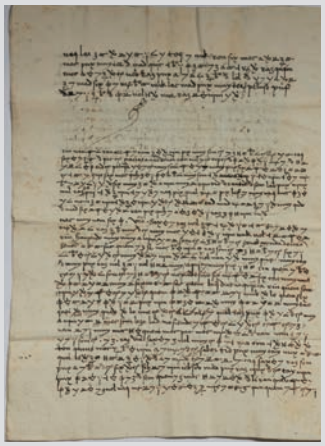
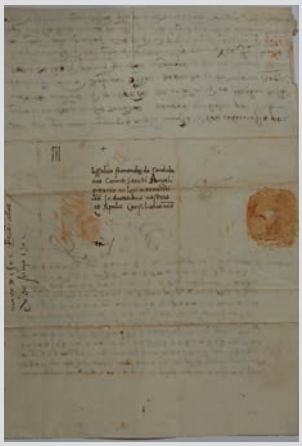
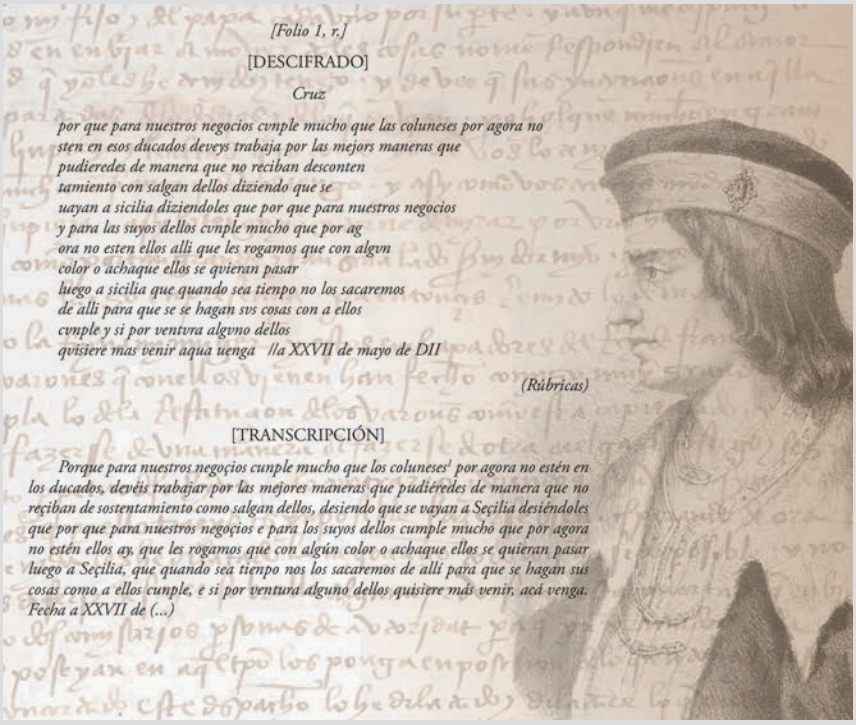




Colección particular Duques de Maqueda

Colección particular Duques de Maqueda



[Folio 1, r.]

[DESCIFRADO]

Cruz

por que para nuestros negocios cvnple mucho que las coluneses por agora no
sten en esos ducados deveys trabaja por las mejors maneras que
pudieredes de manera que no reciban desconten
tamiento con salgan dellos diziendo que se
uayan a sicilia diziendoles que por que para nuestros negocios
y para las suyos dellos cvnple mucho que por ag
ora no esten ellos alli que les rogamos que con algvn
color o achaque ellos se qvieran pasar
luego a sicilia que quando sea tienpo no los sacaremos
de alli para que se se hagan svs cosas con a ellos
cvnple y si por ventvra algvno dellos
qvisiere mas venir aqua uenga //a XXVII de mayo de DII

(Rúbricas)

[TRANSCRIPCIÓN]

Porque para nuestros negocios cunple mucho que los coluneses[1] por agora no estén en los ducados, devéis trabajar por las mejores maneras que pudiéredes de manera que no reciban de sostentamiento como salgan dellos, desiendo que se vayan a Seçilia desiéndoles que por que para nuestros negocios e para los suyos dellos cumple mucho que por agora no estén ellos ay, que les rogamos que con algún color o achaque ellos se quieran pasar luego a Seçilia, que quando sea tienpo nos los sacaremos de allí para que se hagan sus cosas como a ellos cunple, e si por ventura alguno dellos quisiere más venir, acá venga. Fecha a XXVII de (...)

Ministerio de Defensa

En 2015, los duques de Maqueda cedían unas cartas cifradas entre el *Gran Capitán* y Fernando *el Católico* a una exposición en el Museo del Ejército. El Centro Nacional de Inteligencia desentrañó su contenido, que después publicó Defensa con transcripciones (derecha).

[cultura]

CRIPTOGRAFÍA

Del *Gran Capitán* a la MÁQUINA ENIGMA

Cambios de letras, sustituciones alfanuméricas, palabras clave... eran elementos básicos de los mensajes cifrados

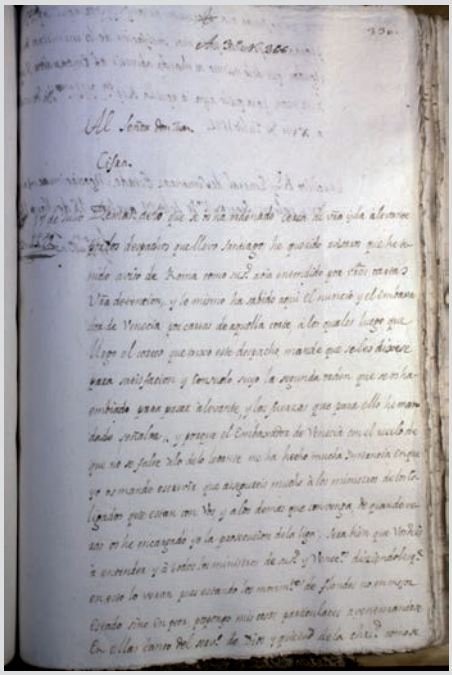
LA Real Academia Española (RAE) indica que la criptografía es el arte de escribir con clave secreta o de un modo enigmático. Son infinidad las técnicas y métodos que se han utilizado para cifrar la información a lo largo de la historia, particularmente en los conflictos armados, donde la necesidad de buscar formas de comunicación seguras cobra una importancia esencial.

El primer sistema criptográfico del que se tiene constancia es la escítala y era usado en Esparta. Su utilización se describe en *Los Nueve libros de la historia* del griego Herodoto (siglo V a. C.) donde se da cuenta de otras técnicas ancestrales para la transmisión oculta de un mensaje. El romano Julio César también utilizó la cifra para transmitir órdenes a sus generales.

La España de los Reyes Católicos es el marco histórico del que parten los documentos cifrados que se recogen en las páginas siguientes, aunque no sean los primeros mensajes encriptados hispanos conocidos. Se trata de cuatro cartas que reflejan un singular ejemplo de la correspondencia entre los monarcas y su lugarteniente Gonzalo Fernández de Córdoba, el *Gran Capitán*, y se pueden consultar en la Biblioteca Virtual de Defensa (www.bibliotecavirtualdefensa.es).

Principalmente, son misivas de Fernando *el Católico* a su jefe militar, enviadas entre el 27 de mayo de 1502 y el 4 de abril de 1506 durante las campañas de Italia, y constituyen un «fondo documental de gran importancia», se subraya en la biblioteca *on line* de Defensa, que, además, tiene dedicado un micrositio específico a esta colección.

Hélène Gicquel



Archivo del Museo Naval

Máquina *Enigma* del Museo Militar de Burgos. A la derecha, misiva cifrada de Felipe II a don Juan de Austria.

El contenido de algunas de estas cartas, como la fechada el 27 de mayo de 1502, en la que el monarca aragonés se dirige a su jefe militar por su título de I duque de Santángelo, no hace tanto que se conoce.

RESUELTAS POR EL CNI

El departamento de Criptología del Centro Nacional de Inteligencia (CNI) desveló su significado hace dos años y ahora se puede consultar en la biblioteca virtual junto a la imagen de cada carta, su descripción, transcripción y un breve comentario.

En el caso de la carta antes apuntada, por ejemplo, la especialista Laura Camino destaca cómo Fernando *el Católico* habla del «delicado equilibrio y juego de alianzas del enfrentamiento italiano» y el cambio experimentado por los miembros de la poderosa familia Colonna, a favor de su causa. Esto, según indica Camino, «explica la cautela del rey aragonés al transmitir al *Gran Capitán* la estrategia que debía llevar a cabo con los coluneses y, justificaría el uso de la escritura cifrada para mantener en secreto una información tan comprometida».

La investigación llevada a cabo por el CNI, en la que tuvo un papel importante la paleografía, surgió a partir de la exposición que en 2015 organizó el Museo del Ejército con motivo del V centenario de la muerte del *Gran Capitán*.

Entonces, de su colección particular, los duques de Maqueda cedieron las mencionadas misivas a la muestra, cuyo catálogo contiene más información y también está disponible en la Biblioteca Virtual de Defensa.

La correspondencia del soberano y su lugarteniente, que —asimismo y entre otras responsabilidades— ejerció funciones diplomáticas para la Corona, deja ver el uso habitual de los mensajes cifrados para manejar «información discreta» sobre cortes extranjeras.

Entonces, el «sistema de inteligencia» más extendido situaba al rey en la cúspide de una pirámide, donde sus ministros, jefes militares, gobernadores, embajadores... constituían el escalón inmediatamente inferior, a partir del cual, la red se ramificaba.

Hélène Gicquel

Para impedir el acceso a información valiosa en la conexión con América se usó esta caja de caudales de cerradura camuflada.

REINADO DE FELIPE II

El modelo estuvo largo tiempo en vigor. De hecho, Carlos I y Felipe II lo utilizaron. Pero, además, el nieto de los Reyes Católicos, apodado el *rey prudente*, dio un nuevo impulso a la criptología española con nuevos modelos de cifra y relevos periódicos de sus claves entre otros aspectos.

Así, en su trabajo *La Criptología Española hasta el final de la Guerra Civil*, el especialista José Ramón Soler destaca que, «uno de los primeros actos de Felipe II como soberano, fue el de cambiar la clave empleada por su padre al considerarla insegura».

Y, por su parte, el estudio de la Universidad de Castilla-La Mancha *Introducción a la Criptología. Historia y actualidad* (2006) asegura que «es, precisamente, durante el reinado de Felipe II, cuando más se ha utilizado la criptografía en nuestro país».

El propio monarca habla del mencionado cambio de cifrado en una carta a su tío Fernando, emperador de Austria,

Sobre los mensajes secretos

EL curioso mundo de los escritos cifrados viene de antiguo. Así lo cuenta el especialista José Ramón Soler en su trabajo *La Criptología española hasta el final de la Guerra Fría*, que se puede consultar en la biblioteca del Museo del Ejército (www.museo.ejercito.es), en Toledo, uno de los lugares posibles para acercarse a este sigiloso ámbito.

La institución también es depositaria, por ejemplo, de correspondencia cifrada entre el *Gran Capitán* y Fernando *el Católico*, conserva una máquina de cifrar *Clave Norte* (siglo XX) y, en sus salas, exhibe una de las singulares *Enigma* alemanas, de la que ofrece un montaje interactivo.

Asimismo, reservan espacios propios a la criptografía otros museos militares, como los de Burgos —partícipe en el estudio *Proyecto Enigma*, con la universidad de la ciudad—, Cartagena o Sevilla. Precisamente, la máquina germana de este último participó en mayo en la *MuseumWeek* 2020.

Los archivos General Militar de Madrid y del madrileño Museo Naval atesoran, por su parte y entre otros textos, documentos cifrados con la firma de Felipe II, soberano —representado en el cuadro de la derecha— que mejoró el sistema de cifra español en su época, y relacionados con las Américas hasta finales del siglo XIX.

Universidad de Burgos/MHM Burgos


Wikipedia/Dominio Público


Museo del Ejército

BIBLIOTECA VIRTUAL

De 1892, la Biblioteca Central Militar (Madrid) conserva el libro *Clave silábica para comunicarse en lenguaje cifrado (…)*, de J.G. Carmona, disponible, además, en la Biblioteca Virtual de Defensa (www.bibliotecavirtualdefensa.es). Dicho repositorio tiene espacio, asimismo, para la ya citada correspondencia del *Gran Capitán* y la *Enigma* del Museo del Ejército, así como para el criptógrafo *Clave Norte/Clave San Carlos*, del Museo de Aeronáutica y Astronáutica, entre otros objetos digitales.

Una referencia más a la ahora de acercarse a este mundo es la Biblioteca Centro de Documentación de Defensa, que dispone de varias publicaciones sobre la materia. El Centro Nacional de Inteligencia recoge en su web (www.cni.es) datos básicos de su devenir y antecedentes, y el Archivo General de Simancas (Valladolid) mantiene en su página virtual amplia información sobre su exposición *Espías: servicios secretos y escritura cifrada en la Monarquía hispánica*, ya cerrada en sala. Incluso, la Fundación *Telefónica* dedicó una muestra a la *Enigma* en 2018, cita aún presente en el epígrafe «Exposiciones pasadas» de su web.

Por último, sobre el legendario *Manuscrito Voynich* del siglo XV —segunda imagen de la serie a la derecha—, el mundo virtual ofrece mil y una referencias, como la del Instituto Geográfico Nacional (www.ign.es). Este centro conserva un facsímil de —según sus propias notas bibliográficas— «el libro más misterioso del mundo».

con fecha del 24 de mayo de 1556, solo unos meses después de haber ascendido al trono (enero, 1556). En ella, Felipe II califica la cifra de Carlos I de «antigua» y «harto divulgada», por lo que no sirve «al buen éxito de los negocios».

Dentro del organigrama de su gobierno, el Despacho Universal, fue el centro neurálgico de comunicaciones y cifras. El máximo responsable era el secretario de Estado, otra de las piezas clave del segundo escalafón de la pirámide antes apuntada. El primer jefe de la oficina durante el reinado de Felipe II fue Gonzalo Pérez, pero a quien la historia recuerda más, por las circunstancias de su cese, condenado por traición a la Corona, es a su hijo, Antonio Pérez.

CÓDIGOS ESPECÍFICOS

La preocupación de Felipe II por la seguridad en este ámbito se tradujo en dos clases de cifras para sus diplomáticos en tierras extranjeras. La «general u ordinaria» estaba reservada a la comunicación del rey con sus representantes en cortes extranjeras y otra de carácter extraordinario y particular, que era para intercambios individualizados con estos, gobernadores, jefes militares... y hombres de confianza.

La conexión con América y otros territorios de ultramar disponía de su código propio y, todos, eran renovados con una frecuencia de entre tres y cuatro años. Ese plazo, que hoy puede parecer inútil por ser demasiado amplio, entonces había quien, como el gobernador de Cuba en 1591, lo debía considerar hasta demasiado breve.

A finales del siglo XVI, este se empeñaba en mantener la muy poca segura «sustitución simple», mientras que en el conjunto de la Monarquía hispánica se usaban nomencladores, homófonos —términos que suena igual con distinto significado y, a veces, grafía diferente—, caracteres nulos, codificación de diagramas, trigramas, repertorio de las palabras más comunes, etcétera.

A pesar de todos sus desvelos y la alta calidad del sistema, el matemático galo Viète logró romper el código ante la incredulidad del propio soberano.

Cuentan que, dada la fe que tenía en su sistema, atribuyó el éxito del científico francés a un pacto con el diablo, por

lo que pidió su apresamiento al Vaticano. El papado desoyó la causa, pero de haberla atendido, Roma hubiera tenido a buen recaudo a un peligroso enemigo para los intereses de la monarquía hispana, verdadera razón de la solicitud.

Aunque el Archivo General de Simancas (Valladolid) es una fuente principal de referencia en este asunto, el patrimonio documental del Ministerio de Defensa conserva más de una carta cifrada de esta época, alguna, incluso firmada por el propio Felipe II. Estas representan una singular muestra de ese cifrado específico e individualizado según el interlocutor y el tema abordado.

A DON JUAN DE AUSTRIA

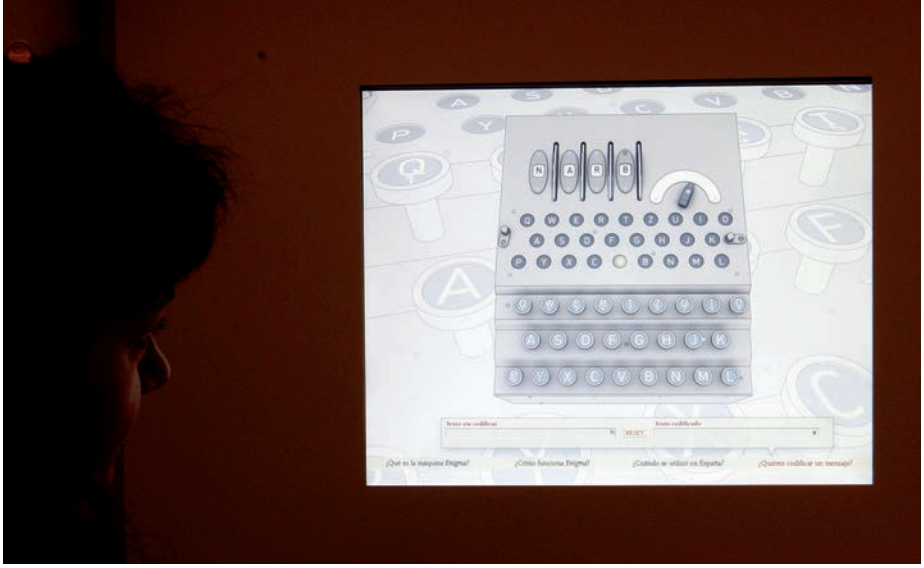
Por ejemplo, el Archivo del Museo Naval de Madrid (AMN) atesora cartas para su afamado general y hermanastro Juan de Austria, con instrucciones muy determinadas, como en la que le dice que «pase a levante para satisfacer los deseos del Papa y de los venecianos», de 4 de julio de 1572. El propio Austria lideró la fuerza cristiana combinada que había vencido meses atrás al imperio turco en Lepanto.

Otra de estas misivas, firmada al mes siguiente, le señala que una parte de su armada debe quedarse en Mesina (Italia) a cargo de Juan Andrea Doria en previsión de un ataque enemigo.

Pero Felipe II, también usó este tipo de correspondencia para, «entre otras cosas, darse por enterado de la llegada a Génova de los príncipes, sus sobrinos, y de su hermano». La carta, en esta ocasión, va dirigida a Luis de Requesens, comendador mayor de Castilla, con fecha de septiembre de 1571.

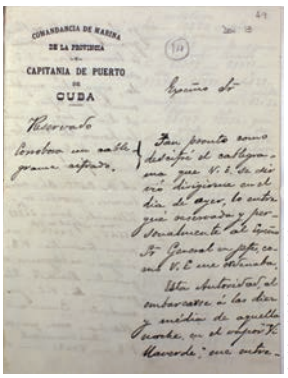
También son numerosos los legajos y documentos que sobre esta materia se pueden hallar en el Archivo General Militar de Madrid (AGMM), entre los que no faltan algunos firmados de la época de los Austria, explican desde el propio centro, con sede en el Cuartel *Infante don Juan*.

Destaca, por ejemplo, el que envía Felipe II a sus embajadores en Italia (1594) para justificar el cambio de cifra: «por avisos ciertos es savido que haviendo caido en manos de herejes algunos despachos mios escritos en la cifra general que se os embio ultimamente.

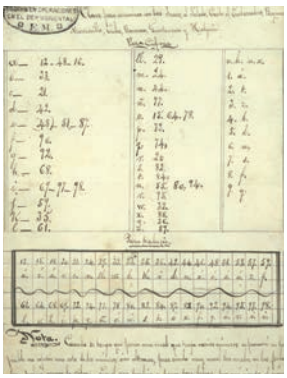


Hélène Gicquel

Arriba, panel interactivo sobre la forma de crear un mensaje en una máquina *Enigma* (Museo del Ejército). A la derecha, documentos sobre el cifrado empleado en la Cuba de finales del XIX.



Archivo del Museo Naval



Archivo General Militar de Madrid

Museo de Aeronáutica y Astronáutica/Biblioteca Virtual de Defensa

Criptógrafo tipo *Clave Norte/Clave San Carlos*, versión española de la máquina *Wheatstone*, que empleó la Aviación en el siglo XX, con carta de código y estuche.

Los archivos del Museo Naval y General Militar de Madrid guardan cartas cifradas del rey Felipe II

Los han descifrado y no se dexa de sospechar, que lo ayan hecho con el mismo abecedario en la mano. Por esto es querido embiaros de nuevo la cifra (...)».

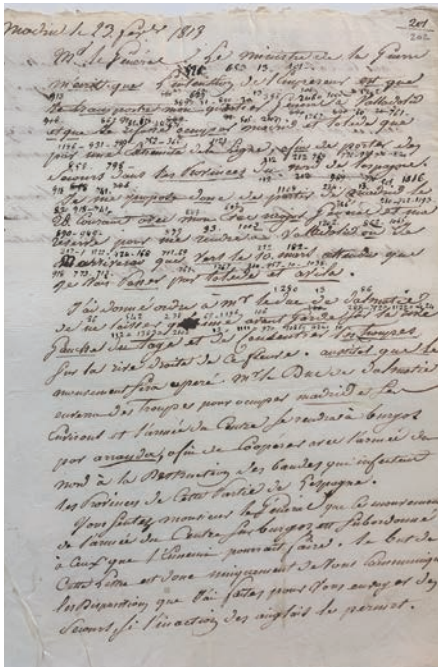
Como ya se ha mencionado, los territorios americanos y de ultramar formaron parte de la red de códigos secretos de la Corona, de lo que se tienen testimonios escritos, como el «Real despacho al marqués de Villarrubia, capitán general de la Armada de Indias, comunicándole la remisión de la cifra particular que ha de usar para avisar de los asuntos reservados de su viaje». Datado en 1658, se conserva en el Archivo Militar Naval.

El celo por mantener bienes e información a salvo también se aplicó a algunos objetos, por ejemplo, la caja de caudales que atesora el Museo Histórico Militar de Sevilla, dotada de una cerradura oculta, tan «invulnerable» como los mensajes encriptados.

VERSIONES MEJORADAS

Las actualizaciones de los sistemas criptográficos continuaron. Hubo sustitución de claves en 1664, 1675 y 1770, época por la que vio la luz el *Tratado de criptografía de 83 hojas de la Secretaría de Estado española,* «una pequeña joya», en palabras de José R. Soler.

A mediados del siglo XVIII, en época de Fernando VI, España mantenía el empleo de libros de códigos. A finales de la centuria se puso de moda el cifrado mediante «el uso de un libro común». Este



Archivo General Militar de Madrid

Carta en clave de José I, en la que deja Madrid por orden de Napoleón.

requiere que emisor y receptor cuenten con idéntica edición del título en cuestión, ya que todos sus elementos son necesarios para elaborar la transmisión.

El XIX irrumpió con el ascenso de Napoleón y su expansión por la vieja Europa, lo que afectó a todos sus sistemas de cifrado. De 1813, el AGMM conserva un texto «oculto» sobre la partida de José I Bonaparte de Madrid siguiendo las órdenes de su hermano el emperador francés.

Ya a mediados de siglo, el telégrafo supondrá un salto cualitativo en el mundo de la criptología que, en apenas unas décadas, va a conocer una de sus estrellas más rutilantes y codiciadas: la máquina de cifrado *Enigma*. No es la única, también está, por ejemplo, la *Clave Norte*, pero es la más famosa.

LA MÁQUINA *ENIGMA*

El proyecto del ingenio de rotores que revolucionará el mundo de los mensajes cifrados fue concebido por A. Scherbius y E.R. Ritter en 1918 y su primer modelo comercial llegó cinco años después. Se presentó en varias ferias internacionales, surgieron nuevos modelos y estuvo a la venta hasta 1934, año de la llegada al poder del nazismo.

Enigma hacía uso de partes mecánicas y eléctricas, era un mecanismo de cifrado rotatorio. La capacidad para cifrar y descifrar mensajes convertiría a la máquina en una pieza clave de la II Guerra Mundial. Al parecer, su modelo *K* llegó a España por recomendación alemana al ejército del general Franco, cuenta el estudio *Proyecto Enigma*, fruto de la colaboración de la Universidad de Burgos y el museo militar de la capital castellana. Se conservan varios ejemplares de esta versión, y la mencionada investigación recoge un sinfín de curiosidades. Por ejemplo, que podía generar hasta 1.800 millones de combinaciones distintas de cifrado en un tiempo, entonces, récord.

Esther P. Martínez

Glosario de criptología

IGUAL que cualquier otra ciencia, «el estudio de la ocultación, disimulación o cifrado de información, así como el diseño de sistemas que realicen dichas funciones, e inversamente la obtención de la información protegida» —es decir, la criptología—, emplea un vocabulario con voces propias y que recoge, entre otras publicaciones, el *Glosario de términos de criptología* (3ª edición, de 1997).

Se trata de un trabajo elaborado por el entonces Centro Superior de Información de la Defensa, editado por MDE y disponible para su consulta en la Biblioteca Centro de Documentación del Ministerio de Defensa. Incluye palabras, como las siguientes:

- **Certeza** (*assurance*, en inglés): seguridad de que un sistema alcanza los objetivos de seguridad para los que ha sido diseñado.
- **Cifra**: transformación de una información (texto claro) en otra ininteligible (texto cifrado) según un procedimiento y usando una clave determinados, que pretende que solo quién conozca dicho procedimiento y clave puede acceder a la información original. Es un mecanismo de seguridad.
- **Criptoanálisis**: pasos y operaciones orientadas a transformar un criptograma en el texto claro original pero sin conocer inicialmente el sistema de cifrado utilizado y/o la clave (es un término ligado a «descriptación» y «ataque»).
- **Criptógrafo**: es el equipo de cifra que se utiliza para el cifrado de un texto determinado.
- **Criptograma**: término que se aplica al texto cifrado ya formateado y preparado para la transmisión.
- **Criptosistema**: conjunto de claves y equipos de cifra que, utilizados coordinadamente, ofrecen un medio para cifrar y descifrar.

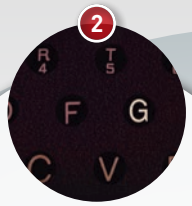
Enigma K-296

El modelo *K* de la singular máquina de cifrado alemana —tan codiciada en la II Guerra Mundial— fue el más usado en España. En concreto, esta *296*, que prestaba servicio en la VI Región Militar en 1938, podía generar hasta 1.800 millones de combinaciones distintas de cifrado. Todo empezaba en su visor de posición.

1

Visor posición inicial
Refleja el orden fijado en la unidad modificadora, básico para la transmisión correcta del mensaje.

2

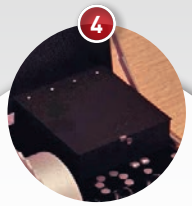


Panel luminoso
Tiene 26 bombillas, una por cada letra del teclado, y su función es mostrar el carácter encriptado.

3

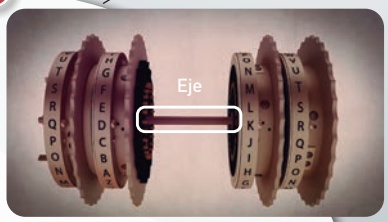
Teclado
Son sus 26 teclas/letras, para introducir el texto inicial como en una máquina de escribir.

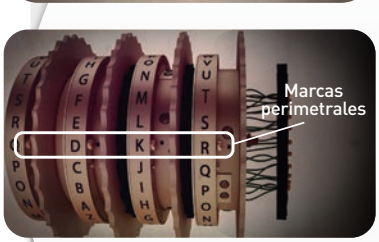
4



Batería
Da energía al sistema. Es su fuente de alimentación más frecuente, aunque puede emplear otras.

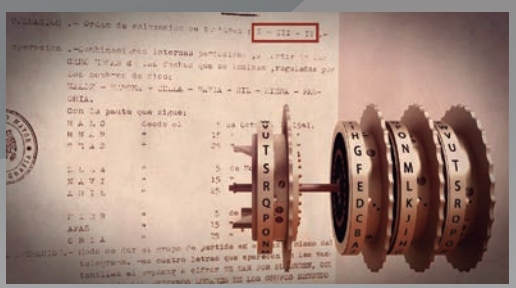
5





Unidad modificadora
Es el alma de la *Enigma*. La forman, en un eje, tres rotores o modificadores —intercambiables en su posición— y un reflector, que envía la señal eléctrica. Sus 26 marcas perimetrales se corresponden con las letras de teclado y panel luminoso. Cada rotor puede fijar, siempre y de forma autónoma, cualquier carácter como letra de inicio.

Instrucciones de uso



Ejemplo de orden de los rotores, del libro de claves.

Mensaje descifrado, con las pautas establecidas.

Rafael Navarro/RED/Textos: Esther P. Martínez/Fuente: Vídeo *Proyecto Enigma* (coordina A. Bustillo; asesor técnico J.R. Soler), Universidad de Burgos y Museo Histórico Militar.