III CICLO DE CONFERENCIAS

Chateando con la Ciencia

DURACIÓN DE CICLO: OCTUBRE 2018–JUNIO 2019

Luis Hernández Encinas
Investigador del CSIC en el Instituto Tecnologías Físicas y de la Información

Criptografía y Seguridad: Realidades, Mitos y Leyendas

La Criptografía es la ciencia que tiene como objetivo diseñar sistemas seguros que permitan las comunicaciones secretas entre individuos. Además, debe ofrecer privacidad y permitir la autenticación de los usuarios y de la información intercambiada. Para ello, hace uso de protocolos como el cifrado de datos, la firma electrónica, el intercambio de claves, etc.

En esta charla se presentarán algunos de los hitos más relevantes de la criptografía a lo largo de su historia (Alejando Magno, Julio César, la máquina Enigma, Alan Turing, etc.) hasta llegar a los aspectos de cómo la criptografía moderna es empleada a diario por los usuarios y la seguridad que ofrece (banca por internet, firmas electrónicas, mensajería instantánea, etc.). Para terminar, se mostrarán los usos actuales y las últimas tendencias que están relacionadas tanto con la seguridad de los dispositivos físicos que empleamos a diario (teléfonos moviles, tabletas, tarjetas inteligentes, etc.) como con la computación cuántica.

Día: jueves, 21 de **marzo de** *2019*

Hora: 19:30

Lugar: Real Zaragoza Club de Tenis

Dirección: Carretera del Aeropuerto Km. 5,800

Entrada gratuita hasta completar aforo

Luis Hernández Encinas nació en 1957 en Navalmoral de la Mata (Cáceres), obtuvo su Licenciatura en Ciencias Matemáticas en 1980 y su doctorado en Matemáticas en 1992 por la Universidad de Salamanca.

Ha sido profesor de Enseñanza Secundaria entre 1980 y 1990 y Profesor Titular de la Universidad de Salamanca entre 1990 y 2000. Desde el año 2000 es Investigador Científico en el Departamento de Tecnologías de la Información y las Comunicaciones (TIC,) en el Instituto de Tecnologías Físicas y de la Información (ITEFI) "Leonardo Torres Quevedo" del Consejo Superior de Investigaciones Científicas (CSIC) en Madrid.

Ha participado en más de 30 proyectos de investigación, tanto nacionales como internacionales. Es autor de varios libros y patentes, más de 200 artículos en revistas especializadas, más de 120 contribuciones a congresos, ha dirigido varias tesis doctorales y es recensor y revisor de diferentes revistas indexadas y de numerosos congresos internacionales. Pertenece a varios comités nacionales e internacionales sobre Seguridad y Ciberseguridad y es asesor criptográfico de Organismos de Seguridad nacionales.

Sus líneas de investigación incluyen la Criptografía y el Criptoanálisis de criptosistemas de clave pública, generadores de números pseudo-aleatorios, esquemas de firma digital, protocolos de autenticación e identificación, criptobiometría, protocolos de compartición de secretos, ataques criptográficos por canales laterales y problemas de teoría de números.

http://www.itefi.csic.es/es/personal/hernandez-encinas-luis

Real Zaragoza Club de Tenis 1907

icma Instituto de Ciencia de Materiales de Aragón