LIBROS CÚPULA

A la venta desde el 10 de noviembre de 2021

LIBROS CÚPULA

LA BIBLIA DE LOS CÓDIGOS SECRETOS

HERVÉ LEHNING

El libro más completo y actualizado sobre los métodos cifrados que han influido en la historia.

Están por todas partes: en tu tarjeta de crédito, en tu móvil o en tu módem. Se trata de los códigos secretos, un procedimiento tan antiguo como Homero, quien ya los utilizaba. César los adoraba. También los usaban los templarios o Enrique IV, quien abusó de los códigos en su correspondencia amorosa.

Han causado guerras, han hecho ganar batallas y puesto en una situación complicada a Estados Unidos (recordad el caso Snowden). Han influido en el desarrollo del comercio, estaban presentes en las intrigas palaciegas…

En estas líneas encontrarás: cifrado zigzag, código púrpura, discos de Alberti, la palabra probable de Bazeries, el cilindro de Gripenstierna, Enigma, máscaras perforables, Vernam, el sistema RSA, y algunos más.

“La Biblia de los códigos secretos” es la obra imprescindible para descifrar misterios. Es un libro eminentemente práctico, que incluye en cada capítulo una explicación y una propuesta para resolver o traducir diferentes textos a partir de la clave explicada.

PRÓLOGO

Tienes en tus manos un documento muy especial.

Hay muchísimos libros sobre códigos secretos, pero ninguno como el que te dispones a leer. Al publicar La Biblia de los códigos secretos, quisimos proponer a los lectores una obra de referencia que tuviera un doble papel. El primero, haceros viajar por el mundo misterioso e intrigante (¡e intrigas encontrarás a granel!) de los secretos de la historia, del manuscrito de Voynich del siglo xv —hasta una lengua élfica.

El mundo en el que te dispones a entrar ha sido durante mucho tiempo un privilegio de los poderosos que se disimuló al gran público a propósito. Los historiadores chocaron durante décadas contra el silencio de las autoridades cuando intentaban obtener la verdad, especialmente sobre el secreto de las transmisiones de la Primera y de la Segunda Guerra Mundial. Durante la Revolución francesa, María Antonieta mantenía su aventura oculta con el conde Axel de Fersen, escribiéndole cartas de amor cifradas, con uno de los mejores códigos de la época, incluso a pesar de que no sabía utilizarlo bien.

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.

Actualmente, los especialistas han desvelado esos secretos antiguos, pero la totalidad de los conocimientos en la materia no se han puesto a disposición pública, en todo caso como una suma rica e informativa que, de la misma manera que las pirámides que contemplaban cuarenta siglos de historia, cubre todas las épocas. ¿Sabes, por ejemplo, que, cuando el Che Guevara quiso exportar la revolución cubana a Bolivia, comunicaba con Fidel Castro con el mismo código que el utilizado entre estadounidenses y rusos? Interesante, ¿verdad? ¿O que los arcanos de la célebre Enigma, la máquina de codificar, fueron descubiertos, en parte, gracias a la traición de un funcionario alemán de la Oficina del Cifrado?

Señora, mañana a las cinco en el parque

El primer objetivo de esta obra, ampliamente enriquecida desde su primera edición en 2012 (El Universo de los códigos secretos, Ixelles), es histórico. La transcripción —el arte de encriptar los mensajes— fue diplomático y militar en primer lugar, antes de servir al secreto de los negocios a partir del siglo xix y también a un campo más anecdótico de las relaciones humanas: las correspondencias amorosas. Su contrario, la descodificación, llevó a una sofisticación de las técnicas del cifrado y, por eso mismo, a una lucha incesante entre codificadores y descodificadores. El segundo objetivo de este libro es darte las claves (en el buen sentido del término) para comprender el verdadero funcionamiento de los códigos secretos. He aquí dos ejemplos:

Hvwd sulphud iudvh kd vlgr fliudgd sru xq vlpsoh ghvsodcdplhqwr.
Rarficsed ed licifid sam res edeup esarf adnuges atse.

Estas dos frases están cifradas. Sin duda, para aquellos que ignoran todo sobre la criptografía, son incomprensibles. Sin embargo, representan los dos métodos clásicos del cifrado en sus formas más simples: la sustitución y la transposición. Cuando hayas leído este libro, descodificar estas frases te parecerá tan fácil como respirar (sí, sí, te lo garantizo).

Este libro contiene a veces algunas partes un poco técnicas, en la segunda mitad. Sin embargo, esas partes pueden hojearse sin problema para una comprensión general. Son para quienes quieran profundizar en el tema. Lo mismo sucede con los ejercicios lúdicos marcados como LQDD (lo que debemos descifrar). Los más motivados, a quienes nada asusta, ni siquiera las páginas matemáticas de los suplementos de verano de las revistas, encontrarán con qué ejercitar sus neuronas.

Errores eternos

A mi entender, esta doble preocupación, histórica y técnica, constituye la originalidad de esta obra sobre códigos secretos. No se contenta con dar importancia estratégica a las proezas de los descodificadores como Antoine Rossignol en la época clásica, Georges Painvin durante la Primera Guerra Mundial o Alan Turing durante la Segunda Guerra Mundial; también trata de mostrar el grado de ingeniosidad que desarrollaron, y cómo supieron explotar los errores de sus adversarios, errores que marcaron todas las épocas. Los métodos cambian, los errores persisten.

Al mismo tiempo, he escogido un plan estructurado alrededor de los métodos de codificación y de la historia. Para comenzar, mostraré a través de ejemplos históricos la necesidad de ocultar y el interés de descifrar las transmisiones. Luego, veremos el gran principio de la criptografía moderna, propuesto al final del siglo xix por Auguste Kerckhoffs, según el cual un sistema criptográfico no debe reposar sobre el secreto de los métodos, de los algoritmos como se lo formularía hoy, sino sobre una clave que se cambia periódicamente.

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.

Estos códigos ya existían en el Renacimiento: son los cifrados por sustitución polialfabética, como el más conocido que se atribuye a Blaise de Vigenère, pero fueron poco usados antes del siglo xix, por la dificultad de ponerlos en práctica a mano. Por eso, en aquella época se prefirieron los cifrados por sustitución monoalfabética.

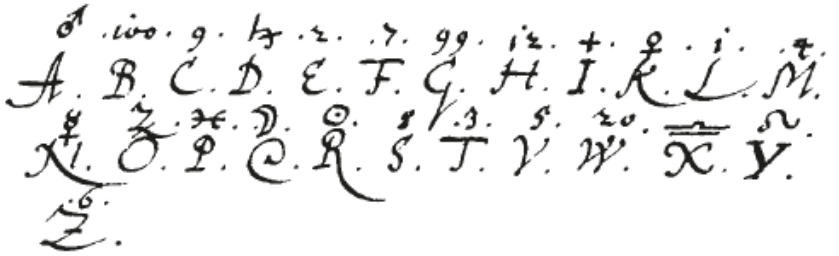
Aquí mostraré qué fáciles son de utilizar, ya sea con ejemplos inventados para la ocasión o con ejemplos de códigos reales.

Dos por dos

En el siglo xix llegó una mejoría con la idea de sustituir las letras de a dos y no individualmente. La idea avanzó en el siglo xx con los trigramas (tres por tres) y luego los poligramas, lo que marcó la primera incursión de las matemáticas como tales en la criptografía.

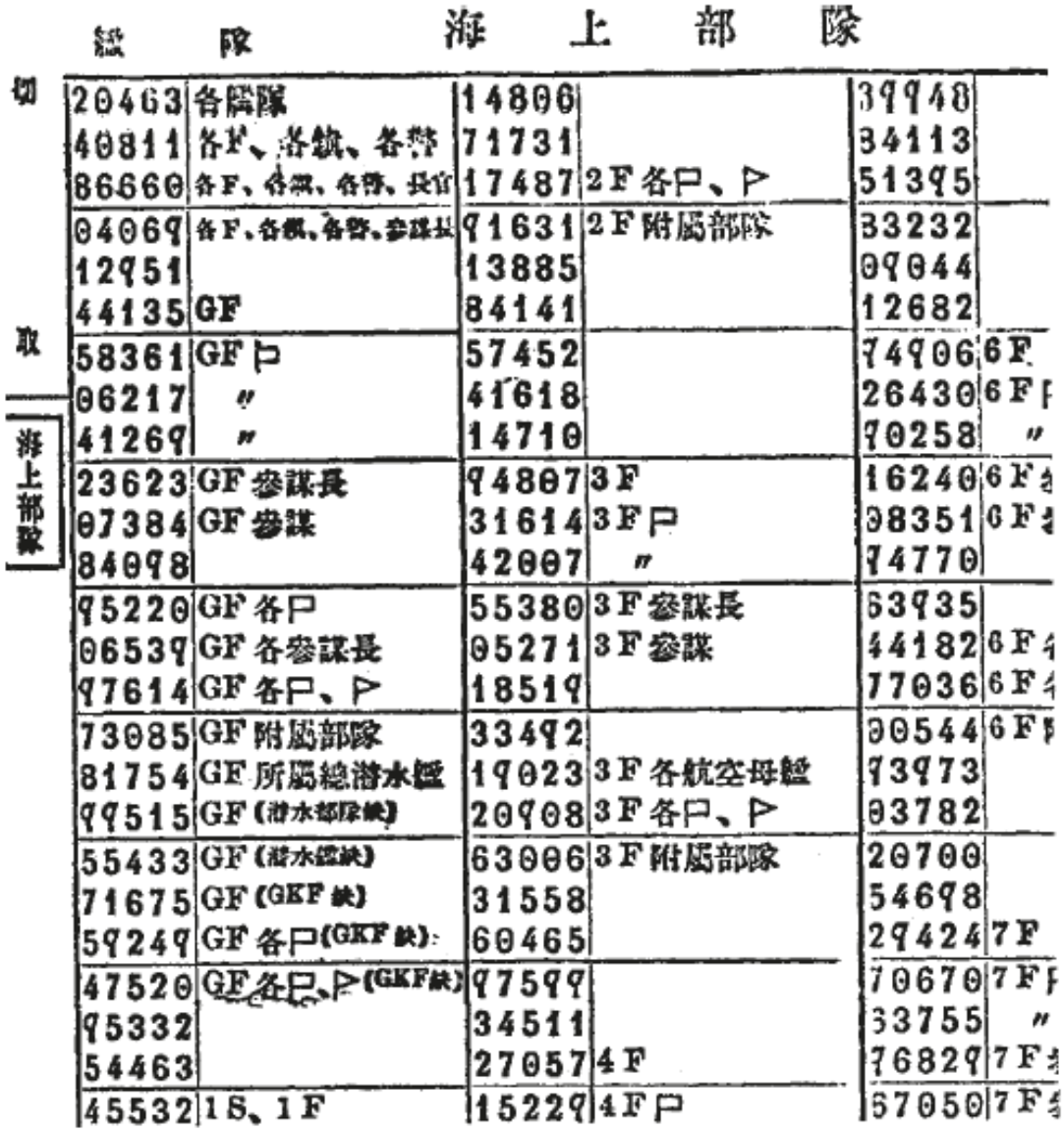
Volveré a los siglos xvii y xviii y a la revolución criptográfica iniciada por Antoine Rossignol, quien tuvo la idea de modificar las sílabas, como las letras o las palabras, por números, concibiendo de esta manera los primeros diccionarios cifrados. Bien utilizados, esos diccionarios podían resistir a los descodificadores, pero también condujeron al desastre a un ejército napoleónico poco avezado en materia de códigos secretos.

Los preludios de la Primera Guerra Mundial vieron el desarrollo de los sistemas por transposición, en los cuales se cifra un mensaje fabricando un anagrama. Combinados con sustituciones polialfabéticas, esos sistemas criptográficos fueron los mejores de la Primera Guerra Mundial. Sin embargo, los mensajes eran muy arduos tanto de codificar como de descodificar y mal adaptados a la guerra de movimiento, lo que llevó al desarrollo de máquinas de cifrar, como la Enigma del ejército alemán. Enigma producía un código polialfabético que se creía indescifrable y que, sin embargo, fue roto primero por los polacos y luego por los británicos.



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.

La utilización de máquinas de cifrado se prolongó después de la Segunda Guerra Mundial, pero las máquinas fueron reemplazadas por ordenadores. Fue entonces cuando se dieron a conocer unos métodos más matemáticos con los que, de manera sorprendente, saber cifrar no bastaba para saber descifrar. Aun si esas técnicas son seguras, están amenazadas, actualmente, por la llegada de un nuevo tipo de máquina: el ordenador cuántico. Todavía hoy continúa la lucha milenaria entre codificadores y descodificadores.



組	隊	海上部隊			
切	20463	各艦隊	14806		99948
	40811	各F、各航、各警	71731		34113
	86660	各F、各艦、各警、長官	17487	2F各P、P	51395
	04069	各F、各艦、各警、参謀長	91631	2F附属部隊	33232
	12951		13885		09044
	44135	GF	84141		12682
取	58361	GF P	57452		74906	6F
	06217	〃	41618		26430	6F
	41269	〃	14710		90258	〃
海上部隊	23623	GF参謀長	94807	3F	16240	6F
	07384	GF参謀	31614	3F P	98351	6F
	84098		42007	〃	94770	
	95220	GF各P	55380	3F参謀長	63935	
	06539	GF各参謀長	05271	3F参謀	44182	6F
	97614	GF各P、P	18519		77036	6F
	73085	GF附属部隊	33492		80544	6F
	81754	GF所属総潜水艦	19023	3F各航空母艦	93973	
	99515	GF(潜水部隊長)	20908	3F各P、P	03782	
	55433	GF(潜水艦隊)	63006	3F附属部隊	20700	
	71675	GF(GKF長)	31558		54698	
	59249	GF各P(GKF長)	60465		29424	7F
	47520	GF各P、P(GKF長)	97599		70670	7F
	95332		34511		33755	〃
	54463		27057	4F	76829	7F
	45532	1S、1F	15229	4F P	57050	7F

Extracto del libro de código JN-25B.

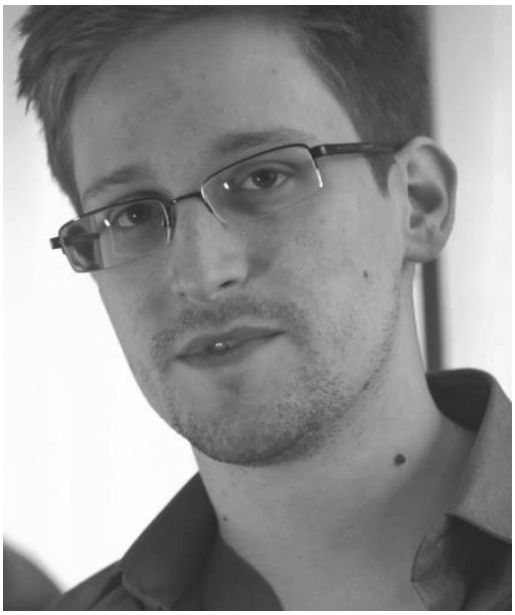
CONCLUSIÓN
Cifrados indescifrables, secretos, espionaje y terrorismo

Hemos llegado al final de este largo recorrido a través de los códigos secretos. Se desprende un punto común: cada uno está constituido de un algoritmo de cifrado y de una clave. En caso de utilización intensa, durante una guerra o, actualmente, en el comercio en internet, parece ilusorio querer conservar el algoritmo en secreto. No: la parte secreta es la clave.
Su ausencia da cifrados muy frágiles desde que su uso se extendió. Actualmente, se prefiere la clave aleatoria para que sea difícil encontrarla, y la única vía practicable para descifrarla es su búsqueda exhaustiva. La fuerza del cifrado se sostiene por el tamaño de la clave (expresada en número de bits, actualmente), pero también por su naturaleza aleatoria. En la época clásica se recurría más bien a claves fáciles de retener de memoria, para que no pudieran ser leídas por el adversario. De hecho, era una debilidad, como hemos subrayado, aun si se compensaba por los pocos medios de cálculo de la época.

(…)

La idea de que los cifrados indescifrables que hemos evocado a lo largo de este libro sean puestos a disposición de todo el mundo, evidentemente, disgusta a los servicios de inteligencia. **El gobierno estadounidense, por ejemplo, exigió recientemente a Apple que la sociedad revelara las claves de los cifrados de sus teléfonos a los investigadores del FBI.** Una solución para satisfacer el deseo del Estado de vigilar el crimen organizado y a los terroristas sería crear una tercera entidad de confianza que conservara las claves de todos, con una legislación que previera apelar a ella en el marco de algunas investigaciones.

Según el informante Edward Snowden, la estadounidense National Security Agency (NSA) prefirió adoptar otra medida y pidió a los proveedores de programas estadounidenses que crearan puertas secretas, simplemente con el objetivo de eludir sus algoritmos de cifrado. Pero esta exigencia es problemática: abre una vía de acceso para penetrar en las ciudadelas digitales. La NSA engendró de este modo una debilidad en todos los sistemas de cifrado que controla: ¿por qué los hackers se privarían de utilizarlos?



La cuestión es particularmente preocupante en el ámbito comercial. En principio, las puertas secretas puestas en marcha por los algoritmos de cifrado dejan que la NSA espíe a todo el mundo. Mientras se trate de tráficos ilegales, el objetivo es noble, pero ¿por qué la agencia estadounidense se detendría si las informaciones recolectadas confieren una ventaja industrial o comercial a una empresa estadounidense como Boeing con respecto a Airbus, por ejemplo? Por supuesto, las empresas de esta talla saben protegerse. Teóricamente. Airbus sabe muy bien hacerlo, o al menos eso afirman sus directivos. Por el contrario, las sociedades de menor envergadura no tienen medios para ofrecerse una seguridad informática digna de ese nombre. Entonces ¿qué precauciones pueden adoptar?

Para evitar el espionaje de la NSA o de otras agencias, una precaución elemental es asegurarse de que los ordenadores que contienen secretos industriales o comerciales no estén conectados a internet ni acoplados a otros ordenadores que sí están conectados a la red. Las comunicaciones importantes deben ser cifradas con la libreta de uso único preferentemente, porque es el único cifrado indescifrable, si se utiliza bien. Estas operaciones de cifrado deben hacerse en este ordenador aislado de internet; de lo contrario, un caballo de Troya podría recoger la clave en el ordenador. Asimismo, al otro lado de la transmisión, el desciframiento debe efectuarse en un ordenador aislado, única respuesta al espionaje organizado. En este contexto, la transmisión de las claves no concierne a la comunicación por internet, sino un intercambio físico. Aquí se sitúa la fragilidad del procedimiento. Otra idea es hacerse invisible en internet para conducir las negociaciones delicadas donde el secreto es necesario (de la ampliación de una fusión-compra de sociedades, por ejemplo). Se trata de convertirse en furtivo y no de cifrar los datos. ¿Cómo esconderse? Utilizando las raíces abiertas cuyos DNS (Domain Name System) no figuran en los servidores de DNS usuales. Algunas sociedades comercializan esta posibilidad, como Open-Root presidida por Louis Pouzin, uno de los padres de internet.

LIBROS CÚPULA

La guerra comercial sigue siendo una guerra y, hoy, como en los campos de batalla de la Primera Guerra Mundial, la victoria será para quien consiga proteger sus secretos.

Un álbum es un tapiz: fibras de creatividad que se tejen para crear un hermoso conjunto. Creo que el hecho de no seguir una educación superior en música fue una elección correcta en mi caso a la que he sabido sacar provecho. Si hubiese estado en el mismo nivel musical que los músicos de mayor talento, habría acabado metiéndoles mis ideas en vez de sacarles a ellos su propia brillantez. Todos los discos sonarían igual.

SUMARIO

EL AUTOR. HERVÉ LEHNING

Normalista y titular de una cátedra en Matemáticas, **Hervé Lehning** está loco por los números. Es miembro de la Asociación de conservadores de las cifras y de la seguridad de la información, y divide su tiempo entre la criptografía y la escritura.

Sus obras *Toutes les mathématiques du monde* y *La Bible des codes secrets* se han convertido en clásicos.

LIBROS CÚPULA

LA BIBLIA DE LOS CÓDIGOS SECRETOS

Hervé Lehning
Libros Cúpula, 2021
15 x 23 cm.
420 páginas
Rústica con solapas
PVP c/IVA: 25 €
A la venta desde el 10 de noviembre de 2021

Para más información a prensa:

Lola Escudero.
Directora de Comunicación Libros Cúpula
Tel: 91 423 37 11 – 619 212 722
lescudero@planeta.es