PROYECTO UNAM

Coordinador: Roberto Arturo Gutiérrez Alcalá robargu@hotmail.com

Recital de piano a cuatro manos

En el Antiguo Colegio de San Ildefonso (Justo Sierra 16, Centro Histórico) Fernando García Torres y Deborah Dewey darán un recital de piano a cuatro manos, con obras de Mozart (Sonata K. 358), Schubert (Fantasía op. 103), Dvorak (Danzas eslavas) y Debussy (Pequeña suite), el próximo domingo 16 de diciembre, a las 12:00 horas

EN AUGE, LA SEGURIDAD INFORMÁTICA

Con ella se busca que la información que posee y maneja cualquier organización sea segura, íntegra y confidencial

Leonardo Huerta Mendoza

La seguridad informática es un área del conocimiento que crea proyectos para brindarle seguridad y certeza a una organización, en relación con la información que posee y maneja; involucra aspectos tecnológicos, matemáticos, sociales, legales y económicos.

Para que la información pueda ser considerada segura, debe tener cinco atributos básicos: disponibilidad, integridad, confidencialidad, no repudio y autenticación. Los tres primeros se aplican a la información en sí; los dos últimos, al proceso de comunicación de esa información.

"Ahora bien, ¿de qué tipo de información hablamos? Depende de la misión, visión y objetivo de la organización. Puede ser la información de un banco, de una empresa manufacturera o de una institución educativa", dice Rubén Vázquez Medina, investigador en estancia posdoctoral bajo la dirección del doctor José Luis Aragón Vera, en el Centro de Física Aplicada y Tecnología Avanzada (CFATA), *campus* Juriquilla, de la UNAM, y experto en el tema.

Por ejemplo, una escuela que ofrece servicios en línea a través de redes públicas, debe garantizar que la información que maneja sea segura, íntegra y confidencial, y que esté disponible para los usuarios válidos pero no para los usuarios mal intencionados.

"Lo que quieren estos últimos es obtener indebidamente esa información o entrar en la infraestructura que la soporta para causar algún daño, como alterar una calificación. La tarea de un especialista en seguridad de la información es otorgar a la organización y a sus usuarios las garantías necesarias para que nadie que no esté autorizado entre en dicha infraestructura", agrega el investigador.

La seguridad informática tiene varias vertientes de aplicación que se concretan en distintos mecanismos relacionados con el uso y la aplicación de la criptología, la esteganografía, la seguridad perimetral, la seguridad física, la seguridad del personal, la seguridad de los sistemas y la infraestructura tecnológica, y el desarrollo de políticas y normas de seguridad de la información, entre otros elementos.

Vázquez Medina ha enfocado sus esfuerzos en el desarrollo de algoritmos y dispositivos criptográficos a partir del empleo de la teoría del caos, y de algoritmos esteganográficos y esquemas de trabajo en forensia digital.

Criptología

La criptología es la disciplina que se dedica al estudio, desarrollo y evaluación de algoritmos y dispositivos que permiten transformar un mensaje en una versión incomprensible para aquellos que no cuenten con la clave correcta.

La criptología incluye dos grandes universos: la criptografía y el criptoanálisis. Con la criptografía se diseñan los algoritmos que otorgan garantías de seguridad a la información y con el criptoanálisis se busca evaluar la calidad de los algoritmos criptográficos desarrollados.

"Al aplicarle los algoritmos criptográficos, una información totalmente entendible se transforma en una versión incomprensible para cualquiera que no sea el destinatario. Ésta sería una definición general de la criptografía", explica el investigador del CFATA.

Esteganografía

La esteganografía es otro mecanismo de protección de la información que permite tomar el mensaje que se quiere proteger e insertarlo dentro de otro objeto (portador) de tal manera que pase inadvertido al enviarlo. Si alguien que no es el destinatario lo intercepta, no sabrá que lo importante está escondido en el objeto portador y tampoco sabrá cómo extraer el mensaje que se quiere proteger.

"Un algoritmo esteganográfico toma relevancia al no despertar sospechas de que se está comunicando algo importante. En cambio, al producir versiones incomprensibles de un mensaje, los algoritmos criptográficos pueden despertar sospechas de que la comunicación contiene algo importante e 'invitar' a alguien malintencionado a buscar la manera de descubrir el mensaje protegido."

Así, cuando un atacante o *hacker* ve que algo en la red de comunicaciones viaja transformado en algo incomprensible, busca descifrarlo mediante técnicas criptoanalíticas y obtener la información importante que se encuentra protegida.

Sin embargo, con la esteganografía se puede usar un archivo de música, una fotografía o un video como medio de transporte (portador) en el que esté escondida la información de interés, y sólo el destinatario podrá extraer esa información con los algoritmos adecuados.

"El *hacker* escuchará la música u observará la fotografía o el video, pero no podrá sospechar que algo se esconde en ese medio de transporte", señala Vázquez Medina.

Forensia digital

Las organizaciones invierten en especialistas, tecnología, capacitación y, sobre todo, seguridad. Sin embargo, eso no cancela el riesgo de que sus sistemas de seguridad puedan ser vulnerados y, en consecuencia, su información sensible quede comprometida. Por eso es necesario que un auditor de seguridad informática los analice periódicamente y compruebe que funcionan bien, sin problemas.

35%
de las computadoras conectadas a Internet en México están infectadas por algún virus

Para ello les hace pruebas de esfuerzo, los "estresa", intenta *hackearlos* y, al final, elabora un dictamen de lo que se tiene que corregir. A pesar de todo, siempre está presente el riesgo de que alguien malintencionado entre en los sistemas de seguridad de una organización, aun cuando éstos hayan superado satisfactoriamente una auditoría.

Si esto ocurre, otro tipo de especialista debe estudiar el caso, decir quién y cómo violó la seguridad, y cuál es el impacto en la organización, y elaborar un informe de carácter legal.

"Y es que, si el impacto en una organización es muy grande, entonces un incidente de seguridad informática llega a convertirse en un asunto jurídico", asegura Vázquez Medina.

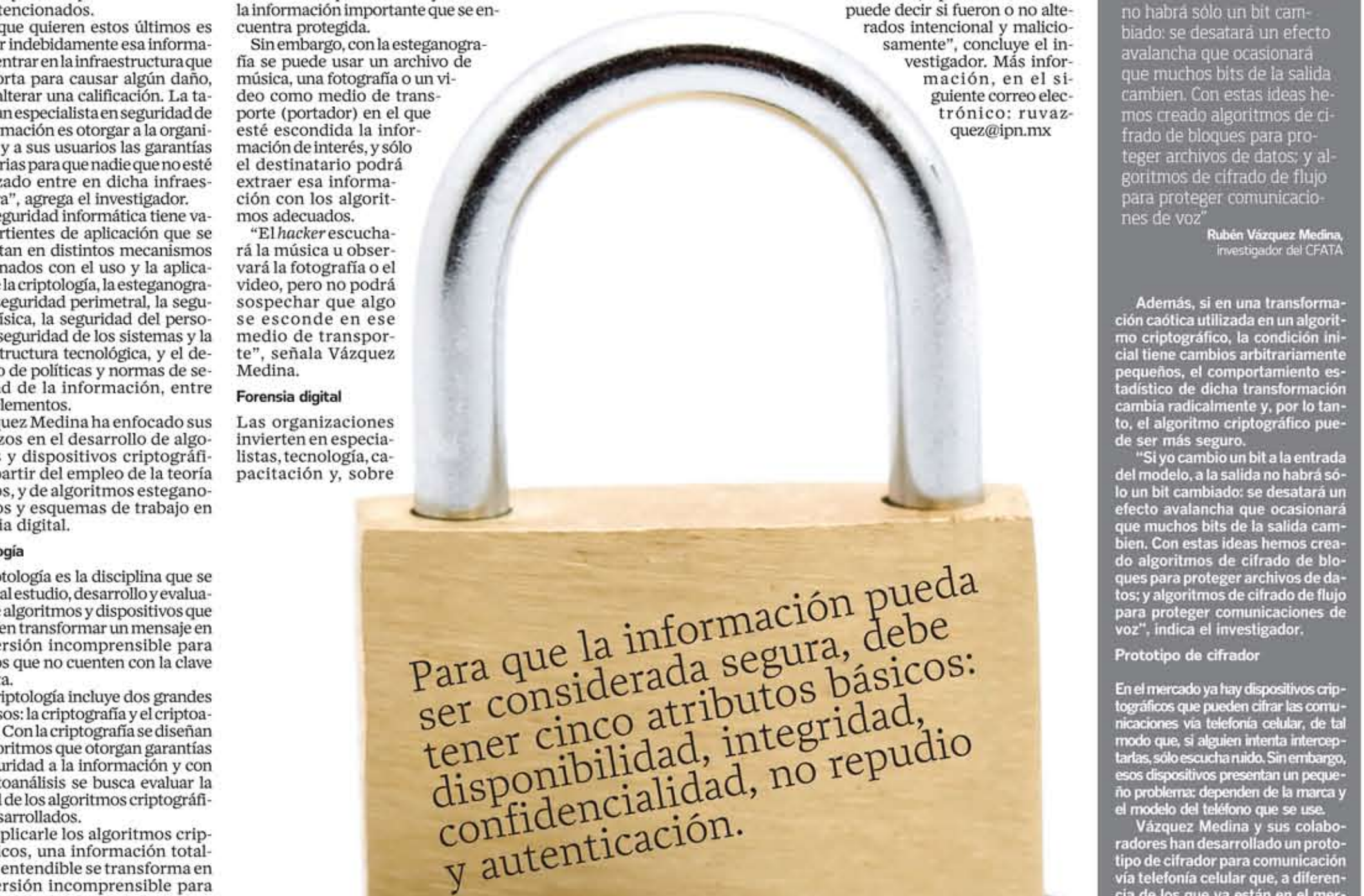
No se trata de traer a un gurú tecnológico, sino a alguien que sepa encontrar las evidencias de lo que pasó y las plasme en un informe legal que pueda ser enviado a un Ministerio Público o a una dependencia de administración de justicia para que la ley actúe. Esto es lo que, a grandes rasgos, atiende la forensia digital.

El campo de la forensia digital se ha ido extendiendo poco a poco. Muchas veces se presentan videos digitales, grabaciones de audio o fotografías como un argumento o un respaldo de alegatos.

Sin embargo, en muchos casos, alguno de esos videos digitales o alguna de esas grabaciones de audio o de esas fotografías está alterado o alterada y un juez no tiene las herramientas necesarias para descubrir el engaño.

Por eso se van a requerir en el futuro inmediato especialistas que analicen esos objetos digitales y emitan un dictamen en el que establezcan si han sido manipulados maliciosamente.

"Queremos formar especialistas que ayuden a establecer si un objeto digital fue alterado o no. Para eso hemos diseñado una metodología que determina los rasgos importantes de los objetos digitales, tanto de voz como de video, a partir de lo cual se puede decir si fueron o no alterados intencional y maliciosamente", concluye el investigador. Más información, en el siguiente correo electrónico: ruvazquez@ipn.mx



Teoría del caos

Vázquez Medina y sus colaboradores encontraron que la teoría del caos y la criptografía tienen algunas características muy parecidas, por lo que es posible crear algoritmos criptográficos con funciones caóticas.

La criptografía debe cumplir con dos propiedades: la difusión y la confusión de la información, que están relacionadas con el modo en que se desorganiza estadística y gramaticalmente un mensaje.

"Esto significa que debemos romper la reglas estadísticas, sintácticas y semánticas de ese mensaje para que, si es intervenido indebidamente, solamente se escuche o se lea 'ruido'."

La teoría del caos proporciona a los investigadores universitarios modelos matemáticos simples que pueden aprovechar en la creación de sistemas criptográficos o esteganográficos.

Tales modelos simples son las transformaciones caóticas unidimensionales, que poseen básicamente dos aspectos importantes cuando se aplican en criptografía: la dependencia ante condiciones iniciales y la propiedad de mezclado.

La primera puede asociarse a las claves con que se hace funcionar un algoritmo criptográfico; y la segunda, a la capacidad de la transformación caótica para lograr los procesos de confusión y difusión en un mensaje protegido criptográficamente.

Así, lo que se busca cuando se diseñan algoritmos criptográficos es que el universo de condiciones iniciales sea lo más grande posible, de manera que el conjunto de claves criptográficas sea también grande.

La importancia de tener un conjunto grande de condiciones iniciales radica en el hecho de que un atacante tendría que probar tantas claves como posibles condiciones iniciales.

> "Si yo cambio un bit a la entrada del modelo, a la salida no habrá sólo un bit cambiado: se desatará un efecto avalancha que ocasionará que muchos bits de la salida cambien. Con estas ideas hemos creado algoritmos de cifrado de bloques para proteger archivos de datos; y algoritmos de cifrado de flujo para proteger comunicaciones de voz"
>
> **Rubén Vázquez Medina,** investigador del CFATA

Además, si en una transformación caótica utilizada en un algoritmo criptográfico, la condición inicial tiene cambios arbitrariamente pequeños, el comportamiento estadístico de dicha transformación cambia radicalmente y, por lo tanto, el algoritmo criptográfico puede ser más seguro.

"Si yo cambio un bit a la entrada del modelo, a la salida no habrá sólo un bit cambiado: se desatará un efecto avalancha que ocasionará que muchos bits de la salida cambien. Con estas ideas hemos creado algoritmos de cifrado de bloques para proteger archivos de datos; y algoritmos de cifrado de flujo para proteger comunicaciones de voz", indica el investigador.

Prototipo de cifrador

En el mercado ya hay dispositivos criptográficos que pueden cifrar las comunicaciones vía telefonía celular, de tal modo que, si alguien intenta interceptarlas, sólo escucha ruido. Sin embargo, esos dispositivos presentan un pequeño problema: dependen de la marca y el modelo del teléfono que se use.

Vázquez Medina y sus colaboradores han desarrollado un prototipo de cifrador para comunicación vía telefonía celular que, a diferencia de los que ya están en el mercado, puede usarse en todas las marcas y modelos de teléfonos con una interfase bluetooth y es más económico.

Lo novedoso es que en él se aplicó la teoría del caos, en particular las transformaciones caóticas unidimensionales, de las que se eligieron las más adecuadas. Éstas son funciones discretas que, dependiendo de cómo se seleccione uno de sus parámetros, pueden generar una secuencia fija de números o una secuencia aleatoria, que parece ruido.

"De esta manera tenemos el control de las características estadísticas de esa secuencia, lo cual es importante para ese tipo de aplicaciones", comenta el investigador del CFATA.