Las matemáticas nos dan seguridad

◆ RAFAEL FERNÁNDEZ FLORES ◆

Desde luego que el título de este artículo no alude a la seguridad personal, entendida como el aplomo con el que Humphrey Bogard se conduce en la pantalla, para envidia de Woody Allen. Se refiere, más bien, a las aplicaciones que las matemáticas tienen en el desarrollo de mecanismos para proteger la información que circula en las cada vez más numerosas redes de cómputo.

El provecho que podemos obtener de una computadora aislada se multiplica enormemente cuando la hacemos formar parte de una red (*Entre los individuos como entre las computadoras, la unión hace la fuerza*). Podemos hacernos una idea de una red de computadoras a partir de la de teléfonos. De hecho, muchas veces las computadoras se enlazan —“enredan”— a través de las líneas telefónicas.

Cada teléfono conectado a la red tiene la posibilidad de establecer comunicación, es decir, proporcionar y extraer información, con cualquier otro aparato en la red. Imaginemos ahora que cada teléfono tuviera integrada una diminuta cámara de video y que, al establecerse la comunicación con nuestro aparato, la persona que llama tuviese acceso visual a nuestro domicilio.

Para empeorar la situación supongamos que la cámara de video pudiera ser teledirigida por quien hizo la llamada, de manera que sin mucha dificultad sería capaz de inspeccionar si la cocina está limpia, las camas tendidas o si guardamos algunos objetos de valor y en dónde se encuentran. Agreguemos algún mecanismo para poder sustraer, mediante el teléfono, los bienes y el esquema estará completo. Con aparatos telefónicos de esta naturaleza ten-

driamos que ser sumamente cuidadosos al proporcionar nuestro número telefónico.

Algo muy semejante es lo que ocurre cuando nuestra computadora se encuentra formando parte de una red. En principio, cualquier máquina conectada a la red puede establecer contacto con la nuestra y, de esta manera, el usuario de aquella tendría la posibilidad de inspeccionar qué guardamos en ella y, eventualmente, de llevarse algunos archivos. Sin embargo, la solución de “desenredar” o desenlazar nuestra computadora es tan útil como la de desconectar nuestro teléfono: nos aísla.

Un primer paso para proteger la información de nuestra computadora consiste en limitar el ingreso a ella mediante la asignación de claves. A partir de ello, para acceder a una máquina dentro de una red no sólo será necesario conocer su dirección —el equivalente al número telefónico—, sino además proporcionar una contraseña que identifique a quien solicita la conexión como alguien previamente autorizado por el responsable de la computadora a entrar en ella, inspeccionar su contenido, retirar, colocar o modificar archivos.

Esta solución no es perfecta, en la medida en la que las contraseñas se pueden robar o descifrar. Crear contraseñas seguras, escribir mensajes en clave (encriptar) y traducirlos (desencriptar), certificar y autenticar usuarios se han vuelto entonces actividades indispensables en la construcción de un universo de intercambio —incluido el comercial— electrónico, que parece ser el futuro ineluctable de sociedades donde el recurso no renovable más importante es el tiempo.

En todas estas tareas las matemáticas desempeñan un papel muy importante. La codificación o encriptamiento debe ser una labor fácil de realizar en una dirección —la de cifrado— y difícil en la otra —la de desentrañamiento—. Obsérvese que en eso consiste precisamente el caso entre multiplicar factores primos para obtener un número (operación relativamente sencilla) y la descomposición en factores primos (proceso que puede volverse muy complicado).

Los mecanismos de cifrado consisten en reemplazar el texto original por otro que se construye a partir de él de acuerdo con algún algoritmo. Existen varios de estos métodos y todos nosotros seguramente hemos jugado, de niños, a escribir mensajes secretos. La forma en que posiblemente lo hacíamos era sustituir cada letra del alfabeto por otra. Por ejemplo, en la novela *2001 Odisea del espacio* aparece una computadora de nombre HAL. Parece evidente que éste es el nombre cifrado que se obtiene de IBM cuando sustituimos cada letra por su antecesora en el orden alfabético.

Este procedimiento es obviamente generalizable a un corrimiento del alfabeto de n lugares para cualquier n menor o igual a 26. Actualmente los mensajes escritos mediante este mecanismo son relativamente fáciles de descifrar, pues basta aplicar un programa de cómputo que reemplace el mensaje que se quiere decodificar por el que se obtiene al recorrer el orden alfabético uno, dos, tres... veintiséis veces y observar cuál es el que tiene sentido. Éste es un método de descifrado que podemos calificar de "fuerza bruta", pero las computadoras modernas lo hacen viable.

En el método descrito anteriormente todas las letras del alfabeto se recorren los mismos lugares, por lo que bastan 26 intentos para romper el código. Un mecanismo más complejo de desciframiento consiste en asignar, mediante una regla arbitraria, a cada letra del alfabeto otra, que puede incluso en algún caso ser ella misma. En este esquema existen para cada una de las 26 letras 26 posibles asignaciones, por lo que el método de la fuerza bruta requiere 26^2 intentos, para asegurar la ruptura del código.

Pero aun esta forma de esconder los mensajes puede resultar poco segura, pues una vez que se descubre qué carácter corresponde a cada letra, esta asociación se mantiene a lo largo de todo el texto. Una manera de dificultar la lectura del mensaje cifrado consiste en hacer que la regla de sustitución cambie a lo largo del mensaje. Para lograr esto podemos auxiliarnos de una palabra secreta que llamamos llave o clave. Ejemplifiquémoslo construyendo la siguiente tabla o matriz:

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	
A	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
B	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	
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A		
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B		
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C		
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D		
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E		
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F		
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G		
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H		
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I		
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J		
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K		
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L		
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M		
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N		
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O		
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P		
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q		
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R		
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S		
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T		
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U		
Y	Y	X	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U		
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W		

Usemos como palabra clave MATEMÁTICAS

Para codificar cualquier otra palabra, por ejemplo, MENSAJE, haremos una correspondencia entre las letras de la clave y la palabra a ser cifrada:

Clave: M A T E M Á T I C A S

Palabra: M E N S A J E

Ello da como resultado parejas de letras: MM, AE, TN...

Si usamos estas parejas como entradas en la matriz, es decir, si buscamos en la primera línea horizontal la primera letra de la pareja, en el caso que nos ocupa M, y en la primera línea vertical la segunda letra, que es también M, y después buscamos qué elemento de la matriz corresponde a esas coordenadas, encontramos las siguientes relaciones:

A la entrada MM en la matriz le corresponde la letra Y; a la entrada AE, la E; a TN, la F, etcétera. Así, al terminar de asignar todas las correspondencias tendremos que MENSAJE se transformó en YEFWMJX. Para aumentar la dificultad de su resolución, podemos cifrar por segunda vez el mensaje con una segunda clave, y así sucesivamente.

La labor de encriptamiento, aunque notablemente más simple que su inversa, puede volverse fastidiosa en extremo si se realiza manualmente. Hoy en día estos algoritmos pueden efectuarse con auxilio de las computadoras electrónicas. Antes se realizaron con la ayuda de ingeniosas máquinas mecánicas, como la célebre *Enigma* usada por los alemanes durante la segunda Guerra Mundial. Un interesante relato acerca de la manera en que funcionaban estos aparatos y de cómo los aliados lograron descifrarlos puede leerse en el libro *Codebreakers*, de Stuart Milner.

Conociendo la palabra clave y la matriz, es posible pasar del mensaje cifrado al texto original. Descifrar los mensajes codificados mediante este mecanismo por pura fuerza bruta puede ser una tarea sumamente difícil.

Obviamente el gran problema de estos métodos de cifrado consiste en la manera de mantener secreta la llave, pues ésta debe ser conocida por quienes reciben los mensajes para poderlos leer.

Una sofisticación del procedimiento de codificación consiste en utilizar un par de llaves: una pública y una privada. La llave pública es usada por quienes quieren enviar un mensaje, para cifrarlo. El mensaje codificado sólo puede ser leído con ayuda de la llave privada, y ésta sólo la conoce el destinatario del texto, además obviamente del emisor. El mecanismo de generación de parejas de llaves para que cumplan estas condiciones puede resultar complicado. Existen varios algoritmos para generar parejas de llaves. Uno de ellos fue desarrollado por Ron Rivest, Adi Shamir y Leonard Adleman, de RSA Data Security.

Otro punto en el que el cifrado de archivos se vuelve importante es en la certificación de su origen y contenido, pues se correrían riesgos si, por ejemplo, alguien intercepta un mensaje entre dos personas, lo altera y lo reexpide al destinatario original, quien no advierte el cambio del texto y toma el contenido del mensaje como verdadero, con las previsibles fatales consecuencias. O bien, en el caso de que alguien envíe a través de la red un mensaje en el que dice ser alguien que no es. Prevenir este tipo de riesgos ha llevado a desarrollar mecanismos de certificación y firma digital que se basan también en métodos de encriptamiento.

Por ejemplo, para asegurar la integridad de un mensaje, no su confidencialidad, puede usarse el siguiente procedimiento: el emisor codifica el texto con su llave privada y envía al receptor ambos mensajes, el cifrado y el normal. El receptor descifra el texto con la llave pública; si esto es posible, significa que el texto proviene de la única persona que conoce la llave privada, es decir, el emisor. A continuación, el receptor compara el texto que acaba de decodificar con el texto normal y comprueba si tiene o no alteraciones. Variantes de este procedimiento se usan para crear firmas digitales que acreditan la identidad del signatario.

Digamos para terminar que algunos de los algoritmos más populares de codificación utilizan las propiedades de las curvas elípticas. No es el propósito de este texto ahondar en el estudio de estos bichos, digamos únicamente que son conjuntos de puntos sobre los que se puede definir la operación de adición y la de multiplicación por un entero positivo por iteración de la suma. La suma cumple las propiedades necesarias para que los matemáticos digan que este conjunto es un grupo Abelian, es decir que la suma cumple

la propiedad de ser conmutativa o, en otras palabras, el orden de los sumandos no altera el resultado.

Escogida de común acuerdo una curva elíptica y un punto perteneciente a ella, un grupo de usuarios puede construir, a partir de la multiplicación del número seleccionado por números enteros, sus llaves públicas y usar números aleatorios como su clave secreta.

El esquema funcionaría de la siguiente manera: cada uno de los miembros del grupo selecciona al azar un número entero y lo utiliza como su llave secreta y da a conocer el producto de ese número aleatorio por el punto previamente escogido de la curva como su llave pública.

Cuando uno de los usuarios desea mandar un mensaje debe multiplicar la llave pública de aquel a quien quiere enviar el mensaje, el receptor, por la llave privada de quien lo envía, el emisor, y usar ese número como clave para construir el bloque de codificación (el equivalente, toda proporción guardada, a la palabra MATEMÁTICAS, que se usó como clave para encriptar un mensaje en la forma de YEFWMJX).

Debido a la conmutatividad del grupo, el receptor puede calcular el número clave con el que se construyó el bloque de cifrado —y por lo tanto ser capaz de descifrar el mensaje— efectuando la multiplicación de su propia clave secreta por la llave pública de quien le envía el mensaje.

La seguridad del esquema reside en la dificultad de factorizar la llave pública de cada usuario, que es —recorremos— el producto de un número aleatorio, la llave privada, por un número conocido, el punto de la curva elíptica.

Para que eso ocurra es necesario que la selección de la curva y el punto se realice de acuerdo con ciertos criterios cuyo cumplimiento implica el conocimiento de algunos algoritmos, como el de Schoof, y de teoremas, como el de Weil, que se ocupan de las propiedades de las curvas elípticas y sus puntos.

Quienes se interesen en los aspectos técnicos relacionados con la utilización de las propiedades de estas curvas para crear esquemas de encriptamiento, así como de sus aplicaciones para producir firmas digitales, pueden encontrar interesantes los libros *A Course in Number Theory and Cryptography*, de Neal Koblitz, y *Elliptic Curve Public Key Cryptosystem*, de A. J. Menezes. El primero fue editado por Springer-Verlag en 1994 y el segundo por Kluwer Academic Publications en 1993.

Al llegar a este punto no puedo dejar de pensar en las personas que invariablemente preguntan a quienes estudian matemáticas: ¿y para qué sirven las matemáticas? En la respuesta, aparte de su principal mérito, que es el ser bellas, se puede expresar: para darnos seguridad. ♦