ARCHIVOS Y DOCUMENTOS

EL CRIPTOSISTEMA DEL VICECÓNSUL GUILLERMO S. SEGUÍN (1916)

Roberto Narváez
Instituto Cultural Helénico

Como lo sugiere la revisión de ciertos grupos documentales en varios archivos, al promediar la segunda década del siglo XX la cancillería mexicana tenía un sistema relativamente firme para administrar y archivar la correspondencia reservada en cifra o código que mantenía con sus enviados, agentes, embajadas y consulados, tanto por medio del correo postal como por vía telegráfica. Limitándonos al servicio consular y las embajadas, con determinada frecuencia les informaba de la conveniencia de sustituir las "claves" –como genéricamente solían llamarlas– que hasta entonces habían empleado ambas partes para incrementar la seguridad de sus mensajes reservados, adjuntando a la vez el nuevo método criptográfico a utilizar en lo sucesivo. El análisis técnico de estos ejemplares revela que prácticamente nunca implicaban una genuina innovación respecto de sus predecesores, y de ordinario representaban apenas una versión modificada en aspectos marginales de los mismos. La tendencia normal era usar criptosistemas de sustitución a partir de uno o más alfabetos, disponiendo una palabra o serie

de números a manera de clave para potenciar la transformación a cifra del texto plano (es decir, automáticamente legible como perteneciente a una lengua conocida) requerido de secrecía. El modelo de la sustitución polialfabética organizado de acuerdo con una matriz de alfabetos apilados, tradicionalmente –pero de manera inexacta– atribuido a Blaise de Vigenère, y el arcaico nomenclátor, gozaban de predilección especial. En cuanto a los códigos (recordar que "código" no es sinónimo de cifra o criptograma), eran poco socorridos, acaso debido a las mayores dificultades que imponen la confección y el manejo de un libro de códigos propiamente dicho, aun para la comunicación telegráfica.

La observación formal muestra también que, entre los criptosistemas de la serie bajo consideración, ninguno aparece firmado por alguien a quien debiera imputarse su diseño. Esta circunstancia también resalta en la documentación de la misma clase generada por cancillerías de otros países. El hecho se debe interpretar como un signo de precaución elemental, pues un servicio diplomático tiene buenas razones para evitar comprometer la identidad de sus criptógrafos. No estoy seguro, sin embargo, de que la Secretaría de Relaciones Exteriores (SRE) de México, durante la guerra de revolución y hasta bien entrada la década de 1920, por lo menos, tuviera criptógrafos especialistas en su nómina; por especialistas no me refiero, por supuesto, a profesionales en el sentido en que actualmente se habla de criptólogos titulados, sino a personas hábiles para refinar o alterar técnicamente los métodos más poderosos disponibles con aditamentos realmente originales, o, incluso, desarrollar criptosistemas cuya estructuración pudiese incorporar la prueba de un teorema radicalmente nuevo en matemáti-

cas. A reserva de investigar esto más a fondo, el examen de los registros a mi alcance me impide creer que tal era el caso, pues, como he dicho, en aquella coyuntura todavía era vigente la costumbre decimonónica de hacer ajustes mínimos a ciertos métodos clásicos de sustitución o transposición y presentarlos como versiones menos frágiles que sus antecesoras, calificándolas en ocasiones, incluso, de indescifrables o "absolutamente indescifrables".[1] Parece, así, lo más creíble por ahora que en estos menesteres el esfuerzo de la cancillería mexicana se redujese a seleccionar métodos de manuales o enciclopedias y adaptarlos conforme a los requerimientos de la lengua española, y que su conocimiento criptológico general era el propio de aficionados. Alfonso Reyes, por ejemplo, citó en algunos de sus ensayos el libro *Ciphergrams* (1932, 1ª edición), del eminente criptólogo estadounidense Herbert O. Yardley (1889-1958), como fuente para entender en tales asuntos;[2] quizá Reyes, por indicación de sus superiores en la cancillería, manejó ese volumen para cifrar mensajes durante alguna de sus misiones diplomáticas posteriores a 1932.

Sea lo que fuere de lo dicho en el párrafo anterior, una cosa es indudable: los propios diplomáticos, embajadores o cónsules, podían comentar críticamente los métodos de cifrado a su disposición e, incluso, proponer criptosiste-

[1] De hecho, el sistema que presento en este trabajo fue calificado de indescifrable, según veremos. Como "absolutamente indescifrable" fue puesta en circulación, por ejemplo, la "clave Murciélago", que estuvo activa para todos los consulados de México en Estados Unidos entre 1916 y 1917. Véase Narváez, "Criptosistemas".

[2] Véase, por ejemplo, "Hermes o de la comunicación humana", en Reyes, *La experiencia literaria*, p. 32.

mas ellos mismos. De este último caso, el más raro, constituye un ejemplo muy interesante la "clave" recomendada por Guillermo S. Seguín en 1916, cuando fungía como vicecónsul en San Francisco, California. Se trata de dos folios mecanografiados que se resguardan en el Acervo Histórico Diplomático de la Secretaría de Relaciones Exteriores de México (AHDSREM), fondo Archivo de la Embajada de México en Estados Unidos de América (AEMEUA), legajo 491, expediente 4, ff. 14-15. A continuación *(i)* transcribiré el folio principal, donde Seguín expone los motivos para sugerir el método y describe su funcionamiento; *(ii)* mostraré la fotografía del folio complementario con la "plana de claves", y para terminar comentaré sobre dos cosas: *(iii)* las razones que inspiraban a Seguín confianza en la viabilidad de su propuesta, y *(iv)* las características técnicas fundamentales del criptosistema.

(I) FOLIO PRINCIPAL[3]

EN VISTA de que las claves que hasta la fecha se han venido usando entre la Secretaría de Relaciones Exteriores y el Servicio Consular, si bien es cierto que son simples y su uso es fácil, también lo es que, un tercero, sin clave alguna, puede con facilidad descifrar el contenido de los mensajes etc. y como ello puede causar graves perjuicios a los intereses de nuestra patria, sobre todo en los actuales momentos, y considerando que es de urgencia establecer un sistema de claves indescifrables, el suscrito, ha creido [*sic*] de oportu-

[3] AHDSREM-AEMEUA, leg. 491, exp. 4, f. 14.

nidad someter a la aprobación de la Secretaría de Relaciones el siguiente sistema para el uso de las claves:

Se toma como base la PLANA DE CLAVES que va adjunta. Cada "clave" consistirá de una COMBINACION de CINCO renglones. Las combinaciones pueden formarse con renglones consecutivos o salteados, siempre que se den a conocer los números de cada renglón que se usó por el órden que se fueron tomando. Para evitar confusión, la Secretaría designará a cada oficina Consular la combinación que debe usar, dando los números de cada renglón. Pero esto no es del todo necesario, pues cada Cónsul puede usar una combinación distinta cada vez que use la clave con sólo dar los números al final del mensaje, éste podrá ser descifrado sin dificultad. También puede adoptarse el sistema que la Superioridad designe a cada Oficina Consular una combinación de renglones para cada día de la semana, y en caso de que por algún motivo se crea conveniente, éstas combinaciones pueden ser cambiadas por otras, sin que se perjudique la plana de claves, puesto que con la simple plana es imposible descifrar un mensaje si no se sabe qué COMBINACIÓN de renglones se usó.

Para cifrar las palabras, se van tomando las letras minúsculas correspondientes a cada mayúscula agrupándolas de CINCO EN CINCO, tomando UNA LETRA DE CADA RENGLÓN DE LA COMBINACIÓN de cinco renglones, empezando en cada grupo de cinco letras de nuevo con el primer renglon [*sic*] de la combinación, v. g. si se usa la combinación 7 6 5 2 9, la primera letra será tomada del renglón número 7, la segunda letra del 6, la tercera del 5 y así sucesivamente, principiando de nuevo cuantas veces sea necesario. Para descifrar, la operación es la misma en sentido inverso.

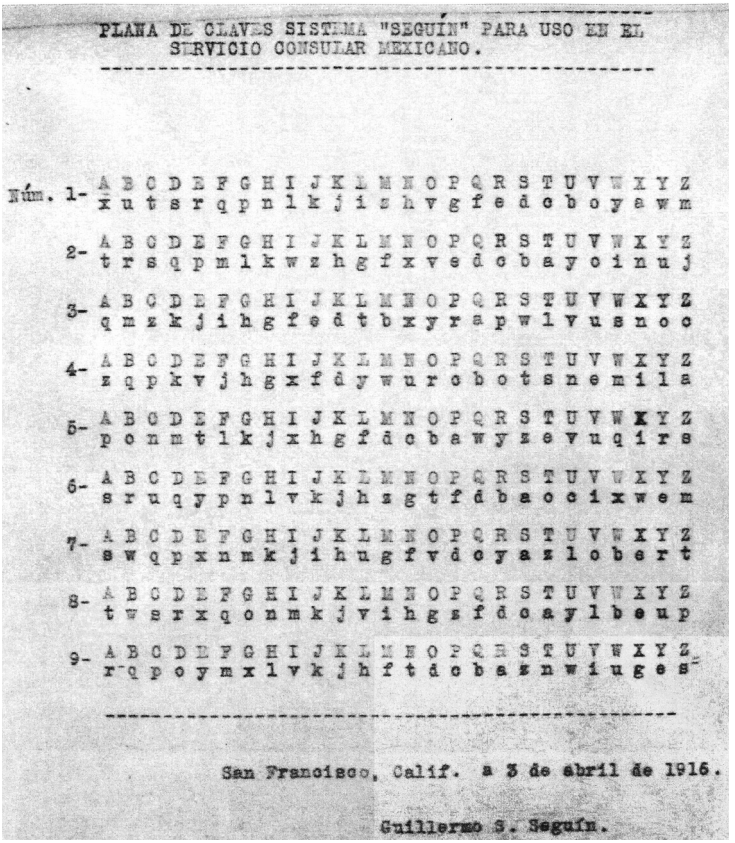
Si se decidiera que se designara a cada Consul [*sic*] una combinación para cada día de la semana, el cónsul puede copiar en papel separado cada combinación y colocarla por orden progresivo, y de este modo se facilitaría la labor, tanto para cifrar como para descifrar.

Como este sistema es susceptible a diversas variaciones sobre el mismo principio, ya cambiando la plana, las combinaciones etc. etc. no vacilo en creer que la Secretaría verá desde luego su conveniencia, y de aceptarla, comlacerá [*sic*] grandemente los esfuerzos del autor.

San Francisco Cal. 3 de abril de 1916.
Guillermo S. Seguín.
(Firmado)

Al C. Consul [*sic*] General de Mexico [*sic*]
San Francisco, Cal.

(II) FOLIO COMPLEMENTARIO[4]



PLANA DE CLAVES SISTEMA "SEGUÍN" PARA USO EN EL SERVICIO CONSULAR MEXICANO.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Núm. 1-	x	u	t	s	r	q	p	n	l	k	j	i	z	h	v	g	f	e	d	c	b	o	y	a	w	m
2-	t	r	s	q	p	m	l	k	w	z	h	g	f	x	v	e	d	c	b	a	y	o	i	n	u	j
3-	q	m	z	k	j	i	h	g	f	e	d	t	b	x	y	r	a	p	w	l	v	u	s	n	o	c
4-	z	q	p	k	v	j	h	g	x	f	d	y	w	u	r	c	b	o	t	s	n	e	m	i	l	a
5-	p	o	n	m	t	l	k	j	x	h	g	f	d	c	b	a	w	y	z	e	v	u	q	i	r	s
6-	s	r	u	q	y	p	n	l	v	k	j	h	z	g	t	f	d	b	a	o	c	i	x	w	e	m
7-	s	w	q	p	x	n	m	k	j	i	h	u	g	f	v	d	c	y	a	z	l	o	b	e	r	t
8-	t	w	s	r	x	q	o	n	m	k	j	v	i	h	g	s	f	d	c	a	y	l	b	e	u	p
9-	r	q	p	o	y	m	x	l	v	k	j	h	f	t	d	c	b	a	z	n	w	i	u	g	e	s

San Francisco, Calif. a 3 de abril de 1916.

Guillermo S. Seguín.

[4] AHDSREM-AEMEUA, leg. 491, exp. 4, f. 15.

(III) ¿POR QUÉ CONFIABA SEGUÍN EN LA VIABILIDAD DE SU CRIPTOSISTEMA?

Guillermo S. Seguín nació el 1 de noviembre de 1892 en Nuevo Laredo, Tamaulipas. No debemos confundirlo con Guillermo M. (Martín) Seguín, que fue su padre (nacido el 30 de enero de 1865 en Camargo, Tamaulipas).[5] De acuerdo con sus respuestas a un cuestionario girado por la sección general de la Dirección General de Consulados, fechado el 11 de mayo de 1916,[6] Seguín, hijo, completó en Piedras Negras, Coahuila, la instrucción primaria y cursó el "cuarto año de preparatoria" y "un año de comercio" en Estados Unidos. Afirma en el mismo lugar que recibió del Draughon's Practical Business College de San Antonio, Texas, el título de estenógrafo, y declara que su profesión está en la industria. Tras mencionar los puestos públicos o privados en los que sirvió durante los gobiernos previos al de Carranza, señala entre sus méritos como "adicto a la revolución Constitucionalista" la ejecución de tres responsabilidades: agente privado en San Antonio, Texas ("pendiendo del Consulado de Eagle Pass"), "taquígrafo traductor (en campaña) de la Secretaría de Relaciones Exteriores" en diferentes localidades, y "oficial segundo de Cancillería, comisionado en la Secretaría Particular" de Isidro Fabela (1914), época en la que asistió a la ocupación de Veracruz y pasó a ser "Jefe Accidental de la Sección de Información de Relaciones". El 23 de noviembre de 1914 fue nombrado vicecónsul canciller del Consula-

[5] AHDSREM, 5-7-53, f. 77. En esta carpeta se incluyen, mezclados, los expedientes de estos dos Seguín.
[6] AHDSREM, 5-7-53, ff. 77-77bis.

do General en San Francisco, California (tomando posesión siete días después).

Tenemos, pues, a Guillermo S. Seguín recibiendo un importante cargo consular cuando acababa de cumplir los 22 años de edad, como inicio de una carrera que se prolongaría por lo menos hasta 1921, trabajando con diferentes rangos en los consulados de San Francisco, Los Ángeles, Laredo y Nueva York. Los detalles de su formación previa, desde luego, nos interesan especialmente porque sugieren una explicación a su iniciativa criptográfica de 1916.

Se antoja muy probable que haya sido durante 1914, al operar como agente privado, taquígrafo traductor en campaña y jefe accidental de la Sección de Información de Relaciones, cuando ganó experiencia en el uso de métodos de cifrado para las comunicaciones del gobierno al que servía. Los criptogramas que facturaba entonces el Gobierno Constitucionalista eran elementales, básicamente de permutación monoalfabética, muy débiles en comparación, por ejemplo, con los de sustitución bipartita cuyo empleo llegaron a convenir Carranza y Madero un año antes.[7] No le habría sido difícil a Seguín, por tanto, lograr su dominio, pareciendo su labor tan satisfactoria al propio Carranza que éste, en telegrama remitido a Seguín, padre (entonces en el Consulado de Eagle Pass), el 5 de julio de 1914, le escribe: "Sírvase decirme cuando [*sic*] puede venir su hijo Guillermo, pues necesito en esta Secretaría sus servicios".[8] Por supuesto, es posible que Carranza estuviera esperando un apoyo que iría más allá de la mera práctica del cifrado; como

[7] Narváez, "Criptosistemas".
[8] AHDSREM, 5-7-53, f. 101.

sea, me parece lícito imaginar a Guillermo S. Seguín familiarizándose con cuestiones criptográficas mientras colaboró con los constitucionalistas en aquel año. Acaso en San Antonio leyó algún material sobre el tema en inglés, o bien estudió libros o manuales que le proporcionaron sus empleadores con la deliberada intención de entrenarlo en semejantes faenas. También es posible que sus actividades como taquígrafo incluyeran el descifrado de comunicaciones crípticas interceptadas al enemigo, reuniendo de tal modo una "experiencia en campo" suficiente para cumplir sus obligaciones. Resultado de todo esto habría sido un progreso de sus facultades críticas en torno a los principios y técnicas criptográficas, al punto de considerarse apto para configurar un sistema novedoso, bien articulado, lo bastante para resistir las embestidas del criptoanálisis con esperanza de prevalecer.

(IV) BREVE ANÁLISIS TÉCNICO DEL CRIPTOSISTEMA DE SEGUÍN

Ante todo es conveniente apreciar, como partes fundamentales del documento íntegro, la prologal exposición de motivos para ofrecer el espécimen, las recomendaciones para flexibilizar su aplicación administrativa y la calidad de las reflexiones criptológicas que se distribuyen por todo el texto. Esto nos permite valorar dos cosas, primera, la franqueza de Seguín al condensar en cuatro líneas una crítica mesurada pero segura contra la calidad de la criptografía vigente entre la SRE y sus consulados, y segunda, los alcances de su conocimiento criptológico personal. Que comprendía el significado del llamado criptoanálisis, una de las

divisiones fundamentales de la criptografía, no hay duda, como lo prueba su aserto "un tercero, sin clave alguna, puede con facilidad descifrar el contenido de los mensajes". Si fue por elipsis que apuntó solamente "tercero" y no "tercero no autorizado", poco importa, pues lo cierto es que pensaba en esa eventual ocurrencia: la penetración forzada de un criptograma interceptado cuyo algoritmo se desconoce, utilizando el análisis de frecuencias o alguna otra estrategia sugerida por el reconocimiento formal –incluyendo la longitud aparente– y estructural del criptotexto. Los criptosistemas diplomáticos mexicanos que estuvieron vigentes entre 1824 y 1926, según lo puedo afirmar por mis investigaciones, pertenecen generalmente a la clase de cifras de nomenclátor, de sustitución polialfabética estilo Vigenère o Gronsfeld (una cándida reorganización del arreglo *a la* Vigenère), o monoalfabética estilo Julio César, siendo por tanto endebles ante los ataques enfocados al conteo de las frecuencias relativas de aparición de ciertos caracteres en el mensaje después de la transformación, que sugieren hipótesis para ubicarlos en una clase particular adecuada y razonar inductivamente o por analogía sobre sus cualidades estructurales y de seguridad, hasta conseguir descifrarlos. Pienso que Seguín se refiere a la presencia de tales inconveniencias en las "claves" a que alude. El núcleo de su proyecto consistía en establecer un mecanismo de encriptación capaz de reducir al mínimo la repetición en el criptotexto de las constantes sintácticas naturales de un texto plano en español, o, dicho llanamente, un mecanismo inmune al análisis de frecuencias. Creía que lograr esto era lo exactamente requerido para generar "cifras indescifrables". Ya discutiremos hasta qué punto era exagerada, por decir lo menos, esta creencia.

También es digno de inquisición su enunciado "este sistema es susceptible a diversas variaciones sobre el mismo principio", pues delata que admitía una definición teórica general bastante apropiada de la criptografía como un instrumento útil, en última instancia, para proteger a las comunicaciones reservadas con medidas de seguridad técnicamente planeadas. No es evidente, sin embargo, a cuál principio se refiere, es decir, de dónde lo juzga deducible por análisis de la estructura y funcionamiento total del criptosistema. Para comentar debidamente este punto, es preciso ejecutar antes ese mismo análisis.

Dada la organización del esquema en 9 grupos de alfabetos diseñados para determinar sustituciones recíprocas, podemos clasificarlo como un método de encriptación polialfabética. De hecho, se trata de una variación del modelo descrito por Giovanni Battista Porta (también referido como Giambattista della Porta) en *De furtivus literarum notis* (1563),[9] un caso memorable de alfabetos múltiples mezclados cuya operación se regía por la siguiente tabla:

AB	a	b	c	d	e	f	g	h	i	j	k	l	m
	n	o	p	q	r	s	t	u	v	w	x	y	z
CD	a	b	c	d	e	f	g	h	i	j	k	l	m
	z	n	o	p	q	r	s	t	u	v	w	x	y
EF	a	b	c	d	e	f	g	h	i	j	k	l	m
	y	z	n	o	p	q	r	s	t	u	v	w	x
…													

[9] Bauer, *Decrypted Secrets*, pp. 117-118.

WX	a	b	c	d	e	f	g	h	i	j	k	l	m
	p	q	r	s	t	u	v	w	x	y	z	n	o
YZ	a	b	c	d	e	f	g	h	i	j	k	l	m
	o	p	q	r	s	t	u	v	w	x	y	z	n

El principio del funcionamiento[10] consiste en una permutación autorrecíproca donde tanto el cifrado como el descifrado surgen como un reflejo, o involución,[11] entre los dos alfabetos de cada renglón. Las mayúsculas en la columna izquierda corresponden al alfabeto de la clave, mientras que los alfabetos en minúscula corresponden a los alfabetos del criptotexto y del texto plano. Éstos pueden operar en dos sentidos, cifrando o descifrando, dependiendo de la letra en la clave con cuyo gobierno se esté realizando la transformación y de la posición del carácter a cifrar o descifrar en los pares de alfabetos. Por ejemplo, si usamos la clave ABAD para cifrar SEGUÍN, la A nos indica que busquemos la S en uno de los alfabetos a su derecha y la sustituyamos con la grafema situada encima o por debajo de ella; en este caso, hallamos a la S debajo de la F, de modo que este carácter es el sustituto críptico; guiándonos por la B, tenemos que la E aparece en la fila superior, así que la R ocupará su sitio en el criptotexto, y continuamos así para ocultar el resto del apellido, notando como siempre habrá la posibilidad de utilizar ambos alfabetos en la columna de la derecha.

Es manifiesta la identidad de organización entre los grupos de alfabetos pareados en este modelo y en la "plana

[10] La tabla antecedente se adaptó de la versión impresa en PARKER HITT, *Manual for the Solution*, p. 56.
[11] BAUER, *Decrypted Secrets*, pp. 44-45.

de claves" (véase el apartado II *supra*) de Seguín: el primer renglón exhibe al alfabeto en su ordenamiento normal, el segundo en una transposición calculada (mucho más caprichosa en Seguín). Lo mismo sucede en cuanto a la rotación entre los alfabetos conforme a los dictados de una clave. Otra similitud es la carencia de signos nulos. Una diferencia significativa, desde la perspectiva estructural e histórica, es que Seguín prescribe la formación de claves, o "combinaciones" en su vocabulario, con dígitos agrupados de cinco en cinco, una particularidad relacionada no tanto con estrategias criptográficas como con la necesidad de satisfacer determinadas condiciones de la transmisión telegráfica.

Ahora, el principio fundamental de la permutación es básico para regular las transformaciones a cifra y el descifrado en los dos ejemplares, si bien el de Seguín no está dispuesto para la involución: el alfabeto superior aparece unívocamente como el de definición (de longitud 26, por exclusión de la Ñ y la LL), esto es, del texto plano, y el inferior como el del criptotexto, de manera que las conversiones deben hacerse invariablemente de arriba abajo para cifrar y de abajo arriba para descifrar. Además, la provisión de caracteres en el alfabeto de la clave es precisamente la mitad de los que se pueden contar en el modelo de Porta.[12] En efecto, valiéndonos de la clave 76529 que improvisa el mismo Seguín en el folio principal, y siguiendo su descripción,

[12] Siendo irrelevante para los fines de esta explicación el que Porta use letras y no números como elementos controladores del cifrado, y es que en un trazado como el de Seguín sería lícito, para potenciar la involución, ubicar hasta nueve pares de números, del 1 al 18, en la columna de la izquierda (1-2/3-4/5-6/7-8/…/17-18), y convenir en que se "combinarán" como "claves" análogas técnicamente a las de Porta.

tomamos del alfabeto de mayúsculas en el renglón 7 la S y la transformamos en A, en el renglón 6 tomamos la E y la cambiamos por Y, en el renglón 5 ubicamos la G y la encriptamos como K, y tras hacer lo mismo con la U, la I y la N, tenemos a su apellido velado con las grafemas AYKYVF, recordando que la clave debe reiniciar siempre, completa y en el mismo orden, cuando la palabra en turno para cifrar tiene más de cinco letras. Por el mismo procedimiento cifra-mos *Historia Mexicana* así: KVZADYVP GYIWPSGP.

Es de observar, sin embargo, que Seguín realmente no aclara en dónde se han de elegir los caracteres crípticos; a mi juicio, la prescripción "se van tomando las letras minúsculas correspondientes a cada mayúscula agrupándolas de CINCO EN CINCO, tomando UNA LETRA DE CADA RENGLÓN DE LA COMBINACIÓN de cinco renglones", tal y como aparece, resulta vaga, pues no especifica en cuál miembro alfabético, por así decir, que compone cada renglón debe ubicarse el carácter para cifrar, lo que vuelve difícil entender el sentido exacto de la correspondencia criptográfica entre las minúsculas y las mayúsculas. He asumido, en fin, que la dirección es de arriba abajo por considerar, como ya expliqué, al ordenamiento normal del alfabeto español en el par superior de cada renglón como el alfabeto del texto plano y por estimar a esta cifra como una variación del consagrado modelo Vigenère.

Es asimismo notable la singular terminología técnica de Seguín. Lo que denomina "combinación", es decir, el agregado de cinco números elegidos a placer, en realidad es la clave para gobernar el sistema, mientras la llamada "plana de claves" representa la serie de alfabetos cuya "combinación" indica, sin más, el paso de uno a otro de acuerdo con

la prescripción de la clave numérica. En una palabra, la clave determina una combinación de alfabetos para el cifrado, y la mudanza en la clave determina una mudanza combinatoria en el empleo de los alfabetos. En síntesis, el vicecónsul tiene razón cuando afirma que el cambio de combinaciones no "perjudica" la "plana de claves", no obstante su fraseología es extraña desde el punto de vista criptológico; en rigor, debió decir, o exponer con la sencillez y brevedad obligadas para la ocasión, que a pesar del cambio de las claves la estructura de los alfabetos mutuamente recíprocos del criptotexto y el texto plano mantiene su funcionalidad, y la mantendrá en tanto la estrategia técnica específica para formar la clave no se altere. Porque es manifiesto que, considerando las combinaciones posibles en razón de los nueve alfabetos pareados disponibles, los usuarios del método pueden convenir en usar claves de mínimo 2 y máximo 9 elementos de extensión y con ello no afectan en modo alguno la capacidad combinatoria de la "plana".[13] En definitiva, lo importante para este criptosistema, como para todos los de su clase en la criptografía clásica o de trazado-en-papel, es proteger la clave a toda costa, cambiándola cuando sea necesario dentro de límites matemáticamente razonables y evitando distorsionarla de cualquier manera.

Siendo esto así, cuando Seguín alega que la "simple plana" no basta para descifrar un mensaje comete una ingenuidad y un error importante. Yerra cuando olvida un hecho nítido: la clave va inserta en la propia "plana", y es deduci-

[13] Una clave de un elemento es posible también, pero no recomendable, ya que destruye de golpe el polialfabetismo del sistema, mermando gravemente su nivel de seguridad.

ble por la inspección técnica de un mensaje cifrado con su auxilio; en efecto, si se reparara en la inevitable aparición de caracteres repetidos y, sobre todo, en el agrupamiento regular en quintetos de todos los elementos en ese mensaje, sobrevendría una conjetura sobre la cantidad de alfabetos combinados, base crucial de una hipótesis tendiente a penetrarlo. En cuanto a la ingenuidad cometida, brota desde luego de no tener a la vista en todo momento las propiedades combinatorias, elementalmente aritméticas, de su método. Es a propósito de criptosistemas análogos que viene a punto reflexionar sobre el dictamen de Charles Babbage, inferido de su propia experiencia lidiando con similares artilugios, en torno a las características compartidas por la destreza en el falseo de cerraduras y el "arte de descifrar": ambas faenas son ramas menores del "más vasto tema de las *combinaciones*".[14]

Detengamos aquí el análisis técnico y las comparaciones. Lo hallado nos basta para situar al sistema de Seguín entre los métodos de sustitución polialfabética, regulado en particular por una clave y donde las transformaciones se concretan en una permuta cíclica de caracteres para cifrar y descifrar. Es indudable que se trata de una cifra, o criptosistema, y no de un código, por cuanto la ocultación es de letras y no de palabras. Dado que cada permuta se realiza entre dos alfabetos recíprocos, la conversión a cifra de una letra en el alfabeto del texto plano marca un desplazamiento alfabético cuya cantidad entre cada uno de los elementos puede calcularse por el análisis de frecuencias, no obstante el desorden del alfabeto inferior –del criptotexto– respec-

[14] Babbage, *Passages*, p. 173.

to del superior; esto lo aproxima a los métodos de sustitución polialfabética por excelencia, caso del Vigenère, donde una serie de alfabetos apilados en una matriz se desplazan mutuamente hacia abajo un lugar a la izquierda partiendo del primero, determinando así, conforme a una clave, la generación de sustitutos múltiples para cada letra del alfabeto normal.

Es tiempo ya de resolver dos cuestiones que dejamos pendientes al iniciar este apartado. La primera se refiere al afán de Seguín por establecer un mecanismo de cifrado prácticamente invulnerable al análisis de frecuencias, reduciendo al mínimo la repetición en el criptotexto de la sintaxis regular en un texto plano en español. Mi opinión es que tal idea se basaba en exagerar la dureza de la articulación total de los componentes; en efecto, ya sea cambiando las "combinaciones", ya la "plana", los mensajes cifrados con el sistema pueden, si no son demasiado cortos, ceder más temprano que tarde ante un criptoanálisis limitado a las frecuencias relativas, como permite suponerlo la posibilidad comparativamente exigua de combinaciones totales. La mera presunción hipotética de que se haya utilizado como alfabeto de definición el alfabeto de la lengua española, a pesar de estar incompleto por motivos de economía operacional (la N puede contar como Ñ según el contexto, la LL se forma con dos L), es valiosa para ensayar un conteo de frecuencias relativas de caracteres hasta averiguar cuántos y cuáles sirvieron para velar una sola letra del texto plano original, con base en nuestro conocimiento inductivo de las letras más frecuentemente utilizadas en nuestro idioma (E, A, O, N, R, etc.). Por otra parte, la idea de cambiar la "plana" periódicamente resulta muy sagaz con vistas a bloquear el criptoanálisis, pues

tal plana, como argumenté, contiene de suyo los elementos probables de la clave; además, la modificación constante del desorden en los alfabetos inferiores opone graves contratiempos al análisis de frecuencias. No obstante, es evidente una cosa: cada mensaje *cifrado* en su momento dependió de un *esquema fijo*, y sólo en virtud de tal circunstancia histórico-técnica fue transformado; así, no sería imposible para un interceptor exhumar sus contenidos reconstruyendo el sistema entero, partiendo de una valoración inmanente del ejemplar entre manos y teniendo en cuenta la información relacionada con su captura (que provino de un emisor en un país de habla hispana durante un conflicto bélico, por ejemplo), ejercitando diferentes tipos de razonamiento hacia las mejores hipótesis en cuanto a la probable extensión y sentido del texto soterrado, hasta que las comprobaciones por ensayo y error devuelvan un resultado satisfactorio.

La segunda y última cuestión surgió cuando juzgamos difícil de entender el "principio" al cual se refiere Seguín como aquel cuya introducción faculta variaciones en el sistema. Cuando apunta que éstas surgen "ya cambiando la plana, las combinaciones etc. etc.", en realidad parece aludir a dos principios: el de la recomendable sustitución de las claves para alterar las combinaciones de los alfabetos, y el de la sustitución polialfabética en general. Ahora, el cambio periódico de las claves no es un principio sino una estrategia derivada del principio de la sustitución polialfabética, por tanto, el único "mismo principio" que menciona, si con tal terquedad deseamos establecerlo, deberá ser exclusivamente el de la sustitución polialfabética, del cual, a su vez, depende el principio de la permutación cíclica de los elementos para cifrar y descifrar. Se podría especular, claro, sobre la

clase de cambios en la "plana de claves" que podría tener en mente al escribir, pero esto nos llevaría demasiado lejos, aunque hay espacio para decir que la "plana" admite ajustes al punto de volver al sistema monoalfabético. Esto último, sin embargo, contravendría lógicamente su ambición de generar una cifra "indescifrable", dado que históricamente ha sido la debilidad crónica de los criptogramas monoalfabéticos el acicate para buscar tácticas diferentes, entre las cuales las de mayor éxito y longevidad han sido, justamente, aquellas basadas en el principio de los agregados alfabéticos como base para dotar a cada letra de sustitutos múltiples, cuya formulación seminal se debió, entre otros, a Leon Battista Alberti,[15] un insigne predecesor de Porta.

Finalmente, ¿cómo recibieron esta iniciativa los jefes de nuestro vicecónsul? Mediante de oficios fechados el 6 de abril de 1916,[16] Ramón P. de Negri, cónsul general de México en San Francisco, notificó del prototipo y sus designios al director general de consulados y al embajador de México en Estados Unidos. Cinco días después el embajador, Eliseo Arredondo, respondió que "lo encontraba bueno" y estaría pendiente de saber si la SRE lo aprobaba, "para utilizarlo en su oportunidad".[17] Esta oportunidad, al parecer, llegó a darse, y quizá con tan buena fortuna que todavía en 1926 un método de idénticas prescripciones operacionales fue puesto a circular entre diplomáticos, aunque con la serie de alfabetos a combinar drásticamente minorada en cinco renglones.[18]

[15] KAHN, "On the Origin", p. 123.
[16] AHDSREM-AEMEUA, leg. 491, exp. 4, s/f.
[17] AHDSREM-AEMEUA, leg. 491, exp. 4, f. 16.
[18] AHDSREM, L-E-1565, ff. 124-125.

SIGLAS Y REFERENCIAS

AHDSREM, AEMEUA Acervo Histórico Diplomático de la Secretaría de Relaciones Exteriores de México, Archivo de la Embajada de México en Estados Unidos de América, México, D. F.

Babbage, Charles

Passages from the Life of a Philosopher, New Brunswick-New Jersey, Rutgers University Press, 1994.

Bauer, F. L.

Decrypted Secrets. Methods and Maxims of Cryptology, Berlín, Springer, 1997.

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.

Narváez, Roberto

"Criptosistemas de origen común durante la época revolucionaria", ponencia presentada en el II Coloquio Internacional y IV Coloquio Nacional "La Revolución Mexicana", Puebla, Instituto de Ciencias Sociales y Humanidades, Benemérita Universidad Autónoma de Puebla, Consejo de la Crónica de la Ciudad de Puebla, Instituto Municipal de Arte y Cultura de Puebla, 24 de noviembre de 2011.

Reyes, Alfonso

La experiencia literaria, México, Fondo de Cultura Económica, 1983.