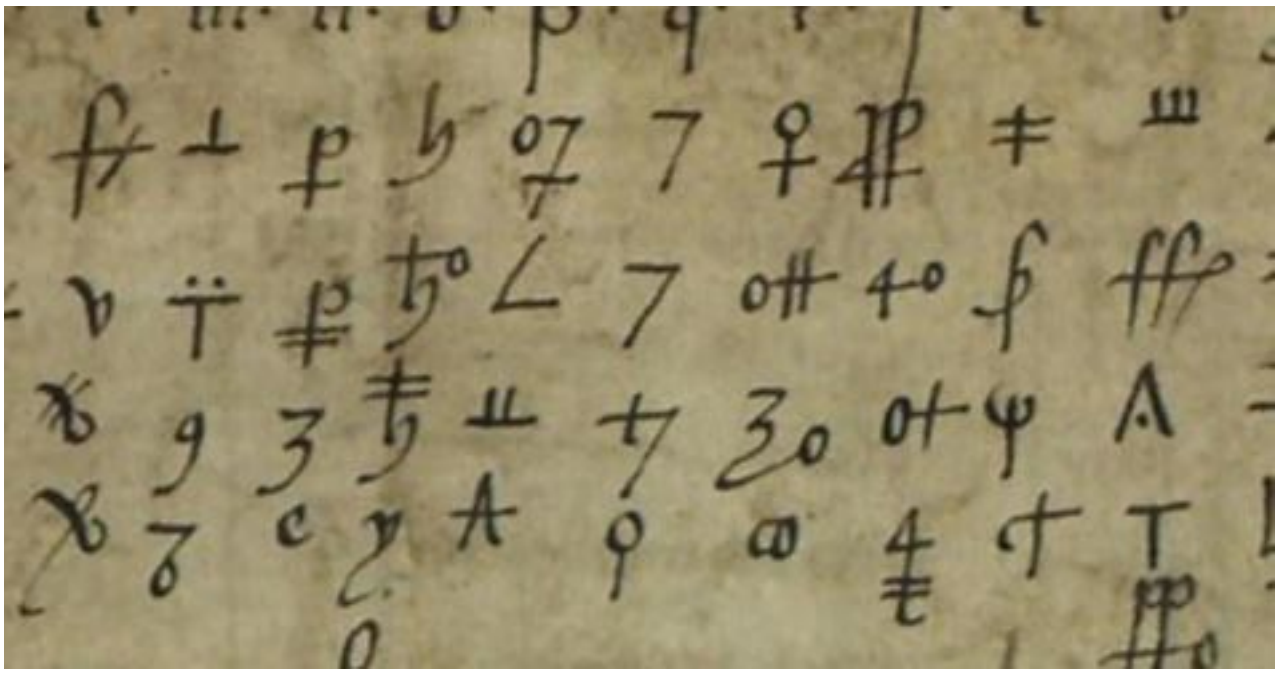
ABC, 16 de Octubre de 2018
CIENCIA - El ABCdario de las matemáticas
Alfonso Jesús Población Sáez

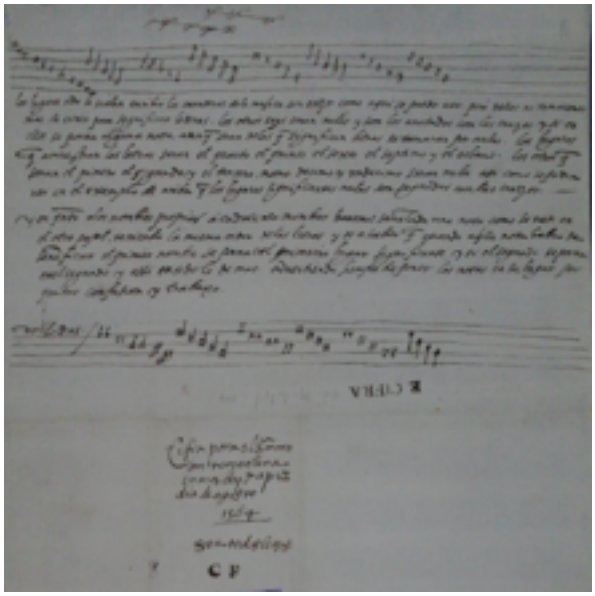
Los textos encriptados eran tan sencillos que se convirtieron en el hazmerreír de Europa. Hasta un niño podría resolverlos



Documento encriptado de la exposición «Espías: Servicios secretos y escritura cifrada en la Monarquía Hispánica» - Alfonso J. Población / Vea en el documental de ABC las cartas cifradas que estuvieron ocultas 500 años

Probablemente todos ustedes hayan oído hablar de la villa de Simancas y su célebre Archivo. Según se indica en un folleto editado por el Ministerio de Cultura y Deporte, el Archivo General de Simancas (AGS) fue iniciado por el rey Carlos V y finalizado por su hijo Felipe II, su verdadero impulsor, y atesora un fondo documental excepcional para el estudio de la historia de España desde finales del siglo XV hasta el siglo XIX. En este enlace se puede ampliar la información más relevante sobre este singular edificio.

Actualmente, y hasta el mes de julio de 2019 (o sea, que tienen tiempo, y ninguna excusa para no ir, si les interesa el tema), se exhibe la exposición «Espías: Servicios secretos y escritura cifrada en la Monarquía Hispánica». Se trata de un recorrido por el mundo del **espionaje en los siglos XVI y XVII**, una práctica que se acrecentó con las monarquías autoritarias y su necesidad de guardar las formas mediante la diplomacia, así como las teorías políticas ligadas a la «razón de estado» y el maquiavelismo, entre otras corrientes.



La muestra está dividida en tres ámbitos: La organización del espionaje (infraestructuras, normativas, financiación que aparecen desde el reinado de los Reyes Católicos); los espías (tipos de agentes, métodos utilizados, contraespionaje, etc.); y la **escritura cifrada** (cifras generales y particulares en los reinados de Carlos I y Felipe II). Más de setenta documentos de la época pertenecientes al Archivo ponen de manifiesto todo lo explicado, algunos realmente curiosos, en un marco realmente magnífico. El visitante se sorprenderá con la mayor parte de lo expuesto, si no conocía nada de historia de la criptografía, y un poco menos si sabe algo. Personalmente me llamaron la atención varios documentos:

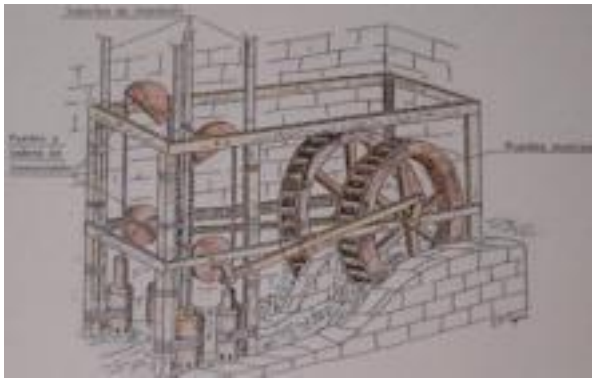
el libro de cifras

del Archivo, ejemplar manuscrito escrito entre 1890 y 1900 por Claudio Pérez Gredilla, que hizo el esfuerzo de recopilar todas las cifras que aparecen en los documentos originales del Archivo, junto a otras estudiadas en el siglo XIX de las que no se conocía la clave. También documentos con

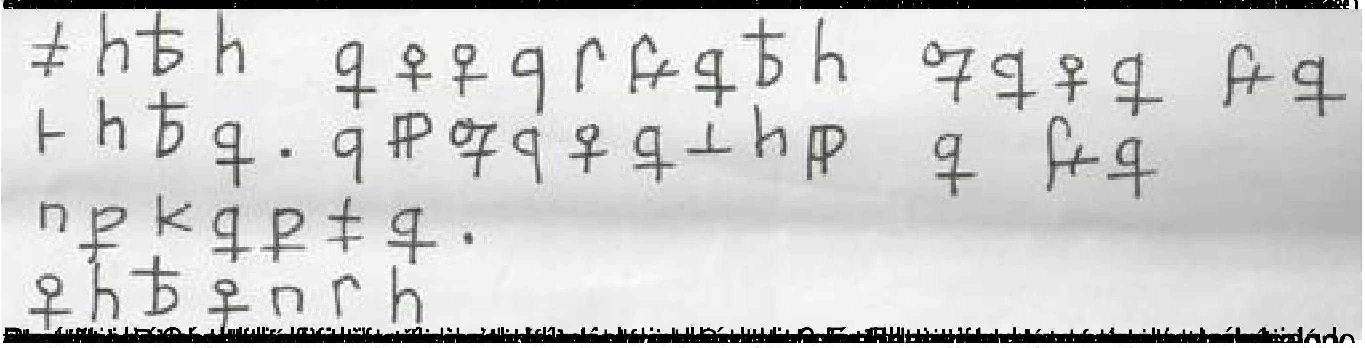
Cifras Generales

(una de Carlos V y otra de Felipe II) y

Cifras Particulares
(para asuntos que requerían de mayor discreción; en la imagen se muestra una basada en la notación musical, en la que cada letra del alfabeto se sustituía por una nota o signo musical).



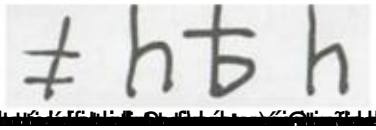
Por supuesto nos encontramos también mapas y dibujos ilustrativos, que nos ponen al corriente de la situación política y geográfica en la que se empleaban mensajes cifrados. Hay un pequeño recuerdo a algunos personajes célebres que utilizaron textos cifrados en su relación con la Corte (se exponen documentos relacionados con Miguel de Cervantes, Francisco de Quevedo o Pedro Pablo Rubens), y el célebre ingenio del vizcaíno Pedro de Zubiaur para bombear agua del río Pisuerga venciendo el desnivel con la ciudad, que acabó, ¡¡cómo no!!, apropiándose el ínclito Duque de Lerma para uso personal (ver imagen). Lo curioso del caso es que Zubiaur se basó en una máquina similar utilizada en Londres para elevar agua del Támesis a la ciudad, en un evidente ejemplo de espionaje industrial (el visitante puede juzgar si es plagio o adaptación, ya que en la muestra se exponen ambos proyectos). En todo caso, no restemos mérito ya que los conocimientos necesarios para trasladar lo visto tuvieron que ser amplios y bien fundamentados. Aunque Pedro de Zubiaur trabajó en principio para el ayuntamiento de la ciudad (el lugar donde se instaló el artefacto aún es identificable en la actualidad), una vez se hizo cargo el de Lerma del mismo, dejó de pagarle dinero alguno al inventor (hay documentación quejándose del hecho), aunque eso sí, transfirió posteriormente algunos dineros a la viuda a cuenta del servicio prestado por su marido. En definitiva, uno puede palpar la historia gracias a los distintos documentos expuestos.



	A	B	C	D	E	F	G	H	I	J	K	L	M	Ñ
	12.53	1.42	4.68	5.86	13.68	0.69	1.01	0.70	6.25	0.44	0.01	4.97	3.15	0.31

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	6.71	8.68	2.51	0.88	6.87	7.98	4.63	3.93	0.90	0.02	0.22	0.90	0.52

Fr.	2	7	4	11	6	3	2	3	2	1	2	1	1	2	2
%	4.1	14.2	8.1	22.4	12.2	6.1	4.08	6.1	4.1	2	4.1	2	2	4.1	4.1



[redacted]

[redacted]

	≠	h	⊬	♀	♁	♀	⌐	⨍	⁷	⊢	⋕	⊥	K	∩	♇
♀	1	0	3	0	3	0	0	3	0	0	0	1	1	1	1
♁	0	1	1	4	1	2	0	0	0	0	0	0	0	1	0
h	1	0	5	0	1	0	1	0	0	1	1	1	0	0	0

[redacted]

Respecto a los otros dos símbolos, todo apunta a que sean ambos vocales, por su "sociabilidad" de acuerdo a los números obtenidos. Y está muy fácil entre las vocales cuál asignarles, porque el símbolo ♀ aparece en solitario una vez, y dos veces seguidas en una palabra de dos letras, ⨍♀. Por tanto, parece razonable que ♀ = *a* , y que h sea la *e*, o la *o*. Veamos cómo queda el texto cambiando únicamente los dos primeros símbolos de acuerdo con nuestras suposiciones:

≠h⊬h arr♀⌐⨍a⊬h ⁷ara ⨍a ⊢h⊬a.

♀⋕⁷♀ra⊥h⋕ a ⨍a ∩♇ka♇≠a.

rh⊬r∩⌐h

Vistas así las cosas, no parece demasiado descabellado que ⨍ = *l*, ⁷ = *p*, lo que nos lleva a

≠h⊬h arr♀⌐la⊬h para la ⊢h⊬a.

♀⋕p♀ra⊥h⋕ a la ∩♇ka♇≠a.

rh⊬r∩⌐h

En este punto, el criptoanalista tanteará a ver si reconoce algunas palabras, o en su defecto irá probando posibilidades. También podría intentar deducir los otros símbolos suponiendo que el que hubiera cifrado el texto hubiera utilizado alguna palabra clave a partir de la cual sacar cada letra. Pero el utilizar símbolos inventados hace que descartemos esa posibilidad: no se ha complicado la vida y sencillamente ha utilizado una simple y elemental ***sustitución monoalfabética*** sin usar palabra clave. Desde luego el resto de vocales casi se intuyen dónde están, aunque no cuáles son. Volvamos al tercer símbolo que más aparece, h, del que dedujimos que pudiera ser o una *e*, o una *o*. En paralelo, observamos que en la segunda palabra, después de la doble *r* tiene forzosamente que encontrarse una vocal, 9, aunque puede ser cualquiera de las que faltan. Pero la primera palabra de la siguiente línea (la segunda frase porque hay un punto antes) empieza por esa misma letra, que se repite después de la letra *p* en la misma palabra. Supongamos entonces que 9 = *e* y que h = *o* (si llegaramos a alguna contradicción con palabras ininteligibles, volveríamos atrás y pondríamos la opción alternativa, como al resolver un sudoku: prueba-error). Esto nos lleva a

≠o⊰o arre⌜la⊰o para la ⊢o⊰a.

e₱pera⊥o₱ a la ∩₽ĸa₽≠a.

ro⊰r∩⌜o

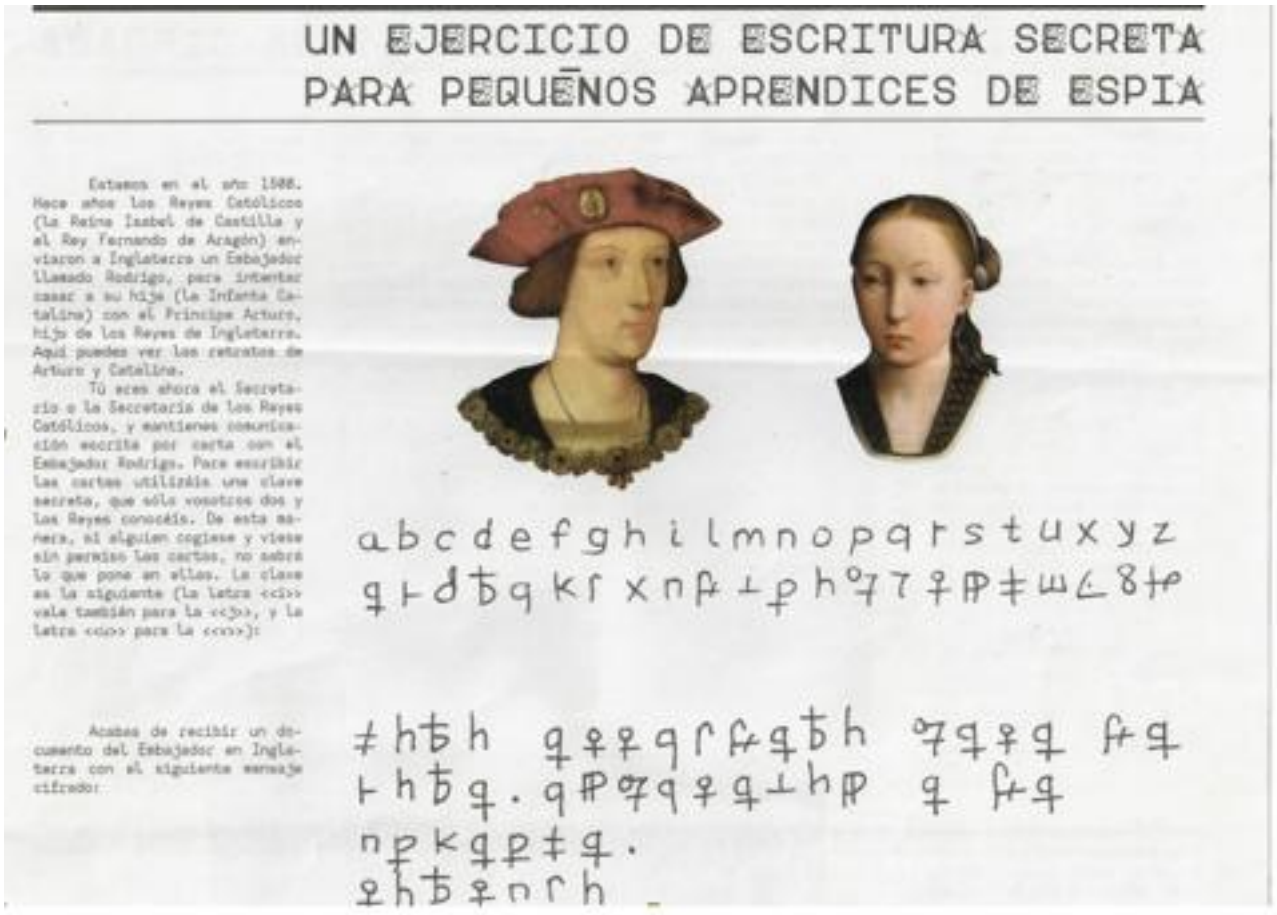
Esto tiene "buena pinta". Otro truco es tratar de averiguar si las palabras son nombres, verbos, preposiciones, artículos, etc. Claramente las dos palabras que van tras el artículo *la* deben ser sustantivos. Y teniendo dos frases, parece claro que debe haber al menos dos verbos, que deben ser los anteriores a las preposiciones. La palabra final, única después de un punto, tiene todo el marchamo de ser un nombre, la persona u organización que firma el mensaje. Vemos claramente ya cuáles son los verbos: la segunda palabra de la primera línea (¿no me digan que no suena a "arreglado"? En el peor de los casos, un participio, luego acaba en *ado*), y la primera de la segunda línea. Simplemente con la idea del participio, tenemos que ⊰ = *d*. Esto convierte el texto en

≠odo arre⌜lado para la ⊢oda.

e₱pera⊥o₱ a la ∩₽ĸa₽≠a.

rodr∩⌜o

Creo que ya lo podrá terminar cualquiera. Es obvio que ≠ = *t*, que ⌜ = *g* (con esto ya sabemos quien firma), y el resto se sigue sin dificultad. Así pues, no es en absoluto necesario incluir la clave en la hoja como han hecho. Aparece así:



UN EJERCICIO DE ESCRITURA SECRETA
PARA PEQUEÑOS APRENDICES DE ESPIA

Estamos en el año 1508. Hace años los Reyes Católicos (la Reina Isabel de Castilla y el Rey Fernando de Aragón) enviaron a Inglaterra un Embajador llamado Rodrigo, para intentar casar a su hija (la Infanta Catalina) con el Príncipe Arturo, hijo de los Reyes de Inglaterra. Aquí puedes ver los retratos de Arturo y Catalina.

Tú eres ahora el Secretario o la Secretaria de los Reyes Católicos, y mantienes comunicación escrita por carta con el Embajador Rodrigo. Para escribir las cartas utilizáis una clave secreta, que sólo vosotros dos y los Reyes conocéis. De esta manera, si alguien cogiese y viese sin permiso las cartas, no sabría lo que pone en ellas. La clave es la siguiente (la letra «i» vale también para la «j», y la letra «u» para la «v»):

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

Acabas de recibir un documento del Embajador en Inglaterra con el siguiente mensaje cifrado: