ARCHIVOS Y DOCUMENTOS

ALGUNOS CASOS CRIPTOGRÁFICOS DEL MOVIMIENTO CONSTITUCIONALISTA, 1914-1915

Roberto R. Narváez

INTRODUCCIÓN

Entre 1914 y 1920, durante las guerras de revolución en México, el movimiento constitucionalista liderado por Venustiano Carranza fue uno de los más constantes y disciplinados en utilizar la criptografía como estrategia básica para proteger sus comunicaciones reservadas contra los interceptores ilegales, o espías, durante la transmisión. El personal del ejército constitucionalista y los colaboradores político-diplomáticos de Carranza (gobernadores, agentes comerciales, agentes confidenciales, embajadores, cónsules, espías) produjeron una cantidad enorme de telegramas, cartas, partes de guerra, oficios, memorándums y otros documentos oficiales –no siempre reservados– de diversas clases en cifra o código, o bien cifrados y codificados a la vez, transformando a cada mensaje original en un texto claro de manera total o parcial. Y si bien su propósito inmediato era impedir a terceros no autorizados (esto es, individuos ajenos a cada particular red de cifra en operación) la lectura de su correspondencia, en muchos casos recurrieron a estos métodos con el solo afán de minimizar los costos de transmisión telegráfica. Por supuesto, esta circunstancia no

eliminaba las propiedades crípticas de un telegrama determinado, pues un eventual interceptor tendría problemas para descifrarlo rápidamente si careciera de la clave o el diccionario de códigos –aun de tipo comercial– utilizado para el caso.

Existen colecciones de estos materiales en archivos de México, Estados Unidos y algunos países de Centroamérica y Sudamérica. Las que se localizan en nuestro país destacan por la variedad de sus contenidos estrictamente criptológicos, los cuales, al organizarlos en series y examinarlos con el auxilio del criptoanálisis, ofrecen datos de la mayor importancia para evaluar la criptografía constitucionalista en sus aspectos técnicos, metodológicos y tecnológicos. Su originalidad estructural y la fortaleza de sus dispositivos de seguridad no supera, salvo en casos aislados, a la de los villistas, los zapatistas y los felicistas, por citar sólo a estos tres grupos revolucionarios. Esto significa que los criptogramas y métodos criptográficos del carrancismo, como los que veremos en las páginas a seguir, eran vulnerables en un grado significativo, esto es, no era difícil romper su secreto por la fuerza o, expresado técnicamente, *decriptarlos*. A muchos les podrá parecer, al observarlos superficialmente y con prisa, que todos son prácticamente idénticos y, en consecuencia, quien entiende uno entiende el conjunto. Pero esto equivale a confundir una mera suposición de identidad con un verdadero criterio criptológico de clasificación y análisis. Y es que, en este tipo de materias, las exigencias de un método crítico, puntual, no pueden eludirse a favor de cualquier apreciación vaga. Lo cierto es que no conviene asumir tal actitud desde la perspectiva histórica-criptológica. La criptografía oficialista de cualquier país, incluyendo a México, no es ni totalmente simple o familiar ni totalmente complicada o excepcional, y la manera más recomendable de investigarla consiste en describirla caso por caso y analizar sus propiedades estructurales y técnicas. De este modo es posible inferir generalizaciones legítimas. En el fondo, se trata de evaluar los alcances del ingenio criptológico de un grupo de individuos que buscó

adaptar tecnologías y tácticas adecuadas (en su época) para la transmisión segura de inteligencia. Lo que aprendemos con esto es instructivo en muchos sentidos, y en última instancia nos motiva para fomentar el criptoanálisis histórico en la investigación de la historia militar, política y diplomática de México.

En las páginas que siguen analizaré modelos de criptosistemas y dos criptogramas en borrador generados por un mismo algoritmo, seleccionados de expedientes que provienen de dos repositorios: *(I)* Archivo Histórico Genaro Estrada de la Secretaría de Relaciones Exteriores de México (AHGE), y *(II)* Archivo Histórico del Centro Cultural Isidro Fabela-Museo Casa del Risco (AHCCIF), ubicado en la Ciudad de México.

I

En el AHGE hay instancias de criptografía constitucionalista en multitud de carpetas y legajos. Abundan las cartas, oficios y telegramas con líneas crípticas autógrafas o mecanografiadas. Muchos de estos documentos se leen fácilmente y no pocos incluyen el descifrado entre renglones (circunstancia favorable, como es lógico, para simplificar el criptoanálisis). También hay, por desgracia, folios de probada naturaleza criptográfica redactados con tales medios, o en tan mal estado de conservación, que su intelección es muy difícil o imposible. Esta condición, sin embargo, no suele afectar a los registros de criptosistemas o reglas para cifrar y descifrar, o codificar y decodificar, o una combinación de ambos procedimientos. Estos métodos se dividen, básicamente, en monoalfabéticos y polialfabéticos. Los polialfabéticos, en muchos casos, prescriben el manejo de una clave para potenciar la transformación a cifra. He revisado en otro lugar varios que presentan aspectos de notable complejidad.[1] Aquí no trataré especímenes parecidos. Debemos entender que

[1] Narváez, *Criptografía diplomática*, caps. III, IX y XI.

muchos criptosistemas –entendiendo aquí por criptosistema, básicamente, un esquema gráfico acompañado de las reglas de transformación a cifra o código– de la época de la criptografía manual o de clave privada (y los de Carranza y asociados pertenecen, todos, a esta categoría general)[2] constituyen su propia clave de operación o, en otras palabras: la representación de los alfabetos, su ordenamiento peculiar, *forma parte de la clave*. Esto es cabalmente definitorio de los sistemas arreglados en torno a un solo alfabeto. Lo que determina la variedad de funciones es el empleo de la transposición y la sustitución simple o directa, mecanismos que, en ocasiones, operan en coordinación con aditamentos metodológicos precisos.

Sobre todas estas propiedades y rasgos distintivos expondré, a continuación, algunas observaciones críticas y comparativas de 11 ejemplares tomados de entre los casi 120 que reúne el legajo "Claves usadas durante el periodo revolucionario de México. Colección de las mismas" (topográfica 14-2-64), fechado en 1915.[3] Como se aprecia en las figuras, todos los folios elegidos para el estudio están mecanografiados, lo que agiliza su criptoanálisis en gran medida.

A) En las figuras 1 a 3 se muestran casos de sustitución monalfabética directa de 1 a 1, basada en la reciprocidad de los caracteres según su posición en dos renglones. El renglón superior corresponde al del alfabeto de la lengua, o de definición (extensión 26 caracteres, con exclusión de la Ñ),[4] y el inferior corresponde al

[2] Significa que los usuarios debían mantener en secreto las claves o llaves y, en algunos casos, los criptosistemas. Esto cambia en la criptografía de clave pública hoy vigente, por motivos que aquí no tiene caso exponer.

[3] No hay en estos folios ninguna indicación de fechas de creación o de operación, se trata de una mera secuencia de ejemplares sin comentarios históricos o técnicos.

[4] La N se tomará como Ñ para cifrar toda palabra que la incluya, de modo que, al descifrar, el tenor del texto gradualmente aclarado la impondrá como grafema a leer.

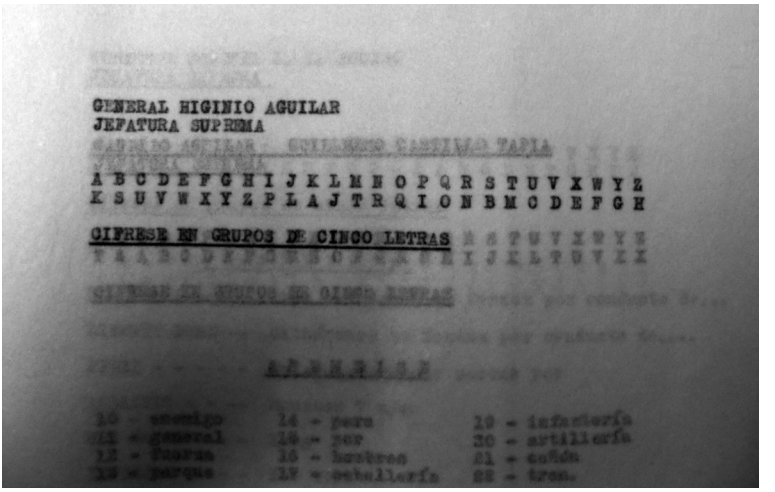
del alfabeto de cifrado (de idéntica extensión y contenido, por necesidad algorítmica). La reciprocidad se actualiza en el sentido de que, cuando una letra, digamos B, se sustituye crípticamente por otra, digamos S, ocurre lo mismo en la dirección inversa: la S se sustituye por la B. Esto, por convención, habrá de verificarse en todos los casos en que se realice la sustitución de cada letra según el pareado predeterminado. En el criptosistema del general Higinio Aguilar[5] con la jefatura suprema (en adelante JS), por ejemplo, se aprecia esta condición en los pares A/K-K/A, D/V-V/D, M/T-T/M (figura 1). A se cifra con K y K, con A; D se cifra con V, V con D, y así en todos los demás casos. El método compartido por el administrador Aguado y la JS (figura 2) comparte con el anterior la estructura, extensión y el procedimiento de encriptación, aunque hay una variación interesante en cuanto al modo de fijar el alfabeto de cifrado. Como se observa, las letras ubicadas en los lugares 13 a 17 forman la palabra "CLAVE"; esto determina que las secuencias respectivas de los conjuntos de caracteres anteriores y posteriores a esos puntos 13 y 17 no incluyan las letras contenidas en "CLAVE". Esas secuencias no pretenden reproducir el orden normal del alfabeto definitorio, sino que se alteran por transposiciones requeridas para mantener la reciprocidad. A esto se debe que, por ejemplo, la P aparezca entre la G y la H (en la mitad izquierda) y no entre la O y la R (en la mitad derecha), manteniendo así la reciprocidad con V.

Una estrategia como la recién descrita se usó al diseñar el método entre Castilla Brito y Zubaran Capmany (figura 3). En este caso se aprecia la palabra "BRITPO" en el alfabeto inferior; la idea fue, sin duda, referir el nombre del remitente principal, o sea Castilla Brito, pero el requerimiento de la reciprocidad determinó la interferencia de la P.

---

[5] Para datos biográficos de los generales mencionados en este artículo véase AA. VV., *Diccionario de generales*.

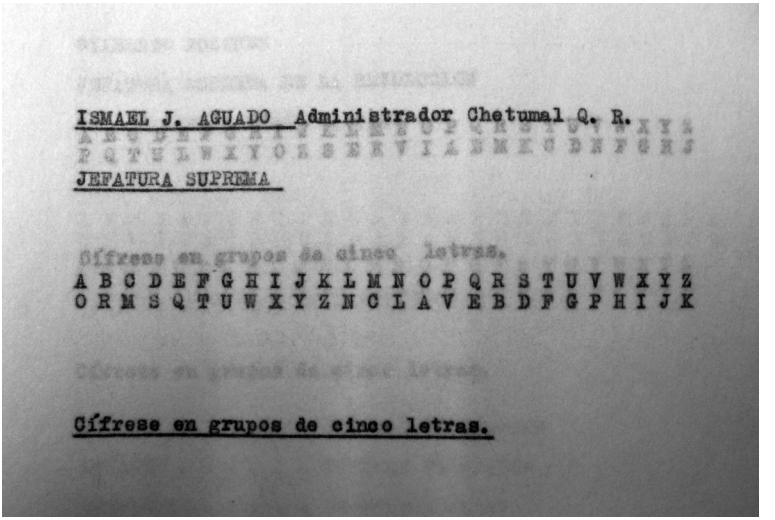
Figura 1


GENERAL HIGINIO AGUILAR
JEFATURA SUPREMA

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

CIFRESE EN GRUPOS DE CINCO LETRAS

Figura 2

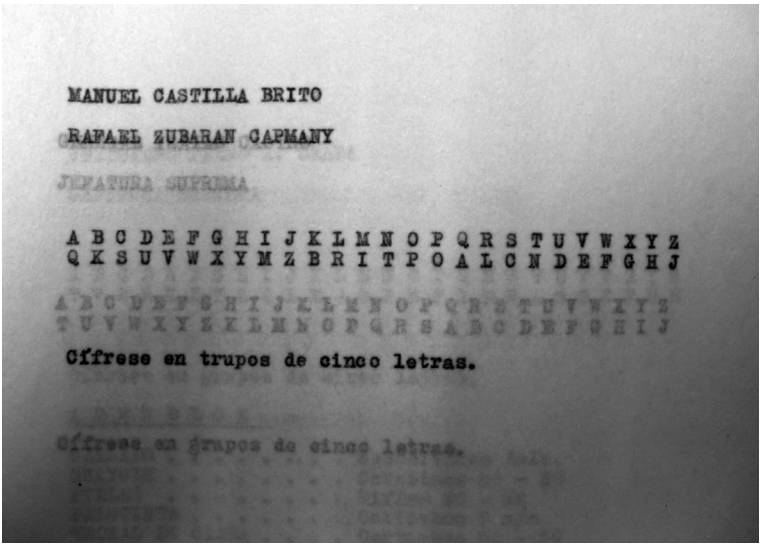

ISMAEL J. AGUADO Administrador Chetumal Q. R.

JEFATURA SUPREMA

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

Cífrese en grupos de cinco letras.

Figura 3



B) En las figuras 4 a 9 se muestran mecanismos de reciprocidad como los anteriores, pero con el complemento (se los introduce como "apéndices") de diccionarios de códigos para términos técnicos, solicitudes, nombres de corporaciones y lugares geográficos, cantidades y otras expresiones. Genéricamente constituyen variaciones modernas del arcaico nomenclátor o nomenclador.[6] Los diccionarios son "de una parte" (esto es, incorporan solamente las equivalencias de codificación)[7] y su utilidad es enorme para robustecer la seguridad del criptotexto, ya que siempre es más difícil decriptar un código que una cifra –al menos tal era la situación cuando los criptotextos eran clave privada.

[6] Véase, por ejemplo, Narváez, *Criptografía diplomática*, pp. 96-97.

[7] Si incorporaran también la lista del código al término claro, serían diccionarios de dos partes.

En las figuras 4 y 5 los diccionarios, a juzgar por su contenido, fueron creados para funcionar en comunicaciones delicadas sobre temas logísticos, financieros y tácticos de operaciones militares. Las entradas no están ordenadas alfabéticamente, siendo aparente que se siguió un criterio de prioridad especial para ordenar los elementos claros de acuerdo con su nivel de urgencia: los referentes al armamento quedan por encima de los referentes a dinero, avisos de interés coyuntural, locaciones e individuos citados por apellido (casos de Frezieres y Elías en la figura 5). Hay también peculiaridades en cuanto a la elección de los términos código. En el caso del criptosistema para Pedro A. Chapa[8] y la JS (figura 6), todos se reconocen como entradas localizables en cualquier diccionario de la lengua, o bien en diccionarios técnicos especializados, sin haber duda de que significan algo en léxico español.[9] Y la mayoría se seleccionó, según parece, por su vinculación al campo de la industria y los ferrocarriles.[10]

Lo mismo se pretende en cuanto al sistema de Hammeken y Díaz, en China, con la JS (figura 5), donde los términos claramente no son propios de ningún diccionario castellano; de hecho, en su mayoría fueron inventados para operar criptográficamente. Así se dota a los medios de un acento especial, digamos, que tiende a señalar su procedencia de un vistazo.[11] Por otra parte, se aprecia que el alfabeto de cifrado se arregló

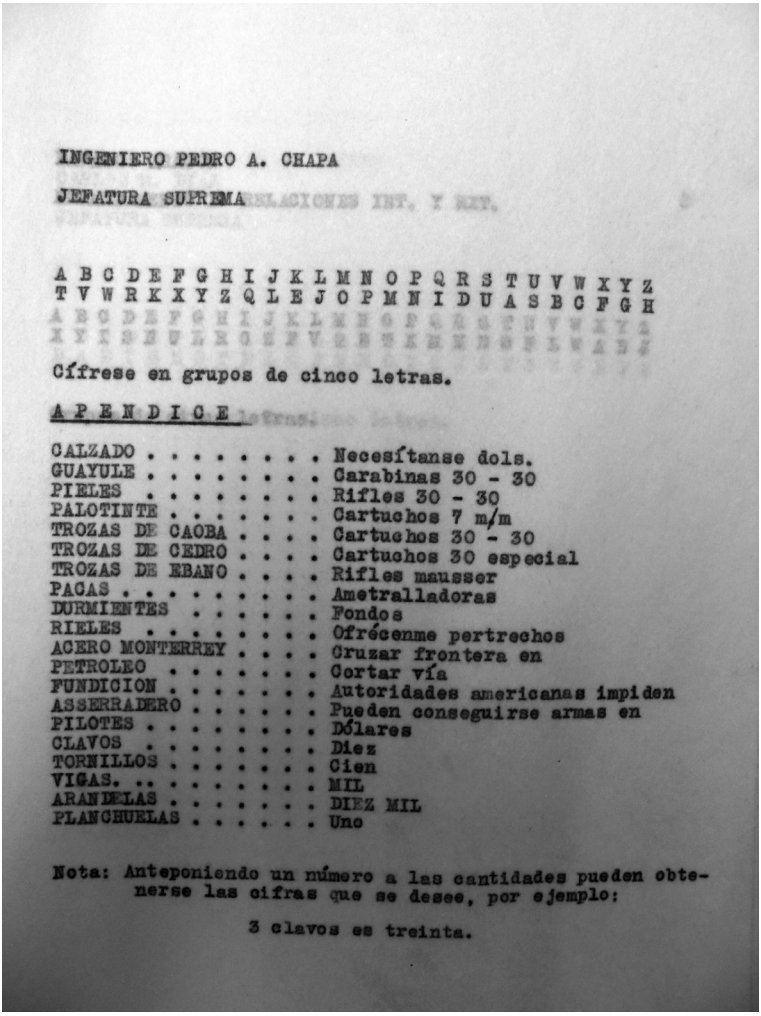
[8] Aunque en el documento de referencia se da a Chapa el título de ingeniero, algunas fuentes afirman que se tituló de arquitecto en Filadelfia, Estados Unidos, en 1911; véase, por ejemplo, Romero Flores, *Historia del Congreso Constituyente*, p. 167.

[9] En el renglón 14 se lee Asserradero: es arcaísmo de Aserradero.

[10] Entre las excepciones destaca el término guayule para "carabinas 30-30", que Francisco I. Madero utilizó de manera similar (propiamente habló de "guayuleras") en una carta a Eduardo Maurer del 28 de octubre de 1910. Madero, *Archivo*, t. II, p. 2111.

[11] Las estrategias de este tipo eran útiles para prevenir las confusiones al archivar los mensajes cifrados o codificados con cada uno de los diferentes criptosistemas.

Figura 4



INGENIERO PEDRO A. CHAPA

JEFATURA SUPREMA

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

Cífrese en grupos de cinco letras.

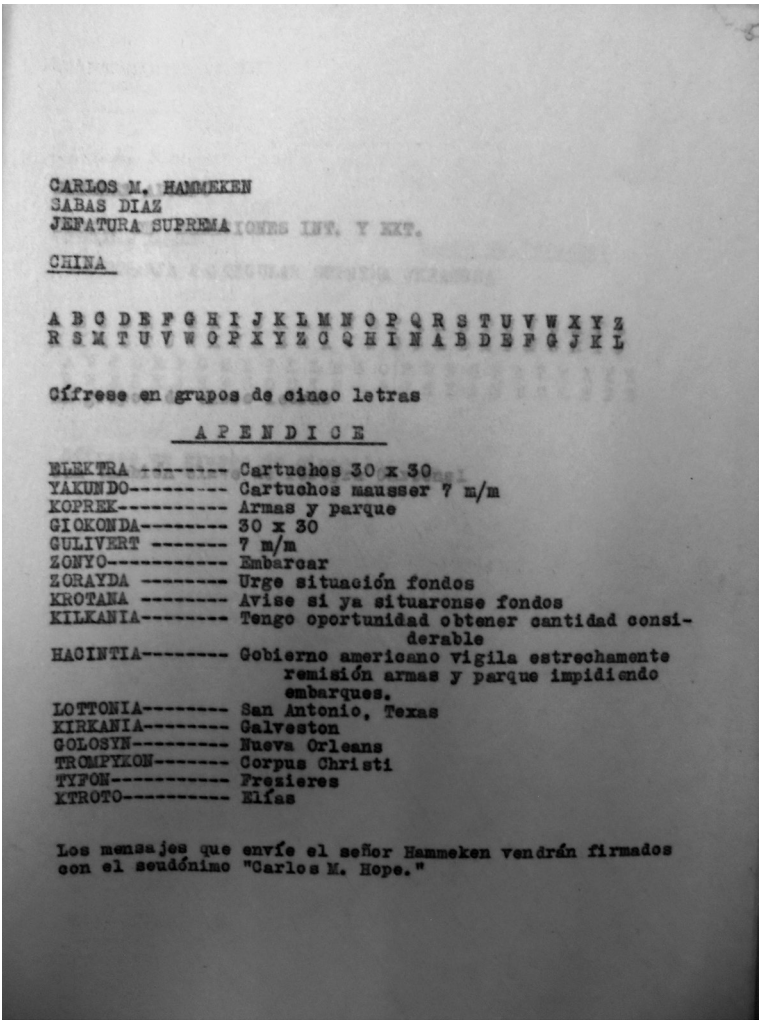
APENDICE

CALZADO . . . . . Necesítanse dols.
GUAYULE . . . . . Carabinas 30 - 30
PIELES . . . . . Rifles 30 - 30
PALOTINTE . . . . . Cartuchos 7 m/m
TROZAS DE CAOBA . . . . Cartuchos 30 - 30
TROZAS DE CEDRO . . . . Cartuchos 30 especial
TROZAS DE EBANO . . . . Rifles mausser
PACAS . . . . . Ametralladoras
DURMIENTES . . . . . Fondos
RIELES . . . . . Ofrécenme pertrechos
ACERO MONTERREY . . . . Cruzar frontera en
PETROLEO . . . . . Cortar vía
FUNDICION . . . . . Autoridades americanas impiden
ASSERRADERO . . . . . Pueden conseguirse armas en
PILOTES . . . . . Dólares
CLAVOS . . . . . Diez
TORNILLOS . . . . . Cien
VIGAS. .. . . . . MIL
ARANDELAS . . . . . DIEZ MIL
PLANCHUELAS . . . . . Uno

Nota: Anteponiendo un número a las cantidades pueden obtenerse las cifras que se desee, por ejemplo:

3 clavos es treinta.

Figura 5



CARLOS M. HAMMEKEN
SABAS DIAZ
JEFATURA SUPREMA [illegible] INT. Y EXT.

CHINA

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

Cífrese en grupos de cinco letras

APENDICE

ELEKTRA -------- Cartuchos 30 x 30
YAKUNDO--------- Cartuchos mausser 7 m/m
KOPREK---------- Armas y parque
GIOKONDA-------- 30 x 30
GULIVERT ------- 7 m/m
ZONYO----------- Embarcar
ZORAYDA -------- Urge situación fondos
KROTANA -------- Avise si ya situaronse fondos
KILKANIA-------- Tengo oportunidad obtener cantidad considerable
HACINTIA-------- Gobierno americano vigila estrechamente remisión armas y parque impidiendo embarques.
LOTTONIA-------- San Antonio, Texas
KIRKANIA-------- Galveston
GOLOSYN--------- Nueva Orleans
TROMPYKON------- Corpus Christi
TYFON----------- Frezieres
KTROTO---------- Elías

Los mensajes que envíe el señor Hammeken vendrán firmados con el seudónimo "Carlos M. Hope."

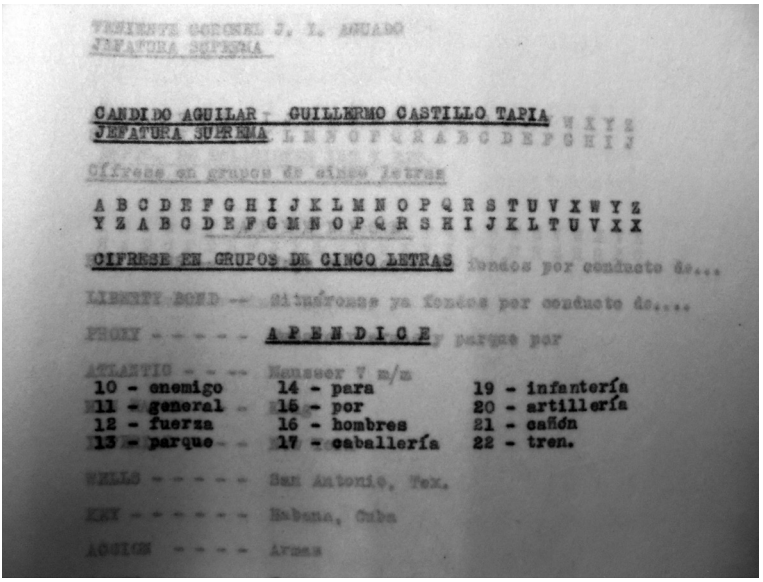
con base en la palabra CHINA, que se registra CQHINA por la misma razón indicada a propósito del caso Castilla Brito-Zubaran Capmany (véase *supra*).

En los siguientes dos ejemplares (figuras 6 y 7) resalta, en los diccionarios, la peculiaridad de que la codificación se realiza con guarismos y no palabras. En ambos casos los códigos son dos dígitos que se ordenan de forma ascendente del 10 al 22, con omisión del 18 en el sistema de Aguilar-Castillo Tapia con la JS, y del 21 al 77 (con múltiples omisiones y algunas repeticiones) en el de Pardio Camara-Zubaran Capmany. En cuanto a las entradas, todas aluden a cuestiones geográficas, financieras, comerciales y del ámbito militar.

Son de notar algunas innovaciones en los artilugios para cifrar, con respecto a lo que llevamos visto. En el caso del método Aguilar-Castillo Tapia-JS (figura 6) hay transposiciones en ambos alfabetos, no sólo en el de cifrado. En el alfabeto superior, efectivamente, la W y la X intercambian lugares, mientras en el inferior el intercambio es entre los quintetos literales HIJKL y MNOPQ. Esta segunda propiedad impide que la sustitución para cifrar opere constantemente por un deslizamiento a la izquierda de dos lugares (-2) para cada letra en el alfabeto definitorio. Que esto se verifica lo revela una observación de las posiciones respectivas entre los primeros 9 elementos de ambos alfabetos: la A se ocultaría como Y, la B como Z, la C como A, la B como D, y así en secuencia hasta la J, que no se cifra con H sino con M, así como la K se cifra con N y no con I, y así, a causa de la transposición de las cinco letras. La transformación por el desplazamiento indicado se reanuda en la V, si bien se prescribe la sustitución Z-X, lo que sugiere la inclusión de la Z como posible término de valor nulo, en tanto su frecuencia relativa de aparición en cualquier texto español es muy baja en comparación con la Y, también pareada con la X.

En cuanto al método Pardio-Zubaran (figura 7), el alfabeto inferior también se arregla mediante un deslizamiento mutuo de

Figura 6



TENIENTE CORONEL J. I. AGUADO
JEFATURA SUPREMA

CANDIDO AGUILAR - GUILLERMO CASTILLO TAPIA
JEFATURA SUPREMA

Cifrese en grupos de cinco letras

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

CIFRESE EN GRUPOS DE CINCO LETRAS

APENDICE

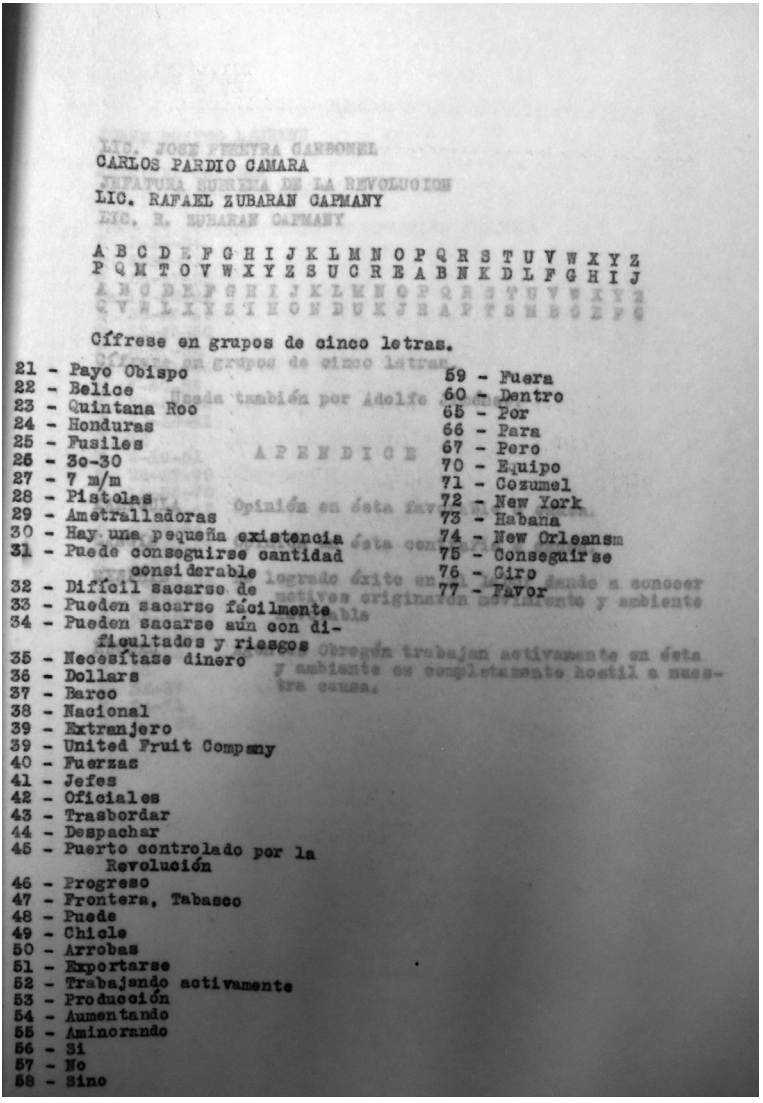
10 - enemigo	14 - para	19 - infantería
11 - general	15 - por	20 - artillería
12 - fuerza	16 - hombres	21 - cañón
13 - parque	17 - caballería	22 - tren.

-15, por lo cual A se cifra P, B = Q, etc., mas esta equivalencia deja de operar para varias letras en el resto de la serie porque el alfabeto de cifrado se organizó en torno al vocablo (una especie de clave) SUCRE. Esta inserción impone la ejecución de deslizamientos variables para cifrar, aunque no elimina la reciprocidad fija.

En la figura 8 tenemos un criptosistema entre Ismael J. Aguado y la JS. (Las iniciales del nombre aparecen "J. I.", pero se trata del mismo individuo citado en el ejemplar de la figura 2, en esta ocasión con el grado de teniente coronel.) En el alfabeto inferior se han efectuado transposiciones por bloques. Al no haber algún dispositivo que determine la reciprocidad fija, algunas sustituciones demandan más de un pareado.

Es de notar, por otra parte, que en el diccionario conviven términos en inglés y en castellano.

Figura 7



CARLOS PARDIO CAMARA

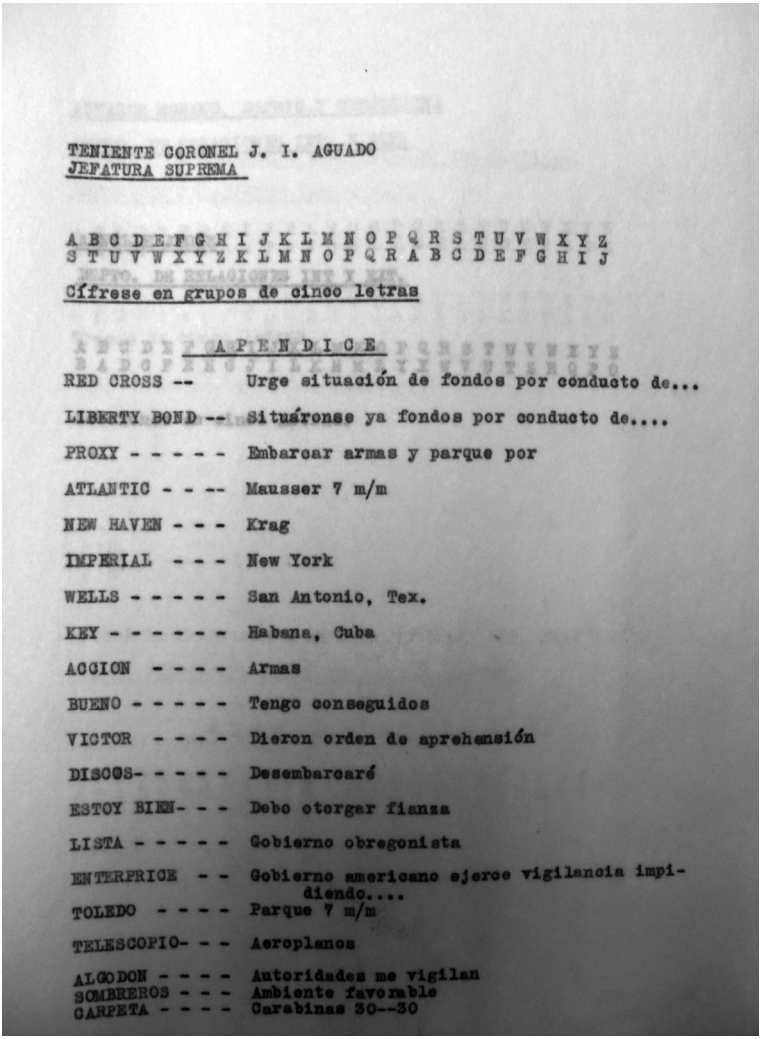
LIC. RAFAEL ZUBARAN CAPMANY

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

Cífrese en grupos de cinco letras.

21 - Payo Obispo
22 - Belice
23 - Quintana Roo
24 - Honduras
25 - Fusiles
26 - 30-30
27 - 7 m/m
28 - Pistolas
29 - Ametralladoras
30 - Hay una pequeña existencia
31 - Puede conseguirse cantidad considerable
32 - Difícil sacarse de
33 - Pueden sacarse fácilmente
34 - Pueden sacarse aún con dificultades y riesgos
35 - Necesítase dinero
36 - Dollars
37 - Barco
38 - Nacional
39 - Extranjero
39 - United Fruit Company
40 - Fuerzas
41 - Jefes
42 - Oficiales
43 - Trasbordar
44 - Despachar
45 - Puerto controlado por la Revolución
46 - Progreso
47 - Frontera, Tabasco
48 - Puede
49 - Chicle
50 - Arrobas
51 - Exportarse
52 - Trabajando activamente
53 - Producción
54 - Aumentando
55 - Aminorando
56 - Si
57 - No
58 - Sino
59 - Fuera
60 - Dentro
65 - Por
66 - Para
67 - Pero
70 - Equipo
71 - Cozumel
72 - New York
73 - Habana
74 - New Orleansm
75 - Conseguirse
76 - Giro
77 - Favor

Figura 8



TENIENTE CORONEL J. I. AGUADO
JEFATURA SUPREMA

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

Cífrese en grupos de cinco letras

APENDICE

RED CROSS -- Urge situación de fondos por conducto de...

LIBERTY BOND -- Situáronse ya fondos por conducto de....

PROXY - - - - - Embarcar armas y parque por

ATLANTIC - - -- Mausser 7 m/m

NEW HAVEN - - - Krag

IMPERIAL - - - New York

WELLS - - - - - San Antonio, Tex.

KEY - - - - - - Habana, Cuba

ACCION - - - - Armas

BUENO - - - - - Tengo conseguidos

VICTOR - - - - Dieron orden de aprehensión

DISCOS- - - - - Desembarcaré

ESTOY BIEN- - - Debo otorgar fianza

LISTA - - - - - Gobierno obregonista

ENTERPRICE - - Gobierno americano ejerce vigilancia impidiendo....

TOLEDO - - - - Parque 7 m/m

TELESCOPIO- - - Aeroplanos

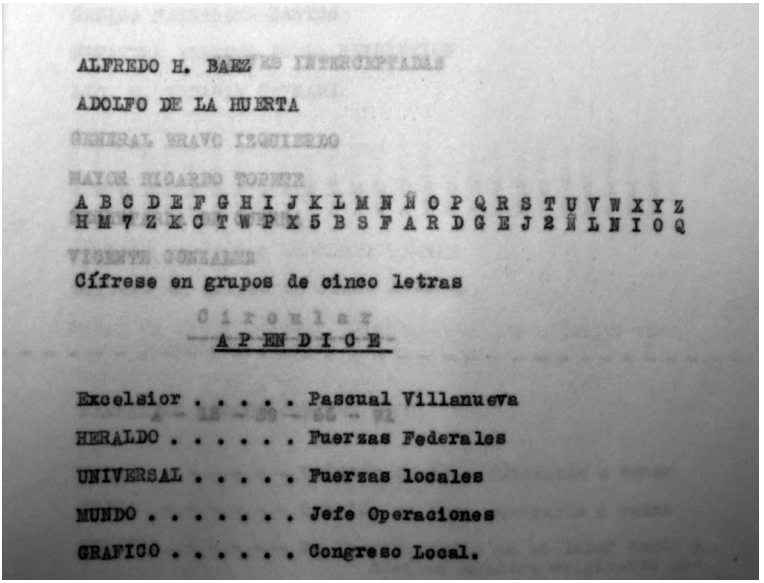
ALGODON - - - - Autoridades me vigilan
SOMBREROS - - - Ambiente favorable
CARPETA - - - - Carabinas 30--30

En el sistema entre Alfredo H. Baez y Adolfo de la Huerta (figura 9) hay varios aspectos dignos de nota. Ante todo, el alfabeto definitorio es de extensión 27 por la inclusión de la Ñ. El alfabeto de cifrado mide lo mismo, sin duda para propiciar sustituciones de 1 a 1, *aunque no recíprocas*. Entre las equivalencias de encriptación hay tres números, 7, 5 y 2, que toman el lugar de las letras U, V y Y. Los pareados en el criptotexto serían 7-C, 5-K y 2-T. Sin contar con más información sobre este caso, es difícil explicar que la K, letra de baja frecuencia relativa en español, tenga asignado un guarismo como sustituto, y no lo es menos el siguiente detalle: la Ñ se cifraría con A y la U con la Ñ; la A y la U, como vocales, tienen frecuencias de recurrencia muy alta en nuestra lengua, a diferencia de la Ñ. Así, no sería previsible que, en un criptotexto generado con este método, la A se repitiera mucho, pero sí la Ñ, en tanto que escondería a la U. Quien tratara de romper uno de tales criptotextos y, en su criptoanálisis, notara la constante repetición de la Ñ, con buena razón podría conjeturar que oculta una vocal, y pensaría muy probablemente lo contrario al apuntar la frecuencia de la A. Estas consideraciones sugieren un crecido nivel de vulnerabilidad en el espécimen, si bien es imposible estar seguro, pues tal vez los usuarios procedían con este método en un estilo cabalmente secreto para nosotros. Hace falta información para incursionar más a fondo en este caso.

En cuanto al breve léxico de códigos adjunto, es manifiesto que se refiere a temas militares y políticos.

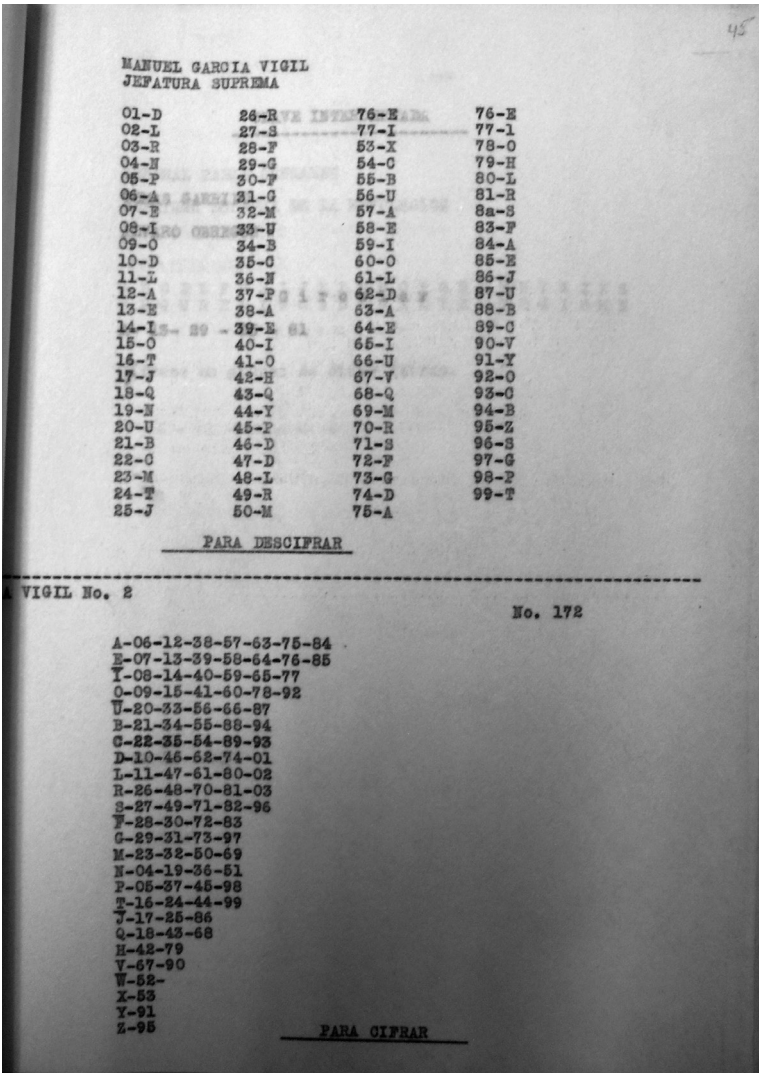
C) El siguiente ejemplar (figura 10) es un sistema de sustitución monoalfabética por guarismos. El alfabeto de definición es de extensión 25, y su ordenamiento no es lexical sino en sentido descendente a partir de los elementos de mayor frecuencia relativa, esto es, las cinco vocales. A la A y la E se les asignan hasta 7 equivalentes, y a la I y la O hasta 6. El resto son las consonantes, y para determinar su sucesión de frecuencia los creadores del sistema se apoyaron, probablemente, en una estadística estandarizada para el idioma español.

Figura 9



Ésta es la serie o lista que aparece en la parte inferior. Funciona para el cifrado. En la parte superior se ha colocado la lista correlativa, "para descifrar", como se distingue claramente. (Antiguamente se le denominaba, en el ámbito hispanoamericano, "contracifra".) Es una progresión numérica del 01 al 99, y junto a cada par de dígitos se apunta el carácter alfabético de texto plano que encripta. Queda fuera el 51, y si bien el 52 claramente se asocia con la W en la lista inferior, en la superior no se localiza. Los pares 20, 33, 56, 66 y 87 ocultan a la U, mientras que 08, 14, 40, 59, 65 y 77 hacen lo mismo con la I. Esta letra, por cierto, se lee Y en el listado de cifrado; fue un error al mecanografiar, sin duda, porque, de otro modo, en la "contracifra" habría confusiones en la asignación de cifras numéricas para la Y y la I.

Figura 10



MANUEL GARCIA VIGIL
JEFATURA SUPREMA

01-D	26-R	76-E	76-E
02-L	27-S	77-I	77-1
03-R	28-F	53-X	78-O
04-N	29-G	54-C	79-H
05-P	30-F	55-B	80-L
06-A	31-C	56-U	81-R
07-E	32-M	57-A	8a-S
08-I	33-U	58-E	83-F
09-O	34-B	59-I	84-A
10-D	35-C	60-O	85-E
11-L	36-N	61-L	86-J
12-A	37-P	62-D	87-U
13-E	38-A	63-A	88-B
14-I	39-E	64-E	89-C
15-O	40-I	65-I	90-V
16-T	41-O	66-U	91-Y
17-J	42-H	67-V	92-O
18-Q	43-Q	68-Q	93-C
19-N	44-Y	69-M	94-B
20-U	45-P	70-R	95-Z
21-B	46-D	71-S	96-S
22-C	47-D	72-F	97-G
23-M	48-L	73-G	98-P
24-T	49-R	74-D	99-T
25-J	50-M	75-A	

PARA DESCIFRAR

VIGIL No. 2

No. 172

A-06-12-38-57-63-75-84
E-07-13-39-58-64-76-85
I-08-14-40-59-65-77
O-09-15-41-60-78-92
U-20-33-56-66-87
B-21-34-55-88-94
C-22-35-54-89-93
D-10-46-62-74-01
L-11-47-61-80-02
R-26-48-70-81-03
S-27-49-71-82-96
F-28-30-72-83
G-29-31-73-97
M-23-32-50-69
N-04-19-36-51
P-05-37-45-98
T-16-24-44-99
J-17-25-86
Q-18-43-68
H-42-79
Y-67-90
W-52-
X-53
Y-91
Z-95

PARA CIFRAR

D) Terminemos esta sección con un breve comentario al método entre Adolfo de la Huerta y F. W. Strickland (figura 11). La aparición del conjunto EJOTYDINSX pareado con los números 1 a 0 sugiere, a primera vista, que se trata de un dispositivo para tramar claves numéricas a partir de una palabra clave general que regularía la selección de caracteres sustitutos en diferentes alfabetos de un bloque. Estas claves podrían variar con determinada periodicidad (diaria, semanal, etc.). Cada clave se formaría de 6 guarismos; el primero indicaría el renglón del alfabeto a usar, y los demás el orden de las letras para encriptación.[12] Para agilizar la ubicación de los alfabetos y, por consiguiente, de cada equivalente críptico, podría inscribirse cada alfabeto en tiras de madera deslizables ordenadas en un cuadro de madera con aperturas en los extremos, al estilo de un ábaco (artilugios que fueron de uso muy normal en la diplomacia mexicana en Europa hasta la década de 1940, por lo menos).[13]

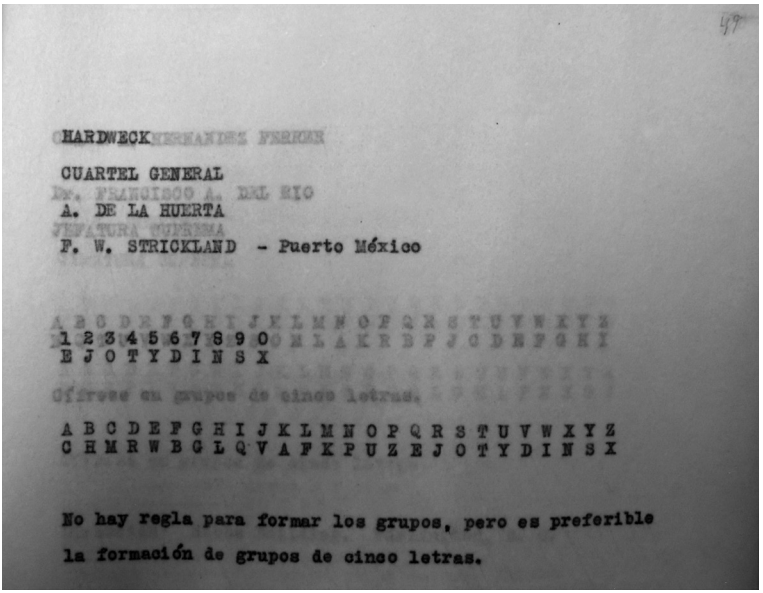
Esta sugerencia preliminar está marcada, sin embargo, por la especulación. El objeto de análisis carece de elementos materiales y formales que apoyen sólidamente tal conjetura. Contamos sólo con un par de alfabetos pareados que, al parecer, se combinan simplemente al estilo básico para potenciar sustituciones monoalfabéticas. El alfabeto inferior sería el de la cifra, alterado de modo que concluya, justamente, con el agregado EJOTYDINSX. Así las cosas, quizá la explicación más plausible sea ésta: se trata de una cifra monoalfabética de sustitución simple, y la mezcla de consonantes y vocales pareada con los guarismos 1 al 0 sólo indica que aquellas letras son los equivalentes crípticos para estos dígitos.

Con todo, es evidente que EJOTYDINSX no tiene caracteres repetidos, detalle importante para mantener la idea del criptosistema basado en la sustitución alfabética rotatoria. Es posible

[12] Consideraciones sobre este tipo de métodos en Narváez, *Criptografía diplomática*, pp. 383-389, 398-404.

[13] Como lo mostraré en un artículo de próxima aparición.

Figura 11


HARDWECK

CUARTEL GENERAL

A. DE LA HUERTA

F. W. STRICKLAND - Puerto México

1 2 3 4 5 6 7 8 9 0
E J O T Y D I N S X

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

No hay regla para formar los grupos, pero es preferible la formación de grupos de cinco letras.

que el alfabeto pareado en la figura 11 no sea sino una sección extraída de un bloque mayor (de 10 pares) y se presente en el documento de manera independiente, por cuanto era de uso exclusivo, fijo, entre los corresponsales mencionados. Si tal resultara ser el caso, la introducción de cuadros de madera y otras cosas en la conjetura sería baladí.

Repito, en fin, que la escasez de datos pertinentes en los registros impide articular una explicación firme para este caso.

En casi todos los ejemplares anteriores se indica explícitamente la necesidad o conveniencia de cifrar en "grupos de cinco letras". Esta era una práctica común en las transmisiones telegráficas y respondía a convenciones internacionales de diverso tipo sobre las que no puedo extenderme aquí. Pero tampoco era extraño subdividir el criptotexto en 8, 10 y hasta 12 elementos.

II

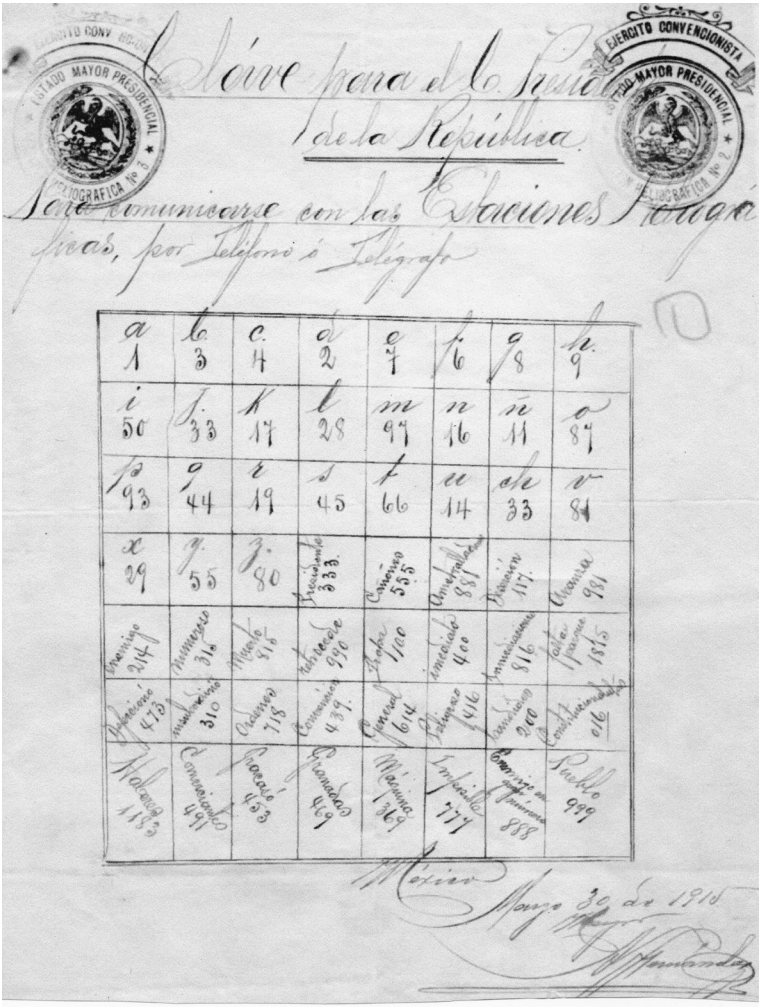
Revisemos ahora algunos documentos que resguarda el AHCCIF, en donde hay numerosos materiales de naturaleza criptográfica cuyo abordaje histórico-crítico y criptoanalítico *a gran escala* todavía está por hacerse.

El primero (figura 12)[14] es monoalfabético y de sustitución numérica simple, acompañado de un breve grupo de códigos para encubrir voces unitarias o frases mediante tres y hasta cuatro dígitos. El alfabeto excluye la W, pero incluye la CH. La estructura es muy similar a la de varios ejemplares que vimos en la sección anterior, siendo la variación más notable el arreglo rectangular (8x7). Evidentemente fue preparado para notificaciones militares entre la Presidencia y las estaciones heliográficas. Al contar solamente con el trazado del criptosistema no es fácil determinar la manera homogénea o diversificada en que los mensajes cifrados se preparaban para la transmisión; es de suponer que se agruparían en quintetos (hasta donde alcanzaran los elementos) para el telégrafo, como era lo habitual en la época, pero varios motivos técnicos, tecnológicos y de otra índole vuelve difícil ceñirse a la misma suposición.

En las figuras 13 a 16[15] tenemos ejemplos de sistemas poligráficos que, en buena medida, reproducen el clásico artificio de telegrafía óptica militar descrito por Polibio en el libro II (10.45-47) de sus *Historias*, operando casi de manera idéntica. También se los puede calificar de tomográficos, mientras no los tomemos como adaptaciones del modelo descrito por Pliny Earle Chase en 1859, que se distingue por imponer una sustitución de factores por multiplicación como paso preliminar a la sustitución criptográfica en el estilo de Polibio.[16] La sustitución es de letras

[14] AHCCIF, RM-I.3-014.
[15] AHCCIF, RM-I.3-014.
[16] Narváez, *Criptografía diplomática*, pp. 464-465, 457-458.

Figura 12


EJERCITO CONVENCIONISTA
ESTADO MAYOR PRESIDENCIAL
CRIPTOGRAFICA Nº 2
Clave para el Servicio
de la República
Para comunicarse con las Estaciones Telegráficas, por Teléfono ó Telégrafo
Mayo 30 de 1915

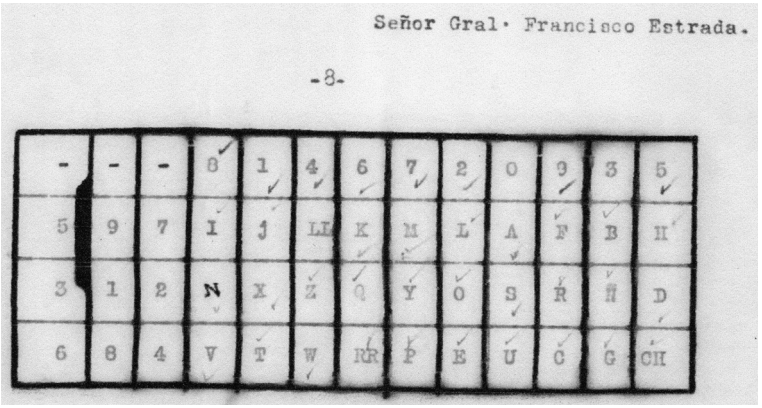
por guarismos que se ubican en la fila superior del rectángulo y en las columnas de la izquierda. Las letras configuran aquí, por supuesto, el único alfabeto literal disponible, que es el definitorio. Son las del alfabeto regular de la lengua, distribuidas a capricho. La extensión llega a 30 por la inclusión de la RR, la LL, la Ñ y la CH. De fijo se proveen tres columnas con numerales a la izquierda para combinarse con los de la fila superior y formar, así, los equivalentes para el ocultamiento. Esto puede generar verdaderas sustituciones múltiples, con todo, su proceso de formación no es confundible con el de varios sistemas polialfabéticos de clave privada, ante todo porque no depende de una palabra clave.

El método que se sigue en estos casos es, en rigor, el siguiente. Cada carácter del mensaje abierto –o en "texto plano"– a encriptar se esconde detrás de una pareja numeral formada por un guarismo de la columna a la izquierda y otro de la fila superior. Cada cifra surge por la intersección del número elegido en la columna de la izquierda y el número de la fila superior. Así, la C se transforma en 69, aunque, dada la presencia de las otras dos columnas, podría resultar en 89 o 49. Del mismo modo, la O puede encriptarse no sólo como 13, sino también como 31 y 22. Usando el esquema para uso del general Francisco Estrada (figura 13), por ejemplo, la palabra *Constitucionalismo* se puede cifrar así: 69 12 28 30 81 98 41 60 69 78 22 38 50 92 58 30 77 30. Todo esto se puede afirmar de los ejemplares restantes.

Para terminar, veamos una clave usada en 1914 por la Agencia Confidencial que, con cuartel en Washington, tuvo un papel relevante durante las así llamadas conferencias del Niágara, negociando con los ministros diplomáticos plenipotenciarios de Argentina, Brasil y Chile (grupo conocido como "ABC", por las iniciales de cada país).[17] En aquel año la agencia estuvo a

[17] Fabela, *Historia diplomática*, t. II, cap. I. Barragán Rodríguez, *Historia del ejército constitucionalista*, p. 139.

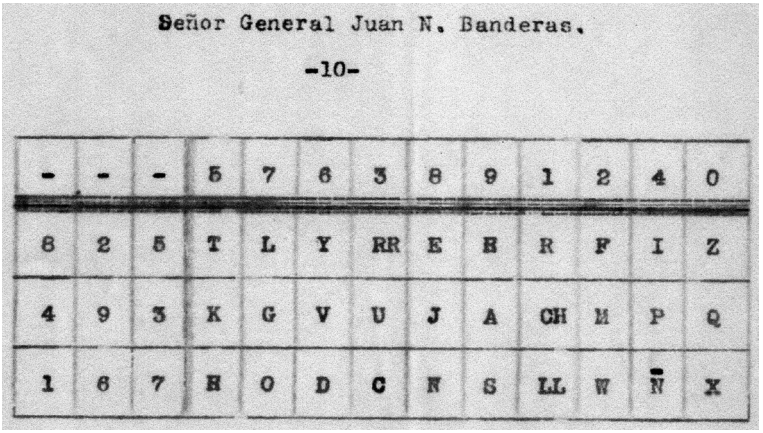
Figura 13


Señor Gral. Francisco Estrada.

-8-

-	-	-	8	1	4	6	7	2	0	9	3	5
5	9	7	I	J	LL	K	M	L	A	F	B	H
3	1	2	N	X	Z	Q	Y	O	S	R	Ñ	D
6	8	4	V	T	W	RR	P	E	U	C	G	CH

Figura 14


Señor General Juan N. Banderas.

-10-

-	-	-	5	7	6	3	8	9	1	2	4	0
8	2	5	T	L	Y	RR	E	H	R	F	I	Z
4	9	3	K	G	V	U	J	A	CH	M	P	Q
1	6	7	H	O	D	C	N	S	LL	W	Ñ	X

Figura 15

Figura 16

cargo de Rafael Zubaran Capmany y los miembros usaron varios tipos de cifras en su correspondencia privada.[18] El análisis se hará sobre dos grupos documentales: *1)* un catálogo explicativo de los criptosistemas disponibles para esta red de cifra en 1914, y *2)* la aplicación de uno de los métodos apuntados en un par de borradores de cartas, o telegramas, que intercambiaron Juan Francisco Urquidi (secretario de la agencia) y Roberto V. Pesqueira.

Las figuras 17 y 18[19] muestran los folios 1 y 3 que describen, con notable claridad, al catálogo mencionado arriba.[20]

Los usuarios podían elegir entre códigos y sistemas de cifrado. Los códigos eran de uso comercial o administrativo de manejo general, público, editados específicamente para la comunicación telegráfica; no se trata, por tanto, de códigos preparados especialmente para la correspondencia secreta de una red de cifra privada. Los tres diccionarios mencionados, A. B. C.,[21] Flint y Slater, eran muy socorridos en la época. Las dos formas de aplicación se explican con claridad en las reproducciones. Una forma era mantener, sin más, las equivalencias marcadas para cada entrada. La segunda demandaba la intervención de un artificio criptográfico, consistente en sumar un determinado número de unidades (9, 49, 99) a partir de la entrada original en cualquiera de los tres diccionarios. Para indicar la cantidad exacta se pondría un sufijo al nombre clave del libro utilizado en cada caso (por ejemplo, LARICSA significa que al usar el código A. B. C. se agregarían 9 unidades). Una variación a esta regla dependía del día de la semana en que se redactaría y enviaría el telegrama. Las cantidades a sumar irían del 10 al 70 progresivamente, partiendo

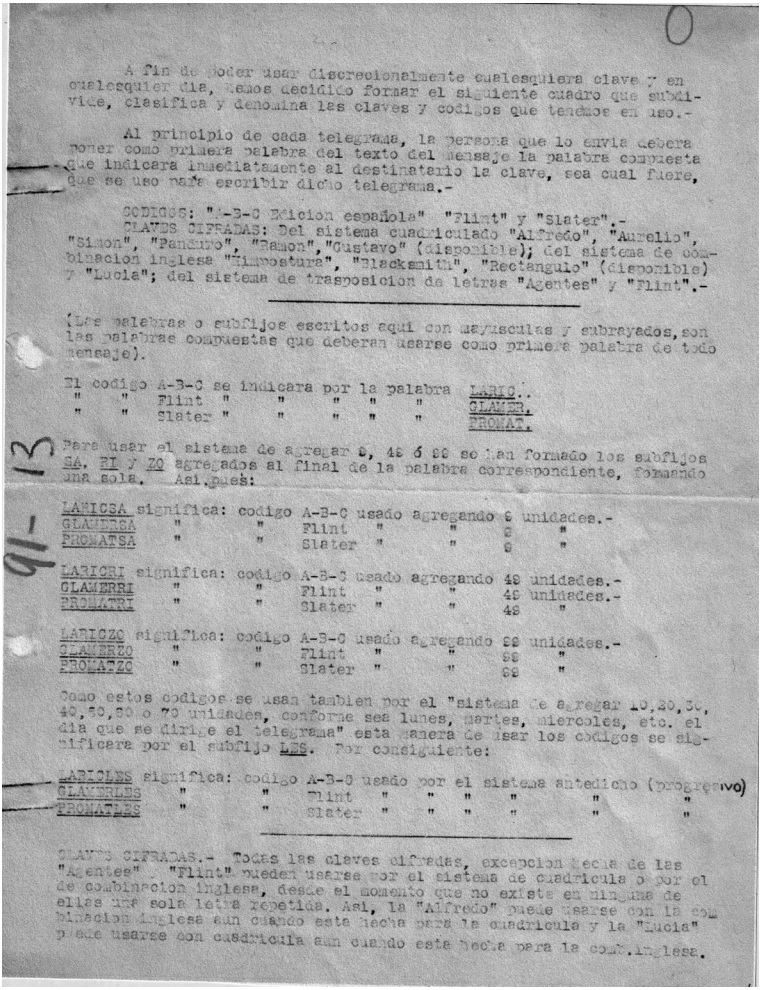
[18] Algunos ejemplos de aplicación en AHCCIF, leg. 90-22, 12 ff.

[19] AHCCIF, RM-II.1-050.

[20] El segundo folio es un *verso* con notas a lápiz y carece de relevancia para nuestros propósitos actuales.

[21] Estas siglas no deben tomarse como las del grupo sudamericano que participó en las conferencias del Niágara.

Figura 17



A fin de poder usar discrecionalmente cualesquiera clave y en cualesquier dia, hemos decidido formar el siguiente cuadro que subdivide, clasifica y denomina las claves y codigos que tendmos en uso.-

Al principio de cada telegrama, la persona que lo envia debera poner como primera palabra del texto del mensaje la palabra compuesta que indicara inmediatamente al destinatario la clave, sea cual fuere, que se uso para escribir dicho telegrama.-

CODIGOS: "A-B-C Edicion española" "Flint" y "Slater".-
CLAVES CIFRADAS: Del sistema cuadriculado "Alfredo", "Aurelio", "Simon", "Panchito", "Ramon","Gustavo" (disponible); del sistema de combinacion inglesa "Limpostura", "Blacksmith", "Rectangulo" (disponible) y "Lucia"; del sistema de trasposicion de letras "Agentes" y "Flint".-

---

(Las palabras o subfijos escritos aqui con mayusculas y subrayados, son las palabras compuestas que deberan usarse como primera palabra de todo mensaje).

El codigo A-B-C se indicara por la palabra LARIO.-
" " Flint " " " " " GLAMER.
" " Slater " " " " " PROMAT.

Para usar el sistema de agregar 8, 48 ó 88 se han formado los subfijos SA, RI y ZO agregados al final de la palabra correspondiente, formando una sola. Asi,pues:

LARICSA significa: codigo A-B-C usado agregando 8 unidades.-
GLAMERSA " " Flint " " 8 "
PROMATSA " " Slater " " 8 "

LARICRI significa: codigo A-B-C usado agregando 48 unidades.-
GLAMERRI " " Flint " " 48 unidades.-
PROMATRI " " Slater " " 48 "

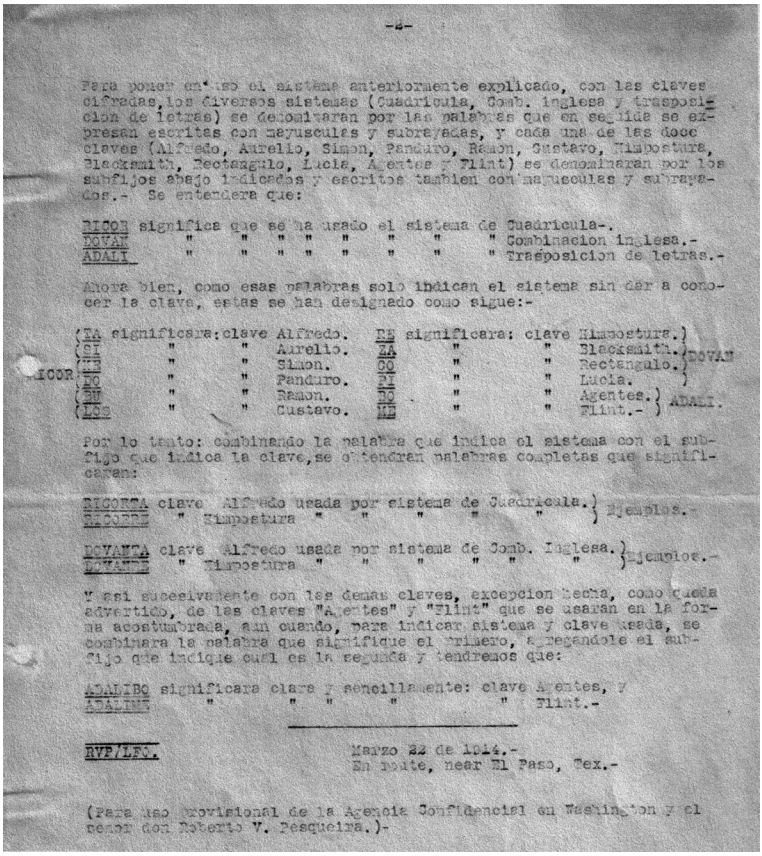
LARICZO significa: codigo A-B-C usado agregando 88 unidades.-
GLAMERZO " " Flint " " 88 "
PROMATZO " " Slater " " 88 "

Como estos codigos se usan tambien por el "sistema de agregar 10,20,30, 40,50,60 o 70 unidades, conforme sea lunes, martes, miercoles, etc. el dia que se dirige el telegrama" esta manera de usar los codigos se significara por el subfijo LES. Por consiguiente:

LARICLES significa: codigo A-B-C usado por el sistema antedicho (progresivo)
GLAMERLES " " Flint " " " " " "
PROMATLES " " Slater " " " " " "

CLAVES CIFRADAS.- Todas las claves cifradas, excepcion hecha de las "Agentes" y "Flint" pueden usarse por el sistema de cuadricula o por el de combinacion inglesa, desde el momento que no existe en ninguna de ellas una sola letra repetida. Asi, la "Alfredo" puede usarse con la combinacion inglesa aun cuando esta hecha para la cuadricula y la "Lucia" puede usarse con cuadricula aun cuando esta hecha para la comb.inglesa.

Figura 18



-6-

Para poner en uso el sistema anteriormente explicado, con las claves cifradas, los diversos sistemas (Cuadricula, Comb. inglesa y trasposicion de letras) se denominaran por las palabras que en seguida se expresan escritas con mayusculas y subrayadas, y cada una de las doce claves (Alfredo, Aurelio, Simon, Panduro, Ramon, Gustavo, Impostura, Blacksmith, Rectangulo, Lucia, Agentes y Flint) se denominaran por los sufijos abajo indicados y escritos tambien con mayusculas y subrayados.- Se entendera que:

RICOR significa que se ha usado el sistema de Cuadricula-.
DOVAN " " " " " " " " Combinacion inglesa.-
ADALI " " " " " " " " Trasposicion de letras.-

Ahora bien, como esas palabras solo indican el sistema sin dar a conocer la clave, estas se han designado como sigue:-

(IA significara: clave Alfredo. RE significara: clave Impostura.)
(GI " " Aurelio. ZA " " Blacksmith.) DOVAN
(MI " " Simon. OO " " Rectangulo.)
-ICOR (PO " " Panduro. PI " " Lucia.)
(AM " " Ramon. NO " " Agentes.) ADALI.
(TOS " " Gustavo. MU " " Flint.-)

Por lo tanto: combinando la palabra que indica el sistema con el sufijo que indica la clave, se obtendran palabras completas que signifiquen:

RICORTA clave Alfredo usada por sistema de Cuadricula.) Ejemplos.-
RICORRE " Impostura " " " " " ")

DOVANTA clave Alfredo usada por sistema de Comb. Inglesa.)
DOVANRE " Impostura " " " " " ") Ejemplos.-

Y asi sucesivamente con las demas claves, excepcion hecha, como queda advertido, de las claves "Agentes" y "Flint" que se usaran en la forma acostumbrada, aun cuando, para indicar sistema y clave usada, se combinara la palabra que signifique el primero, agregándole el sufijo que indique cual es la segunda y tendremos que:

ADALIBO significara clara y sencillamente: clave Agentes, y
ADALINT " " " " " Flint.-

AVP/LES. Marzo 22 de 1914.-
En route, near El Paso, Tex.-

(Para uso provisional de la Agencia Confidencial en Washington y el señor don Roberto V. Pesqueira.)-

del lunes (según parece), y bastaba un único sufijo, LES, para indicar que el texto se estaba usando conforme a tal convención; así, si se usaba el Flint un martes, el código sería GLAMERLES y el receptor sabría que al usar ese código *ese día* tendría que agregar 20 unidades a partir de la entrada. Si el intercambio fuera en un *miércoles*, la suma sería de 40, pero la clave única de codificación, GLAMERLES, permanecería.

Pasemos a los criptosistemas de transformaciones con base en una palabra clave. Estos ejemplares son estrictamente de cifrado y no de codificación. El documento en la figura 18 se refiere genéricamente a estos métodos como "claves cifradas" y propone tres variedades: "cuadrícula", "combinación inglesa" y transposición. Una vez más, se establecen nombres clave, prefijos y sufijos para determinar los sistemas y claves a utilizar en coordinación. Se proporcionan 12 claves para funcionar en combinación con tres modelos de cifrado distintos. Dejando aparte el método de transposición literal, del que sólo se ofrecen dos casos y se explica por sí solo (en el mismo documento se insinúa su simplicidad), el así llamado "sistema de cuadrícula" se refiere, sin duda, al modelo general de sustitución polialfabética basado en una matriz de alfabetos alineados conforme a determinada convención, a menudo deslizándose mutuamente una cantidad calculada de lugares; modelos clásicos son el de Alberti y el Belaso-Vigenère.[22]

Ahora, el sistema denominado de "combinación inglesa" es también clasificable, genéricamente, entre los de "cuadrícula". Pero se comprende mejor al tratarlo como una variedad de las *cifras geométricas*, tal y como las ha explicado, por ejemplo, Helen Gaines.[23] La transformación se gobierna con una clave numérica que se deriva de un término específicamente seleccionado, o bien inventado.

Para guiar la explicación criptoanalítica, examinemos los ejercicios de Urquidi y Pesqueira en los borradores de un intercambio de mensajes entre ellos (figuras 19 y 20).[24] De entre las 12 claves enlistadas en el oficio de referencia, nuestros corresponsales usaron HIMPOSTURA. Para formar la clave concreta

[22] Muchos políticos y diplomáticos mexicanos usaron variaciones de este criptosistema durante la década de 1920; véase, por ejemplo, Narváez, *Criptografía diplomática*, pp. 330-346.
[23] Gaines, *Cryptanalysis*, cap. IV. Hitt, *Manual for the solution*, pp. 26-29.
[24] AHCCIF, RMII-1-0116-I, ff. 114, 116.

de encriptación en este caso, asignaron números a cada letra según su lugar progresivo, de izquierda a derecha, en el alfabeto regular de la lengua española; así, a la A le tocó el 1, a la H el 2, a la I el 3, a la M el 4, y así hasta la U=10. Como se ve, la clave es de extensión 10, y como faltan hasta 17 letras del alfabeto común español, a la primera reconocible en la progresión, A, le siguen necesariamente la H y la I, en ausencia de B, C, D, E, F y G. Y como faltan asimismo la J, K y L, a la I le sigue la M, y así hasta la U, donde la numeración se detiene por obvia condición aritmética.

La clave numérica resultante es, pues, 2-3-4-6-5-8-9-10-7-1. El texto del mensaje a cifrar se escribe en orden normal debajo de estos números, sin contar espacios entre palabras; al llegar a una décima letra, se desciende un renglón y continúa el escrito. Procediendo así con el resto del mensaje hasta el final, aparece un bloque de letras cuya interpretación criptográfica *debe ser por columnas de arriba abajo, y no por líneas en cualquier dirección*. Es de observar que, como muestran los ejemplos, algunos fragmentos quedan sin cifrar. Los números de la clave no marcan sino el orden en que se inscribirán esas columnas para formar, propiamente, el criptograma a remitir telegráficamente o por correo postal. Esto muestra que HIMPOSTURA y las demás claves en el oficio de referencia, cuando han de funcionar por "combinación inglesa", son tan solo una máscara del verdadero algoritmo para encriptar: una *transposición de columnas*. En este sentido, es manifiesto que la transposición es un aspecto formal de primer orden en este tipo de métodos. Por esta y otras razones criptoanalíticas, la clave AGENTES, a pesar de tener una letra repetida, sí podría operar en los sistemas de "cuadrícula" y "combinación inglesa",[25] y en este último mediante un expediente básico: la A contaría como 1, por supuesto, pero la E, al seguirla en orden de aparición progresiva pero figurar dos veces,

[25] Contra lo indicado en el oficio, véase la figura 17.

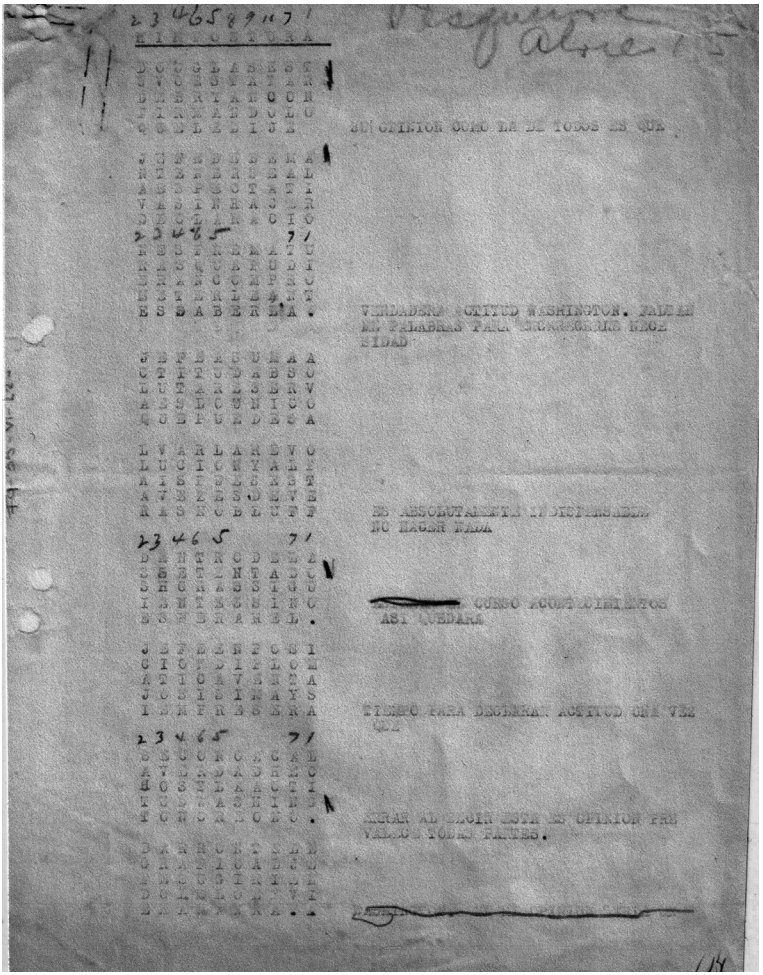
tendría los números 2 y 3 en dirección izquierda a derecha, y al cabo el efecto de encriptación ya explicado sería el mismo.[26]

Para facilitar la intelección del mensaje preparado por Pesqueira para enviar a Urquidi (figura 19), lo presentaré más abajo extendido, por así decir, y no en bloques. El texto se reproduce sin modificaciones ortográficas, gramaticales o de puntuación. Los elementos de lectura conjetural o ilegibles se sitúan entre corchetes. Las partes en negritas aparecen originalmente en texto plano:

DOUGLAS ESTUVO ESTA TARDE BRYAN CONFIRMANDOLO QUE LE DIJE **SU OPINION COMO LA DE TODOS ES QUE** JEFE DEBE MANTENERSE A LA ESPECTATIVA SIN HACER DECLARACIONES PREMATURAS QUE PUDIERAN COMPROMETERLE ANTES SABER LA **VERDADERA ACTITUD WASHINGTON. FALTANME PALABRAS PARA ENCARECERLE NECESIDAD** JEFE ASUMA ACTITUD ABSOLUTA RESERVA ES LO UNICO QUE PUEDE SALVAR LA REVOLUCION Y AL PAIS PUES ESTA VEZ ES DE VERAS NO BLUFF [*SIC* EN INGLÉS: HABLADURÍA] **ES ABSOLUTAMENTE INDISPENSABLE NO HACER NADA** DENTRO DE LAS SETENTA DOS HORAS SIGUIENTES SI NO ESPERAR EL **CURSO ACONTECIMIENTOS ASÍ QUEDARA** JEFE EN POSICIÓN DIPLOMATICA VENTAJOSISIMA Y SIEMPRE SERA **TIEMPO PARA DECLARAR ACTITUD UNA VEZ QUE** SE CONOZCA LA VERDAD HECHOS Y LA ACTITUD WASHINGTON CREO NO **ERRAR AL DECIR ESTA ES OPINION PREVALECE TODAS PARTES.** BARRON [TELEGRAFIA AL] JEFE SUGIRIENDOLE LO ENVIEN A… [ILEGIBLE] [*TACHADO AL MARGEN IZQUIERDO*] USA TEMEMOS MUY SERIAS COMPLICACIONES ALEGASE CAÑONEROS **DESTRUYERON PROPIEDADES EXTRANGEROS** SIN CAUSA JUSTIFICADA HABLASE MUCHO POSIBLE BLOQUEO PARA **IMPEDIR CAÑONEROS CONTINUAR** HACIENDO FUEGO HOY HAB[R]A JUNTA MINISTROS CON LIND MEDIODÍA

[26] Con todo, en estos casos era técnicamente preferible que la clave no tuviera elementos repetidos, a fin de volver más difícil todo intento de recuperarla mediante un análisis de frecuencias relativas o de otro tipo. Por otra parte, también era posible asignar la numeración yendo de derecha a izquierda, aunque esto no prevendría la repetición de algunos caracteres crípticos.

Figura 19



CONSIDERASE GENERALMENTE INCIDENTE PUEDE DETERMINAR CRISIS HASTA AHORA HUERTA REHUSA ACCEDER [*ILEGIBLE*] INCIDENTE TAMPUCO [*SIC* TAMPICO] COMIENZA REVERTIR GRAVES CARACTERES LA **ACTITUD ALMIRANTE MAYO FUERTEMENTE** SOSTENIDA WILSON GOBIERNO EXIGE SALUDO BANDERA LA DEMANDA **PARECE JUSTA CONFORME LEYES NACIONES.** SEGÚN ABOGADOS Y LA OPINIÓN PUBLICA LA RECLAMA SI HUERTA REH **XXXXXX**

Veamos ahora un arreglo especial de los primeros tres bloques (quince renglones numerados de caracteres a cifrar) de la "combinación" para destacar el pareo entre la clave numérica y la palabra clave.

Clave numérica:	*2*	*3*	*4*	*6*	*5*	*8*	*9*	*10*	*7*	*1*	Elementos que se dejan sin cifrar
Palabra clave:	**H**	**I**	**M**	**P**	**O**	**S**	**T**	**U**	**R**	**A**	
Renglón - 1	D	O	U	G	L	A	S	E	S	T	
R - 2	U	V	O	E	S	T	A	T	A	R	
R - 3	D	E	B	R	Y	A	N	C	O	N	
R - 4	E	I	R	M	A	N	D	O	L	O	
R - 5	Q	U	E	L	E	D	I	J	E		**SU OPINIÓN COMO LA DE TODOS ES QUE**
R - 6	J	E	F	E	D	E	B	E	M	A	
R - 7	N	T	E	N	E	R	S	E	A	L	
R - 8	A	E	S	P	E	C	T	A	T	I	
R - 9	V	A	S	I	N	H	A	C	E	R	
R - 10	D	E	C	L	A	R	A	C	I	O	
R - 11	N	E	S	P	R	E	M	A	T	U	
R - 12	R	A	S	Q	U	E	P	U	D	I	
R - 13	E	R	A	N	C	O	M	P	R	O	
R - 14	M	E	T	E	R	L	E	A	N	T	
R - 15	E	S	S	A	B	E	R	L	A	.	**VERDADERA ACTITUD WASHINGTON. FALTANME PALABRAS PARA ENCARECERLE NECESIDAD [...]**

Conforme a la regla de transposición por columnas como paso final de encriptación, estos bloques quedarían cifrados así:

TRNO. DUDEQ OVEIU UOBRE LSYAE GERML SAOLE ATAND SANDI ETCOJ ALIRO JNAVD ETEAE FESSC DEENA ENPIL MATEI ERCHR BSTAA EEACC UIOT. NREME EARES SSATS RUCRB PQNEA TDRNA EEOLE MPMER AUPAL [...]

A continuación, tenemos la respuesta que Urquidi preparó para su compañero de la Agencia Confidencial (figura 20). Se transcribe de forma extendida, o sea, previa al cifrado. Notar que las tres líneas finales en texto abierto, dado su contenido, no podían estar planeadas para incorporarse al criptotexto. De nuevo, las partes a dejar en texto plano en el telegrama van en negritas.

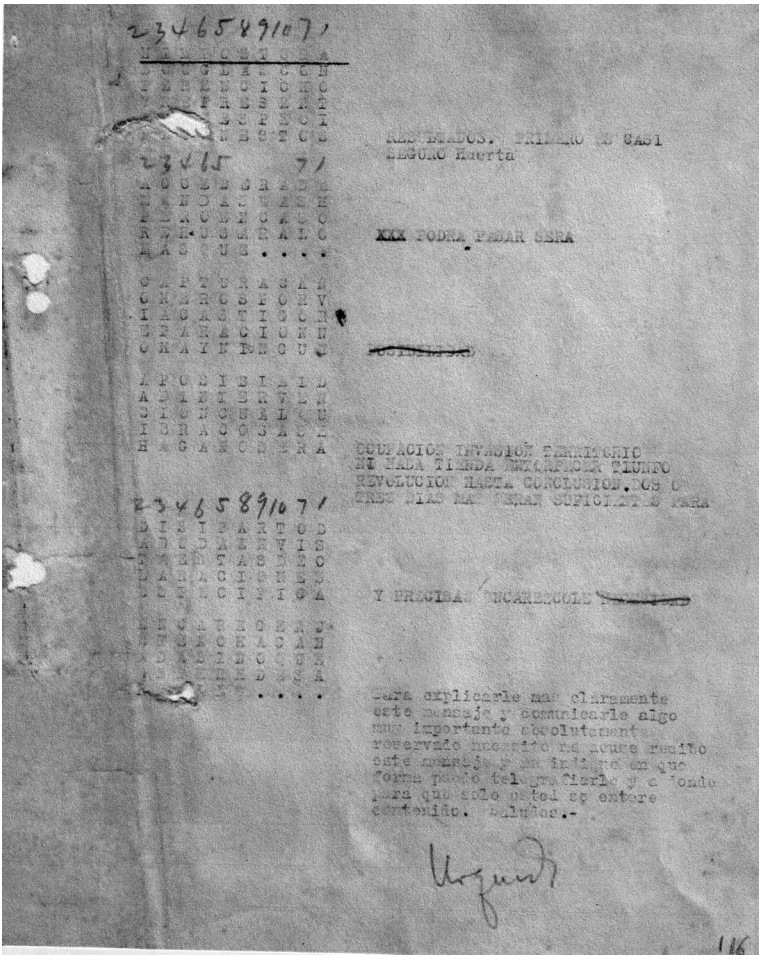
DOUGLAS CONFERENCIO HOY REPRESENTANTE ESPECIAL CON ESTOS **RESULTADOS. PRIMERO ES CASI SEGURO HUERTA** ACCEDERA A DEMANDAS WASH [INGTON], PERO EN CASO REHUSARA LO MAS QUE **PODRA PASAR SERA** CAPTURA CANONEROS [*SIC* CAÑONEROS] POR VIA CASTIGO REPARACION NO HAY NINGUNA POSIBILIDAD INTERVENCION CUALQUIERA COSA SE HAGA NO SERÁ **OCUPACIÓN INVASIÓN TERRITORIO NI NADA TIENDA ENTORPECER TRIUNFO REVOLUCIÓN HASTA CONCLUSIÓN. DOS O TRES DIAS MAS SERAN SUFICIENTES PARA** DISIPAR TODA DUDA EN VISTA ESTAS DECLARACIONES ESPECIFICA [SIC] **Y PRECISAS ENCAREZCOLE** ENCARECER JEFE NO HAGA NADA SINO QUE ESPERE DESARROLLO...

Para explicarle más claramente este mensaje y comunicarle algo muy importante absolutamente reservado necesito me acuse recibo este mensaje y me indique en qué forma puedo telegrafiarle y a dónde para que sólo usted se entere contenido. Saludos.

Urquidi [autógrafo]

Y aquí también, como en el caso de la "combinación" de Pesqueira, presentamos un arreglo especial de los primeros

Figura 20



tres bloques para resaltar el pareo jerárquico de las dos claves operativas:

Clave numérica	*2*	*3*	*4*	*6*	*5*	*8*	*9*	*10*	*7*	*1*	Elementos que se dejan sin cifrar
Palabra clave	**H**	**I**	**M**	**P**	**O**	**S**	**T**	**U**	**R**	**A**	
R - 1	D	O	U	G	L	A	S	C	O	N	
R - 2	F	E	R	E	N	C	I	O	H	O	
R - 3	Y	R	E	P	R	E	S	E	N	T	
R - 4	A	N	T	E	E	S	P	E	C	I	
R - 5	A	L	C	O	N	E	S	T	O	S	**Resultados. Primero, es casi seguro Huerta**
R - 6	A	C	C	E	D	E	R	A	D	E	
R - 7	M	A	N	D	A	S	W	A	S	H	
R - 8	P	E	R	O	E	N	C	A	S	O	
R - 9	R	E	H	U	S	A	R	A	L	O	
R - 10	M	A	S	Q	U	E					**Podrá pasar será**
R - 11	C	A	O	T	U	R	A	C	A	N	
R - 12	O	N	E	R	O	S	P	O	R	V	
R - 13	I	A	C	A	S	T	I	G	O	R	
R - 14	E	P	A	R	A	C	I	O	N	N	
R - 15	O	H	A	Y	N	I	N	G	U	N	[…]

Estas quince líneas quedarían cifradas como sigue para la transmisión telegráfica:

NOTIS DFYAA OERNL URETC LNREN GEPEO OHNCO ACESE SISPS COEET EHOO. AMPRM CAEEA CNRHS DAESU EDOUQ DSSL. ESNAE RWCR. AAAA. NVRNN COIEO ANAPH OECAA UOSAN TRARY ARONU RSTCI APIIN COGOG […]

SIGLAS Y REFERENCIAS

AHGE Archivo Histórico Genaro Estrada, Ciudad de México, México.

AHCCIF Archivo Histórico del Centro Cultural Isidro Fabela-Museo Casa del Risco, Ciudad de México, México.

AA. VV., *Diccionario de generales de la Revolución Mexicana*, México, Instituto Nacional de Estudios Históricos de las Revoluciones de México, 2014, 2 tomos.

Barragán Rodríguez, Juan, *Historia del ejército constitucionalista*, México, Instituto Nacional de Estudios Históricos de las Revoluciones de México, 2013.

Fabela, Isidro, *Historia diplomática de la revolución mexicana*, t. II *(1912-1917)*, México, Buenos Aires, Fondo de Cultura Económica, 1959.

Gaines, Helen F., *Cryptanalysis. A Study of Ciphers and Their Solution*, Nueva York, Dover, 1956.

Hitt, Parker, *Manual for the Solution of Military Ciphers*, Kansas, Fort Leavenworth, Press of the Army Service Schools, 1916.

Madero, Francisco I., *Archivo de Don Francisco I. Madero. Epistolario* (ed., introducción, edición y notas de Roberto R. Narváez), México, Instituto Nacional de Estudios Históricos de las Revoluciones de México, 2012 (1ª edición electrónica corregida), 2 tomos.

Narváez, Roberto R., *Criptografía diplomática, política y militar en México, 1813-1926*, México, Secretaría de Relaciones Exteriores, Acervo Histórico Diplomático, 2019.

Romero Flores, Jesús, *Historia del Congreso Constituyente, 1916-1917*, México, Secretaría de Cultura, Universidad Nacional Autónoma de México, Instituto Nacional de Estudios Históricos de las Revoluciones de México, 2014.