madri+d

Matemáticas y sus fronteras

- BLOGS madri+d
- PORTADA BLOG
- GALERIAS IMAGENES

El hombre que se enfrentó a la NSA

Publicado por **Matemáticas y sus fronteras** el **22 noviembre, 2016** Editar
Comentarios (0)

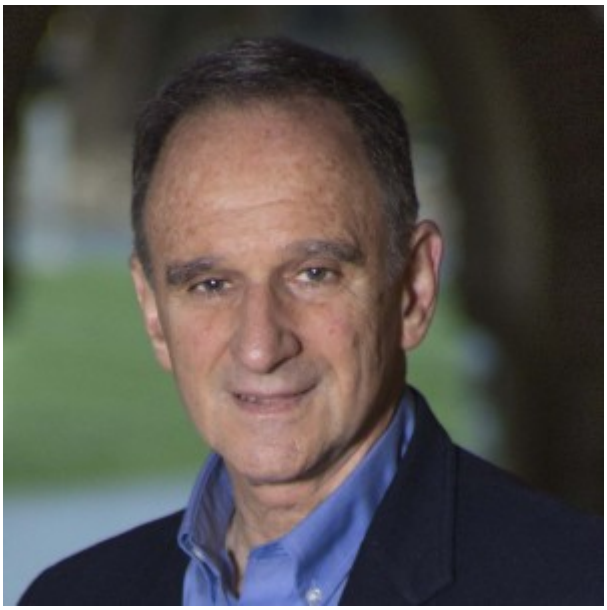
Tweet

En la entrada anterior contábamos el nacimiento hace unos cuarenta años de los protocolos criptográficos llamados de clave pública. Estos avances científicos supusieron el comienzo de una batalla entre la comunidad científica y la Agencia Nacional de Seguridad de los Estados Unidos (NSA) que continúa a día de hoy.

Sede de la NSA en Fort Meade, Maryland

Nos vamos atrás en la historia al año 1977. Hasta entonces, la criptografía era cosa de seguridad nacional, pero los avances que estaban experimentado los computadores anunciaban esta necesidad también para el sector privado.

El campo de batalla fue el ***International Symposium on Information Theory***, que se celebró en la Universidad de Cornell el 10 de octubre de 1977; y el detonante, la presentación de un grupo de investigadores de la Universidad de Stanford, Martin Hellman, profesor asociado de ingeniería eléctrica y sus dos estudiantes de doctorado, Steve Pohlig y Ralph Merkle. Ya un año antes, Hellman había publicado con otro de sus estudiantes, Whitfield Diffie, un artículo titulado “New Directions in Cryptography”, en el que introducía lo que se llama protocolo Diffie-Hellman.



Martin E. Hellman

El artículo se había publicado en las revistas del IEEE (Institute of Electrical and Electronics Engineers) una sociedad científica centrada en las ingenierías, un auténtico monstruo que hoy cuenta con 420.000 miembros. Y la NSA lo leyó y enviaron una carta no oficial amenazando a Hellman con represalias, ya que consideraban que la criptografía sólo podía estar en manos de la seguridad nacional. Incluso se argumentaba que la criptografía era un arma y su publicaión contravenía la ley de exportación de armas. Temiendo represalias, Hellman defendió su causa con la ayuda de su universidad. Esta concluyó que todo era legal.

Sin embargo, ya que Pohlig y Merkle eran estudiantes, las presentaciones corrieron a cargo del propio Hellman. Todo transcurrió sin incidentes. Y realmente, el uso que se dió a este protocolo fue sobre todo en seguridad por el gobierno (y por los traficantes de drogas).

Bobby Inman

El nuevo director de la NSA, Bobby Ray Inman, contactó con los investigadores, descubriendo que

su interés había sido el de buscar protección para los ordenadores, lo que entonces era un problema incipiente y que había pasado inadvertido a la NSA.

El problema se complicó cuando en agosto de 1977, Ron Rivest, Adi Shamir y Leonard Adleman, del Massachusetts Institute of Technology (MIT), dieron a conocer su sistema RSA. El tema era ya incontrolable, aunque el gobierno ha contado siempre con un poderoso instrumento, la financiación a través de la National Science Foundation (NSF) y de la propia NSA. Y ha creado el National Bureau of Standards (NIST), que homologa los productos criptográficos.

Es digno de reconocimiento el valor de Martin Hellman, nacido en octubre de 1945, y entonces un joven de 32 años. Hellman fue el principal protagonista en esta primera "crypto war" con la administración gubernamental. Son muchos los premios y honores que Hellman ha conseguido desde entonces, y quizás el más relevante es el Premio Turing en 2015, que se suele considerar como el Nobel de la Computación. Hellman está usando el millón de dólares del premio para impulsar sus proyectos para el diálogo y la paz en el mundo. También ha sido reconocido su trabajo para disminuir las tensiones étnicas. Las personas interesadas pueden seguirle en su página web y en su blog.

No cabe duda de que en un mundo cada vez mas interconectado, esta disputa continuará, pero no será fácil ponerle puertas al campo de la investigación.

Manuel de León (CSIC, Fundador del ICMAT, Real Academia de Ciencias, Real Academia Canaria de Ciencias, ICSU) y **Cristina Sardón** (ICMAT-CSIC).

Etiquetas: criptografía, IEEE, NSA, seguridad
General

Si te gustó esta entrada anímate a escribir un comentario o suscribirte al feed y obtener los artículos futuros en tu lector de feeds.

Comentarios

Aún no hay comentarios.

Escribe un comentario

Registrado como Matemáticas y sus fronteras. Salir »

Tu Comentario

Enviar

RSS

Buscar en el blog... IR

noviembre 2016

L	M	X	J	V	S	D
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

« oct

Contador de visitas

00576280

Archivos

- noviembre 2016
- octubre 2016
- septiembre 2016
- agosto 2016
- julio 2016
- junio 2016
- mayo 2016
- abril 2016
- marzo 2016
- febrero 2016
- enero 2016
- diciembre 2015
- noviembre 2015
- octubre 2015
- septiembre 2015
- agosto 2015
- julio 2015
- junio 2015
- mayo 2015
- abril 2015
- marzo 2015
- febrero 2015

- octubre 2010
- septiembre 2010
- agosto 2010
- julio 2010
- junio 2010
- mayo 2010
- abril 2010
- marzo 2010
- febrero 2010
- enero 2010
- diciembre 2009
- noviembre 2009
- octubre 2009
- septiembre 2009
- agosto 2009
- julio 2009
- junio 2009
- mayo 2009
- abril 2009
- marzo 2009
- febrero 2009
- enero 2009
- diciembre 2008
- noviembre 2008
- octubre 2008
- septiembre 2008
- agosto 2008
- julio 2008
- junio 2008
- mayo 2008
- abril 2008
- marzo 2008
- febrero 2008
- enero 2008
- diciembre 2007
- noviembre 2007
- octubre 2007
- septiembre 2007
- agosto 2007
- julio 2007
- junio 2007
- mayo 2007
- abril 2007
- marzo 2007
- febrero 2007
- enero 2007
- diciembre 2006
- noviembre 2006
- octubre 2006
- septiembre 2006
- agosto 2006

- julio 2006
- junio 2006

Entradas recientes

- El hombre que se enfrentó a la NSA
- ¿Estamos seguros?
- Las raíces de los matemáticos
- Haciendo historia en St Andrews: MacTutor
- La física de Fermat
- Los otros teoremas de Fermat
- Lecciones de una mesa redonda
- Transferencia del conocimiento matemático
- El monumento a Abel
- ICSU e ISSC afrontan un día histórico para la ciencia

Enlaces

- DivulgaMAT
- ESTALMAT
- La Hoja Volante
- MATEMATICALIA

WEBLOGS

- :: ZTFNews.org
- Bloc de la Biblioteca de Matemàtiques
- Blog para anti-matematicos
- BUCM :: 2+2=5 :: Biblioteca Complutense
- Complejidad
- Democracia electronica
- Francis (th)E mule Science's News
- Gaussianos
- MATBUS
- Michael Trick’s Operations Research Blog

Páginas

- GALERIAS IMAGENES

Comentarios recientes

- Pedro Alonso en Las raíces de los matemáticos
- JOSE DAVID AREVALO COBOS en Las raíces de los matemáticos
- JOSE DAVID AREVALO COBOS en Las raíces de los matemáticos
- Darryl Holm en La física de Fermat
- Estuardo aquino en La mujer que explicó la fisión nuclear

Etiquetas

Abel Astronomía conjetura abc criptografía ecuación de quinto grado Escuela de Doctorado Formación Física estadística Johannes Kepler luz mochizuki Mujeres matemáticas Música Neurociencia suicidios científicos Sísifo teoría de números transferencia matemáticas

- **Acceso usuarios**

- Administrador del sitio
  Desconectar

- Inicio
- GALERIAS IMAGENES
- - Desconectar