

El País, 27 de septiembre de 2001

CiberPaís, Única, pág. 4 - Noticias

LA GUERRA DEL SIGLO XXI

FERNANDO GARCÍA **José Luis Salazar: "No sirve de nada prohibir el cifrado de mensajes"**

José Luis Salazar, de 31 años, licenciado en Matemáticas, es el encargado de impartir criptografía en el departamento de Ingeniería Electrónica y Comunicaciones de la Universidad de Zaragoza. Salazar define la criptografía como "la ciencia que estudia la forma de mandar mensajes cifrados". Tras los atentados del pasado 11 de septiembre en Nueva York y Washington, se ha abierto el debate sobre la prohibición de la criptografía.

Pregunta: ¿Los mensajes cifrados son inviolables?

Respuesta: En principio, la criptografía es segura. Pero siempre hay que tener en cuenta que el factor humano puede fallar. No hace falta interceptar los mensajes. Las claves necesarias para cifrar y descifrar mensajes se pueden obtener en el cubo de la basura e, incluso, en la basura digital. No hay que olvidar que cuando borramos algo del ordenador, lo tiramos a la papelera y luego la vaciamos. La información que contiene el archivo no se ha eliminado porque, aunque no está enlazada, continúa almacenada en el disco duro del ordenador y alguien puede recuperarla.

P. ¿Quién usa criptografía?

R. Además de las aplicaciones que tiene para el comercio electrónico, la utilizan tanto los delincuentes como los agentes de los diferentes gobiernos.

P. Estados Unidos debate la prohibición de la criptografía o abrir puertas para intervenir los mensajes.

R. Si se quieren intervenir las comunicaciones cifradas, es necesario disponer de las claves y no creo que sea la solución. No obstante, dudo mucho que sean capaces de aplicar ese tipo de restricciones. Otra cosa es que ciertas agencias gubernamentales dispongan de la capacidad computacional para romper las claves. En este momento no se tiene la seguridad de que sea posible, pero si fuera así, no necesitarían prohibir la criptografía porque podrían saltarse las claves. De todas formas, si los terroristas no pueden utilizar la criptografía, emplearán otros métodos. No sirve de nada prohibir la criptografía. El problema no es la herramienta. Si no es con pistolas, los terroristas matarán con arcos y flechas.

P. La prohibición de la criptografía afectaría al desarrollo del comercio electrónico.

R. Naturalmente. La confianza en el comercio electrónico reside en la seguridad de las transacciones que, en una gran parte, se sustenta en la criptografía.