Introducción

La necesidad de guardar secretos

Desde siempre, el hombre ha sentido la necesidad de tener secretos y guardarlos a buen recaudo. Tan solo en algunas situaciones deseaba compartirlos con determinados amigos o aliados, asegurándose de que aquellos no eran conocidos por terceras partes.

Esta necesidad ha hecho que, a lo largo de la historia, el hombre haya aguzado su ingenio con el fin de proteger determinada información, inventando métodos que le permitieran ocultarla o convertirla en secreta ante los que consideraba enemigos. A la vez, debería poder acceder a ella en caso de necesidad o permitir que, bajo determinadas condiciones, sus aliados pudieran conocerla.

Tradicionalmente, existen dos formas de lograr este objetivo. Una de ellas consiste en ocultar el propio hecho de la existencia de un mensaje secreto, de modo que si se desconoce que tal mensaje existe, un adversario no tendrá la preocupación de buscarlo. La otra es la de llevar a cabo diferentes modificaciones o transformaciones en el mensaje para que, si este cae en manos no deseadas, sea imposible conocer la información a que hace referencia. Además, tales transformaciones deben permitir que el mensaje pueda ser

recuperado más adelante, bien por el propietario, bien por el destinatario.

Ocultamiento de mensajes: esteganografía

El método de guardar secretos que consiste sencillamente en ocultar el mero hecho de la existencia de un mensaje se conoce como *esteganografía* (Van Tilborg *et al.*, 2005). El término procede de las palabras griegas *steganos*, que significa "que cubre", "que protege", "cubierto", y *graphein*, que es "escribir". Así pues, la esteganografía trata de cómo escribir un mensaje de modo que quede encubierto u oculto.

Uno de los primeros métodos esteganográficos documentados fue mencionado por Heródoto (484-425 a.C.) en *Las Historias* (Heródoto, 1985). Este señala que Demarato (515-491 a.C.), para avisar a sus conciudadanos griegos de los planes de invasión de Jerjes (519-465 a.C.), allá por el año 480 a.C., limpió la cera de una tablilla, escribió sobre la madera el mensaje y volvió a colocar la cera, de modo que la tablilla parecía estar sin escribir. Al llegar la tablilla a su destino, bastó con quitar la cera para leer el mensaje.

El mismo Heródoto narra otro sistema para la ocultación de un mensaje, posiblemente más curioso que el anterior. En este caso se trataba de cómo Histaiaeo (o Histieo, c.a. 494 a.C.) pidió a Aristágoras de Mileto (finales del siglo VI-principios del siglo V a.C.) que se rebelara contra el rey de Persia. Histaiaeo afeitó la cabeza del que iba a ser el mensajero, escribió el mensaje en su cabeza y cuando le creció el pelo, lo envió a su destino. Al llegar, le volvieron a afeitar la cabeza con lo que el mensaje quedó al descubierto sin que nadie tuviera conocimiento siquiera de la existencia del mismo. Detalles como estos ponen de manifiesto que la medida del tiempo en aquella época no era la misma que la empleada hoy en día.

A lo largo de la historia se han utilizado otros muchos métodos esteganográficos. Así, se sabe que en la antigua China se escribían mensajes sobre seda fina; luego se hacía

una pequeña pelota con la seda, que era envuelta en cera y que el mensajero se tragaba.

Otro método utilizado a lo largo de la historia ha sido el uso de las denominadas "tintas invisibles". En este caso se trata de escribir el mensaje con una tinta que desaparece y que lo vuelve invisible.

Plinio el Viejo (o Gayo Plinio Segundo, 23-79) señaló que la leche de la planta *Tith ymalus* podía utilizarse como tinta invisible, puesto que al secarse se volvía transparente, mientras que si se calentaba reaparecía con un tono marrón (Plinio, 2007). Por su parte, Giovanni Battista della Porta (o Giambattista della Porta, 1535-1615) describió cómo era posible ocultar un mensaje dentro de un huevo cocido. Para ello bastaba con elaborar una tinta a base de alumbre y vinagre y luego escribir en la cáscara del huevo. La tinta atraviesa la cáscara y deja el mensaje en el huevo, de modo que solo es posible leerlo si este se pela.

Otro método para ocultar un mensaje consiste en hacerlo formar parte de otro mensaje, de modo que el primero pase inadvertido dentro del segundo.

Uno de los ejemplos más conocidos de la literatura española es el de los acrósticos de *La Celestina* (De Rojas, 2013), es decir, los versos cuyas letras iniciales forman un mensaje; en este caso, el nombre del autor de la obra: Fernando de Rojas (1470-1541):

> […]
> **F**uertes más que ella por cebo la llevan:
> **E**n las nuevas alas estaba su daño.
> **R**azón es que aplique a mi pluma este engaño,
> **N**o disimulando con los que arguyen;
> **A**sí que a mí mismo mis alas destruyen,
> **N**ublosas e flacas, nacidas de hogaño.
> **D**onde esta gozar pensaba volando,
> **O** yo aquí escribiendo cobrar más honor,
> **D**e lo uno y lo otro nació disfavor:
> **E**lla es comida y a mí están cortando

Reproches, revistas e tachas. Callando
Obstara los daños de envidia e murmuros;
Y así navegando, los puertos seguros
Atrás quedan todos ya, cuanto más ando.
Si bien discernís mi limpio motivo,
[…]

Este método, con bastante mayor sofisticación, aparece con frecuencia en las películas de espías, de modo que para leer un mensaje hace falta un libro o texto de referencia y una guía o clave de lectura. Esta guía suele ser una colección de grupos de tres números que hacen referencia a la página, al número de línea en esa página y a la posición de la palabra en dicha línea. En algunas ocasiones esta forma de ocultar un mensaje se conoce como "canal subliminal".

Más recientemente, la esteganografía ha sido utilizada por los agentes de los servicios secretos de algunos países para enviar información de forma secreta. En esta ocasión, el avance de la tecnología permitía microfilmar documentos, de modo que el microfilme era pegado en cartas ordinarias sustituyendo el punto de una *i*, de una *j* o un punto de fin de frase. Parece ser que el FBI descubrió por primera vez un micropunto en 1941, a partir de un soplo que informaba que debían buscar un pequeño brillo en una carta procedente de agentes alemanes en Latinoamérica.

Hoy en día, el uso de la esteganografía se ha generalizado con el fin de proteger determinados mensajes o información relacionada con estos, aunque se conozca su existencia. Se trata de incluir información adicional al mensaje e íntimamente ligada al mismo de modo que se detecte cualquier modificación del mensaje, en general, para proteger su contenido.

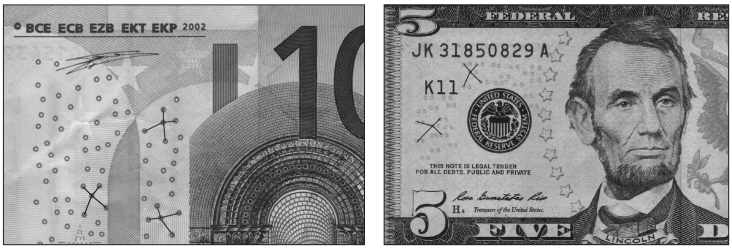
Así, los billetes de banco, cheques o archivos multimedia, por ejemplo, incluyen información no visible que permite protegerlos contra su falsificación o duplicación indebida.

Uno de los usos más sorprendentes para la protección de los billetes de cualquier denominación de euro (y actualmente

de otros muchos billetes de curso legal) es la impresión en cada uno de ellos (a lo largo de todo el billete y en cualquier posición) de una configuración especial de cinco pequeños círculos denominada *eurión* (una forma muy esquemática de la constelación de Orión) con un color determinado en cada billete (figura 1).

Figura 1

Representación del eurión en billetes de curso legal.



Fuente: Luis Hernández Encinas.

Esta configuración es detectada por todas las fotocopiadoras de color modernas[1], de modo que si se intenta fotocopiar un billete que lleve impresa esta configuración la fotocopiadora mostrará en su pantalla un aviso señalando que se intenta fotocopiar un billete y que la acción no se completará por ser ilegal. De hecho, la medida es tan eficaz que si se intenta fotocopiar una hoja de papel en blanco con un eurión impreso, de un color adecuado, se producirá el mismo resultado que si se tratara de un billete de curso legal.

Transformación de mensajes: criptografía

El otro medio para lograr ocultar información, de modo que pueda ser recuperada por quien la emite o por su legítimo destinatario, pero que a la vez impida a un oponente acceder a ella, consiste en transformar el contenido de un mensaje

1. Véase http://www.rulesforuse.org/pub/index.php?currency=eur&lang=es

siguiendo determinadas reglas (en general, el mensaje original se suele denominar "mensaje en claro" o "texto claro"). Estas reglas modifican la información del mensaje, de modo que, aplicando las reglas inversas o adecuadas, será posible recuperar el mensaje original.

Este procedimiento de transformar un mensaje en claro en otro ininteligible, llamado *criptograma* o mensaje cifrado (texto cifrado), se conoce como *criptografía*, término que procede de la palabra griega *kryptos*, cuyo significado es "secreto", "oculto" o "disimulado". Así pues, el objetivo de la criptografía es permitir el intercambio de información haciendo el mensaje ilegible sin ocultar la existencia de dicho mensaje (Van Tilborg *et al.*, 2005).

El emisor del mensaje debe asegurarse de que las reglas que utiliza no serán fácilmente deducibles o supuestas por un atacante. En otro caso, el sistema utilizado no tendrá la validez que se espera de él y su uso perjudicará al emisor y al receptor.

De forma más general, el objetivo de la criptografía es garantizar que la información transmitida (o almacenada) posea las siguientes tres cualidades: *confidencialidad*, *integridad* y *autenticidad*. La confidencialidad consiste en lograr que la información permanezca secreta y solo sea conocida por quienes tienen autorización para ello. Por su parte, la integridad hace referencia a la necesidad de que la información no haya sido manipulada ni alterada desde su origen a su destino. Finalmente, la autenticidad obliga a que tanto el origen como la información transmitida sean auténticos, es decir, no se produzcan suplantaciones. Otras cualidades relacionadas con la información que considera la criptografía son su *disponibilidad* y *no repudio*.

El estudio para intentar alterar alguna de las cualidades de la información, anteriormente mencionadas, que persigue la criptografía se conoce como *criptoanálisis*. El objetivo de un criptoanalista es conocer la información original que el emisor transmite al receptor, para lo cual utilizará todos los medios a su alcance.

La unión de la criptografía y el criptoanálisis se conoce como *criptología*, si bien, por abuso de lenguaje, se suele hablar de criptografía para referirse a ambos conceptos.

A lo largo de la historia, las reglas criptográficas de transformación de los mensajes han ido modificándose, haciéndose cada vez más complejas y sofisticadas. Esta evolución ha corrido pareja a la de la tecnología. De hecho, hoy en día todos los métodos criptográficos hacen uso de los ordenadores, pues en caso contrario es muy probable que el sistema utilizado pueda ser vulnerado o roto y el contenido del mensaje conocido por un atacante o adversario.

Estas reglas de transformación suelen hacer uso de tres métodos diferentes: transposición, sustitución y cifrado.

El *método de transposición* consiste en barajar o recolocar las letras del mensaje, obteniendo uno o varios criptogramas (también llamados, en este caso, anagramas). Si el mensaje es corto, por ejemplo una única palabra, el método es inseguro porque solo hay unas pocas formas de combinar las letras de la palabra (como máximo el número de permutaciones de las letras). Sin embargo, el método se hará más complicado a medida que aumente la longitud del mensaje. No obstante, si se desea que el destinatario pueda recuperar la información, el anagrama no puede haberse generado al azar, sino siguiendo una regla, lo que facilita, a la vez, su análisis.

Para simplificar la notación y mientras no se diga lo contrario, los mensajes originales se escribirán en minúsculas, mientras que los transformados se escribirán en mayúsculas; además, las claves se escribirán en mayúsculas y en letra cursiva. Finalmente, no haremos uso ni de los espacios ni de los acentos para no dar pistas en los mensajes. Por ejemplo, el mensaje "criptografía" podría ser transformado, mediante transposición, en alguno de los siguientes, tengan sentido o no: "ATACIRFOGRIP, FATIGARPICOR, GRAFICOTRIPA, CRIPTAGARFIO". El número de posibles criptogramas que se pueden obtener a partir del mensaje original es de 59.875.200 (permutaciones de 12 letras de las que se repiten varias de ellas). Este número parece elevado,

pero con la ayuda de un ordenador es fácil obtener todos los criptogramas. Luego, bastará con buscar cuáles de ellos tienen sentido o, de forma más sencilla aún, buscar cuáles están en un diccionario. Sin embargo, si el mensaje fuera "consejosuperiordeinvestigacionescientificas", el número de posibles transposiciones a que da lugar este mensaje es mucho más elevado. De hecho, es el número de permutaciones de 43 letras entre las que hay varias repetidas. Tal número, en este caso, es:

$$1.254.523.149.834.885.970.632.671.420.998.656.000.000 \approx 1{,}2 \cdot 10^{39}$$

Este número tiene 40 dígitos y para hacernos idea de cuán grande es podemos considerar las siguientes cifras: la población mundial puede estimarse en unos 7.000 millones de personas y la edad del universo, es decir, el tiempo transcurrido desde el Big Bang hasta ahora, es de unos 13.800 millones de años. Con estos datos, si una persona pudiera leer en un segundo una transposición de las posibles y si todas las personas del mundo trabajaran día y noche sin descanso, el número de transposiciones que habrían leído desde el principio del universo sería 7.000.000.000·13.800.000.000·365·24·60·60, es decir, habrían leído 3.046.377.600.000.000.000.000.000.000 transposiciones. Dividiendo el número de posibles transposiciones del mensaje anterior entre el número de transposiciones leídas por toda la población mundial desde el Big Bang, obtendríamos un valor de 411.808.158.600. En resumen, toda la población del universo debería repetir más de 411.000 millones de veces la lectura de una transposición por segundo durante toda la vida del universo para agotar toda la lista.

El destinatario legal podría, sin embargo, recuperar el mensaje original fácilmente a partir del transformado si supiera cómo se transformó el primero en el segundo, dado que bastaría con aplicar la transformación inversa.

Una de estas transformaciones podría ser una sencilla regla, fácil de recordar, como es la conocida como "regla del

riel" de tres filas (de forma análoga se podrían considerar rieles de dos filas, cuatro, etc.). Esta regla consiste en escribir el mensaje alternando sus letras en tres filas consecutivas y separadas, de la siguiente forma:

c	s	o	p	i	d	n	s	g	i	e	i	t	i	s										
o	e	s	e	o	e	v	t	a	o	s	e	i	c											
n	j	u	r	r	i	e	i	c	n	c	n	f	a											

De este modo, el mensaje transformado sería en realidad el siguiente: "CSOPIDNSGIEITISOESEOEVTAOSEICNJURRIEICNCNFA".

Para recuperar el mensaje original bastaría con aplicar la regla inversa. Ahora bien, si el adversario supiera o tuviera motivos para pensar que la transposición anterior se ha logrado mediante algún sistema relacionado con la regla del riel, el número de posibles transformaciones que tendría que analizar sería mucho menor y sus posibilidades de éxito mucho mayores.

El "método de sustitución" cambia unas letras del mensaje por otras letras o por símbolos. De este modo, salvo que se conozca la equivalencia entre las primeras y los últimos, el mensaje original puede resultar muy difícil de recuperar. Por el contrario, si se dispone del diccionario de sustitución, este proceso será relativamente fácil.

Un sencillo ejemplo de método de sustitución puede ser el de seguir la regla dada por el siguiente diccionario:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
\	·	$	%	&	/	(	+	)	=	(	-	)	{	*	}	0	1	2	3	4	5	6	7	8	9

De este modo, el mensaje "criptologia" se transforma en el siguiente: $1)}3*-*()\

Parece obvio que, salvo que se conozca el diccionario utilizado, no será fácil recuperar el mensaje original. Así pues, es importante que tanto el remitente del mensaje como su

destinatario tengan la misma copia del diccionario y que la guarden en lugar seguro para evitar su pérdida o robo.

Finalmente, el "método de cifrado" consiste en codificar las letras del mensaje de modo que se transformen en números y luego efectuar determinadas operaciones matemáticas con ellos. Parece claro que para recuperar el mensaje original se deberán realizar las operaciones en orden inverso (o las operaciones inversas a las originales) y luego descodificar los números obtenidos para transformarlos en letras y poder leer el mensaje.

Debe recordarse que la Real Academia Española (RAE, 2015) define, en su primera acepción, el verbo *cifrar* como "transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje cuyo contenido se quiere ocultar". En este caso, la clave serán las operaciones realizadas y su orden.

Por otra parte, *codificar* es "transformar mediante las reglas de un código la formulación de un mensaje". Debe notarse que en este caso no se considera que esta transformación requiera ser secreta. De hecho, la mayoría de los códigos que empleamos no tiene como finalidad ser secreto, sino escribir la información de otro modo, con determinados objetivos, según el código empleado: código Morse (para ser enviado por telégrafo), Braille (para ser leído por invidentes), de circulación (para identificar mediante dibujos las pautas a seguir en el tráfico), de barras (para su lectura por medios electrónicos), etc.

Podría pensarse que el método de cifrado es una forma particular del método de sustitución, donde se cambian letras por números. Sin embargo, aquí los consideramos distintos porque existen métodos de sustitución que hacen exactamente eso: cambiar letras por números, pero en la cifra se va más lejos: primero se codifican las letras en números (no de forma secreta) y luego se realizan determinadas operaciones matemáticas que son el fundamento de la seguridad del método.

A modo de ejemplo, para cifrar el mensaje "codigo" se puede codificar primero dicha palabra siguiendo el Código

Estándar Estadounidense para el Intercambio de Información (*American Standard Code for Interchange of Information*, ASCII) y luego cifrar el número resultante llevando a cabo diferentes operaciones. El ASCII extendido codifica letras, números y caracteres mediante 8 bits (lo que da lugar a 2^8 = 256 caracteres codificables). Algunos de estos caracteres y su codificación en binario y decimal se presentan en la tabla 1.

Tabla 1
Algunos caracteres del código ASCII.

CARÁCTER	ESCAPE	1	ñ	Ñ	©	Ë
Binario	00011011	00110001	10100100	10100101	10111000	11010011
Decimal	27	49	164	165	184	211

Así, la letra *A* se codifica, en binario, como 01000001 (el 65 en decimal); la *B* como 01000010 (el 66); la *a* mediante 01100001 (el 97), etc. Es decir, el ASCII asigna a las letras *a*, *b*, *c*…, *z*, los números 97, 98, 99…, 122, por lo que la codificación de cada una de las letras del mensaje anterior da lugar al siguiente grupo de números: "99 111 100 105 103 111".

Si ahora consideramos que el cifrado de cada número consiste en multiplicarlo por 23, luego dividir el producto entre 256 y finalmente considerar como resultado el resto de esa división, tenemos que:

$99 \cdot 23 = 2277,$
$2277 = 256 \cdot 8 + \underline{229}.$

Por lo que la letra *c*, que se codifica como 99, pasa a ser cifrada como 229.

Repitiendo el proceso para todos los demás números, se tiene que el mensaje cifrado es: "229 249 252 111 65 249".

Para descifrar el criptograma y recuperar el mensaje original, se debe multiplicar cada uno de los números que forman el criptograma por 167, luego dividir el producto entre

256 y considerar como resultado el resto de esa división (más adelante, en el apartado "Algunos conceptos matemáticos" del capítulo 3, se explicará por qué este proceso invierte las operaciones anteriores). A modo de ejemplo, para el 229 se obtiene lo siguiente:

$229 \cdot 167 = 38243,$
$38243 = 256 \cdot 149 + \underline{99}.$

Ahora, se descodifica el 99 obtenido siguiendo el ASCII y resulta la letra *c*. Para el resto de los números se procede de modo análogo.