

## CLAVE DE ACCESO INCORRECTA

Por Magnus Dagon

El arte de la codificación ha llevado siglos interesando a la humanidad. La necesidad de ocultar datos ha motivado al hombre a ser tremendamente ingenioso a la hora de hacerle la vida imposible a otros que pretenden descifrar mensajes o claves, ya sea por motivos bélicos, de espionaje o meramente lúdicos. Esta disciplina no ha pasado desapercibida en el mundo de la ciencia ficción y fantasía, ni mucho menos. Eso sí, ha sido usada y abusada hasta el punto de hacer de ella poco menos que una ridícula anécdota o un fallo a comentar al salir de la sala de cine o charlar acerca de una novela con otro que la ha leído.

Por poner algunos ejemplos:

En la película *Superman Returns*, Clark Kent y el marido de Lois deben acceder a los datos del ordenador de ésta, pero se les solicita una contraseña. Tras probar toda clase de palabrejas al final deciden usar la que todos estábamos pensando, Superman. Bingo. De ese modo queda claro que, para Lois, Superman es importante en su vida, o al menos lo fue cuando instauró la clave. Traído por los pelos, pero pasable.

En el libro *El Código Da Vinci* (y espero que esto no apareciera en la película), bajo circunstancias especiales que no vienen al caso el protagonista, Robert Langdon, se encuentra en el Louvre con un mensaje cifrado, que reza como sigue:

13-3-2-21-1-1-8-5  
¡Diabole in Dracon!  
Límala, asno

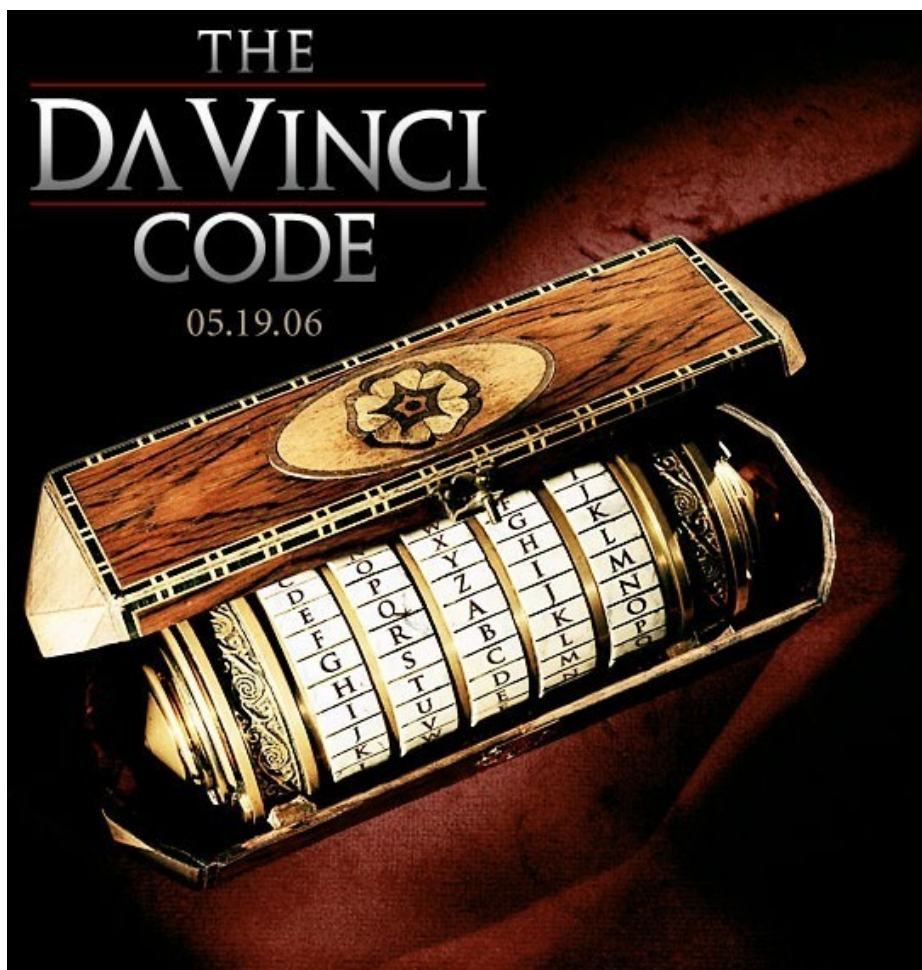
Según comentarios de otro personaje, los criptógrafos de la policía francesa estaban trabajando sin éxito en ello, y Robert Langdon, el protagonista, “volvió a observar aquellos dígitos, con la sensación de que tardaría horas en averiguar alguno”. Bien, para empezar, una creencia popular bastante arraigada es que a la hora de descifrar un mensaje numérico como el de arriba, olvidándonos por un momento de las letras, como posee ocho números, pues debe haber ocho palabras, ocho letras ú ocho sílabas. Falso. Esa es sólo una de tantas maneras de cifrar, muy antigua de hecho, y relativamente fácil de descifrar en nuestra moderna era de ordenadores e incluso a mano con paciencia y conocimientos del idioma. Lo más importante es que un servidor, de un vistazo y tras unos pocos minutos de observación, obtuvo una relación entre los números. Veámoslos en orden ascendente:

1-1-2-3-5-8-13-21

Y, tachán, tenemos la secuencia de Fibonacci. Esta secuencia se caracteriza por empezar con 1, 1 y seguir la sencilla regla de que cada número es la suma de los dos anteriores.

Una secuencia, por cierto, que debe gustar mucho a los profanos de las matemáticas porque aparece también en *El Ocho*, de Katherine Neville, con desigual suerte, y también, y de manera magistral y maravillosa, en la película *Pi (Fe en el Caos)*, relacionándola, como en efecto lo está, con las espirales.

Volviendo al controvertido *Código Da Vinci*, estuve más tiempo rompiéndome los sesos y tratando de pensar en qué influiría el orden, cuando esa respuesta me llegó leyendo el libro de manera casi ofensiva: ninguna. “Se trata de una broma criptográfica muy simple. Algo así como coger las palabras de un poema famoso y mezclarlas aleatoriamente para ver si alguien reconoce lo que tienen en común”, como dice otro de los protagonistas. Si lo de Superman estaba traído por los pelos, esto ya roza, en efecto, la broma, pero al lector. Para rematarlo, el narrador suelta que “igualmente rara era la serie numérica”, cuando ya no para un criptógrafo sino para un matemático, incluso de primeros años de carrera, saltaría a la vista enseguida la secuencia de Fibonacci, y por si el grado de mongolismo de Langdon no fuera ya claro, pocas líneas después dice que “[Langdon] estaba acostumbrado a las progresiones simbólicas que parecían tener algún sentido”.



Pero más adelante en la narración lo de los mensajes cifrados roza el infantilismo. Capítulo 71, Langdon se encuentra con unos “extraños caracteres”. A mí y a mi madre (con los mismos conocimientos de mensajes cifrados que yo de botánica) nos bastaron cinco segundos para darnos cuenta de que era un párrafo escrito al revés. Langdon especula con que quizá sea una lengua semítica, entre otras grotescas teorías. Para colmo de males las pistas son claras pues mucha gente sabe de la afición de Leonardo Da Vinci a escribir al revés.

Es una pena que Dan Brown se aproveche de las matemáticas de un modo tan burdo y falaz y encima pretenda hacerse pasar por un gran documentador, agradeciendo a su padre, que es matemático, su ayuda en lo relativo a la secuencia de Fibonacci. Este desconocimiento de las matemáticas a la hora de presentar códigos en una obra de ficción ha sido parodiado en muchas ocasiones, como por ejemplo en el *Manual del Perfecto Tirano* de Peter David, un famoso guionista de comics, el cual habla de tópicos en los que un supervillano no debe incurrir:

*Uno de mis consejeros será un niño normal de 5 años. Cualquier fallo en mi plan que sea capaz de detectar será corregido antes de ser llevado a cabo [...]. Mi consejero de cinco años también será requerido para descifrar cualquiera de mis códigos. Si lo descifra en menos de 30 segundos no será usado. Nota: lo mismo para las contraseñas.*

Otra parodia aparece en la película de Mel Brooks *La Loca Historia de las Galaxias*. Los Spaceballs raptan a la princesa del mundo de Druidia y proponen cambiarla por el código que otorga acceso a las reservas de aire del planeta. El monarca de Druidia accede y procede a dictar el código: 1, 2, 3, 4, 5. Uno de los Spaceballs comenta que “es la combinación más estúpida que he visto en mi vida, es la que un idiota pondría en sus maletas”. Poco después llega el mandamás de los Spaceballs, y al escuchar el código exclama que “es asombroso, yo tengo la misma combinación en mis maletas”.

En ninguno de estos ejemplos entra la criptografía como ciencia. Ni siquiera se recurre a técnicas elementales de codificación, siendo algunas de ellas de una sencillez abrumadora. Ya desde la antigüedad se conocen interesantes procesos como el cifrado del César. Este procedimiento, llamado así por razones obvias, consistía en lo siguiente:

Elegimos una palabra que no posea letras repetidas, por ejemplo gato. A continuación escribimos el alfabeto, pero saltando las letras ya incluidas en nuestra palabra, en este caso g, a, t, o. Al acabar obtenemos la siguiente asociación entre el alfabeto estándar y el codificado:

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
g	a	t	o	b	c	d	e	f	h	i	j	k	l	m	n	p	q	r	s	u	v	w	x	y	z

Llamaremos a este cifrado “cifrado gato”. De ese modo la palabra *poema* en cifrado gato sería *nmbkg*. Cuanto más larga la palabra, más compleja su descryptación, y las posibilidades son tantas como palabras sin letras repetidas nos dé por usar. Este sistema,

actualmente, está en desuso, pero en su momento debió ser muy eficaz. Y es que la criptografía, al ser una ciencia práctica, no perdona. Si algún método empieza a ser poco fiable, nadie lo usará. De más está decir que los bancos están muy interesados en todo lo que tenga que ver con criptografía, y que hay muy poca bibliografía de libros de criptoanálisis, la rama de la criptografía que muestra cómo descifrar (en el argot romper) códigos.

La criptografía moderna nació a partir de una premisa básica que mucha gente de hecho desconoce acerca de las matemáticas: las matemáticas no son una ciencia donde todo está hecho. Ojalá. Hay muchos, muchísimos problemas sin resolver en absolutamente todas sus ramas, que son una gran cantidad. Allá donde exista un aspecto de la física no resuelto las matemáticas pueden ayudar, y los problemas abstractos también están lejos de ser un cuerpo cerrado en términos de investigación. Por lo tanto se aprovecharon estas premisas con una idea tan simple como brillante: descifrar un mensaje sin conocer el código debe implicar enfrentarse a un problema no resuelto de las matemáticas.

Ojo, un problema no resuelto no quiere decir que no se puede obtener la solución, aunque parezca un absurdo. Los problemas que interesan a la criptografía son los llamados problemas intratables. Son problemas para los que se conocen procedimientos que, aunque son teóricamente válidos, a la hora de la aplicación práctica su utilidad es nula.

Por ejemplo, los números primos son aquellos tales que sus únicos divisores son 1 y el propio número, como 7 o 103. Dado un número, es un hecho conocido que se puede descomponer de manera única en factores primos salvo el orden. Cien, por ejemplo, se descompone como  $100 = 2 \cdot 2 \cdot 5 \cdot 5$ . El problema de, dado un número, hallar sus factores primos, es intratable. Claro, con cien es fácil, pero traten de hallar a mano los factores primos de 25780432047204727. Y aunque una computadora puede echar una mano en el asunto, no lo tiene mucho más fácil. A medida que el número crece, la cantidad de operaciones a realizar crece demasiado en proporción.

Este problema es muy complicado, y de hecho no está resuelto, es decir, no existe una manera *buena* de descomponer un número en sus factores primos. Pero pensemos el problema inverso: dada una serie de primos, encontrar el número del que son factores. Este problema no es que sea fácil, es que es trivial, pues basta con multiplicarlos. Por ejemplo, dados los primos 5, 7, 3 y 3 (pueden ser repetidos), el número del que son factores son  $5 \cdot 7 \cdot 3 \cdot 3 = 315$ .

Resumiendo, tenemos un problema que es muy fácil en un sentido y casi imposible en el otro.

Ésta es la base de la criptografía moderna. En criptografía moderna, llamada de clave pública, existen dos claves, de encriptación y de descifrado. La clave de encriptación es conocida por todo el mundo, y todos podemos usarla para encriptar mensajes. La de descifrado, por el contrario, es secreta, pero se sabe que se puede obtener a partir de la de encriptación. Todo el mundo sabe cómo obtenerla. El único problema es que se tarda tanto en hacerlo (pues el proceso involucra un problema intratable de las matemáticas) que para cuando lo conseguimos la clave ya ha sido cambiada. Ese es el gran secreto de la criptografía moderna: no hacer códigos

imposibles de descifrar, sino códigos para los que se sabe que se tardará tanto que con sustituir la clave cada cierto tiempo prudencial será más que suficiente.



En el caso de los primos, lo que se usa es un número enorme, muy grande, el cual se sabe que es producto de sólo dos primos. Todo el mundo puede usarlo para codificar un mensaje, pero para descodificarlo hay que conocer los primos. Si no se conocen, la alternativa es factorizar el número, pero éste es un problema intratable. Este procedimiento, uno de los mejores de la actualidad, es conocido como RSA, y cuando fue inventado en 1977 se pensó que era el procedimiento perfecto, infranqueable incluso para los ordenadores del futuro. Pero sus autores (Ron Rivest, Adi Shamir y Len Adleman, del MIT) no contaron con una cosa: Internet y su capacidad para hacer trabajar a muchos ordenadores como uno solo. El RSA fue derrotado, pero sentó las bases de futuros procedimientos. De hecho, los bancos compran números primos que aún no hayan sido descubiertos.

Por último, como no todo son críticas, mencionar un relato corto en el que el uso de la codificación es ejemplar, no incurriendo en errores fáciles como los del *Código Da Vinci*. Me refiero a *El Escarabajo de Oro* de Edgar Allan Poe, un relato donde los

protagonistas se encuentran con un mensaje cifrado que, a pesar de resultar sencillo, es explicado, justificado y desmenuzado por el autor, tanto desde el punto de vista de la elección del método de cifrado como del procedimiento para resolverlo. Una explicación que llena varias páginas y resulta muy divulgativa y didáctica, además de ser tremendamente verosímil, pues llega a emplear aspectos concretos del idioma en el que el mensaje está escrito. Una prueba más de la maestría de Poe para tratar temas en los que otros menos experimentados han naufragado.

**Autor: Magnus Dagon (seudónimo literario de Miguel Ángel López Muñoz); Madrid, España. Artículo inédito. Teorema Z [www.libroandromeda.com](http://www.libroandromeda.com)**

-----  
El autor ha cedido a Libro Andrómeda el derecho de publicación de esta obra en nuestra web, con la siguiente condición, de acuerdo con las opciones de protección de los derechos de propiedad intelectual existentes para la difusión en Internet:

-----  
**Reconocimiento – Sin obra derivada – No comercial:** El material creado por un artista puede ser distribuido, copiado y exhibido por terceros si se muestra en los créditos. No se puede obtener ningún beneficio comercial. No se pueden realizar obras derivadas.