EL MUNDO DE CASTILLA Y LEON(INNOVADORES) 05/03/12
VALLADOLID

Prensa: Semanal (Lunes)
Tirada: 25.906 Ejemplares
Difusión: 20.081 Ejemplares

Cod: 55614223

Página: 3

Sección: OTROS Valor: 1.028,00 € Área (cm2): 260,1 Ocupación: 27,94 % Documento: 1/1 Autor: Núm. Lectores: 80324

LA RED AVANZA

PROTECCIÓN

La Universidad de Salamanca trabaja en la modificación de protocolos y algoritmos de intercambio de información en la web

Sistema 'multifirma' para mejorar la seguridad en internet

Un proyecto de la Universidad de Salamanca busca mejorar la seguridad para la identificación electrónica de los usuarios de internet y la autentificación de la información que envían, es decir, contribuir a que las comunicaciones sean más seguras. Para ello, los investigadores trabajan en la modificación de protocolos y de algoritmos de intercambio de información que se emplean en la actualidad y tratar de implementar otros nuevos.

Usos como la banca electrónica, el comercio electrónico o distintos servicios de las administraciones públicas requieren contar con una identidad electrónica. Aunque la seguridad es cada vez mayor en la red, también se están incrementando los ataques que buscan conseguir suplantar identidades y acceder a información privilegiada. Por eso, Araceli Queiruga, investigadora del Departamento de Matemática Aplicada de la Universidad de Salamanca, trabaja en esta línea y ya el pasado año desarrolló un sistema calificado de multifirma, es decir, que permite que varias personas puedan firmar digitalmente un mismo documento, lo que se plasmó en un programa diseñado en lenguaje Java.

Araceli Queiruga, experta en criptografía./ DICYT

La investigadora explica las claves del nuevo trabajo. «Para usar un servicio electrónico tienes que identificarte y, cuando envías algo a alguien, esa persona tiene que estar segura de que eres tú quien envía la información y de que esa información es la que tú envías, que nadie la modifica en medio», comenta, distinguiendo así entre identificar a los usuarios y autentificar la información.

Cada sistema de criptografía se basa en diferentes problemas matemáticos. El RSA es un algoritmo basado en la factorización de números enteros y su funcionamiento depende de dos números primos secretos. Se trata del sistema más común, pero estos números son muy largos para aumentar la seguridad y esto complica las operaciones en dispositivos con poca capacidad. Por eso también se utilizan los logaritmos discretos basados en ecuaciones, aunque el problema es parecido. / DICYT