novática
UPGRADE Revista de la Asociación de Técnicos de Informática

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática). ***Novática*** edita también ***Upgrade***, revista digital de **CEPIS** (*Council of European Professional Informatics Societies*), en lengua inglesa, y es miembro fundador de **UPENET** (*UPGRADE European NETwork*)

<http://www.ati.es/novatica/>
<http://www.upgrade-cepis.org/>

ATI es miembro fundador de **CEPIS** (*Council of European Professional Informatics Societies*) y es representante de España en **IFIP** (*International Federation for Information Processing*); tiene un acuerdo de colaboración con **ACM** (*Association for Computing Machinery*), así como acuerdos de vinculación o colaboración con **AdaSpain**, **AI2** y **ASTIC.**

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Padilla 66, 3º, dcha., 28006 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Composición, Edición y Redacción ATI Valencia
Av. del Reino de Valencia 23, 46005 Valencia
Tlfn./fax 963330392 <secreval@ati.es>
Administración y Redacción ATI Cataluña
Via Laietana 41, 1º, 1ª, 08003 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>
Redacción ATI Andalucía
Isaac, Newton, s/n, Ed. Sadiel,
Isla Cartuja 41092 Sevilla, Tlfn./fax 954460779 <secreand@ati.es>
Redacción ATI Aragón
Lagasca, 9, 3-B, 50006 Zaragoza.
Tlfn./fax 976235181 <secreara@ati.es>
Redacción ATI Asturias-Cantabria <gp-astucant@ati.es>
Redacción ATI Castilla-La Mancha <gp-clmancha@ati.es>
Redacción ATI Galicia
Recinto Ferial s/n, 36540 Silleda (Pontevedra)
Tlfn.986581413; fax 986580162 <secregal@ati.es>
Suscripción y Ventas
<http://www.ati.es/novatica/interes.html>,o en ATI Cataluña o ATI Madrid
Publicidad
Padilla 66, 3º, dcha., 28006 Madrid
Tlnf.914029391; fax.913093685 <novatica.publicidad@ati.es>
Imprenta
Derra,S.A., Juan de Austria 66, 08005 Barcelona.
Depósito legal: B.15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Portada: Antonio Crespo Foix / © ATI 2004
Diseño: Fernando Agresta / © ATI 2004

Nº 172, noviembre-diciembre 2004, año XXX

sumario

Monografía del próximo número: "*XML*"

Arturo Ribagorda Garnacho[1], Javier Areitio Bertolín[2], Jacques Stern[3]

[1] Depto. de Informática, Universidad Carlos III de Madrid; [2] Universidad de Deusto (Bilbao); [3] Département d'Informatique, École Normale Supérieure, París (Francia)

<arturo@inf.uc3m.es>, <jareitio@eside.deusto.es>, <Jacques.Stern@ens.fr>

Presentación
Criptografía: la clave de la seguridad de la información en el siglo XXI

Editores invitados

Arturo Ribagorda Garnacho es Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid y Doctor en Informática por la misma Universidad. Es Catedrático de Universidad y Director del Depto. de Informática de la Universidad Carlos III de Madrid, de cuya Escuela Politécnica Superior ha sido director. Su actividad académica se centra en la Seguridad de las Tecnologías de la Información, campo en el que participa en diversos proyectos de investigación nacionales y europeos, ha publicado más de 100 artículos en revistas nacionales e internacionales, y presentado numerosas ponencias en congresos. Asimismo es autor de cuatro libros sobre la citada materia.

Javier Areitio Bertolín es Doctor en Físicas por la Universidad del País Vasco. Es Catedrático de la Facultad de Ingeniería, ESIDE, Departamento de Telecomunicaciones de la Universidad de Deusto y Director del Grupo de Investigación Redes & Sistemas. Es evaluador de CORDIS (*Community Research and Development Information Service*), Comisión Europea, Dirección General XIII-D.2, y tutor de la AECI (Agencia Española de Cooperación Internacional). Su especialización y áreas de investigación son la Seguridad en Tecnologías de la Información y las Comunicaciones (utilizando la Criptografía aplicada y el Criptoanálisis) un campo donde ha trabajado en numerosos proyectos de investigación nacionales e internacionales. Es ponente, moderador y evaluador habitual de congresos, seminarios y simposios, y autor de numerosos artículos científicos en revistas especializadas y de diversos libros técnicos sobre Seguridad en Redes de Computadoras, Criptografía y Criptoanálisis. Actualmente dirige proyectos sobre Seguridad / Criptografía en Tecnologías de la Información y las Comunicaciones con empresas españolas y participa en proyectos europeos con otras iniversidades. Pertenece a diversas asociaciones españolas y extranjeras, entre ellas a ATI, siendo coordinador de la Sección Técnica "Seguridad" de su revista ***Novática***.

Jacques Stern obtuvo el Doctorado en la *École Normale Supérieure* de París (Francia), en la que, después de ejercer labores docentes en diversas universidades, es actualmente Profesor y Director de su Laboratorio de Informática. Es experto en Criptografía y autor de más de un centenar de publicaciones, habiendo registrado 10 patentes. También ha trabajado como consultor para diversas empresas y organizaciones. Fue Presidente del Comité de Programa de Eurocrypt 99 y orador invitado en Eurocrypt 03. Sus actividades de investigación se centran en las siguientes áreas: teoría de la complejidad, criptografía de clave pública, cifrado convencional de bloques, protocolos criptográficos, criptoanálisis, teoría de la codificación y correción de errores, firma, autentificación y corrtrol de acceso, y aplicaciones de tarhetas inteligentes. Es miembro de diversos comités consultivos del Gobierno francés, tiene el título de *Chevalier de la Legion d'Honneur* y en 2003 obtuvo el Premio Lazare Carnot otorgado por la Academia Francesa de las Ciencias..

Hoy en día la Criptografía presenta una pujanza inusual tratándose de una disciplina ancestral que hunde sus raíces en la antigüedad clásica. Además cubre una gran cantidad de campos, prácticamente la totalidad de los que hoy conforman la llamada "Seguridad de la Información". Por ello hemos escogido un puñado de artículos que ponen de manifiesto esta diversidad y dinamismo, concentrándose en algunos de los aspectos más candentes que esta disciplina presenta hoy, pero dejando al margen --no por falta de interés, sino para adecuar los contenidos a los lectores de ***Novática*** y de ***UPGRADE***-- aquellos aspectos más algorítmicos de la materia, más difíciles de seguir por el no especialista.

Comenzamos con una breve introdución sobre lo que hoy es y significa la Criptografía, titulada "*Criptografía: una breve panorámica*", y continuamos con un artículo en el que se trata un problema latente en Internet que genera una acusada desconfianza y, a menudo, lleva incluso a desechar la red como medio de intercambio de información: su falta de anonimidad; este problema es abordado por ***Joan Mir Rubio***, ***Joan Borrell Viader*** y ***Vanesa Daza Fernández*** en "*Un Canal de Comunicaciones Anónimo*", donde se presenta una solución elegante y robusta a dicho problema. A renglón seguido, ***Mónica Breitman Mansilla***, ***Carlos Gete Alonso***, ***Paz MorilloBosch*** y ***Jorge L. Villar Santos,*** en "*Aplicación del Doble Cifrado a la Custodia de Claves*", estudian, y proponen una solución, a otro problema candente en la actualidad: la custodia de las claves usadas en los sistemas de clave secreta.

Por su parte, ***Slobodan Petrovic*** y ***Amparo Fúster Sabater***, en "*Reconstrucción de la secuencia de control en Generadores con Desplazamiento Irregular*", plantean un novedoso ataque criptoanalítico sobre un tipo de cifradores muy usuales, los de flujo controlados por generadores constituidos por registros de desplazamiento alimentados linealmente. El cifrado de imágenes, poco contemplado hasta hace escasos años, está siendo objeto en la actualidad de un creciente interés, y a su examen se dedica el artículo, "*Cifrado de imágenes usando Autómatas Ccelulares con Memoria*", cuyos autores -- ***Luis Hernández Encinas***, ***Ascensión Hernández Encinas***, ***Sara Hoya White***, ***Ángel Martín del Rey*** y ***Gerardo Rodríguez Sánchez***-- exponen un nuevo criptosistema gráfico, que soslaya los inconvenientes de otras propuestas anteriores.

A continuación, ***María de Miguel de Santos***, ***Carmen Sánchez Ávila*** y ***Raúl Sánchez Reillo***, en "*Aplicaciones de la Criptografía de Curva Elíptica*", comparan los cifrados basados en curvas elípticas frente a aquellos, mucho más extendidos hoy en día, basados en problemas clásicos de la Teoría de Números, como la factorización de enteros o el logaritmo discreto, concluyendo que estos criptosistemas basados en curvas elípticas son idóneos para su uso en sistemas con recursos restringidos. Seguidamente, en "*Hacia una herramienta de enseñanza por ordenador para la Criptografía*", sus autores ***Vasilios Katos, Terry King*** y ***Carl Adams***, presentan un sistema de enseñanza de la Criptografía basado en una herramienta automatizada, cuya lectura presenta el interés añadido de proporcionar una sucinta y completa visión de múltiples aspectos tratados por la actual disciplina. Cerramos la monografía con un artículo más centrado en la seguridad, de la que la Criptografía constituye un pilar fundamental, escrito por ***Yvo Desmedt***; "*Análisis científico del ciberterrorismo*" es un profundo estudio, de innegable actualidad, en el que se propone un modelo de identificación de las infraestructuras críticas para nuestras sociedades avanzadas, así como de los ataques a las mismas.

Al cerrar esta presentación, que va seguida de las habituales "Referencias útiles" sobre la materia, queremos agradecer a los editores de ***Novática*** y ***UPGRADE*** la oportunidad de elaborar esta monografía, que esperamos sea de interés para los lectores de ambas revistas.

Referencias útiles sobre Criptografía

Las siguientes fuentes, junto con las referencias que figuran en los artículos de esta monografía, posibilitarán a los lectores interesados conocer más en detalle y profundidad el tema objeto de la misma.

Congresos y reuniones científicas

■EuroCrypt2005, evento organizado por la IARC (*International Association for Cryptologic Research*) y la Universidad de Aarhus (Dinamarca). <http://www.brics.dk/eurocrypt05/>.
■ RECSI (Reunión Española sobre Criptología y Seguridad de la Información), última edición celebrada en Madrid en septiembre de 2004. <http://www.uc3m.es/recsi/>.
■SECURMATICA (Congreso de Seguridad en Tecnologías de Información y Comunicaciones). <http://www.securmatica.com/>.

Libros

■**Blake, G. Seroussi, and N. Smart**. *Advances in Elliptic Curve Cryptography: Further Topics v.2.* Cambridge University Press, 2004.
■**K. Bruen**. *Encryption, Error-Correction and Information Theory for the 21st Century.* John Wiley and Sons Inc., 2004.
■**N. Ferguson and B. Schneier**. *Practical Cryptography.* John Wiley & Sons Ltd., 2003.
■ **S. Katzenbeisser**. *User's Guide to Cryptography and Standards.* Artech House Publishers, 2004.
■**P. Gutmann**. *Design and Verification of a Cryptographic Security Architecture.* Springer Verlag, 2003.
■**S. Levy**. *CRYPTO: How the Code Rebels Beat the Government. Saving Privacy in the Digital Age.* Viking Press, 2001.
■**W. Mao**. *Modern Cryptography: Theory and Practice.* Prentice-Hall. PTR, 2003.
■**M. McLoone, J.V. McCanny**. *System-On-Chip Architectures and Implementations for Private-Key Data Encryption.* Plenum Pub Corp., 2004.
■**J. McNamara**. *Secrets of Computer Espionage: Tactics and Countermeasures.* John Wiley & Sons Ltd., 2003.
■**H.X. Mel, D.M. Baker**. *Cryptography Decrypted.* Addison-Wesley Publishing Company, 2000.
■ **R.A. Mollin**. *RSA and Public-Key Cryptography.* Chapman & Hall, 2002
■**M.Y. Rhee**. *Internet Security: Cryptographic Principles, Algorithms and Protocols.* John Wiley & Sons, 2003.
■**K. Schmeh**. *Cryptography and Public Key Infrastructure on the Internet.* John Wiley & Sons Ltd., 2003.
■ **B. Schneier**. *Applied Cryptography. Protocols, Algorithms and Source code in C.* 2nd. edición, John Wiley, 1996.
■**R.J. Spillman**. *Classical and Contemporary Cryptology.* Pearson Education, 2004.
■**W. Stallings**. *Cryptography and Network Security. Principles and practice.* Prentice Hall, 1999.
■**J. Stern**. *La Science du Secret.* Editions Odile Jacob, 2004.
■ **P. Thorsteinson**. *NET Security and Cryptography.* Prentice-Hall. PTR, 2003.

Sitios web

■CERT y Seguridad. <http://www.rediris.es/cert>.
■*Computer Security Group* de la Universidad de Cambridge (Reino Unido), página sobre recursos e intereses sobre Seguridad, incluida la Esteganografía. <http://www.cl.cam.ac.uk/Research/Security/>.
■COSIC (*Computer Security and Industrial Cryptography*). <http://www. esat.kuleuven.ac.be/>.
■IARC (*International Association for Cryptologic Research*), organización científica que investiga en Criptlogía y campos afines. <http://www.iacr.org>.
■Integración de la Criptografía dentro del mundo de las finanzas. <http://www.financialcryptography.com/>.
■Museo Criptológico Nacional de la NSA (*National Security Agency*), Maryland (EE.UU.). <http://www.nsa.gov/museum>.
■PGP (*Pretty Good Privacy*), programa desarrollado por Phil Zimmerman para proteger información digital como correos electrónicos. <http://www.pgpi.org>.
■ Red temática CriptoRed. <http://www.criptored.upm.es/>.
■RSA Security, empresa líder en soluciones criptográficas RSA. <http://www.rsasecurity.com/>.
■SCSI (*Service de Cryptografie et Securité Informatique, Université Libre de Bruxelles*, Bélgica). <http://www.ulb.ac.be/rech/inventaire/unites/ULB516.html>.
■Universidad de Columbia (EE.UU), enlaces sobre Criptografía. <http://www.columbia.edu/acis/rad/secure-server/crypto-policy-links.html>.

Un documento importante

■OCDE (Organización para la Cooperación Económica y el Desarrollo), Directrices para una Política Criptográfica. <http://www.csi.map.es/csi/pg4811.htm>.