ARCHIVOS Y DOCUMENTOS

ALGUNOS EJEMPLOS DE CRIPTOGRAFÍA MILITAR MEXICANA (1860-1879)

Roberto Narváez
Universidad Nacional Autónoma de México

En el Archivo Histórico de la Secretaría de la Defensa Nacional (AHSEDENA) se resguardan varios expedientes de documentos parcial o totalmente encriptados por medio del cifrado, la codificación, o una mezcla de estos dos métodos.[1] En esta contribución examinaré, con el apoyo del criptoanálisis (acaso el modelo más iluminador y fecundo para cultivar el razonamiento hipotético en la investigación histórica), las propiedades técnicas, formales y estructurales y el nivel de seguridad en una serie de telegramas facturados por militares mexicanos entre 1860 y 1879, en los cuales se aprecia el recurso a diferentes criptosistemas con la obvia meta de obstaculizar su interpretación automática si por cualquier incidencia, durante la transmisión, caían en manos de lectores no autorizados. Entre tales legajos crípticos abundan los que carecen de versión en texto plano (esto es, inmediatamente legible) o siquiera de materiales correlativos cuya inspección

[1] Toda la documentación examinada para este artículo se puede localizar también en el sitio web http://www.archivohistorico2010.sedena.gob.mx/ (último acceso: julio de 2014).

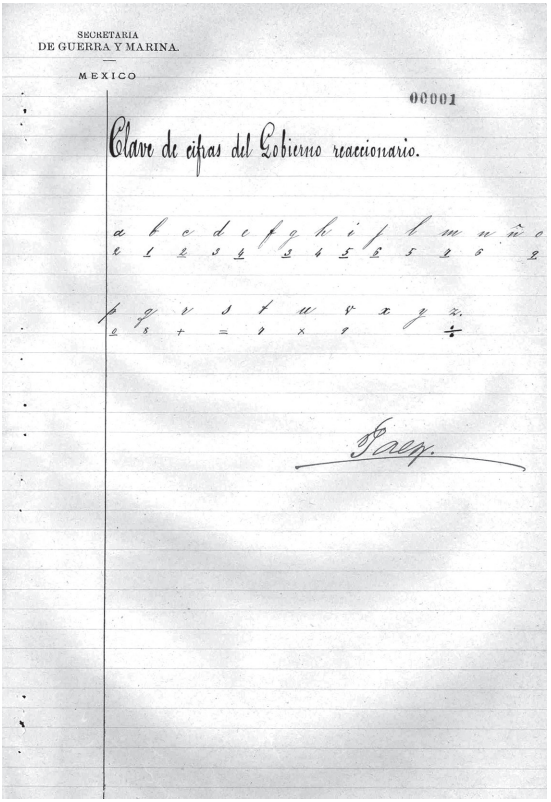
crítica podría inspirar conjeturas acerca de sus contenidos originales en lenguaje abierto. Sin embargo, he conseguido decriptar —es decir, exhumar la escritura inteligible sin conocer el criptosistema utilizado, pues la descripción de estos métodos generalmente no consta en el AHSEDENA— un porcentaje importante, deduciendo además, por consecuencia criptológica, los esquemas de encriptación que sirvieron (probablemente) para generarlos. Aquí presentaré una selección de estos logros criptoanalíticos, de manera que puedan ser analizados, criticados y, eventualmente, manejados como evidencia por historiadores militares, de la lingüística, las comunicaciones y disciplinas afines, así como, por supuesto, de la criptología mexicana y general.

UN CRIPTOSISTEMA EMPLEADO DURANTE LA PRESIDENCIA DE MIGUEL MIRAMÓN (1860)

El expediente 7621, titulado "Operaciones militares. Año de 1860", resulta de singular interés porque incluye la descripción completa de un criptosistema, lo cual de ningún modo es la norma en el AHSEDENA, según lo expresé líneas arriba. Denominado "Clave de cifras del Gobierno reaccionario", va seguido de tres documentos cifrados por su medio y las correspondientes versiones en texto plano. Actualmente hablamos de criptosistema y no de clave para fomentar la propiedad terminológica que conviene al buen empleo de las herramientas y conceptos criptológicos, pero desde la perspectiva histórica es importante recordar que en el siglo XIX la costumbre dictaba referirse genéricamente como "claves" tanto a cualquier pieza redactada en cifra o código como a los diferentes métodos criptográficos o codificadores.

Dicha "Clave de cifras" está conformada por un alfabeto de definición de 25 elementos y un alfabeto de cifrado de la misma extensión (imagen 1), dejando de manifiesto de golpe que se trata de un criptosistema monoalfabético de sustitución 1 a 1.

Imagen 1

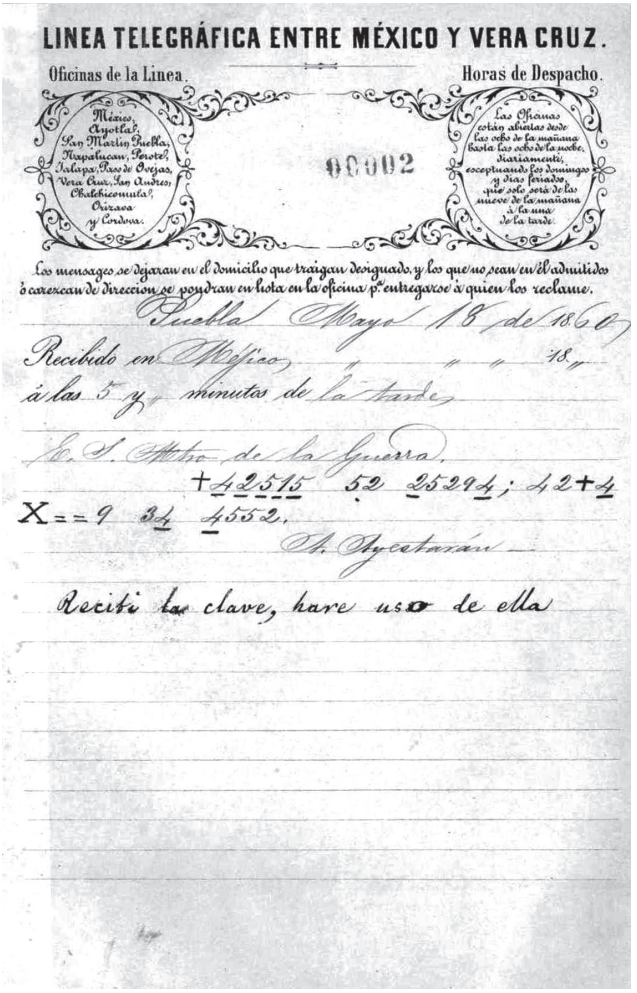


"Clave de cifras del Gobierno reaccionario" (1860).
Fuente: AHSEDENA, exp. 7621, f. 1.

Como vemos, carece de elementos codificadores —esto es, la transformación se realiza en el nivel sintáctico exclusivamente— y de signos nulos (caracteres sin equivalencia que se añaden como "ruido" para desanimar a quien pretende romper la cifra sin autorización), aunque se aprecia la inteligencia criptográfica del diseñador al no proveer sustitutos para letras poco frecuentes (X, Y) o convertibles a otras por similitud gráfica o fonética (la Ñ en N). No se prescriben caracteres de sustitución para signos de puntuación, espacios entre palabras u otros factores de valoración sintáctica o gramatical. En el alfabeto de la cifra participan los números arábigos del 0 al 9 y los signos matemáticos +, =, ×, y ÷. Todos los guarismos salvo el cero aparecen dos veces, una de ellas encima de una línea. Cada guarismo puede ocultar hasta dos letras (exceptuando la X, la Y y la Ñ), a una sin el subrayado y a la otra, con él. Semejante auxiliar de la escritura constituye la única providencia que el creador de esta "clave" incorporó con el propósito de repeler el análisis de frecuencias relativas, quizá el método de "ataque" —para decirlo en el argot criptoanalítico— más comúnmente utilizado contra cifras en que la observación recurrente de caracteres individuales o en grupo sugiere como conjetura elemental el uso de uno o varios alfabetos en esquemas transformadores de diversas clases. El único hecho cierto es que la fragilidad del sistema está garantizada por su estructura monoalfabética.

Un primer ejemplo de aplicación lo tenemos en el siguiente telegrama (imagen 2) enviado desde Puebla por el general Antonio Ayestarán el 18 de mayo de 1860:

Imagen 2


LINEA TELEGRÁFICA ENTRE MÉXICO Y VERA CRUZ.

Oficinas de la Linea. Horas de Despacho.

México, Azotla, San Martin, Puebla, Acapulcan, Tezote, Jalapa, Paso de Ovejas, Vera Cruz, San Andres, Chalchicomula, Orizava y Cordova.

00002

Las Oficinas estan abiertas desde las ocho de la mañana hasta las ocho de la noche, diariamente, exceptuando los domingos y dias feriados, que solo serán de las nueve de la mañana á la una de la tarde.

Los mensages se dejaran en el domicilio que traigan designado, y los que no sean en él admitidos ó carezcan de direccion se pondran en lista en la oficina p.a entregarse á quien los reclame.

Puebla Mayo 18 de 1860

Recibido en Mexico, " " " 18 "

á las 5 y " minutos de la tarde.

E. S. Ministro de la Guerra.

+42515 52 25294; 42+4

X==9 34 4552.

A. Ayestarán.

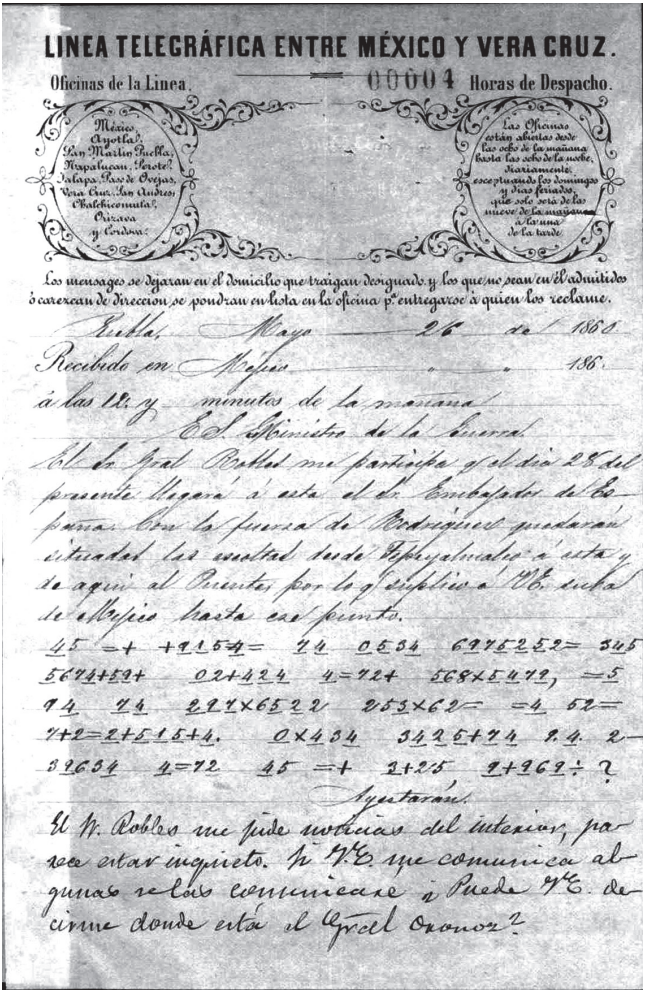
Reciti la clave, hare uso de ella

Telegrama cifrado del general Antonio Ayestarán, 18 de mayo de 1860.
Fuente: AHSEDENA, exp. 7621, f. 2.

El criptoanálisis prueba que la sustitución es de 1 a 1, fija, y se ha cometido un error al inicio de la segunda línea, en donde X==9 se debe leer USSV y no USO, como lo indica el descifrado en la parte inferior de la foja: "Recibí la clave, haré uso de ella". Por otra parte, la observación repetida del 5, el 4 (así subrayado) y el bigrama 52, y la proximidad con que unos y otro aparecen en un mensaje de tan corta longitud, imponen la hipótesis de que su generación debió estar regulada por un criptosistema monoalfabético o por uno polialfabético basado en una clave de extensión ínfima, propiamente de 1, en tanto se supondría que el alfabeto de la cifra se desplazaría no más de un lugar a la derecha o a la izquierda respecto del alfabeto definitorio. Pero no es necesario explorar esta segunda posibilidad más a fondo, pues el registro de archivo muestra, sin lugar a dudas, que la cifra es monoalfabética.

En la imagen 3 apreciamos otro telegrama encriptado con el mismo método:

Imagen 3


LINEA TELEGRÁFICA ENTRE MÉXICO Y VERA CRUZ.

Oficinas de la Linea. 00004 Horas de Despacho.

México, Ayotla, San Martin Puebla, Nopalucan, Tlaxcala, Jalapa, Paso de Ovejas, Vera Cruz, San Andres, Chalchicomula, Orizava y Cordova.

Las Oficinas estan abiertas desde las ocho de la mañana hasta las ocho de la noche, ordinariamente; exceptuando los domingos y dias feriados, que solo serán de las nueve de la mañana á la una de la tarde.

Los mensages se dejaran en el domicilio que traigan designado y los que no traigan en él admitidos ó carezcan de direccion se pondran en lista en la oficina p.ª entregarse á quien los reclame.

Puebla Mayo 26 de 1860

Recibido en Méjico . . 186

á las 12 y minutos de la mañana

Al Sr. Ministro de la Guerra.

El Sr. Gral Robles me participa q. el dia 25 del presente llegará á esta el Sr. Embajador de España con la fuerza de Rodriguez: q. quedarán situados los cuerpos desde Tepeyahualco á esta y de aquí al Puente, por lo q. suplico á V.E. cuide de dejarlos hasta ese punto.

45 =+ +9154= 74 0534 6276252= 345 5674+534 024424 4=724 568×5472, =5 94 74 2274×6522 253×62= =4 52= 7+2=2+5154. 0×434 3425+74 8.4. 2= 39634 4=72 45 =+ 2+25 9+9629÷ ?

Ayestarán.

El Sr. Robles me pide noticias del interior, parece estar inquieto. Si V.E. que comunica algunas se las comunicare á Puede V.E. decirme donde está el Gral Oronoz?

Telegrama cifrado del general Antonio Ayestarán, 26 de mayo de 1860.
Fuente: AHSEDENA, exp. 7621, f. 4.

El documento está firmado por el mismo general Ayestarán. Es interesante observar que, en el descifrado, aparece la abreviatura "Gral." Quien asumiera, desconociendo el criptosistema mostrado en la imagen 1, que en el criptograma debió incluirse tal braquigrafía, daría muestras de una genuina sagacidad criptológica, pues no es infrecuente el cifrado de palabras o frases contraídas por cualquier medio, sin embargo, lo ideal sería que desarrollara su criptoanálisis sobre el criptotexto tal y como aparece, sin adelantar predicciones hipotéticas. Cuando terminara (y no le tomaría demasiado tiempo, dada la vulnerabilidad del ejemplar) podría comparar su resultado con el descifrado oficial, por así llamarlo, y darse cuenta entonces de que el grupo "Gral." ha sido encriptado, en efecto, como 3+25.

PECULIARIDADES DE CIFRADO MONOALFABÉTICO EN SEIS TELEGRAMAS MILITARES

La carpeta 9288 lleva por título "Telegramas en cifras cuya traducción se ignora" del periodo 1869-1872. Reúne 18 telegramas con informes de actividades remitidos por ocho jefes militares desde diferentes ciudades a la capital del país. De este total conseguí decriptar 16 y entregué los resultados al Archivo Histórico de la SEDENA (7 de diciembre de 2013), como un modesto tributo al Ejército Mexicano por la celebración de su primer centenario.[2] En esta ocasión, por limitaciones de espacio, presentaré las versiones aclaradas de

[2] La Dirección General de Archivo e Historia de la SEDENA me expresó su gratitud a través del oficio núm. S. H.-275, fechado el 5 de febrero de 2014.

seis telegramas en esa muestra, describiendo sucintamente la metodología que me facilitó inferir la clase de los criptosistemas utilizados en cada caso.

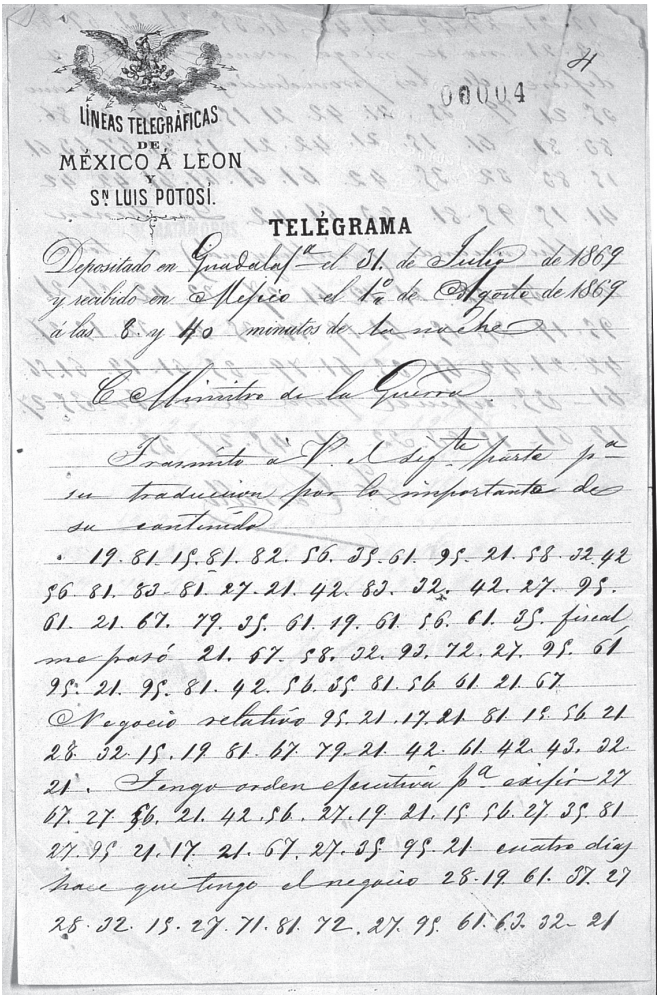
Se trata, en general, de cifras de sustitución con pretensiones polialfabéticas, que en realidad se basan en el empleo de sustituciones a partir de un alfabeto único. La estrategia para proteger contra el análisis de frecuencias consistió en asignar dos y hasta tres pares de números arábigos como equivalentes de las letras de uso más frecuente en español, casos de las cinco vocales y de las N, R, S y T. Se denomina técnicamente sustitutos homofónicos a tales equivalencias, y funcionan exactamente según las prescripciones de Simeone de Crema para un criptosistema de 1401.[3] Cada grupo críptico está separado por un punto. Al parecer, la elección de los guarismos respondió al mero capricho, pues no es evidente que se haya establecido algún criterio de progresión ascendente o descendente. No se han agregado signos con función de nulos.

Criptosistema del coronel José de Jesús Carrillo

Este coronel firma, entre otros, el siguiente par de telegramas (imágenes 4, 5 y 6):

[3] Mendelsohn, "Blaise de Vigenere", pp. 114-115. Una diferencia es que De Crema introdujo tanto números como símbolos esteganográficos para las sustituciones homofónicas.

Imagen 4


LÍNEAS TELEGRÁFICAS
DE
MÉXICO Á LEON
Y
Sn LUIS POTOSÍ.

H

00004

TELÉGRAMA

Depositado en Guadalaxa el 31. de Julio de 1869
y recibido en Mexico el 1º de Agosto de 1869
á las 8. y 40 minutos de la noche

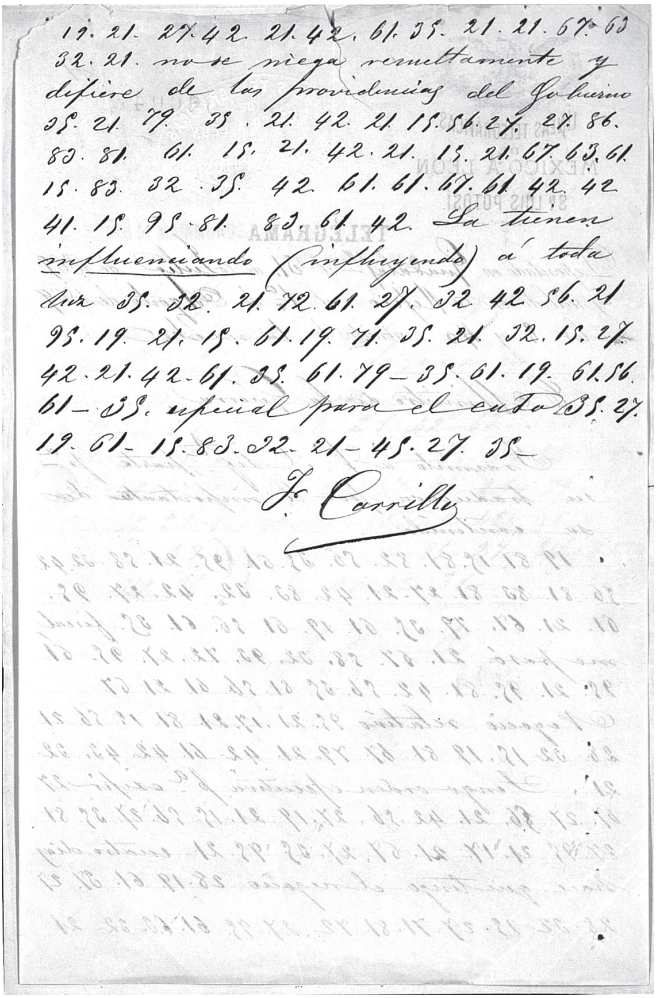
C. Ministro de la Guerra.

Trasmito á V. el dep.te parte p.a
su traduccion por lo importante de
su contenido

19. 81. 15. 81. 82. 56. 35. 61. 95. 21. 58. 32. 42
56. 81. 33. 81. 27. 21. 42. 83. 32. 42. 27. 95.
61. 21. 67. 79. 35. 61. 19. 61. 56. 61. 25. final
me paró 21. 67. 58. 32. 93. 72. 27. 95. 61
95. 21. 95. 81. 42. 56. 35. 81. 56 61 21. 67
Negocio relativo 95. 21. 17. 21. 81. 19. 56. 21
28. 32. 15. 19. 81. 67. 79. 21. 42. 61. 42. 43. 32
21. Tengo orden ejecutiva p.a existir 27
67. 27. 56. 21. 42. 56. 27. 19. 21. 15. 56. 27. 35. 81
27. 95. 21. 17. 21. 67. 27. 35. 95. 21 cuatro dias
hace que tengo el negocio 28. 19. 61. 37. 27
28. 32. 15. 27. 71. 81. 72. 27. 95. 61. 63. 32. 21

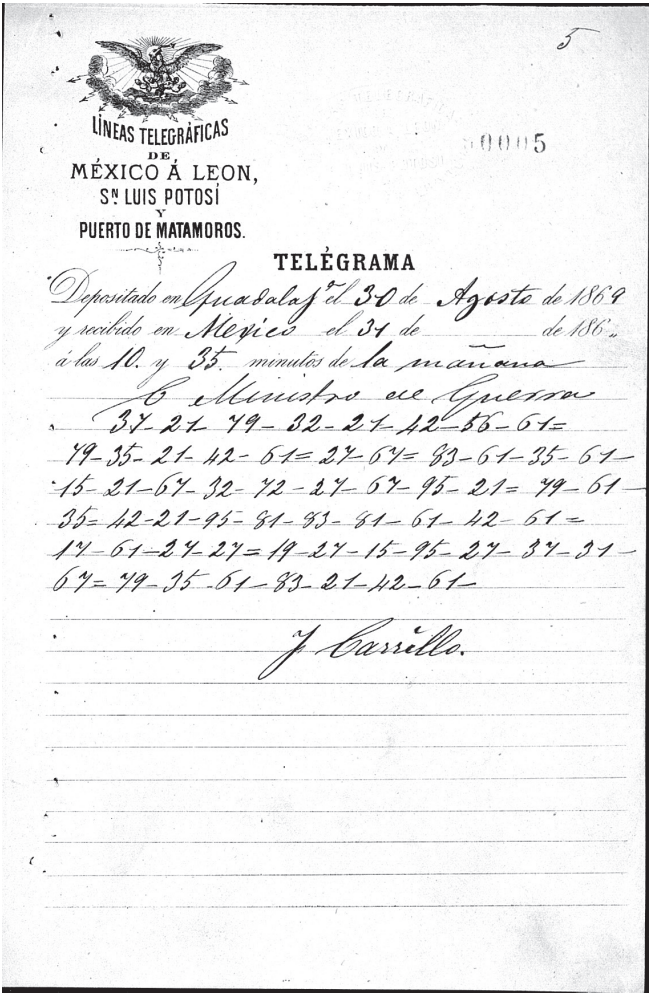
Telegrama cifrado del coronel José de Jesús Carrillo, 31 de julio de 1869.
Fuente: AHSEDENA, exp. 9288, f. 4r.

Imagen 5



Telegrama cifrado del coronel José de Jesús Carrillo, 31 de julio de 1869.
Fuente: AHSEDENA, exp. 9288, f. 4v.

Imagen 6


LÍNEAS TELEGRÁFICAS
DE
MÉXICO Á LEON,
Sn LUIS POTOSÍ
Y
PUERTO DE MATAMOROS.

5

TELÉGRAMA

Depositado en Guadalaj el 30 de Agosto de 1869
y recibido en Mexico el 31 de ____ de 186_
á las 10. y 35. minutos de la mañana

Al Ministro de Guerra

37-27-79-32-27-42-56-61=
79-35-21-42-61=27-67=93-61-35-61-
15-21-67-32-72-27-67-95-21=79-61-
35-42-21-95-31-93-81-61-42-61=
17-61-24-27=19-27-15-95-27-37-31-
67=79-35-61-93-21-42-61-

J. Carrillo.

Telegrama cifrado del coronel José de Jesús Carrillo, 30 de agosto de 1869.
Fuente: AHSEDENA, exp. 9288, f. 5.

Para descubrir el monoalfabetismo en estos especímenes, conviene reparar en la aparición recurrente de varios números agrupados y considerar lo que sabemos acerca de la frecuencia relativa de bigramas, trigramas y conjuntos mayores de letras en nuestra lengua.[4] Si revisamos, por ejemplo, el telegrama enviado desde Guadalajara el 31 de julio de 1869, nos damos cuenta de que el grupo 63.32.21 aparece dos veces, la primera al calce de la foja 4 r. y la segunda, al final de la primera línea en la foja 4 v. Ahora, en el idioma español es inevitable que se forme por lo menos un bigrama partiendo de la Q, pues esta letra siempre va seguida de U; podemos conjeturar, entonces, que 63.32 vale por QU. Y si reparamos, además, en que el 21 tiene una frecuencia magna en toda la pieza bajo estudio, al grado de aparecer por lo menos una vez cada dos renglones, podemos concederle, probatoriamente, una equivalencia por cualquier vocal excepto U, ya que ésta nunca compone un trigrama significativo en sociedad con cualquier consonante.[5] Tampoco la A y la O son candidatas promisorias, como lo indica la falta de voces en el diccionario que inician con QUA o QUO. Restan la E y la I. Ensayando con estas grafías, pronto eliminamos la combinación con la I para quedarnos con la equivalencia definitiva 63.32.21 = QUE, válida por su congruencia con los elementos anteriores y posteriores para formar una oración reconocible. En este mismo telegrama, el conjunto 63.32.21, en su primera aparición, va seguido por 19.21.27.42.21.42.61.35.21.21.67.63.32.21, todo lo cual, una

[4] Ortega Triguero, López Guerrero *et al*., *Introducción a la criptografía*, p. 32.
[5] Hitt, *Manual for the Solution*, p. 10.

vez decriptado, reza QUE ME ASESORE EL QUE (nótese como el .21. aparece 5 veces en esta breve cadena críptica, remarcando el hecho de que la E representa la letra de frecuencia máxima en esta muestra particular).

Procediendo con este mismo tipo de análisis sobre las demás unidades numéricas y aprovechando, además, las palabras o frases en texto plano intercaladas por todo el manuscrito (ventaja rara vez disponible al criptoanalista) para predecir soluciones gramaticales apropiadas en la redacción, pude finalmente construir la siguiente tabla de equivalencias, válida para decriptar tanto el telegrama del 31 de julio de 1869 como el próximo en la serie, fechado a 30 de agosto del mismo año.

Texto plano	A	B	C	CH	D	E	F	G	H	I	J	K	L	LL	M
Criptotexto	27	71	83		95	21 31	43	72	37	81	88		67		19

Texto plano	N/Ñ	O	P	Q	R	RR	S	T	U	V	W	X	Y	Z
Criptotexto	15	61	79	63	35	69	42 48	56	32	17		86	28	93

Considerando el tamaño de las muestras analizadas, parece claro que en esta cifra se decidió suprimir la CH, la K y la W, dado su exiguo porcentaje de repetición en el español regular. Sólo la E y la S tienen asignados equivalentes homofónicos; es curioso que no suceda lo mismo con la A, vocal que de ordinario compite con la E por el primer lugar como la más frecuente en muchos idiomas de derivación latina, y también con la R y la N, consonantes que, en composiciones castellanas relativamente grandes, bien pueden superar

a la S en su reaparición estadística. Por otra parte, notar que incluye caracteres numéricos para la RR mas no para la LL, aun cuando ambas letras (hoy en desuso) pueden formarse al yuxtaponer dos R y dos L. Para comentar con el adecuado rigor técnico esta y otras cuestiones, necesitaríamos tener a la vista el criptosistema original.

A continuación presento las versiones en texto plano de los dos telegramas. Las partes descifradas están en cursivas y las fracciones ilegibles se indican con una reticencia entre corchetes.

(F. 4 r. y v.)
Depositado en Guadalaj.a el 31 de Julio de 1869 y recibido en Mexico el 1º de Agosto de 1869 a las 8 y 40 minutos de la noche.

C. Ministro de la guerra
Trasmito a V. C. sig.te parte p.a su traduccion por lo importante de su contenido.
Ministro de justicia escusado el promotor final me pasó *el juzgado de distrito* el Negocio relativo *de veinte y un mil pesos fue*. Tengo orden ejecutiva p.a exijir *a la testamentaria de Velarde* cuatro días hace que tengo el negocio *y mo* [sic] *hay un abigado* [*sic*] *que me asesore el que* no se niega resueltamente y difiere de las providencias del […] *representa axciones* [*sic*] *en el qoncurso* [*sic*] *o los síndicos*. La tienen *influenciando* [subrayado en el original] (influyendo) á toda luz. *Ruego a usted me nombre un asesor promotor* especial para el esta[…] *Ramón Cuéllar*.
J. Carrillo

(F. 5)
Depositado en Guadalaj.a el 30 de Agosto de 1869 y recibido en Mexico el 31 de [Agosto] de 186" a las 10 y 35 minutos de la mañana

C. Ministro de Guerra
He puesto preso al coronel Ugalde por sedicioso. Voa [*sic*] *a mandah* [*sic*] *el proceso.*
J. Carrillo

Criptosistema del general Manuel Larrañaga

Veamos estos tres telegramas en cifra (imágenes 7, 8 y 9) firmados por el general Manuel Larrañaga y remitidos desde San Luis Potosí los días 19, 23 y 24 de septiembre de 1869.

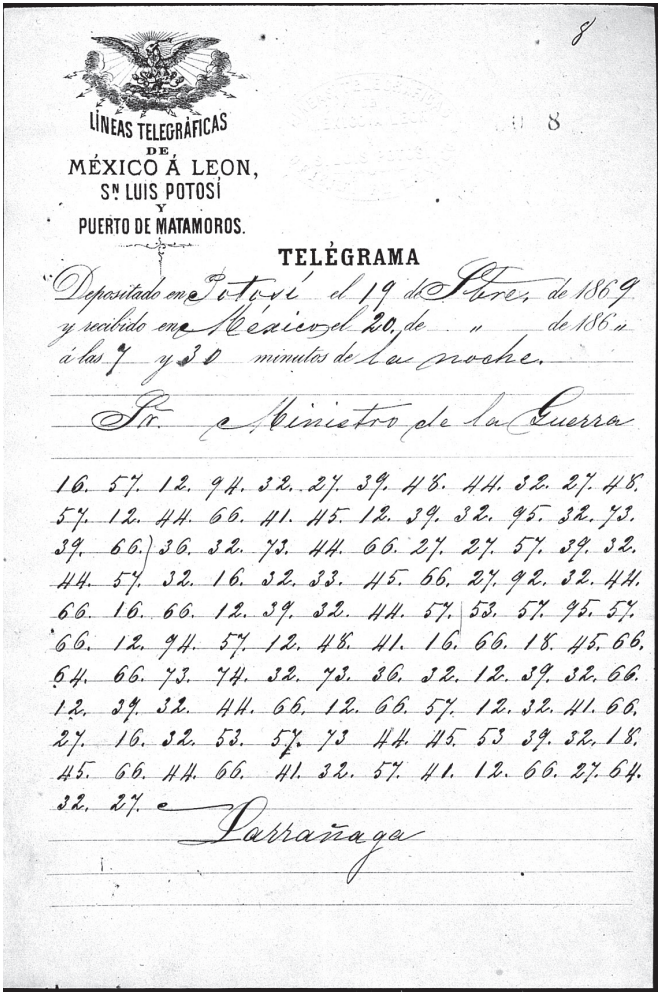
El cifrado también pertenece a la clase de la sustitución monoalfabética. Tiene las mismas características estructurales y propiedades técnicas de funcionamiento que el criptosistema de Carrillo. El telegrama del 19 de septiembre es el único que está encriptado en su totalidad. Enseguida muestro la tabla de sustituciones simples y homofónicas o, para decirlo al estilo decimonónico, la "clave" para decriptar los tres telegramas.

Texto plano	A	B	C	CH	D	E	F	G	H	I	J	K	L	LL	M
Criptotexto	32 22 42	41	53		44	66	33	74	36	48	24		16		95

Texto plano	N	Ñ	O	P	Q	R	RR	S	T	U	V	W	X	Y	Z
Criptotexto	73 74	73	57	94	18	27		12	39	45	64			45 85 86	

Es probable que careciera originalmente de las letras CH, K, W, X y Z por idénticas razones criptográficas a las referidas en el caso de Carrillo. No se identificaron equivalentes

Imagen 7


8

LÍNEAS TELEGRÁFICAS
DE
MÉXICO Á LEON,
Sn. LUIS POTOSÍ
Y
PUERTO DE MATAMOROS.

TELÉGRAMA

Depositado en Potosí el 19 de Setre. de 1869
y recibido en México el 20. de " de 186"
á las 7 y 30 minutos de la noche.

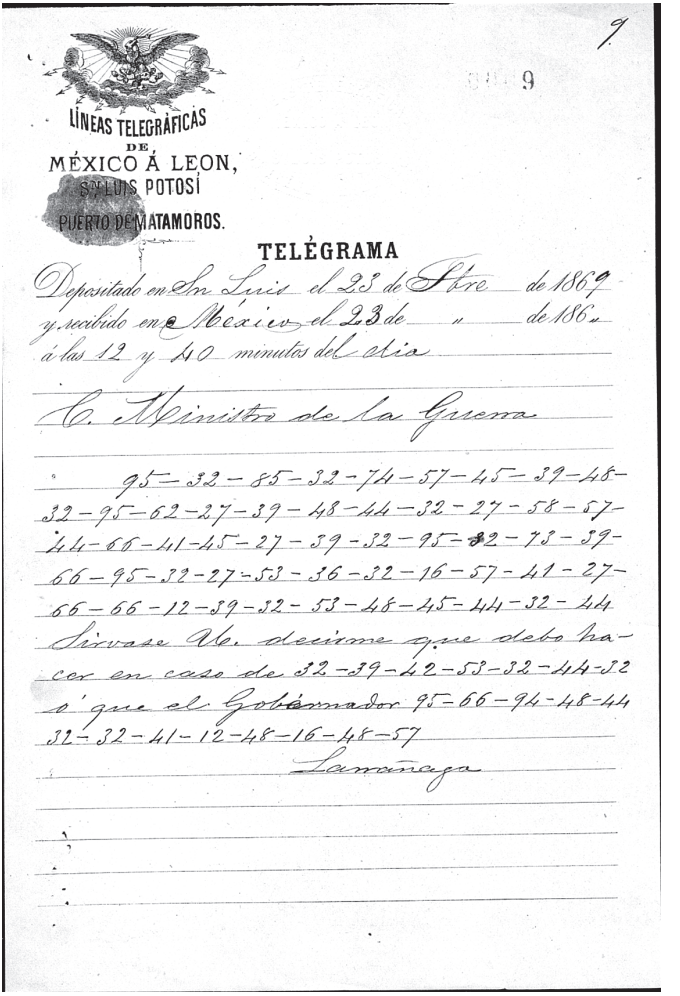
Sr. Ministro de la Guerra

16. 57. 12. 94. 32. 27. 39. 46. 44. 32. 27. 45.
57. 12. 44. 66. 41. 45. 12. 39. 32. 95. 32. 73.
39. 66. 36. 32. 73. 44. 66. 27. 27. 57. 39. 32.
44. 57. 32. 16. 32. 33. 45. 66. 27. 92. 32. 44.
66. 16. 66. 12. 39. 32. 44. 57. 53. 57. 95. 57.
66. 12. 94. 57. 12. 46. 41. 16. 66. 18. 45. 66.
64. 66. 73. 74. 32. 73. 36. 32. 12. 39. 32. 66.
12. 39. 32. 44. 66. 12. 66. 57. 12. 32. 41. 66.
27. 16. 32. 53. 57. 73 44. 45. 53 39. 32. 18.
45. 66. 44. 66. 41. 32. 57. 41. 12. 66. 27. 64.
32. 27.

Larrañaga

Telegrama cifrado del general Manuel Larrañaga, 19 de septiembre de 1869.
Fuente: AHSEDENA, exp. 9288, f. 8.

Imagen 8


LÍNEAS TELEGRÁFICAS
DE
MÉXICO Á LEON,
SAN LUIS POTOSÍ
Y
PUERTO DE MATAMOROS.

9

TELÉGRAMA

Depositado en San Luis el 23 de Sbre de 1869
y recibido en México el 23 de " de 186
á las 12 y 40 minutos del dia

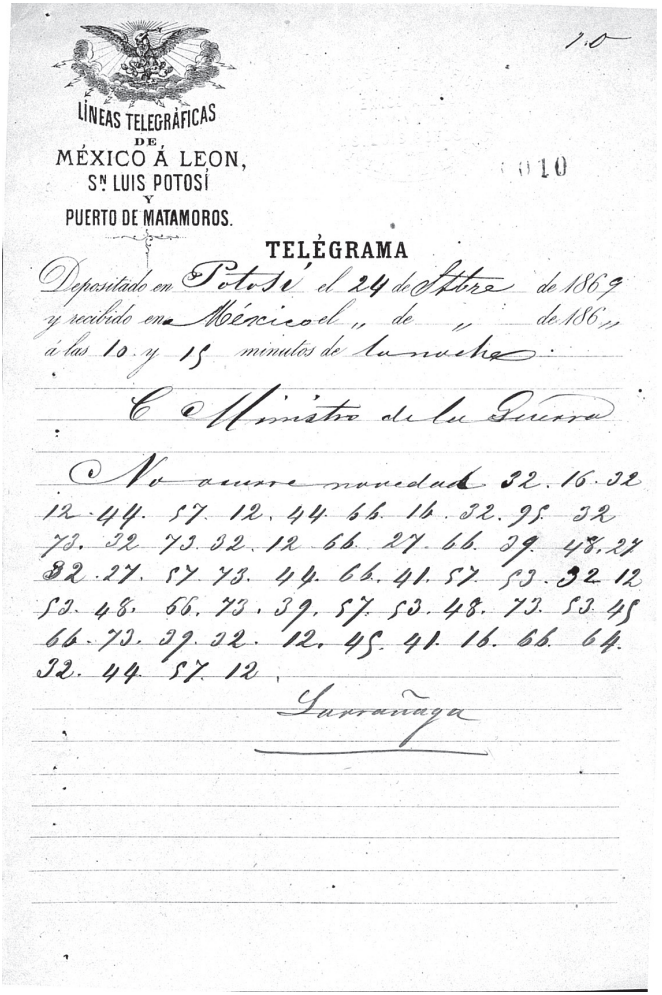
C. Ministro de la Guerra

95-32-85-32-74-57-45-39-48-
32-95-62-27-39-48-44-32-27-58-57-
44-66-41-45-27-39-32-95-82-73-39-
66-95-32-27-53-36-32-16-57-41-27-
66-66-12-89-32-53-48-45-44-32-44
Sírvase V. decirme que debo ha-
cer en caso de 32-39-42-53-32-44-32
á que el Gobernador 95-66-94-48-44
32-32-41-12-48-16-45-57

Larrañaga

Telegrama cifrado del general Manuel Larrañaga, 23 de septiembre de 1869.
Fuente: AHSEDENA, exp. 9288, f. 9.

Imagen 9



Telegrama cifrado del general Manuel Larrañaga, 24 de septiembre de 1869.
Fuente: AHSEDENA, exp. 9288, f. 10.

para la LL y la RR, suponiendo que se las incluyera en el criptosistema original. A diferencia de la tabla de Carrillo, la A presenta múltiples homófonos de sustitución y la E solo uno, mientras que la N tiene dos, el doble que la S. También resulta notable que la E, la O y la I solo tengan un sustituto, mientras que la Y tiene tres (lo cual se explica por la frecuencia de esta conjunción).

Ya podemos, en fin, leer completamente los tres textos en su versión aclarada; las cursivas indican las partes descifradas:

(F. 8)
Depositado en Potosí el 19 de Stbre de 1869 y recibido en México el 20 de "de 1869 a las 7 y 30 minutos de la noche.

Sr. Ministro de la Guerra
Los partidarios de Bustamante han derrotado a la fuerza del estado. Como es posible que vengan hasta ésta, deseo saber la conducta que deba observar.
Larrañaga

(F. 9)
Depositado en Sn Luis el 23 de Stbre de 1869 y recibido en México el 23 de " de 1869 a las 12 y 40 minutos del día.

C. Ministro de la Guerra
Mayagoytia martidario [*sic*] *de Burtamante* [*sic*] *marcha lobre* [*sic*] *esta ciudad*. Sirvase U. decirme que debo hacer en caso de *atacada* ó que el Gobernador *me pida ausilio*.
Larrañaga

(F. 10)
Depositado en Potosí el 24 de Sbre de 1869 y recibido en México el " de " de 186" a las 10 y 15 minutos de la noche.

C. Ministro de la Guerra
No ocurre novedad *a las dos de la mañana se retiraron de Bocas ciento cincuenta sublevados*.
Larrañaga

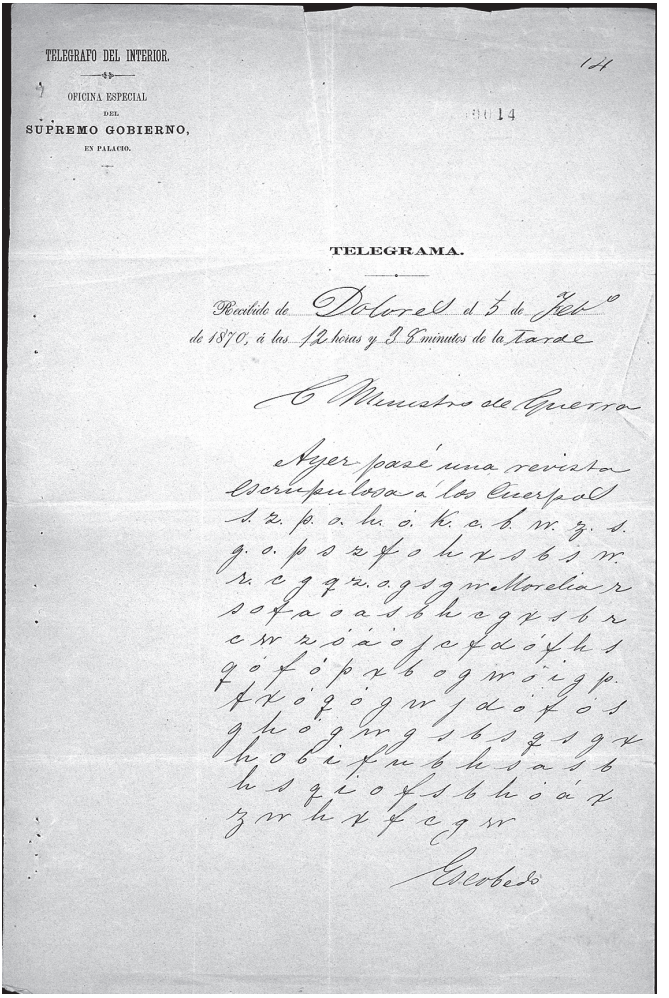
El criptosistema del general Mariano Escobedo

Se deduce por el criptoanálisis de un telegrama en la misma carpeta 9288 (f. 14), firmado y enviado por el general Mariano Escobedo desde Dolores el 5 de febrero de 1870. Encriptado en su práctica totalidad, se distingue en el expediente por ser el único cuyos elementos de cifrado fueron letras y no guarismos, según permite reconocerlo la imagen 10. Dejando aparte tal diferencia, este criptograma comparte con el resto la propiedad de haber sido generado por sustitución monoalfabética.

En este caso, sin embargo, la sustitución no se basó en asignar equivalentes a cada una de las letras en el alfabeto definitorio, sino en el arcaico método de Cayo Julio César,[6] que prescribe desplazar las letras sobre el alfabeto único tres lugares a la derecha con el fin de localizar a los sustitutos fijos para cada elemento. El conteo de ciertos bigramas y trigramas repetidos y el cálculo de la media entre sus

[6] Lo refiere Suetonio en el capítulo 56 de su *Vida del divino Julio César*, pp. 99-100. Entre otros autores, Albert C. Leighton, "Secret Communication", p. 153, n. 61, ha propuesto que el método cifrador atribuido a César Augusto por Suetonio (véase el cap. 88 de su *Vida del divino Augusto*, p. 130), consistente en mover un lugar a la derecha cada letra para encontrar el equivalente y sustituir a la X con AA, representa una modificación del de Julio César. Pero no es evidente, creo, la forma en que se debe evaluar la supuesta modificación, en tanto el principio de sustitución no varía y sólo destaca como novedad el modo de esconder la X.

Imagen 10


TELEGRAFO DEL INTERIOR.

OFICINA ESPECIAL
DEL
SUPREMO GOBIERNO,
EN PALACIO.

14

14

TELEGRAMA.

Recibido de Dolores el 5 de Febº de 1870, á las 12 horas y 38 minutos de la tarde

Al Ministro de Guerra

Ayer pasé una revista escrupulosa á los cuerpos

Escobedo

Telegrama cifrado del general Mariano Escobedo, 5 de febrero de 1870.
Fuente: AHSEDENA, exp. 9288, f. 14.

intervalos puede sugerir la extensión posible del desplazamiento prefijado como regla. Veamos el siguiente fragmento del criptotexto:

(1) s. z. p. o. h. o. k. c. b. w. z. s.
(2) g. o. p. s. z. f. o. h. x. s. b. s. w.
(3) r. c. g. q. z. o. g. s. g. w. Morelia r
(4) s. o. f. a. o. a. s. b. h. c. g. x. s. b. r.
[…]

En los renglones (1) y (2) aparece dos veces el bigrama S.Z. Entre el final y el inicio de las primeras dos líneas, y una vez más en medio de la tercera, tenemos al bigrama S.G. Otros de fácil localización son O.H. y X.S. En la cuarta línea, S.B.H. es un trigrama que se repite en la penúltima línea del texto (véase imagen 10). La O, la S y la G aparecen una y otra vez durante el conteo. Estos datos avalan la inferencia hipotética de que se utilizó un solo alfabeto para el cifrado en su ordenamiento regular, es decir, sin haberlo transpuesto previamente. Para probar esta hipótesis, nada más recomendable que aplicar la técnica de "completar el componente plano", según la llamó Edgar C. Reinke en un fino trabajo sobre la criptografía grecorromana.[7] Consiste en escribir debajo de cada letra del criptotexto su consecutiva normal, leyendo las filas emergentes de izquierda a derecha según es tradicional para la escritura alfabética latina.

[7] Reinke, "Classical Cryptography", p. 117. Leighton, "Secret Communication", p. 153. Para un criptoanálisis muy similar a partir de un criptograma militar mexicano, véase Hitt, *Manual for the Solution*, pp. 40-42.

Procedamos en tal estilo con las nueve letras iniciales de nuestro criptotexto:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Criptotexto	**0**	**S**	**Z**	**P**	**O**	**H**	**O**	**K**	**C**	**B**
	1	T	A	Q	P	I	P	L	D	C
	2	U	B	R	Q	J	Q	M	E	D
	3	V	C	S	R	K	R	N	F	E
	4	W	D	T	S	L	S	O	G	F
	5	X	E	U	T	M	T	P	H	G
	6	Y	F	V	U	N	U	Q	I	H
	7	Z	G	W	V	O	V	R	J	I
	8	A	H	X	W	P	W	S	K	J
	9	B	I	Y	X	Q	X	T	L	K
	10	C	J	Z	Y	R	Y	U	M	L
	11	D	K	A	Z	S	Z	V	N	M
Texto plano	**12**	**E**	**L**	**B**	**A**	**T**	**A**	**W**	**O**	**N**

Descubrimos que, después de avanzar 12 veces hacia abajo —12 lugares a la derecha en el alfabeto único— se forma la generatriz EL BATAWON. En realidad, Escobedo quiso decir BATALLÓN y, desde el punto de vista criptográfico, lo hizo sin fallar, ya que representó a la LL con una W tras convenir con sus corresponsales en que esa última consonante valdría por una letra doble para varios usos. La LL probablemente no fue incluida en el alfabeto de definición, en todo caso no se localiza en el criptotexto. Por otra parte, Escobedo se sirve de laletra clara I, escrita mediante la W por convención para dos posibles fines: (a) ocultar la conjunción Y —la cual, curiosamente, jamás opera

en el criptotexto, no obstante ocupar su sitio normal en el alfabeto definitorio— y (b) usarla como nulo, insertándola entre grupos desiguales de palabras. Todo esto lo posibilita la "clave" con cuya guía se desplaza el alfabeto único 14 lugares a la izquierda desde cada letra en el texto plano en un alfabeto definitorio de 26 letras (por exclusión de CH, LL, Ñ y, acaso, RR) para encontrar el sustituto. Como se ve, Escobedo se habría servido de una variación respecto del clásico modelo de César.

Es verosímil, así, enunciar que la clave para este sistema, entendida técnicamente como factor gobernante de las transformaciones a cifra, es 12.

Tras la decriptación, el mensaje de Escobedo transmite, a la letra, lo siguiente (decriptados en cursivas):

(F. 14)
Recibido de Dolores el 5 de Feb.o de 1870, á las 12 horas y 38 minutos de la tarde

C. Ministro de Guerra
Ayer pasé una revista escrupulosa a los cuerpos. *El batawon ilesabelra tjene i dos clases i de armamentos j endo i la mavor parte carabjnas i ausbrjacas i v para estas i se necesitan urintemente cuarenta mjl i tjros i.*
Escobedo

Después de omitir los posibles nulos intercalados, establecer la identidad gráfica y fonética de varias letras que se presentan con elementos de morfología similar (la J por la I, notablemente), corregir los evidentes errores de cifrado y suplir los caracteres faltantes, el texto claro se lee:

C. Ministro de Guerra

Ayer pasé una revista escrupulosa a los cuerpos. *El batallón ilesabelva (?) tiene dos clases de armamentos, siendo la mayor parte carabinas austriacas, y para éstas se necesitan urgentemente cuarenta mil tiros*.
Escobedo

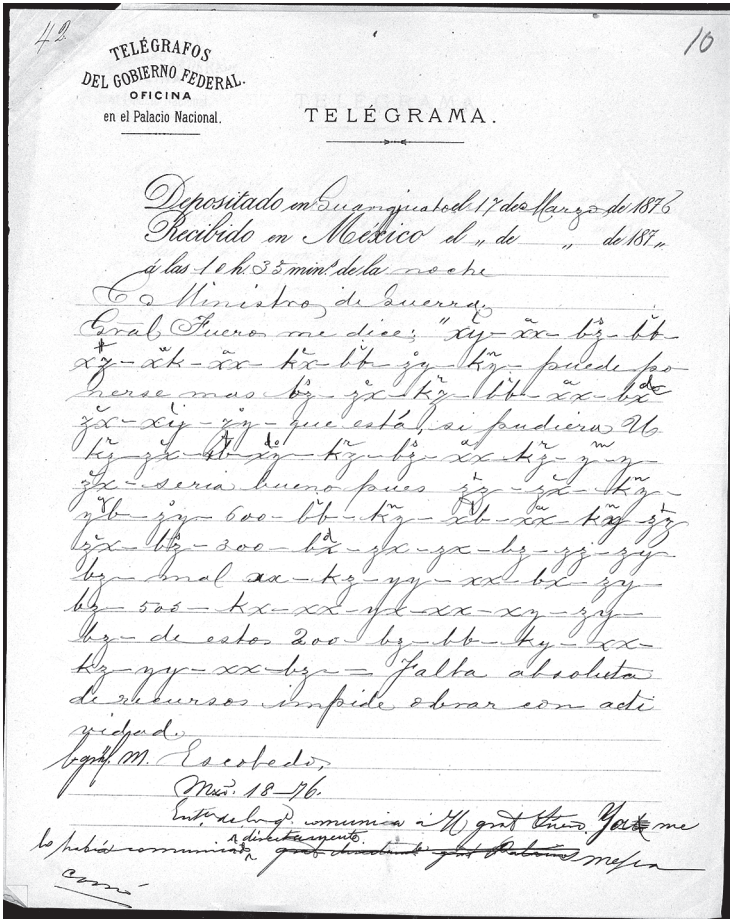
DOS CIFRAS MILITARES DE 1876

Un criptosistema de sustitución con bigramas

En el expediente 11632 se contienen varios telegramas en cifra, destacando por su aspecto intrincado uno que se debe al general Fueros, según la versión retransmitida por el general Escobedo en un telegrama depositado en Guanajuato el 17 de marzo de 1876 (imagen 11).

Una ventaja es que contiene más de 50% de las equivalencias del texto plano entre líneas, suficiente para permitirnos deducir los valores de las cifras restantes y aclarar el documento en su totalidad. Técnicamente, el cifrado es monoalfabético, de 1 a 1, y se ejecuta con bigramas de sustitución exclusivamente. Los guiones introducidos para distinguir a cada bigrama como unidad promueven el éxito criptoanalítico al facilitar la observación de repeticiones cuya valoración crítica, en el caso de que faltara el descifrado entre líneas, recomendaría examinar dos hipótesis contrapuestas: *(a)* que la transformación se logró con un solo alfabeto de cifrado, o *(b)* que resultó de aplicar un sistema polialfabético, aunque gobernado por una clave demasiado breve. No tardamos en reconocer que *(b)* difícilmente sería

Imagen 11



Telegrama cifrado del general Mariano Escobedo (retransmisión de mensaje del general Fueros), 17 de marzo de 1876.
Fuente: AHSEDENA, exp. 11632, f. 10.

el caso, considerando que los pares XX=A, ZX=E, ZY=O y KZ=R, por mencionar solo cuatro equivalentes para letras de alta frecuencia en español, generalmente aparecen o yuxtapuestos o separados entre sí por una cantidad nunca superior a 12 de términos en criptotexto. Ahora, por factorización, vemos que la probable longitud de la supuesta clave será de 2 o, cuando hay yuxtaposición o no es posible factorizar, apenas de 1. En efecto, para XX=A, por ejemplo, tenemos una separación máxima de 12, por tanto 4×3 y dos factores, o una menor de 9, 3×3, todavía dos factores, y para ZX=E medimos distancias de 4, 2×2, y 7, que no se factoriza. La constancia del factor 2 en este análisis sugeriría, pues, la hipótesis de que, si se usó una clave, ésta deberá estar formada por dos caracteres, ya sean letras, números o signos de cualquier otra índole.[8] Pero, en tal caso, la rotación alfabética para elegir los sustitutos nunca cumpliría más de dos ciclos, indicando que el criptosistema original está formado tan solo por dos alfabetos, uno para el texto plano y el otro para los criptogramas. No obstante, un arreglo semejante debe ser, por principios de clasificación criptográfica, monoalfabético y no polialfabético. En definitiva, concluimos lógicamente que *(a)* representa la mejor hipótesis explicativa en cuanto a la clasificación del ejemplar. La inspección crítica y técnica del documento más el descifrado directo nos convencen, a la postre, de que nuestra elección es la correcta.

[8] Encontré un ejemplo modélico —pero en el cual se omitieron los guiones o cualesquiera otras marcas de función análoga— para desarrollar este criptoanálisis en Langie, *Cryptography*, pp. 70-72.

En la siguiente inscripción del telegrama completamente aclarado, donde las partes descifradas van en cursivas, he mantenido la ortografía del original.

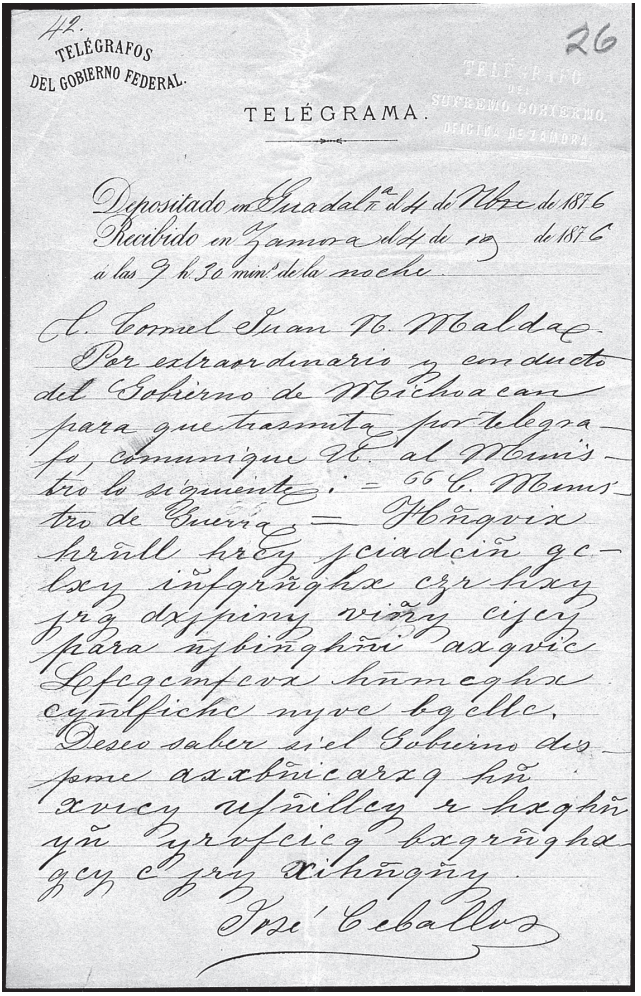
> C. Ministro de Guerra.
>
> Gral. Fuero me dice: "*la situación* puede ponerse mas *seria de lo* que está, si pudiera U *reforzarme* seria bueno pues *tengo* 600 *infantes* 200 *de estos* mal *armados* 505 *caballos* de estos 200 *sin armas*["] = Falta absoluta de recursos impide obrar con actividad.
> [C. Gral. M.] Escobedo.

Una permutación elemental en dos criptogramas del general José Ceballos

En el mismo expediente se conservan dos telegramas (imágenes 12 y 13) parcialmente cifrados que el general José Ceballos transmitió desde Guadalajara la noche del 4 de noviembre de 1876, destinados al coronel Juan N. Malda.

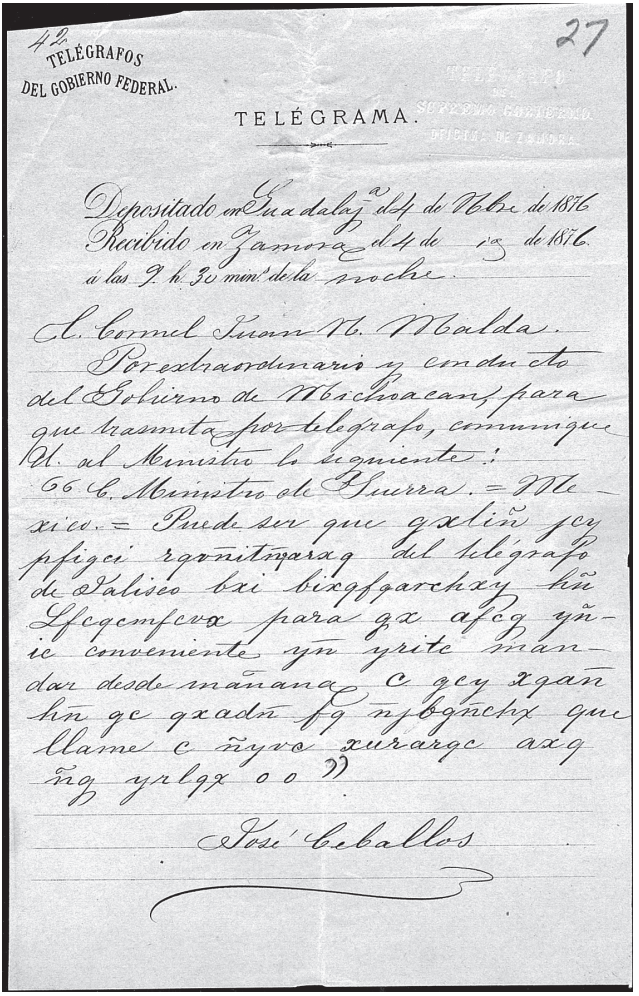
Se trata de cifras cuya clase y fragilidad se reconocen más a partir de la lectura y posición de los fragmentos en texto plano, nítidamente demarcados por los espacios entre palabras y letras, que como fruto de cualquier "ataque" criptoanalítico. Esta condición formal resalta en la f. 27, misma que pude decriptar en minutos tras ensayar con el método de "la palabra probable" (no confundir con el de "completar el componente en texto plano"). La revelación surgió tras reflexionar sobre estas partes de los renglones 11 y 12 en la imagen 13: "conveniente YÑ YRITC mandar desde mañana C GCY XQAÑ…". Se trataba de conjeturar o,

Imagen 12



Telegrama cifrado del general José Ceballos, 4 de noviembre de 1876.
Fuente: AHSEDENA, exp. 11632, f. 26.

Imagen 13



Telegrama cifrado del General José Ceballos, 4 de noviembre de 1876.
Fuente: AHSEDENA, exp. 11632, f. 27.

francamente, de adivinar si a "conveniente" sigue un artículo o un verbo conjugado. Al ensayar con LO, LA y LE no era fácil determinar la continuación de manera que se enlazara coherentemente con "mandar", aunque de aquí no se pudiera concluir la inviabilidad de la conjetura. En cuanto a ensayar con un verbo, la cosa se complicaba por la necesidad de probar numerosas conjugaciones posibles. En parecidas ocasiones, la adivinación puede refinarse con la orientación del criptoanálisis. En efecto, el verbo podía ser HABER pero, suponiendo que el ejemplar fuera de sustitución monoalfabética, la repetición cercana de la Y en el par YÑ YRITC haría difícil creer que la Y ocultara a la H en ambos casos, dada la relativamente baja frecuencia de la H en el español regular; además, en el total de la cifra la Y aparece ocho veces, demasiadas para sugerir como plausible la inferencia de que su equivalente fuera la H en cada caso —en tanto, repito, se mantuviera el supuesto de estar lidiando con un criptograma monoalfabético de sustitución simple. Ahora, prosiguiendo el análisis bajo la presunción de que Y debe ocultar una consonante y suponiendo a YRITC también como un verbo en conjugación, ensayé a convertir la Y en S, resultando la solución preliminar SÑ SRITC. Al ver, en este punto, la notable repetición de la Ñ en la cifra total, le asigné el valor de E, quedando ahora la porción de texto SE SRITC. Acto seguido consideré ciertos elementos de redacción compartidos por muchos documentos en la serie total compulsada durante esta investigación, especialmente los giros corteses al enunciar órdenes o requerimientos urgentes a destinatarios de rango elevado en el escalafón. Según esto, me pareció que la lectura SE SIRVA era una postulante sólida. La porción bajo análisis rezaba

entonces: "conveniente SE SIRVA mandar desde mañana A GAS XQAE…".

En este punto crecía la certidumbre sobre la sustitución simple, monoalfabética, como el principio de cifrado. Era extraño pensar que la G en el segmento estaba en lenguaje abierto, pues ello imponía la idea de un "gas" como objeto de la solicitud; pero el elemento inmediatamente anterior a la G ya estaba aclarado, A, luego era lícito suponer que la G escondía otra consonante. Juzgué plausible que fuera la L en tanto A y S en GAS ya estaban también aclaradas. Sustituyendo, pues, la G por L hallé A LAS XQAE. En esta latitud, el lector habrá podido resolver por su cuenta el misterio de las X, Q y A en esta última fracción, que es ONC, restituyendo así el conjunto claro A LAS ONCE. La decriptación completa de este fragmento devuelve, pues, "CONVENIENTE SE SIRVA MANDAR DESDE MAÑANA A LAS ONCE". Esto es coherente y, lo más importante, prueba la legitimidad de asignar determinados caracteres en texto plano a buena parte de las letras en cifra, en tanto muchas de éstas aparecen con porcentajes desiguales a lo largo del documento, facultando de tal modo las mejores inferencias hacia el descubrimiento de cada par carácter claro-carácter críptico, a partir del conteo elemental de frecuencias relativas.

En definitiva, debí más a la adivinación (educada técnicamente, como se ha visto) de palabras probables —muy similar a la descrita por Richard V. Andree en un ilustrativo texto sobre la relación disciplinaria entre criptografía y matemáticas—[9] que a la factorización del criptotexto (concebido

[9] Andree, "Cryptography as a Branch of Mathematics", p. 505.

como si fuera un polinomio) la ruptura de los dos telegramas del general Ceballos. Guiándome por las equivalencias encontradas en un inicio, poco a poco fui deduciendo la necesaria identidad del resto de los caracteres crípticos, hasta lograr finalmente definir las correspondencias entre el alfabeto de definición y el de cifrado, ambos con extensión de 26, lógicamente —pues el especimen es monoalfabético.

Alfabeto de definición	A	B	C	D	E	F	G	H	I	J	L	LL	M	N
Alfabeto de cifrado	c	p	a	h	ñ	u	l	d	r	m	g	z	j	q

Alfabeto de definición	Ñ	O	P	Q	R	S	T	U	V	X	Y	Z
Alfabeto de cifrado	e	x	b	n	i	y	v	f	t	o	s	ll

Ahora, una revisión superficial de estos pareos basta para detectar que la sustitución criptográfica se reduce a la permutación recíproca de unas mismas letras por otras, definiendo así a la operación de cifrado como un mero reflejo de la operación opuesta. En efecto, cuando C es A, A es C; cuando D es H, H es D; cuando N es E, E es N, y así con los demás pares definidos, en un ir y venir cuyos puntos de llegada los determina el requerimiento alternado de cifrar o descifrar. Todo esto vuelve discutible la idea de que nos enfrentamos con un criptosistema monoalfabético en el sentido técnico y teórico normal en criptología, pues la distinción entre alfabeto del texto plano y alfabeto de la cifra se disuelve tras efectuar la observación recién expuesta (de donde se sigue, además, que el desorden en el pretendido alfabeto de cifrado carece de real importe criptográfico). Podría decirse, de hecho, que para facturar este sistema basta con dividir el alfabeto de longitud 26 en dos partes de 13 elementos

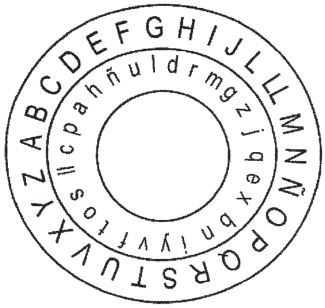
cuya mutua unificación, para fines criptográficos, depende de situar a cada letra en relación recíproca (especular) con su letra imagen, del siguiente modo:

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

La flecha de bidirección en la primera columna de la izquierda indica que se toma una letra por otra según se desee cifrar o descifrar, siendo baladí preguntarse cuál de los dos alfabetos corresponde a la cifra y cuál al texto plano.[10] Es interesante proponer, sin embargo, dos posibilidades a la reflexión criptoanalítica. *1*) Un semejante ordenamiento de letras alfabéticas *sí podría* servir como generador de cifras en tanto se lo agregara, junto con otros de formato idéntico pero alterando la correlación de los caracteres, en una matriz polialfabética como la descrita por Giovanni Battista della Porta en su tratado *De Furtivus Literarum Notis* (1563). En un modelo así, la sucesión de, digamos, paquetes

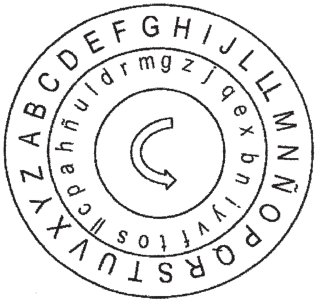
[10] No se trata de alfabetos inversos, a la manera del Atbash hebreo o, para citar un ejemplo del mundo hispánico, del criptosistema descrito por Pedro Mártir Anglés en la parte final de su *Prontuario Orthologi-graphico trilingüe* (Barcelona, 1742), que consiste en una "tabla idiagráfica" para escribir "en secreto", formada por dos alfabetos colocados uno encima del otro; el superior está normalmente ordenado y numerado del 1 al 24, el inferior aparece desplazado cuatro lugares a la derecha, empezando, por tanto, con la E y su correspondiente número 5. La idea es tomar el sustituto críptico del inferior, llamado "llave idiagráfica"; así, por ejemplo, en lugar de la A se mostrará o bien la E o bien el 5, aunque también se podría invertir el orden y hacer del alfabeto superior el de la cifra. La explicación detallada del mismo Mártir Anglés se puede leer en Galende Díaz, "Pedro Mártir Anglés", pp. 137-144. Para ejemplos de alfabetos recíprocos formalmente idénticos al aquí comentado, véase Gaines, *Cryptanalysis*, pp. 69-70.

de letras emparejadas en vertical ocuparía el espacio derecho en la matriz, y cada letra sería un posible sustituto críptico para cada elemento del texto plano, tomándose de la línea superior o de la inferior según lo indicara una palabra clave cuyo alfabeto se ordenaría por pares en la primera columna de la izquierda, manteniendo la sucesión regular del alfabeto (AB, CD, EF…).[11] *2)* Si mantenemos la opinión de que este criptosistema es monoalfabético en el sentido técnico normal, hay por lo menos una forma de trabajar con él a fin de potenciar, instantáneamente, verdaderas sustituciones polialfabéticas, capaces de resistir con mayor aptitud los "ataques" criptoanalíticos hasta donde sea posible. El procedimiento es muy simple. Colocamos los dos alfabetos en un par de aros concéntricos en un disco, sujetados de modo que uno (de preferencia el interior) o ambos puedan rotar a izquierda o a derecha. El alfabeto del texto plano se despliega en el aro externo y el del criptotexto en el interno, así:



[11] Bauer, *Decrypted Secrets*, pp. 129-130.

En esta organización inicial no se altera, por supuesto, la situación recíproca de las letras; todo lo que se ha hecho es doblar las líneas alfabéticas hasta formar un dúo de círculos anidados. El cambio se opera en cuanto movemos el aro interno en cualquier dirección, pues con ello se anula en el acto la reciprocidad y brotan combinaciones múltiples para elegir sustitutos.



Como se aprecia en este segundo disco, el alfabeto de la cifra se ha desplazado tres lugares a la izquierda respecto del alfabeto definitorio, resultando que la A ya no se cifra por la C sino por la H, mientras que la U es ahora el equivalente críptico de la C y no de la A. Por su parte, la H se cifrará por la G y no por la D, y la U por la S y no por la F. La cantidad de los movimientos se indicará por una clave literaria o numérica. Por supuesto, el cambio periódico de las claves implica una renovación total de las combinaciones en cada ocasión. Sería posible, asimismo, añadir guarismos, signos nulos, de puntuación y otros auxiliares de la escritura en el aro de la cifra, con el fin de mezclar las letras con símbolos varios y dotar a los criptogramas creados de un aspecto más enrevesado.

Este ideal recurso a los discos móviles para fortalecer un criptosistema monoalfabético no exige sino adoptar el modelo presentado por Leon Battista Alberti en su manuscrito "De Cifris" (*c.* 1466),[12] un aporte de ingentes consecuencias para todo desarrollo ulterior del polialfabetismo en criptografía.

La cifra del general Ceballos, en fin, podría haber sido dispuesta para un funcionamiento polialfabético eficaz por la incorporación de discos u otros implementos tecnológicos, pero, juzgando por el modo en que probablemente se diseñó y aplicó (según las hipótesis manejadas), es tan vulnerable como cualquier criptosistema basado en la mera reciprocidad monoalfabética.

Los textos aclarados de los dos telegramas, tal y como los devuelve la decriptación, se leen como sigue.

(F. 26)
Depositado en Guadalajara el 4 de nov de 1876
Recibido en Zamora el 4 de ig. de 1876
A las 9 h. 30 min.s de la noche

C. Coronel Juan N. Malda
Por extraordinario y conducto del Gobierno de Michoacan para que trasmita por telegrafo, comunique U. al ministro lo siguiente: "C. Ministro de Guerra.= *Dentro diez días marchare Lagos reuniendo allí dos mil hombres tres armas* para *emprender contra Guanajuato dejando asegurada esta plaza*. Deseo saber si el Gobierno dispone *cooperación de otras fuerzas i donde se situaran poniéndolas a mis ordenes*.
José Ceballos

[12] Kahn, "On the Origin".

(F. 27)
Depositado en Guadalaj.a el 4 de Nbre de 1876
Recibido en Zamora el 4 de ig. de 1876
A las 9 h. 30 min.s de la noche

Por extraordinario y conducto del Gobierno de Michoacan para que trasmita por telegrafo, comunique U. al ministro lo siguiente:
"C. Ministro de Guerra.= Mexico.= Puede ser que *logremas* [sic] *burlar intervencion* del telégrafo de Jalisco *por pronunciados de Guanajuato* para *lo cual sera* conveniente *se sirva* mandar desde mañana *a las once de la noche un empleado* que llame *a esta oficina con el signo xx*".[13]
José Ceballos

MEZCLA DE CÓDIGOS Y CIFRAS EN UN TELEGRAMA DE 1879

Veamos, por último, un caso en donde se mezclan el cifrado y la codificación. Ejecutar esa mezcla es recomendable porque un código, al representar una transformación criptográfica a nivel de la semántica y no de la sintaxis, genera dificultades enormes a quien pretende romperlo sin conocer el método de su formación. En tal caso, la esperanza es realizar una hábil investigación eminentemente histórico documental y no técnica, sirviéndose a menudo de evidencia circunstancial para tratar de inferir los nombres propios o comunes que probablemente oculta.

El ejemplar en cuestión está incluido en el legajo 9924 con el rótulo "1879. Telegramas reservados y cifrados.

[13] Es posible que esta "xx" final deba traducirse como "oo", pero este detalle no reclama por ahora un tratamiento pormenorizado.

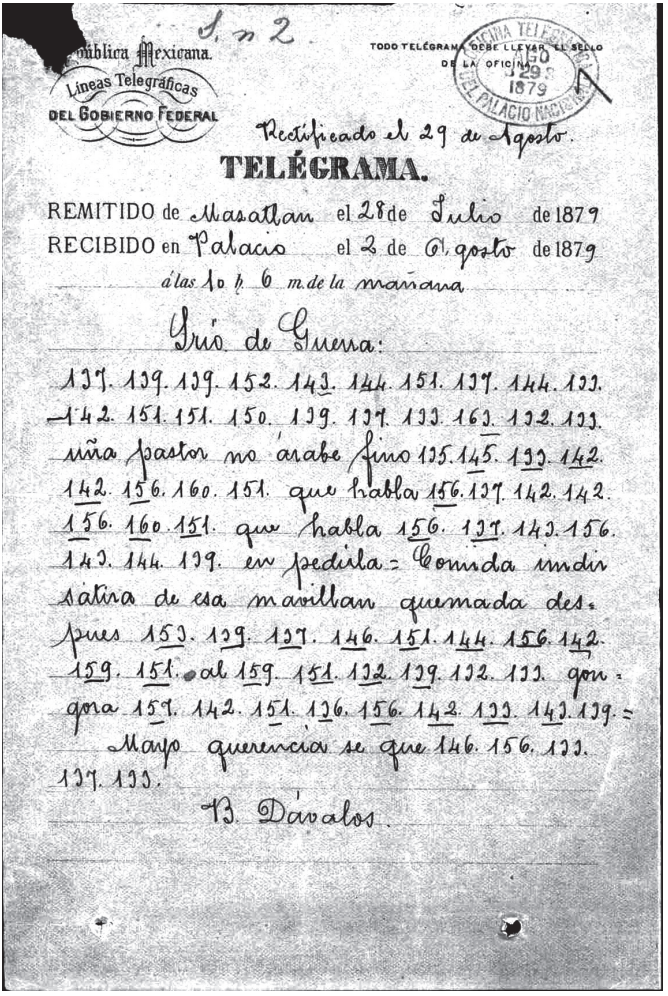
Preparación de sublevados y otros diversos asuntos", dentro de la carpeta 12065. Es un telegrama remitido desde Mazatlán el 28 de julio de 1879 y lo firma B. [Bibliano] Dávalos (imagen 14).

Afortunadamente, el mismo legajo incluye la versión aclarada del mensaje (f. 8), que transcribo a continuación (las partes ilegibles van como reticencia, entre corchetes):

> Srio. de Guerra:
> No obstante razones de Ud. para no autorización formar guerrillas que habla, insisto en pedirla= Conviene utilizar servicio de esa gente, que después combatirla al lado de Gral Ramirez o Gral O[…]gel Martinez, quien sé que viene = B. Dávalos.

Los elementos de cifra son guarismos de tres elementos y las palabras constituyen, en su mayoría, los códigos. En ausencia del texto plano habría sido necesario evaluar la posibilidad de que los números representaran códigos cifrados, pues el método de sobreencriptar tanto cifras como códigos ha sido utilizado en muchas ocasiones, aún en el caso de que se codifique por medio de números y no de palabras —lo cual es poco frecuente, pero muy viable—. Con la información disponible podemos inferir que el cifrado se limitó a la asignación de numerales como equivalentes para las letras del alfabeto de definición, en correspondencias de uno a uno. Algunos trigramas numéricos aparecen subrayados o no subrayados alternativamente, por ejemplo 142, 143, 144 y 151, pero al comprobar su significado constante en el mensaje claro se impone la creencia de que el subrayado no estaba destinado a cumplir una función técnica especial, como sí lo hace en el ejemplo del criptosistema de 1860

Imagen 14



Telegrama cifrado del general Bibliano Dávalos, 28 de julio de 1879.

Fuente: AHSEDENA, exp. 9924, f. 7.

revisado en el primer apartado *supra*. Que la equivalencia es uniforme y sistemática lo muestra el siguiente gráfico para la línea inicial del criptotexto:

Cifra	137	139	139	152	143	144	151	137	144	133	142	151	151	150	139
Texto plano	N	O	O	B	S	T	A	N	T	E	R	A	-	-	O

Cifra	137	133	163	132	133
Texto plano	N	E	-	D	E

También observamos que, al parecer, el criptógrafo cometió errores o se confundió al inscribir los numerales 151, 150 y 163. El 151 en la primera línea (imagen 14) es una repetición, pero el 150 debería significar Z, sin embargo, en la última línea del criptotexto aparece el 143 ocultando a la Z final de "Ramirez"; ese guarismo, por cierto y de notar, equivale a la S en la primera línea, sugiriendo que en el criptosistema se dispuso usarlo como sustituto tanto de S como de Z, atendiendo a la similitud fonética de estas letras y, en consecuencia, fomentando la economía de medios para configurar el sistema íntegro. Y si esto es así, entonces el 163 que aparece en la segunda fila del gráfico fue confundido con el 143. En verdad, es necesario para el criptoanalista tener en cuenta estas posibilidades, ya que no era (ni es) difícil equivocarse al operar con criptosistemas de diseño y operación manual, como en su abrumadora mayoría lo fueron los creados desde la antigüedad clásica y hasta buena parte del siglo xx.

Pasemos a los códigos. La inspección indica que se asignaron a frases completas y sílabas, como lo exhibe la siguiente tabla ejemplar:

Código	UÑA	PASTOR	NO	ARABE	FINO
Texto plano	UD.	PARA	NO	FOR-	MAR

En este fragmento la palabra NO está sin codificar, mientras que las dos primeras se han codificado completas cada una y sólo silábicamente la última, FORMAR. Un caso análogo es el de GON GORA 157, situado en las antepenúltima y penúltima líneas, como código de GENE y RA más el cifrado de la L. Lo cierto, en definitiva, es que la codificación se efectuó sobre nombres propios y comunes exclusivamente.

Un problema especial es determinar cómo se eligieron los términos código para forjar este criptosistema. Dado que todos los términos código se reconocen como palabras de uso normal en el léxico español, es probable que hayan sido seleccionados del diccionario. Mi opinión actual es que, en efecto, cada sustituto proviene de un diccionario usado como "clave", pero no al azar sino en obsequio a la regla dependiente, quizá, de un hecho. Como se observa, casi todos los elementos en código inician con la misma letra que los elementos en texto plano, por ejemplo, UÑA-UD., PARA-PASTOR, COMIDA-CONVIENE, y GON-GENE. Podemos conjeturar, así, que la prescripción se redujo a concretar el número de veces en que, partiendo de la entrada correspondiente a cada palabra a cifrar en el diccionario, se habría de subir o bajar, o subir y bajar, para encontrar el término código. En el par UÑA-UD., por ejemplo, la dirección a seguir tendría que ser arriba, pues la Ñ va después de la D en el alfabeto regularmente ordenado. En cambio, para GON-GENE la dirección tendría que

ser la contraria, por la misma determinación que fija la progresión alfabética regular.

Confío, además, en la fuerza de esta hipótesis por la razón histórica de que tal estrategia fue utilizada más de una vez por enviados diplomáticos de México en Gran Bretaña al promediar la década de 1820, sirviéndose como "clave" del *Diccionario de la Lengua Castellana por la Real Academia Española* en su quinta edición (1817), según lo pude comprobar por la incursión minuciosa en ciertos expedientes del Archivo Histórico Diplomático de la Secretaría de Relaciones Exteriores de nuestro país.[14] Ahora, para informar debidamente y confirmar, si acaso, la hipótesis de que Dávalos y los destinatarios de su telegrama "híbrido" (de cifras y códigos) usaron un diccionario de la lengua como "clave" de codificación en la forma señalada, sería preciso, ante todo, averiguar si en 1879 la Secretaría de Guerra contó con algún diccionario de ese tipo en su biblioteca, y si así fue, localizar las entradas para los términos claros en el ejemplar y medir las distancias entre éstas y las de los vocablos elegidos como sus respectivos códigos. A reserva de hacer esto, sería precipitado juzgar imposible que Dávalos y sus corresponsales hayan elegido a capricho los códigos para esconder fragmentos del mensaje en la comunicación examinada.

SIGLAS Y REFERENCIAS

AHSEDENA Archivo Histórico de la Secretaría de la Defensa Nacional de México, D. F. Sitio web: http://www.archivohistorico2010.sedena.gob.mx/

[14] Explico mi procedimiento analítico en Narváez, "Some Diplomatic Ciphers", pp. 66-71.

Andree, Richard V.

"Cryptography as a Branch of Mathematics", en *The Mathematics Teacher*, 45: 7 (nov. 1952), pp. 503-509.

Bauer, F. L.

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

Gaines, Helen Fouché

Cryptanalysis: A Study of Ciphers and Their Solution, Nueva York, Dover Publications, 1956.

Galende Díaz, Juan Carlos

"Pedro Mártir Anglés y su sistema criptográfico", en *Quaderns d'Història Tarraconense*, xii, 1993, pp. 127-145.

Hitt, Parker

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

Kahn, David

"On the Origin of Polyalphabetic Substitution", en *Isis*, 71:1 (mar. 1980), pp. 122-127.

Langie, André

Cryptography, traducido del francés por J. C. H. Macbeth, Londres, Bombay, Sidney, Constable & Company Limited, 1922.

Leighton, Albert C.

"Secret Communication among the Greeks and Romans", en *Technology and Culture*, 10: 2 (abr. 1969), pp. 139-154.

Mendelsohn, Charles J.

"Blaise de Vigenère and the 'Chiffre Carré'", en *Proceedings of the American Philosophical Society*, 82: 2 (1940), pp. 103-129.

Narváez, Roberto

"Some Diplomatic Ciphers of the First Mexican Federal Republic (1824-1830)", en *Cryptologia*, 39: 1 (2014), pp. 66-83.

Ortega Triguero, Jesús J., Miguel Ángel López Guerrero *et al.*

Introducción a la criptografía: historia y actualidad, Cuenca, Ediciones de la Universidad de Castilla-La Mancha, 2006.

Reinke, Edgar C.

"Classical Cryptography", en *The Classical Journal*, 58: 3 (dic. 1962), pp. 113-121.

Suetonio

Vida del divino Julio César, presentación de Antonio Ramírez de Verger, traducción de Rosa Ma. Agudo Cubas, Madrid, Gredos, 2010.

Vida del divino Augusto, presentación de Antonio Ramírez de Verger, traducción de Rosa Ma. Agudo Cubas, Madrid, Gredos, 2010.