ISSN: 1697-4328
DOI: http://dx.doi.org/10.5209/rev_DOCU.2015.v13.49742

RECIBIDO: 08/06/15
REVISADO: 22/06/15
ACEPTADO: 23/06/15

SOBRE ALGUNOS CRIPTOSISTEMAS MEXICANOS DE PRINCIPIOS DEL SIGLO XX

ON SOME MEXICAN CRYPTOSYSTEMS FROM THE BEGINNING OF THE 20TH CENTURY

Roberto NARVÁEZ
Instituto Cultural Helénico
Universidad Nacional Autónoma de México

Resumen: Descripciones, criptoanálisis y comentarios técnicos e históricos a propósito de una serie de criptosistemas utilizados por diversos individuos y grupos políticos en México entre 1907 y 1921.
Palabras clave: Criptografía, criptoanálisis, magonismo, Ricardo Flores Magón, México, siglo XX, felicismo, carrancismo.

Abstract: Descriptions, analyses and technical and historical commentaries about a number of cryptosystems used by different political groups and individuals in Mexico between 1907 and 1921.
Keywords: Cryptography, cryptanalysis, magonismo, Ricardo Flores Magón, Mexico, twentieth century, felicismo, carrancismo.

1. SOBRE LA CRIPTOGRAFÍA DE RICARDO FLORES MAGÓN Y SUS CORRELIGIONARIOS (1907-1908)

En octubre de 1903, Ricardo Flores Magón y sus seguidores se exiliaron en la ciudad de Laredo, Texas, para escapar de la persecución del gobierno mexicano. Más tarde, acosados por agentes del presidente Porfirio Díaz, Flores Magón y los redactores del órgano de comunicación de su movimiento, *Regeneración*, se trasladaron a Saint Louis, Missouri, en donde se formó la Junta Organizadora del Partido Liberal Mexicano (PLM) (28 de septiembre de 1905) y se afinó un proyecto insurreccional basado en el programa del mismo partido (1 de julio de 1906). En esa misma ciudad los magonistas trabaron relaciones con el movimiento anarquista internacional. Posteriormente Ricardo y su hermano Enrique se dirigieron a Canadá y El Paso, Texas, participando en el intento de tomar Ciudad Juárez, Chihuahua, y más tarde uniéndose a la insurrección liberal que comenzó con la toma de Jiménez, Coahuila. Esta operación falló y Ricardo inició un escape que lo llevó hasta Los Ángeles, California, pasando por San Francisco y Sacramento. Se reunió poco después con el resto de la directiva del PLM y juntos perseveraron

en el esfuerzo insurreccional que tenía comprometidos a unos setenta grupos liberales en México y en los estados fronterizos de Arizona y Texas, apoyándose en la pequeña publicación semanal *Revolución* (junio de 1907 a marzo de 1908).[1]

El célebre detective Thomas Furlong incluye en su libro *Fifty Years a Detective* un capítulo sobre la operación que lo llevó a detener a Ricardo Flores Magón y seguidores.[2] Fue contratado en 1907 por el entonces gobernador de Chihuahua, Enrique Clay Creel Cuilty, para localizar el cuartel de los revolucionarios o "revoltosos" magonistas —como de ordinario los llamaban los agentes del gobierno—, cuyo objetivo último, según él, era derrocar el gobierno de Díaz. Que tal fuera en última instancia el propósito del magonismo y el PML es discutible (no se tenían por reformadores, eso es un hecho), pero lo que nos interesa saber aquí es que Furlong y su agencia pronto localizaron el dicho cuartel en el 900 de la avenida North Channing en Saint Louis.[3] La vigilancia constante y las pesquisas se prolongaron hasta que Ricardo y algunos de sus correligionarios fueron arrestados el 23 de agosto de 1907 en Los Ángeles. Pasaron dos años en prisión por haber sido hallados culpables de violar las leyes de neutralidad estadounidenses, y después fueron extraditados a Tombstone, Arizona.[4]

Según lo anterior, es claro que Furlong y compañía culminaron con éxito la misión encomendada, si bien ello no significó el final del movimiento magonista. Furlong declaró en su libro que este caso fue el más difícil y uno de los más importantes en su carrera. Aduce para ello varias razones, de entre las cuales me interesa resaltar cinco: "La astucia de Ricardo Magón y el hábito de secrecía que ocasionó en sus seguidores, el hecho de que ninguno de ellos hablara inglés, que todos y cada uno usaran muchos alias y escribieran toda su correspondencia importante en varios sistemas de cifra...".[5] Esta enumeración sugiere que nuestro detective coordinó un buen trabajo de espionaje, interceptando, leyendo y retransmitiendo a sus empleadores en México no pocas cartas de los magonistas.

En efecto, muchos lugares en la correspondencia de Ricardo Flores Magón entre 1905 y 1918, cuando fungía como presidente del PLM, dejan ver un constante recurso a los seudónimos y las claves. Como ejemplo veamos la siguiente

[1] Esta síntesis de acontecimientos se basa en la semblanza biográfica de Ricardo Flores Magón escrita por Jacinto Barrera Bassols, disponible desde internet en el sitio http://archivomagon.net/inicio/biografia/. Entre las monografías celebradas en torno a los Flores Magón y el PML en los Estados Unidos destaca la de W. DIRK RAAT, *Revoltosos: Mexico's Rebels in the United States, 1903-1923*, Texas, 1981.

[2] T. FURLONG, *Fifty Years a Detective*, St. Louis, Miss., 137-148.

[3] T. FURLONG, *Fifty Years a Detective*, St. Louis, Miss., 137-138.

[4] T. FURLONG, *Fifty Years a Detective*, St. Louis, Miss., p. 139.

[5] T. FURLONG, *Fifty Years a Detective*, St. Louis, Miss., p. 147-148.

colección de extractos tomados de cinco cartas escritas a diferentes destinatarios entre el 9 de marzo y el 8 de julio de 1907.

Extracto 1

[Sacramento, California], marzo 9 de 1907

Querido Chamaco [Manuel Sarabia]:

Me refiero a su cartita del 1º del actual. Debe estar usted ya sumamente desesperado, pero tenga una poca de paciencia. Yo también lo estoy porque no me mandan el famoso archivo. Pardiez. La que contesto, viene marcada con el número 17. Está completa la serie. Al mandarle la vista le mandaré pormenores de los correligionarios que se han portado mejor. Extensamente le hablaré del asunto. Ahora recibí seis cartas de Arcuijo [Antonio de P. Araujo][6]... Al marchar me escribirá usted con la misma dirección de don Pilar [Saucedo], es la más segura por ahora. Le mandaré a usted un escrito para que no tengan desconfianza los correligionarios.

[...]

No conozco al señor Bosques. Tal vez sea un buen elemento en la próxima lucha. Si puede usted entrevistarlo será muy bueno. Me alegro de haber recibido la dirección de Fakir [Librado Rivera]. Gracias. No he sabido nada de Verea [Antonio I. Villarreal]. Tal vez ya se haya puesto en camino. Le adjunto una clave que usarán usted, Arcuijo y Foca [Aarón López Manzano]. No escriban todas sus cartas en clave, sino solamente los nombres de personas, poblaciones, estados, etcétera o cualesquiera otros datos que pudieran servir a la dictadura para deshacer nuestros planes si cogiera alguna carta.

A Arcuijo no le escribo más porque tengo que hacer la clave.

Reciba un abrazo de su hermano

R. M. Caule [Ricardo Flores Magón][7]

Extracto 2

[Los Ángeles, California,] junio 1º de 1907

Señor don Eulalio Treviño
[s.l.]

Mi querido y fino amigo:

Recibí su grata del 19 del pasado. No debe usted desalentarse por las contestaciones que ha recibido de los ricos de quienes habla. Los ricos no pueden amar una causa que es de los humildes, de los de abajo, de los hombres que quieren ser libres y felices. No hay que tomar en consideración a esos ricachos...

Recibí carta de Aurelio [N. Flores] en la que detalla su disgusto con el doctor Mondragón. Respecto de Juan José Arredondo hemos recibido muchos informes desfavorables. Como quiera que sea, no hay que desmayar.

[...]

Espero sus letras. Usen para usted y Aurelio alguna clave que sirva solamente para poner nombres propios de lugares o de personas pues escribir todo en clave, es perder el tiempo. Denme a conocer su clave y con ella me escribirán nombres propios como le digo a usted.

[6] Este nombre, sin siglas, es de Antonio de Pío Araujo (1883-1944), pero en los documentos aparece unas veces como Antonio de P. Araujo y otras como Antonio P. de Araujo.

[7] Disponible desde Internet en el sitio http://archivomagon.net/obras-completas/correspondencia-1899-1922/c-1907/cor139/. (Acceso: 12 de abril de 2015).

Estoy esperando carta de Aurelio, para saber sus planes, porque si no tiene a dónde ir, puedo dirigirlo a algún estado para que hable con los amigos.[8]

Extracto 3

[Los Ángeles, California,] junio 13 de 1907

Señor Antonio P. de Araujo
[s.l.]

Mi querido, fino amigo y correligionario:

Ya desesperaba de no tener carta de usted y hasta me estaba temiendo que habría usted sido víctima de alguna celada. Afortunadamente nada de eso ha pasado. Por lo que veo no ha recibido mis anteriores...

Espero contestación de mis anteriores. Yo creía que iba usted a estar más tiempo en Del Río. Le envié una carta para que se la entregara al señor [Atilano] Barrera.

Ruego a usted que a nadie enseñe las cartas del ingeniero. Sería desastroso que también a él lo arrestaran. ¿Tiene usted bien asegurados sus papeles? Porque no es remoto que de un momento a otro practiquen un cateo en la casa donde reciben usted y Tomás [L. Sarabia] la correspondencia. La correspondencia de Tomás está en el proceso que se instruye a Aarón [López Manzano]. Hay muchas cartas de él y pudiera ser que, pretextando la violación a las leyes de neutralidad, se mandase practicar un cateo. Con mucha anticipación le dije a Aarón que pusiera en clave las listas y todos los datos interesantes para sus trabajos. Parece que no hizo aprecio de dicha sana observación. Ruego a usted que no eche en saco roto la experiencia que nos ha proporcionado este último golpe y que ponga a salvo papeles y datos.

Las claves ya no sirven. Hay que hacer nuevas, pero para entendernos usted y yo, quiero una clave especial. Hay que darle también una clave al ingeniero. No le escriba usted, deme su dirección y yo le escribiré, porque tengo buenos conductos para enviar cartas sin que lleven el sello de los Estados Unidos. Además no disfraza usted su letra que tan conocida es ya, porque entre los papeles recogidos a Aarón, iban muchos escritos con todas las letras de nosotros...[9]

Extracto 4

[Los Ángeles, California,] junio 25 de 1907

Señor don Antonio P. Araujo
[s.l.]

Mi querido amigo y compañero:

Hasta que por fin recibí carta de usted. Ya me estaba desesperando a causa de su prolongado silencio que no sabía a qué atribuir. Por fortuna lo veo como siempre, dispuesto a seguir bregando hasta que seamos libres. No desmaye pues, y adelante.

Recibí sus cinco claves. La verdad, resulta un trabajo demasiado pesado. No pude traducir el pequeño párrafo que escribió usted en clave, porque se pierde lastimosamente el tiempo. Es preferible que haga usted una clave sencilla, por el estilo de la que tenía con usted y con la cual se podía escribir aprisa, una vez teniendo cierta práctica. Con una clave nos basta. Ponga en la clave que invente la ll, la rr, la k y la w. Que no falte ninguna letra porque todas se usan. También la numeración de uno al 9, incluyendo el cero, conviene tener en clave. No la haga de signos difíciles de hacer, sino de signos sencillos. Espero pues

[8] Disponible desde Internet en el sitio http://archivomagon.net/obras-completas/correspondencia-1899-1922/c-1907/cor197/. (Acceso: 12 de abril de 2015.)

[9] Disponible desde Internet en el sitio http://archivomagon.net/obras-completas/correspondencia-1899-1922/c-1907/cor210/. (Acceso: 12 de abril de 2015.)

la clave. La clave no debe ser conocida más que por nosotros. Usted no se la dará a nadie, ni a los más íntimos amigos de San Antonio [, Texas].[10]

Extracto 5

[Los Ángeles, California,] julio 8 de 1907

Querido Tomás:

[San Antonio, Texas]

Tengo a la vista su grata de 27, 28 y dos de 3 del pasado junio, números 5, 6 y sin números las de fecha 30.

Dice Aarón [López Manzano] que ha visto en el proceso que se le instruye las cartas de usted, y por eso creo que sus cartas provocaron su arresto. Sin duda alguien que ya conoce la letra de usted sorprendió esas cartas antes de que llegaran a su destino y por eso pararon en poder de las autoridades. No se las quitaron a Aarón, porque entonces así lo dijera. Es pues de creerse que se estaba violando la correspondencia de usted. Lo comprueba la existencia de esas cartas en el proceso que a nuestro amigo se le está instruyendo.

Es mejor que no empleemos la clave de Charalito [Juan Sarabia]. Dejémosla especial para tratar con él. No vaya a suceder que nos aprehendan y entonces podría caer dicha clave en poder de nuestros enemigos. Invente usted una clave que no sea complicada y con la cual escribiremos solamente nombres de personas o lugares y alguno que otro detalle interesante, pues ya sabe usted que se pierde mucho tiempo escribiendo en clave.[11]

Tan sólo en esta breve muestra contamos 8 seudónimos, 7 de ellos en la primera pieza, entre otros "Arcuijo" por Antonio P. de Araujo, "Fakir" por Librado Rivera, "Verea" por Antonio I. Villarreal, "Foca" por Aaron López Manzano y "R. M. Caule" por el mismo Ricardo Flores Magón. En lugar de seudónimos podríamos hablar más bien de nombres código, en tanto la codificación es esa parte de la criptografía donde la transformación a lenguaje velado se realiza al nivel semántico y no sintáctico de las palabras. Como sea, los extractos corroboran el apunte de Furlong a propósito de la ingente secrecía con que el grupo magonista procuraba rodearse para evadir las amenazas a sus proyectos libertarios.

Por otra parte, ciertas declaraciones de Ricardo nos permiten vislumbrar la calidad y alcances de sus nociones acerca del sentido y los propósitos últimos de la criptografía. En el extracto 1, por ejemplo, urge a no escribir las cartas íntegramente en clave, "sino solamente los nombres de personas, poblaciones, estados, etcétera o cualesquiera otros datos que pudieran servir a la dictadura para deshacer nuestros planes si cogiera alguna carta". Ecos de esto vibran en el extracto 5. Esto indica una buena comprensión de la conveniencia de no generar criptotextos muy vastos, ya que, en el caso de intercepción, se ofrece una ventaja notable a quien

[10] Disponible desde Internet en el sitio http://archivomagon.net/obras-completas/correspondencia-1899-1922/c-1907/cor222/. (Acceso: 12 de abril de 2015).

[11] Disponible desde Internet en el sitio http://archivomagon.net/obras-completas/correspondencia-1899-1922/c-1907/cor230/. (Acceso: 12 de abril de 2015).

intente decriptarlos por medio del análisis de frecuencias, pues a mayor la cantidad de criptogramas en un mismo escrito mayor es la posibilidad de localizar patrones de repetición de grupos crípticos (bigramas, trigramas o conjuntos aún más largos) cuya cuantificación y posterior análisis pueden sugerir hipótesis fecundas para deducir las equivalencias y, al cabo, la estructura completa del criptosistema utilizado.

También parece desprenderse de otras fracciones citadas que Ricardo tenía conciencia de la necesidad de multiplicar las claves en proporción al número de los corresponsales y de renovarlas en cuanto hubiera pruebas de que habían caído en manos del adversario. Es acaso por esta razón que, en el extracto 3, dice a Araujo: "Las claves ya no sirven. Hay que hacer nuevas, pero para entendernos usted y yo, quiero una clave especial".

En vista de lo anterior, creo que nuestro líder anarquista entendía suficientemente el objetivo último de toda criptografía: ofrecer medios de *asegurar*, en lo posible, las comunicaciones reservadas durante su transmisión. Sin embargo, valoraba sobre todo lo que podríamos denominar la economía en el uso del cifrado. Era común entre los activistas revolucionarios de su época manejar volúmenes considerables de correspondencia, en tanto la presteza y variedad de las comunicaciones significativas representaba un factor crucial para sostener la lucha y, por tanto, ganar nuevos adeptos a su favor. Día tras día se redactaban y enviaban mensajes propios y se acusaba recibo de los ajenos. Como comenta Ricardo a Araujo en el extracto 4, todo esto "resulta un trabajo demasiado pesado. No pude traducir el pequeño párrafo que escribió usted en clave, porque se pierde lastimosamente el tiempo". Entonces le recomienda elaborar claves sencillas, con las que se pueda "escribir aprisa, una vez teniendo cierta práctica", además, no hacen falta cinco claves, "con una... nos basta". Y de paso le sugiere una estrategia técnica: "Ponga en la clave que invente la ll, la rr, la k y la w. Que no falte ninguna letra porque todas se usan. También la numeración de uno al 9, incluyendo el cero, conviene tener en clave. No la haga de signos difíciles de hacer, sino de signos sencillos". Se manifiesta, pues, el interés de Ricardo en convenirse sobre "claves" de tal factura, que su puesta en práctica no quite demasiado tiempo. Pero es, justamente, por aquella factura que se revela un defecto importante en sus nociones criptográficas. Su consejo de que la clave debería incluir la LL, la RR, la K y la W "porque todas se usan" parece implicar que tanto él como sus correligionarios escribían en inglés y en español, pero según declaraciones como la de Furlong, mencionada más arriba, no eran bilingües. Quizá la sugerencia cobra sentido cuando pensamos en que habría casos cuando sería recomendable cifrar incluso los términos en có-

digo, por ejemplo, "Fakir". Por otra parte, no está de más disponer de equivalentes en cifra para guarismos.

Lo más interesante, sin embargo, para identificar por su clase técnica y criticar a los criptosistemas típicamente utilizados por los magonistas viene implícito en la propuesta de disponer "signos sencillos" como elementos crípticos. En efecto, la práctica totalidad de los criptosistemas originales diseñados por magonistas son de sustitución simple monoalfabética, sustituyéndose cada letra del alfabeto de definición con un solo símbolo, muy al estilo de las tablas para cifrar que normalmente acompañaron a los venerables nomencladores durante su apogeo entre los siglos XVI y XIX. (Esta es una razón, supongo, de que en los copiadores de la correspondencia magonista no se reproduzcan los grupos encriptados, pues a veces no es fácil siquiera identificar todos sus trazos.) Muchos de ellos pueden revisarse en el Acervo Histórico Diplomático de la Secretaría de Relaciones Exteriores de México (AHDSREM). En la figura 1 tenemos un ejemplo típico, mecanografiado, sin fecha, en donde faltan equivalencias para la J, K y Z (siendo de notar como la Ñ se agregó manuscrita).

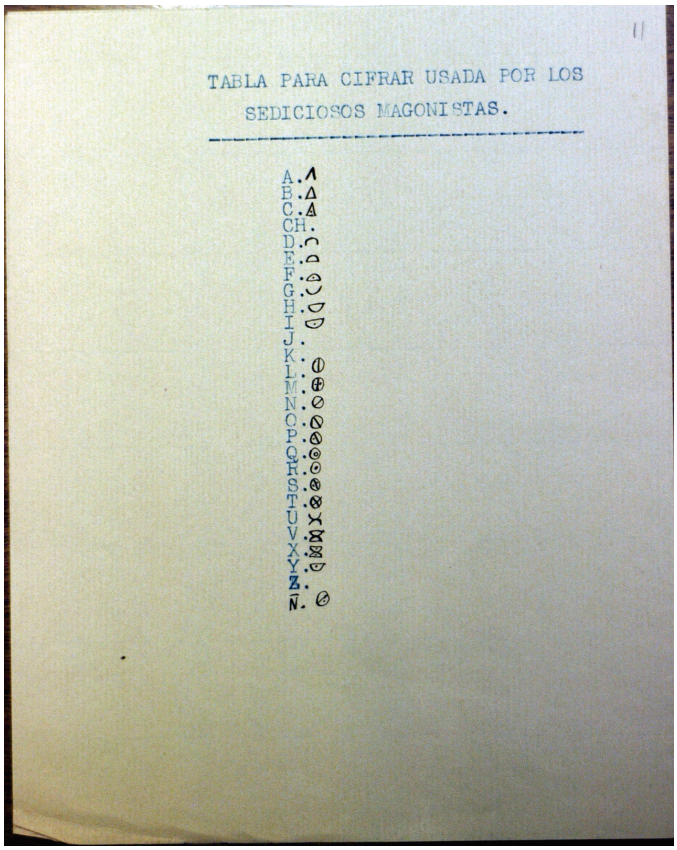


TABLA PARA CIFRAR USADA POR LOS
SEDICIOSOS MAGONISTAS.

Figura 1. *Una tabla para cifrar usada por los magonistas. Fuente: AHDSREM, exp. 11-4-198, f. 11.*

Veamos otras dos instancias para terminar. El 24 de marzo de 1908, cuando Enrique Flores Magón trataba de dar continuidad al proyecto de su hermano (entonces preso), un agente consular remitió desde Saint Louis un oficio a Ramón Corral, vicepresidente de México, notificándole que adjunta dos anexos: 1) carta de Enrique Flores Magón a Antonio de P. Araujo y 2) la clave que se menciona en dicha carta. Y el emisor añade: "La Agencia 'Furlong's Secret Service Co.' de esta ciudad, por unos cuantos días dejó de entregar á (*sic*) esta Oficina las cartas que intercepta, sin que hasta la fecha haya yo podido saber el modus operandi que usa para conseguirlas... Pero antier la referida Agencia, me entregó un paquete de más de cincuenta cartas, con la carta explicativa que original, con su respectiva traducción, tengo la honra de remitir á (*sic*) Usted".[12] En la figura 2 tenemos el "cliché fotográfico" —como se expresa en el documento de referencia— de la "clave" interceptada.

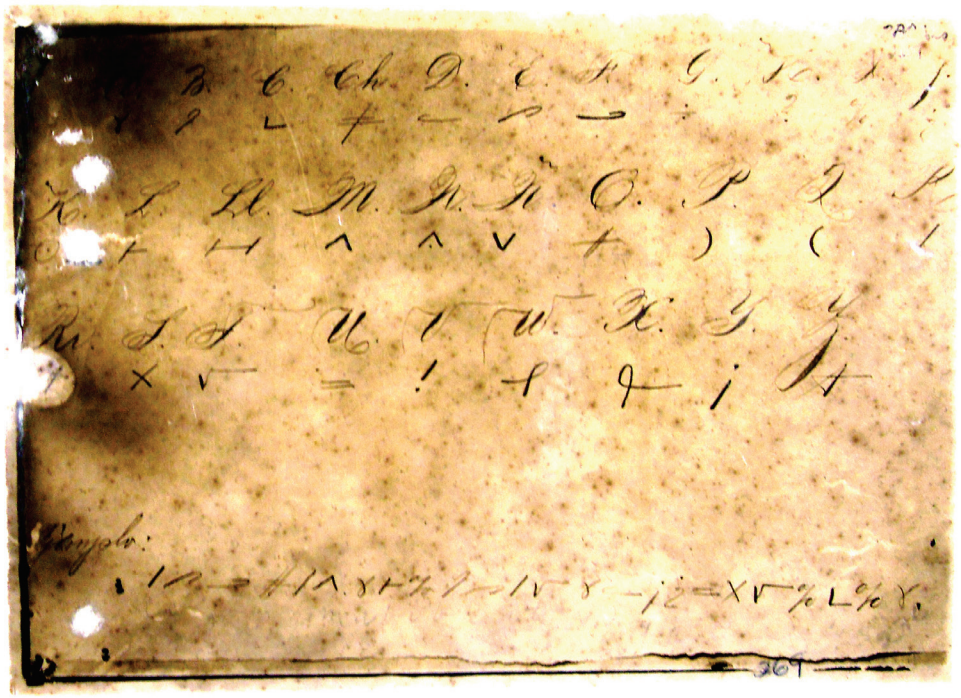


Figura 2. *Cliché fotográfico de una clave enviada por Enrique Flores Magón a Antonio de P. Araujo en 1908. Fuente: AHDSREM, L-E-954 II, f. 269.*

La adaptación mecanografiada, que consta en el mismo expediente, facilita la observación de los elementos del criptosistema.[13]

[12] AHDSREM, L-E-954 II, f. 267.
[13] AHDSREM, L-E-954 II, f. 270.

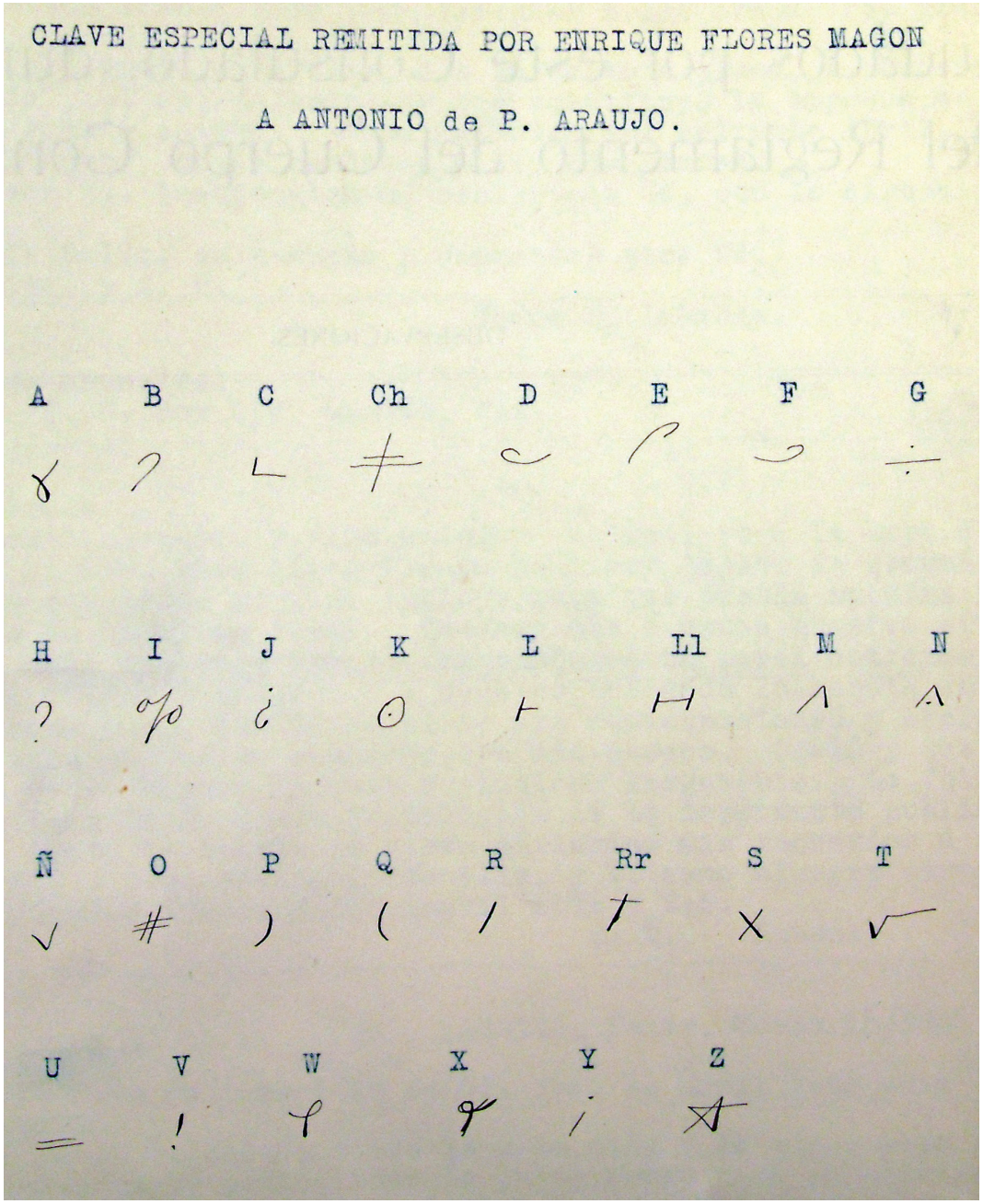


Figura 3. *Adaptación mecanografiada de la clave entre Enrique Flores Magón y Araujo, mostrada en la figura 2. Fuente: AHDSREM, L-E-954 II, f. 270.*

El 10 de abril de 1908 se envía al secretario de relaciones exteriores de México, también desde Saint Louis, un oficio cuyo adjunto es la "tabla alfabética de una clave" que Práxedis G. Guerrero, en Los Ángeles, trató de hacer llegar a To-

más Sarabia en San Antonio, Texas.[14] En la figura 4 se aprecia la referida "clave", donde se incluye un vocablo de 10 caracteres para cifrar en orden consecutivo a los numerales del 1 al 0.

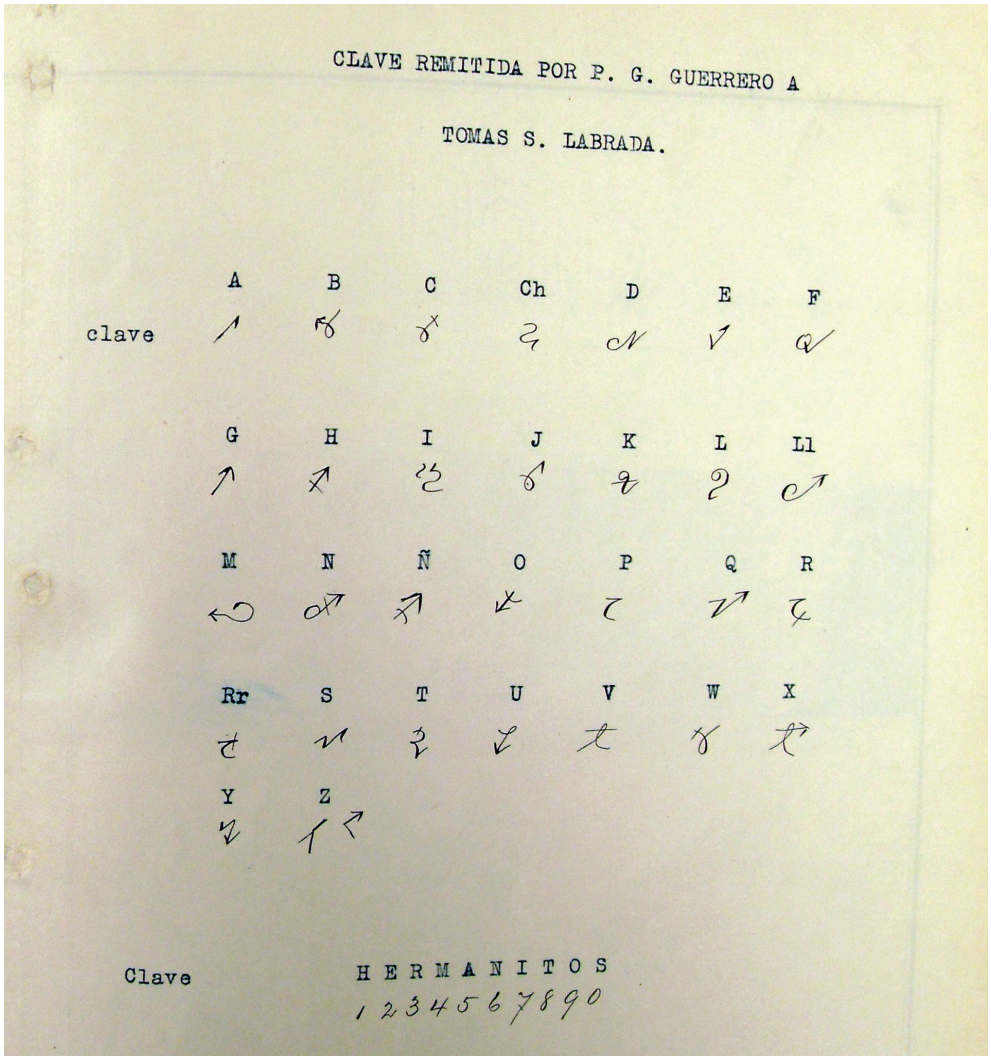


Figura 4. "*Tabla alfabética*" *de una clave que Práxedis G. Guerrero trató de hacer llegar a Tomás S. Labrada en 1908. Fuente: AHDSREM, L-E-954 II, f. 316.*

Podríamos robustecer la ilustración de estos métodos con más ejemplares de archivo que comparten las mismas o parecidas características técnicas, pero ni contamos con espacio ni es realmente necesario hacerlo. Los análisis precedentes nos mueven a concluir que la criptografía del movimiento magonista, entre 1907 y 1908, fue generalmente de sustitución monoalfabética de 1 a 1, lo bastante simple (y arcaica, en cuanto a sus raíces) como para ceder más temprano que tarde a su

[14] AHDSREM, L-E-954 II, f. 316.

identificación y ataque criptoanalítico por los agentes hostiles del gobierno mexicano.

2. EL CRIPTOSISTEMA DE CRISTÓBAL M. ARGUMEDO

Como saben los investigadores de los más diversos asuntos y periodos históricos, no es raro encontrar por lo menos una vez, en acervos documentales públicos o privados, materiales cuyos contenidos aparecen total o parcialmente cifrados o codificados. En ocasiones, las versiones descifradas o decodificadas correspondientes también van incluidas en los legajos, o bien el criptosistema que se utilizó en cada caso para efectuar las transformaciones criptográficas, por todo lo cual es factible imponerse con relativa presteza de los mensajes en lenguaje abierto, o texto plano, para decirlo en el argot técnico de la criptología. Sin embargo, también puede suceder que los expedientes revisados carezcan de las versiones traducidas o los auxiliares requeridos para descifrar o decodificar tal criptograma o código en un documento dado. Es en casos así cuando el estudioso se pregunta si en los catálogos o manuales de apoyo que suelen hallarse en los acervos hay algo de valor para resolver la dificultad. Considerando mi experiencia en los archivos de México, lo común es decepcionarse luego de realizar la consulta. Y de ordinario sucede lo mismo al solicitar el apoyo de los archivistas encargados. Lo regular es que un archivista sea por lo menos capaz de identificar las porciones crípticas en un legajo, asentando así en el catálogo o donde corresponda que tal escrito está "en clave", pero de ahí a puntualizar detalles de orden técnico o histórico sobre la clase de cifra o código en cuestión hay un largo trecho.

Nada de esto implica, sin embargo, que el investigador deba cruzar los brazos y resignarse a no enterarse jamás de los contenidos deliberadamente ocultados. En los propios documentos puede haber datos relevantes cuya observación y análisis permite formular las mejores hipótesis hacia la ruptura de una encriptación cualquiera (debiéndose reconocer que los códigos normalmente oponen una resistencia muy superior a las cifras). En otras palabras, cabe siempre mantener la esperanza y practicar el criptoanálisis con tesón si se desea suprimir la irritación que naturalmente genera una inesperada dificultad de índole criptográfica durante la investigación archivística (o bibliográfica, pues no faltan volúmenes con algunas o todas las páginas en cifra o código). Asumir tal actitud vale la pena en muchos casos, y para mostrarlo dedicaré el resto de esta sección y la siguiente a explicitar los procedimientos críticos, de observación y análisis que seguí para descriptar dos ejemplares de archivo parcialmente cifrados.

Los expedientes se resguardan en el archivo histórico del Centro de Estudios de Historia de México CARSO (CEHM-CARSO), situado en la capital mexicana. El primero está formado por varias cartas que fueron parcialmente cifradas con el mismo método. La primera que veremos aquí, mecanografiada, está fechada en 5 de octubre de 1921 y firmada con un criptograma, pero se atribuye a "Cristóbal M. Argumedo" por los motivos que trataremos de explicar.[15] No hay indicaciones de lugar. En la ficha catalográfica se apuntan, entre sus contenidos, los siguientes: "Acusa recibo de cartas y comenta lo dispendioso de las fiestas del centenario. Comunica que obtuvo fondos para la causa y del negocio que maneja y adquisición de maquinaria que Francisco Chávez hiciera. Solicita respuesta. Se incluyen claves no descifradas". Esta última expresión, "claves no descifradas", puede resultar equívoca desde un punto de vista criptoanalítico, pero si la interpretamos como "todas las partes escritas con pares de números son ilegibles", podemos admitirla como adecuada en sí misma y por lo que se refiere a este documento en particular.

Esta carta tiene dos fojas, bastará transcribir fragmentos para tomar nota de los datos relevantes hacia la conjetura sobre el tipo exacto de cifrado. En la redacción se omitieron sistemáticamente las tildes.

> Octubre 5 de 1921
>
> Señor 03-15-34-08,-37-05-34-23.
>
> Se [sigue un largo espacio en blanco, después prosigue:] Al tener el gusto de contestar sus cartas 6 y 23 del mes ppmo pdo, le hago saber que todas me han llegado aunque dilatadas; y refiriéndome a ellas en la contestación que me da en la del 6, sobre los párrafos 4/o y 8/o de mi fechada el 16 de Agosto, lamento que por ahora no le sea posible cumplimentar lo que en ella con tanta justicia pide y que me sería de grande utilidad. Por lo demás, tomo buena nota de su contenido en general, y cumpli su indicación preferente cerca del Sr. 08-05-36.-P.
>
> [...]
>
> No entraré en materia de información sin antes decir a Ud. algunas palabras sobre las ultimas y dispendiosas fiestas que en todo el pasado mes y con dinero del pueblo sostuvo la 04-12-15-37-34. reinante. Estas son, según frace (*sic*) de un escritor, la imagen de un grupo de demoledores sociales poniendo en juego todos los medios adecuados para acabar de embrutecer al pueblo y hundirlo en los abismos de la mas cinica abyección. Los groseros alardes jacarandosos de la turba de 34-06-18-34-13-15-05-01-17-34 ante las muchedumbres durante las verbenas trashumantes no tuvieron mas que la tendencia característica a aturdirse, a embotar sus pensamientos a degenerarse y embriagarse juntos con este nuestro pobre 13-18-01-35-08-12. tan falto de cultura y fácil a todas las sugestiones; unidos por desgracia a muy altas dignidades que acudieron por el canto de la sirena...
>
> Ya tuve el gusto de informarle en mi última de Septiembre 9 que logré fondos y con ellos poner a salvo al buen amigo 03-15-34-08-19-05-36-01-10-17-01-35-01-10-05-L7(*sic*)-01-23. Pues bien: como dicho Sr. se encuentra mucho muy enfermo, a consecuencia

[15] CEHM-CARSO, exp. DCXXI.3.244.1.

de las penalidades que pasó, no me fue posible hablar con él, pero lo hice con 36-34-16-17-18-08-12. su hijo que vino amí (*sic*) debidamente autorizado por su padre y esa conferencia la celebramos en lugar preparado para el efecto, y en presencia del Médico de la casa y otras personas de las mas caracterizadas en ese grupo.

[...]

El Sr 06-18-34-10-17-37-01-34-15-34-10-34. – y otros buenos amigos que lo saludan, están listos y prontos para el trabajo.

Y yo, con respetuoso afecto y como siempre, a su disposición.

37-12-10-. 09-34-17-01-12.-

Veamos ahora fragmentos de la segunda carta que me interesa examinar, también atribuida a Cristóbal M. Argumedo, mecanografiada y fechada 15 días después de la anterior.[16] Incluye, para fortuna del observador, varias marcas de lápiz entre algunas líneas, aparentemente intentos de decriptación o descifrado.

Oct 20/21

Sr. 03-15-34-08=37-05-34-23

Confirmo en todas sus partes mi anterior 5 del actual, y aunque de ella todavía no tengo respuesta, me apresuro a dirijirle (*sic*) esta para llamar su atención sobre el 13-01-08-05-03-15-10 que nos amenaza según verá por el recorte incluso, pues ya Ud. comprenderá que en todo esto va la mano de nuestro buen amigo 37-12-10=13-37-10-36-04-12 y 16-12-36-05-12-16. Todos los amigos en este ramo, esperan llenos de fé (sic), pero se muestran impacientes por lo tardío del negocio...

En esta primera mitad del párrafo inicial aparece cruzado con una diagonal cada elemento de la cadena 13-01-08-05-03-15-10, y debajo del 13 se lee "que", no más. Acaso la misma mano escribió debajo de la serie 37-12-10=13-37-10-36-04-12 lo siguiente: "w – de – la – que- w- u- v- a- de", y debajo de la cifra final, 16-12-36-05-12-16, puso "de – J- [blanco] – de – [blanco]".

En la foja complementaria se tienen cifras en el párrafo previo a la fórmula de despedida y la firma: "Ya por fin a dale y dale, obtuve el documento que a 37-12-10=09-05-03-18-01-08 pedí para la persona de 13-34-10-05-10-37-05-36-18-34-15-12- de quien le hablé en mi anterior, y el cual se le concedió con el 03-15-34-37-12 de 36-12-15-12-10-01-08". En este caso no hay intervenciones con lápiz entre líneas, pero después de la despedida "Lo saludo con respeto y cariñozo (*sic*) afecto, su siempre leal", la firma está cifrada: "34-15-03-18-09-01-37-12", y debajo se lee "C. M. Argumedo".

Ahora bien ¿cómo despejar estos enigmas? Los apuntes con lápiz son demasiado escasos y su morfología delata que su autor estaba totalmente inseguro de su procedimiento. Sin embargo, en la segunda misiva uno de ellos, "C. M. Argumedo", luce nítido debajo de la firma cifrada, por lo cual es creíble que su autor no

[16] CEHM-CARSO, exp. DCXXI.3.250.2.

dudara de quién había suscrito el texto. A primera vista sería de presumir que cada elemento de la frase C. M. Argumedo fue encriptado como 34-15-03-18-09-01-37-12, en tanto la extensión del texto plano se antoja igual a la del criptotexto. Pero coloquemos ahora en pares recíprocos a los caracteres hipotéticamente relacionados. Descubrimos que nuestro cálculo ha sido precipitado, pues dos elementos del texto plano, "do" al final de Argumedo, no alcanzan par. Esta constatación vuelve problemática la inferencia de que el cifrado haya sido específicamente de sustitución simple monoalfabética, numérica, de uno a uno. Pero no desechemos la posibilidad aún. La palabra "Argumedo" tiene una extensión de 8 elementos, exactamente la misma que el criptotexto bajo análisis. Si suponemos que el autor del cifrado original no vio razones para encriptar las iniciales C. M., ello autorizaría la conjetura de que "Argumedo" está ocultado por sustitución de uno a uno en la cadena 34-15-03-18-09-01-37-12.

A	r	g	u	m	e	d	o
34	15	03	18	09	01	37	12

El responsable del apunte posterior habría agregado C. M. por saber de cierto que los nombres del tal Argumedo eran Cristóbal y otro de inicial M., y juzgó suficiente inscribir esa constancia con las siglas. Ahora, si esto es así, entonces las equivalencias 34=a, 15=r, 18=g, 09=u, etc., que se fijan entre el criptotexto y el hipotético texto plano correspondiente, deberán conservarse en otras fracciones cifradas, presuponiendo que el mismo criptosistema se utilizó en toda instancia. Probemos con la primera cifra en la segunda carta, "Sr. 03-15-34-08=37-05-34-23". Después de sustituir tenemos "Sr. G-R-A-08=D-05-A-23". Cinco de 8 elementos admiten el descifrado con las partes conocidas de la posible "clave" que vamos formando, siendo de notar la doble aparición de la A (34) porque, tratándose de una vocal, su frecuencia relativa es elevada, y si podemos confiar que en este grupo experimental la equivalencia 34=A podría mantenerse es porque el 34 recurre señaladamente en ambas cartas. Sin embargo, no parece fácil descubrir cuáles son las letras que se disimulan bajo 08, 05 y 23. Si 08 está por L, entonces quedaría "GRAL" antes del signo = en la fracción de prueba. Se trataría entonces de la abreviatura del término "General". ¿Por qué no? Nada impide que la braquigrafía sea transformada criptográficamente, además, abreviar "General" como "Gral" en documentos de diversas clases es una costumbre extendida en inglés y otros idiomas, no sólo en español.

Admitamos provisionalmente que 08 equivale a L. Si esto ha de ser así por definiciones del criptosistema utilizado, entonces el fragmento "sobre el 13-01-

08-05-03-15-10 que nos amenaza" del párrafo inicial en la segunda carta se descifrará parcialmente "sobre el 13-E-L-05-G-R-O que nos amenaza". En este caso particular, la consideración de las palabras antecedentes y posteriores en texto plano sugiere de inmediato la plausibilidad hipotética de que el criptotexto deba traducirse completamente como PELIGRO, obteniendo de tal modo la decriptación de nuevas correspondencias crípticas: 13=P, 05=I. Pero, una vez más, para encontrar elementos que fomenten la verdad en la conclusión de que el criptosistema es de uno a uno, monalfabético, esas nuevas equivalencias deben repetirse en otros conjuntos encriptados. Tomemos como instancia de prueba el fragmento "este nuestro pobre 13-18-01-35-08-12. tan falto de cultura y fácil a todas las sugestiones" de la primera carta. Con lo que ya hemos descubierto hasta el momento, partiendo del análisis de tan sólo 8 caracteres numéricos, sustituimos los numerales y resulta "este nuestro pobre PUEBLO. tan falto de cultura", etc. El vocablo exhumado se reconoce sin falta y su inserción es consistente gramatical, sintáctica y semánticamente con el resto de la oración.

Volvamos al grupo a medias decriptado "Sr. G-R-A-L=D-05-A-23". Si la regla de trasformación general es que 05 valga por L, tenemos "Sr. G-R-A-L=D-I-A-23". Ahora, considerando que ambas cartas están fechadas en 1921 y provienen del "Fondo Félix Díaz" del CEHM-CARSO, podemos apostar a que 23 equivale a la Z y decriptar finalmente "GRAL DIAZ", por tanto, la inferencia será que Argumedo se dirigió al general Félix Díaz Prieto (1868-1945), nieto de Porfirio Díaz y tenaz contrarrevolucionario, enemigo mortal de los gobiernos de Francisco I. Madero, Victoriano Huerta y Venustiano Carranza; encabezó un movimiento militar y político importante entre 1917 y 1920, conocido históricamente como "Felicismo", que nunca logró el éxito anhelado: poner a su líder en la silla presidencial. Al parecer, pues, Cristóbal de Argumedo era un "felicista" que trataba de mantenerse útil a la causa de su líder enviándole despachos informativos regularmente.

Procediendo en el mismo estilo que pautan los hallazgos conseguidos en otros fragmentos encriptados, gradualmente restituimos los componentes del criptosistema hasta donde nos lo permite la cantidad de criptotexto disponible, pero que lógicamente basta para decriptar los textos bajo análisis en su totalidad. El tercer extracto de la carta número uno se leerá ya sin tropiezos, pues, como sigue (partes decriptadas en cursiva):

> Ya tuve el gusto de informarle en mi última de Septiembre 9 que logré fondos y con ellos poner a salvo al buen amigo *General Vicente Benit-L7(sic)-ez*. Pues bien: como dicho Sr. se encuentra mucho muy enfermo, a consecuencia de las penalidades que pasó, no me fue posible hablar con él, pero lo hice con *Castulo*. su hijo que vino amí (sic) debidamente

> autorizado por su padre y esa conferencia la celebramos en lugar preparado para el efecto, y en presencia del Médico de la casa y otras personas de las mas caracterizadas en ese grupo.

Y la línea final, la despedida y la firma rezan en texto plano:

> El Sr *Juan T. de Arana*. – y otros buenos amigos que lo saludan, están listos y prontos para el trabajo.
> Y yo, con respetuoso afecto y como siempre, a su disposición.
> *Don Mateo*.-

Sólo después de esto llegamos a descubrir que esta primera misiva no fue firmada "Argumedo" sino "Don Mateo", por donde aprendemos que las iniciales C. M. al cabo de la segunda carta son de "Cristóbal Mateo".

Y el párrafo inicial de la segunda carta se lee ya sin obstáculos así:

> Confirmo en todas sus partes mi anterior 5 del actual, y aunque de ella todavía no tengo respuesta, me apresuro a dirijirle (*sic*) esta para llamar su atención sobre el *peligro* que nos amenaza según verá por el recorte incluso, pues ya Ud. comprenderá que en todo esto va la mano de nuestro buen amigo *Don Pdncho* (*sic* por "Pancho", cifró con 37 en lugar de 34) y *socios*. Todos los amigos en este ramo, esperan llenos de fé (sic), pero se muestran impacientes por lo tardío del negocio...

Ahora es posible reconstruir, en su virtual totalidad, la tabla de sustituciones que muy probablemente usó Argumedo en esta correspondencia. Se observa una progresión correlativa entre los números y las letras del alfabeto definitorio (de extensión 27, cuando menos) en su orden regular, condición que faculta para deducir el valor críptico y lugar de los sustitutos no utilizados en la muestra. No sería extraño que también se hubieran agregado de origen caracteres para ocultar números, sílabas, nulos y hasta nombres propios (que se situarían en los lugares 23 a 33).

A	B	C	D	E	F	G	H	I	J	K	L	M	N
34	35	36	37	01	02	03	04	05	06	07	08	09	10
Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
11	12	13	14	15	16	17	18	19	20	21	22	23	

El lector puede guiarse por esta tabla para traducir y leer sin interrupciones las dos cartas tratadas y otras de este autor, accediendo a las versiones completas en el sitio web del CEHM-CARSO.[17] Como se ha mostrado, un poco de pacien-

[17] CEHM-CARSO, sitio web http://www.cehm.com.mx/ES/archivo/Paginas/archivo_cehm.aspx. Buscar por "Argumedo".

cia, atención, imaginación y perseverancia experimental bastan para no intimidarnos o hacernos desesperar fácilmente ante advertencias como la de "incluye claves no descifradas" en acervos públicos o privados.

3. EL MODERNO MÉTODO CRIPTOGRÁFICO EN UNA CARTA DE J. W. WELLINGTON

Veamos ahora el caso de una carta parcialmente cifrada, mecanografiada, firmada por J. W. Wellington, dirigida a "Señor don José González, N. O. (New Orleans)" y sin fecha, pero probablemente escrita en los albores de la década de 1920 y relacionada con el movimiento felicista, considerando la sinopsis en el catálogo: "Indica que los factores de la movilización de [Francisco] Murguía unido a Cándido Aguilar, el reconocimiento de [Juan] Carrasco, [Domingo] Arrieta y [Carlos] Green a Murguía como jefe supremo del movimiento y la tentativa de [Manuel] Peláez desembarcar en Veracruz, con considerable contingente, sugiere aprovechar el momento del desprestigio del obregonismo a fin de unificar al felicismo y convertirse él, en el salvador de México. Incluye claves no descifradas...".

La carta empieza así:

> Muy estimado señor y fino amigo:
> Me permito dirigirle la presente, no sólo para reiterarle mi anterior en atención a que han prevalecido las razones que la motivaron, sino para agregar nuevos hechos importantes que debe usted conocer, emitiéndole igualmente algunas ideas que hemos delineado de acuerdo el ñLFVVDUFCHTFDMDPUH y yo, persona de que le he hablado ampliamente en mi anterior y le hablará también el señor HPURñD.

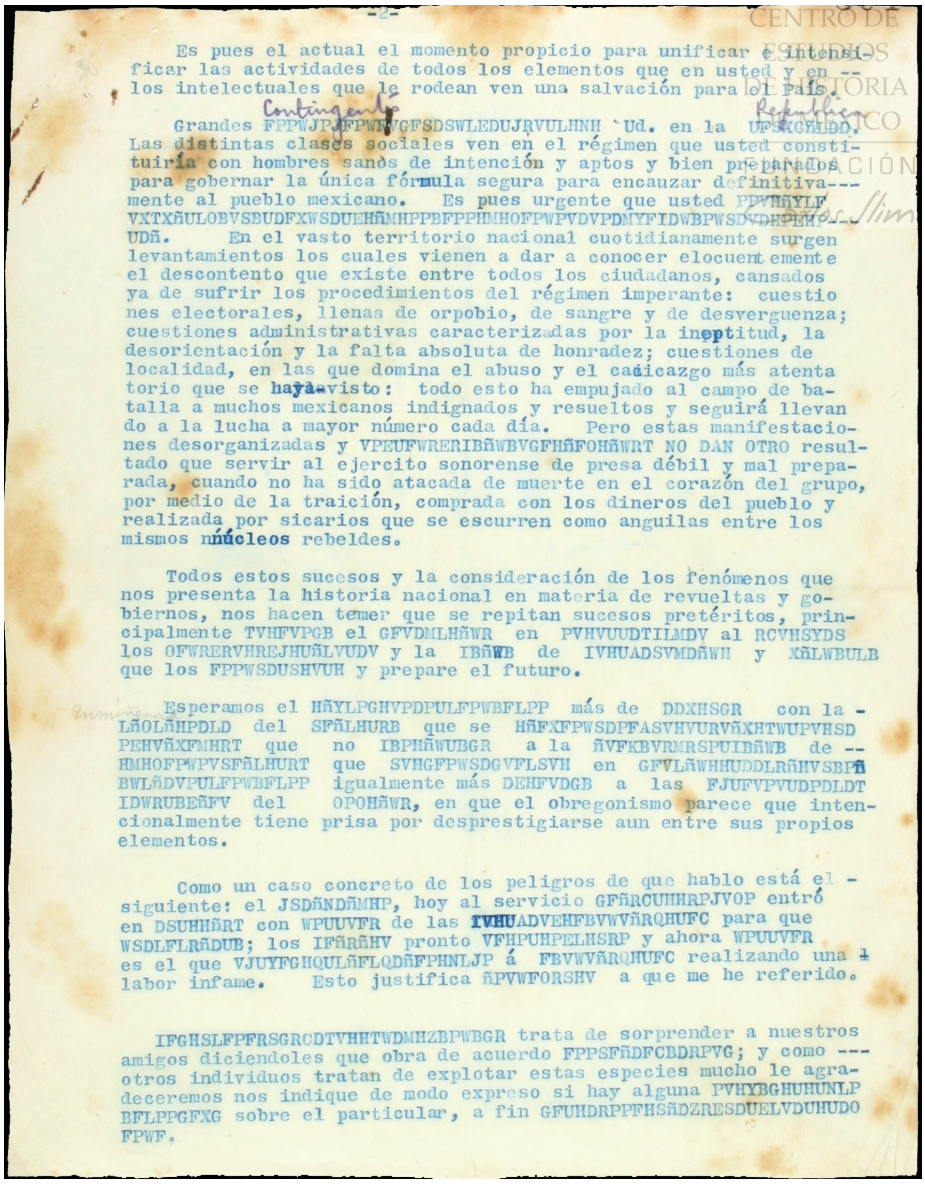
Ocupa tres fojas y se divide en 12 párrafos, de los cuales sólo dos no incluyen cifras, mismas que difieren de las de Argumedo, ante todo, por emplear letras en lugar de guarismos como elementos crípticos. Pero la diferencia entre ambos criptosistemas es más amplia, como veremos.

El según párrafo de la segunda foja inicia como sigue:

> Grandes FPPWJPJFPWFVGFSDSWLEDDUJRVULHNH Ud. en la UFSXCñLDD. Las distintas clases sociales ven en el régimen que usted constituiría con hombres sanos de intención y aptos y bien preparados para gobernar la única fórmula segura para encauzar definitivamente al pueblo mexicano. Es pues urgente que usted PPVHÑYLFVXTXÑULOBVSBUDFXWSDUEHÑMHPPBFPPHMHOFPWPVDVPDMFIDWBPWSDVDHPEHPUDñ. En el vasto territorio nacional cuotidianamente surgen levantamientos los cuales vienen a dar a conocer elocuentemente el descontento que existe entre todos los ciudadanos [...] Pero estas manifestaciones desorganizadas y VPEUFWRERIBÑWBVGFHÑFOHÑWRT NO DAN OTRO (sic) resultado que servir al ejército sonorense de presa débil y mal preparada, cuando no ha sido atacada de muerte en el corazón

del grupo, por medio de la traición, comprada con los dineros del pueblo y realizada por sicarios que se escurren como anguilas entre los mismos núcleos rebeldes.

En la primera línea se aprecian dos palabras garabateadas con tinta por encima de otros tantos criptogramas, como permite distinguirlo la figura 5.



Es pues el actual el momento propicio para unificar e intensificar las actividades de todos los elementos que en usted y en los intelectuales que le rodean ven una salvación para el País.

Grandes FPPWJPJFPWFVGFSDSWLEDUJRVULHNH Ud. en la UFSXCñLDD. Las distintas clases sociales ven en el régimen que usted constituiría con hombres sanos de intención y aptos y bien preparados para gobernar la única fórmula segura para encauzar definitivamente al pueblo mexicano. Es pues urgente que usted PPWHñYLF VXTXñULOBVSBUDFXWSDUEHñMHPPBFPPHMHOFPWPVDVPDMYFIDWBPWSDVDHPEMP UDñ. En el vasto territorio nacional cuotidianamente surgen levantamientos los cuales vienen a dar a conocer elocuentemente el descontento que existe entre todos los ciudadanos, cansados ya de sufrir los procedimientos del régimen imperante: cuestiones electorales, llenas de orpobio, de sangre y de desverguenza; cuestiones administrativas caracterizadas por la ineptitud, la desorientación y la falta absoluta de honradez; cuestiones de localidad, en las que domina el abuso y el caciqazgo más atentatorio que se haya visto: todo esto ha empujado al campo de batalla a muchos mexicanos indignados y resueltos y seguirá llevando a la lucha a mayor número cada día. Pero estas manifestaciones desorganizadas y VPEUFWRERIBñWBVGFHñFOHñWRT NO DAN OTRO resultado que servir al ejercito sonorense de presa débil y mal preparada, cuando no ha sido atacada de muerte en el corazón del grupo, por medio de la traición, comprada con los dineros del pueblo y realizada por sicarios que se escurren como anguilas entre los mismos núcleos rebeldes.

Todos estos sucesos y la consideración de los fenómenos que nos presenta la historia nacional en materia de revueltas y gobiernos, nos hacen temer que se repitan sucesos pretéritos, principalmente TVHFVPGB el GFVDMLHñWR en PVHVUUDTILMDV al RCVHSYDS los OFWRERVHREJHUñLVUDV y la IBñWB de IVHUADSVMDñWH y XñLWBULB que los FPPWSDUSHVUH y prepare el futuro.

Esperamos el HñYLPGHVPDPULFPWBFLPP más de DDXHSGR con la LñOLñHPDLD del SFñLHURB que se HñFXFPWSDPFASVHVURVñXHTWUPVHSD PEHVñXFMHRT que no IBPHñWUBGR a la ñVFKBVRMRSPUIDñWB de HMHOFPWPVSFñLHURT que SVHGFPWSDGVFLSVH en GFVLñWHHUDDLRñHVSBPñ BWLñDVPULFPWBFLPP igualmente más DEHFVDGB a las FJUFVPVUDPDLDT IDWRUBEñFV del OPOHñWR, en que el obregonismo parece que intencionalmente tiene prisa por desprestigiarse aun entre sus propios elementos.

Como un caso concreto de los peligros de que hablo está el siguiente: el JSDñNDñMHP, hoy al servicio GFñRCUHHRPJVOP entró en DSUHHñRT con WPUUVFR de las IVHUADVEHFBVWVñRQHUFC para que WSDLFLRñDUB; los IFñRñHV pronto VFHPUHPELHSRP y ahora WPUUVFR es el que VJUYFGHQULñFLQDñFPHNLJP á FBVWVñRQHUFC realizando una labor infame. Esto justifica ñPVWFORSHV a que me he referido.

IFGHSLFPFRSGRCDTVHHTWDMHZBPWBGR trata de sorprender a nuestros amigos diciendoles que obra de acuerdo FPPSFñDFCBDRPVG; y como otros individuos tratan de explotar estas especies mucho le agradeceremos nos indique de modo expreso si hay alguna PVHYBGHUHUNLP BFLPPGFXG sobre el particular, a fin GFUHDRPPFHSñDZRESDUELVDUHUDO FPWF.

Figura 5. *Segunda foja de la carta de J. W. Wellington a José González. Fuente: CEHM-CARSO, exp. DCXL.6.588.1.02.*

Por encima de FPPWJPJFPWFVGFSDSWLEDDUJRVULHNH se lee “Contingentes”, mientras que UFSXCñLDD está coronado por la palabra “Republica”. Es el único lugar del documento donde hallamos tales aparentes intentos

de descifrado o decriptación. Para iniciar el análisis, conviene atender al hecho de que "Republica" y UFSXCñLDD tienen idéntica longitud, 9 caracteres. Esto sugiere que el criptosistema utilizado pudo basarse en múltiples alfabetos y operar conforme a una clave literal o numérica, o bien, que a cada letra de un único alfabeto de definición se le asignó un solo equivalente fijo, como (hipotéticamente) sucedió en el caso Argumedo. Para guiar nuestras inferencias a este respecto, conviene iniciar graficando la correspondencia entre los caracteres del criptotexto y los del texto plano.

R e p u b l i c a
U F S X C ñ L D D

Dado que la c y la a comparten a la D como letra sustituta, parece que la opción del modelo de Argumedo debe descartarse. Pero, si se usó una clave para regir las transformaciones a partir de varios alfabetos, o incluso de uno solo, entonces deberíamos identificar algún patrón que lo delate. Una inspección concentrada nos permite detectar que los elementos 2º, 5º y 8º del texto plano, o sea E, B y C, fueron cifrados cada uno con la letra que le sigue en el alfabeto de la lengua regularmente ordenado, esto es, E por F, B por C, y C por D. Según esto, la operación consistió en elegir el carácter críptico desplazando un espacio hacia la derecha cada letra a ocultar.

Texto plano	R	e	p	u	b	l	i	c	a
Criptotexto	U	F	S	X	C	ñ	L	D	D
Desplazamiento		+1			+1			+1	

También observamos que entre la E, la B y la C hay dos letras cuya criptografía sin duda no se realizó sumando 1. Mas esto no implica que el *principio de sustitución* por desplazamiento a la derecha tantos lugares haya dejado de intervenir. Para probar si tal no ha sido el fenómeno, basta con hacer el conteo correspondiente hacia la derecha partiendo de las letras restantes en el texto plano, R, P, U, L, I, A. De inmediato se advierte que cada una se sustituye por la que resulta después de sumar 3.

Texto plano	R	e	p	u	b	l	i	c	a
Criptotexto	U	F	S	X	C	ñ	L	D	D
Desplazamiento	+3	+1	+3	+3	+1	+3	+3	+1	+3

Considerando la porción de criptotexto y texto plano que estamos analizando, al parecer 313 se aplicó como clave en ciclos fijos, invariables, al estilo del modelo clasificado como de Gronsfeld (o "clave del nihilista") o de Hirsh —según lo han llamado también algunos tratadistas—, que puede describirse como un agregado calculado de cifras de Julio César en combinación con una reducción drástica del número de alfabetos en la matriz característica del modelo generalmente atribuido a Blaise de Vigenère. [18] Técnicamente se concebiría, pues, como una mezcla de cifrado monoalfabético y polialfabético.

Podrá objetarse que semejante verificación difícilmente se repetirá en el caso de "Contingentes", agregado encima del primer grupo críptico bajo examen, FPPWJPJFPWFVGFSDSWLEDDUJRVULHNH, por la disparidad manifiesta entre las extensiones respectivas. Supongamos, pues, que para cifrar "Contingentes" se usó un método basado en asignar hasta dos pares de letras como sustitutos por cada elemento del texto plano; así, C se cifraría por FP, O por PW, N por JP, etc. Se trataría, entonces, de un criptosistema de tipo tomográfico que representa una variación del clásico modelo de Polibio y fue, por cierto, muy utilizado en México por varias fuerzas beligerantes —destacando los maderistas y los carrancistas— durante la revolución, especialmente entre 1907 y 1920,[19] aunque también se tienen ejemplares de años muy próximos a 1930. Sin embargo, milita contra esta posibilidad el hecho de que "Contingentes" tiene una longitud de 12, siendo de 31 la de FPPWJPJFPWFVGFSDSWLEDDUJRVULHNH. Si ésta última fuera de 24, entonces cabría suponer —abstrayendo la posibilidad de iteraciones involuntarias u otros errores cometidos durante la encriptación— que cada unidad de texto plano fue velada con dos unidades elegidas por la combinación entre los elementos de una palabra clave y los del alfabeto de cifrado establecido.

Al ensayar con este procedimiento alternativo, como vimos, nada se logra excepto generar dificultades innecesarias. De hecho, "Contingentes" fue cifrado con la misma clave que "Republica". Sucede que el primer término es tan sólo el descifrado de una parte del criptotexto correspondiente, el cual no esconde una sino hasta seis palabras, dándose la circunstancia de que el criptógrafo eliminó los espacios entre las mismas, táctica muy aconsejable para operar con criptosistemas

[18] D. SALOMON, *Data Privacy and Security*, New York, 2003, p. 75. J. C. GALENDE DÍAZ, *Criptografía: historia de la escritura cifrada*, Madrid, 1995, p. 41. H. GAINES, *Cryptanalysis. A Study of Ciphers and Their Solution*, New York, 1956, p. 117.

[19] R. NARVÁEZ, "Nota técnica sobre la criptografía de Francisco I. Madero en 1910", en su edición del *Epistolario* de F. I. Madero, tomo II, México, 2012, pp. lxviii-lxxii.

de todas clases. Para probar que la "clave" 313 fue aplicada sistemáticamente, veamos el siguiente gráfico.

Texto plano	C	o	n	t	i	n	g	e	n	t	e	s
Clave	+3	+1	+3	+3	+1	+3	+3	+1	+3	+3	+1	+3
Criptotexto	F	P	P	W	J	P	J	F	P	W	F	V

Si tal regla de transformación criptográfica devolvió semejantes correspondencias, entonces Wellington debió utilizar un alfabeto de definición formado por los siguientes 27 elementos:

A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z

Tras aclarar, conforme al método de descifrado inferido, los fragmentos crípticos, el mismo párrafo de la segunda foja en el material que venimos analizando se lee:

> Grandes CONTINGENTES DE PARTIDA A RIOS TIEME (*sic*) USTED[20] Ud. en la REPUBLICA. Las distintas clases sociales ven en el régimen que usted constituiría con hombres sanos de intención y aptos y bien preparados para gobernar la única fórmula segura para encauzar definitivamente al pueblo mexicano. Es pues urgente que usted NOS ENVIE SUS ULTIMAS PARA EUTRAR (*sic*) DE LLENO Y CON ELEMENTOS A UNA LVCHA (*sic*) TAN TRASCENDENTAL. En el vasto territorio nacional cuotidianamente surgen levantamientos los cuales vienen a dar a conocer elocuentemente el descontento que existe entre todos los ciudadanos [...] Pero estas manifestaciones desorganizadas y SOBRE TODO FALTAS DE ELEMENTOS NO DAN OTRO resultado que servir al ejército sonorense de presa débil y mal preparada, cuando no ha sido atacada de muerte en el corazón del grupo, por medio de la traición, comprada con los dineros del pueblo y realizada por sicarios que se escurren como anguilas entre los mismos núcleos rebeldes.

Asimismo se traducen con 313 las dos cifras del párrafo transcrito al comenzar esta sección (LKC —por LIC, error evidente— JUAREZ ESCALANTE y EORONA, en realidad *Corona*; de nuevo se cometió error al encriptar la primera letra) y todas las restantes, como podrá comprobarlo quien trabaje sobre el documento íntegro.[21]

[20] En el carácter número 23 de esta cadena, una U (la primera de dos), el criptógrafo equivocó la secuencia de aplicación de la clave; cifró con 3 cuando tocaba 1, y quien lo ignora descifra un galimatías. Es, por tanto, necesario ensayar hasta darse cuenta de que se debe continuar con 3 en el punto indicado.

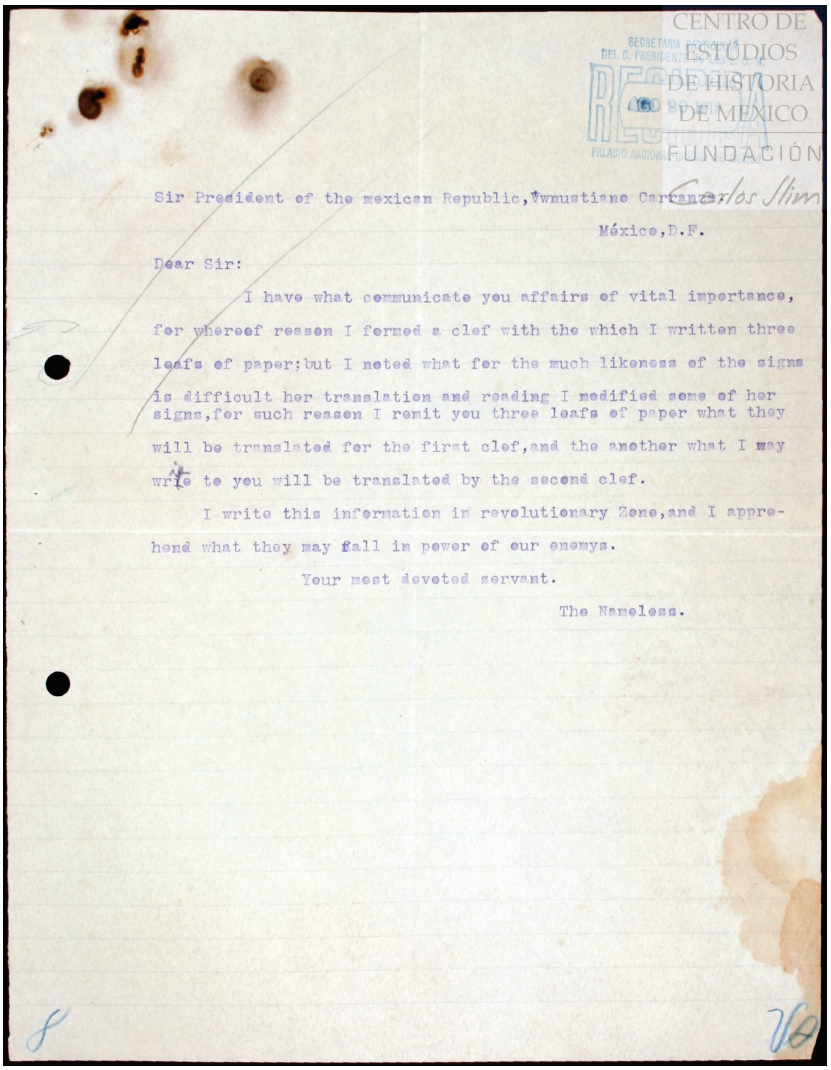
[21] Al cual se puede acceder en el sitio web http://www.cehm.com.mx/ES/archivo/Paginas/archivo_cehm.aspx. Buscar por "Wellington".

Después de este ejercicio analítico nos persuadimos de que la advertencia en la ficha catalográfica, "incluye claves no descifradas", es tanto inexacta como precipitada, pues, en primer lugar, debería hablar de "cifras no traducidas" o algo por el estilo, mas no de claves, y en segundo lugar porque la clave del criptosistema (hablando con propiedad técnica) sí se incluye, sólo es cuestión de recuperarla con un poco de atención, un bien seleccionado criterio comparativo y diligencia, aprovechando información contenida en el mismo legajo. Por supuesto, la faena se acelera si se poseen conocimientos de historia criptológica general.

4. LAS CURIOSAS "CLAVES" DE "THE NAMELESS"

Como mencioné al iniciar el apartado 2 *supra*, ciertos archivos públicos y privados resguardan documentos donde se explicitan las reglas y exhiben los auxiliares gráficos, ejemplos y otros anexos de criptosistemas a utilizar en una correspondencia reservada. He localizado más de diez en el acervo del CEHM-CARSO, los cuales mantienen identidades o analogías técnicas con los modelos que con mayor frecuencia se usaron durante la época manual de la criptografía y son, por tanto, legítimamente ubicables bajo alguna de las clases generales bien asentadas en criptología, siendo por lo común irrelevante el que hayan sido o no redactados con una máquina de escribir. La factura y el aparente modo de aplicación de uno de ellos me han parecido a tal punto estrambóticos y fuera de serie, que decidí describirlos y criticarlos brevemente para rematar este artículo.

Se trata de dos fojas en el expediente XXI.139.16091.1. La primera es una carta en inglés, mecanografiada, sin fecha ni lugar de remisión, dirigida al "Señor presidente de la república mexicana, Venustiano Carranza", y firmada con el seudónimo "The Nameless", que los catalogadores tradujeron como "El Innominado". Si el receptor era Carranza, el afamado "Primer Jefe del Ejército Constitucionalista", la fecha no puede ser posterior a 1920. El par de rayas con lápiz que cruzan la esquina superior izquierda de la primera foja sugiere que el documento fue recibido, leído y archivado. Ahora bien, este Innominado corresponsal, como lo percibirá de inmediato quien recorra superficialmente el texto en la figura 6, estaba muy mal versado en las normas de composición del idioma inglés.



Sir President of the mexican Republic, Venustiano Carranza. Carlos Slim

México, D.F.

Dear Sir:

I have what communicate you affairs of vital importance, for whereof reason I formed a clef with the which I written three leafs of paper; but I noted what for the much likeness of the signs is difficult her translation and reading I modified some of her signs, for such reason I remit you three leafs of paper what they will be translated for the first clef, and the another what I may write to you will be translated by the second clef.

I write this information in revolutionary Zone, and I apprehend what they may fall in power of our enemys.

Your most devoted servant.

The Nameless.

Figura 6. *Carta de* "*The Nameless*" *a Venustiano Carranza (c. 1920). Fuente: CEHM-CARSO, exp. XXI.139.16091.01.*

Se suceden con insistencia los tropiezos gramaticales, ortográficos y semánticos, empezando con lo de que "for whereof reason I formed a clef with the which I written three leafs of paper..." y terminando con "I write this information in revolutionary zone, and I apprehend what they may fall in power of our enemys". Ahora, el uso repetido de la voz francesa *clef*, clave, en lugar de *key* o *cipher*, que se usaban genéricamente en inglés para referirse a claves en el sentido (actual) de criptosistemas, nos hace pensar que nuestro anónimo espía —su función debía ser tal, como parece insinuarlo— era francés, belga o suizo, en todo caso un individuo francófono procedente de un país europeo o una colonia de Francia, antes que un hablante nativo del inglés, no digamos del español. Por qué

"The Nameless" trataba de favorecer los intereses del Primer Jefe arriesgando su libertad o su vida "en zona revolucionaria", es una interrogante que no nos interesa elucidar aquí. A pesar de las inconsistencias y fallas lingüísticas en su nota, es posible asir el sentido básico de fondo: informa que tiene asuntos de "vital importancia" para comunicar y ha escrito tres páginas con una primera clave; le envía esta clave y otra más, con la cual cifrará un mensaje posterior. Sin duda, persisten las dificultades de interpretación en cuanto a las advertencias o anuncios referentes a la primera "clef", lo importante es que en la segunda foja encontramos los dos criptosistemas en cuestión (figura 7).

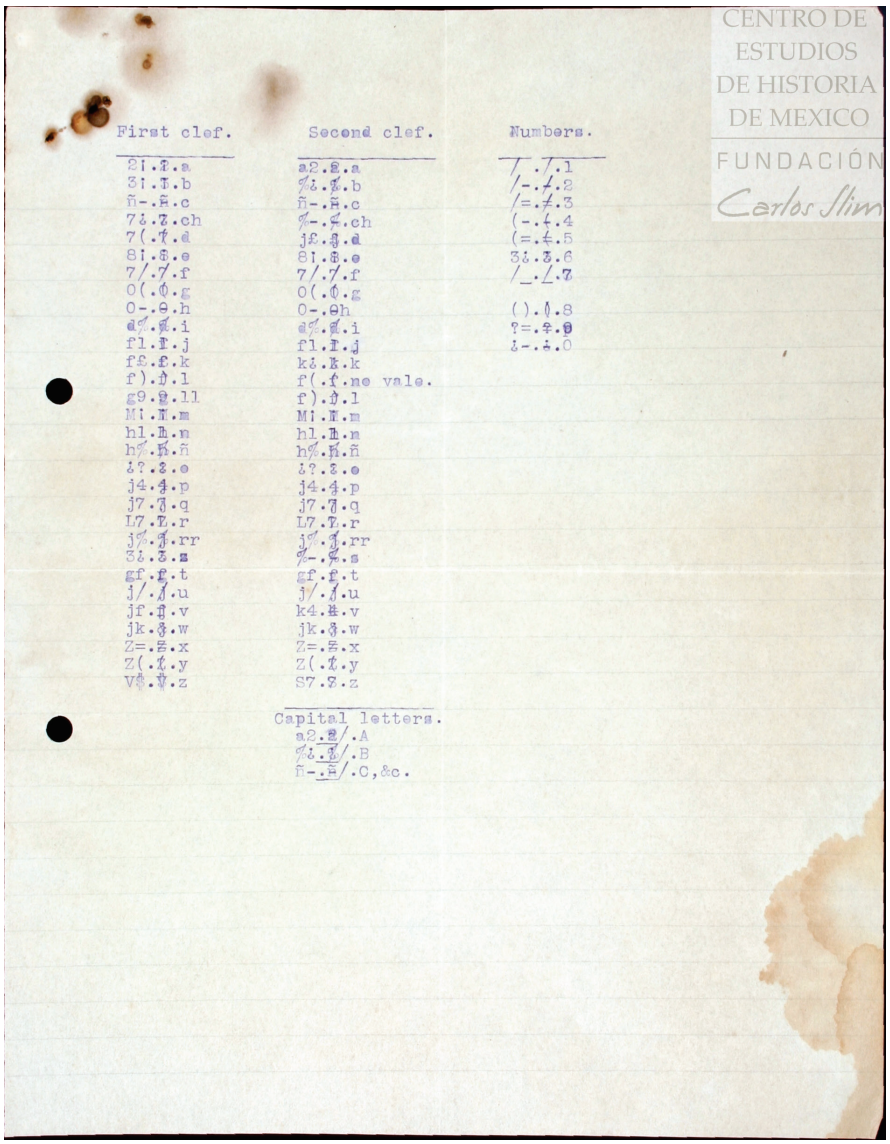


Figura 7. *Las "claves" de "The Nameless" para su comunicación secreta con Carranza. Fuente: CEHM-CARSO, exp. XXI.139.16091.02.*

Ambos son de sustitución simple monoalfabética. El primero se basa en un alfabeto definitorio de 30 caracteres (por inclusión de la CH, la LL y la RR) y el segundo en uno de 29. Sólo en esta última se inserta un elemento de valor nulo, tomando el sitio de la LL, y se distingue un equivalente críptico compartido, %- para CH y S. También se proporciona una serie, al parecer común, de equivalentes para las letras mayúsculas A, B, C y el signo &c, y para los números del 1 al 0 (un ordenamiento más apropiado habría sido del 0 al 9). El hecho de agregar letras como la CH y la RR hace pensar que planeaba cifrar mensajes tanto en inglés como en español, pero ya comentamos nuestras razones para no concederle un manejo respetable de este idioma; probablemente podía leerlo tolerablemente bien, por tanto confiaba en entender notas emitidas ocasionalmente en castellano. Como método de encriptación general se prescribe que la sustitución, tanto para letras como para números, se realice por la superposición de una letra o guarismo y una grafía o signo auxiliar (puntuación, exclamación, etc.) o símbolo con alguna función gráfica específica (matemática, de identificación monetaria, etc.). Es muy difícil encontrar un algoritmo parecido —sin importar que se usara o no la máquina de escribir— en los anales criptográficos, por lo menos hasta donde yo he podido recorrerlos.

Sin embargo, no descartemos que la idea fuera registrar dos opciones a escoger: (1) cifrar con un par de caracteres, por ejemplo, la A con 2¡ en la primera *clef* y con a2 en la segunda, o (2) cifrar encimando esos dos caracteres. Si es así, (1) se antoja más propicio para economizar en tiempo (haciendo eco de la exigencia suprema de Ricardo Flores Magón, véase la sección 1 *supra*), siempre que se conviniese además la supresión de los blancos entre las palabras y no su sustitución con guiones, puntos u otra marca, pues con (2) el trabajo se retrasa inevitablemente por la necesidad de retroceder el carro de la máquina cada vez para teclear el dúo de caracteres formadores de cada cifra. También sería preciso comprobar siempre que la cinta entintada se mantenga húmeda y sin rasgaduras, so pena de imprimir tenuemente o con fracturas los signos hibridados (por así decir), lo cual dificultaría el proceso de lectura y, por supuesto, descifrado, aun teniendo la *clef* a la vista.

Dejando de lado la excentricidad en el diseño de este criptosistema, lo cierto es que la decriptación de un criptotexto creado por su medio se puede lograr, en circunstancias normales, por el recurso al mero análisis de frecuencias relativas. ¿Por qué nuestro hipotético espía no asignó más de un equivalente a las vocales y las consonantes de aparición más frecuente en español y, para el caso, en inglés? Acaso dio por sentado que sus criptogramas lucirían como una densa y oscura

empalizada, lo bastante ríspida para desanimar de golpe a quien la contemplara y pretendiese disolver su secreto sin autorización. O tal vez no encontró más signos disponibles en la máquina, o le faltó imaginación para combinar de múltiples maneras los que podía utilizar, o simplemente careció de tiempo y paz para refinar los dispositivos de seguridad en su método propuesto. Estas y otras inquietudes las resolverá quien decida prolongar el estudio de tan peculiar espécimen criptológico.