El grupo de investigación del Departamento de Computación del Cinvestav del IPN figura entre los cuatro primeros lugares del mundo en la competencia para analizar la solidez y seguridad real proporcionada por los sistemas e-gobierno y bancanet.

A principios de año el equipo de Francisco Rodríguez Henríquez logró el cómputo de un logaritmo discreto de un elemento de campo finito de 1551 bits en tiempo equivalente a 918 horas o 38.25 días de cómputo, para romper el récord mundial impuesto por un grupo japonés en 2012.

Si bien el cómputo alcanzado por el equipo mexicano se mantuvo como récord mundial por poco tiempo, pues días después lo superó un grupo suizo-irlandés, su trabajo científico le ha valido colocarse entre los primeros cuatro lugares a nivel internacional, al ser el primer grupo en romper ese problema criptográfico.

Las aplicaciones de seguridad en el ramo buscan garantizar la seguridad de la información e impedir su robo como, por ejemplo, de atacantes maliciosos que cotidianamente intentan leer los números de las tarjetas de crédito utilizadas en transacciones por internet.

Si éstos han sido cifrados adecuadamente se espera que las aplicaciones informáticas sean capaces de resistir esos ataques, explicó Rodríguez Henríquez en un comunicado.

El doctor por el Departamento de Ingeniería Eléctrica y Computación de la Universidad de Oregon detalló que la información e identidades digitales se protegen a través de candados virtuales.

Las garantías de seguridad de esos mecanismos se sustentan en problemas matemáticos que se consideran extremadamente difíciles de ser resueltos y que son puestos a prueba de manera científica a través de técnicas conocidas como criptoanálisis.

> “Los criptógrafos proponen problemas matemáticos que suponen difíciles de

> resolver y que pueden actuar como candados, mientras que los cripto-analistas los estudian para encontrar sus debilidades e inutilizarlos a fin de hacer el sistema de seguridad más confiable.

“De modo que el diseño de candados virtuales que no puedan ser rotos sean los utilizados en un futuro”, destacó Francisco Rodríguez.

Precisó que con base en la dificultad de resolver ese problema se ha desarrollado una infraestructura de software que asegura la confidencialidad en el contenido de los correos electrónicos.

De igual forma, evita el robo de los números de tarjetas de crédito enviados por Internet y permite verificar la identidad de las personas y entidades con las que se interactúa en línea, entre otros aspectos.

Fuente: eleconomista