

## **El sistema de criptografía de Curvas Elípticas roto por medio de fuerza bruta.**

**Después de dos años, un grupo académico acaba de romper el desafío ECCp-109, propuesto por Certicom Corporation y consistente en obtener un mensaje cifrado con una implementación del Criptosistema de clave pública de 109 bits de Curvas Elípticas.**

Certicom Corporation confirmó que para romper la Criptografía de Curvas Elípticas (Elliptic Curve Cryptography -ECC-) de 109 bits se empleó un sistema red de más de 10.000 ordenadores, que durante las 24 horas del día durante más de 549 días fueron capaces de obtener la clave de cifrado, empleando la fuerza bruta.

El premio por vencer el reto que planteaba ECCp-109 es 10.000 dólares. Por su parte, ahora Certicom ofrece 20.000 dólares en un desafío relativo a una clave de 131 bits, que es más fuerte que su sistema ECCp-109.

Para más información;

[http://www.certicom.com/about/pr/02/021106\\_ecc\\_winner.html](http://www.certicom.com/about/pr/02/021106_ecc_winner.html)

**Fecha artículo: 2002-11-10 16:19:26 - url artículo: <http://www.internautas.org/html/60.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](mailto:asociacion@internautas.org)