Ciudad de México, a 10 de abril de 2016

COMUNICADO DE PRENSA

CREAN POLITÉCNICOS APLICACIÓN QUE EVITA HACKEOS

- **Con el uso de autómatas celulares se asegura que los archivos de texto, imagen y audio no podrán ser leídos por terceras personas**

C-116

Cada que se envía un *e-mail*, W*hatsApp* o *inbox* existe el riesgo de que la información sea interceptada y se haga un mal uso de ella, por esa razón un grupo de politécnicos, de la Escuela Superior de Cómputo (*Escom*), creó una aplicación que cifra y descifra todo tipo de archivos, para asegurar que sólo puedan ser leídos por los destinatarios, que son usuarios autorizados que cuentan con la llave acordada. Si el mensaje es interceptado será ininteligible.

Los politécnicos desarrollaron este sistema criptográfico que se puede instalar en cualquier sistema operativo, equipo de cómputo o dispositivo móvil. A diferencia de otros, el creado por los estudiantes Erick Eduardo Aguilar Hernández y Jessica Matías Blancas utiliza un autómata celular que optimiza y reduce el tiempo del proceso de cifrado y descifrado.

Los profesores de la *Escom* y asesores de tesis, Genaro Juárez Martínez y Nidia Cortez Duarte, explicaron que un autómata celular es un modelo matemático que simula fenómenos naturales, así como sus propiedades físicas, químicas, biológicas o computacionales, las cuales afectan a las unidades vecinas.

Éste no aparece de manera evidente, pero un ejemplo cotidiano es el tránsito vehicular, ya que el movimiento de los autos representa una abstracción del mundo real, que altera un estado o posición, en la biología simula epidemias, crecimiento de plantas, sistemas auto reproductivos. Además describe comportamientos de colonias de hormigas o de células, como un sistema complejo.

El proceso para cifrar la información en la aplicación es muy sencillo, en una computadora se ubica el archivo a mandar por correo (texto, imagen o audio), se aplica la opción "cifrar con el autómata celular" y se coloca la llave o clave. El usuario podrá observar el comportamiento del autómata para el cifrado en una imagen.

De esta forma, el mensaje está listo para ser enviado, pero se muestra ininteligible. Cuando llega al receptor se deberá usar la misma llave y el método para descifrar el archivo, y de ese modo podrá leer el texto, ver la imagen o escuchar el audio, detalló Erick Aguilar.

Para asegurar la confidencialidad, la clave de 16 caracteres debe compartirse previa y físicamente al envío de datos para que nadie tenga acceso a ella. Durante la operación de cifrado el autómata celular descompone toda la información en bloques de 128 bits.

Se realizó un estudio para seleccionar uno de los algoritmos criptográficos existentes que fuera factible para ser caracterizado a través de autómatas celulares. El elegido fue AES (Advanced Encryption Standard) de 128 bits, se analizó su funcionamiento, propiedades y patrones en sus operaciones para ser representados como estados de un autómata celular, especificó el joven politécnico.

Con lo anterior se diseñó un autómata celular con la capacidad de cifrar y descifrar, equivalente al algoritmo AES en su versión de 128 bits. Para comprobar su eficacia se comparó el comportamiento de ambas vías y se observó que durante el proceso de descifrado, el tiempo de ejecución con la alternativa politécnica fue menor que el tradicional.

Las pruebas se realizaron con los datos del Instituto Nacional de Normas y Tecnología (NIST por sus siglas en inglés, National Institute of Standards and Technology), ubicado en Estados Unidos, para avalar internacionalmente el funcionamiento de su aplicación, así como detectar los casos óptimos y el peor de ellos.

"La importancia de esta investigación radica en que existe una cantidad enorme de funciones en el dominio de los autómatas celulares, los politécnicos descubrieron una función en particular que cifra la información basada en un algoritmo, el hallazgo fue el *autómata celular 256 factorial* que evoluciona en una dimensión. Este hecho es inédito ya que dentro de este universo numérico, es el primero con la capacidad de realizar este cifrado en particular dentro del algoritmo AES", resaltó el profesor Genaro Juárez Martínez.

===000===