera se vería reducido a pertenecer a la clase de cifras por sustitución simple monográfica o poligráfica, vertidas esencialmente en el modelo del sistema de Polibio (siglo II a. C.), aunque también evocadoras de sistemas renacentistas de sustitución polialfabética como los de Giovanni Battista Porta, Giovanni Battista y Mateo Argenti, y el denominado método "Larrabee" (variación del sistema Vigenère clásico, del cual hablaremos más adelante) que usó el Departamento de Estado de los Estados Unidos desde 1913, según lo delata la observación de la numeración en doble columna para el cifrado aparentemente polialfabético, situada a la izquierda de la matriz y cuyo papel era funcionar como "clave" del cifrado.

Tales son las características fundamentales que me parece suficiente mencionar de esta "Clave telegráfica con el señor don Francisco I. Madero" de Baroquiel M. Alatriste, fechada en "Puebla, septiembre 10 de 1911". La conclusión criptológica básica es que pertenece a la clase general de cifras por sustitución monoalfabética simple, destacando no obstante el interés de sus analogías estructurales con métodos típicamente aplicados para la formación de códigos o cifras polialfabéticas.

Examinemos ahora la cifra en una carta de Antonio Sirión Sarabia a Madero, fechada en Parras el 8 de octubre de 1911. Transcribiré un fragmento: "Suplícote telegrafiarme motivo Emilio ordena, (Clave Adrian) HRFMTI TLKMFA esta PRTISOPR OTOHRFM PMFMHAPO…".[3] En primer lugar, el hecho de que no todo el mensaje iba cifrado parece revelar en los corresponsales una conciencia madura, bien enterada sobre el genuino propósito de la criptografía (aumentar la seguridad en la transmisión del mensaje previniendo la intromisión de terceros no autorizados a leerlo) y las potencialidades de los métodos de decriptación para "romper" la cifra. En segundo lugar, la remisión a una "Clave Adrian" sugiere que los maderistas usaban sistemas compartidos, esto es, que por lo menos tres usuarios podían servirse de una misma clave "bautizada" con el nombre del individuo que la diseñó, o del destinatario principal, o en atención a otros motivos, hábito muy propagado entre los revolucionarios de todas las facciones. En tercer lugar tenemos, por fin, a los elementos en cifra. Una observación superficial basta para descubrir que la sustitución es con letras, pero de poco nos asiste si partiendo de ella conjeturamos que se trata de una cifra polialfabética; de hacerlo caeríamos en importantes contratiempos analíticos, comenzando por suponer, mediando un conteo, que la sustitución fue de uno a uno (hecho, por lo demás, de ocurrencia normal en los criptosistemas de sustitución simple). Para evitar esto debemos concentrarnos en la posibilidad de que una valoración estadística de ciertas parejas de letras, elegidas de

Pública y Acervo Patrimonial. Fondo Histórico Francisco I. Madero (FHFM). Folio 23517.

[3] FHFM. Folio 19930.

acuerdo con criterios de yuxtaposición o aparente transposición, sugerirá que lidiamos con una cifra cuya estructuración específica depende de una complejidad en el alfabeto de cifrado y no el de definición (como sucede con el de Alatriste); hacer esto, además, debe forzarnos a pensar que el mensaje velado probablemente no es igual en longitud a la cadena de elementos crípticos inserta en la carta, disparándose así la inferencia hipotética de que debió utilizarse un criptosistema ordenado conforme a la sustitución simple monoalfabética, al menos en lo esencial.

Consideraciones de índole similar también resultarían apropiadas a propósito de los criptogramas en una carta del 9 de julio de 1911, remitida por Francisco Vázquez Gómez desde la Ciudad de México.[4] Los grupos crípticos GATHI, NKBCB, BTFCO y ZBGQT, por ejemplo, mueven a pensar que la organización en quintetos no es caprichosa (idéntico caso es el de la mayoría de cifras telegráficas, aunque por motivos especiales, típicamente ajenos a consideraciones criptológicas), lo mismo sucede acaso con la repetición, en los tres últimos grupos, de la B seguida o precedida de consonantes exclusivamente. Una comparación con las cifras en la carta de Sirión Sarabia sugiere que el sistema efectivamente usado no fue el mismo, esto es, que la "Clave Adrian" usada en el primero no se utilizó en el segundo. Pero esto de ningún modo repercute negativamente en la probabilidad de que ambas constituyan casos de criptosistemas pertenecientes a una misma clase general.

Sin embargo, hay por lo menos un ejemplar cuyas peculiaridades lo separan, hasta cierto grado de importancia criptológica, del modelo configurado por el estudio de los casos expuestos hasta aquí. Me refiero a un telegrama remitido a Madero, ya entonces presidente, por Nicolás Meléndez desde Puebla. El mensaje trata de un asunto militar y el aspecto del cifrado es así: 8.24.98.21.19.41.11.61.48.21.12.41 […] 29.20.28.98.41.73 […] 28.98.89.78.77.[5] La sustitución es numérica; cada cifra está formada por un máximo de dos dígitos y la separación entre cada una está marcada por puntos invariablemente. Ahora bien, aquí el detalle crucial a estimar es la sistemática colocación de tales puntos. Sería fácil pensar que su función podría explicarse por consideraciones técnicas relativas al telégrafo, pero la verdad es muy otra y su discernimiento habrá de obtenerse por exclusiva ruta criptoanalítica.

Ante todo debemos decir que los criptógrafos de reputación, en todas las épocas, han reprobado la inserción de cualesquiera signos auxiliares de la escritura en un criptograma. La razón es muy comprensible desde la perspectiva criptoanalítica, y tendremos ocasión de analizarla detenidamente conforme progresemos en el análisis de la cifra en la carta de Leyva Solano. Por lo pronto, el hecho es que debemos lidiar con esta cifra particular, facturada por un individuo identificable en una fecha y lugar establecidos. Para tratar de explicar, entonces, la distribución de los puntos de separación en un patrón indiscutible, conviene preguntarse si la necesidad de compartimentar, digamos, a cada unidad o par de cifras por medio de puntos es indicativo de la organización del texto oculto, lo cual equivale a inquirir sobre una razón cuantitativa entre los elementos del texto plano, esto es, inmediatamente legible, y los del criptotexto; en otras palabras, si por cada número hay una letra oculta, o bien si por hasta cada par de números habremos de suponer escondida una letra sola o con pareja. En el fondo, se trata de formular un supuesto hipotético adecuado a la esperanza de que estas cifras derivan de un criptosistema de sustitución o monoalfabético o polialfabético, de modo que para resolverlas nos baste configurar un método de lectura centrado en el análisis de frecuencias.

[4] FHFM. Folio 8502.
[5] FHFM. Folios 22787 y 22771.

Como es manifiesto, la investigación aquí también se orienta, en buena medida, por la comprobación historiográfica de que, vista la fecha del documento y su lugar de creación, entre otros aspectos, trátase de una cifra manual, clásica, y es un hecho reconocido que el análisis de frecuencias constituye el procedimiento fundamental para "romper" a todas las cifras de tal época. Una observación meticulosa, guiada por la teoría enunciada, nos impone la hipótesis provisional de que enfrentamos aquí cifras de sustitución simple monoalfabética, vulnerables por tanto al análisis de frecuencias; así lo exhibe la repetición de grupos como el .28.98. No sería extraordinario que se usaran hasta 4 dígitos para ocultar una sola letra, sin embargo, el progreso del análisis frecuencial nos prohibiría mantener la idea de que tal es el caso, pues ocurre también que tanto el .28. como el .98. aparecen varias veces unidos a otros pares de dígitos. Al cabo, en fin, nos daríamos cuenta de que cada letra del texto plano se ha encubierto con un máximo de dos dígitos, por medio de una sustitución simple basada en alguna matriz de transformación similar a la de Alatriste, aunque desde luego con números en lugar de letras como "claves" de la transformación.

Restaría descubrir, sin embargo, cómo pudo ser que una misma letra se hubiera encubierto con hasta tres pares distintos de grupos numerales, en todos los cuales, empero, el primer dígito siempre era el mismo. Esto sería interesante desde la perspectiva comparativa, pues un fenómeno idéntico se observa en la correspondencia de muchos participantes en la lucha revolucionaria, destacando la del ejército constitucionalista comandado por Venustiano Carranza. El hecho actual es que esto sucede en el ejemplar de Meléndez que revisamos, al cual no es difícil analizar y caracterizar técnicamente por la razón de que el descifrado aparece manuscrito entre líneas. Esta circunstancia documental nos enseña que un historiador, cuando se ve precisado a ejercitar el criptoanálisis, puede y debe aprovechar no sólo las lecciones técnicas y metodológicas de la historia criptológica general, sino también las ventajas concedidas por los registros mismos y la insospechada riqueza de los acervos, siendo el caso extremo hallar un legajo donde se describen las reglas de transformación a cifra o código para un texto críptico determinado.

El tomo II del *Epistolario* de Francisco I. Madero, editado por primera vez en 1963, reúne telegramas o cartas en cifra en 11 de sus páginas. Todos estos materiales están fechados en 1910 y su cifrado dependió de sistemas análogos a los que usaron los maderistas en 1911. Se trata, pues, de cifras basadas en alguna variedad de los métodos de sustitución simple monoalfabética. Veamos un par de ejemplos.

En un telegrama enviado por Madero a su hermano Gustavo, fechado el 25 de mayo de 1910 y totalmente cifrado, hallamos estos sintagmas: "PHBJR BFMKO AHYQX LCKQD ÑMODV NODQP DKRFN ÑAMJO PXAÑA BKSGK BKY".[6] Descontando el último trigrama, es clara la división general en grupos de 5, justo como sucede en los casos del Fondo Madero antes reseñados (exceptuando al de Nicolás Meléndez). Un arreglo similar se aprecia en una carta remitida por Madero a Federico Werther desde San Antonio, Texas, el 30 de octubre de 1910: "Si tiene listas de EMAHD PIPDG ELSCIHOB, de los que están por acá en la frontera hoy que están IGEPA QSHDL EGALI FECOM NPEGOM, mándemela […] Le he mandado decir varias veces que no conviene por ningún motivo NHDBE QOLIH DFOCE INPEM IPEGD HOLDE ELIHS GAMIH DBIFD CEQSL NPDGEL…"[7] Aquí la organización de las cifras en quintetos no indica un patrón evidente, lo que demanda una explicación, sobre todo porque la misma peculiaridad se detecta en una carta de Madero a Francisco Cosío Robelo, fechada también en San Antonio el 31

[6] F. I. MADERO, *Epistolario* (1910). *Archivo de don Francisco I. Madero*, tomo II, México, p. 160.
[7] F. I. MADERO, *Epistolario (1910)*…, tomo II, p. 297.

de octubre del mismo año; veamos este fragmento: "[…] LEPAB NHIBO HIFNG IHIPE GAQDP OHEQNPEG".[8] La última cifra reúne 8 grafemas, detalle que inmediatamente nos debería indicarnos dos cosas: 1) no se trata de un telegrama y 2) por aparecer al final del texto, la convención debía responder a un intento por nivelar el análisis de frecuencias impidiendo la unión constante de elementos que, de otra manera, exhibirían una constancia de yuxtaposición sospechosa.

En resumen, el análisis de estos y otros ejemplares muestra que la sustitución monoalfabética era la regla criptográfica entre Madero y sus colaboradores. La cifra en la epístola de Leyva Solano de 1910 constituye, sin embargo, una excepción muy interesante a esa regla.

ANÁLISIS Y DECRIPTACIÓN DE LA CIFRA EN LA CARTA DE LEYVA SOLANO

El mensaje completo que consta mecanografiado en el documento, después de haberme esforzado cuanto pude para establecerlo por la observación del original, está formado por todos estos elementos:

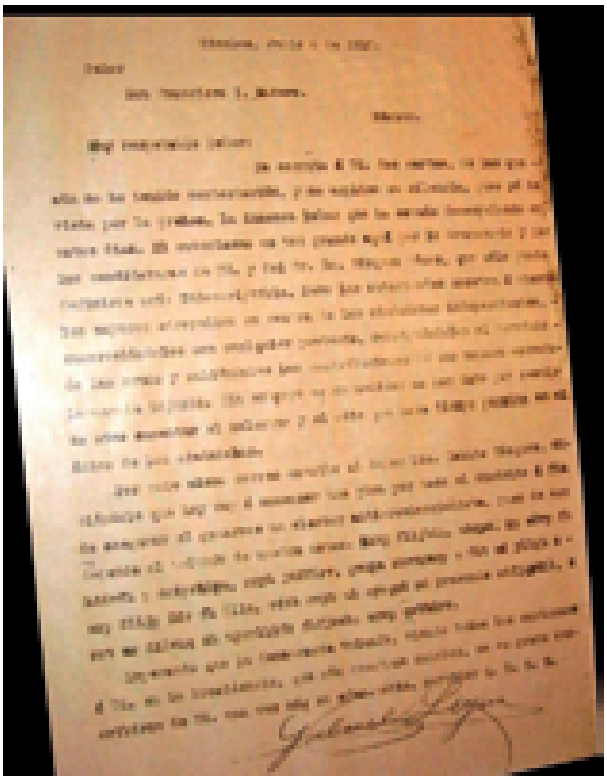
> Sinaloa, Junio 6 de 1910
> Señor
> Don Francisco I. Madero.
> México.
>
> Muy respetable Señor:
> He escrito a Ud. dos cartas, de las que aún no he tenido contestación, y me explico su silencio, pues yá he visto por la prebsa (sic), la inmensa labor que ha estado desempeñando en estos días. El entusiasmo es tan grande aquí por la democracia y por las candidaturas de Ud. y del Sr. Dr. Vázquez Gómez, que sólo puede definirse así: Indescriptible. Pero las autoridades cometen á diario los mayores atropellos en contra de los ciudadanos independientes, encarcelándolos con cualquier pretesto (sic), consignándolos al servicio de las armas y subiéndoles las contribuciones de una manera escandalosamente injusta. Sin embargo estas medidas no han dado por resultado sino aumentar el malestar y el odio que hace tiempo germina en el ánimo de los ciudadanos.
> Por este mismo correo escribo al Señor Lic. Emilio Vázquez, diciéndole que hoy voy á comensar (sic) una gira por todo el distrito á fin de asegurar el ganarnos un elector antireeleccionista, pues de eso depende el triunfo de nuestra causa. Rhtp flljbñh, uhqps, gp edvp fhhtdvfh q oxtprhñpu, rryh jdffhrv, gvxpa shvvgnxp o fñt md yllgb zerp ñlljp ñdv fh ñlln, rdtb rryh uh eyoqmd md yrnvoxde odfjqpdll, zrrt mr ñllvnq mh uyrrlllfr fhfjsoh: erep qetbñrv.
> Esperando que la democracia triunfe, viendo todos los mexicanos á Ud. en la Presidencia, que són (sic) nuestros anhelos, me es grato suscribirme de Ud. una vez más su afmo. atto. servidor Q. S. S. M.
> [Firma]

[8] F. I. MADERO, *Epistolario (1910)*…, tomo II, p. 297.

El criptograma está compuesto de 36 unidades y grupos mezclados de cifras y 176 caracteres de sustitución. Sin embargo, los lugares que ocupan en las líneas correspondientes del original no aparecen calcadas en la copia, lo cual debe ocurrir como condición fundamental para el éxito de las observaciones, inferencias e hipótesis que impone su estudio cuidadoso. Por tanto, a fin de avanzar con las precauciones técnicas necesarias, presento en seguida un gráfico con la secuencia numerada de cada fracción del criptotexto según el propio Leyva terminó consignándolas, haciendo que las rupturas al final de los renglones coincidan:

1) Rhtp flljbñh, uhqps, gp edvp fh
2) Htdvfh *q* oxtprhñpu, rryh jdffhrv, gvxpa shvvgnxp o fñt md yllgb z -
3) erp ñlljp ñdv fh ñlln, rdtb rryh uh eyoqmd md yrnvoxde odfjqpdll, z
4) rrt mr ñllvnq mh uyrrlllfr fhfjsoh: erep qetbñrv.

Para descubrir el criptosistema que Leyva, con mucha probabilidad, usó efectivamente en este caso, se necesita conducir el análisis con paciencia, imaginación y, sobre todo, un tipo de observación caracterizado por una suerte de inocencia capaz de rendir mejores y más rápidos beneficios en un criptoanálisis de los que se obtendrían con cualquier matemática rigurosa. Pero, si hay casos en que conviene al criptoanalista ser inocente, su razón surge normalmente por haber sabido apreciar la comisión de una inocencia por parte del criptógrafo. Esto fue lo que ocurrió a nuestro revolucionario maderista, y de ello dependió el triunfo de mi empresa, como se hará patente al cabo del siguiente análisis.



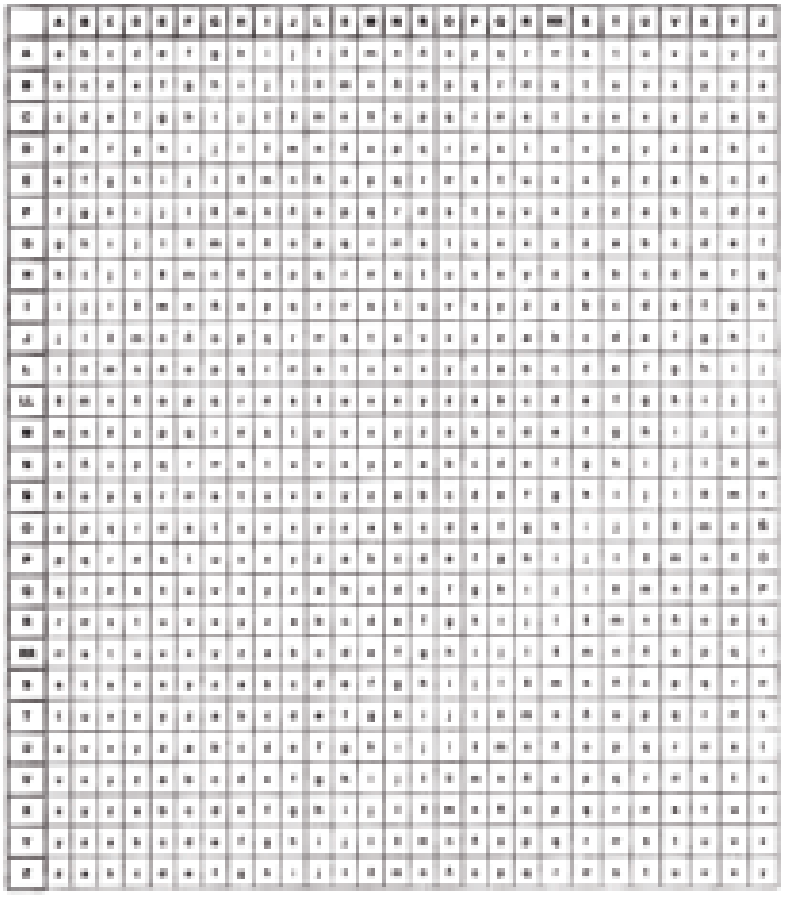
Original de la carta de Leyva Solano en el Museo Regional de Sinaloa.

Crédito por la fotografía: Rosendo Castro Amarillas.

1. Varios datos de la observación me hicieron admitir que se trata de una cifra de sustitución polialfabética. El dato crucial es la aparición repetida de ciertos grupos literales, por ejemplo, HT, FH, MD, ÑLL y RRYH. Como vemos, en exclusiva son bigramas, trigramas y tetragramas, asumiendo que los blancos entre los términos valen como caracteres independientes. Este detalle, por cierto, me inclinó a dar por seguro que no podía tratarse de un código. La transformación, entonces, debió acontecer a nivel de las letras y no de las palabras.

2. Supuse que el cifrado había dependido de un sistema básicamente idéntico al diseñado por Giovanni Battista Belaso hacia 1553 —y no por Vigenère, como se cree tradicionalmente; el verdadero método de Vigenère se distingue por cuanto impone un pareo doble de las letras de la clave y la palabra de texto plano a cifrar a causa de que las filas de la tabla forman pares. En tal sistema la transformación se regula por el uso de una tabla donde series de alfabetos se apilan hasta formar una matriz; cada nuevo alfabeto después del primero aparece deslizado a la izquierda una letra, de modo que el último en la lista comienza con la última letra del alfabeto utilizado y termina con la penúltima, lo que se verifica tanto en sentido horizontal como vertical. La función del deslizamiento recíproco (de arriba abajo, a la izquierda; de abajo arriba, a la derecha) es garantizar que los puntos de la matriz para cifrar una misma letra, tomados como coordenadas en un mapa, se multipliquen en una cantidad considerable, limitada tan sólo por la extensión del alfabeto y determinada, en cuanto a la fijación de la coordenada precisa, por la extensión o el tamaño de la palabra clave, técnicamente definido como su "espacio".

3. Para cultivar con esperanzas de fruto este supuesto hipotético era necesario satisfacer dos requisitos mutuamente vinculados: (a) calcular el "espacio de la clave" y (b) determinar el número y la identidad precisa de las letras en el alfabeto utilizado, técnicamente denominado "alfabeto de definición". Fue durante la investigación de (a) que me vi obligado a practicar con operaciones matemáticas e inducciones numerológicas muy fatigosas. No hablaré de las planas que llené con ejercicios aritméticos o algebraicos, me bastará decir que sus resultados me afirmaron en una creencia cuya validez fundamental se probó a la larga: la "palabra clave" de Leyva debía constar de cuatro grafemas a lo sumo, como lo inferí partiendo de un análisis especial de las cantidades regulares de elementos crípticos entre cada aparición de los tetragramas en la cifra. Sin embargo, con estas bases y el auxilio de la matriz que diseñé tras el estudio de (b) no logré inferir la palabra clave. En cambio, para resolver lo pertinente a (b) fue suficiente anotar todas las letras que aparecen en la cifra, la cual por alegre circunstancia es muy larga para estos propósitos. La observación de hasta tres L juntas me inclinó a pensar que el alfabeto de Leyva contenía la LL, y la aparición aleatoria de la R sola unas veces y duplicada otras me sugirió que la hoy eliminada RR del alfabeto castellano había sido mantenida por nuestro criptógrafo. Consideraciones a partir de mis investigaciones previas sobre problemas análogos, y la ausencia de la K en la cifra, me sugirieron que dicha letra faltaría en el alfabeto original. Al cabo, pues, di por buena la conclusión de que Leyva había utilizado un alfabeto de definición de 27 elementos, y como paso inicial para probar la hipótesis de que procedió al estilo de Belaso (o, si se quiere, de Vigenère, para el caso la distinción ya no importa mucho), organicé dicho alfabeto en la siguiente matriz de 27 x 27:



4. Sin embargo, en este punto se volvía urgente conocer la palabra clave, pues sólo así podría realizar la prueba de manera expedita, esto es, revirtiendo automáticamente cada elemento del criptograma pareando sucesivamente las grafemas de la cifra con las de la clave, siguiendo una determinada prescripción técnica para emplear la matriz. Esto implica sustituir a cada letra cifrada con cada letra que se va ubicando en el espacio abierto por el alfabeto del texto plano, lo cual exhuma gradualmente a cada elemento del mensaje original.

5. Antes de resolver la cuestión de la clave importa entender que un sistema como el que Leyva, por suposición hipotética, probablemente usó, está formado por un conjunto indisoluble de tres elementos: (i) la matriz (organizada por adecuación al alfabeto usado, por supuesto), (ii) la palabra clave, y (iii) la manera de aplicar esa clave —normalmente es peculiar a cada caso. Ahora, si bien es factible decriptar una clave cuando la situación criptoanalítica demanda un ataque de sólo criptotexto, como lo impone el criptosistema en cuestión; aún en el caso de restituirla, digo, no se aprende automáticamente la forma exacta en que se la aplicó, ni siquiera por vía matemática. Sea esto como fuere, la condición criptoanalítica preliminar sigue siendo la de poseer la clave, y esto era justamente lo que me faltaba en las postrimerías de julio de 2009, cuando había dedicado ya tres semanas a esta faena. Y en tanto así fuera, no podía estar totalmente seguro de que la matriz diseñada por mí era la indicada, considerando las condiciones de formación de una cifra de esta clase, como lo señalé en el punto anterior. En semejante coyuntura, pues, mis avances eran precarios, y en lo absoluto me facultaban para estimar en cualquier sentido el valor de la probabilidad de la hipótesis general que orientaba mis afanes, a saber, la utilización de un criptosistema polialfabético en este caso. Revisé mis ejercicios matemáticos, consulté manuales e historias de la crip-

tología general en busca de modelos que me inspirasen un razonamiento por analogía sugerente, pero nada conseguí. Entonces reflexioné que semejantes estrategias quizá no hacían sino alejarme de lo que verdaderamente debía interesarme: *una observación inmanente, minuciosa y prolongada del ejemplar en mis manos*. Reflexioné también que mis dificultades brotaban tal vez por afincarme demasiado en la perspectiva del criptoanalista, cuando me convenía situar ésta en una posición relativa y, más aún, de subordinación —en muchos aspectos legítimos— a la del historiador. Recordemos que el historiador está entrenado en la observación minuciosa de documentos, particularmente los escritos, pero no sólo de sus características gráficas, lingüísticas y semánticas, sino de todos aquellos cuyo estudio detenido puede revelar conexiones de valor explicativo con los caracteres propios del objeto bajo análisis. El desarrollo progresivo de esta habilidad ha impulsado la conciencia de las ventajas lógicas que reportan los criterios clasificatorios a la concepción científica de la Historia. Así, de manera similar a como el criptoanalista sabe reconocer una pieza ininteligible de comunicación por su pertenencia a una determinada clase general (o cifra o código) o clase particular (monoalfabético, polialfabético, lineal, etcétera), el historiador especializa su método para tratar a un documento comenzando por identificarlo según su clase o tipo, además de ubicarlo en un parámetro temporal. Así, las exigencias analíticas que impone la inspección de una bula papal del siglo XVI no serán iguales a las de un tratado científico del siglo XX, y ocurrirá lo mismo si comparamos las apostillas de Napoleón Bonaparte a la *Guerra de las Galias* de Julio César con una epístola parcialmente cifrada de un sinaloense revolucionario en 1910. Genéricamente, para un historiador varían los problemas críticos e inferenciales debido a que organiza en un caso de estudio concreto, peculiar, único, al autor y todos los posibles destinatarios de un texto, mismo que puede clasificarse bajo multitud de rubros posibles, como son el despacho, la minuta, el epítome, el diario, la bitácora, etcétera. En cada caso, de la lectura del documento se inferirán juicios y premisas especiales en torno a las intenciones del autor, los caracteres particulares del texto, etcétera, surgiendo de tal modo un complejo informativo cuyo abordaje lógico-crítico faculta la creación de hipótesis tratables por métodos tanto deductivos como probabilísticos. Ahora, durante la fase heurística de la investigación histórica tales hipótesis deben funcionar como auxiliares principales en el establecimiento de un texto —sin importar, en rigor, la clase del soporte donde se halla inscrito—, la consideración crítica de sus rasgos taxonómicos y la valoración cualitativa de sus singularidades, para después refinar de varios modos el esquema explicativo que se haya inferido (ante todo se recurrirá, por supuesto, a conocimientos antecedentes que la historiografía misma proporciona; en casos como éste se consulta preeminentemente la historia de la criptología, desde luego).

6. Al cabo de estas meditaciones entendí que mi renovada incursión debía comenzar, para expresarlo en síntesis, con la búsqueda de las probables intenciones de Leyva al redactar su carta, estimando en particular aquellos datos que las fuentes me proporcionaban acerca de su personalidad y trayectoria en relación con la figura del único destinatario cuya identificación se puede considerar desde un principio, y por la sola crítica interna, como evidente: Francisco I. Madero. Procediendo, sin dilación admití como mi premisa básica el hecho de que Leyva contaba entre la legión de mexicanos para quienes Madero, en tanto figura simbólica, representaba grandeza, esperanza, justicia; algo grande, digno de admiración, seguimiento y hasta inmolación. La visualización de todas estas cualidades encarnadas en un sujeto viviente, matizada por complacencia con estereotipos y ciertos dictados de la imaginación (popular, religiosa, etcétera), les despertaba la idea de un individuo merecedor de respeto y deferencia como ningún otro. Ahora bien, la parte automáticamente legible de la carta muestra la sistemática deferencia del autor hacia su líder ideológico —o, si se quiere, su ídolo. Me pregunté si podía imaginar alguna razón para suponer

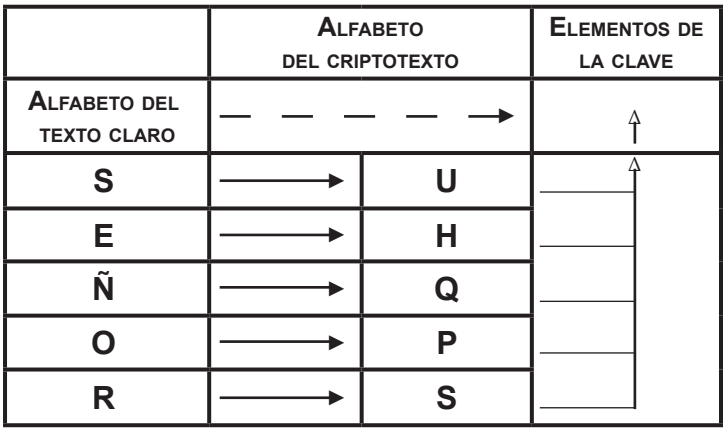
que semejante estilo cambiaría en la parte cifrada. Semejante interrogación fue crucial, pues como no podía imaginar esa posible razón debí suponer que por lo menos una fórmula de retórica halagadora presente en el texto claro se repetiría en el criptograma. Sea el caso, por ejemplo, de "respetable señor". La dificultad criptoanalítica para probar esta hipótesis, organizada fundamentalmente —recordarlo— en torno a la convicción de que el sistema empleado era polialfabético y de sustitución uno a uno, yacía en seleccionar el criterio para situar un grupo de caracteres crípticos que muy probablemente ocultaría la frase "respetable señor". En otros términos, mi problema era elegir correctamente un grupo de hasta 15 caracteres de sustitución que, una vez descifrados, permitieran leer "respetable señor". Esto era tanto como adivinar de golpe que el primer carácter de tal grupo sería exactamente el que escondería la primera letra clara de nuestra expresión ejemplar, o sea, la "r" de "respetable…", esta letra y no otra. ¿Cómo "adivinar" esto? Me propuse inferirlo, mejor, por las reglas del criptoanálisis y la reflexión historiográfica.

7. En primer lugar me pregunté si acaso la repetición de aquella fórmula completa no le habría parecido al mismo Leyva una franca zalamería, cuando él, por lo demás, no pretendía componer un panegírico de Madero (de hecho, el texto tenía fines de acción política, como veremos). Así, la duplicación del "respetable" *en la parte cifrada* de un manuscrito de esta clase resultaba poco menos que impertinente. Pero, me dije, nada de esto impide que lo contrario pueda ocurrir con el término "señor". Mientras trataba de ubicar el sitio de este vocablo en la cifra realicé la observación suprema, de importancia tanto lingüística como criptológica, que tanto había necesitado para dar un cauce triunfal definitivo a mi ejercicio heurístico. Me refiero a *los espacios entre las palabras y las comas* en el criptotexto.

Entonces advertí la fatal inocencia en que incurrió Leyva. Y digo bien fatal, pues, como lo he mencionado ya, si algo recomiendan los criptógrafos, en particular los de la época manual o clásica de la criptología, es eliminar los espacios entre palabras, la puntuación y cualesquiera otros signos auxiliares de la escritura en el criptotexto. Nuestro revolucionario incumplió estos requisitos o por ignorancia de la técnica criptológica rigurosa o por un descuido inocente; en cualquier caso, podemos ver aquí un índice del grado de comprensión que tanto él como Madero tenían de los objetivos y métodos criptográficos. Tal grado debía ser bajo, provisto que ambos convinieron en utilizar un criptosistema fallido de origen, esto es, armado con dispositivos de seguridad muy vulnerables. (No podemos razonablemente dudar que Madero conocía este criptosistema, o de otro modo ¿cómo descifraría la carta, una vez recibida? Es absurdo imaginar a Leyva confiando en que Madero consumiría tiempo y esfuerzo en decriptar la parte cifrada, como si en aquella época tensa del inicio revolucionario bajo su mando no lo absorbieran labores más urgentes.)

8. Al suponer que la función sintáctica, gramatical y de puntuación de las comas y espacios en el texto plano subyacente se reproducía en la cifra, perfilé una orientación técnica precisa, de orden básicamente lingüístico, para aislar un grupo de cinco caracteres que, según la hipótesis, probablemente sustituían a "SEÑOR". Ahora, si recorremos el criptograma de izquierda a derecha y notamos la pausa marcada por las comas, hallamos un grupo como el buscado después de la primera coma: "UHQPS". Tomemos la matriz de 27 x 27. Si este arreglo era el indicado, entonces el experimento del descifrado expedito devolvería, si resultaba positivo, dos pruebas y una revelación: las primeras son (i) que "UHQPS" ocultaba "SEÑOR" y (ii) que la matriz era de buen diseño —pues sólo así habríamos podido develar la palabra oculta en una sola secuencia de pasos—, y la revelación será la palabra clave. Así queda exhibida con toda fuerza la cabal imbricación de la clave y la matriz en los métodos clásicos de sustitución polialfabética. Sin embargo, como el alfabeto del criptotexto en la matriz carecía de función reguladora en ausencia de la clave, mi experimento debía limitarse a ubicar cada elemento de la cifra dentro del mapa o la red —como

se podría denominar topológicamente— formada por los nodos de todas las posibles coordenadas en el conjunto de los alfabetos apilados, y ver qué sucedía. Las líneas de correspondencia debían trazarse del exterior al interior del mapa, partiendo en secuencia desde cada letra en el vocablo "SEÑOR" del alfabeto vertical hasta llegar a cada una de las grafemas del grupo "UHQPS" en los correspondientes alfabetos deslizados, y en la intersección girar en ángulo recto hacia el alfabeto horizontal. Cada grafema que resultara por este medio debía representar, en principio, un elemento de la palabra clave. Para expresarlo gráficamente, con la palabra elegida el procedimiento, en su primera parte, era como sigue:



Moviéndonos desde el alfabeto número 21 de la serie, tenemos que de la "S" hasta la "U" hay tres lugares, y si, de acuerdo con la hipótesis, "U" equivale a "S" en la cifra, entonces la primera letra de la clave es "C", que aparece luego de ascender desde la "U" hasta el alfabeto regulador del criptotexto. Haciendo lo mismo con la "E" del texto plano y la "H" de la cifra, tenemos que la "D" sigue a la "C" como parte de la clave. Procediendo igual con los tres caracteres restantes de cada grupo, aparece "CDDBC" como la clave buscada.

9. También yo quedé perplejo en este punto. Semejante liga consonántica no forma un sustantivo, o un verbo, ni siquiera un adjetivo, ¿cómo suponer que representa una genuina clave criptográfica? La práctica común es diseñar o elegir dichas claves con base en algún vocabulario reconocible, más o menos convencional pero efectivamente operativo en su propio ámbito; sean, por ejemplo, vocabularios como el de la química, la mitología, la astronomía, la caza o la geografía. ¿Cómo averiguar, me pregunté, la especie de léxico en donde "CDDBC" tiene algún significado? Se me ocurrió que podía tratarse de las siglas o el término código de una organización política relacionada con el maderismo. Juzgando verosímil esta idea, pero sin ulteriores investigaciones sobre los partidos o grupos políticos amigos de Madero, ya en Sinaloa o en cualquier otro estado (que de suyo eran irrelevantes para llevar a sus últimas consecuencias la hipótesis criptológica), me dispuse a probar aquel singular quinteto de letras como la clave real del sistema. Lo hice con los mismos 5 caracteres crípticos que, según el experimento anterior, debían equivaler a "SEÑOR". Si la cadena "CDDBC", asumida como clave, funcionaba de la manera estándar para *revertir* el procedimiento que originalmente se habría usado para transformar "SEÑOR" a cifra, el nuevo experimento probaría que la identificación inicial estaba justificada. El método, ahora, consistía en partir del alfabeto superior en la matriz y descender hasta intersectar cada elemento de la cifra, para después girar a la izquierda y situar la letra correspondiente del texto claro en su respectiva columna. Bajando de la C a la U y girando a la izquierda, encontramos la S. Esto sucede

en el alfabeto 21 de la serie. Descendiendo de la D a la H y apuntando al alfabeto del texto claro localizamos a la E (quinto alfabeto de la serie). Procediendo del mismo modo con las letras restantes, tenemos que la clave CDDBC funciona efectivamente para descifrar SEÑOR de UHQPS. El acomodo de los elementos puede graficarse así:

■Clave: **C D D B C**
■Criptotexto: **U H Q P S**
■Texto plano: **S E Ñ O R**

10. Según todo lo anterior, mi suposición de que "SEÑOR" se repetía en la cifra era correcta. Por otro lado, necesariamente debía juzgar como válida la clave inferida, cuando menos la evidencia me imponía ese juicio, en tanto cada ensayo me mostraba que bajo su gobierno y la guía de la matriz la palabra "SEÑOR" se transformaba en "UHQPS" y viceversa. Mi hipótesis general, entonces, parecía comprobada favorablemente sin lugar a dudas. No obstante, cierta reflexión me hizo temer que me precipitaba. De pronto ya no me parecía, digamos, sospechoso que "CDDBC" pudiera ser la clave, sino el hecho de que tal clave, aún habiendo probado su efectividad, estuviera compuesta de cinco elementos. Me explico: en un sentido criptológico, probar que ese conjunto operaba con éxito en el cifrado de un vocablo de hasta 5 letras no implicaba que dicho conjunto debía constituir una clave criptográfica de hasta 5 caracteres. Hacerlo sería tanto como postular una medida de 5 al espacio de la clave sin mucho fundamento, considerando que derivaba de un experimento más bien tosco, diseñado sin especial rigor técnico. El hecho más importante a considerar, sin embargo, era que de ninguna manera se observa como un patrón que los grupos crípticos en la carta tienen 5 caracteres como máximo (como se puede observar, el grupo de cifras más largo reúne hasta 10 caracteres). Si se verificara lo contrario, entonces la postulación sería lícita. Esta circunstancia resultó irónica, pues me forzó a reconocer que provenía directamente y con toda limpieza de la presencia de comas y espacios en el criptotexto, misma observación cuya valoración hipotética me había inspirado las ideas requeridas para salvar mi análisis en un momento crítico. Por fortuna, recordé que mis ejercicios matemáticos preliminares me habían indicado que la clave utilizada por Leyva debía cubrir 4 espacios alfabéticos a lo sumo. Si este era el caso, por sí mismo se ofrecía un tercer experimento a realizar tomando como objeto a cualquier grupo de hasta 4 elementos en este criptograma, y con ello se renovaba mi esperanza de haber conducido hasta este punto un análisis correcto en lo general. Obviamente, sólo una de dos combinaciones posibles, CDDB o DDBC, tenía que ser la clave buscada de 4 espacios. Elegí CDDB porque lógicamente había probado ya su aptitud, aunque parcial, en ensayos anteriores, y seleccioné la cadena RHTP, inaugural de la cifra, por cierto. Sirviéndome de la matriz descubrí lo siguiente:

■Clave: **C D D B**
■Criptotexto: **R H T P**
■Texto plano: **P E R O**

Surgía una palabra reconocible, magnífica señal. En consecuencia, la variación DDBC quedó eliminada (la probé, con todo, para sonreír ante el galimatías resultante).

11. Un experimento más era obligado para despejar la última incógnita pendiente sobre la clave: la periodicidad con que la aplicó Leyva. Parecía seguro que debía reiniciar completa cada cuatro caracteres, pues de otro modo se tornaba inválido asignar el valor 4 al espacio de la clave. Procedí a descifrar con CDDB el siguiente conjunto al inicio del criptograma:

■**Clave:**	**C D D B C D**
■**Criptotexto:**	**F LL J B Ñ H**
■**Texto plano:**	**D I G A M E**

Éxito una vez más, aunque todavía no decisivo. Me convencí de que el reinicio cíclico fue la norma sólo hasta consumar un nuevo ensayo:

■**Clave:**	**C D D B C D C D D B C C D C D D B**
■**Criptotexto:**	**F LL J B Ñ H U H Q P S G P E D V P**
■**Texto plano:**	**D I G A M E S E Ñ O R E N C A S O**

Los primeros 21 elementos crípticos, pues, una vez descifrados con el método descrito y agregando, por evidente conveniencia de la prueba, los espacios y las comas, reza: "Pero dígame, señor, en caso". La probabilidad criptológica y matemática de que Leyva usara CDDB como su clave para cifrar ese fragmento postrero de su carta era ya, por tanto, demasiado elevada para tomarla por un prodigio de adivinación.

Gracias a esto podemos leer el documento completo de manera automática. Lo presentaré con el aspecto que adquirió al cabo del análisis, antes de suplir los acentos ortográficos y efectuar las correcciones, distribuido en el esquema de 4 renglones que usé para presentar la cifra en su configuración original:

1) **RHTP FLLJBÑH, UHQPS, GP EDVP FH**
   PERO DIGAME, SEÑOR, EN CASO DE
2) **HTDVFH *Q* OXTPRHÑPU, RRYH JDFFHRV, GVXPA SHVVGNXP O FÑT MD YLLGB *Z* –**
   FRAUDE O NTROPELLOS, QUE HACEMOS, ESTOY RESUELTO N DAR LA VIDA X
3) **ERP ÑLLJP ÑDV FH ÑLLN, RDTB RRYH UH EYOQMD MD YRNVOXDE ODFJQPDLL, *Z***
   CONMIGO MAS DE MIL, PARA QUE SE CUMPLA LA VOLUNTAD NACIONAL, X
4) **RRT MR ÑLLVNQ MH UYRRLLLFR FHFJSOH: EREP QETBÑRV.**
   ***POR LO MISMO LE SUPLICO DECIRME: COMO OBRAMOS*.**

Acaso los errores que se advierten en los renglones 2 y 3 deben atribuirse a confusiones o descuidos al momento de cifrar. Es común equivocarse al cifrar un texto manualmente. Se aprecia en este caso que los deslices forman patrones bien diferenciados: la "a" se sustituye con "o" en lugar de "y", mientras que la conjunción "y" termina velada con la "z" en lugar de la "a". Esto es indicativo de una confusión sistemática en el criptógrafo, debida muy probablemente a un uso precipitado de la matriz, quizá por tener el tiempo en contra o porque el denso tejido de las letras en el "mapa" le provocaba cuando menos un par de insistentes alteraciones en su enfoque visual.

A continuación presento la versión del original mecanografiado corregida, con las tildes en su lugar, automáticamente legible de principio a fin, por primera vez en 100 años.

Sinaloa, Junio 6 de 1910

Señor

Don Francisco I. Madero.

México.

Muy respetable Señor:

He escrito a Ud. dos cartas, de las que aún no he tenido contestación, y me explico su silencio, pues yá he visto por la prebsa (sic), la inmensa labor que ha estado desempeñando en estos días. El entusiasmo es tan grande aquí por la democracia y por las candidaturas de Ud. y del Sr. Dr. Vázquez Gómez, que sólo puede definirse así: Indescriptible. Pero las autoridades cometen á diario los mayores atropellos en contra de los ciudadanos independientes, encarcelándolos con cualquier pretesto, consignándolos al servicio de las armas y subiéndoles las contribuciones de una manera escandalosamente injusta. Sin embargo estas medidas no han dado por resultado sino aumentar el malestar y el odio que hace tiempo germina en el ánimo de los ciudadanos.
Por este mismo correo escribo al Señor Lic. Emilio Vázquez, diciéndole que hoy voy á comensar (*sic*) una gira por todo el distrito á fin de asegurar el ganarnos un elector anti-reeleccionista, pues de eso depende el triunfo de nuestra causa. *Pero dígame, señor, en caso de fraude o atropellos, ¿qué hacemos?; estoy resuelto a dar la vida y conmigo más de mil, para que se cumpla la voluntad nacional, y por lo mismo le suplico decirme: ¿cómo obramos?*
Esperando que la democracia triunfe, viendo todos los mexicanos á Ud. en la Presidencia, que són (*sic*) nuestros anhelos, me es grato suscribirme de Ud. una vez más su afmo. atto. servidor Q. S. S. M.

[Firma]