Criptoanálisis de una carta en cifra del conde de Oñate al archiduque Alberto y reconstrucción del nomenclátor

José Luis Rodríguez Gómez

La mayoría de las cartas en cifra pertenecientes al epistolario del conde de Gondomar cuentan con el correspondiente texto en claro, bien en folios contiguos, cuando se trata de cartas cifradas en su totalidad, o bien en los márgenes, cuando la ocultación es parcial y se limita a unos cuantos fragmentos [cfr. *Avisos*, 89 (2019)]. En menor medida, se localizan también algunas cartas sin descifrar, como la remitida por el conde de Oñate al archiduque Alberto, fechada en Viena, a 28 de junio de 1620 (RB II/2209, doc. 69), cuya desencriptación y reconstrucción del nomenclátor de la cifra general que le sirvió de clave es objeto de este trabajo.

Louis Morin, *L'infant prodigue*. Paris: Delagrave, 1898 [RB INF/3144]

Desde el punto de vista del criptoanálisis, dado que contamos con un buen número de cartas cifradas de esa fecha que utilizan la misma cifra general junto con los correspondientes textos en claro, nuestra labor de desencriptado se encuadra en el método KPA, del inglés *Known-Plaintext Attack*. En un trabajo semejante, con conocimiento de textos en claro, Tomokiyo [2018] describe de forma precisa los pasos seguidos en el proceso de recontrucción para una carta de 1591 perteneciente al mismo paradigma de encriptación que la que aquí se analiza. Para la labor de cotejo de textos cifrados con sus versiones en claro, que conlleva este tipo de análisis, en nuestro caso se han tenido en cuenta las misivas encuadernadas en los volumenes con signatura II/2291 (24, 33, 39, 41, 46, 57, 63) y II/2209 (67, 68, 71, 72), descritas en IBIS.

Como resultado de este examen se ofrece, en primer lugar, el texto de la misiva desincriptado casi en su totalidad, en un volumen suficiente al menos para su comprensión y contextualización histórica, evitando siempre la conjetura para completar lagunas, a la que en algunos casos invita el contexto, de modo que las cifras no resueltas se marcan en cursiva a la espera de que el cotejo de otras cartas sometidas a la misma cifra general nos revele su solución. En segundo lugar se expone el nomenclátor, dispuesto de forma semejante a los que conocemos de la época, si bien con algunas modificaciones. En concreto, excepto en el bloque del alfabeto, damos en primer término la forma cifrada, priorizando de este modo la labor de desencriptado, que es, obviamente, la única que se beneficiará de este trabajo, frente a su inversa, la encriptación.

Para una caracterización formal del nomeclátor, siguiendo a Bauer [2000], observamos que los conjuntos que contienen, respectivamente, los elementos del texto en claro y del cifrado son distintos, tal como se muestra en (1) y (2), siendo V el conjunto de elementos del texto plano y W el de la cifra. Estamos, por tanto, ante un criptosistema no homogéneo. Por otra parte, determinados elementos del espacio del texto plano tienen más de una equivalencia en el espacio del texto cifrado, lo que define a este criptosistema como cifrado de sustitución homonímica. En particular, para evitar la ruptura por análisis de frecuencias, en el bloque 1, correpondiente al alfabeto, observamos, como es habitual, que las letras de mayor frecuencia cuentan con un número mayor de correspondencias.

$$V = \mathbb{Z}_{26} + \{0,1,2,3,4,5,6,7,8,9\} \quad [1] \qquad W = \mathbb{Z}_{26} + \{0,1,2,3,4,5,6,7,8,9\} + \{\mathrm{q}, \mathrm{p}, \Theta, \Lambda, \forall, \overline{\forall}, 4+\} \quad [2]$$

Los bloques 2 y 3 corresponden al silabario, es decir, a la encriptación de grupos de dos o tres letras, denominadas de bígrafos y trígrafos, y formalizadas en (3), (4) y (5). Estas tres reglas de transformación se designan, respectivamente, como digráfica bipartita, trigráfica bipartita y trigráfica tripartita.

$$X_i : V^2 \longrightarrow W^2 \quad [3] \quad X_i : V^2 \longrightarrow W^3 \quad [4] \quad V^3 \longrightarrow W^3 \quad [5]$$

A continuación, los bloques 4-6 constituyen la parte de diccionario, en el que el objeto de la cifra es una palabra o sintagma de significado completo. En el bloque 4 cada palabra es sustituida por un número de tres cifras, en dos grupos, uno que correspende a la primera centena y otro a la cuarta. En los textos podemos encontrar estos números con o sin vírgula superpuesta, dado que en ningún caso esa marca es un rasgo diacrítico, ya que no resuelve ambigüedad alguna al ser combinaciones únicas. No ocurre lo mismo con el bloque 6, en el que el subrayado es rasgo pertinente para el significado. En efecto, la serie del 72 al 79 tiene coincidencia en el silabario y resuelve la ambigüedad con el subrayado. El bloque 5, por su parte, utiliza letras en lugar de números para la encriptación.

Como es habitual en los criptosistemas de la época, en nuestro nomenclátor se utilizan símbolos para marcar los finales de vocales ('+', ':', ':'), las combinaciones dúplices (arco atravesado con un trazo) y las nulas (vírgula superpuesta), recursos todos ellos encaminados a dificultar el criptoanálisis.

NIPO: 093-20-007-5 · DEPÓSITO LEGAL:M-1496-1996

Finalmente, la trascripción respeta al máximo la trasformación de cifra a texto en claro, sin intervenir con puntuación o acentuación, separando las líneas con una barra vertical y marcando en cursiva las cifras sin resolver. Se respeta la división de párrafos del original.

Referencia bibliográficas

Bauer, F. L., 2000, *Decrypted Secrets. Methods of Cryptology*, Berlin, Springer-Verlag.

IBIS. Base de datos del patrimonio bibliográfico de Patrimonio Nacional. https://realbiblioteca.patrimonionacional.es

Tomokiyo, S. 2018, «How I reconstructed a Spanish cipher from 1591», *Cryptologia*, vol. 42, núm. 6, 477-484. Disponible en: https://doi.org/10.1080/01611194.2017.1370038.

Texto en claro

El duque de baviera ha escrito a los electores alemanes que su gente ha|bia pasado ya todos los pasos peligro|sos y que asi la juntaria quel duque de bir|tenberg y los marqueses de baden y anspach | hacian lo mismo de la suya y que les pensa|ba enviar a preguntar que seguridad le dari |an de no ofender a los *zu*-s y que si se | la daban vendría luego a executarlo del|a austria superior y si no se la | querían dar pensaba acometerlos.

El emperador le responde se alegra de que haya j|untado su gente le pide que quanto antes pro|cure obrar con ello y no tiene por mal que p|rocure asegurar a los príncipes *zu*-s más que | supuesto quel de saxonia no se mobe|ra sin que el se mueba y el peligro g|rande que ay de que sin estas asistencias los un|garos se declaren totalmente contra | su majestad desea que dejando allá parte de gente para | defensa de aquel distrito y corespo|ndiendose con Su Alteza para que con la gente que quando es|ta llegue estará lebantada atie|nda a la defensa de los principes regnanos | venga a la *sel* de la austria superior| lo qual sin duda para las cosas de acá es | muy necesario porque ni el conde de *81*coy puede ofen | der[l]o y al*sah* essecto de las fuerzas que | el uno y el otro tienen ni el duque de saxonia | [fol. [1]v] se mobera sin que se mueba primero el de baviera | y el peligro de los ungaros y que por ellos | se mueban los *422*s es de harta [*símbolo infinito*] porque quando no | hagan mas de romper la guerra por esta parte y me| ter algún golpe de *vu* que arruinen el | el país será muy perjudicial contra peso | y que pondria en manifiesto peligro| la stiria.

Por todas estas razones viendo lo que tarda l|a gente de *75* y sospechando quel duque de Baviera con barios pre| textos ba difiriendo el negocio hasta be|r entradas las fuerzas de esos estados en alemani|a con una estafeta quel aleman despacha a baviera y que | podría ser pasase de allí a su alteza me ha pa | recido poner en las cosas siguie|ntes:

Que si no se ha enviado a dar quenta al conde de| saxonia de la entrada de ese ejercito en la forma que avise | a de este o en la que mas convenga se h|aga luego porque es conveniente hacer con el esta demo|stracion y asegurarle.

Que supuesto que su alteza sabrá ya la gente que le es | de *75* si esta no llegare al tiempo que le dema|nda el ejercito que ai se prebie-ne estuviere apa|rejado mande su alteza se consulte si se podria | sacar otra tanta gente de la vieja de esse ejercito para que no | se difieriese su entrada pues en los | dias que puede haber de dilacion de lo uno a lo | otro parece que alli no se haría mucha falta y | para lo de aca inportan las oras.

[En claro] Y quando no se puede hazer sirvase V.A. de mandar [en cifra] considera|rar si de lo menos a titulo de presidia| [f. 2r] r las plaças del elector de maguncia y de otros príncipes | *zus* se podrían enviar ocho o 10 mil hombres de | delante que diesen animo al duque de baviera pa|ra romper esta guerra y juntamente asigura|se a esse ejercito el paso del rin que sigun yo | entiendo es una de las mayores dificultades | que esse ejercito hallara en Alemania y no pienso | se aventuran enviándolos a lados de | principes zus y por países *fus* y tiniendo l|a gente que dejara el de baviera en los paíse|s superiores que les guarden las es|paldas en caso que los protestantes los | quieran acometer.

[En claro] Como no se las ordenes que truxo el agente moreo a | monaco no puedo hablar en esto con el fundamento que | quesiera mas todavia me ha parecido obligacion mia el | representarlo a V.A. que supuesto que se vee quanto | [cifrado] el duque de Baviera pende de esas armas y lo que el | ha prometido a S.A. no tendria por malo | que S.A. se sirviese de concertarse desde a | y con el sobre lo que se hubiere de h|acer pues se ahorra mucho tiempo escusando el | rodeo de hacerlo por esta corte.

Tambien prosupe a S.A. días ha una *105* entre el | alemán S.A. y los duques de saxonia y babiera para asi|stirse en la execucion de los mandatos de S.M. cesa|rea y conserbacion de lo que en virtu|d dellos se ocupare yo la tengo por necesaria | por las razones que se dexan considerar si es|tos duques entrasen bohemia como se lo pro|pondra el conde de coleren entonces me pa|rece *81* en tiempo para tratarla y concluy|lla mas si respeto de lo que aquí digo del |[f. 2v] deseo que a mi parecer tiene el duque de babiera de que | lo del imperio se anteponga se hubiese de come|nçar por allí la guerra en este caso aprobando S.A. es|ta *105* seria necesario tratarla y concluir|la desde *100* [en claro] en que V.A. mandara resolver y ordenar | lo que fuere servido y los medios que se huvieren de poner para | executarlo sin lo qual no moveré esta platica. Guarde nuestro señor.

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	y	z	x
7 10 11 12 13 22	n m	H 70 80	⊖ p	14 15 16 17 27 77	g z	x	A D	18 19	Y 4+		t v ψ	2 4 25	Λ f		K q	∇ ♀	3	26 29	50 60	70	40 90 99 30

Bloque 1

71 as	72 es	73 is	74 os	75 us	76 ba	77 be	78 bi	82 da	83 de	84 di	85 do	86 du	87 ça	88 ce	89 ci	91 co	92 cu
93 ma	94 me	95 mi	96 mo	97 mu	▽ de	As na	Es ne	Is ni	Os no								

Bloque 2

fan sa	fen se	fin si	fon so	fun su	far pa	fer pe	fir pi	for po	fur pu	gan ta	gen te	gin ti	gon to	gun tu	lan ya	lon yo	len ye
san ra	sun ru	sen re	sin ri	sar fa	ren se	xar ga	xor go	xur gu	A de	car par	cer per	cor por	fro cho	zen que	zin qui	zan que	

Bloque 3

107 Libertad	127 Misma	143 Orden	165 Plática	181 Remedio	408 Sospecha	432 Vuestra
109 Lugar	128 Manda	146 Ocasión	166 Príncipe	183 Rey de	410 Socorro	Majestad
110 Luego	131 Negociación	147 Obligación	169 Persona	Inglaterra	412 Servicio	435 Vuestra
113 Marqués	133 Ningún	149 Para que	171 Particular	187 Roma	413 Señor	Señoría
117 Marqués	135 Necesario	152 Puerto	172 Quando	188 Respuesta	414 Seguridad	438 Vos
de Espínola	136 Negocio	153 Prudencia	174 Qualquiera	189 Resolución	416 Secretario	440 Vuestra
118 Marqués	137 Nueva	156 Presupuesto	175 Quales	190 Relación	424 Tratar	441 Hungría
de Bedmar	138 Navio	158 Procura	176 Quanto	194 Razón	426 Tiempo	446 Venecia
123 Mente	140 Oficio	161 Posible	177 Rey	195 Rebelde	427 Tanto	
124 Mucho	141 Opinión	163 Pontifice	178 Infante	401 Su Majestad	431 También	
125 Muy	142 Otro	164 Poder	178 Reyno	407 Suceso	433 Su Alteza	

Bloque 4

13 España	25 Flandes	40 Final	66 Hacer	71 Hereje	79 Inglaterra	89 Indias
16 Estado	33 Fuerza	54 Gente	67 Hecho	72 Imperio	80 Inglés	
17 Execución	36 Forma	60 Guerra	69 Hermano	73 Importancia	83 Instrucción	
18 Ejército	39 Flota	65 Honra	70 Hijo	78 Infantes	87 Justicia	

Bloque 5

be Archiduque	cus Diligencia	ge Allí	me Bueno	re Consejo	ti Como	xo Caso
ca Aviendo	da Así	gi Alguno	mu Baviera	si Conde	ton Después	xu Casamiento
ce Aunque	de Asistencia	go Aleman	ni Criado	sil Efecto	tor Dicho	za Camino za
cis Daño	fa Armada	gos Emperador	po Conveniente	sol Embajada	tra Duque	ze Carta
co Aviso	fi Año	gu Adelante	pu Conviene	ter Dificultad	tun Despacho	
cos Dilación	gas Elector	ja Bien	que Cuidado	ti Como	xa Caballo	

Bloque 6