Península
vol. XIX, núm. 2
julio-diciembre de 2024
pp. 163-178

MARÍA ESTUARDO, LA REINA CRIPTÓGRAFA

Ricardo Mansilla Corona[1]

Resumen

María Estuardo es un controvertido personaje de la historia universal. Cuando sólo tenía seis días de nacida heredó la Corona de su padre Jaime V de Escocia. A la edad de veinticinco años fue obligada a abdicar el trono y huyó a Inglaterra en busca de refugio en la corte de su prima, Isabel I, quien, al percibirla como una amenaza, la mantuvo prisionera por diecinueve años, hasta 1586, cuando fue encontrada culpable de participar en una conspiración en su contra. Durante el periodo de su cautiverio sostuvo un intenso intercambio epistolar con muchas personalidades de la sociedad francesa, española y escocesa, utilizando varios sistemas de encriptación de mensajes muy sofisticados para la época. En este trabajo se analiza el corpus epistolar codificado y su relación con los sucesos que llevaron a su ejecución el 8 de febrero de 1587.

Palabras clave: María Estuardo, criptoanálisis, sir Francis Walsingham.

MARY STUART, THE CRYPTOGRAPHER QUEEN

Abstract

Mary Stuart is a controversial character of universal history. After six days of her birth, inherited the Crown from her father James V of Scotland. At the age of twenty-five, she was forced to abdicate the throne and fled to England to seek for refuge at the court of her cousin Elizabeth I, who, perceiving her as a threat, kept her prisoner for nineteen years, until 1586, when she was found guilty of involvement in a conspiracy against her. During her captivity, she had an intense letter exchange with many personalities from French, Spanish, and Scottish society, using several and very sophisticated message encryption systems for that epoch. This paper analyzes the encoded epistolary corpus and its relation to the events that led to her execution on February 8, 1587.

Keywords: Mary Stuart, cryptanalysis, Sir Francis Walsingham.

[1] Centro Peninsular en Humanidades y Ciencias Sociales (cephcis) / Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades (ceiich), Universidad Nacional Autónoma de México (unam), mansy@unam.mx.

fecha de recepción: 24 de junio de 2023
fecha de aceptación: 27 de noviembre de 2023

Introducción

Fotheringday Castle era una fortaleza normanda, construida alrededor del año 1100 d. C. por Simon de Senlis, conde de Northampton, un noble normando al servicio de Guillermo I. Hasta su destrucción en 1630, fue el escenario de algunos hechos importantes en la historia inglesa, como el nacimiento de Ricardo III en 1452, y el juicio, sentencia y ejecución de María Estuardo. En la mañana del sábado 15 de octubre de 1586, la reina escocesa entró a una sala de justicia, que había sido instalada en este castillo, a enfrentar el cargo de conspiración en contra de la vida de Isabel I, soberana inglesa.

Ésta era una acusación muy peligrosa para la Corona. Ejecutar a María Estuardo podía asentar incómodo precedente: si el Estado británico decidía ejecutar a una reina, eventuales rebeldes podrían tener en el futuro pocos escrúpulos para matar a otra, por ejemplo, a la monarca Isabel I. En esa época, la nación inglesa estaba inmersa en fuertes conflictos entre católicos y protestantes. Por otra parte, muchos cuestionaban si una corte inglesa tenía autoridad para juzgar y condenar a una monarca extranjera. Por último, estaba el vínculo sanguíneo entre ambas mandatarias, lo cual ponía a Isabel I en una posición aún más delicada.[2] Cualquier argumento que se presentara en un juicio en contra de la monarca escocesa debía ser lo suficientemente sólido como para establecer su culpabilidad más allá de cualquier duda razonable.

Ésta era la situación que enfrentaba María Estuardo a la entrada del tribunal, aunque ella tenía la seguridad de que no podría ser implicada en los hechos que se le pretendían imputar. Antes del inicio de su largo cautiverio, en 1568, había comenzado a utilizar técnicas criptográficas para ocultar los mensajes de sus cartas.[3] Estaba convencida de que sus códigos no habían sido descifrados, por lo cual (siempre en su opinión) no podría ser inculpada.

Lamentablemente para María Estuardo, el secretario de Estado de Isabel I, sir Francis Walsingham, además de ser un burócrata que atendía los asuntos de la reina, era un consumado espía. La seguridad de la reina inglesa estaba constantemente bajo la amenaza de enemigos locales y foráneos. Por tal motivo, Walsingham había creado a principio de los años 1570 una genuina escuela de espionaje, desarrollando una red vigilancia en toda Europa continental. La misma estaba constituida por informantes de todo tipo y criptoanalistas reconocidos, como Thomas Phelippes, un lingüista que dominaba el francés, el italiano, el

[2] Los fantasmas de esta decisión persiguieron a Isabel I después de la ejecución de María Estuardo. El Fotheringhay Castle permaneció sin cuidados durante la última parte de su reinado, provocando su deterioro; en 1630, por ejemplo, se cayó la mayor parte de la mampostería y quedaron sólo los montículos que señalan la posición original.

[3] Este proceder tiene su origen en las llamadas *Cartas del ataúd* (Guy 2004, 432; Weir 2008, 464), ocho cartas, sin firma, supuestamente de María Estuardo al conde de Bothwell, las cuales la hacían cómplice de la muerte de Enrique Estuardo. Las cartas originales estaban escritas en francés. A partir de entonces, María Estuardo decidió encriptar toda su correspondencia.

español, el latín y el alemán y que, además, era considerado uno de los mejores criptoanalistas de Europa (Singh 1999, 4). Walsingham recolectó copias de la correspondencia de María Estuardo con los complotados, las cuales fueron decodificadas por Phelippes.[4] Como se sabe, esto selló su destino.

Sin embargo, son poco conocidos los cifrados utilizados por María Estuardo y el complejo proceso de decodificación de éstos. Recientemente han visto la luz cartas no conocidas de la reina escocesa, cuyo estudio comienza a mostrar aspectos hasta ahora ignorados de la conspiración en que se vio involucrada, así como en la riqueza de los códigos criptográficos utilizados (Lasry *et al.* 2023). Esto es un ejemplo paradigmático de la influencia de un hallazgo científico en la comprensión de un suceso histórico. El objetivo de este trabajo es realizar un análisis de los hechos que condujeron a la ejecución de la reina escocesa y el papel de las técnicas criptográficas en el desenlace de éstos.

Dado que es imposible adentrarse en la temática antes referida sin un somero conocimiento de los procedimientos criptográficos, en el siguiente apartado se hace una revisión de los conceptos básicos del criptoanálisis, con el objetivo de establecer el marco teórico a partir del cual se analizará el *corpus* epistolar. La tercera sección contiene los detalles, tanto históricos como técnicos, de todo el proceso de descifrado de las cartas y las consecuencias que esto implicó. Enseguida, se describen los nuevos hallazgos y algunas conclusiones sumarias y, finalmente, se presentan las referencias bibliográficas.

Algoritmos criptográficos y de criptoanálisis

La posibilidad de enviar mensajes que sólo puedan ser leídos por sus destinatarios ha sido el anhelo de reyes, generales y amantes a lo largo de la historia de la humanidad. Todo tipo de ardides (muchos de ellos de gran originalidad) se han utilizado para transmitir información a los destinatarios deseados, de forma segura e inadvertida para curiosos fortuitos, eventuales censores o para enemigos y adversarios.

El procedimiento más elemental ha sido enviar los mensajes ocultos. Según relata Herodoto,[5] en su obra *Las guerras de Persia* (Herodoto 1942), fue Demaratus, quien avisó a los atenienses y espartanos de las intenciones de Jerjes I de invadirlos para castigar su rebeldía. La rivalidad entre griegos y persas había alcanzado un nivel crítico poco después de que Jerjes I decidiera construir la ciudad de Persépolis. Alrededor del 500 a. C.,[6] los tributos llegaban de todas partes del Imperio

[4] En honor a la verdad y sin quitar méritos al talento de Phelippes, en ciertas ocasiones la efectiva máquina de espionaje de Walsingham lograba interceptar las claves del cifrado (Pollen 1922, IV; Guy 2004, 480; Fraser 2015, 691).

[5] Según Cicerón, el Padre de la Historia.

[6] La evidencia arqueológica demuestra que los restos más tempranos de Persépolis datan de 515 a. C.

persa y sus alrededores, con la notable excepción de Atenas y Esparta; por tal motivo, el emperador persa decidió castigarlos. Las intenciones de Jerjes I fueron dichas en presencia de Demaratus en la ciudad de Susa. Este último decidió avisar a los griegos de lo que pretendía el persa. La manera característica de anotar información en aquella época era por medio de tablillas de madera cubiertas de cera. Demaratus quitó la cera de un par de tablillas y escribió su mensaje sobre la madera misma, cubriéndola después con cera de nuevo. Así, los guardias persas que vigilaban los caminos del imperio sólo verían las tablillas vacías, sin generar ninguna suspicacia.

Cuando el mensaje llegó a manos de los griegos nadie fue capaz de adivinar el secreto. Fue Gorgo, esposa de Leónidas, hija de Cleomenes, la que acertó con el mismo, de modo que se descubrieron las intenciones de Jerjes I. Así, el 23 de septiembre de 480 a. C. la flota persa se acercó a la bahía de Salamis a las afueras de Atenas y, para su sorpresa, los griegos la estaban esperando.

Estos procedimientos (muy originales como se ha advertido)[7] de enviar un mensaje escondido se conocen con el nombre de "esteganografía". Recientemente, estas técnicas han recibido un nuevo e inesperado auge por medio de algoritmos de inteligencia artificial (Ornes 2023; Schroeder de Witt *et al.* 2023).

El otro gran grupo de procedimientos algorítmicos para enviar mensajes seguros no se basa en ocultar el mensaje mismo, sino en ocultar su significado. Al conjunto de tales métodos se le conoce como "criptografía".[8] Los métodos criptográficos se dividen en dos grandes grupos: los métodos de transposición y los métodos de sustitución.

El proceso de ocultar el significado de un mensaje (es decir, la utilización de algoritmos criptográficos) se denomina "cifrado". Los métodos dirigidos a descifrar un mensaje encriptado se conocen por el nombre de "criptoanálisis". De esta forma, la criptografía y el criptoanálisis son técnicas con objetivos antagónicos: la primera pretende ocultar el significado del mensaje y la segunda, revelarlo.

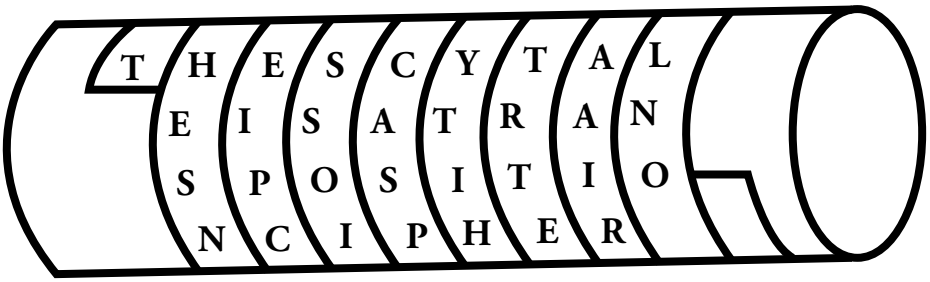
El primer dispositivo criptográfico de la historia fue utilizado con fines militares y se conoce como la "escítala" (figura 1), la cual consistía en un cilindro de madera, alrededor del cual se enrollaba una cinta de cuero. El mensaje se escribía

[7] Otro famoso episodio de escritura oculta en la Antigüedad fue el de Histiaeus de Mileto, coronado como sátrapa de Susa por Darío I, rey de Persia, debido a los notables servicios que aquel le había brindado durante la guerra con los escitas. Darío le pidió que dejara Mileto y se fuera a Susa junto a él como amigo y consejero. Mileto quedaría bajo el control de un sobrino de Histiaeus y su yerno Aristágoras. Sin embargo, según Herodoto, Histiaeus no era feliz viviendo en Susa e hizo planes para volver a Mileto. En 499 a. C., le afeitó la cabeza a un esclavo de gran confianza, le tatuó un mensaje en la cabeza y luego esperó a que su cabello creciera de nuevo. El esclavo fue entonces enviado a Aristágoras, quien fue instruido de afeitar la cabeza del esclavo de nuevo y leer el mensaje, en el cual le decía que se rebelara contra los persas. Cuando Darío se enteró de la revuelta, envió a buscar a Histiaeus, que pretendía no tener conocimiento del asunto, pero pidió ser enviado de regreso a Mileto para poner fin a la revuelta. Herodoto escribe que Darío le permitió marcharse.

[8] Que proviene de la palabra griega χρυπτός que significa escondido.

sobre la cinta, en forma transversal (es decir, en la dirección del eje del cilindro). Cuando se desenvolvía quedaba una colección de caracteres sin orden. La única forma de recuperar el mensaje era volver a enrollar la cinta en un cilindro del mismo diámetro del original.[9]

Figura 1. Una escítala con un mensaje[10]



La escítala es un caso particular del conjunto de procedimientos de cifrado que, como ya se dijo, se conocen como transposiciones. La característica distintiva de este tipo de cifrados es construir, a partir del texto original, una permutación de sus letras. Por ejemplo, para la palabra "hola" se pueden hacer veinticuatro transposiciones distintas:

olah, lhoa, aolh, hloa, ohla, ahlo, aohl, olha, ohal, hlao, laho, laoh, loah, loha, aloh, hola, etcétera.

Nótese que el procedimiento de transposición no es efectivo en mensajes muy cortos pues, como puede verse en el ejemplo anterior, es posible construir todas las permutaciones con facilidad. Sin embargo, "para una frase como esta" (que tiene veinticuatro caracteres incluidos los espacios) existen más de 620 450 000 000 000 000 000 000 transposiciones diferentes.

Uno de los posibles cifrados por transposición de "para una frase como esta" podía ser el siguiente:

o atorp racnsaa u easfme

[9] Lisandro, el Grande, fue el comandante de la flota de Esparta que derrotó a los atenienses en Aegospotami en 405 a. C. Esto obligó al líder ateniense Alcibíades a refugiarse con Farnabazos, sátrapa de Frigia. Al año siguiente Lisandro recibió a cinco soldados espartanos, provenientes de Persia. Uno de ellos le entregó una cinta de cuero en la cual se le informaba que Farnabazos preparaba una expedición en su contra. Gracias a la escítala, Lisandro pudo prepararse y vencer a las fuerzas de Farnabazos.

[10] Las imágenes de este artículo son de libre acceso y están tomadas de Taylor & Francis Online (2023).

para decodificarla, sería necesario conocer la permutación con la cual se cifró el mensaje, que en este caso es:

19 15 8 23 17 11 1 9 3 24 16 7 13 2 4 5 6 20 21 12 22 10 18 14.

Ésta es la desventaja de los métodos de transposición:[11] para que sean funcionales, es indispensable enviar al destinatario de manera segura la permutación precisa con la que se reconstruye el mensaje. Si quisiéramos cifrar los datos de nuestra tarjeta de crédito (número, nombre del titular, vencimiento y dirección postal), deberíamos enviar también la permutación con la que se codificó el mensaje y, esto, sin dudas pondría en riesgo la seguridad de nuestros datos, pues se debería enviar la permutación en otro mensaje (el cual presumiblemente debería cifrarse también).[12]

El otro tipo de métodos criptográficos son los llamados métodos de sustitución, que tienen su primera mención no en la historia de un suceso militar, sino en la más hedonista de las obras literarias: el *Kamasutra*. Compilado por Vātsyāyana entre 400 a. C. y 200 d. C., esta obra literaria contiene, en el capítulo 3, de su primera parte, la lista de las 64 artes que las mujeres deben conocer. En el número 45 de esa lista se encuentra "Mlecchita Vikalapa o el arte de entender la escritura en cifrado y la escritura de palabras de una manera peculiar". Los algoritmos sugeridos en el *Kamasutra* consisten en cifrar los mensajes, sustituyendo cada letra por otra tomando en cuenta consideraciones fonéticas.[13]

Los métodos de sustitución, como su nombre lo indica, consisten en sustituir una letra por otra en el alfabeto o símbolos de otro conjunto, a partir de una clave preestablecida. Por ejemplo, si usamos la clave siguiente:

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

para cifrar la oración "para una frase como esta", el texto codificado sería:[14]

avbv xsv gbvdk cozo kdrv

[11] En realidad, es una deficiencia de todos los métodos criptográficos de clave simétrica.

[12] Una discusión elemental de otros métodos de transposición puede verse en Smith (1943, 29-56) o en Gaines (1956, 9-67).

[13] Si bien el *Kamasutra* no ofrece detalles de los cifrados, algunos estudiosos posteriores de la obra sugieren básicamente tres métodos: Kautilya, Muladeviya y Gudhayojya. Ver, por ejemplo, a Kahn (1996, 74).

[14] Es bueno señalar que, en los procedimientos de cifrado, no es conveniente dejar espacio entre las palabras, ya que esto puede ayudar al criptoanalista en su tarea. Dicho de otro modo, para el ejemplo del texto, se transmitiría el código avbvxsvgbvdkcozokdrv.

El primer uso militar conocido de un algoritmo de sustitución fue por parte de Julio César, en su campaña en las Galias, de los años 58 al 50 a. C. (Julio César 2006).[15] Por la obra de Suetonio (2000), sabemos que la clave de estos algoritmos se construía desplazando las letras del alfabeto latino tres posiciones hacia adelante, sustituyéndolas luego por la letra correspondiente del alfabeto griego.[16] Por ejemplo, si se utilizara en el original y en el mensaje cifrado el mismo alfabeto latino y el orden del desplazamiento es tres, se tendría:

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

Con lo cual "una frase como esta" se cifraría en:

rkxcoxpbzljlbpqx

Sin embargo, los métodos de sustitución tienen un talón de Aquiles cuyo origen se hunde en los inicios de la cultura islámica. Es un hecho aparentemente inocuo, que pudiera clasificarse como una curiosidad lingüística, pero que permite desmantelar la supuesta fortaleza de los cifrados por sustitución: la frecuencia de aparición de las letras en los textos de diferentes idiomas.

Cuentan las escrituras que alrededor de 610 d. C., el arcángel Gabriel visitó a Mahoma en el monte Hira, lugar donde se refugiaba para orar y meditar, cuando aún no era el profeta de la religión islámica. A partir de entonces, y durante los veinte años siguientes, Mahoma estuvo recibiendo revelaciones. Las mismas fueron documentadas de manera fragmentada por diferentes escribas durante la vida del profeta. La tarea de compilar las 114 revelaciones (que constituyen los 114 capítulos del Corán) fue hecha mediante un relevo generacional que comienza con Abu Bark,[17] primer califa del islam, y culmina con Uthman ibn Affan, tercer califa islámico.

[15] En el libro 5, capítulo 48, de Julio César, se lee: "Se indujo a cierto jinete galo a llevar una carta a Cicerón, que se encontraba sitiado por las hordas galas. Esta se envía escrita en caracteres griegos, para evitar que, si la carta era interceptada, nuestras medidas no sean descubiertas por el enemigo. Se le instruye que, si no puede entrar, arroje su lanza con la carta atada a una correa, dentro de las fortificaciones del campamento. En la carta se le suplica a Cicerón que mantenga su antiguo valor, pues las legiones van en su ayuda. El galo arroja su lanza como ha sido instruido. Esta por casualidad se atasca en una torre y no fue observada por nuestros hombres por dos días, fue vista por un soldado al tercer día: cuando fue llevada a Cicerón. Él, después de leerla, lo lee en una asamblea de soldados, y llena a todos de la mayor alegría" (Julio César 2006).

[16] A este tipo de algoritmos de encriptación se les conoce como algoritmos de desplazamiento. Se llama orden del algoritmo al número de desplazamientos con los que se construye el alfabeto codificado.

[17] Abu Bakr Abdallah bin Abi Quḥafah aṣ-Ṣiddiq, 573-634 d. C. Dirigió el califato Rashidun desde 632 hasta 634 d. C., convirtiéndose en el primer califa musulmán después de la muerte de Mahoma.

Los árabes fueron, de hecho, los inventores del criptoanálisis. A partir de 750 d. C., con el inicio del califato de Abbasid, la cultura islámica floreció en el propicio ambiente de la fértil y pacífica sociedad islámica de aquellos tiempos.[18]

Una sociedad con fuertes basamentos religiosos precisa de sólidos centros de investigación teológica que sustenten y expandan su legitimidad. En las ciudades de Bagdad, Basra y Kufa se desarrollaron notables escuelas teológicas. Entre sus tareas más importantes se encontraba el ordenamiento cronológico de las revelaciones del Corán. La técnica usada por estos teólogos era contar la frecuencia con que las palabras aparecían en estas escrituras. Esto estaba sustentado por la idea de que el uso de ciertas palabras había variado a lo largo del tiempo. Si una revelación determinada contenía muchas palabras "jóvenes", implicaba que debió escribirse recientemente.[19] Los teólogos no se quedaron en este nivel de indagación y también estudiaron la frecuencia con que las letras aparecían en los distintos documentos. Descubrieron que ciertas letras son más frecuentes que otras.[20]

El destacado médico, músico, astrónomo, matemático y lingüista árabe al-Kindi[21] publicó, alrededor de 850 d. C., un tratado titulado *Un manuscrito para descifrar mensajes criptográficos*,[22] donde mostraba cómo se podían utilizar las diferentes frecuencias de aparición de las letras para romper cifrados de tipo monoalfabéticos.[23]

[18] Algo que es muy difícil de conciliar con la visión que ofrecen los extremistas islámicos actuales. Es necesario un desarrollo social con cierto nivel de sofisticación para que una técnica como el criptoanálisis florezca, dado que la misma precisa de cierto nivel de erudición en matemáticas, estadística y lingüística. La dinastía Abbasid estaba mucho menos interesada en las conquistas que sus predecesores. Se enfocaron en desarrollar una sociedad culta y próspera, fundaron en Bagdad la Bait al-Hikmah (la Casa de la Sabiduría), que fue un centro sin rival para el estudio de las humanidades y para las ciencias en el islam medieval, incluyendo matemáticas, astronomía, medicina, alquimia y química, zoología, geografía y cartografía. Se dedicaban también, de manera muy intensa, a hacer traducciones al árabe de documentos en otras lenguas. Bajo la égida de los Abbasid se desarrolló un sistema de administración estatal notable para su época. Los servidores públicos protegían los depósitos bancarios y las declaraciones de impuestos del escrutinio de terceros por medio del uso de cifrados monoalfabéticos. Ver, por ejemplo, Súlí (1922).

[19] Aproximadamente 1200 años después, Google retomó esta idea con su gigantesco proyecto Google Ngram Viewer (Google 2023).

[20] Por ejemplo, en árabe las letras *a* y *l* son muy frecuentes dado que el artículo *al* es muy común.

[21] Director, en su momento, de la Casa de la Sabiduría.

[22] El profesor Mohammed Mrayati, un ingeniero e historiador con base en el Líbano, descubrió, en 1987, en el archivo otomano Sulaimaniyyah, en Estambul, la única copia conocida del libro de al-Kindi (1992).

[23] Los cifrados monoalfabéticos son aquellos algoritmos de sustitución donde la clave puede estar compuesta por letras de un solo alfabeto y otros símbolos simultáneamente. El punto básico es que cada letra del alfabeto original se sustituye por un solo símbolo. En el cuento de Edgar Allan Poe "El escarabajo de oro", aparece un mensaje cifrado con una clave monoalfabética (Poe 2008, 377). Como se verá más adelante, María Estuardo utilizó de manera indistinta procedimientos criptográficos monoalfabéticos con ciertas variantes distractoras, que se explicarán en el texto principal.

La frecuencia de aparición de las letras en el idioma español se refleja en la siguiente tabla. Es importante señalar aquí que las frecuencias mostradas son un promedio sobre un gran número de documentos en ese idioma. Por tanto, en algún texto en particular éstas pueden variar, lo cual obviamente ocurre también en otros idiomas.[24]

Letra	Porcentaje	Letra	Porcentaje
E	13.68	P	2.51
A	12.53	B	1.42
O	8.68	G	1.01
S	7,98	V	0.9
R	6.87	Y	0.9
N	6.71	Q	0.88
I	6.25	H	0.7
D	5.86	F	0.69
L	4.97	Z	0.52
C	4.68	J	0.44
T	4.63	X	0.22
U	3.93	W	0.02
M	3.15	K	0.005

El Renacimiento puso de nuevo al ser humano en el centro de la discusión epistemológica, retomando los ideales de la antigüedad. Terminó con la era de oscurantismo religioso, que la larga noche de la Edad Media había tendido sobre Europa. Revivió el desarrollo de las ciencias, las artes y de una concepción inter-

[24] A veces de manera drástica. En 1939, E. V. Wright escribió la novela "Gadsby", un lipograma en lengua inglesa de cincuenta mil palabras, ninguna de las cuales contenía a la letra *e*. En 1969 G. Perec, escribió la novela "La disparition", de doscientas páginas, en ninguna de las cuales se observaba la letra *e*.

disciplinaria de la comprensión del mundo. Las ciudades-Estado, nacidas alrededor del siglo x, se habían desarrollado debido al comercio e intentaban superarse unas a otras en todos los ámbitos. Era, pues, una época propicia para el uso de técnicas criptográficas. Diplomáticos y comerciantes eran intercambiados entre estos pequeños estados, en ocasiones con la sola intención de vigilarse entre sí.

El paso del acervo criptoanalítico musulmán a Europa ocurrió a través de los monasterios, interesados en la búsqueda de mensajes ocultos en la Biblia.[25] Roger Bacon, el erudito monje franciscano publicó su *Epistola de secretis operibus artis et naturae et de nullitate magiae* (Bacon 1859), donde describe varios métodos de cifrar mensajes.

La característica común de todos los procedimientos de cifrado que se inician con la escítala y llegan al Renacimiento (un intervalo de casi mil seiscientos años de la historia de la humanidad) es el uso de claves monoalfabéticas, esto es, el alfabeto original se traduce en una colección de símbolos que pueden ser una permutación del alfabeto inicial u otros símbolos diferentes. Sin embargo, como se verá más adelante, la trágica muerte de María Estuardo lanzó una llamada de alerta a diplomáticos y espías en las cortes europeas, restándole confiabilidad a los métodos de sustitución monoalfabéticos.

Por tanto, los criptógrafos intentaron desarrollar algoritmos de cifrado más herméticos, que permitieran en particular que una letra del alfabeto original se tradujera en varios signos distintos dentro de un mismo mensaje. La construcción de esta nueva familia de algoritmos fue la obra colectiva de un grupo de intelectuales de muy distinta formación que culminó en el trabajo del diplomático francés Blaise de Vigenère ([1586] 2006).[26]

El proceso de María Estuardo

Durante los años que María Estuardo estuvo prisionera se desarrollaron numerosos complots dirigidos a destronar a Isabel I.[27] Estas maquinaciones han sido documentadas en la historia a través del nombre de las figuras más notables en ellas implicadas. Entre las más connotadas se encuentran el complot Ridolfi en 1571, el complot Throckmorton en 1583 y el complot Babington en 1586. En este último, María Estuardo se involucró decisivamente.

[25] Una fascinación que aparentemente no se ha mitigado aún. Ver, por ejemplo, Drosnin (1997).

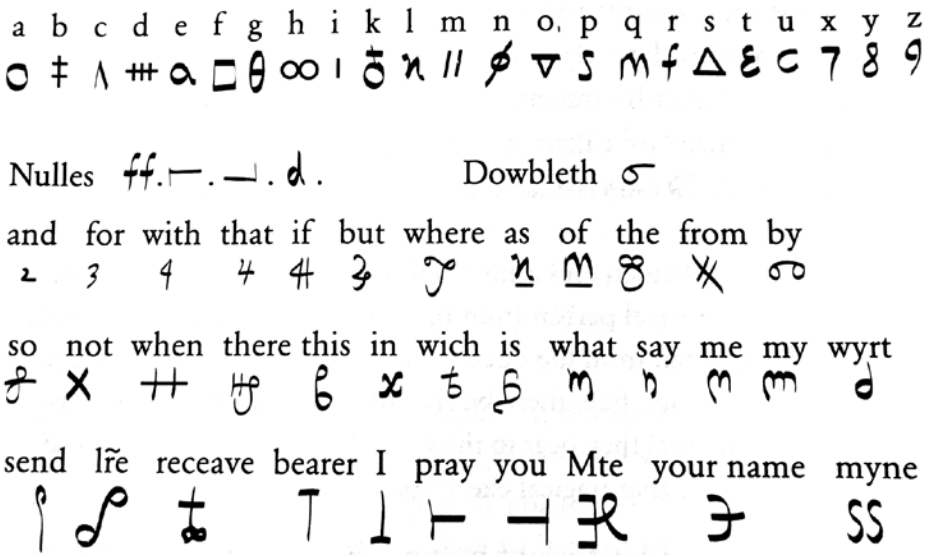
[26] La primera etapa de esta construcción es debida al erudito florentino León Battista Alberti, quien, a mediados del siglo xv, fue introducido al tema de la criptografía por el secretario pontificio de aquel entonces, Leonardo Dato. Alberti construyó una versión mínima de un algoritmo de cifrado multialfabético. En él se usaban dos permutaciones de alfabetos simultáneamente, eligiéndose alternadamente. Este trabajo fue refinado y extendido por el abad alemán Johannes Trithemius y el científico italiano Giambattista della Porta. La versión final quedó en manos de Vigerène.

[27] El papa Pío V, en su bula *Regnans in Excelsis* de 1570, excomulgó a la protestante Isabel I y permitió que todos los fieles católicos hicieran todo lo posible para deponerla (Dures 1983, 17).

El 6 de enero de 1586, María Estuardo recibió un grupo de cartas de sus partidarios en Francia. Habían sido introducidas en Charteley Hall (sitio donde permanecía prisionera) por Gilbert Gifford, un cura católico afín a la embajada francesa en Londres. La forma de ocultarlas de los celadores fue dentro de la tapa de un barril de cerveza.[28]

Mas adelante, el 6 de julio de 1586, Gifford se presentó en la morada de Babington. Le traía una carta de María Estuardo, donde le comentaba que estaba interesada en conocer los detalles de la conjura que organizaba. Babington le contestó de inmediato, explicándole los detalles, entre los cuales se encontraba el asesinato de Isabel I (Singh 1999, 36-38).[29]

Figura 2. Detalles del código usado por Babington en su carta a María Estuardo



La carta no fue encriptada a través de un código monoalfabético, sino por medio de un *nomenclador*, esto es, un tipo de cifrado por sustitución que permutaba las letras por símbolos de diferente origen, que agregaba además los llamados "nulos", símbolos que no tienen ningún significado y ciertos símbolos que significaban palabras o frases completas. En la figura 2 se muestran los detalles de este código.

Para el infortunio de Anthony Babington y María Estuardo, Gifford era un agente doble, que entregaba todas las esquelas a Walsingham antes de llevarla a

[28] Este es, obviamente, un procedimiento esteganográfico.

[29] El plan consistía en la liberación de María Estuardo, el asesinato de Isabel I y una invasión desde Francia con tropas católicas leales.

sus verdaderos destinatarios. De esta carta se hizo una copia que se le envió al criptoanalista Phelippes. A pesar de la complejidad del código, este fue capaz de descifrarlo.[30] En el texto descifrado se podía leer la frase *el despacho de la Competidora usurpadora* en franca referencia a Isabel I. Esto selló el destino de Anthony Babington, pero en ninguna medida inculpaba aún a María Estuardo. Sin embargo, el 17 de julio de 1586, María Estuardo comunicó (con la oposición de sus asistentes) a Babington su aprobación para llevar adelante todo el plan, con lo cual firmó su sentencia de muerte.

Walsingham le pidió además a Phelippes (quien era también un hábil falsificador) que agregara un párrafo (cifrado con el código que él mismo recién había descifrado) en la carta de María a Babington donde, supuestamente, la reina escocesa se interesaba por "la identidad del resto de los conspiradores". Babington accedió, y en la siguiente misiva dirigida a María Estuardo (que también cayó en manos de Walsignham) le compartía los nombres de los complotados.[31] Con esto, la conjura quedó completamente desarticulada, pues todos sus miembros fueron detenidos y la participación de María Estuardo quedaba completamente al descubierto.

Nuevos hallazgos

La enorme hazaña de Thomas Phelippes como criptoanalista ha sido objetada con frecuencia, basado en ciertas evidencias circunstanciales que sugerían o documentaban el conocimiento de las claves de codificación (Pollen 1922, IV; Guy 2004, 480; Fraser 2015, 691). Por otra parte, es sabido que para el desciframiento de la correspondencia entre Babington y María Estuardo sólo se valió de la frecuencia relativa de aparición de los diferentes caracteres en el mensaje cifrado, y un largo y tortuoso proceso de prueba y ensayo (Singh 1999, 40).

Donde quiera que haya sido necesario realizar un trabajo intelectual repetitivo y tedioso, el poder de las computadoras digitales ha venido en nuestro auxilio. La enorme capacidad de cálculo y de almacenamiento de datos de las actuales computadoras digitales, ha sido crucial en la puesta a punto de algoritmos capaces de jugar ajedrez y GO con una maestría suficiente para ganarle a los mejores jugadores a nivel mundial (Hassabis 2017; Silver *et al.* 2017).

Recientemente, un trío de criptoanalistas (Lasry *et al.* 2023) ha logrado decodificar 57 de las cartas escritas por María Estuardo, entre 1578 y 1584, a Michel

[30] La herramienta básica utilizada por Phelippes fue la frecuencia de aparición de las letras en el idioma inglés y la frecuencia de aparición de los símbolos en la carta encriptada (Singh 1999, 40).

[31] El uso de un sello de lacre era el procedimiento estándar en aquella época para cerrar las cartas. Para evitar la apertura adúltera de la correspondencia se le agregaba a los ingredientes habituales de la mezcla (pasta a base de colofonia, goma laca y trementina, además de bermellón u otro color mineral) una porción de extracto de belladona, cuyos vapores (se suponía) tenían la propiedad de dilatar la pupila por intervalos largos de tiempo. A partir de esto, era frecuente que, en el momento de la entrega de la correspondencia, se les hiciera un examen ocular a los portadores. En la novela *Rule of Four* de I. Caldwell y D. Thomason, por ejemplo, se describe con detalle el procedimiento.

de Castelnau, el embajador de Francia en Inglaterra, que permanecían sin descifrar en la Biblioteca Nacional de Francia. La correspondencia se encontró dentro de un atado de notas. Con anterioridad se pensaba que estas cartas en su mayoría estaban perdidas, pues sólo se conocía siete de ellas.

La técnica utilizada por los criptoanalistas es un magnifico ejemplo de investigación interdisciplinaria: un algoritmo de optimización matemática basado en un principio de la termodinámica aplicado a la resolución de un problema lingüístico.

El recocido simulado (*Simulated Annealing*) es una técnica de obtención de los valores máximos o mínimos de una función de varias variables independientes muy efectiva cuando el espacio de búsqueda es muy grande. Este procedimiento está inspirado en el proceso termodinámico homónimo, que consiste en mover la temperatura de las piezas en proceso de fundición de forma oscilatoria, con el objetivo de lograr una mayor pureza del producto final. Ha sido utilizado con mucho éxito para resolver el *problema del viajante* (Kirkpatrick 1983).

Los detalles técnicos del procedimiento utilizado por los criptoanalistas (Lasry *et al.* 2023) se escapan por mucho del alcance de esta publicación, pero, a grandes rasgos pueden sintetizarse como sigue:

1. Construir las frecuencias relativas de todos los 5-gramas (conjunto de cinco letras) que aparecen en un *corpus* de textos en francés de los siglos XVI y XVII.[32]
2. Elegir una clave al azar como la que aparece en la primera fila de la figura 2.
3. Contar el número de ocurrencias de cada uno de los 5-gramas en el texto descifrado con la clave elegida al azar.
4. Contar el número de ocurrencias de cada letra en el texto descifrado con la clave elegida al azar.
5. La función de *score* para la clave tentativa era:

$$S = \sum_g N_g \log \left[\frac{F_g}{\sum_c N_c^2} \right]$$

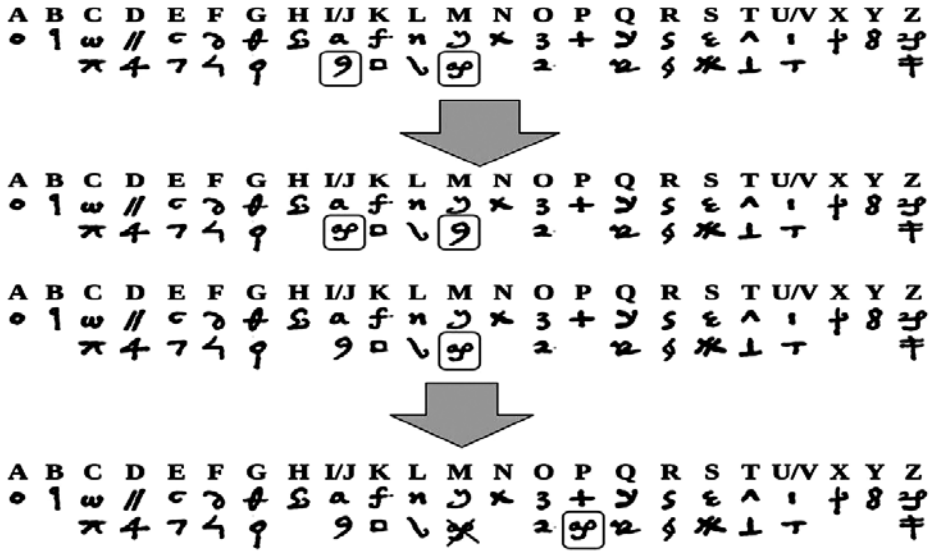
Como se sabe, el método de recocido simulado opera haciendo cambios al azar en la clave tentativa y aceptando el cambio si la función de *score* aumenta. Algunos ejemplos de los cambios posibles se muestran en la figura 3. Es necesario resaltar que el uso del método de recocido simulado sólo es posible gracias a la enorme capacidad de cálculo de las actuales computadoras digitales.

Los resultados antes descritos ponen en una nueva perspectiva los hallazgos hechos por Thomas Phelippes en su trabajo como criptoanalista. Muestran, además, la posibilidad del uso de las computadoras digitales para el criptoanálisis de

[32] Los autores de (Lasry *et al.* 2023) utilizaron varios textos en francés del proyecto Gutenberg.

grandes *corpus* literarios escritos, como el *Manuscrito de Voynich* (Clemens 2016). Por último, abre una interesante posibilidad de usar las técnicas referidas en Lasry *et al.* (2023) para el estudio de los conjuntos de grafemas mayas (Ershova 2013, 221-229).

Figura 3. Ejemplos de modificaciones utilizadas por el algoritmo de recocido simulado



Referencias

Bacon, Roger. 1859. "Opera quaedam hactenus inedita, vol. I: opus tertium, opus minus". En *Compendium philosophae*, edición de J. Brewer. S. l.: Longman-Green & Roberts.

Clemens, Raymond. 2016. *The Voynich Manuscript*. Londres: Beinecke Rare Books-Manuscript Library.

Drosnin, Michael. 1997. *The Bible Code*. Nueva York: Touchstone.

Dures, Alan. 1983. *English Catholicism, 1558-1642: Continuity and Change*. Essex: Longman.

Ershova, Galina. 2013. *Epigrafía maya. Introducción al método de Yuri Knorosov*. Ciudad Guatemala: cemyk.

Fraser, Antonia. 2015. *Mary Queen of Scots*. Londres: Weidenfeld & Nicolson.

Gaines, Helen. 1956. *Cryptanalysis*. Nueva York: Dover.

Google. 2023. Book Ngram Viewer. Consultado el 5 de diciembre. https://books.google.com/ngrams.

Guy, John. 2004. *"My Heart is my Own": The Life of Mary Queen of Scots*. Londres: Fourth Estate.

Hassabis, Demis. 2017. "Artificial Intelligence: Chess Match of the Century". *Nature*, 544: 413-414.

Herodoto. 1942. *The Persian Wars*, traducción de G. Rawlinson. Londres: The Modern Library-Random House.

Julio César. 2006. *Gallic Wars (a partir de los Bello Gallicum, 50 a. C.)*. S. l.: Dover, 23-24.

Kahn, David. 1996. *The Codebreakers*. Nueva York: Simon and Schuster.

Kirkpatrick, Donald *et al.* 1983. "Optimization by Simulated Annealing". *Science* 220 (4598): 671-680.

Kindi al, Ibraham A. 1992. "The Origins of Cryptology: The Arab Contributions". *Cryptologia* 16 (2): 97-126.

Lasry, George *et al.* 2023. "Deciphering Mary Stuart's Lost Letters from 1578-1584". *Cryptologia* 47 (2): 101-202. Consultado el 8 de febrero de 2024. https://doi.org/10.1080/01611194.2022.2160677

Ornes, Stephen. 2023. "Secret Messages Can Hide in AI-Generated Media". *Quanta Magazine*. Consultado el 18 de mayo de 2023. https://www.quantamagazine.org/secret-messages-can-hide-in-ai-generated-media-20230518.

Poe, Edgar Allan. 2008. *Cuentos completos*. Madrid: Páginas de Espuma.

Pollen, John Hungerford. 1922. *Mary Queen of Scots and the Babington Plot*. Edimburgo: Edinburgh University Press.

Suetonio. 2000. *Lives of the Caesars*. Traducción de Catharine Edwards. Oxford: Oxford University Press.

Silver, David *et al.* 2017. "Mastering the Game of Go without Human Knowledge". *Nature* 550: 354-359.

Schroeder de Witt, Christian *et al.* 2023. "Perfectly Secure Steganography Using Minimum Entropy Coupling". Consultado el 18 de mayo de 2023. https://arxiv.org/pdf/2210.14889.pdf.

Singh, Simon. 1999. *The Code Book*. Nueva York: Anchor Books.

Smith, Laurence Dwight. 1943. *Cryptography, the science of secret writing*. Nueva York: Dover.

Súlí, Muhammad ibn Yahyá. 1922. *Adab al-Kutták*. S.l.: Al-Daira al-Matbáah al-Salfiyah.

Taylor & Francis Online. 2023. Consultado el 1 de diciembre de 2023. https://www.tandfonline.com.

Vigenère, Blais de. [1586] 2006. *Traicte des chiffres, ou secretes manieres d'escrire*. París: Hachette bnf.

Weir, Alison. 2008. *Mary, Queen of Scots and the Murder of Lord Darnley*. Londres: Random House.