DESCRIPTADO DE LA CLAVE G

Tomás Félix Tornadijo Rodríguez

tomas@narceadigital.com

1. Introducción

El catorce de julio de 1936 el Teniente Coronel Yagüe envía desde Marruecos una misiva al General Mola, comunicándole la marcha de los preparativos para el golpe de Estado que estaban urdiendo contra el Gobierno de la República (Nadal Sánchez, 1978:34).

En dicha carta (*vid*. Apéndice I) se alternan los pasajes con el texto en claro y con el texto en cifra, utilizándose la clave G, que era una clave militar clasificada como *nacionalista*, utilizada en aviación, y de la que no hay constancia de su captura o descriptado (Soler Fuensanta, 2008:212).

Esta clave parece, a priori, clasificable como del tipo Tabla de Homófonos, pues falta la posición de los pares de letras que se suelen indicar en el criptógrafo de cinta móvil. Ambos métodos fueron de los más utilizados durante la Guerra Civil por los dos bandos (Soler Fuensanta, 2008:126).

El cifrado por tabla de homófonos consiste, simplemente, en representar cada letra del abecedario mediante varios números, entre el 0 y el 99, de forma que cada número quede asignado a una sola letra. De esta manera se dificulta mucho el criptoanálisis por medio del análisis de frecuencias, aunque no sea posible impedirlo completamente.

Debido a la imposibilidad de consultar toda la amplia bibliografía existente sobre el inicio y gestación de la Guerra Civil Española no se ha podido verificar si la carta de Yagüe estaba ya descifrada, aunque Nadal la da por poco conocida. En

cualquier caso sirva este pequeño trabajo de muestra y ejemplo de descriptado de este tipo de criptogramas.

2. Descriptado

Podemos ver que varios bloques cifrados se corresponden con nombres propios o apellidos, como se colige de las partes no cifradas. Esta circunstancia facilita mucho el criptoanálisis, puesto que las distintas posibilidades para un nombre o apellido con un determinado tamaño no son excesivamente elevadas, menores aún si disponemos de una lista de candidatos. Además el bloque [E] se corresponde con las 7 últimas posiciones del bloque [A], salvo 3 cifras. Es decir: se ha cifrado el mismo nombre con distintos homófonos.

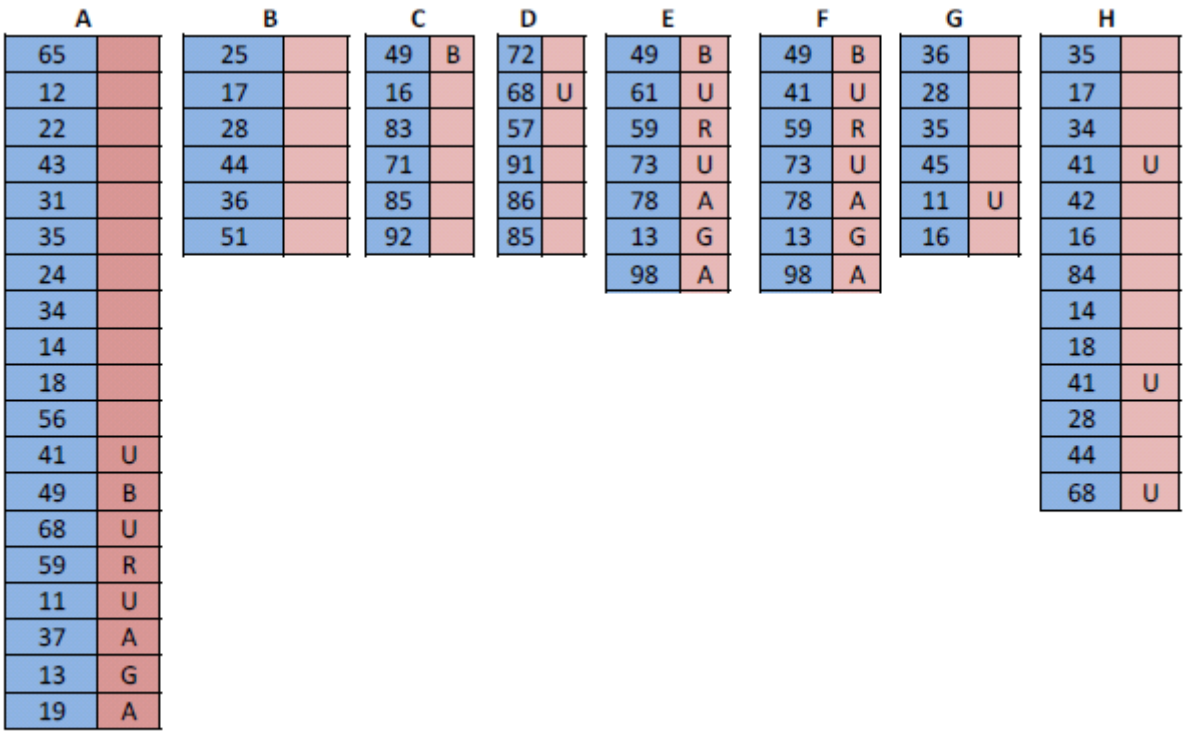
Este proceder no se comprende, pues si el enemigo lograse interceptar la misiva e identificar ese nombre, obtendría, además, la correspondencia de los otros tres homófonos, que, aunque no sean utilizados en otras partes del mensaje, sí facilitarían el criptoanálisis de subsiguientes criptogramas cifrados con la misma clave.

Pero además, el mismo nombre vuelve a cifrarse en el bloque [F], cambiando un homófono con respecto al bloque [E]. Esto compromete aún más la seguridad de la clave, puesto que el homófono 41 sí se repite en otros bloques que no tienen relación con este nombre, y de los que podríamos obtener información, de conseguirse romper la cifra de ese nombre o apellido. Parece, pues, evidente empezar el criptoanálisis por ahí.

Podemos obtener una lista de candidatos para ese nombre del excelente relato de Sánchez Montoya (Sánchez Montoya, 2006) sobre el inicio de la Guerra Civil en el Norte de África.

Entre los nombres de los conspiradores, elegiremos a los de más alto rango, probando con todos los que tengan nombres o apellidos de siete letras, por ejemplo BURUAGA.

Colocando el nombre, vemos (figura 1) que el bloque [H] termina con una palabra en U, lo que no es muy frecuente en el castellano.



A		B		C		D		E		F		G		H	
65		25		49	B	72		49	B	49	B	36		35	
12		17		16		68	U	61	U	41	U	28		17	
22		28		83		57		59	R	59	R	35		34	
43		44		71		91		73	U	73	U	45		41	U
31		36		85		86		78	A	78	A	11	U	42	
35		51		92		85		13	G	13	G	16		16	
24								98	A	98	A			84	
34														14	
14														18	
18														41	U
56														28	
41	U													44	
49	B													68	U
68	U														
59	R														
11	U														
37	A														
13	G														
19	A														

Figura 1.

Con todo, podemos probar con TETUAN para el bloque [B], que por el texto en claro sabemos que es un nombre de lugar, y que conviene especialmente: por tener seis letras y por ser la plaza donde el Teniente Coronel tenía el encargo de organizar el Alzamiento.

Sin embargo en la figura 2 vemos que el bloque [H] termina con UU, lo que no se corresponde con ninguna palabra del castellano.

.

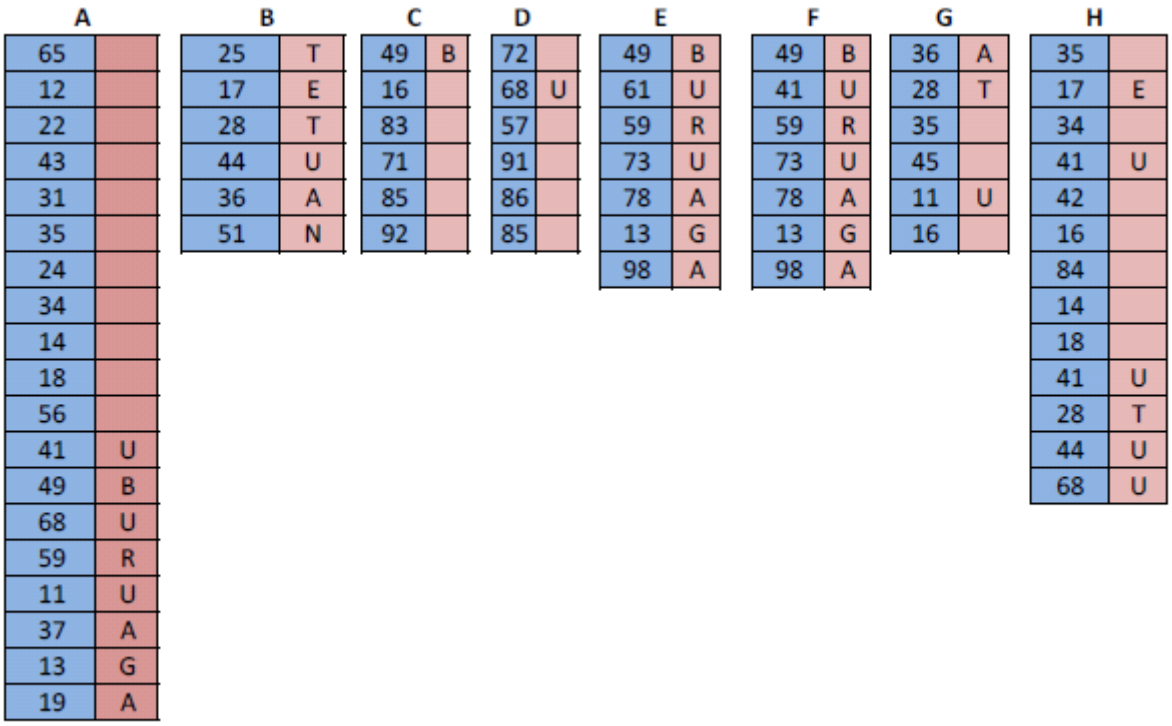


Figura 2.

Podemos probar con el nombre de pila de Buruaga, EDUARDO, que también tiene 7 letras, pero nuevamente la terminación del bloque [H] nos lleva a un callejón sin salida. (Figura 3).

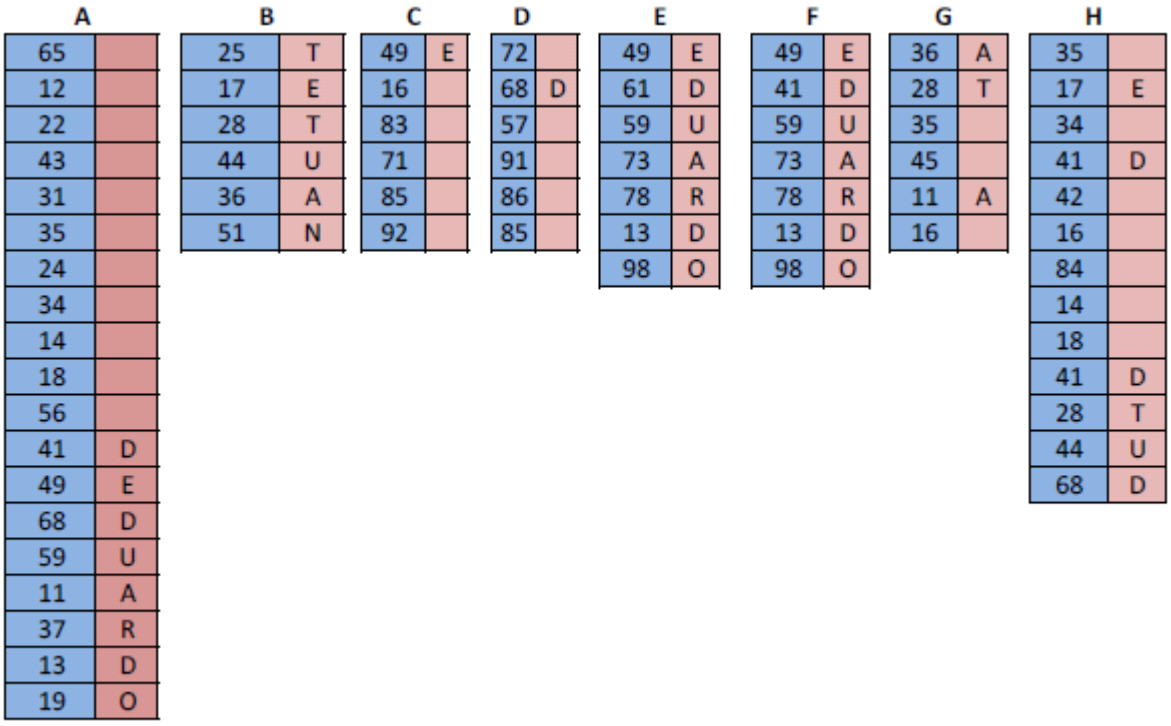


Figura 3.

Otro nombre con el que podemos probar es el de ASENSIO (Teniente Coronel Carlos Asensio Cabanillas), pero tenemos el mismo problema. (Figura 4).

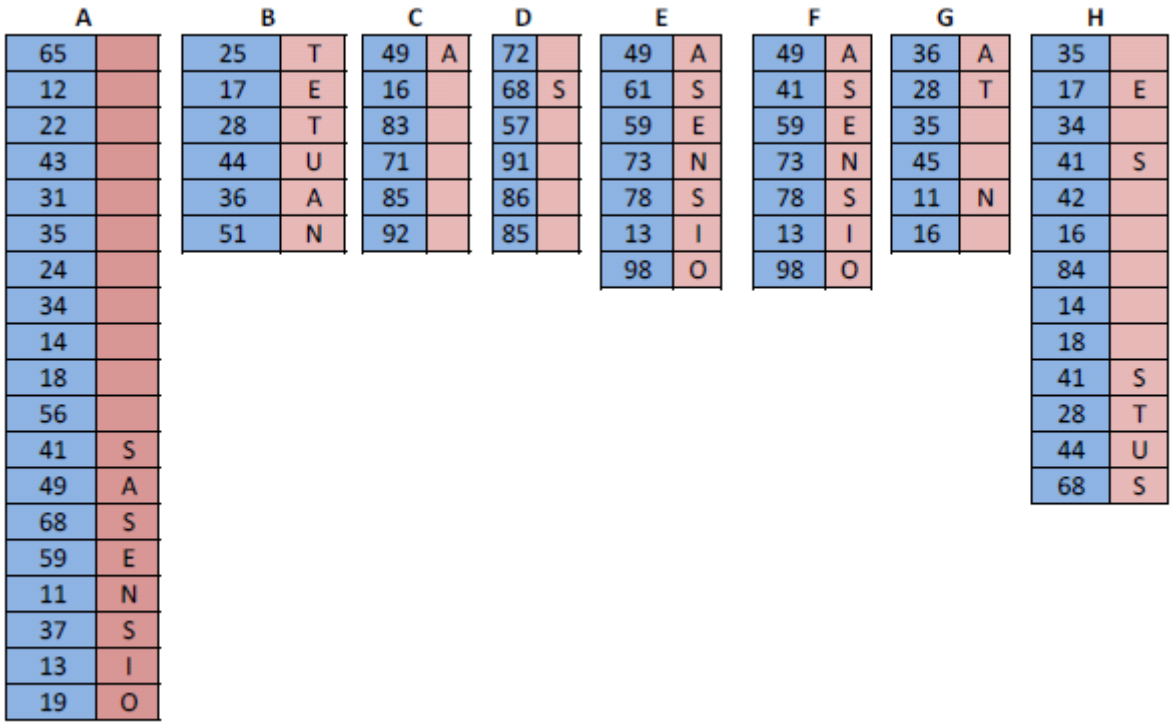


Figura 4.

En vista de las dificultades para encontrar un nombre que encaje, podemos buscar un texto válido para el bloque [H] que, como leemos en la carta, es algo de lo que hay que *hacerse cargo*. Dado que la más alta autoridad del Protectorado español en Marruecos emanaba de la Alta Comisaría, resulta inmediato colegir que esa institución era precisamente aquello de lo que había que *hacerse cargo*. De modo que probaremos con ALTACOMISARIA, que tiene 13 letras y además son iguales la cuarta y la décima (Figura 5).

A		B		C		D		E		F		G		H	
65		25		49		72		49		49		36		35	A
12		17	L	16	O	68	A	61	A	41	A	28	R	17	L
22		28	R	83		57		59		59		35	A	34	T
43		44	I	71		91		73		73		45		41	A
31		36		85		86		78		78		11		42	C
35	A	51		92		85		13		13		16	O	16	O
24								98		98				84	M
34	T													14	I
14	I													18	S
18	S													41	A
56														28	R
41	A													44	I
49														68	A
68	A														
59															
11															
37															
13															
19															

Figura 5.

Ahora, en el bloque [G], aparece un resultado que encajaría a la perfección con el apellido Franco. Sin embargo, éste sería el sujeto de una frase en la que el verbo está en tercera persona del plural, con lo cual no guardaría concordancia, circunstancia ésta que nos estorbó un poco el criptoanálisis. Resultaría irónico que el mayor problema para el descriptado nos viniera más de la falta de sintaxis del texto que del propio cifrado, si bien tampoco podemos suponer una completa ausencia de erratas en el mismo.

Por lo demás utilizando FRANCO para el bloque [G] no aparece ningún problema, y sí nos surgen nuevas posibilidades. (Figura 6).

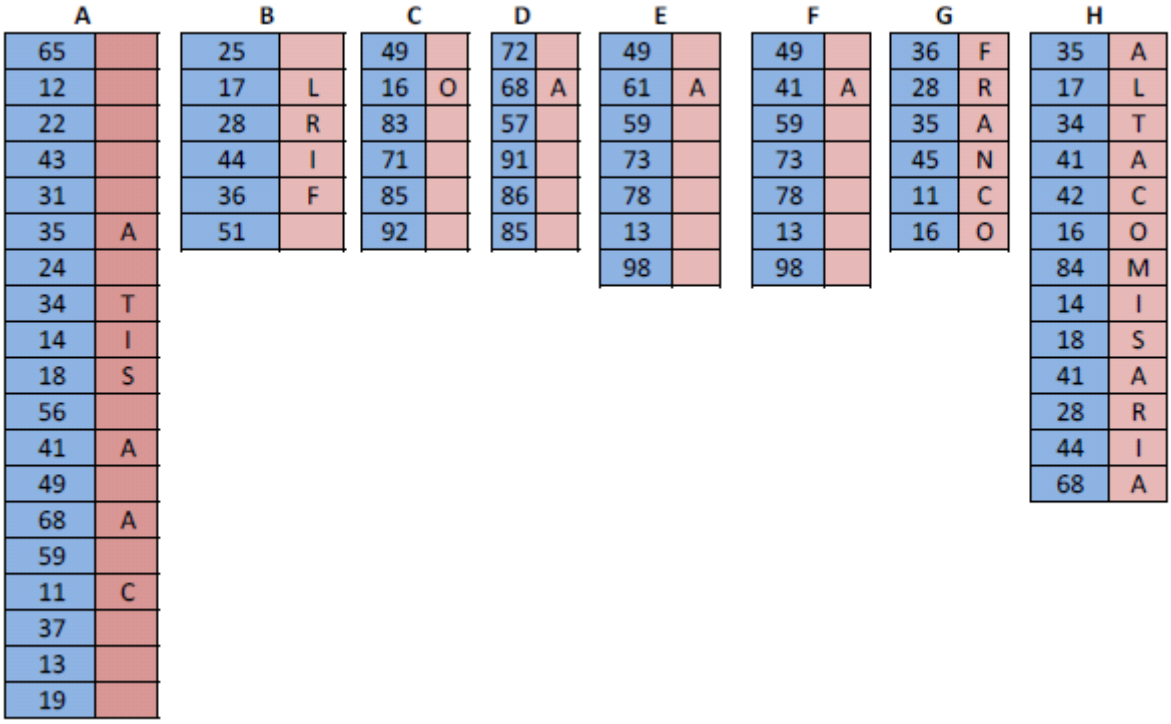


Figura 6.

Ya estamos en condiciones de poner un nombre o apellido al final del bloque [A]. Un apellido muy común: Sánchez, encaja a la perfección con la correspondencia de los homófonos 68 y 11. En el texto de referencia (Sánchez Montoya, 2006:3) comprobamos que ese apellido pertenecía a un destacado militar, Juan Bautista Sánchez, que se menciona en Villa Alhucemas, en el Rif, lo que además nos permite completar los bloques [A] y [B] (Figuras 7 y 8).

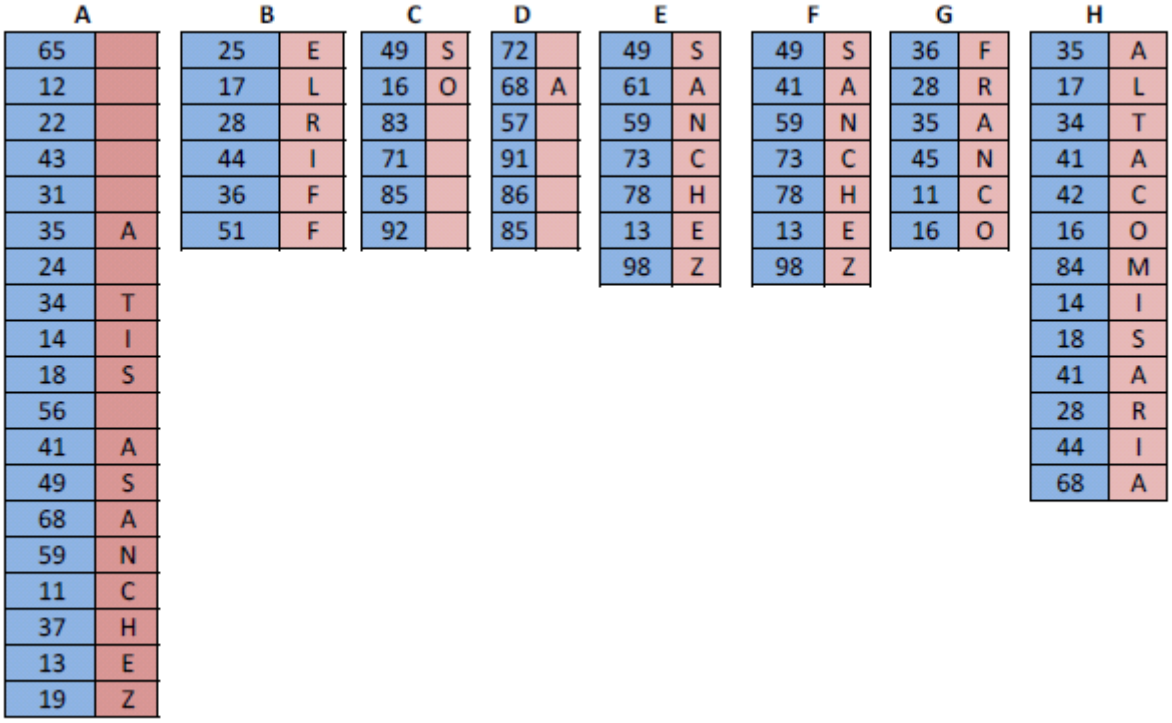


Figura 7.

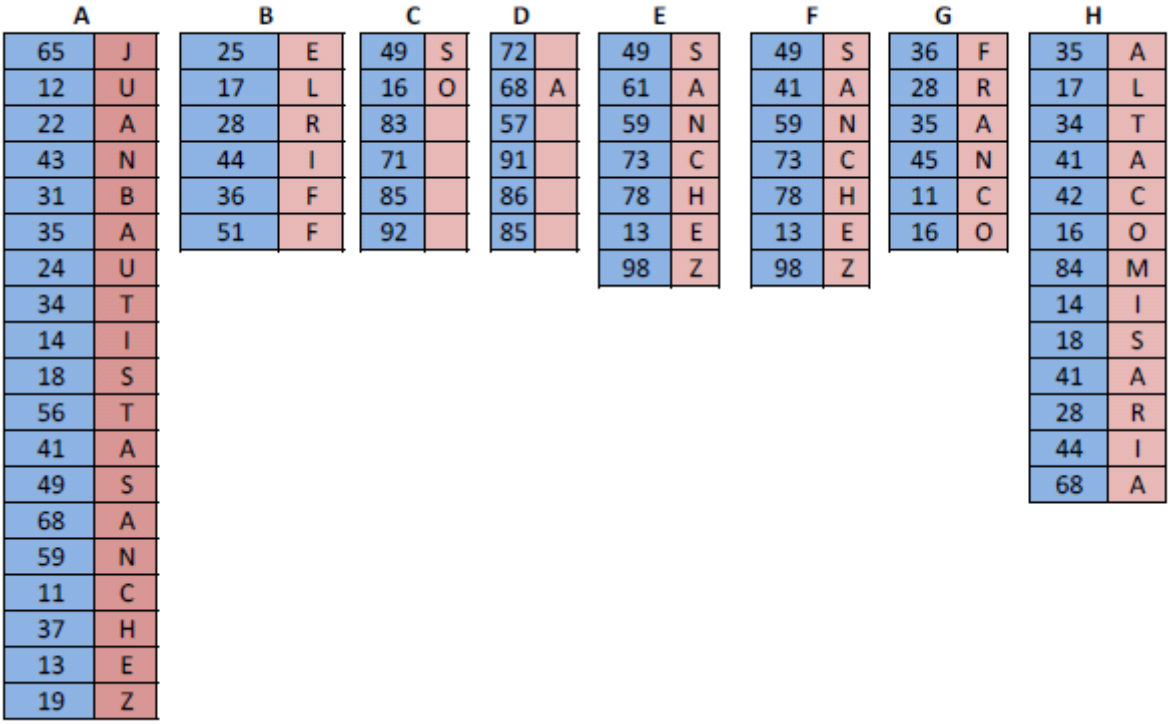
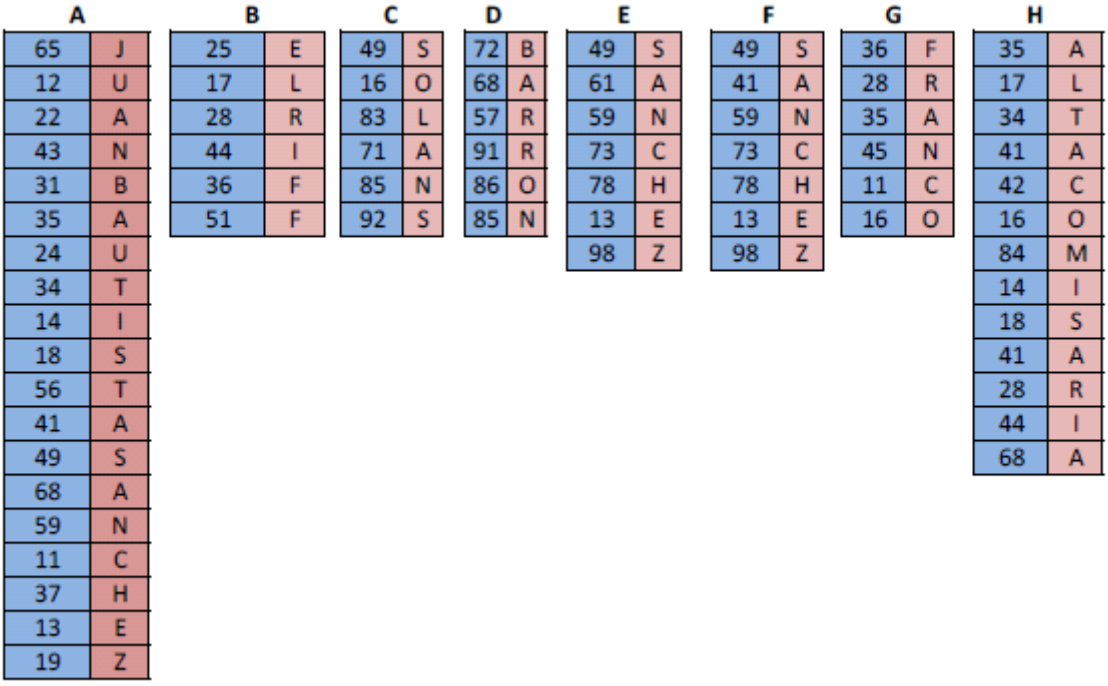


Figura 8.

Casi hemos completado el criptograma, a falta de los bloques [C] y [D], que también son nombres o apellidos. SOLANS (Sánchez Montoya, 2006:3), encaja perfecto en el bloque [C], en tanto que BARRON (Fernando Barrón Ortiz, 1892-1953) resulta adecuado para el [D] (Figura 9).



A	
65	J
12	U
22	A
43	N
31	B
35	A
24	U
34	T
14	I
18	S
56	T
41	A
49	S
68	A
59	N
11	C
37	H
13	E
19	Z

B	
25	E
17	L
28	R
44	I
36	F
51	F

C	
49	S
16	O
83	L
71	A
85	N
92	S

D	
72	B
68	A
57	R
91	R
86	O
85	N

E	
49	S
61	A
59	N
73	C
78	H
13	E
98	Z

F	
49	S
41	A
59	N
73	C
78	H
13	E
98	Z

G	
36	F
28	R
35	A
45	N
11	C
16	O

H	
35	A
17	L
34	T
41	A
42	C
16	O
84	M
14	I
18	S
41	A
28	R
44	I
68	A

Figura 9.

3. Conclusión

Desde el punto de vista de la criptografía, esta carta solo nos sirve para constatar el escaso nivel que la criptografía tenía en España a esas alturas del siglo XX, manteniendo sistemas de cifrado completamente desfasados ya en el siglo anterior y cuyas debilidades, además, eran perfectamente conocidas (García Carmona, 1894).

Lo primero que llama la atención en la carta de Yagüe es la fragilidad del sistema cifra empleado al que, sin embargo, se confían los mayores secretos, debilidad que se ve acrecentada por la alternancia con el texto en claro, a pesar de tal proceder estaba expresamente prohibido por el reglamento para el Enlace y el Servicio de

Transmisiones de 1925 (Soler Fuensanta, 2008:132), cometiendo, además, uno de los fallos criptográficos más serios: cifrar el mismo texto con claves distintas.

APENDICE I

CLAVE G.

Terminadas las maniobras ha empezado la dislocación y si no hay orden en contra el día 16 estarán todas las fuerzas en sus bases.

El trabajo efectuado ha sido fecundo 65-12-22-43-31-35-24-34-14-18-56-41-49-68-59-11-37-13-19 **[A]** *se encarga de todo en* 25-17-28-44-36-51 **[B]** *y se pone incondicionalmente a sus órdenes.*

49-16-83-71-85-92 **[C]** *está también con nosotros; dice que el movimiento debe hacerse en España y nosotros a la espectativa como fuerza en reserva. Pide establecer contacto con usted.*

72-68-57-91-86-85 **[D]** *también está con nosotros y opina lo mismo que* 49-16-83-71-85-92, *pero yo le he dicho que no hay más que obedecer y está conforme.*

49-61-59-73-78-13-98 **[E]** *como le digo incondicionalmente y donde se le necesite ofrece mandar si es necesario dos mil hombres a España para allí armarlos.*

El resto de la Cir, que estaba desorientada, pero ya se han ido con órdenes terminantes, circularán inmediatamente las órdenes a las distintas unidades con misiones concretas y estarán dentro de tres o cuatro días en disposición de ponerse en movimiento.

Todos y especialmente 49-41-59-73-78-13-98 **[F]** *dicen que deben venir* 36-28-35-45-11-16 **[G]** *para hacerse cargo de la* 35-17-34-41-42-16-84-14-18-41-28-44-68 **[H]** *y evitar trascienda el movimiento al campo.*

Aquí todo está listo, sólo necesitamos mando y barcos. He recibido por una carta una orden de ponerme en movimiento el día 14 y otra al mismo tiempo aplazando la cosa. Si esta segunda se pierde se arma lío.

Esto no puede ser, insisto en que el día y la hora debe mandarse a priori y traerlo en mano por dos personas de confianza, mejor que por una.

Tengo todo preparado, los bandos de guerra hechos. No dudo un momento en el triunfo. El espíritu de todos magnífico.

Mando, barcos y adelante.

14-7-36. *¡Viva España!*

Referencias

1. Nadal Sánchez, Antonio. "*Málaga, 18 de Julio de 1936"*, Jábega, ISSN 0210-8496, Nº. 21, 1978 , pag. 34.

   Disponible en: http://www.cedma.com/archivo/jabega_pdf/jabega21_28-39.pdf

2. García Carmona, Joaquín. "*Tratado de criptografía con especial aplicación al ejército*". Madrid: sucesores de Rivadeneyra, 1894.

3. Soler Fuensanta, José Ramón; López-Brea Espiau, Francisco Javier. "*Soldados sin rostro: los servicios de información, espionaje y criptografía en la Guerra Civil española*". Inédita Editores 2008.

4. Sánchez Montoya, Francisco. "*17 de julio de 1936. Inicio de la Guerra Civil en el Norte de África"*. Congreso La Guerra Civil Española 1936 – 1939, 2006.

   Disponible en: www.secc.es/media/docs/2_2_FSanchez_Montoya.pdf