

La criptografía cuántica supera los 100 kilómetros.

Un grupo de investigadores de Toshiba Research Europe, en el Reino Unido, [ha conseguido romper la barrera de los 100 kilómetros](#) en la criptografía cuántica transmitida a través de fibra óptica, una tecnología teóricamente inviolable que según Andrew Shields, que ha capitaneado el proyecto, será desarrollada con fines comerciales en menos de tres años.

Los científicos han presentado su récord en la [CLEO](#) (Conference on Lasers and Electro-Optics), que anteriormente ostentaban una compañía japonesa y que databa de Noviembre de 2002 con 87 kilómetros de distancia.

Las claves criptográficas de hoy en día (usadas en el protocolo SSL para transacciones seguras entre clientes y bancos, por ejemplo), se componen de cadenas aleatorias de números y letras. Para comenzar una transacción segura, estas claves deben ser intercambiadas entre los interlocutores. En este paso previo es donde se producen la mayor parte de los espionajes, interceptando la clave (encriptada a su vez con otros mecanismos) en el momento de la transmisión cuando viaja electrónicamente por redes convencionales. Si todo ha ido bien, el otro interlocutor puede descifrar el mensaje con una copia de la clave empleada originalmente.

La criptografía cuántica consigue *conectar* cada dígito de la clave a un mínimo conjunto de fotones, enviados en un minúsculo haz de luz. Al contrario que con la tecnología electrónica de hoy en día, leer la clave en su *viaje* alteraría el estado cuántico de los fotones de tal forma que el receptor sabría que ha sido manipulada o leída de alguna manera. Es en esto donde radica su seguridad, pero la atenuación periódica que sufren los estados de los fotones según la distancia recorrida y el medio en el que viajen, limita el uso de esta técnica a pequeñas redes experimentales hasta que se vayan desarrollando nuevas tecnologías de transmisión y ganando en distancia.

La carrera por la distancia está abierta en dos frentes, la fibra óptica, donde ya se han alcanzado los 100 kilómetros, y el aire como transmisor. En octubre de 2002, científicos de la firma [QinetiQ](#), la rama comercial de la agencia británica de investigación de defensa, consiguieron enviar con éxito una clave criptográfica a una distancia [de más de 23 kilómetros](#) de espacio abierto entre dos montañas en Alemania. Se espera que dentro de seis años, esta técnica esté lista para enviar claves a cualquier parte del mundo utilizando satélites de órbita baja.

Sergio de los Santos
<http://www.forzis.com>

Fecha artículo: 2003-06-12 19:09:04 - url artículo: <http://www.internautas.org/html/155.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org