
LA
BIBLIA
DE LOS
CÓDIGOS
SECRETOS
Hervé Lehning

HERVÉ LEHNING

# LA BIBLIA DE LOS CÓDIGOS SECRETOS

LIBROS CÚPULA

Título original: *La Bible des codes secrets*
Primera edición en Francia en colaboración con Xavier Müller.



Diseño de la cubierta: Planeta Arte & Diseño

Primera edición: noviembre de 2021


Av. Diagonal, 662-664, 08034 Barcelona (España)
Libros Cúpula es marca registrada por Editorial Planeta, S. A.
www.planetadelibros.com

ISBN: 978-84-480-2739-1

Depósito legal: 3.976-2020

Impreso en España – *Printed in Spain*

El papel utilizado para la impresión de este libro está calificado como papel ecológico y procede de bosques gestionados de manera sostenible.

# SUMARIO

# 1

# EL ARMA DE LA GUERRA SECRETA

Existe la historia con «H» mayúscula y existen *las* historias.

Las que terminan en las notas al pie de los manuales escolares. Sin embargo, son ellas quienes inflaman la imaginación de los novelistas y de los guionistas. Desde César desafiando a los germanos con sus mensajes cifrados a Radio Londres y la emisión «Los franceses hablan a los franceses», la guerra vista a través del prisma de los códigos secretos está llena de episodios de ese tipo, a veces anecdóticos, a veces impresionantes (como el resultado de la batalla). Hojear las páginas de esta epopeya es recorrer en desorden dos mil años de una «contrahistoria» de nuestra civilización, tan palpitante y útil de conocer como la «contrahistoria» de la filosofía que algunos han desvelado.

¿Un ejemplo de esos bastidores de la historia? Lombardía, 23 de diciembre de 1796. Hace ya diez meses que el ejército de Italia de Bonaparte asedia la ciudad de Mantua, donde se ha recluido el ejército austriaco. Un ejército (igualmente austriaco) de socorro ha intentado abrirse paso para ayudar, pero ha sufrido una grave derrota durante la célebre batalla del puente de Arcole, en noviembre. En esta víspera de Navidad, los centinelas que vigilan en las fronteras de Mantua detienen a un don nadie que busca penetrar en la ciudad ocupada. A pesar de la ausencia de pruebas, sospechan de su complicidad con los austriacos y lo conducen hasta el general Dumas, el padre del futuro Alexandre Dumas que contará la anécdota en sus memorias. ¿El pobre diablo, en realidad, es un espía? El general piensa entonces en un método antiguo descrito por César en *La guerra de las Galias*, pero que

ya utilizaban en Extremo Oriente mucho antes. Los señores chinos escribían sus mensajes sobre una tela de seda muy fina, que cubrían luego con cera. El mensajero no tenía más que tragarse la bolita de cera para estar seguro de que el mensaje no sería interceptado.

Dumas hizo servir un purgativo al prisionero, que poco después... dio a luz... ¡un mensaje encerrado en una bolita de cera! Escrito a mano por el general austriaco Alvintzy, el texto anunciaba la llegada de refuerzos:

> Según las posibilidades, el movimiento que haré tendrá lugar el 13 o el 14 de enero; desembocaré con treinta mil hombres en la meseta de Rivoli, y enviaré a Provera diez mil hombres por el Adige hacia Legnago con un convoy considerable. Cuando escuchen el cañón, salgan para facilitar su movimiento.

El procedimiento era hábil y los franceses estaban encantados por haber interceptado el mensaje. Bonaparte envió exploradores hacia el norte de Italia que confirmaron que el ejército de Alvintzy, efectivamente, se había dividido en dos cuerpos que debían reunirse en Rivoli. En ese conflicto, los franceses se batían uno contra dos. Gracias a esa información robada, los soldados de Napoleón compensaron su inferioridad numérica. Afrontaron por separado a los dos ejércitos y consiguieron expulsar a los austriacos fuera de la península itálica hacia 1797. Un laxante salvó al portador del bicornio.

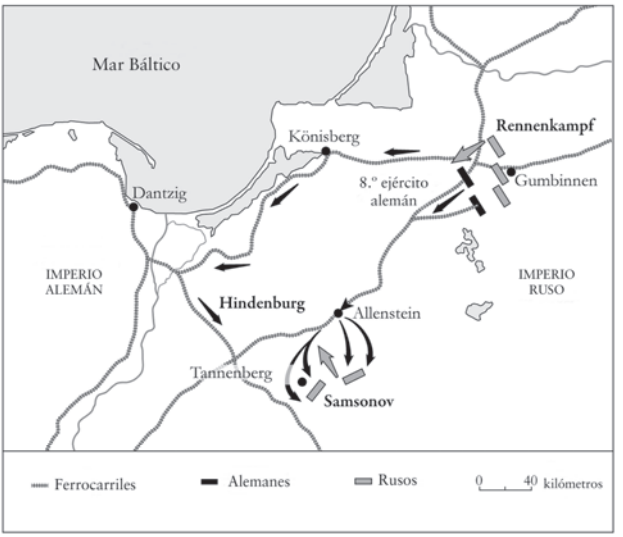
## Leer en el juego de sus adversarios

¿Por qué el general austriaco Alvintzy no codificó su mensaje? La historia retiene raramente las lecciones del pasado. Un siglo más tarde, los rusos cometieron el mismo error y sufrieron una derrota a la altura de ese imperdonable olvido. Cuando estalló la Primera Guerra Mundial, el 4 de agosto de 1914, Rusia no estaba lista para lanzar su enorme ejército de más de cinco millones de hombres sobre Alemania. Por eso, esta intentó aprovechar el

plazo para aniquilar a los ejércitos franceses en un vasto plan de asedio en seis semanas. Alemania solo había dejado en Prusia oriental un ejército de 200.000 hombres. Para sorpresa de los alemanes, los rusos atacaron el 17 de agosto con dos ejércitos de 400.000 hombres cada uno. El plan ruso era simple: coger al enemigo en un movimiento de pinza. Mientras el primer ejército ruso, dirigido por Pavel Rennenkampf, atacaba por el este, el segundo, bajo las órdenes de Alexandre Samsonov, rodearía las líneas alemanas por el sur, para cogerlos por detrás. Sobre el papel, la victoria estaba asegurada salvo por un detalle: las comunicaciones. Incapaces de equipar con líneas telegráficas las distancias recorridas, los rusos utilizaban la radio que, evidentemente, los alemanes escuchaban. No obstante, como no se habían entregado a tiempo ninguno de esos preciosos libros de códigos necesarios para cifrar los mensajes, las transmisiones se hacían en claro. Dicho de otra manera, ¡los alemanes estaban invitados a las reuniones del estado mayor ruso! A pesar de esta ventaja, la invasión de Prusia oriental comenzó bajo buenos auspicios: los alemanes se vieron obligados a retirar del frente oeste dos cuerpos del ejército, lo que alivió otro tanto la presión sobre el ejército francés. Para evitar el asedio, el general alemán ordenó la retirada del río Vístula, abandonando así la totalidad de Prusia oriental. Fue inmediatamente relevado de sus funciones y reemplazado por Paul von Hindenburg, asistido por Erich Ludendorff, quienes reanudaron la ofensiva.

Ese cambio en el mando marcó un giro en la batalla. Cuando Hindenburg y Ludendorff supieron, gracias a los mensajes enemigos captados, que su homólogo ruso Rennenkampf había reducido su marcha, temiendo que los alemanes escaparan a la maniobra, dejaron un fino cordón de caballería por delante y utilizaron la excelente red ferroviaria alemana para concentrar todo su esfuerzo sobre Samsonov, su segundo perseguidor, del que conocían la localización exacta. La batalla de Tannenberg que siguió fue la única victoria decisiva de la Primera Guerra Mundial. El segundo ejército ruso fue derrotado y Samsonov se suicidó para escapar a la captura y la vergüenza. Los rusos retuvieron la dolorosa lección: se pusieron a codificar sistemáticamente sus mensajes, pero

con unas técnicas aproximativas. Tanto que, hasta el final de la guerra, libraron combate sin suponer que el adversario ¡seguía leyendo sus planes por encima del hombro!




En agosto de 1914, durante la invasión de Prusia oriental, los rusos buscaban vencer al ejército alemán rodeándolo. Su plan fue aniquilado por la ausencia de transmisiones cifradas, que condujeron al desastre de Tannenberg.

Tropas rusas en ruta hacia el frente en 1916. Lo que se llamó en aquella época «la apisonadora» se mostró mal preparada e incapaz de luchar seriamente contra Alemania, porque su cifrado era muy deficiente.

## El milagro del Vístula

Los reveses de Rusia no terminan aquí. Inmediatamente después de la Gran Guerra, pagaron nuevamente el precio de su falta de sabiduría en materia de cifrado. El teatro del conflicto esta vez fue el Vístula, el principal río de Polonia. En 1920, Rusia, ahora soviética, se lanzó a la reconquista del país, independiente desde el Tratado de Versalles. Lenin, en el poder en Moscú, soñaba también con exportar la revolución a Europa occidental y Polonia constituía un cerrojo frente al proyecto.

Más poderoso, el ejército ruso parecía vencedor, pero su adversario poseía un as en la manga: el servicio encargado de la descodificación de las transmisiones, la Oficina del Cifrado, donde trabajaban matemáticos de alto nivel como Waclaw Sierpinski (1882-1969) —más conocido por el público por los fractales que llevan su nombre— y Stefan Mazurkiewicz (1888-1945), dos grandes nombres del análisis matemático —la rama de las matemáticas que se interesa en las funciones.

Esa Oficina del Cifrado descodificó los comunicados rusos y reveló en el dispositivo soviético una debilidad que condujo al ejército polaco a la victoria. El clero polaco, que había pedido a la población que rezara por la salvación del país, calificó ese triunfo como el «milagro del Vístula» por el nombre del lugar donde se situó la batalla clave. El único milagro que tuvo lugar allí fue la descodificación de las comunicaciones rusas.

## El mensaje era una cortina de humo

Históricamente, el «milagro del Vístula» no fue la primera victoria a contabilizar en el crédito de los descifradores. Para citar un ejemplo del *Grand Livre de la France*, ya en 1626, Enrique II de Francia había sabido beneficiarse de las competencias de la Oficina del Cifrado. He aquí los detalles de la situación. El príncipe de Condé, católico, asediaba Réalmont, una plaza fuerte protestante situada en el departamento del Tarn, desde hacía cierto tiempo. El adversario resistía con coraje, especialmente gracias a

sus cañones y él se disponía a marcharse por fin cuando sus tropas interceptaron a un hombre que salía de la ciudad. ¿Te recuerda a la historia de Lombardía que ya hemos contado? Sí, con una diferencia y es que el hombre llevaba encima el mensaje, bien cifrado esta vez. Pero ¿qué significaba ese galimatías formado de letras y símbolos?

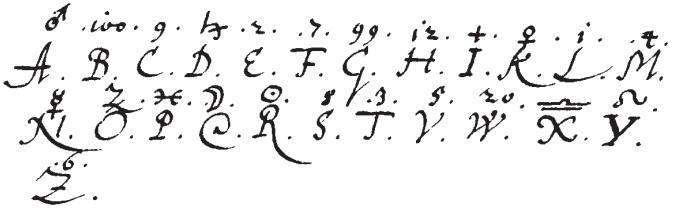
Para descodificar el mensaje, hicieron viajar a Antoine Rossignol, un joven matemático conocido en la región por su talento de descifrador. Consiguió comprender el galimatías. ¿Qué decía? Que la ciudad carecía de pólvora y que, si no la recibían, estarían obligados a rendirse. Los destinatarios de la misiva eran los hugonotes de Montauban.

Antoine Rossignol (1600-1682). Según una leyenda, gracias a su capacidad para descifrar los mensajes codificados, el matemático dio su nombre al instrumento que permite abrir las puertas sin llave, como se ha visto en muchas películas. Es falso, el término fue certificado unos doscientos años antes del nacimiento de Rossignol.

Hábil, Condé reenvió el mensaje descifrado a Réalmont, que se rindió. En solitario, ¡Rossignol acababa de influenciar el curso de la historia!

Reiteró su hazaña durante el sitio de La Rochelle el año siguiente, de tal manera que el cardenal Richelieu lo tomó a su servicio. Este excelente criptoanalista (un especialista del desciframiento) modificó luego en profundidad la criptografía de su época (ver el capítulo 5).

La historia no ha conservado la naturaleza del cifrado del mensaje que salía de la fortaleza. Sin embargo, es probable que utilizara un alfabeto cifrado como el que sigue, fechado en la misma época (1627), y que proviene de los archivos de la ciudad de Estrasburgo.



Alfabeto cifrado utilizado en 1627 por un delegado de Estrasburgo. De manera clásica, I y J por una parte, U y V por otra están confundidas. En cuanto a V y W, el hecho que esas dos letras sean distintas en el código deja pensar que ese alfabeto servía más bien a cifrar los mensajes redactados en alemán.

Para aprovechar este alfabeto, se reemplaza cada letra por el símbolo situado encima. Algunas advertencias sobre la calidad de esa codificación: es frágil, porque si el texto es suficientemente largo, basta con aislar el símbolo más frecuente para saber que corresponde a la letra E (la letra más corriente en francés y en castellano junto con la A). Las repeticiones en el interior de un mismo término son igualmente susceptibles de servir para descubrir el mensaje: palabras que contienen un duplicado de letras como *municiones*, que cuentan dos N y dos I, tienen estructuras particulares que permiten buscarlas en forma «..*+.+.*» donde cada punto corresponde a un símbolo cualquiera.

La aptitud para reconocer las estructuras, incluso fuera de las matemáticas avanzadas, forma parte de las capacidades requeridas tanto en matemáticas como en criptología (la ciencia del cifrado). Esto explica, sin duda, que, desde el siglo XVII, los grandes criptólogos fueran a menudo matemáticos.

En ese terreno, encontramos a François Viète (1540-1603) que puso su ciencia al servicio de Enrique IV de Francia, incluso si es más conocido en nuestros días por sus investigaciones en álgebra. Su enfoque era propiamente matemático porque era sistemático. En particular, había establecido una regla, que él decía infalible, según la cual en tres letras sucesivas, una al menos era una vocal. Incluso si esto no es totalmente exacto en francés, como lo muestran las palabras que contienen la secuencia «ntr» en particular, se trata de una ayuda valiosa para localizar las vocales con seguridad o casi.

Los dones de Viète casi lo envían a la hoguera. Entre todas las cartas que consiguió descifrar figuraban las del rey de España, Felipe II. Este terminó por saberse espiado y, pensando en fastidiar a los franceses, advirtió al papa que Enrique IV no podía haber leído sus mensajes sin utilizar la magia negra. La información hizo sonreír al papa: su propio criptólogo había roto algunos códigos de Felipe II treinta años antes. Fue así como Viète escapó a un eventual proceso de brujería.

## Venganza del corazón

Existe otro escenario de guerra en el que la tinta de los mensajes puede revelarse venenosa: la justa amorosa. La historia más antigua que mezcla juegos de amor y códigos viene de Homero. La mujer de Preto, el rey de Tirinto, había sido rechazada por Belerofonte «a quien los dioses habían dado belleza y vigor» y decidió vengarse de él, acusándolo de ser su pretendiente ante su marido:

> –Muere, Preto, o mata a Belerofonte que, por medio de la violencia, quiso unirse a mí. –Ante estas palabras, el rey monta en cólera, pero no mata a Belerofonte, temiendo piadosamente un asesinato, sino que lo envía a Licia con unas tablas donde había trazado unos signos de muerte, para que los entregara al rey, su suegro, y que este lo matara.

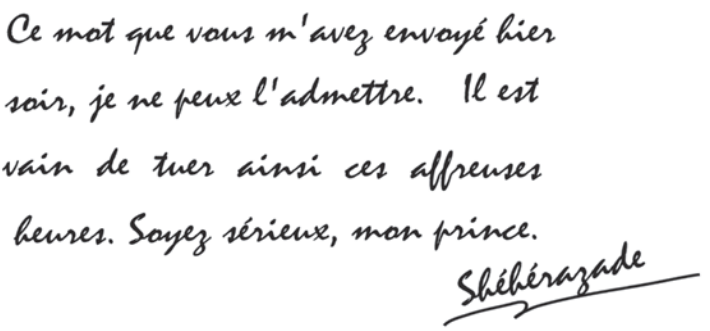
En realidad, los acontecimientos no sucedieron así. Cuando el rey de Licia recibió las famosas tablas con signos de muerte, vi-

siblemente un mensaje codificado, antes que matar a Belerofonte de inmediato, prefirió enviarlo a combatir contra los monstruos, epopeya de la que salió vivo. Pero el verdadero uso de los códigos secretos en amoríos se utilizó, sobre todo, para mantener en secreto el contenido de los mensajes epistolares. «Hay particularidades que no puedo describir por haber perdido el código que tenía contigo», lamentó Enrique IV en una carta a su amante, la condesa de Gramont. La práctica parece tan antigua como el amor mismo. En la India antigua, la escritura secreta era una de las 64 artes que debía poseer la perfecta concubina según el *Kamasutra*.

Esconder el contenido de sus mensajes está bien. Disimular el acto mismo de escribir es mucho mejor. Eso evita despertar las sospechas. En la página siguiente te propongo un mensaje que Scheherezade habría escrito a su amante.

En apariencia, nada comprometedor. Sin embargo, esas cuatro líneas contienen el mismo mensaje que la frase sospechosa «GI WSMV ZMRKX LIYVIW», es decir, «Ce soir, vingt heures» [Esta noche a las ocho].

Las dos técnicas empleadas aquí para cifrar el mensaje se llaman esteganografía y criptografía. La primera esconde el mensaje en un envío decoroso, mientras que la segunda lo codifica.




Carta de una princesa a su amante.

[Nota de la traductora: **Esta** carta que me escribió ayer a la / **noche** no puedo admitirla es / **vano** matar así esas / **horas** espantosas / Conserve la compostura, príncipe mío. Si se lee en francés la primera palabra de las frases de la carta dicen fonéticamente «esta noche veinte horas».]

Nuestra princesa tenía razón en recurrir a la esteganografía. Al final del siglo XIX, los amantes se dedicaban a jugar a los aprendices criptólogos vía los anuncios de los periódicos. Un mensaje como «GI WSMV ZMRKX LIYVIW» en medio de las ventas de leña o de búsqueda de vivienda es totalmente inocente. En la actualidad, los SMS autorizan mayor libertad, pero ya hablaremos de ello. Por sorprendente que pueda parecer, las cartas de amor intercambiadas por los enamorados, en versión cifrada, tuvieron su importancia en la historia de la criptografía. Étienne Bazeries, una de las grandes figuras del final del siglo XIX y comienzos del XX, se divertía leyendo los mensajes personales cifrados que, en la época, servían de medio de comunicación a las parejas ilegítimas. En el pabellón de los oficiales de su guarnición, entretenía a sus colegas con historias escabrosas que leía sin dificultad, hasta el día en que anunció que también podía leer los mensajes cifrados del ejército sin conocer el código. Su general tomó este comentario en serio y le pidió que descifrara algunos informes del ministerio, lo que Bazeries realizó sin problemas. Más tarde se convirtió en uno de los eminentes criptólogos del ejército francés y, más adelante, del Ministerio de Asuntos Exteriores.

## A un tris de la derrota

Si Scheherezade quizá embrujaba a los hombres con sus cuentos de las mil y una noches, el ejemplo que hemos dado antes de esteganografía comenzando por «Ce mot que vous m'avez envoyé» [Esa carta que me escribió anoche] tendría pocas posibilidades de sorprendernos actualmente porque la estratagema parece grosera. ¿Otro ejemplo de esteganografía? La ilustración más antigua que se conoce de la técnica se remonta al siglo V antes de nuestra era y nos la cuenta el historiador griego Heródoto. Recordemos que la criptografía es el arte de esconder el sentido de un mensaje cuya presencia es evidente. Por ejemplo, es manifiesto que «HVWR HV XP OHPVDMH FLIUDGR» es un mensaje cifrado. Al contrario, la esteganografía consiste en disimular la existencia misma del mensaje.

¿Qué cuenta Heródoto? Aristágoras, el tirano (el equivalente de un déspota en la época) de la ciudad de Mileto tenía un tío que se llamaba Histieo. Cuando este último se encontraba en la corte de Persia como consejero, quiso informar a su yerno que había llegado el momento de rebelarse contra Persia, justamente. Para transmitir ese mensaje, Histieo eligió un esclavo muy fiel, le rapó la cabeza y escribió en su cuero cabelludo. Esperó a que los cabellos crecieran y lo envió a Aristágoras. Cuando llegó a Mileto, el esclavo solo tuvo que raparse para entregar su mensaje. Un poco largo, pero eficaz como técnica esteganográfica.

En sus obras, Heródoto describe otro método muy cercano, aprovechado esta vez por Demarato, exiliado en la corte de Persia. Para advertir al rey de Esparta de un ataque inminente, Demarato cogió unas tabletas de cera con las cuales se solía escribir, rascó la superficie, grabó un mensaje secreto directamente sobre la madera, luego le devolvió su apariencia original. Aparentemente vírgenes, no llamaron la atención durante el camino. A su llegada a Esparta, la reina Gorgo, una mujer de gran inteligencia, se sorprendió frente a esas tablillas intactas y tuvo la idea de rascar la cera. Así descubrió el mensaje de Demarato.

Étienne Bazeries (1846-1931), uno de los más famosos criptólogos de su tiempo.

El primer descifrador de la historia fue una mujer. Su discernimiento salvó al mundo griego del peligro persa (pero causó la muerte de su esposo, Leonidas, durante la famosa batalla de las Termópilas).

## Tinta simpática alemana

Un siglo después de Heródoto, le tocó el turno a un militar griego que reveló algunos de sus métodos secretos de esteganografía. Ese señor de la guerra era el bien llamado Eneas, el estratega. En su libro sobre el arte del asedio, contó cómo disfrazar un mensaje en el interior de un libro marcando ciertas letras de manera imperceptible, con una aguja, por ejemplo. El mensaje aparece copiando en orden las letras así elegidas. Esta astucia fue utilizada también por los espías alemanes durante la Segunda Guerra Mundial para transmitir informaciones a su jerarquía. La tinta simpática descubría las letras. Todos los medios son buenos, en realidad, si el mensaje es descifrable por su destinatario y no despierta ninguna sospecha en los otros, lo cual no siempre se puede dar por sentado.

Inténtalo tú mismo: para esto, coge un libro y consigue tinta invisible, que se hace visible solo después de un ligero calentamiento. Puedes utilizar leche, jugo de limón o incluso orina; con un bastoncillo, tacha los caracteres para formar tu mensaje. Deja secar y absorbe el sobrante con un secante: ahora, solo falta transmitir el libro a su destinatario. Una versión modernizada del mismo método consistiría en pasar por páginas anodinas de internet, como las ventas en subasta, para transmitir tus mensajes designando las letras por espacios dobles o triples entre las palabras.

Inversamente, si no tienes tinta simpática, puedes contentarte agregando marcas finas bajo algunos caracteres del libro. Así, la frase de Marcel Proust: «Durante mucho tiempo, me acosté te**M**prano. **A** veces, apenas apagada la vela, mis ojos se ce**R**raban **T**an rápido que no t**E**nía tiempo de decirme a mí mi**S**mo: Me duermo», traslada el mensaje «martes» que puede constituir la respuesta a una pregunta.

LO QUE DEBEMOS DESCIFRAR:

**Un mensaje disimulado en un libro**

Se encontró un libro en la celda de un prisionero.
He aquí una de sus páginas:

**▶¡Las abejas tenían razón y no los logaritmos!**

Las arañas no son los únicos animales matemáticos. En esta área, las abejas son mucho más asombrosas. El panal de cera construido por estos insectos voladores para depositar su miel está formado por dos capas de celdas opuestas por su fuente. Desde la antigüedad, notamos que los alvéolos se parecían a prismas rectos con una base hexagonal regular (ver la figura *Los alvéolos de las abejas*). No fue hasta el siglo XVIII que se percibió que el fondo era el ensamblaje de tres diamantes homogéneos, cada uno perteneciente a dos celdas opuestas.

Se esconde un mensaje: ¿cuál es?

## Reconocimiento tardío

La esteganografía puede llevarnos hacia las delicias del amor, pero el verdadero tema de este libro es el arte de codificar las informaciones, dicho de otra manera, la criptología. A pesar de su importancia en los campos de batalla, así como nos lo han mostrado las repetidas derrotas del ejército ruso, esta ciencia pocas veces ha sido reconocida en su justo valor por los historiadores. ¿Por qué? Simplemente porque está cubierta por el secreto. Por ejemplo, en 1968, los historiadores supieron que los mensajes alemanes de la Primera Guerra Mundial (ha leído bien: ¡la Primera!) fueron descifrados por los servicios franceses durante todo el conflicto. La historia ya estaba escrita y nadie se preocupó realmente por ahondar en un tema que ni siquiera los militares habían aclarado.

La misma discreción rodeó los éxitos británicos durante la Segunda Guerra Mundial. En particular, gracias a la célebre máquina Enigma, ellos también supieron descifrar una gran parte de los mensajes alemanes, decididamente poco capaces para disi-

mular sus secretos. Sin embargo, los británicos no se enorgullecieron de ello, incluso después de la guerra. Todo lo contrario: hasta 1973, pretendieron que Enigma era indescifrable, lo que les permitió revender las máquinas confiscadas al ejército alemán a gobiernos y a empresas extranjeras.

## El César al mejor cifrado

Hemos hablado mucho de criptografía hasta ahora, pero sin abordar un ejemplo propiamente dicho. Viajemos hacia la antigüedad para ese primer contacto con la técnica (que un niño que sepa leer puede utilizar). Si te dijera que en esa época uno de los grandes lugares del uso criptográfico era un territorio rico en ambiciones militares e intrigas políticas, no te sorprendería ¿verdad? Por supuesto, me refiero a Roma. En la biografía que dedicó a los doce Césares que se sucedieron a la cabeza de la ciudad imperio (*Vidas de los doce Césares*), Suetonio describe una manera de cifrar que utilizaba Julio César (el único):

> César empleaba, para sus asuntos secretos, una especie de cifrado que volvía ininteligible el sentido (las letras estaban dispuestas de tal manera que nunca formaban una palabra). Y consistía, lo digo para aquellos que quieran descifrarlo, en cambiar el rango de las letras del alfabeto, escribiendo la cuarta por la primera, es decir la D por la A y así sucesivamente.

Volvamos al ejemplo «HVWR HV XP OHPVDMH FLIUDGR» que ya hemos visto antes. Lo he cifrado con este método. Aquellos que deseen familiarizarse con las técnicas de la criptografía elementales están invitados a practicar. Para los demás, basta con desplazar cada letra tres letras hacia el sentido opuesto. Así F se vuelve C, H se vuelve E, etcétera. Si se sigue ese procedimiento, se obtiene el mensaje (no demasiado original) «CECI EST UN MESSAGE CODÉ» [Esto es un mensaje cifrado]. Si el paso de desplazamiento te resulta desconocido, puedes determinarlo por el método de las frecuencias sin problema.

Lo que debemos descifrar:

**Un mensaje de César**

Vercingetórix intercepta el siguiente mensaje de sus generales a César:

HVWR HV XP OHPVDMH FLIUDGR

¿Sabrás descifrarlo?

A pesar de su antigüedad y su simplicidad (por no decir más), el cifrado de César fue utilizado al menos dos veces en la época moderna. Sorprendente ¿no? Hay que creer que la facilidad para ponerlo en práctica prevalecía frente a su debilidad.

Shiloh significa «puerto de paz» en hebreo, nombre ideal para una pequeña capilla de madera. Ironía de la historia, la batalla más sangrienta de la guerra de Secesión debutó allí el 6 de abril de 1862 con una ofensiva sorpresa de las tropas sudistas. Habían sabido mantener el secreto de su plan de ataque codificando simplemente sus transmisiones con el cifrado de César. Grabado de Frank Leslie, 1896.

Así, en 1862, antes de la batalla de Shiloh durante la guerra de Secesión, el general sudista Albert Johnston, excelente oficial, pero pésimo criptólogo, intercambió mensajes con su adjunto recurriendo a un cifrado de desplazamiento —con éxito al parecer, puesto que los nordistas fueron cogidos por sorpresa. Sin embargo, estos tuvieron su revancha al día siguiente y transformaron la derrota en victoria, al precio de un coste humano tremendo.

Al comienzo de la Primera Guerra Mundial, quien utilizó el cifrado de César fue el ejército ruso. Los generales descubrieron la necesidad de cifrar sus mensajes. Ese tipo de código les fue inspirado por un ejército mal formado y constituido por numerosos soldados iletrados. Como evocamos al comienzo de este capítulo, esto los llevó a la derrota.

## ¿Cifrado o código?

En el relato biográfico de Julio César, Suetonio (o más bien su traductor) utiliza el término «cifrado» y no «código». Hasta ahora, yo mismo lo he utilizado de manera indiferente. Sin embargo, existe una diferencia sutil entre los dos términos. Un cifrado opera más bien sobre las unidades elementales que componen un mensaje: letras, sílabas u otras. Por el contrario, un código se aplica a las palabras o a las frases de un mensaje y a su significado.

Por ejemplo, en el código de los emoticonos, (😊) significa «estoy contento», (😞) lo contrario. El conjunto de los códigos está, en general, reunido en un libro de códigos, así que lo veremos con los diccionarios cifrados en el capítulo siguiente. La confusión entre cifrado y código no es muy grave y yo preferiré en esta obra el sentido común, que gira alrededor del secreto.

## Cuando las dos técnicas se disputan

Os he presentado la esteganografía y la criptografía como métodos separados.

Pero es posible mezclarlas, de la misma manera que dos colores primarios se combinan para producir un nuevo color. Mu-

hámmad al-Mutamid, el rey árabe de Sevilla de finales del siglo XI, nos proporciona un ejemplo muy visual. Poeta, tuvo la idea de emplear nombres de pájaros para transmitir sus mensajes secretos. Cada pájaro se asociaba a una letra del alfabeto. Muhámmad al-Mutamid comenzó por hacer una lista de los pájaros que correspondían a su mensaje, luego compuso un poema a partir de esta letanía. Si hacemos corresponder los nombres de los pájaros con su primera letra, en francés, el poema es:

> La tourterelle du matin craint le vautour,
> Qui pourtant préfère les nuées d'étourneaux,
> Ou au moins les loriots
> Qui, plus que tout, craignent les éperviers.
>
> *La tórtola de la mañana teme al buitre,*
> *que, sin embargo, prefiere las bandadas de*
> *estorninos, o al menos a las oropéndolas*
> *que, más que nada, temen a los gavilanes.*

transmite el siniestro mensaje: «tue-le» [mátalo] (he hecho un poco de trampas confundiendo la «u» y la «v»). Este tipo de código, donde el mensaje está escondido y además cifrado, se sitúa entre la esteganografía y la criptografía.

LO QUE DEBEMOS DESCIFRAR:

**Un mensaje florido**

Interceptamos el siguiente mensaje:

> Cuántas flores en su jardín: enebro perfumado, salvia a raudales, tréboles que se esparcen entre las flores, azucenas brillantes, nardos enhiestos, orquídeas olorosas y claveles por doquier..., pero sobre todo unas plantas de hortensias azules entre las ramas de endrino...

¿Qué mensaje se esconde aquí?

## Las letanías de Tritemio

Heredero espiritual del rey de Sicilia, el abad Johannes Trithemius (1462-1516) imaginó un sistema de criptografía disimulado en las letanías religiosas. En su época, los rezos litúrgicos constituían un buen biombo para disimular los mensajes. La lista de términos a las que recurría figura en los cuadros que siguen. Las letanías están en latín, pero es inútil dominar la lengua para utilizar el sistema, que busca cifrar o descifrar un mensaje. A cada letra del alfabeto corresponden varias palabras o frases. Tritemio efectuaba su elección entre 18 posibilidades, pero aquí he dado solo 8 a modo de ejemplo.

Ocupémonos del mensaje «ALERTA». De acuerdo con los cuadros, una posibilidad de letanía sería:

> Pater generatium qui existis in aevum beatificetur vocabulum Sanator

El método de Tritemio tenía un defecto: la extensión de los mensajes producidos. Sin contar con que, si el mensaje caía en manos de un buen latinista, ¡no valía nada!

Encontraremos a Tritemio en las sustituciones polialfabéticas, cuyas letanías son un primer ejemplo.

LO QUE DEBEMOS DESCIFRAR:

### Una extraña oración

Un discípulo de Tritemio propone una nueva oración:

> Honoreficetur liberator Creator pater rector pater Cognomentun tuum sanator.

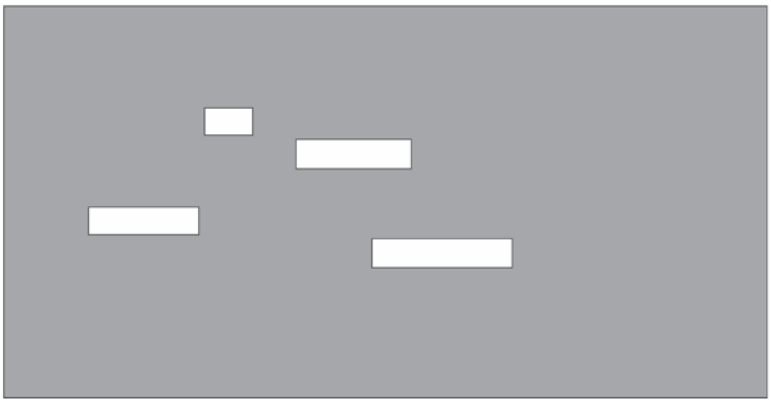
¿Sabes cuál es el verdadero mensaje?

| | | | | |
|---|---|---|---|---|
| A | Pater | Noster qui | Es in | Caelis |
| B | Dominus | Nostrum qui | Gloriosus in | Celo |
| C | Creator | Omnium qui | Graditur in | Altis |
| D | Benefactor | Cunctorum qui | Extas in | Alto |
| E | Sanator | Universorum qui | Existis in | Exelsis |
| F | Salvator | Chistianorum qui | Manes in | Exelso |
| G | Conservator | Predestinorum qui | Permanes in | Altissimo |
| H | Justificator | Supercolestium qui | Resplendes in | Altissumis |
| I | Adjutor | Universalium qui | Dominaris in | Celestibus |
| L | Auxiliator | Generatium qui | Luces in | Omnibus |
| M | Autor | Generis nostri qui | Principaris in | Universis |
| N | Index | Hominum qui | Triomphas in | Supernis |
| O | Rex | Justororum qui | Imperas in | Paradiso |
| P | Rector | Bonorum qui | Regnas in | Celesti |
| Q | Defensor | Piorum qui | Reluces in | Empireo |
| R | Imperator | Mitium qui | Sedes in | Aevum |
| S | Liberator | Fidelium qui | Resides in | Aeviternum |
| T | Vivificator | Sanctorum qui | Refulges in | Aeternum |
| V | Consolator | Credentium qui | Habitas in | Perpetuum |
| X | Magister | Angelorum qui | Rutilas in | Aeternitate |
| Y | Admonitor | Spiritum qui | Splendescis in | Eminentissimo |
| Z | Arbiter | Orthodoxorum qui | Glorificaris in | Supremis |

| | | | | |
|---|---|---|---|---|
| A | Sanctificetur | Nomen tuum | Adveniat tuum | Regnum tuum |
| B | Magnificetur | Domicilium tuum | Conveniat tuum | Imperium tuum |
| C | Glorificetur | Aedificium tuum | Perveniat tuum | Dominium tuum |
| D | Benedicatur | Latibulum tuum | Proveniat tuum | Institutuum tuum |
| E | Honorificetur | Vocabulum tuum | Accedat tuum | Documentium tuum |
| F | Superexaltetur | Imperium tuum | Appropinquet tuum | Beneplacitum tuum |
| G | Honoretur | Regnum tuum | Magnificetur tuum | Repromissum tuum |
| H | Exaltetur | Scabellum tutum | Multiplicetur tuum | Constitutum tuum |
| I | Laudetur | Consilium tuum | Sanctificetur tuum | Promissum tuum |
| L | Oeiligatur | Eloquium tuum | Dilatetur tuum | Verbum tuum |
| M | Ametur | Institutum tuum | Pacificetur tuum | Dogma tuum |
| N | Adoretur | Constitutum tuum | Amplietur tuum | Ovile tuum |
| O | Colatur | Alloquium tuum | Proevaleat tuum | Opus tuum |
| P | Invocetur | Mysterium tuum | Convaleat tuum | Placitium tuum |
| Q | Celebretur | Testimonium tuum | Exaltetur tuum | Complacitum tuum |
| R | Collandetur | Evangelium tuum | Augeatur tuum | Promium tuum |
| S | Clarificetur | Cognomentum tuum | Firmetur tuum | Amuletum tuum |
| T | Beatificetur | Cognomen tuum | Confirmetur tuum | Adjutorium tuum |
| V | Manifestetur | Proenomen tuum | Crescat tuum | Remedium tuum |
| X | Agnoscatur | Pronomen tuum | Veniat tuum | Domicilium tuum |
| Y | Cognoscatus | Templium tuum | Veniens esto tuum | Testimonium tuum |
| Z | Notium esto | Agnomentum tuum | Crescens esto tuum | Sanctuarium tuum |

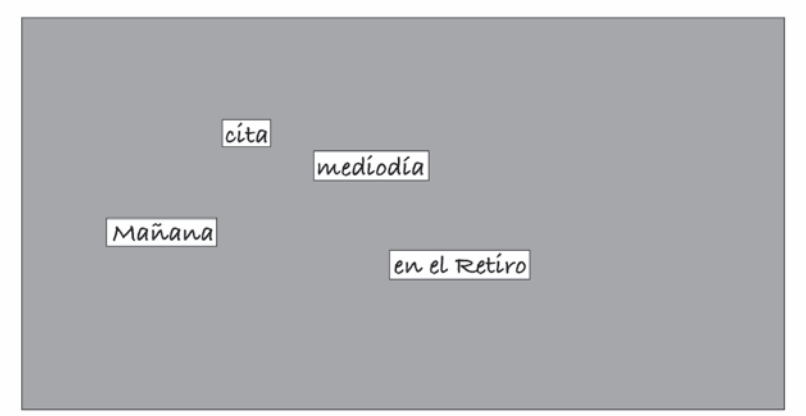
## ¡Abajo las máscaras!

Para terminar con este aperitivo sobre el arte de cifrar los mensajes, te propongo que dejes caer las máscaras. Literalmente. Nuestra historia se desarrolla en Italia, habríamos podido dirigirnos al festival de Venecia, pero dirijámonos mejor a Pavía, donde nació, en el siglo XVI, Girolamo Cardano, llamado Jérôme Cardan en Francia. Sabio consumado, Cardan es conocido hoy en día, sobre todo, por sus ecuaciones de tercer grado y el famoso sistema de transmisión que lleva su nombre. También fue el inventor de un dispositivo situado entre esteganografía y criptografía, destinado a cifrar mensajes con ayuda de una especie de máscara en forma de tarjeta perforada. Para comunicar de manera secreta, dos personas deben compartir la misma hoja de cartón denso o de metal, agujereado con formas rectangulares.



### Una rejilla de Cardan

Para utilizarla, hay que poner la rejilla sobre una hoja de papel y escribir un mensaje en los agujeros previstos. Por ejemplo, si se quiere dar cita a un contacto, al día siguiente en Saint-Germain, se escribirá:




Cita mediodía mañana en el Retiro.
Escritura del mensaje secreto en los agujeros.

Luego, se levanta la rejilla y se completa el mensaje para que se vuelva natural y anodino.

Querido amigo,

Démonos **cita** pronto. Estoy encantado de nuestro encuentro hoy al **mediodía**. ¡No se desespere!

**Mañana** será un día mejor... ¡Hará buen tiempo en Madrid, y sobre todo **en el Retiro**!

Afectuosos saludos.
Caroline.

El destinatario coloca entonces su propia rejilla sobre la carta y revela el mensaje. Este dispositivo se llama la rejilla de Cardan.

Codificar un mensaje de esta manera es un ejercicio de naturaleza más literaria que científica. Sin embargo, la idea llevó a un método criptográfico complejo a base de rejillas que giran, como

veremos más adelante. Mientras tanto, las rejillas de Cardan ilustran hasta qué punto la criptografía, siempre y en todas las épocas, estimuló la imaginación. Cuando muchos solo veían un arte guerrero, otros gozaban manifiestamente de un cierto placer.