Estrategias políticas del Conde de Siete Fuentes. Descrifrando una carta del siglo XIX

Jezabel Molina-Gil,Néstor García-Moreno
Cándido Caballero-Gil,Pino Caballero-Gil
Departamento de Ingeniería Informática y de Sistemas
Universidad de La Laguna
{jmmolina,ngarciam,ccabgil,pcaballe}@ull.edu.es

Judit Gutiérrez-de-Armas
Grupo de Investigación 'Tierra,
Familia y Sociedad en la Edad Moderna'
Departamento de Geografía e Historia
jgutiear@ull.edu.es

***Resumen*—Este documento presenta el descifrado de una carta hallada fortuitamente como parte de los trabajos de catalogación del Fondo Conde de Siete Fuentes en San Cristóbal de La Laguna, Tenerife. Se trata de una carta conservada por varias familias de élite de Tenerife desde el siglo XVI al XX. Concretamente, se trata de una carta junto a la que se adjuntaban un documento con 16 tablas de búsqueda. Ambos documentos, tanto la carta como las tablas fueron digitalizadas para descifrar el contenido. Las técnicas utilizadas para el descifrado son las usualmente utilizadas para este tipo de cifrados, análisis estadístico de frecuencias, criptoanálisis diferencial, etc. Finalmente, gracias a estos análisis, se logró obtener la clave para descifrar el mensaje.**

***Palabras Clave*—cifrado polialfabético, criptoanálisis, criptografía histórica**

I. Introducción

El cifrado presentado en este trabajo es un documento hallado fortuitamente como parte de los trabajos de catalogación del Fondo Conde de Siete Fuentes, un archivo de familia de más de 26.000 documentos que contiene la documentación generada y conservada por varias familias de la élite de Tenerife desde el siglo XVI al XX. Concretamente, la carta y la clave se encontraban juntas en un legajo de correspondencia del VI Conde del Valle de Salazar, don Cristóbal Salazar y Porlier (1789-1866).

Sobre la criptografía durante los siglos XVIII y XIX, tal como muestra [1], cabe mencionar nombres como Jefferson, Wheatstone, Playfair, incluso un joven Bazeries, y por supuesto los "gabinetes negros (u oscuros)"de diversos estados, tan importantes en el desarrollo militar de las comunicaciones cifradas. Sin embargo, también existían cifrados que no proporcionaba mucha protección. Un claro ejemplo de ello son los cifrados utilizados por el emperador Napoleón, *Le Grande Chiffre de Paris* y la *petite chiffre* [2], para la comunicación de los generales y el estado mayor. Estos cifrados eran muy simples y consistían en cambiar sílabas por números.

En España, durante este período, hay constancia del uso de la criptografía en la Guerra de Independencia Española. En concreto, un español Juan Van Halen, logró forzar la cifra de Suchet y usarla para facilitar la toma de Mequinenza y Lérida [3]. Por su parte, en las guerras carlistas poco se sabe sobre el uso de la criptografía, tan solo se cuenta con información sobre el uso del jugo de limón para ocultar los mensajes por parte del capitán general Zumalacárregui. Don Carlos Luis de Borbón además, usó una clave en la cual los términos fueron reemplazados por combinaciones de hasta tres dígitos y hasta dos letras [3].

El cifrado utilizado en la carta presentada en este artículo consiste en un cifrado de sustitución polialfabético. En concreto, cuenta con 16 alfabetos diferentes que como veremos más adelante, no serán tantos e incluso existe uno que ni siquiera está presente en la misma. El objetivo de este artículo, además de presentar los pasos y resultados del criptoanálisis llevados a cabo para descifrar la carta, es proponer hipótesis que nos ayude a entender cómo el receptor obtenía la clave que permitía descifrar el mensaje. Para ello se ha realizado un análisis que intenta relacionar la clave obtenida con alguna otra información en claro que proporciona la carta. Además, nos planteamos la búsqueda del origen y utilización del cifrado aquí presentado.

La estrecha relación de Canarias con el Nuevo Mundo y la relación de éste con algunas personalidades nombradas en el escrito, podría llevar a plantear el uso de un cifrado utilizado para el intercambio de correo con las Américas. Éste solía hacerse cifrado, por lo que igual esta carta podría mantener relación con alguna personalidad en torno a la colonización del Nuevo Mundo. Por otro lado, el propio general Ricafort (1776-1846), al que como veremos hace alusión la carta, hacía uso de un cifrado que se conoce como la primera clave y segunda clave del general Ricafort [4], [5]. Aunque se ha podido encontrar la primera clave del general, ésta no coincide con el tipo de cifrado utilizado en esta carta; del segundo cifrado aún no se ha encontrado información.

El contenido de este artículo se organiza de la siguiente forma: en la sección II se analizan los posibles cifrados que podrían mantener cierta relación con el cifrado encontrado en la carta. En la sección III se presenta el proceso de criptoanálisis realizado para poder descifrar el contenido de la carta. En la sección IV se analiza el cifrado utilizado, sus peculiaridades y su relación con otros posibles cifrados. La seccion V presenta las hipótesis planteadas para la obtención de la clave de cifrado. Por último, en la sección VI se ofrecen las conclusiones y se proponen trabajos futuros.

II. Estado del Arte

El cifrado utilizado en la carta, como se detallará más adelante, es un cifrado por sustitución, polialfabético y bidireccional. Consiste en 16 tablas que divide el alfabeto en dos partes: la primera mitad del alfabeto está comprendido entre [a-m] y se encuentra en la parte superior de cada tabla,

mientras que el resto está comprendido entre [n-z] pudiéndose localizar en la parte inferior (Tabla I). Es un sistema de cifrado en el que es imposible que una letra perteneciente a una de las mitades del alfabeto sea reemplazada por otra localizada en su misma mitad. En este sentido hemos encontrado varios cifrados que podrían corresponderse con la técnica utilizada, sin que ninguno de ellos se correspondan al 100 % con el utilizado en esta carta. Este hecho se debe a que era una práctica común que las personas crearan sus propios cifrados a partir de los ya existentes.

En orden cronológico, el primer cifrado que mantiene cierta relación con el expuesto en este trabajo es el Atbash (Jer 25,26.). Es un cifrado por sustitución también denominado cifrado en espejo y utilizado entre el 600 y 500 a.C. por los hebreos. Este cifrado era monoalfabético por lo que no se corresponde exactamente con el cifrado utilizado en la carta que aquí se analiza. Sin embargo, es un método en espejo, al igual que el cifrado de este trabajo, que, sustituye la primera letra por la última, la segunda por la penúltima, y así sucesivamente.

Otro de los cifrados que siguen este funcionamiento es el cifrado de Giovan Battista Bellaso [6]. Publicó su primer trabajo en 1553, tratándose de un cifrado también en espejo y bidireccional pero polialfabético ya que originalmente empleaba 11 alfabetos distintos. Este sistema mantiene la primera mitad del alfabeto estable, mientras que la segunda mitad es desplazada un número, aparentemente aleatorio, de lugares respecto a la mitad superior. Este cifrado puede complicarse un poco más colocando en primer lugar las vocales y luego las consonantes. El cifrado se lleva a cabo mediante el uso de una frase acordada, colocado sobre el texto en claro. Con referencia a la tabla, se sustituye la letra de texto plano con la letra que está por encima o por debajo de ella en el alfabeto identificado por la letra mayúscula de la clave. Este cifrado es el que más guarda concordancia con el cifrado presentado en este trabajo, sin embargo, la clave en nuestro caso debe ser numérica. En 1555 Battista presenta una segunda propuesta, semejante a la anterior pero en el que las letras índice se mezclan por medio de una frase clave mnemónica, que puede ser diferente con cada corresponsal. En 1564 se publica el tercer libro de Bellaso donde se proponen nuevas tablas con diferentes variaciones, y además, se pueden utilizar con o sin contraseñas. En el caso de que el emisor y receptor no tengan una clave compartida, se propone utilizar como clave las iniciales de cada palabra.

En 1563 surge el método criptográfico denominado tabla de reciprocidad Della Porta [7]. Fue creado por por Giambattista della Porta, famoso científico italiano. Sin embargo, este cifrado no es más que una réplica del cifrado anterior. En España existe constancia del uso de este cifrado, en [8] habiéndose encontrado una versión de la tabla Della Porta que data de 1591.

Por último, se ha encontrado otro cifrado que guarda también una estrecha relación con el que se utiliza en la carta. Se trata del ROT13 [9] que también utiliza una tabla y sustituye cada letra por la letra que está trece posiciones más adelante, posteriormente la secuencia se invierte. Aunque es el cifrado más fácil de encontrar y su uso se asemeja al de la carta, ha sido descartado ipso facto, ya que su origen está datado en 1980.

En cuanto a la criptografía utilizada en el siglo XIX en España, existen diferentes obras, un ejemplo es la del catedrático de taquigrafía D. Francisco Paula Martí [10]. El libro, más bien un libreto, constaba de tan solo 56 páginas y fue editado en 1808 con el título "Polígrafía o arte de escribir en cifra". Sin embargo, su valor en términos de seguridad criptográfica no es muy relevante. No podemos dejar de mencionar también algunas obras españolas de finales del siglo XIX, como son:

III. Criptoanálisis

Para iniciar el proceso de descifrado no teníamos demasiado contexto, lo único que sabíamos es que se trataba de una carta del siglo XIX escrita por alguna personalidad de alto rango y relacionada con Tenerife. Contábamos con el texto manuscrito de tres páginas, con alrededor de 200 palabras cada una de ellas, y 16 tablas de cifrado, mostradas en la Tabla I, que supuestamente deberían ser utilizadas para el descrifrado de la misma. La existencia de estas tablas nos hizo pensar que estábamos ante un cifrado polialfabético en el que a partir de una clave, se utilizaría una u otra tabla.

Tabla I
Tablas originales del cifrado.

1	l	j	i	h	g	f	e	d	c	b	a	m	ll
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
2	f	e	d	c	b	a	m	ll	l	j	i	h	g
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
3	j	i	h	g	f	e	d	c	b	a	m	ll	l
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
4	a	b	c	d	e	f	g	h	i	j	l	ll	m
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
5	f	e	d	c	b	a	m	ll	l	j	i	h	g
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
6	a	b	c	d	e	f	g	h	i	j	l	ll	m
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
7	e	d	c	b	a	j	i	h	g	f	m	ll	l
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
8	l	j	i	h	g	f	e	d	c	b	a	m	ll
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
9	e	d	c	b	a	j	i	h	g	f	m	ll	l
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
10	g	f	e	d	c	b	a	m	ll	l	j	i	h
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
11	h	g	f	e	d	c	b	a	m	ll	l	j	i
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
12	a	b	c	d	e	f	g	h	i	j	l	ll	m
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
13	a	b	c	d	e	f	g	h	i	j	l	ll	m
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
14	c	a	b	f	e	d	i	h	g	ll	l	j	m
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
15	a	b	c	d	e	f	g	h	i	j	l	ll	m
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
16	f	e	d	c	b	a	l	ll	k	j	i	h	g
	n	ñ	o	p	q	r	s	t	u	v	x	y	z

Siguiendo los principios del criptoanálisis, el primer paso consistía en analizar el texto de la carta en busca de algún patrón como palabras repetidas, o alguna estructura sintáctica que tuviera algún sentido. Además, se podía presuponer que el idioma del texto original era el español y de esta forma, plantear hipótesis sobre las letras, digramas y trigramas más probables. Esta tarea no fue muy ardua dado que la carta terminaba con algo parecido a una fecha. Este hecho, junto a la existencia de espacios entre palabras, la utilización de mayúsculas, la utilización de números, etc., son algunos de

los fallos que comete el emisor a la hora de cifrar la carta, y que incluso en esa época, sin la potencia computacional con la que contamos hoy en día, llevaría a un posible interceptor a criptoanalizarla. Todo esto concuerda con la pobreza criptográfica que existía en la época. En (1) podemos ver la estructura sintáctica con la que cierra la carta, junto a las iniciales del emisor encriptadas y su firma.

$$Yqrgut\ 21\ tn\ tsc \tag{1}$$

Las posibles cribas que forman parte de una fecha son: *de, en* y *el*, que corresponderían al texto cifrado"tn".

- Se descarta la criba *en* ya que la n no puede ser cifrada (ninguna letra puede ser codificada como sí misma).
- Se descarta la criba *el* ya que no existe ninguna combinación e → t en las tablas para cifrar/descifrar.
- La criba *tn* descifrada es *de* en las siguientes configuraciones: 1,7 1,9 , 8,7, 8,9, es decir, esas 4 configuraciones utilizando para la primera letra la tabla 1 ó 8, para la segunda letra la tabla 7 ó 9 dan como resultado la criba obtenida.

Como se puede observar en la Tabla I, las tablas 7 y 9 son idénticas con lo que para descifrar la segunda letra se reduce el problema a una única tabla, quedando para la primera letra solo dos posibilidades 1 ó 8.

Para continuar el descifrado, fué necesario realizar un análisis de frecuencia, donde mediante repeticiones de palabras pequeñas conocidas como: *a, y, de, el, la, que, uno ...*, se podrían inferir al menos las tres primeras tablas. En las siguientes imágenes podemos ver los bigramas, (Figura 1) y trigramas, (Figura 2) , que no necesariamente son monosílabos, más repetidos en una parte del texto analizado, así como los más frecuentes en el español.

En las gráficas correspondientes a los bigramas más repetidos en el texto (en rojo), buscamos los que se corresponden con monosílabos en el texto cifrado. El primero se corresponde con *tn* que, comparándolo con el monosílabo, de dos letras, más repetido en el español (en azul), se corresponde con *de*. Se puede observar que los trigramas que más se repiten son *jgq y fcd* que además, coinciden con monosílabos en la carta. Si nos fijamos en las estadísticas del lenguaje español, los monosílabos de tres letras que más se repiten son *del y que*. Volviendo a las tablas que proponíamos como iniciales y conociendo la segunda, buscamos combinaciones válidas. Los resultados son *ñu* → *jg y ro* → *fc* con las tablas 1-7 y *qu* → *jg y po* → *fc* con las tablas 8-7. Por lo tanto, de estos monosílabos se puede deducir que la primera tabla es 8 y tenemos dos nuevas propuestas, *que y por* para buscar una tercera tabla. Con esta información el proceso es fácil, se debe encontrar una tabla que cumpla las siguientes sustituciones *q* → *e y d* → *r* existiendo una única posibilidad en la tabla 14.

Según lo visto en los párrafos anteriores, el orden de las tablas iniciales es: 8, 7 o 9 y 14 . Llegados a este punto, la obtención de la cuarta tabla sería algo trivial. En la Tabla II podemos ver algunos ejemplos de palabras de 4 letras cifradas y su descifrado utilizando las tablas obtenidas y deduciendo cual sería la letra que ocupa la cuarta posición. Una vez más, aplicamos el mismo procedimiento descrito anteriormente, en busca de alguna tabla que se corresponda con las letras obtenidas. Sin embargo, si se observan las tablas, no hay

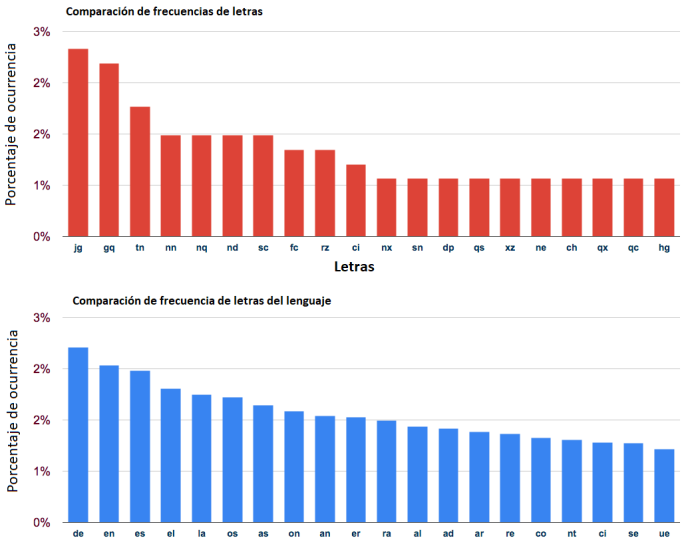

Figura 1. Frecuencia de bigramas.

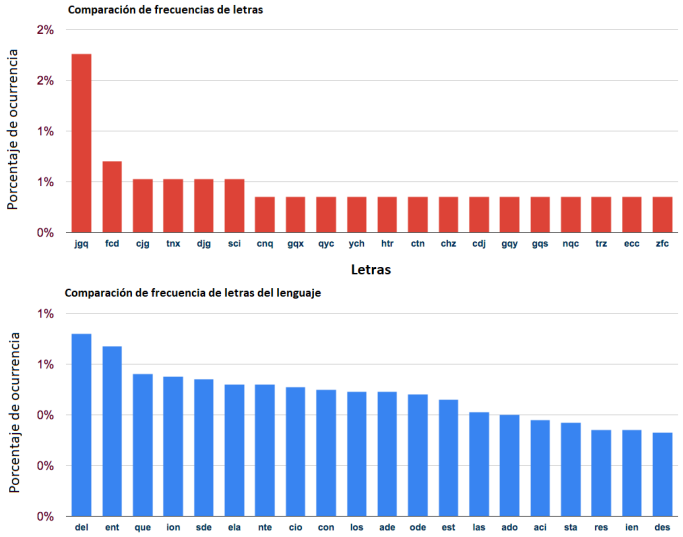

Figura 2. Frecuencia de trigramas.

ninguna que funcione para todas las palabras. En este punto se dió por finalizado el criptoanálisis manual y se optó por diseñar e implementar un código para el descifrado.

III-A. Fuerza Bruta

Un ataque de fuerza bruta consiste en probar todas las combinaciones posibles hasta lograr encontrar un resultado satisfactorio. En muchos casos la fuerza bruta hace uso de diccionarios, de manera que a partir de las combinaciones obtenidas, busca palabras existentes en los mismos. Para el

Tabla II
TABLA DE CIFRADO DESAPARECIDA.

lhñ Ujg**i**	Sta Cru**z**
tqh**b**	dat**o**
ln lnf**p**	se sep**a**
hc sc nqn**t**	no lo hac**e**
10 g 12 tsñ**f**	10 o 12 día**s**
fcd rz zsq**d**	por el bie**n**

caso que nos ocupa, este tipo de ataques podría verse limitado, ya que las combinaciones a realizar estarían restringidas a las 16 tablas disponibles. Por lo tanto, conociendo el funcionamiento del cifrado utilizado en esta carta, haciendo variaciones sin repetición de las 16 tablas se puede obtener las distintas posibilidades. Se tratan de variaciones ordinarias de 16 elementos tomados de n en n. Con esto se pueden obtener todas las combinaciones de las tablas, que se representarían como se muestra en la ecuación (2).

$$e_{16,n} = m(m-1)...(m-n+1) = \frac{m!}{(m-n)!} \quad (2)$$

Según la transcripción de la carta, la palabras más larga sería de 13 letras por lo que el número máximo para n sería 13. Sin embargo, como se comentó anteriormente, muchas de las tablas están repetidas con lo que se nos disminuiría el problema a tan solo 9 tablas diferentes. Por lo tanto, si se aplica la fórmula para todas las combinaciones posibles de tablas, se obtiene la ecuación que se muestra en (3).

$$\sum_{n=2}^{n=9} \frac{m!}{(m-n)!} \quad (3)$$

Si para cada una de las combinaciones de tablas tenemos en cuenta las combinaciones de letras para el afabeto utilizado, tendremos que añadirle a la fórmula anterior las variaciones que se generan con los diferentes alfabetos de las tablas implicadas. Por ejemplo:

$$\sum_{\mathrm{n}=2}^{9} \frac{9!}{(9-\mathrm{n})!} \cdot \frac{26!}{(23-\mathrm{n})!} \cdot \mathrm{n} = 1{,}60285\ldots E22 \quad (4)$$

Por lo tanto, la fuerza bruta para obtener las combinaciones en las sucesivas posiciones de cada palabra en el texto fue descartada debido a la complejidad computacional.

Descartada la idea original para el descifrado de todo el texto, se opta por volver a las cribas e ir escalando de manera progresiva. Sabiendo ya las posibles combinaciones para las tres primeras letras de todas las palabras del texto, fácilmente se pueden obtener las palabras descifradas de tamaño 4. Al tener solo las dos primeras posiciones, hay que seleccionar las palabras de tamaño 4 del texto y descifrar sus tres primeras letras para predecir la letra final.

Para aumentar la veracidad de estas combinaciones hay que comprobar el resto de palabras de tamaño 4 utilizando la misma tabla en la posición 4. Para automatizar este proceso se ha desarrollado un script en Python que según el orden de tablas que establezca el usuario, el programa descifra el texto introducido utilizando dicho orden. Las tres primeras tablas las tenemos, con lo que solo nos faltaría hacer todas las permutaciones posibles con el resto de tablas para obtener la que ocuparía la cuarta posición. En este caso y teniendo en cuenta que existen tablas repetidas, nos quedaría un total de 6 tablas posibles entre las las 9 que son diferentes entre ellas. Esto implica un total de 720 combinaciones diferentes, siendo un resultado algo más abordable. En el siguiente código se puede ver la utilidad para descifrar la palabra *Madrid*. Como es un cifrado en espejo, se ha utilizado la librería de mapeo bidireccional para Python *bidict* [11]. El objetivo es recorrer la palabra letra a letra e ir descifrando cada una de ellas, con las tablas correspondientes y en el orden establecido por *tablas*. Si la letra pertenece a la segunda mitad del alfabeto, se busca la letra a sustituir en forma inversa *tablas[j].inverse[prueba[i]]*. Si es un espacio, simplemente se avanza. Si pertenece a la primera mitad del alfabeto, se sustituye por la letra correspondiente *tablas[j][prueba[i]]*. Con este código, lo que se busca es automatizar la reorganización de las tablas utilizando aquellas que podrían ser candidatas según las cribas.

```
tablas = [
bidict({'B': 'Z', 'M': 'Y','A': 'X','K': 'V',
'C': 'U','D': 'T','L': 'S','E': 'R','J': 'Q',
'F': 'P','G': 'O','I': 'Ñ','H': 'N'}),# T8

bidict({'E': 'N', 'D': 'Ñ','C': 'O','B': 'P',
'A': 'Q','J': 'R','I': 'S','H': 'T','G': 'U',
'F': 'V','M': 'X','K': 'Y','L': 'Z'}), # T7

bidict({'C': 'N', 'A': 'Ñ','B': 'O','F': 'P',
'E': 'Q','D': 'R','I': 'S','H': 'T','G': 'U',
'K': 'V','L': 'X','J': 'Y','M': 'Z'}),# T14
                .
                .
                .
 ]

prueba = "Yqrgut"
prueba = prueba.upper()
print(prueba)
resultado = ""

j = i = 0
while i < len(prueba):
   if((re.search('[N-Z]|Ñ', prueba[i]))):
       resultado += tablas[j].inverse[prueba[i]]
       i += 1
       j += 1
   elif(prueba[i] == " "):
        resultado += ' '
        j = 0
        i += 1
   else:
       resultado += tablas[j][prueba[i]]
       j += 1
       i += 1

print(resultado)
\end{lstlisting}
```

Una vez automatizado el descifrado con las nuevas combinaciones establecidas, ya era posible descifrar practicamente aquellas palabras de hasta 8 letras casi en su totalidad. Sin embargo, los resultados obtenidos no son los esperados ya que hay un orden de tablas que funciona correctamente en ciertas palabras, siendo en otras incorrectos. En la Figura 3 podemos ver los resultados obtenidos con las cribas, y el código planteado. Además, como se puede observar y tal como se había visto en el proceso manual, la tabla que ocuparía la cuarta posición continuaba sin tener una correspondecia con alguna de las tablas existentes. Este hecho nos llevó a realizar un análisis más exhaustivo de lo que estaba ocurriendo, examinando más en profundidad el cifrado como veremos en la siguiente sección.

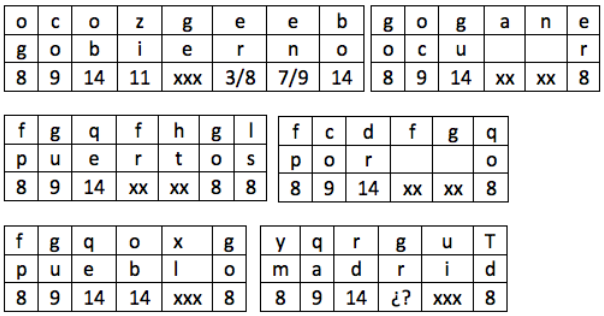

Figura 3. Combinación de subtablas probables.

IV. Análisis del cifrado

El número de letras del alfabeto utilizado en este cifrado es de 26, y sus características se corresponden con el lenguaje utilizado en el siglo XIX ya que no existe la letra k. Volviendo a buscar alguna similitud con el cifrado Della Porta, podría darnos alguna pista de cómo hacer uso de las tablas proporcionadas. Este cifrado proporciona a cada fila dos letras del alfabeto ordenadas. Por lo que usando una palabra clave nos daría las diferentes tablas a utilizar por cada letra a cifrar. Si analizamos el método de cifrado, como se explicó en el apartado anterior, el número de tablas queda reducido a 9, (ver Tabla III), ya que las siete restantes son una copia de alguna de las 9 anteriores. Por lo tanto, es posible pensar que eran estas y solo estas, las tablas que se utilizaban para el cifrado y descifrado de la carta. Por lo tanto, se puede concluir que el resto de tablas se han añadido a la carta para confundir a un posible receptor, no legítimo, de la misma. Además, se podría pensar que este sería el tamaño de la clave ya que, como se ha visto, el orden se repite cíclicamente en el texto por cada palabra. Uno de los métodos más conocidos para obtener el tamaño de la clave utilizada en un cifrado polialfabétido es el método Kasiski [12], sin embargo, tras su aplicación la conclusión fue que el tamaño de la clave con más probabilidad era 2.

Es posible que esto se deba a dos posibles factores:

- El hecho de que la carta esta manuscrita lo que dificulta entender la letra exacta.
- Posibles errores de la persona al cifrar la carta. Por ejemplo, durante toda la carta aparece la palabra, una vez descifrada, *pue*. Se llegó a la conclusión de que podría tratarse de un error arrastrado a lo largo de la carta porque, la palabra correcta y que tendría sentido utilizar es *que*. Lo más probable es que en algún momento el emisor transcribió mal este monosílabo y lo repitió a lo largo de todo el manuscrito.

Tabla III
Subtablas de cifrado.

1	l	j	i	h	g	f	e	d	c	b	a	m	ll
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
2,5,16	f	e	d	c	b	a	m	ll	l	j	i	h	g
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
3	j	i	h	g	f	e	d	c	b	a	m	ll	l
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
4,6,12	a	b	c	d	e	f	g	h	i	j	l	ll	m
13,15	n	ñ	o	p	q	r	s	t	u	v	x	y	z
7,9	e	d	c	b	a	j	i	h	g	f	m	ll	l
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
8	l	j	i	h	g	f	e	d	c	b	a	m	ll
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
10	g	f	e	d	c	b	a	m	ll	l	j	i	h
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
11	h	g	f	e	d	c	b	a	m	ll	l	j	i
	n	ñ	o	p	q	r	s	t	u	v	x	y	z
14	c	a	b	f	e	d	i	h	g	ll	l	j	m
	n	ñ	o	p	q	r	s	t	u	v	x	y	z

Otra de las cuestiones que nos quedaba pendiente era el descifrado de la cuarta letra, ya que era imposible encontrar una tabla que encajara correctamente con la letra que ocupaba dicha posición en el cifrado. Es claro que ninguna de las 9 tablas coincidía o funcionaba para descifrar la carta. Se intentó la posibilidad de utilizar diferentes tablas para esta posición, pero esto sería un trabajo realmente tedioso para el cifrado y descifrado de la misma, y no correspondería con la existencia de una palabra clave. Teniendo en cuenta que las letras que ocupan la cuarta posición se podía deducir, se optó por crear manualmente la tabla correspondiente con el cifrado de dicha posición. El resultado es la Tabla IV, y tras su utilización en el código, se concluyó que se trataba de una única tabla y que funciona correctamente para todas las palabras en dicha posición. Además, no se corresponde con ninguna de las tablas que acompañaban a la carta. Por lo tanto, la tabla se debía deducir de la propia clave o bien, se trata de una tabla que compartían previamente el emisor y el receptor o dicha tabla de cifrado no fué enviada. Otra hipótesis es que se tratara de un error a la hora de cifrar la carta pero, se descartó porque la nueva tabla funciona perfectamente a lo largo de la carta. Además, no existen indicios que prueben que el receptor llegara a descifrar el contenido del manuscrito.

Una vez obtenidas las 4 primeras tablas que funcionaban correctamente a lo largo de la carta, se procedió a intentar averiguar el tamaño de la clave. Analizando detenidamente las tablas, la primera mitad del alfabeto comprendido entre [a-m] se encuentra modificado, aparentemente por un desplazamiento, manteniéndose la segunda mitad estable [n-z]. Las tablas enumeradas 1, 2, 3, 4, 10, 11 y sus copias correspondientes, presentan un desplazamiendo de 10, 5, 9, 0, 6 y 7 posiciones a la derecha respectivamente. Sin embargo, las tablas restantes, la 8, 7, 14 y la nueva Tabla IV, presentan un patrón diferente tal como puede verse en la Figura 4.

Volviendo al patrón de tablas utilizado hasta el momento para el descifrado de las 4 primeras letras se puede observar una clara correspondencia entre estas tablas, que no siguen el patrón de desplazamiento, y las tablas que se usaron en el código implementado para el descifrado de la carta. Son estas las tablas que han funcionado para descifrar la mayor parte del mensaje. Además y como vemos en la Figura 4, la quinta posición estaría ocupada por la subtabla 4 o cualquiera de sus réplicas. Con esta nueva conjetura, se asume que esta es la clave y se procede a utilizarla en el código a lo largo del descifrado y en el orden establecido 8, 7, 14, Tabla IV y

Tabla IV
Subtabla de cifrado desaparecida.

17	d	c	b	a	h	g	f	e	m	ll	l	j	i
	n	ñ	o	p	q	r	s	t	u	v	x	y	z

n	ñ	o	p	q	r	s	t	u	v	x	y	z	Tabla
h	i	g	f	j	e	l	d	c	ll	a	m	b	8
e	d	c	b	a	j	i	h	g	f	m	ll	l	7o9
c	a	b	f	e	d	i	h	g	ll	l	j	m	14
d	c	b	a	h	g	f	e	m	ll	l	j	i	x
a	b	c	d	e	f	g	h	i	j	l	ll	m	4

Figura 4. Subtablas que no siguen patrón desplazamiento.

4.

El resultado fue el esperado, se había dado con la clave del descifrado. La última tabla correspondiente a la tabla número 4 es el alfabeto sin ningún tipo de desplazamiendo. Ahora quedaba deducir de dónde obtenía el receptor que este era el orden para descifrar la carta. Esto se analiza más profundamente en el apartado V.

V. Hipótesis sobre la clave empleada

En el apartado anterior se concluye que estamos ante un cifrado de sustitución polialfabético que tiene una clave de tamaño 5. Además, esta clave podría ser una palabra que nos llevara a una correspondencia numérica o bien directamente una cifra. En este apartado presentamos las hipótesis que barajamos para concluir cómo el emisor y el receptor se podrían haber puesto de acuerdo para el intercambio u obtención de la clave. De todas formas, entre nuestras hipótesis, preguntas sobre la carta, el objetivo de cifrarla, la clave utilizada, etc., siempre aparece la cuestión de si fue realmente el receptor capaz de descifrarla.

A continuación se presentan diferentes opciones que se barajaron por el contenido de la carta.

V-A. Relación con el texto en claro

En el apartado IV se concluyó que la clave utilizada en el cifrado se corresponde con las tablas 8, 7, 14, Tabla IV, 4. Aunque se tratan de cifras numéricas, es posible que exista alguna palabra que nos lleve a obtener esta relación. Además, parece claro que debe ser una palabra de 5 letras.

En la parte superior de la carta aparece una frase con texto en claro. Lo primero que se pensó es que podía existir alguna relación entre este texto y la clave. Puede ser que la frase contenga la clave en sí o bien algún patrón que permitiese al receptor obtener la misma.

El texto en claro que proporciona la carta es el siguiente:

$$Urge.\ Con\ ayuda\ de\ Aaron \tag{5}$$

En el lenguaje natural se podría pensar que la carta fue cifrada con la ayuda de Aaron, lo que podría ser algún mensaje que solo en el contexto del receptor tuviese sentido y le proporcionara información suficiente para obtener la clave utilizada y el método de descifrado.

Otra posibilidad es que el emisor le estuviese indicando al receptor que contactara con Aaron, que este sería la persona encargada de ayudar a descifrar el mensaje. Por lo tanto, sería Aaron el que tuviese la relación numérica de las tablas a utilizar, el método de descifrado, así como la tabla desaparecida.

Por último, es posible que se encuentre en este texto la clave. Deducimos que debe ser objeto de análisis ya que de otra manera, no se puede entender por qué existe texto en claro estando el resto de la carta, incluso las iniciales del emisor, cifradas. En busca de alguna combinación de 5 letras, tenemos que son las palabras *ayuda*, *Aaron*, o incluso las iniciales de cada palabra las que constarían de 5 letras, *U-C-A-D-A*. No obstante, ninguna corresponde con la clave utilizada.

VI. Conclusiones y trabajos futuros

Las crónicas de Canarias y las Américas esconden un sinfín de historias poco o nada conocidas acerca de las personalidades involucradas en ella. La formación geopolítica actual y la elección de capitales y provincias han estado marcadas a lo largo de la historia por decisiones principalmente políticas donde la influencia de las personas podía ser clave para marcar el devenir de las cosas. En este trabajo se ha descubierto el contenido de un manuscrito cifrado, conteniendo conversaciones privadas entre partidarios de una misma formación de gobierno en las que intercambiaban información que podía ser relevante, en aquel momento, para influenciar a ciertas personalidades de las que podían depender decisiones que se tomaban en la época.

Para obtener dicha información se ha tenido que transcribir y descifrar dicho manuscrito sin más información que los documentos que se encontraron. Para ello mediante técnicas de análisis estadístico, estudio de los cifrados utilizados en la época y el diseño e implementación de un programa informático para obtener los posibles resultados de descifrar el documento, se pudo resolver el enigma y conocer el contenido de la carta.

Como trabajo futuro sería interesante obtener la clave que da lugar a la elección de las tablas a utilizar, no obstante, es posible que dicha información se encuentre en otros documentos a los que no se tiene acceso. También se puede seguir estudiando en más profundidad la utilización de cifrados durante este siglo para la comunicación y envíos postales con las Indias. En concreto, sería interesante indagar más sobre la segunda clave del general Ricafort, ya que hay constancia de la existencia de las mismas. Además, se debería hacer un estudio en profundidad de los cifrados polialfabéticos usados en esa fecha. Por otro lado, falta esclarecer la identidad de la persona que envía el documento. Tal y como se comenta en el artículo, no existen otras cartas cifradas por lo que no se tienen muestras suficientes para poder deducir cuál de las hipótesis barajadas en la obtención de la clave podría ser la correcta. Esta carta se encuentra digitalizada y cedida de forma gratuita a la comunidad Universitaria para permitir su descifrado, no teniendo constancia de ninguna otra carta cifrada. También sería interesante que la carta sea revisada por un equipo paleográfico con el objetivo de asegurar que el texto manuscrito se corresponde con el contenido extraído en este trabajo.

Agradecimientos

Investigación apoyada por el Ministerio de Ciencia, Innovación y Universidades de España y el Centro de Desarrollo de Tecnología Industrial CDTI mediante los Proyectos RTI2018-097263-B-I00 y C2017/3-9.

Referencias

[1] Kahn, D., The Codebreakers : The Comprehensive History of Secret Communication from Ancient Times to the Internet, Scribner. 1996.

[2] Prieto, M. J., Historia de la criptografía: cifras, códigos y secretos desde la antigua Grecia a la Guerra Fría.. Editorial: La esfera de los libros. 2020.
[3] Soler Fuensanta, J. R., La Criptología Española hasta el final de la Guerra Civil. Consultado el 18/02/2021 en http://www.criptohistoria.es/files/historia.pdf
[4] Bakula, J. M., Apuntes de historia, criptografía y diplomacia de la emancipación, Imprenta Torres Aguirre, Lima, 1949.
[5] Galende Díaz, J. C., "Sistemas criptográficos empleados en Hispanoamérica", Revista Complutense de Historia de América, 2000, 26, pp. 57-71.
[6] Belaso, G. B., 1553, La cifra del sig. Giovan Battista Bellaso, gentil'huomo bresciano, nuovamente da lui medesimo ridotta à grandissima brevità et perfettione, Venecia, 1553.
[7] Della Porta, G., De Furtivis literarum Notis vulgo de ziferis libri IIII, GM Scoto, Neapolitano 1563.
[8] Díaz, J., Soler Fuensanta, J. R. y López-Brea Espiau, F. J., Mensajes secretos. La historia de la criptografía española desde sus inicios hasta los años 50. Documenta & Instrumenta - Documenta et Instrumenta. 15. 10.5209/DOCU.2017.v15.56214. 2017.
[9] Early uses of ROT13 found in the Google USENET archive date back to 8 October 1982, posted to the net.jokes newsgroup. Consultado el 18/02/2021 en https://groups.google.com/g/net.jokes/c/kT6z3p4fmbM/m/F6NC4laekd0J
[10] De Paula Martí, F., Poligrafía o Arte De Escribir En Cifra De Diferentes Modos. Madrid, Imprenta de Sancha, 1808 (reeditado en Valencia, 1993).
[11] bidict 0.21.2. Consultado el 18/02/2021 en https://pypi.org/project/bidict/
[12] Kasiski. F. W., Die geheimschriften und die dechiffrir-kunst: Mit besonderer berücksichtigung der deutschen und der französischen sprache. E. S. Mittler und sohn. 1863.

ANEXO

VII. Transcripción de la carta

Nota: Cada vez que aparece una *k* se corresponde con la *ll*. Se ha puesto así para poder sustituir esta letra correctamente en el código.

D. Cccnq sgqrc jgq lgft rz hczofxxstadc tn Esnprgjh yn xpbhir x rz m nn yndtoññb lg xxsfhxñ: Sn vngt dcrbg sci zcxthñeqf tn xts jgq:sn yqczrriht rz gpythg tnx fjbdihospzñncec tn uqcpfñq: sc jgq ychzjg rz tn lhñ Ujgi: jgq xxopg rjñd rnhtzfcdparci (m xis ln ysdpfge re rz Ocozqeeb); y fcd sc ysiuc hgxb dcrb sc jgq nqc gpdppg:sqi kncenqqi tn jgq sq uqfzhxz riht re dnctfñvq m rz fcd jgq: gstari uczhchnc ceñ m ghdp m lgi uqdpodndtg m xestorñqdhri jgq nqj: jgq ychzjg ksdeixzztadn sq tsibxcosba tn riq Xkgdhxx. m fcd jgq hc rehgnecc sci tn 37 m 38 x gogane sci fgqfhgi____ m pcztadc sqi tsntcimsbdqt: jgsta sqi pcztadq m fcct re yckzzñncec rz fgqoxg____ucc riht ychzjg sn nsnt ceñ fsceieq tn sci fgq xyñ lcc yqxbg ____Jgstari lcc sci fgqoxgi fgq vnkpa sq kcm: Jgq sq Squmax dsqdq dcrpg sqi lszandsñf: jgq Lhn UJgi hc. Sn rnnbzrert m tsyt jgq rz ycrb tn fqizrñoñg rib ri fcctfln tn xogtftc ucc Pfnfecshb U?, ucc Pchenv, ucc Uspgn, m ghdbg: ucc C., ucc Hqkp ucc sci Kcxbsxi, m sci Ecxpari, ucc Snñx &[a].____ Sn tsut jgstars sci nczofri tn tsqd tn xts, m jgstars sci yqxbg m rz fcd fgq____ Uczb ucceneg ucc sqi pgqgmxi, m rehbauni sn nqoxq tn sci ucdbarzgf. Yn nsmb ygnqnl fjqrihhñf. Fniairi nn ññb uqiz dcrpg sqi hcnqql x lg uqip. Sn nn tqrb ceñf ñeiefconzchni fgq yn fsrzc m lcd Tn 4 fzstsgi. Ce rihppg tn sqi rznñoñcctg czhzzxi m sqi ssienl rzqñhgjñxql

Uczb yn fjqrihhb fcd sqi fndfchqi ñepximneql tn xyñ, m sqi vnkp xbgdhxnñf. Ri fjqfulc jgq xz ycztadc ln xpbhirc x rz C., Snñx rz Utñdhen, Hqkp sci Ucxbsxi, Lqñkjtjn, Ycdp m Ogqinsq & jgq kgj ennbzrerppgi rz ri ygj djñenzzq, m kq fjqaneqrb uccegx rz zgvzoñc.

Fnx gpsfdg sn nsnt ceñ pgdzñcerp fsceieq, fcdhir fcd rz yn neenuesb; m sn xdñnu jgq rz Utñdhen sn fcrgux (tqd yqi tqhbg Hc jgstfr jgq ln lnfp jgq mc sn nn ñxfmqlhb tn hqrp. M sni lgfxuuc jgq hc yn hczcfre, ls rz hc sc nqnt; yqczrrihputc CG. rihpf xuqdcl tn dcrb

Mc ln jgq ys enxpoñcc tniafrisppx fcdhir tniairi tn 10 g 12 tsñf jgq mq mc sc ksnzhxpñ sc nsnzqecc Zgxdql m Znvb. Mc sni fjqrihhq jgq rjñ sc jgq rz tnnzn, m yn nsgzgecc ceñ fsceieq lnztyxeht x sqi ññqpg jgq mc sn nqozn ñepmatsrb. Znvb yn tsb x rehtatnd jgq rz sc nqozn nnnqc dcrb m mc yn rnj fcdhir rvbf hc lqota jgq mc sc djñec m rz Onctfxz yn nqozn tsnqc mq sc jgq sn nqoznh nñb x nqoxne

Zgienyqceq sn nqoxc dqzoure m sc ñenxuhc x usqghx riftoñn tn ñertdrer rehgq sqi tci ñixpg lscb dchpx x sc yncbg fqdnnxz. Sc jgq xfsfc

Mc yn lciaqutb jgq rz Occtfxz jgqgfx jgq CG hczofre tsfmhxñb x Zgxdql m riht sc tontn, hc fcd rz zsqd tn xyñ lscb fcd nqoxne re sqi ucdeql x pqobf tn sq Nqopax, jgq xis sc nq tsnqc; jgq tsianeqht hqdpa CG= Ri rz nczofr yqs lcotfzsb fgq nn kshb. X hqrzq lsdkq hs gkq m dcrbg sci Uqcpfñci ln jgqynh tn rib____Znduitc ri ceb tn sci jgq lqdpa ceñ ññqn tn rz

Xz Onctf. sn nn ennbzrrppg rz xaqtpcohb tn xti, m rz uqzzag Zsqd uccbor C. jgq hc dcrbg tn sci hgqfheci tnota lqotf rihb Yqrgut 21 tn Tsc

C.O.