El Mundo, 23 de Febrero de 2001
ENCRIPTACION
-
DAVID LACASA MADRID.- Los científicos acaban de descifrar el código genético del hombre. Un joven sueco decodificó el código de seguridad del DVD. Pero ahora, un profesor de la facultad de informática de Harvard asegura haber creado la encriptación indescifrable.

El Dr. Michael Rabin y su ayudante Yan Zong Bing, ambos de la universidad de Harvard, han anunciado el hallazgo de un medio de enviar mensajes cifrados imposibles de decodificar incluso por la máquina más poderosa.

El sistema consiste en que la clave de decodificación desaparece a la vez que se crea el mensaje cifrado. La idea no es nueva, pero nadie antes había logrado que funcionara y probarlo matemáticamente. "Este es el primer código indescifrable que es realmente eficiente", ha declarado Rabin al New York Times.

La fórmula indescifrable comienza en la generación de una cadena continua de números aleatorios desde un punto concreto, por ejemplo un satélite. El emisor y el receptor del mensaje acuerdan el momento exacto en el que el programa de codificación comienza a cifrar el mensaje. Es entonces cuando el programa captura una parte de la cadena aleatoria de números que utilizará en la fórmula de cifrado y su posterior descodificación.

Así, la clave de decodificación se esfuma al mismo tiempo que se crea el mensaje cifrado. La única forma de que alguien pudiera dar con la clave sería guardando toda la cadena de números generados o grabándolos en el mismo momento exacto. Lo primero requeriría un ordenador con una gran capacidad de memoria (bastante más de lo que hoy existe), y lo segundo mucha suerte.

Pues nada, ya hay otro reto más en la Red para los amantes de las cosas difíciles.