Los criptosistemas oficiales de la Legación Mexicana en Washington, 1824-1826

Roberto R. Narváez*

Resumen

Se presentan rectificaciones o ajustes a las conclusiones anteriormente desarrolladas sobre la criptografía utilizada por Pablo Obregón mientras fungió (1824-1827) como enviado extraordinario y ministro plenipotenciario de México en Washington. Al estudiar una serie documental resguardada en el Acervo Histórico Diplomático de la Secretaría de Relaciones Exteriores, de la que previamente no se tenía conocimiento, surgieron nuevas luces que son necesarias incorporar en el análisis. En concreto, la meta es describir y caracterizar técnicamente, pero con exactitud histórica, la clase definida del criptosistema preferido por Obregón durante su misión estadounidense. El análisis permite asimismo demostrar que el también ministro José Anastasio Torrens aplicó el mismo método para cifrar por lo menos un despacho enviado desde Colombia en 1825. Se comentan en apéndice las características de un segundo método oficial, el cual, según los registros, ambos diplomáticos tuvieron a su disposición.

Palabras clave: historia diplomática, criptografía, Pablo Obregón.

Abstract

The paper provides a series of rectifications or adjustments to the conclusions reached in a previous article on the cryptography used by Pablo Obregón while he acted as extraordinaire envoy and plenipotentiary minister of Mexico in Washington (1824-1827). New lights on the issue appeared by the study of series of documents kept in the Historical Diplomatic Archive of the Secretary of Foreign Relations of

*Instituto Cultural Helénico.

Mexico, not previously known to the author. In sum, the paper aims at technically describing and characterizing, with historical exactitude, the particular class of cryptosystem preferred by Obregón during his mission in the United States.Likewise, the analysis allows to demonstrate that José Anastasio Torrens, also minister, applied the same ciphering method in at least one dispatch sent from Colombia in 1825. The characteristics of a second official method are referred in the appendix, which, according to the records, was available to both diplomats.

Key words: history, diplomatic, cryptography, Pablo Obregón

Introducción

En el artículo "Los despachos codificados de Pablo Obregón desde Washington en 1825. Análisis y dos decodificaciones", publicado en la revista *Historia mexicana* (volumen LVIII, número 3, enero-marzo 2009, pp. 1093-1153), propuse la hipótesis de que Pablo Obregón (1796-1827) había utilizado un código y no una cifra para comunicar noticias u opiniones requeridas de alta discreción al secretario del Despacho de Relaciones Interiores y Exteriores de México, mientras fungió como enviado extraordinario y ministro plenipotenciario en la capital estadounidense (1824-1827). Este resultado surgió de analizar, en forma inmanente y comparativa, una serie documental totalmente redactada en lenguaje críptico, referente a los movimientos favorables a la independencia de Cuba en 1825 y que se resguarda en el Acervo Histórico Diplomático de la Secretaría de Relaciones Exteriores de México (AHDSREM).[1] Por ciertos motivos de orden teórico y metodológico, me pareció suficiente restringir mis observaciones críticas a dicha serie para inferir el método apropiado de restituir la legibilidad a dos de sus miembros.[2] El éxito me llevó a repetir pocos meses después el ensayo con un tercer

1 AHDSREM, legajo encuadernado L-E-1333, "Independencia de Cuba".
2 *Ibid*., ff. 15-30bis (reservado 3, fechado el 23 de marzo) y 10-12 (reservado 14, fechado el 1 de noviembre).

despacho, firmado en 1826 y ya no relacionado con el asunto cubano.[3] En tales circunstancias no tuve reparos en aprobar la conclusión sugerida por la prueba de la hipótesis, a saber, que Obregón se había servido de un libro de códigos y no un criptosistema de distinta variedad, en tanto los elementos inferidos como parte de aquel supuesto dispositivo permiten, sin lugar a dudas, aclarar los despachos ininteligibles a primera vista.

Esta conclusión es aceptable desde la perspectiva criptológica, pues no requiere de investigaciones ulteriores para confirmar, en cualquier sentido práctico, la validez de las deducciones realizadas. Carece, sin embargo, de la información teórica necesaria para constituir un aporte significativo al desarrollo de la historiografía de la criptología mexicana y, por implicación disciplinaria, de la historia general de las comunicaciones en México. Este reconocimiento me lo impuso el escrutinio de un legajo también custodiado en el AHDSREM, al cual pude acceder en las postrimerías del año 2010. Gracias a esto me encuentro en la posición de realizar algunos ajustes obligados a las consideraciones fundamentales que vertí en mi artículo citado al comienzo, por medio de un análisis histórico y técnico mejor encauzado de la clase exacta de criptografía utilizada por Obregón durante su misión, a partir de la nueva evidencia.

Urge advertir que el coronel José Anastasio Torrens (1790-1857), quien había precedido a Obregón como jefe de la Legación Mexicana en Washington, se sirvió de un idéntico criptosistema al redactar en cifra (probablemente a mediados de marzo de 1825) el extracto de una larga epístola en texto plano –es decir, inmediatamente legible– cuando laboraba como enviado extraordinario en Colombia (1825-1830), según lo argumenté en un artículo sobre los criptogramas de Torrens en esa república sudamericana[4] y puedo confirmarlo actualmente merced al estudio del mismo legajo del AHDSREM tardíamente compulsado, el cual, por cierto, revela también que la cancillería entregó a nuestros ministros dos criptosistemas y no uno.

---

3 Roberto Narváez, "Decodificación de un despacho de Pablo Obregón fechado en 1826", artículo presentado como complemento al anterior en la misma revista. El texto "decodificado" en este lugar pertenece al reservado 4 (16 de enero) de 1826.

4 Roberto Narváez, "Dos criptosistemas". La hipótesis tendiente a fijar la fecha de redacción del extracto en cifra ocupa las pp. 37-38.

Presentar y comentar, con el apoyo de breves análisis comparativos, la cifra definitiva y no hipotética cuyo uso privilegiaron Obregón y Torrens para facturar notas en cifra constituye la meta suprema de esta colaboración. Me referiré a ella como criptosistema I. En el apéndice describo la cifra restante que consta en las instrucciones oficiales, denominándola criptosistema II.

El criptosistema I de Pablo Obregón y José Anastasio Torrens

La mayoría de los folios de Obregón en el legajo encuadernado L-E-1333 (AHDSREM), rotulado "Independencia de Cuba", contiene el descifrado entre líneas –obra de alguna persona especializada en realizar faenas de este género en la cancillería–[5], caso del reservado número 4 fechado el 30 de marzo de 1825 cuya página final se reproduce abajo (figura 1).

5 En el mismo legajo citado en la nota 1 se incluye una relación de la correspondencia reservada de Obregón en 1825; reúne información diversa, por ejemplo si el material recibido estaba en cifra y, en varios casos, el nombre de la persona que lo "tradujo". En cuanto al reservado 15 (31 de marzo) se aclara: "En cifra y traducido. Fue entregado á colección por el Sr. Larrañaga".

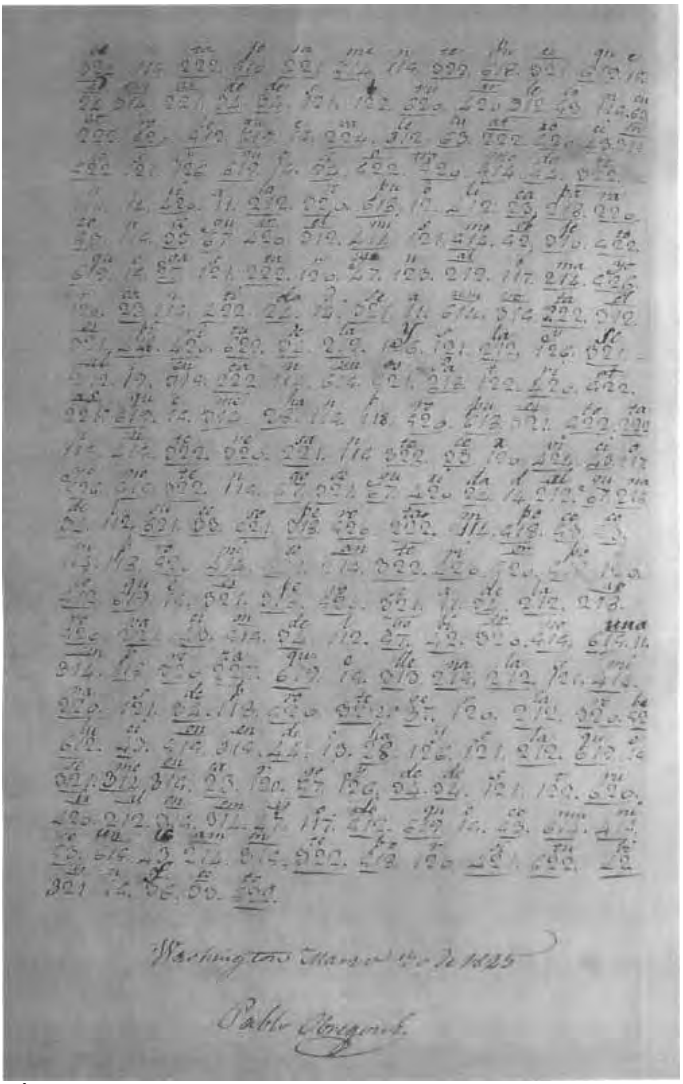

Figura 1. Última página del despacho reservado número 3 (30 de marzo de 1825) de Pablo Obregón. Fuente: AHDSREM, L- E- 1333, "Independencia de Cuba", f. 36bis.

Los reservados 3 y 14 son los únicos que no presentan esta característica (figura 2).

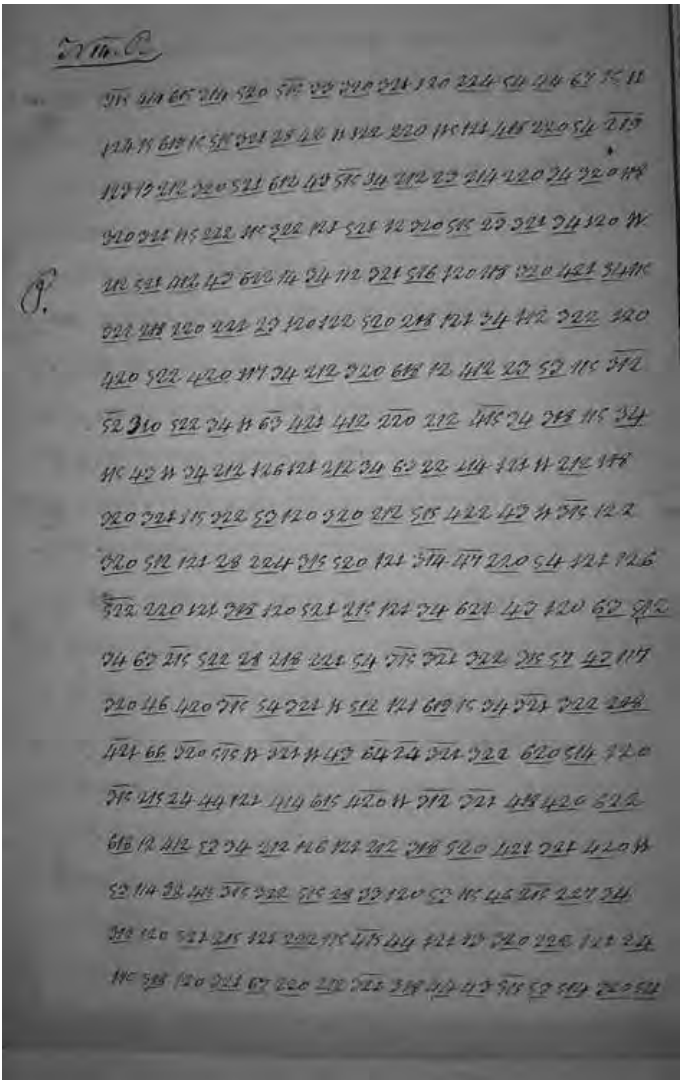

Figura 2. Primera página del despacho reservado número 14 (1 de noviembre de 1825) de Pablo Obregón. Fuente: AHDSREM, L- E- 1333, "Independencia de Cuba", f. 10.

Ahora, la observación atenta revela que una serie definida de caracteres numéricos de sustitución criptográfica reaparecen con elevada frecuencia, si bien variable, en *el total* de los documentos considerados. Por esta analogía inferí que si el carácter 11, por ejemplo, está inscrito entre líneas como equivalente a la vocal A, sin excepciones, en los folios donde así se puede comprobar, debería mantener el mismo valor de sustitución, sin excepciones, en los folios carentes de descifrado; es decir, que si en el reservado 4, digamos, un 11 siempre representa a la A, pero también un 120 a la R, un 114 a la M y un 34 (así subrayado) a la sílaba o preposición DE y un 619 al bigrama QU, por citar sólo cuatro más entre la vasta diversidad de combinaciones identificables, entonces las mismas representaciones deberán valer para los mismos dígitos en los manuscritos sin "traducir". La consecuencia experimental era fácilmente deducible: si con los equivalentes que conocía lograba convertir directamente a texto plano cada uno de los caracteres aún sin descifrar en los reservados 3 y 14, entonces probaba la hipótesis de que todos los folios habían sido criptografiados con el mismo sistema. Realicé las sustituciones y hallé que la deducción era correcta, descifrando en consecuencia los reservados 3 y 14 totalmente (el resultado se puede ver en la última sección de mi artículo en *Historia mexicana*).[6]

Este procedimiento bastó para establecer como un hecho prácticamente cierto que, en este caso, el método pertenece a la clase general de criptosistemas por sustitución; en cambio, no alcanza para deducir rigurosamente sus propiedades técnicas y, por consiguiente, determinar su clase particular. Fue la posterior comparación entre su aspecto y el de métodos afines en los manuales e historias de la criptografía lo que me inclinó a reconocerlo como una especie de código. Esto pone de manifiesto el grado extremo en que me permití guiar esta investigación, esencialmente criptográfica, según los razonamientos inductivo y analógico. En el nivel criptográfico el éxito fue evidente, mas no sucedió lo mismo desde el punto de vista historiográfico, debido justamente a que la excesiva confianza en la inducción, basada en el escrutinio inmanente de los folios, me llevó a juzgar como irrelevante la posibilidad de que el documento donde se

6 Narváez, "Los despachos codificados", pp. 1135-1149. Véase también Narváez, "Decodificación de un despacho", pp. 446-448, para examinar los resultados de la misma prueba efectuada sobre el reservado 4 de 1826.

describe el criptosistema realmente usado por Obregón y Torrens estuviera depositado en algún archivo particular o público, asumiendo que la corrección probada de mi criptoanálisis para aclarar los despachos velados alcanzaba para restituir también, por necesidad criptológica, los principios reguladores del criptosistema original (por otro lado, al seguir tal estrategia inquisitiva deseaba patentizar las ventajas del criptoanálisis para enriquecer a la metodología histórica común de tratamiento documental –como sigo creyéndolo, firmemente–, especialmente si aquél se aplica cuando se desconocen las reglas criptológicas del caso tratado, faena llamada técnicamente *decriptar*).[7] Y como, a juzgar por las apariencias, aquellos principios reguladores consistían, fundamentalmente, en la sustitución de uno a uno entre monogramas, bigramas y trigramas, estimé adecuada la versión de que nuestros diplomáticos habían codificado sus notas en lugar de cifrarlas, o, dicho en términos técnicos, que habían transformado sus respectivas notas al nivel de las sílabas y palabras y no el de las letras. De este modo terminé declarando como lo más probable que ambos habían utilizado un código, al que atribuí determinadas características partiendo de comparaciones con especímenes parecidos de otras épocas y países.[8]

Es forzoso conceder, sin embargo, que el material examinado no proporciona la información suficiente para decidir, con un grado importante de certeza teórica, si es un producto del cifrado, el anagrama, la esteganografía o cualquier otro método criptográfico diferente a la codificación (si bien es francamente imposible suponer, a primera vista por lo menos, que se trata de anagramas o esteganogramas). Por tanto, para conocer positivamente y sin la interferencia de hipótesis o especulaciones la clase definida del criptosistema realmente aplicado, se volvía indispensable conseguir un esquema del mismo. En verdad, desde el punto de vista económico se debe proceder así en cualquier caso similar, a efectos de no gastar energía intelectual en vanas presunciones teóricas.

Ahora bien, el criptosistema oficial y la segunda cifra a que aludí en la introducción se localizan en el fondo Archivo de la Embajada de México en los Estados Unidos de América (AEMEUA) del AHDSREM, formando parte

7 Cf. Narváez, "Los despachos codificados", pp. 1122-1128.
8 *Ibid*., pp. 1107-1121.

del legajo 1, expediente 4, ff. 42-43 y 44-46, bajo el título "Reglas para cifrar y descifrar", precedido de las instrucciones abiertas y reservadas (ff. 38-39bis y 40-41bis) que Lucas Alamán, entonces el canciller mexicano, entregó a Pablo Obregón después de que éste fuera nombrado (4 de agosto de 1824) enviado extraordinario y ministro plenipotenciario en Washington por el Supremo Poder Ejecutivo de la primera República Federal mexicana. Las descripciones, notablemente concisas, categorizan al par de sistemas como "claves", en un estilo arcaizante que ha perdido vigencia (porque técnicamente es ambiguo). A continuación transcribo la del primer criptosistema, dejando intacta la ortografía y situando entre corchetes las fracciones conjeturales o tres puntos para indicar ilegibilidad:

> Explicación.= La clave adjunta comprehende seis renglones: el 1.º es de las Letras del Alfabeto pero simples con la numeracion que toca á cada letra. Los otros cinco renglones son compuestos de la convinacion que forman las vocales con todas las letras del Alfabeto: por consiguiente el 2.º renglon es de la convinacion de la vocal a: el 3.º de la vocal e: el 4.º de la i: el 5.º de la o: y el 6.º de la vocal u y cada uno de esos renglones con su numeracion respectiva.= Para cifrar con esta clave deben dividirse los vocablos del texto en tantas fracciones como vocales tenga de manera que á la vocal se le junte la letra anterior ó la posterior; y si resultare consonante ó vocal de sobra querrá decir que aquella no se debe ver como fraccion compuesta sino como simple para cifrarla como corresponde. Pongamos un ejemplo=
>
> | | | | | |
> |---|---|---|---|---|
> | Sa | n | ti | a | go |
> | 221 | 115 | 422 | 27 | 117 |
>
> Hecha esta fraccion buscaré la convinacion a/s en el segundo renglon de la clave y en ella veré el n.o 21 que pondré bajo la fraccion sa pero con una rayita abajo del numero para que se advierta que la convinacion es de abajo á arriba y se lea sa y no as. Sigo a cifrar la simple fraccion n y esta la hallaré en el primer renglon de la clave con el numero 15 que pondre en la cifra sin raya alguna. Sigue la fraccion ti cuya convinacion hallare en el 4.o renglon de la clave con él n.o 22 de abajo á arriba y por eso al numero le pondré su raya abajo. Sigue la fraccion ag y hallaré su convinacion en él segundo renglon con el num.o 7 de arriba á bajo

por lo que al numero le pondre su raya arriba. Ultimamente concluiré con [la] simple fraccion o que hallaré en él primer renglon […] el n.o 17 que pondré en la cifra sin raya alguna. Entendido este modo de cifrar resta la circunstancia que debajo de la fraccion no solo se hade poner el n.o que le toca á la convinacion sino tambien él del renglon que se vé al margen de la clave, figurando [en] él el carácter de centenas o de decena en él numero cifrado v. g. la fraccion sa se cifra con el n.o 21: [y] este n.o se hade poner asi 221 para que [aparezca] doscientos veinte y uno siendo asi que él 2 que pa[…] doscientos no es otra cosa que indicar él segundo renglon donde está la convinacion 21 ayudando la raya abajo para que se lea la convinacion de abajo á arriba sa [y] no de arriba abajo as.= Reducida pues la palabra Santiago á la cifra que queda demostrada [que]dará de esta manera.= 221 115 422 27 117. Teniendo la clave en la mano se decifra muy pronto de esta manera.= Atiendase al primer numero de cada partida y este indica el renglon donde se hallará la convinacion señalada con el resto de los numeros de la propia partida, v. g. veo en la cifra anterior 221 pues el primer 2 será la indicacion del 2.º renglon de la clave donde hallaré él 21 que me demostrará la convinacion de letras a/s que lere de abajo á arriba como lo dá á entender la raya abajo del numero 221. El siguiente numero de la cifra es 115: el primer 1 es él que me dice que en él primer renglon de la clave vea el 15 [resto] de la partida donde hallaré la letra n siendo de advertir que pues este numero cifrado no tiene raya ni arriba ni abajo es señal de que habla de letra simple sin convinacion de otras.[9]

La “clave adjunta” mencionada al inicio se muestra en la figura 3.

9 AHDSREM- , “Reglas para cifrar y descifrar”, leg. 1, exp. 4, ff. 44-46.

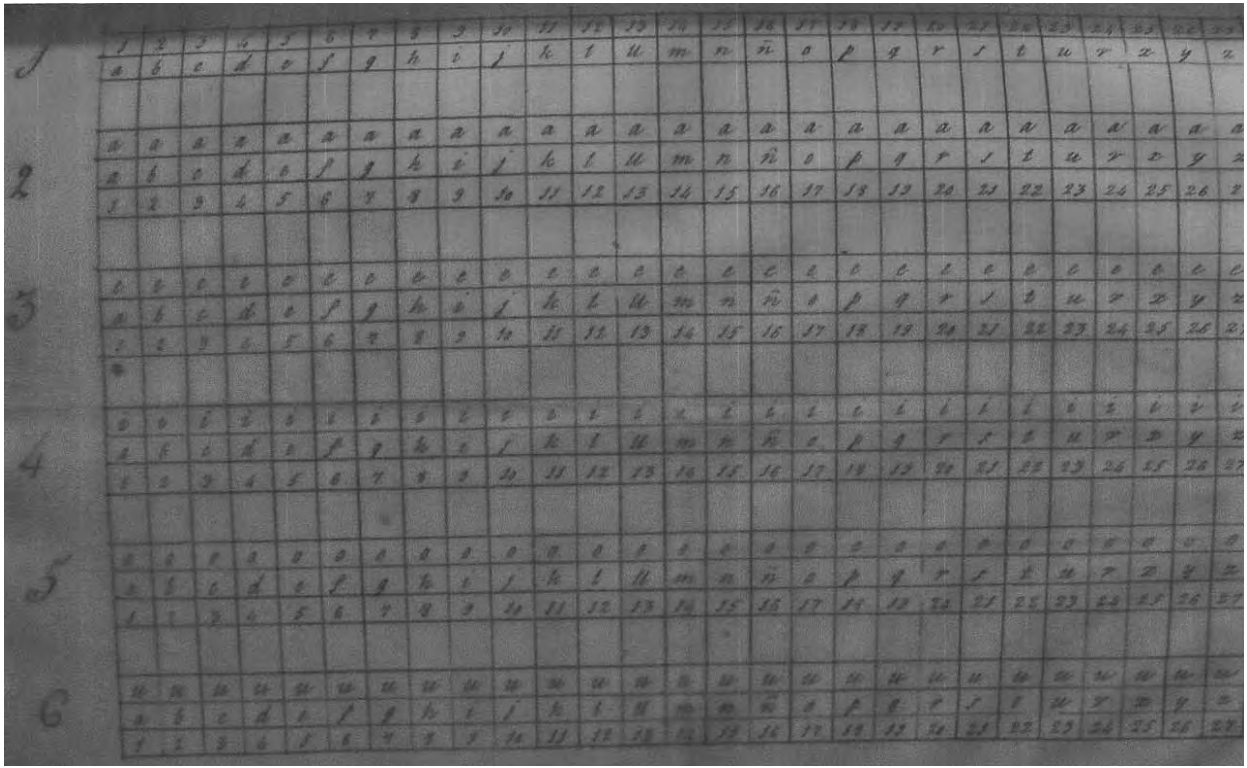

Figura 3. “Clave” adjunta a la explicación del criptosistema I oficial. Fuente: AHDSREM-AEMEUA, Leg. 1, Exp. 4, “Reglas para cifrar y descifrar”.

La transcribiré también para facilitar la observación de sus componentes mientras se leen los comentarios posteriores:

Como se ve, la “explicación” está compuesta de dos partes: la primera ocupa el tercio inicial del manuscrito y en

1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
	a	b	c	d	e	f	g	h	i	j	k	l	ll	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z
2	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a
	a	b	c	d	e	f	g	h	i	j	k	l	ll	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
3	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e
	a	b	c	d	e	f	g	h	i	j	k	l	ll	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
4	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i	i
	a	b	c	d	e	f	g	h	i	j	k	l	ll	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
5	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o
	a	b	c	d	e	f	g	h	i	j	k	l	ll	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
6	u	u	u	u	u	u	u	u	u	u	u	u	u	u	u	u	u	u	u	u	u	u	u	u	u	u	u
	a	b	c	d	e	f	g	h	i	j	k	l	ll	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

ella se puntualizan las directrices para entender el sentido de las divisiones y la estructura general de la tabla; la segunda consiste en un ejemplo con el cual se ilustran los pasos para cifrar y descifrar, y cubre los dos tercios restantes. El alfabeto prescrito, denominado técnicamente "alfabeto de definición", tiene una extensión de 27 (W=27), resultando largo para estas faenas en tanto se incluyen las grafemas LL, Ñ y V, mismas que en otros criptosistemas coetáneos –y aun posteriores– en lengua española solían excluirse (aunque indicando su presencia y sonido en el criptotexto por diferentes medios que no viene al caso mencionar), con la finalidad principal de evitar un pareo exacto entre los alfabetos que se sustituirán mutuamente durante la operación criptográfica, neutralizando así, en lo posible, la exhibición de frecuencias relativas en los caracteres crípticos derivados. De no hacer esto, un eventual espía se vería facultado para medir tales frecuencias y conjeturar la posesión de cualidades determinadas en el ejemplar, por ejemplo, si su estructura se asienta en múltiples alfabetos o uno solo.

El criptosistema bajo análisis, de hecho, es monoalfabético y de sustitución simple. Sería un error identificar los alfabetos de cada "renglón" como una multitud de función autónoma al encriptar, sobre todo por cuanto la instrucción es nítida al respecto: el propósito de los alfabetos 2 al 6 es trabar combinaciones fijas de guarismos para una, dos y hasta tres letras, y aunque podría parecer que la regla de yuxtaponer una vocal a una consonante en órdenes de precedencia variable según cada término a velar debería imponer la formación de combinaciones en alfabetos distintos (caso de las fracciones Sa y ti de Santiago, por ejemplo), realmente no sucede así gracias al expediente de situar una raya o tilde encima o debajo de grupos numéricos cuya elección se hizo en alfabetos diferentes; en efecto, la posición de la raya es indicativa del sentido sintáctico de los caracteres en el texto plano. Este dispositivo revela un ingenio criptográfico no del todo original, según veremos, pero resulta evidente la ventaja económica que representa: suprimirlo haría forzoso enlistar alfabetos independientes para combinar cada una de las consonantes, aumentando en dieciocho la cantidad de los renglones en la "clave".

Mas es tiempo ya de precisar nuestro vocabulario técnico y la clasificación de este criptosistema. Juzgando por el registro que venimos

comentando, no se trata ni de una clave ni de un código sino, propiamente, de una *cifra*, como lo delata en primer lugar el hecho de que *los objetos de la encriptación son grafemas y no vocablos*. Además, el paso inaugural de dividir los términos en razón del sitio de las vocales constituye un dato fundamental para clasificarlo en lo particular, mediando comparaciones técnicas con sistemas análogos. Así, en tanto la descomposición léxica previa al cifrado no debe ser total en caso alguno, es decir, seccionando a las palabras letra por letra, este criptosistema reúne la propiedad básica del cifrado digráfico bipartito, consistente en una continua permutación de bigramas –esto es, grupos de dos letras que no necesariamente forman sílabas– organizados en una matriz rectangular,[10] distinguible sin embargo por cuanto la sustitución se genera por una yuxtaposición de numerales e interviene la raya o tilde con la función ya señalada. También acusa rasgos que lo emparentan con la familia de las sustituciones simples multipartitas, pues, exceptuando a los caracteres individuales del alfabeto cuya transformación la norma el renglón 1 y se opera en monogramas –denominados "letras simples" en las instrucciones–, las particiones forman bigramas o trigramas.[11]

El renglón 1, por cierto, es el mecanismo dentro del sistema para cuyo diseño hizo falta una previsión criptoanalítica más alerta, pues de su aplicación surgen los caracteres crípticos de la máxima y más peligrosa frecuencia relativa, empezando naturalmente por las vocales; el peligro es, obviamente, para la seguridad del criptosistema entero. Y es que tal frecuencia resalta en el criptotexto por su aspecto inequívoco, debido a que se juzgó innecesario el empleo de tildes u otro signo auxiliar que tendiese a difuminar las repeticiones excesivas.

La vulnerabilidad del criptosistema I se patentiza tras observar que carece de tres cosas: (i) un grupo de nulos, (ii) los elementos mínimos para generar caracteres homófonos, y (iii) una clave reguladora de las transformaciones. Los llamados nulos son cifras falsas, desprovistas de cualquier significado pero que se introducen para contrarrestar el efecto visual de las frecuencias relativas, buscando así promover una contrariedad analítica en quien

10 Bauer, *Decryped Secrets*, pp. 56-57.

11 Un ejemplo clásico de cifra multipartita es la propuesta por Giovanni Battista Argenti en 1580. El sistema se organiza en un rectángulo donde se distribuyen los elementos de un alfabeto de 10 caracteres arreglados de acuerdo con la posición de una palabra clave. Bauer, *op. cit.*, p. 52.

buscare penetrar la cifra sin autorización. Los homófonos o variantes son conjuntos de equivalencias que se conviene en usar alternativamente para cifrar un mismo grafema o un grupo de caracteres; generalmente se comprenden en la organización de los nomencladores, caso del que utilizó Hernán Cortés en 1532 y 1533.[12] Por último, la clave, en términos propiamente criptológicos, es el instrumento por antonomasia con cuya asistencia se regula el funcionamiento de un criptosistema, a fin de permitir variaciones en el cifrado de un mismo texto plano en momentos sucesivos; esto equivale a decir: cambia la clave periódicamente y determinarás cambios en la forma del cifrado. Este artificio se considera el más apto para impedir a los intrusos en el circuito de la comunicación reservada descubrir el tipo general o la clase específica del criptosistema utilizado. La selección y variación inteligente de las claves es, por tanto, una condición necesaria para fortalecer la seguridad del sistema y, en consecuencia, prolongar su vigencia.

Es verdad que las claves intervienen, por lo común, para gobernar cifras polialfabéticas, siendo el ejemplo clásico la matriz de alfabetos sucesivos conforme al famoso modelo Belaso-Vigenère.[13] Sin embargo, la citada cifra de Alberti es un caso perfectamente funcional de cifrado monoalfabético regulado por una clave, y se puede proponer, dicho sea de paso, como el modelo general de los criptosistemas que aplicaron en ciertos momentos los diferentes bandos antagonistas durante la revolución mexicana.[14] Es notable, además, que el diseño de estos artilugios contiene lo requerido incluso para generar nulos.

No quiero decir, por supuesto, que el sistema oficial elegido por Obregón y Torrens habría sido indefectiblemente más poderoso si se le hubieran incorporado nulos, homófonos y una clave. Desde el punto de vista técnico, sin embargo, es indudable que por su estructura y modo de operación se impone sospechar una infravaloración de la urgencia de

12 Véase Narváez, "Historia y criptología".
13 Las (aparentes) dificultades para decidir si la paternidad de este modelo debe atribuirse al italiano Giovanni Battista Belaso o al francés Blaise de Vigenère se ha convertido en un tópico de la historiografía general de la criptología, que en realidad está injustificado técnicamente. *Cf*. Kahn, *The Codebreakers*, pp. 137, 145-148; Shumaker, *Renaissance Curiosa*, pp. 124-126, y Narváez, "La criptografía de los maderistas", pp. 70-71.
14 Actualmente preparo un ensayo donde analizo los registros criptológicos que inspiraron esta suposición hipotética.

dotarlo con otros implementos reforzadores de su seguridad, aparte de las tildes. No he descubierto documentos donde conste o se insinúe, al menos, que los despachos de Obregón o Torrens, cifrados por este sistema, fueron interceptados y aclarados alguna vez. Acaso no lo fueron en virtud de que cursaron por rutas postales bien salvaguardadas. Pero, si los capturaron y no lograron leerlos, entonces he fallado en observar alguna cualidad especial en el criptosistema, o bien los espías eran lo bastante ineptos –o perezosos– para exhumar su mensaje oculto en tiempo y forma para reportarlo a sus empleadores. Quizá en el futuro alguien obtendrá un material pertinente a la elaboración de una hipótesis fecunda en torno de estas posibilidades.

Resumen y consideraciones finales

1. De lo expuesto se concluye que el método criptográfico en cuestión es, hablando técnicamente, una cifra y no un código. Las instrucciones definen claramente una transformación gradual iniciada por el fraccionamiento de las palabras y para nada recomiendan la codificación.[15]

2. Es evidente que Obregón en 1825 y 1826, y Torrens en 1825, generalmente aplicaron sin fallas el mecanismo,[16] en tanto recurrir a éste, hoy, permite descifrar el contenido de sus despachos (y cifrarlo de nuevo si se desea, naturalmente). El lector puede valorar la justeza de esta conclusión probando a descifrar con la tabla estas líneas en el reservado 14 (1 de noviembre de 1825) de Obregón:

   315 414 619 314 520 519 33 320 321 120 224 54 44 67 15 11
   124 15 619 19 919 321 28 42 11 122 220 115 121 418 220 54

   Como lo comprobará, la traducción literal que surge es “En mi

15 Sería interesante, por ejemplo, que ordenaran una codificación postrera del cifrado, paso lógicamente valioso para incrementar la seguridad del criptosistema.
16 Pero, en más de una ocasión fallaron. Para comentarios técnicos en torno de los errores cometidos por Obregón al cifrar, véase Narváez, “Los despachos codificados”, pp. 1126-1127.

número once reservado digue a V. E. que no se había transpirado", pudiendo hacer más ensayos viendo la figura 2 y confrontando el descifrado en el apéndice 2 de mi artículo primigenio sobre este asunto, o examinando la porción del extracto cifrado de *c.* marzo de 1825, remitido por Torrens desde Colombia (figura 4).

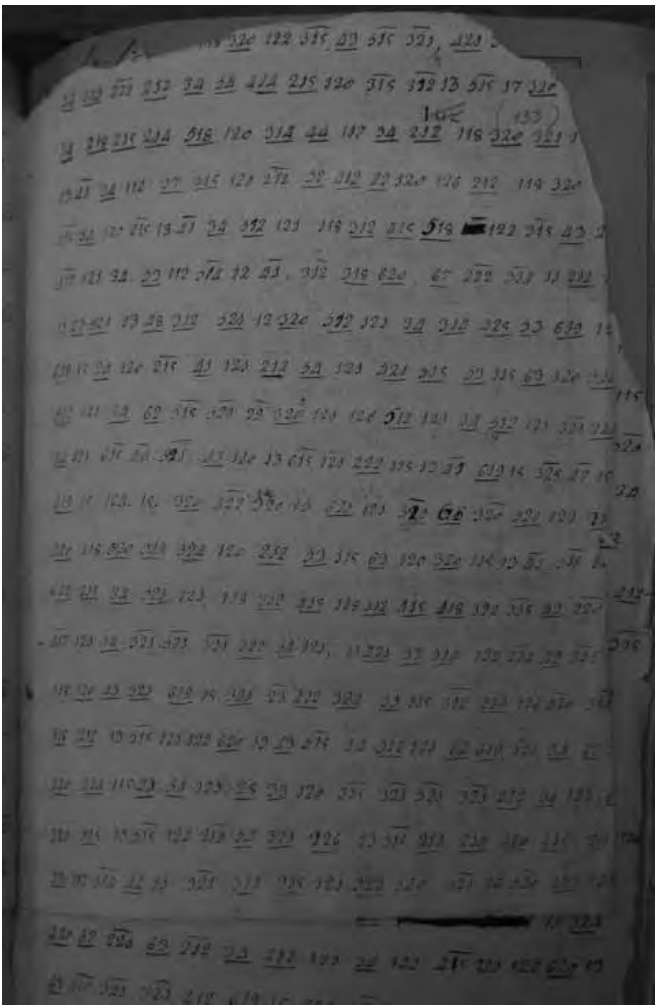

Figura 4. Detalle del extracto cifrado c. marzo de 1825, atribuido a José Anastasio Torrens. Fuente: AHDSREM, L-E-1699 (3ª parte), tomo III, f. 133.

3. Al comentar la ventaja económica de las rayas o tildes, aludí a que un expediente similar tiene precedentes. Veamos un par de casos en la historia de la "criptografía indiana", según la denominó Guillermo Lohmann Villena. Luis Jerónimo Fernández de Cabrera y Bobadilla, conde de Chinchón, gobernó Perú de 1629 a 1639; a poco de haber iniciado este mandato, recibió del monarca español hasta tres "claves" (por motivos políticos y diplomáticos que Lohmann explica).[17] Las dos primeras pertenecen a la familia de los nomencladores, como lo delata el vocabulario de nombres-código y el equipamiento de nulos. El resto de la configuración consiste en una serie de sustituciones simples para cada letra del alfabeto de definición y un grupo de sílabas frecuentes cuya sustitución directa se realizaba con letras, numerales o símbolos varios. En ambos ejemplos, la tilde –Lohmann la llama "línea serpentina"– tiene un papel asignado en elementos determinados del elenco silábico; así, en la "clave" 1 se prescribe cifar ÑI y ÑO con el $\overline{48}$ y el $\overline{49}$ respectivamente; la función específica de la raya es distinguir las equivalencias de estos dígitos de las del 48 y el 49 que deberán ocultar a NI y NO, respectivamente. En este caso, resultaba crucial atender al sentido de la estratagema porque, si bien el alfabeto definitorio utilizado carecía de la Ñ (W=23, con la Z y la Ç intercambiables) para fines prácticos, al parecer se estimó que la fonación exacta de Ñi y ÑO era crucial y, por tanto, ameritaba la designación de sustitutos individuales a cada una.

   La "clave" 2 es más compleja, su alfabeto definitorio es W=22 (con la Z intercambiable por la Ç), incluye homófonos para las vocales y consonantes de aparición frecuente y una carga de nulos más amplia. También aquí las rayas funcionan para distinguir la equivalencia de dígitos repetidos, caso del 12, 14, 16, 18 y 60, usados asimismo para cifrar monogramas. Así, el 12 sólo equivale a F y con raya encima equivale a RI; sin línea el 14 valdrá por G, pero coronado por la "sierpe" valdrá por RU.

   Entre estos métodos y el criptosistema I la indicación gráfica en cuestión está fijada con sagacidad, pero su aparición es

17 Lohmann Villena, "Cifras y claves indianas", pp. 326-328.

necesariamente más continua en el segundo, debido al listado de los renglones conforme al orden sucesivo normal de las vocales.

4. Una observación final. Existen razones documentales, como hemos aprendido, para desechar la hipótesis criptoanalítica del libro de códigos, sin embargo, su corrección técnica persiste en razón de su evidente suficiencia práctica. Por otra parte, debemos reparar en el sentido teórico de un detalle: como lo prueba la operación con la tabla oficial, el cifrado de los elementos en el texto plano devuelve, invariablemente, sustituciones fijas de uno a uno, en razón, obviamente, del monoalfabetismo. Y tal fijación, tal estricta correspondencia no cambia siquiera, como se ha explicado, por la incorporación de las tildes en caracteres determinados; al contrario, se solidifica por la misma causa de que las rayas funcionan en dos únicos sentidos posibles. Todo esto genera un fenómeno curioso: al fijar los guarismos de sustitución para cada monograma, bigrama y trigrama, lo que hacemos en última instancia es asignarles un código irrenunciable. Dicho en otros términos: tan pronto como inicia su operación, este método se condiciona para formar automáticamente una serie de sustitutos unívocos cuya identificación estructural con los componentes de un código se ofrece a sí misma, por así decir, naturalmente. Y esto sucede por la repetición del alfabeto único en su ordenamiento regular dentro de cada fila. Para empeorar las cosas, en ausencia de homófonos u otros auxiliares aumenta su vulnerabilidad al análisis de frecuencias (justo el tipo de criptoanálisis cuyo ejercicio me bastó para decriptar los reservados de Obregón en 2009).

   En vista de lo anterior, terminaré jugando con la idea de que este criptosistema sería más vigoroso si en su diseño se hubieran tomado en cuenta las siguientes previsiones básicas: a) no ajustar la numeración de los renglones al ordenamiento normal de las vocales, b) usar un alfabeto de definición más corto, de W=23 a lo sumo – eliminando la J, la LL, la Ñ y la V por las consideraciones expuestas en un párrafo precedente –; c) formar secuencias de vocales agrupadas en cada renglón hasta limitar su número a cuatro (en el segundo renglón se yuxtapone la serie de la A con la de la E, en el tercero se hace lo

propio con las series de la I y la O, y se deja el cuarto para la U), y d) sobre todo, desordenar los elementos alfabéticos a combinar en cada renglón para dar la impresión de polialfabeticidad.

Nunca concebí a estas propuestas como soluciones ideales, tan sólo creo que las mismas o unas mejor calculadas autorizarían la clasificación técnica, inequívoca, del sistema como una cifra, expulsando de la operación a todos los factores que propician la mutación del cifrado en una codificación automática.

Apéndice. El criptosistema II en las instrucciones oficiales de la Legación Mexicana en Washington (1824)

Esta pieza, en realidad, va inserta como la primera en el expediente, y la he subordinado a la referida como criptosistema I dado el propósito fundamental de este ensayo. Su explicación es concisa, de fácil comprensión y manejo con el auxilio de la tabla adjunta. La transcribo sin modificaciones o agregados de ningún tipo:

Para cifrar

Se encarga ante todas cosas que no se escriba ninguna palabra con abreviatura, sino que el texto y sus palabras contengan todas sus letras: procediendo de esta suerte se dividirán las propias letras del texto de seis en seis, numerando estas secciones con sus numeros ordenados de 1 a 6, y hecho esto, se procederá á cifrar examinando la primera letra de la primera seccion para el primer alfabeto de la tabla: alli se observa el numero que toca á la tal letra, y ese es el que se pone debajo de ella en la cifra. Con la segunda letra se hace lo mismo: id. con la 3ª, 4ª, 5ª, y 6ª. Despues la segunda seccion se cifra por el mismo metodo con el segundo renglon de la tabla: la 3ª. seccion con el tercer renglon: la 4ª con el 4º, la 5ª. con el 5º, y la 6ª con el 6º; y si la cifra tubiere mas, se comienza con el mismo orden.

Para descifrar

Se dividen los numeros de la cifra de seis en seis, señalando estas secciones con los numeros de 1 á 6, y cada seccion segun su numero, asi en el renglon de la tabla por donde se descifra, poniendo debajo del numero la letra que significa.

Exemplo para cifrar

1						2						3		
D	i	o	s	L	i	b	e	r	t	a	d	é	Y	n
4	9	17	21	12	9	27	3	18	20	26	2	27	21	10

3			4						5	
d	e	p	e	n	d	e	n	c	i	a
26	27	13	24	7	23	24	7	22	25	17

Nota: Aun cuando no se cifre toda la carta sino algunas palabras […], siempre se observará con estas la misma division de secciones en los terminos dichos, lo mismo que si las palabras cifradas estubieran sin intercalacion de palabras no cifradas, ó estubieran continuadas.
Rúbrica[18]

18 AHDSREM-AEMEUA, “Reglas para cifrar y descifrar”, leg. 1, exp. 4, ff. 42-43.

La tabla luce así:

1	a	b	c	d	e	f	g	h	i	j	k	l	ll	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
2	c	d	e	f	g	h	i	j	k	l	ll	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z	a	b
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
3	f	g	h	i	j	k	l	ll	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
4	i	j	k	l	ll	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
5	l	ll	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	k
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
6	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	ll	m	n	ñ	o
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

Ofrece siete aspectos técnicos dignos de una inspección detenida:

1. El sistema es polialfabético, de W=27 por la inclusión de la LL, la Ñ y la V (como en el criptosistema I).
2. Es un algoritmo de sustitución múltiple, basado en el principio históricamente derivado de la llamada "cifra de Julio César" –descrita en todo manual respetable de criptología– y consistente en desplazar las letras a la derecha una cantidad convenida de lugares, lo cual se verifica desde el segundo alfabeto en estas proporciones: del 1 al 2, 2 lugares; del 2 al 3, 4 lugares; del 3 al 4, 4 lugares; del 4 al 5, 4 lugares, y del 5 al 6, 6 lugares. Por supuesto, la aritmética modular sería el instrumento básico para graficar en una ecuación la dirección de los movimientos.
3. Aunque la propiedad no se expresa en las instrucciones, resulta evidente que el sistema depende de claves para gobernar el paso entre los diferentes alfabetos. Digo claves porque, en efecto, son varias y gradualmente modificables, apareciendo en sucesión debido al fraccionamiento textual en seis unidades. El texto plano es concebido como un todo unitario, predisponiendo a cifrar de corrido, por así decir, cúmulos de letras y no las letras formadoras de cada palabra, diferencia notable respecto del criptosistema I. De este modo, el requisito de usar el primer alfabeto para encriptar el primer sexteto de letras, el segundo para su correspondiente, y así, determina que las agrupaciones de grafemas en cada caso forman su propia clave de cifrado. Valiéndonos del ejemplo en el documento,

tenemos que el grupo “DiosLi” guía la selección en el alfabeto 1 del numeral sustituto correspondiente a cada una de sus letras: la D está en el lugar 4, la I en el 9, la O en el 17, etcétera, hasta quedar 4 9 17 21 12 9. Ocurre lo mismo con el siguiente agregado, “bertad”, operando en el segundo alfabeto, y el proceso se repite hasta agotar las filas.

4. Considerando lo anterior, se aprecia la manera efectiva en que funciona la polialfabeticidad, o sea, la nivelación de las frecuencias relativas: supongamos que en el texto plano a cifrar ocurre una segunda vez el conjunto “DiosLi”, pero a tal altura que para cifrarla deberá usarse el renglón 4 de la tabla; el criptotexto se leerá entonces 23 1 9 13 4 1 y no 4 9 17 21 12 9. Surgirían guarismos novedosos al experimentar la misma encriptación con la guía de un renglón distinto. Es fácil de observar la repetición del 1 en el primer ejemplar y del 9 en el segundo, pero semejante dato no pone en riesgo inmediato la seguridad del sistema, debiéndose imaginar todas las ocasiones en que el 1 y el 9 aparecerán en un criptotexto completo y no fragmentario: la suma podría ser formidable, sin embargo, la estructura del sistema basta para moderar la fijación de equivalencias invariables (y también, por consiguiente, vuelve innecesario el recurso a las tildes). Así se produce una rotación seriada de los alfabetos tras alterar su ordenación por el desplazamiento de las letras a capricho, lo que sería lógicamente imposible si el alfabeto se repitiera invariablemente de la A a la Z fila tras fila, como sucede en la tabla del criptosistema I.
5. Las equivalencias múltiples que surgen de la manera señalada pueden considerarse homófonos de un carácter determinado. Es una proposición válida para fines descriptivos, me parece, aunque desde la perspectiva rigurosamente criptológica se podría rechazar como trivial o innecesariamente forzada.
6. La falta de nulos puede comprometer su seguridad. Habría sido fácil crearlos y distribuirlos con perspicacia: previa eliminación de la LL, la Ñ y la V, se agregan tres columnas en sitios planeados y en la coordenada de cada fila se inscribe un símbolo, una figura estrambótica o cualquier otro carácter exento de significado lingüístico, pero que

se combinará también con el propósito deliberado de confundir a quien intente penetrar en el secreto del mensaje.

7. Este criptosistema es históricamente moderno, pues la organización básica de los alfabetos en bloques de 6, 8 o 10 filas fue muy común para generar cifras polialfabéticas por desplazamiento –con tablas, discos y tiras móviles en sentido horizontal, por citar los tres artificios más socorridos– en el siglo XX, por ejemplo en España y México (desde el inicio de la revolución y hasta las postrimerías de la década de 1920, según lo he podido comprobar en archivos varios). Con todo, me permitiré comentar sucintamente la estructura de un antecesor muy lejano en el tiempo para evaluar sus analogías formales con el criptosistema II, entretenimiento que podría despertar un interés teórico. Se trata de una "clave" usada en el año inaugural del siglo XVII por los provinciales de la Compañía de Jesús en Perú.[19] Hasta donde sé, nadie la ha revisado con alguna profundidad –aunque sin apoyarse en comparaciones– salvo Lohmann Villena, el investigador por excelencia de la "criptografía indiana". La "clave" es un rectángulo de alfabetos en bloque. (Ver siguiente tabla)

	41	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**	**51**	**52**	**53**	**54**	**55**	**56**	**57**	**58**	**59**	**61**	**62**
1	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	Z	A	B
2	U	Z	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T
3	M	N	O	P	Q	R	S	T	U	Z	A	B	C	D	E	F	G	H	I	L
4	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	Z	A
5	R	S	T	U	Z	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q
6	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	Z	A	B	C	D

El alfabeto de definición excluye la J, la V y la Y, identificándose a la V con la B y la J y la Y con la I por similitud fonética. Las instrucciones, nos dice Lohmann:

> […] Recomendaban que se buscara la primera letra del texto que se deseaba criptografiar en el alfabeto número 1, inscribiéndose en la comunicación el número que se hallare encima; la segunda letra se tomaría del alfabeto número 2; la tercera, del número 3, y así sucesivamente, hasta el número 6, volviendo entonces a comenzar por el alfabeto número 1. Ni se tomarían dos letras del

19 Lohmann Villena, *op. cit.*, pp. 321-323.

mismo renglón sucesivamente, ni tampoco se omitiría ninguno, habida cuenta de que un solo yerro de esta índole tornaría poco menos que indescifrable el texto sometido a interpretación.[20]

La fórmula de recorrer cíclicamente los alfabetos para localizar cada elemento de sustitución es idéntica a la del criptosistema II. Asimismo, en ambos métodos hay cero espacio para nulos, tildes u otros signos auxiliares. La coincidencia fundamental, empero, es la prescripción de cifrar con el gobierno de una clave. Ya expliqué cómo, en el criptosistema II, la intervención de claves (autoclaves, de hecho) cíclicamente renovadas debe inferirse por la reflexión sobre el mecanismo, pero lo cierto es que la rotación alfabética se debe a ellas. Por su parte, la cifra de los jesuitas peruanos funciona por el expediente de una sola clave materialmente identificada, digamos, como la única reguladora de las transformaciones criptográficas biyectivas (esto es, tanto las que producen criptotexto como las que lo revierten a texto plano). Esa clave, CUMBRE, se lee en la primera columna. Lohmann, cosa rara, la pasó por alto completamente, luego su descripción es técnicamente defectuosa. Mas resulta importantísimo reparar en el dato, pues a la clave se debe aquí el desplazamiento alfabético entre la sucesión de filas y, por tanto, la nivelación de las frecuencias relativas. Como vemos, en el renglón 1 el alfabeto empieza en la C y termina en la Z, reiniciado sin embargo en la A sin interrupción; en el renglón 2 empieza con la U y termina en la Z, reiniciando nuevamente con la A, y así MBRE van cada una jalando, por así decir, a las letras subsiguientes en sus respectivos alfabetos para ocasionar los desfases observados cuando se leen las columnas. La seguridad del sistema, como es lógico, dependía de mudar constantemente la palabra clave.

Ignoro si Torrens, Obregón u otro diplomático mexicano practicó alguna vez con el criptosistema II. Acaso la cancillería esperaba que Obregón y Torrens, por motivos de seguridad, alternaran el uso de los dos métodos entregados junto con las instrucciones. He aquí el germen de una hipótesis criptológica que muy bien podría explicar aquella doble provisión. Como sea, lo mejor será esperar que otras investigaciones técnicas e históricas

20 *Ibid*., p. 322. Entonces, la palabra Santiago quedaría cifrada 56 43 42 58 55 58 45 56.

devuelvan materiales adecuados para nutrir la mejor hipótesis y despejar esta incógnita.

Fuentes consultadas

Archivos

AHDSREM, Acervo Histórico Diplomático de la Secretaría de Relaciones Exteriores de México.
Fondo: Archivo de la Embajada de México en los Estados Unidos de América (AEMEUA).

Bibliografía

Bauer, F. L., *Decrypted Secrets. Methods and Maxims of Cryptology*, Berlin, Springer, 2002, 3rd edition.

Kahn, David, *The Codebreakers. The Story of Secret Writing*, New York, MacMillan Publishing Co., Inc., 1967.

Lohmann Villena, "Cifras y claves indianas. Capítulos provisionales de un estudio sobre criptografía indiana", en *Anuario de Estudios Americanos*, t. XI, 1954, pp. 287-380 + láminas.

Narváez, Roberto, "La criptografía de los maderistas (1910-1911). Análisis pormenorizado del criptosistema de Gabriel Leyva Solano y Francisco I. Madero (1910)", en *Memorias de la Academia Mexicana de la Historia*, t. LI, 2010, pp. 47-89.

_____, "Decodificación de un despacho de Pablo Obregón fechado en 1826", en *Historia mexicana*, vol. LIX, núm. 1 (233), julio-septiembre 2009, pp. 443-448.

_____, "Los despachos codificados de Pablo Obregón desde Washington en 1825. Análisis y dos decodificaciones", en *Historia mexicana*, vol. LVIII, núm. 3 (231), enero-marzo 2009, pp. 1093-1153.

_____, "Dos criptosistemas empleados por el coronel José Anastasio Torrens en Colombia (1825-1826). Una contribución a la historia de la criptología mexicana", en *Memorias de la Academia Mexicana de la Historia*, tomo XLIX, 2007-2008, pp. 7-43.

_____, "Historia y criptología. Reflexiones a propósito de dos cartas cortesianas", en *Estudios de historia novohispana*, vol. 36, enero-junio 2007, pp. 17-62.

Shumaker, Wayne, *Renaissance Curiosa*, Binghamton, New York, Center for Medieval and Renaissance Studies, 1982.