

Nuevo código de encriptación absolutamente irrompible.

Meganet, una compañía israelí con apoyo estadounidense, ha desarrollado una nueva tecnología de encriptación que parece ser irrompible. Toda un revolución en el mundo de la criptografía que usa claves de un millón de bits, cuando lo más avanzado del mercado hoy en día llega sólo hasta las 2048, siendo lo habitual 256.

La encriptación de los datos, esto es, codificarlos de manera que si se intercepta el mensaje este sea incomprensible para el atacante, es algo habitual entre las comunicaciones establecidas entre gobiernos en épocas de guerra. Hasta ahora, la encriptación más avanzada, la que usa claves de 256 bits resulta una excelente solución, pero aún puede llegar a plantear problemas. Hace poco, el grupo de trabajo distribuido distributed.net, logró averiguar una clave encriptada con 64 bits. Actualmente se encuentra trabajando para romper claves de 72 bits.

Saul Backal, fundador de Meganet, cree haber obtenido la solución definitiva. VME (Virtual Matrix Encryption) es una nueva tecnología de mapeo no lineal de datos que crea un complejo sistema aleatorio de texto y clave de un millón de bits. Las combinaciones posibles para averiguar esta clave, dos elevado a un millón, traducida a cifras, puede superar en miles de millones la edad del universo en años.

Meganet se ganó desde un principio la confianza del gobierno estadounidense. En Febrero del año pasado le fueron concedidos 4 millones de dólares para proporcionar a uno de sus departamentos, de 18.000 empleados, encriptación y firmas digitales. Más tarde esta cifra se incrementó a 7 millones.

Meganet está tan convencida de su producto y de que no se trata de un snake oil (término parecido a "charlatanería" usado en criptografía) que ofrece un millón de dólares o un Ferrari a quien consiga descifrar un fichero encriptado con VME. Hasta ahora, dos millones de personas lo han intentado y nadie lo ha conseguido.

Más información www.meganet.com SERGIO DE LOS SANTOS
www.forzis.com

Fecha artículo: 2003-02-27 17:56:43 - url artículo: <http://www.internautas.org/html/89.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