Diario de Ávila
Ávila
29/11/15
Prensa: Diaria
Tirada: 2.633 Ejemplares
Difusión: 2.323 Ejemplares
Cod: 98652576
Página: 9
cción: LOCAL Valor: 2.582,00 € Área (cm2): 757,9 Ocupación: 79,68 % Documento: 1/1 Autor: MARTA MARTÍN GIL | ÁVILA marta.martin@di Núm. Lectores: 15000

ENTREVISTA

## Ángel Martín del Rey • Profesor de la Escuela Politécnica de Ávila

# «En un futuro todo se conectará a internet y eso es fantástico, pero vulnerable»

MARTA MARTÍN GIL | ÁVILA
marta.martin@diariodeavila.es

El profesor Ángel Martín del Rey, a la derecha de la imagen, durante su charla de esta semana en la Politécnica. / VANESSA GARRIDO

LA Semana de la Ciencia de Castilla y León de la Universidad de Salamanca ha contado esta semana con la intervención del profesor Ángel Martín del Río, experto en Matemáticas y Criptografía. Sobre estas materias charla con Diario de Ávila.

**En la conferencia que ha pronunciado esta semana al amparo de la Semana de la Ciencia ha hablado sobre protocolos criptográficos, ¿qué son y para qué sirven?**

A día de hoy, aparte de la actividad que desarrollamos en la vida corriente, también desarrollamos una actividad cada vez más grande en el ciberespacio. Para ello necesitamos que esa información que viaja o que se almacena esté protegida. La criptografía es una parte fundamental de todo este proceso y es la parte de las matemáticas que se dedica a crear algoritmos para proteger la información que está en formato digital, la confidencialidad, la privacidad, la integridad.

**¿Y es cada vez más complicado proteger esa información a la vista de cómo avanza todo y de los conocimientos que tiene gente que no los va a usar lícitamente?**

Soluciones criptográficas existen y son seguras y lo utilizan los gobiernos, las administraciones públicas y nosotros para protegernos pero, como dices tú, también están los malos que las utilizan para sus fines. Por ejemplo, los terroristas para comunicarse de forma segura, como con la aplicación Telegram que permite cifrar los mensajes. Claro, los malos también intentan atacar los sistemas informáticos que están protegidos, como los de una central nuclear. Para atacarla tendrían que romper esos protocolos criptográficos, luego necesitan saber de criptografía. Es la pescadilla que se muerde la cola. Por un lado la comunidad gubernamental y académica que intenta ir sacando soluciones criptográficas cada vez más avanzadas y por otra los malos que intentan romper esos protocolos.

**¿Hay que intentar ir siempre un paso por delante?**

Sí, claro.

**¿Y se está consiguiendo?**

Aparentemente sí. Por ejemplo en el DNI electrónico se utiliza un criptosistema que es el RSA, que supone que con la longitud de claves que utilizamos de 2.048 bits es segura. La Agencia de Seguridad Americana tiene unas directrices que indica a que tendencias en criptografía tenemos que tender. Decían que cuando el RSA se vea que empieza a ser inseguro habría que emigrar todos los sistemas hacia otros. Ese era el plan. Pero ahora dicen que ese plan hay que olvidarlo y hay que investigar en la criptografía postcuántica. Quiere decir que si existieran los ordenadores cuánticos, por ejemplo el RSA se rompería. Osea, que ya existen ordenadores cuánticos y que los malos pueden romper el RSA. Es un tema que está muy vivo, que siempre están saliendo soluciones informáticas, que los malos están intentando romperlas siempre y que hay que estar constantemente investigando.

Las agencias gubernamentales tienen la dicotomía de intentar crear soluciones cada vez mejores pero al mismo tiempo, ver cómo son capaces de que si los malos usan esas soluciones, cómo romperlas.

**Hablamos de protección pero supongo que también tendrá mucho que ver en la prevención de atentados...**

Claro, los servicios de inteligencia siempre tienen sus agencias propias que se dedican a ello. Así se ha podido saber lo de Telegram, porque después de la bomba del avión ruso y de los atentados de París hubo un pico de comunicaciones usando esta mensajería. Cifran la información y si fuéramos capaces de descifrar esas comunicaciones podríamos ir por delante de ellos y tratar de evitarlo. Pero claro, estás usando unas aplicaciones que tienen que ser seguras para el ciudadano normal y corriente pero no las puedes romper directamente.

**¿Hay que hacer mucho trabajo de educación en el buen uso de la información?**

Sí, sobre todo enseñando a los niños como protegerse en internet, porque tienen todo a su alcance.

> «Los servicios de **inteligencia** siempre tienen sus agencias propias que se dedican a ello»
>
> «Las empresas que se vuelcan a la seguridad están **creciendo** un 10% anual»
>
> «Hay que **desarrollar** aplicaciones para proteger todo»

**¿Y cómo se podría animar a un chico de instituto a que se lance a estudiar Matemáticas?**

En este mundo hay gente de Matemáticas, ingenieros, informáticos... Es una materia pluridisciplinar. A este mundo se dedican matemáticos que han estudiado informática y al contrario. El mundo de la seguridad de la información tiene mucho futuro. Las empresas que se dedican a seguridad están creciendo del orden de un 10% anual. ¿Y por qué crecen a ese ritmo? Porque es necesario. En un futuro muy cercano todo se conectará a internet. Y ese escenario, que es fantástico, también es muy vulnerable. Así que por una parte hay que desarrollar aplicaciones informáticas para proteger todo esto y por otra concienciar a la gente de que cuando vayas a usar todo esto hay que hacerlo de forma segura.

**¿Y qué hay que hacer para trabajar en esta materia?**

Hacer una titulación y un master que te especialice. Y la gente sale colocada.