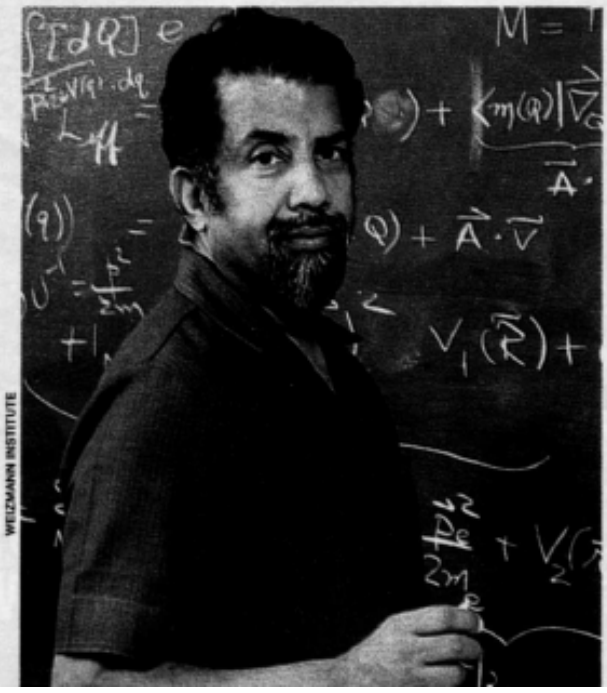
Una lista de números para gente muy lista

Esta serie muestra marcados en naranja los que son primos, o sea, los que sólo son divisibles por sí mismos y por uno. La mayoría de los códigos de encriptación de mensajes, que sirven para transacciones comerciales e informaciones secretas, están basados en productos de números primos.



WEIZMANN INSTITUTE

El código más secreto

Adi Shamir, matemático del Instituto Científico Weizmann de Israel, es uno de los inventores del código RSA, una fortaleza criptográfica de 129 cifras. Cuando lo inventó en 1977 dijeron que harían falta 40.000 billones de años para descifrarlo, pero en 1996 se logró.

Si nos hablan de matemáticas enseguida nos viene a la cabeza una imagen: un individuo algo huraño sentado ante una mesa y con cientos de papeles garrapateados con fórmulas ininteligibles. Esto podía ser cierto hace bastantes años, pero desde el advenimiento de los ordenadores se ha desarrollado una nueva matemática destinada a resolver problemas antaño irresolubles: la matemática computacional.

De hecho, la información es poder. Intervenir, contaminar, desinformar, ocultar y descubrir es parte de ese juego de poder. Quien más información acumula y quien mejor la oculta posee más poder. Aquí es donde nace la criptografía, el arte de escribir mensajes en clave secreta o enigmáticamente. Desde las guerras entre Esparta y Atenas se han empleado diferentes sistemas para ocultar información vital al enemigo, pero en la actualidad la necesidad de encriptar información se ha vuelto completamente imprescindible. El ritmo vertiginoso de producción, el ingente tráfico de documentos y la rapidez necesaria para la mayoría de las transacciones exige un método rápido, efectivo, cómodo y, sobre todo, seguro de comunicación.

● Mensajes secretos

La gran revolución se dio en 1975 cuando dos ingenieros electrónicos de la Universidad de Stanford, Whitfield Diffie y Martin Hellman, sugirieron el primer concepto nuevo en criptografía desde el tiempo de los griegos. Hasta entonces todo se basaba en una clave que permitía tanto cifrar como descifrar el mensaje. En el nuevo esquema, llamado criptografía de clave pública, existen dos claves: una de cifrado, que es conocida por todos, y otra de descifrado, que es secreta. Si alguien necesita recibir un mensaje cifrado sólo tiene que crear ambas claves y enviar por la red sólo la de cifrado.

Ésta fue la idea genial de Diffie y Hellman: sugerir que una manera de diseñar sistemas criptográficos seguros era utilizando problemas computacionalmente intratables, esto es, aquellos que un ordenador tardaría millones de años en resolver. Pero ¿cuáles son?

En la actualidad, el método más utilizado es el llamado RSA, desarrollado en 1977 por Ronald Rivest, Adi Shamir y Leonard Adleman. Este sistema se basa en que no existe un algoritmo suficientemente eficiente para factorizar grandes números que sean producto de dos números primos. Los ordenadores más potentes del mundo tardarían muchísimos años en *reventar* una clave basada en la factorización. Sin embargo, Internet ha venido a cambiar las tornas. ¿Para qué construir ordenadores cada vez más grandes si a través de la red tenemos acceso a cientos de miles de ellos y entre todos constituyen un gigantesco ordenador? Fue así como se consiguió romper el RSA.

● Dinámica de fluidos

Otro de los problemas que sería intratable sin la ayuda de la matemática computacional generada por los ordenadores es el movimiento de los fluidos, ya sean líquidos o gases. Predecir cómo se va a mover el agua por una tubería o la sangre por las arterias es un arte considerablemente difícil y que tiene una gran importancia. Una de las técnicas que se ha desarrollado con más rapidez en las últimas décadas, gracias al aumento en la potencia de cálculo de los ordenadores, es la llamada Dinámica de Fluidos Com- →

Cómo me lo *factoriciaría* yo

EL matemático Leonhard Euler (1707-1783) factorizó el quinto número de la serie de Fermat. El noveno número de Fermat lo factorizaron 200 matemáticos y 1.000 ordenadores, en 1990.

Seguro que todos recordamos, de nuestros tiempos de colegio, los ejercicios de factorización o descomposición de un número primo en producto de factores que también sean números primos. Por ejemplo, 15 es el producto del 3 y del 5 (ambos, primos). Factorizar números se convierte en algo casi imposible cuando el número es grande, por ejemplo, 4.294.967.297, producto de 641 por 6.700.417, dos números primos y precisamente el quinto número de una serie que inventó Fermat.

Con tal despliegue de pirotecnia matemática uno se pregunta para qué sirve perder el tiempo factorizando números. Pero bancos, tarjetas de crédito y ministerios de defensa encriptan sus datos con códigos basados en los factores de grandes números. Si alguien descubre una forma rápida de hacerlo podría saltarse los controles de seguridad de todas esas organizaciones y provocar un lío mayusculo. Por eso, cualquier descubrimiento relacionado con la factorización se convierte enseguida en cuestión de seguridad nacional. ●