CRIPTOGRAFÍA

Un recorrido histórico por la ciencia de los mensajes secretos

Daniel Martín Reina

EDITORIAL TERRACOTA ET

Colección **Sello de Arena**

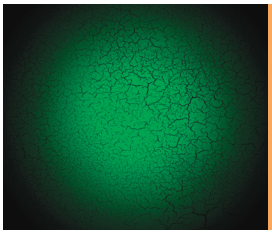
Contenido

La criptografía entra en juego

Cifrar un mensaje es como convertir una imagen en un rompecabezas.

A lo largo de muchos siglos, la esteganografía ha ofrecido ingeniosas ideas para garantizar las comunicaciones secretas. En muchos casos, estas técnicas han resultado ser muy útiles para ocultar la existencia de mensajes y cumplir con éxito su cometido. Sin embargo, la esteganografía tiene una debilidad básica: la estrategia para la comunicación secreta se basa simplemente en la ocultación del mensaje. Todo se reduce a que el mensaje pueda pasar inadvertido, ya que en el momento en que éste se descubre, el contenido de la comunicación se revela. Si los padres hojean el libro donde se ha escondido una nota de amor, si el bizcocho con los planos de la cárcel pasa por el detector de rayos X o la bolita de papel cae a los pies del profesor, sólo queda cruzar los dedos y esperar un milagro de esos que únicamente ocurren en las películas.

Por eso, al mismo tiempo que se desarrollaba la esteganografía, se produjo la evolución de la llamada criptografía, término derivado de las palabras griegas *kryptós*, que significa "escondido", y *graphein*, que significa "escribir". El objetivo de la criptografía no es ocultar la existencia de un mensaje —para eso está la esteganografía—, sino ocultar su significado. Es



decir, la criptografía se encarga de enmarañar la información de tal manera que el mensaje que se quiere transmitir no lo entienda nadie, excepto la persona a la que va destinado. De esta manera, aunque el mensaje sea interceptado, su contenido seguirá seguro. ¡Claro que eso no te salvaría de la reprimenda del profesor!

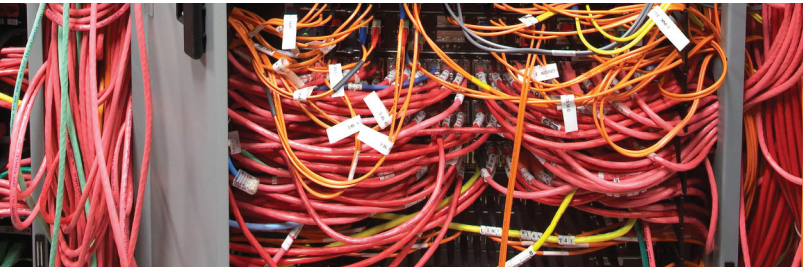
Juguemos a los espías

Cada ciencia o arte tiene su propio vocabulario y para trabajar en ellas hay que conocerlo. La criptografía no es la excepción, así que para adentrarnos en su fascinante mundo, lo primero será familiarizarnos con su lenguaje. Y qué mejor manera que con un ejemplo práctico.

La criptografía tiene un lenguaje propio, como toda ciencia o arte

Supongamos —y no es mucho suponer— que un espía que vive en un país enemigo consigue una información vital para la seguridad de ese país.

Por este motivo, decide verse lo antes posible con su contacto para facilitarle esa valiosa información. Como tiene que concretar la hora y el lugar, lo primero que debe hacer es transmitirle a su contacto el siguiente mensaje: "Cita en la puerta del parque a las nueve".



Uno de los fines de la criptografía es desordenar la secuencia de letras de un mensaje hasta el grado de hacerlo ininteligible.

Como es lógico, el espía debe tomar sus precauciones. No quiere enviar el mensaje tal cual, pues una tercera persona que lo intercepte puede entenderlo fácilmente. Por ejemplo, podría ser que el teléfono estuviera intervenido. El espía y su contacto deben establecer una comunicación secreta, así que eligen la criptografía para mantener la privacidad de la misma. La criptografía los ayudará a ocultar el significado del mensaje. ¡Por algo se dice que la criptografía es el lenguaje de los espías!

La criptografía se encarga de enmarañar la información para que nadie la entienda

En la jerga de la criptografía, la información original que se quiere proteger se llama texto llano; en el ejemplo actual, el texto llano sería: "Cita en la puerta del parque a las nueve". Para poder esconder su significado, el espía debe cifrar el texto. El cifrado es el proceso que transforma el texto llano en otro que sólo puedan entender las personas que estén autorizadas para ello. A ese texto se le llama texto cifrado o criptograma. El cifrado requiere un conjunto de reglas preestablecidas entre quienes se comunican, que se conoce como algoritmo de cifrado, y una clave que define los detalles exactos del cifrado.

El éxito de miles de intercambios de comunicaciones secretas se debe a la criptografía. Los espías no pueden quejarse.

El espía cifrará el mensaje de la siguiente manera: sustituirá cada letra del abecedario llano —el que se usa comúnmente— con otra de un alfabeto cifrado, y luego aplicará esta correspondencia al texto llano. Esto es el algoritmo de cifrado, que explica el procedimiento general. Pero no lo especifica exactamente, porque no se sabe cuál de todos los alfabetos posibles es el cifrado. Para eso está la clave. En este caso, el espía y su contacto han decidido que a cada letra

Sustituyendo letras

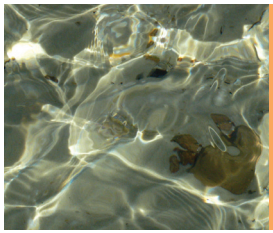
Columnas romanas.

En el siglo I a.C., el Imperio Romano se extendía por el mar Mediterráneo, desde el sur de Hispania hasta la actual Turquía, en Asia, pasando por la costa norte de África. Pero eso no era suficiente para el ambicioso cónsul de Roma en la Galia, quien pretendía someter también el territorio de lo que hoy es Francia, Bélgica y parte de Alemania. Su nombre era Cayo Julio César, quien más tarde pasaría a la historia por sus conquistas y por ser asesinado por un grupo de senadores, entre los que se encontraba su propio hijo, Bruto.

Julio César empleó la criptografía para sus fines de conquista

Entre 58 y 51 a.C., Julio César emprendió una serie de campañas para someter a los pueblos galos. Estas batallas pasaron a la historia como la Guerra de las Galias. En una de ellas, una legión al mando de Quinto Cicerón fue asediada por unas tribus galas que se habían rebelado contra el dominio romano. Cuando César recibió la noticia, decidió acudir con dos de sus legiones en su ayuda y envió también a un

soldado de su caballería para llevar a Cicerón un mensaje. En caso de que no pudiera dárselo en mano, el mensajero tenía la orden de arrojarlo dentro del campamento, atándolo a una flecha. Al acercarse al campamento de Cicerón, el mensajero comprobó que todas las sendas estaban tomadas por el enemigo, por lo que, temiendo ser descubierto, disparó la flecha según las instrucciones recibidas. Finalmente, un soldado reparó en la presencia del mensaje y se lo llevó a Cicerón, quien estaba entonces a punto de rendirse. Después de leerlo, Cicerón convocó a las tropas y repitió el mensaje en voz alta, lo que provocó un gran estallido de alegría.



El contenido de la carta, motivo del júbilo de Cicerón y sus soldados, era el siguiente:

TVSQXS PI ZIVEW GSQ PMW OIKMSQIW

La cifra de César

Podría parecer que Cicerón y toda su legión sufrieron un ataque de locura provocado por el largo asedio, pero no se trataba de eso. Lo que ocurrió es que Julio César había utilizado la criptografía para asegurar la privacidad de la comunicación, por si el mensaje caía en manos enemigas. Al parecer, según cuenta Suetonio en su libro *Vida de los doce Césares,* era práctica habitual de Julio César emplear la escritura secreta, e incluso llegó a crear su propia cifra, que consistía sencillamente en sustituir cada letra del mensaje por la letra que está tres lugares después en el alfabeto, tal y como se muestra a continuación:

Durante la Guerra de las Galias, Julio César utilizó la criptografía para comunicarse con sus generales.

Alfabeto llano:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z
Alfabeto cifrado:	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

En su honor, esta cifra se conoce como la cifra de César. Y de la misma manera que se ha desplazado cada letra tres lugares, podrían haber sido dos, cinco o 14: cualquier desplazamiento entre uno y 26 lugares hubiese sido igualmente válido. Por lo tanto, existen 26 claves distintas para la cifra de César. Desplazar el alfabeto 27 posiciones no sería nada práctico, porque en tal caso el resultado sería el mismo alfabeto llano.

Por ejemplo, si para distinguir a César quisiéramos cifrar su famosa frase *Veni, vidi, vici,* el resultado sería YHPL, YLGL, YLFL. Ahora bien, si César hubiera usado su cifra en el mensaje que envió a Cicerón, pero desplazando cada letra cuatro lugares en vez de tres, ¿podrías decir cuál era entonces el contenido del mensaje que provocó la alegría de los soldados?

Estampilla de correos de Italia con la efigie de Julio César.

La cifra de César sustituye cada letra del mensaje por la letra que se encuentra tres lugares adelante

Para ayudarte, puedes construir tu propio instrumento para escribir y leer mensajes con la cifra de César. Sólo tienes que recortar dos círculos, uno más grande que el otro, y sobre una cartulina juntarlos con una tachuela por sus centros. Escribe, en minúsculas y en color morado sobre el círculo pequeño, el alfabeto llano, y en mayúsculas y en color naranja sobre el grande, el alfabeto cifrado. Al girar una rueda sobre la otra se emparejan las letras de los círculos,

Códigos y cifras

Información representada por ideogramas chinos.

El término "código" tiene un significado muy amplio en el lenguaje cotidiano, que depende mucho del contexto en el que se use. Por ejemplo, un conjunto de normas de conducta puede definirse como un código de honor o un código ético. La palabra "código" también puede referirse a una recopilación de leyes, como el código civil o el código penal. Pero, en general, un código suele ser un símbolo, una señal o cualquier forma de representar una información determinada con alguna intención.

El ejemplo más básico de código es el lenguaje. Todas las palabras que forman una lengua codifican información. Las letras *g*, *a*, *t* y *o* aisladas no nos dicen nada, pero si las juntamos hacen referencia a un animal peludo de cuatro patas, amante de cazar ratones y que maúlla. Si al leer esas cuatro letras juntas piensas en un gato de carne y hueso, significa que entiendes el código. En China utilizan otra lengua —otro código— y por lo tanto no entienden el significado de "gato". Ellos tienen otra palabra para designar a ese animal. ¡Pero no me preguntes cuál es!

Los códigos se usan a diario como una forma rápida y sencilla de enviar información. Por ejemplo,

sabes que si un semáforo está en verde, puedes pasar; si está en rojo, tienes que detenerte, y si está en amarillo, ¡ten cuidado, que se va a poner en rojo!

Con el tiempo, el hombre ha ideado muchos otros códigos para simplificar y facilitar su vida. Así, el código de barras permite no sólo leer el precio de un producto cuando el empleado lo pasa por el lector, sino también localizar cualquier artículo en cualquier parte del mundo, de manera rápida y sin posibilidad de error. El código postal identifica una zona geográfica mediante una serie de números, facilitando así que las cartas lleguen más rápido a tu casa. Y así podríamos seguir enumerando códigos: las señales de tráfico, el código de banderas que usaban los marineros, etcétera. En definitiva, existen infinidad de códigos que afectan de una u otra manera nuestra vida, aunque muchas veces no nos demos cuenta. ¿Se te ocurren más a ti?

Códigos *vs.* cifras

Toda esa información codificada que acabamos de ver está al alcance de cualquiera. A veces, sin embargo, es necesario que sólo determinadas personas entiendan la información que se quiere enviar. En tal caso, los códigos también nos pueden servir para

Vivimos en un mundo repleto de códigos simples y otros mucho más complejos.

La invención del telégrafo

Los postes del telégrafo modificaron el paisaje.

Cada civilización desarrolla un sistema para comunicarse a larga distancia. Los destellos de un espejo desde una torre árabe, el sonido de un tambor africano o un cuerno vikingo, las señales de humo de los indios americanos: todas son formas primitivas, a la vez que ingeniosas, de comunicación a distancia.

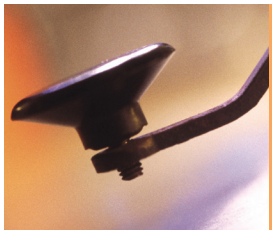
Con el tiempo, el hombre ha ido perfeccionando sus técnicas de comunicación. Esto significa llegar más lejos y más rápido. Al descubrirse la electricidad en el siglo XVIII, se buscó la forma de utilizar señales eléctricas para enviar mensajes. Esta búsqueda cristalizó a principios del siglo XIX con la invención del telégrafo, el primer aparato que nos permitió comunicarnos instantáneamente, sin importar las distancias.

El telégrafo revolucionó las comunicaciones en el mundo, pero también supuso un quebradero de cabeza más para los gobiernos y otras entidades que debían proteger el contenido de sus mensajes. Cualquier mensaje pasaba por las manos de un telegrafista quien, para poder enviarlo, tenía que leerlo. Por lo tanto, los telegrafistas tenían acceso a todos los mensajes y, aunque estaban bajo juramento de guardar secreto, existía la posibilidad de que cualquiera de

ellos revelase información confidencial al enemigo.

Pero el telégrafo también afectó al ciudadano común. En su caso, más que la seguridad, estaba en juego la privacidad. El telegrafista podía tener acceso a secretos íntimos que su dueño no estaba dispuesto a compartir con terceras personas, y menos aún con el telegrafista de su ciudad.

En ambas circunstancias, la solución era la misma: la criptografía.



La cifra ADFGVX

Además de revolucionar las comunicaciones, la invención del telégrafo supuso un nuevo impulso para la criptografía, gracias al cual se desarrollaron más cifras. Quizá la más famosa de todas sea la cifra ADFGVX, una hábil mezcla de sustitución y transposición. Se llama así porque el texto cifrado contiene sólo estas seis letras. El motivo de esta elección es que, cuando se transforman en las líneas y puntos del código Morse, estas seis letras son muy diferentes entre sí, lo que hace más difícil equivocarse durante la transmisión de un mensaje.

Si quieres utilizar esta cifra, debes empezar dibujando un cuadrado de 6 por 6 casillas y rellenar las 36 casillas resultantes con las 26 letras del abecedario (sin la *ñ*) y los diez dígitos del 0 al 9, en el orden que quieras. Como se muestra en la siguiente figura, cada línea y cada columna de la cuadrícula se identifica con una de las seis letras, *A*, *D*, *F*, *G*, *V* o *X*.

	A	D	F	G	V	X
A	w	5	h	0	9	7
D	2	c	f	g	k	3
F	a	v	m	t	j	b
G	y	8	d	s	6	q
V	4	r	u	x	1	l
X	n	z	o	i	p	e

Joven aprendiz utilizando un telégrafo.

A: ·—

D: —··

F: ··—·

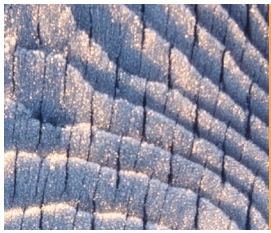
G: ——·

V: ···—

X: —··—

Código Morse

Babbage *vs.* Vigenère



Desde el momento en que la cifra de Vigenère se dio a conocer, fue llamada la "cifra indescifrable", debido a su enorme fortaleza. El escritor Lewis Carroll —también criptógrafo, como ahora sabemos— llegó a afirmar que la cifra de Vigenère era imposible de descifrar sin conocer la palabra clave. Como él, la mayoría de los criptoanalistas habían abandonado toda esperanza de llegar a descifrar la cifra de Vigenère.

Puede que muchos se sintieran derrotados, pero no era el caso de Charles Babbage, polifacético científico inglés. Inventor del velocímetro y del primer aparato para examinar el interior del ojo humano, el oftalmoscopio, fue también uno de los fundadores de la Real Sociedad Astronómica inglesa, en 1820. Durante su vida, escribió sobre temas tan diversos como ajedrez, geología, eclipses solares, economía, submarinos, estadística y, por supuesto, criptografía.

La fascinación de Babbage por la criptografía se remonta a los días de su juventud, y con el paso de los años se fue ganando la fama de ser un reputado criptoanalista. Finalmente, se propuso intentar lo que nadie había conseguido hasta entonces: vencer a Vigenère.

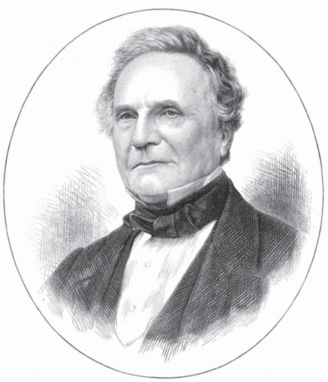
Fortaleza en España.

Recordemos que la fuerza de la cifra de Vigenère se basa en que una misma letra se puede cifrar de distintos modos y, a su vez, la misma letra del mensaje cifrado puede emparejarse con más de una del texto llano. Para refrescar la memoria, cifremos con la clave LUIS el título de un relato de Jorge Luis Borges: "Los dos reyes y los dos laberintos".

Clave:	L U I	S L U	I S L U I	S	L U I	S L U	I S L U I S L U I S
Texto llano:	L o s	d o s	r e y e s	y	l o s	d o s	l a b e r i n t o s
Texto cifrado:	V J A	V Z N	Z W J Y A	Q	V J A	V Z N	S S M Y Z A X Ñ W L

Efectivamente, la primera *s* se cifra como *A*, mientras que la segunda lo hace como *N*. A su vez, las primeras dos *l* se cifran como *V*. Sin embargo, si te fijas un poco en el texto cifrado, podrás observar un hecho que llama poderosamente la atención. La palabra "los", que aparece dos veces, se cifra en ambos casos de la misma manera, *VJA*. La causa de esta repetición es que la distancia entre los dos *los* es de ocho letras, que es un múltiplo de la longitud de la clave, de cuatro letras. Esto hace que las dos palabras se cifren de acuerdo con las mismas letras de la clave, *LUI*, dando lugar a la misma palabra cifrada.

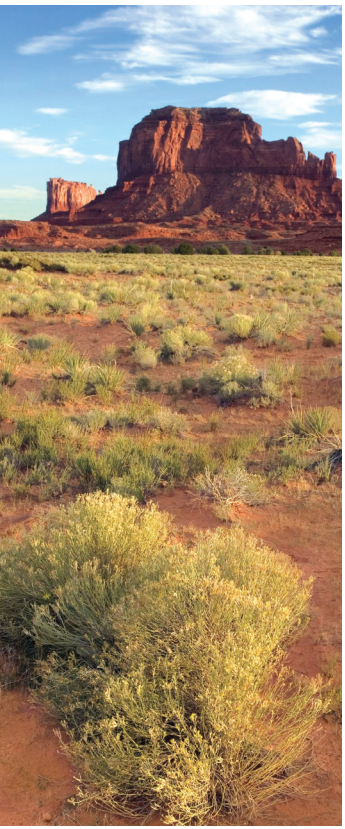
Lo que ocurre es que la cifra de Vigenère es polialfabética, pero no tanto. De los 26 alfabetos de la *tabula recta*, sólo se utilizan los que son definidos por las letras que forman la palabra clave. Por lo tanto, cada letra sólo se puede cifrar de tantas maneras posibles como alfabetos cifrados se utilicen, o lo que es lo mismo, como letras tenga la palabra clave. En el ejemplo, la *e* sólo se puede transformar en *O* (si se usa la *L),* como *Y* (si se usa la *U),* como *M* (si se usa la *I)* o como *W* (si se usa la *S).*



Charles Babbage vivió fascinado por la criptografía.

Pero aún hay más. Los alfabetos cifrados definidos por la clave no se pueden combinar como uno quie-

El código navajo



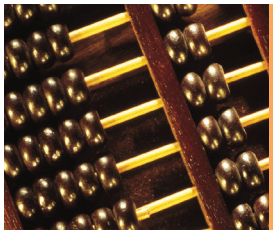
Paisaje característico del territorio navajo, en el suroeste de Estados Unidos.

Uno de los episodios más singulares de la Segunda Guerra Mundial tiene como protagonista a una tribu india descendiente de los apaches: los navajos. Su participación en la guerra fue muy limitada en cuanto a número: en 1942 había apenas 29 navajos en servicio. Sin embargo, su contribución fue vital para su país y salvaron la vida de incontables soldados aliados. Si Alemania creía tener una cifra invencible en la máquina Enigma, Estados Unidos demostró que su código navajo sí que era inexpugnable.

Una misma vocal en lengua navaja puede tener hasta diez sonidos distintos

La idea de usar la lengua navaja como código secreto fue de Philip Johnston. Hijo de una pareja de misioneros, Johnston creció en la reserva de los indios navajos en Arizona. Cuando era un niño aprendió la lengua de los navajos y con apenas cinco años ya servía de traductor a sus padres. A los nueve años, en vez de andar en bicicleta y jugar al beisbol, acom-

pañó como intérprete a una delegación de navajos enviada a Washington D.C., a reclamar los derechos de los indios. Johnston era una de las contadas personas en el mundo que conocía la lengua de los navajos sin ser uno de ellos.



Durante la Segunda Guerra Mundial, los criptoanalistas japoneses estaban metiendo en apuros a Estados Unidos en la campaña del Pacífico. Johnston, que era un veterano de la Primera Guerra Mundial, pensaba que la lengua navaja sería casi imposible de descifrar para el enemigo. Los indios navajos vivían en grupos aislados, por lo cual era muy difícil acceder a ellos. Además, esta lengua no estaba escrita y es tan compleja que es muy difícil de aprender. Una sola vocal puede tener hasta diez sonidos diferentes. Conocer otras lenguas indias tampoco es muy útil para aprender navajo, porque la lengua navaja es muy diferente del resto.

Finalmente, Johnston ofreció su idea al ejército y, a pesar de las dudas iniciales, consiguió hacer una demostración. En condiciones normales, cifrar un mensaje letra a letra, enviarlo y volver a descifrarlo letra a letra era un proceso que podía tardar media

El equipo navajo envió incontables mensajes secretos en su idioma.