Matemáticas en la Sociedad de la Información

La Suite B de la National Security Agency

Anna Rio

Departament de Matemàtica Aplicada II
Universitat Politècnica de Catalunya

Murcia, 24-25 de Nov. de 2006

Recent Events (NIST)

- FIPS 186-3 Digital Signature Standard began Public Review
  - Extend DSA to include 2048-bit and 3072-bit keys
  - ECDSA and RSA also updated
  - Public Review ends June 12th
- NIST SP 800-56A: Recommendation for Par-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
  - Posted: March 2006
  - Covers FFC and ECC Diffie-Hellman and MQV schemes

The Future - Near Term (NIST)

- Start issuing Pub. Key certificates with at least 2k FFC or 224 bit ECC keys and SHA-256 or SHA-224 by 2008
- Stop using 80-bit equivalent crypto by 2010

  Don't rely on 2key TDEA, SHA-1 (for signatures), 160-bit ECDSA, 1024-bit RSA, 1024-bit DSA, 1024-bit DH and MQV key agreement after Dec 31, 2010

Sym. Key	80	112	128	192	256
Hash functions	160	224	256	384	512
FFC and IFC	1k	2k	3k	7.5k	15k
ECC	160	224	256	384	512

Future for Public Key Crypto (NIST)

- NIST expects to allow continued use of finite field public key cryptography for the foreseeable future

  Need 2048-bit keys after 2010

- NIST encourages movement to Elliptic Curve methods for 128-bit equivalent public key crypto

  May never see wide use of 3k FFC and IFC PK algorithms

  ECC patents should be a minor issue long before we need 128-bit equivalent public key crypto in most unclassified applications

  With bigger keys, ECC is much more efficient

- NIST encourages adoption of MQV key agreement protocol

NSA Names ECC as the Exclusive Technology for Key Agreement and Digital Signature Standards for the U.S. Government (www.certicom.com)

- Elliptic Curve Cryptography (ECC) will soon become the standard to protect U.S. government communications.
- On February 16, 2005 at the RSA conference, the National Security Agency (NSA) presented its strategy and recommendations for securing U.S. government sensitive and unclassified communications.

  > *NIST and NSA have been working to offer a standardized, public set of algorithms that can be used to protect both unclassified and classified information*

- The strategy included a recommended set of advanced cryptography algorithms known as **Suite B** for securing sensitive but unclassified data.

Suite B - the algorithms

- Encryption Algorithm AES (FIPS 197)
  AES-128 up to SECRET
  AES-256 up to TOP SECRET
- Digital Signature (FIPS 186-3)
  ECDSA with 256-bit prime modulus up to SECRET
  ECDSA with 384-bit prime modulus up to TOP SECRET
- Key Agreement (NIST SP 800-56A)
  EC Diffie-Hellman or EC MQV with 256-bit prime mod. up to SECRET
  EC Diffie-Hellman or EC MQV with 384-bit prime modulus up to TOP SECRET
- Hash Functions (FIPS 180-2)
  SHA-256 up to SECRET
  SHA-384 up to TOP SECRET

16/3/2006 El ministro de Interior, José Antonio Alonso, ha presidido esta mañana en Burgos el acto de entrega del primer DNI electrónico a un ciudadano. El nuevo documento, que incluye mayores medidas de seguridad y un microchip en el que almacena información sobre el titular en formato digital, podrá expedirse en todo el territorio nacional en 2008.

El DNIe es una tarjeta en la que figura un chip que almacena datos sobre el usuario. Éste está dotado con las últimas tecnologías de cifrado de datos, protección destinada a evitar que la información sobre su titular sea revelada sin su consentimiento.

Datos criptográficos eDNI

- Clave RSA pública de autenticación (Digital Signature).
- Clave RSA pública de no repudio(ContentCommitment).
- Clave RSA privada de autenticación (Digital Signature).
- Clave RSA privada de firma (ContentCommitment).
- Patrón de impresión dactilar.
- Clave Pública de root CA para certificados card-verificables.
- Claves Diffie-Hellman.

Claves eDNI

- El tamaño de las claves de la AC Raíz es de 4096 bits
- El tamaño de las claves de las AC Subordinadas será de 2048 bits
- El tamaño de las claves de los certificados de identidad pública es de 2048 bits

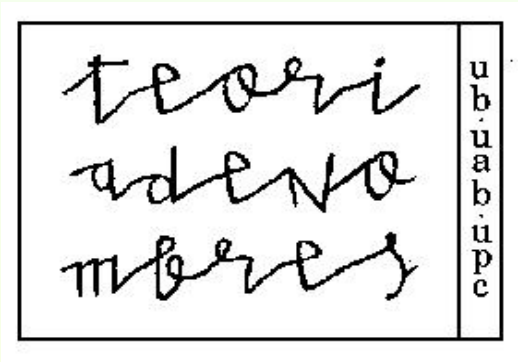
Autoridades Certificadoras

- Fábrica Nacional de Moneda y Timbre (http://www.fnmt.es)
- CATCert (http://www.catcert.net)
- Camerfirma (http://www.camerfirma.com)
- Firma Profesional (http://www.firmaprofesional.com)
- Asociación Nacional de Fabricantes (http://www.anf.es)
- Autoridad de Certificación de la Abogacía (http://www.acabogacia.org)
- Agencia Notarial de Certificación (http://www.ancert.com)
- Autoritat de Certificació de la Comunitat Valenciana (http://www.accv.es)
- Izenpe (http://www.izenpe.com)

Objetivos

- Incorporar la firma digital y los protocolos de intercambio de claves con curvas elípticas
- Construcción de curvas adecuadas para la criptografía

Equipo de investigación



Seminario de Teoría de Números de Barcelona

Dirigido por Pilar Bayer y formado por una treintena de profesores de la UB, la UAB y la UPC

- Seminario temático anual desde 1986-87
- En 1995 organizamos el congreso **Journées Arithmétiques**
- **Arithmetical problems in number fields, abelian varieties and modular forms**
  Contributions to Science, **1** (2) (1999) 125-145

Grupo de investigación UPC

TN - Teoría de Números

15 profesores y becarios de investigación de los departamentos MAII, MAIII y MAIV

- **Grupo de Investigación Consolidado** 2005SGR 00443 1/1/2005-31/12/2008
- BFM2003-06768-C02-01 **Curvas y Variedades abelianas modulares**
- 4 tesis dirigidas y 4 estudiantes de doctorado
- Euroconferencia: **Modular Curves and Abelian Varieties** Progress in Mathematics 224, Birkhäuser-Verlag (2004)
- Desde el curso 2003-04: Seminario internacional de periodicidad quincenal
- **Primeras Jornadas de Teoría de Números** (30-6 al 2-7-2005)

Docencia

Asignaturas optativas de 7.5 créditos

Ingeniería Informática

- **Criptografía** (desde 98-99)

Licenciatura en Matemáticas

- **Criptografía** (desde 97-98)

Tesis dirigida

Subgrupos de Sylow de las curvas elípticas definidas sobre cuerpos finitos
Ramiro Moreno Chiral

- Codirector: J. M. Miret (Universidad de Lleida)
- Programa de doctorado de Matemática Aplicada de la UPC
- Defendida el 29 de junio de 2005

Publicaciones: artículos

- **An octahedral-elliptic type equality in $Br_2(k)$**
  Comptes Rendus Acad. Sci. Paris, (1995)
- **Elliptic modularity for octahedral Galois representations**
  Mathematical Research Letters, (1996)
- **On curves of genus 2 with Jacobian of GL_2-type**
  Manuscripta Mathematica, (1999)
- **Dyadic exercises for octahedral extensions**
  Journal für die reine und angewandte Mathematik, (1999)
- **Octahedral Galois representations arising from $\mathbb{Q}-$curves of degree 2**
  Canadian Journal of Mathematics, (2002)
- **Determining the $2-$Sylow subgroup of an elliptic curve over a finite field**
  Mathematics of Computation, (2005)
- **On twists of the modular curve $X(p)$**
  Bulletin of the London Mathematical Society, (2005)
- **Dyadic exercises for octahedral extensions II**
  Journal of Number Theory (2006)

Artículos sometidos a publicación

- **Computing the $\ell-$power torsion of an elliptic curve over a finite field**
  J.M. Miret, R. Moreno, A. Rio, M. Valls
  Mathematics of Computation
- **Generalization of Vélu's formulae for isogenies between elliptic curves**
  J.M. Miret, R. Moreno, A. Rio
  Publicacions Matemàtiques
  Primeras Jornadas de Teoría de Números (Vilanova, 2005)

- **Algoritmo para rechazar ciertas curvas elípticas no criptográficamente útiles**
  J.M. Miret, R. Moreno, A. Rio.
  VII Reunión Española sobre Criptología y Seguridad de la Información,
  Actas Tomo II (2002), pp. 589–600.
- **Algoritmo para discriminar curvas elípticas con potencias elevadas de 2 ó 3 en su cardinal**
  J.M. Miret, R. Moreno, A. Rio, M. Valls, A. Albajes.
  VIII Reunión Española sobre Criptología y Seguridad de la Información,
  Avances en Criptología y Seguridad de la Información
  Ed. Díaz de Santos (2004), pp. 13–19.

Minisymposium: Métodos Geométricos en Criptografía

RSME 2002. Puerto de la Cruz (Tenerife)

Ponentes

- J. Tena (UVA): Criptosistemas elípticos
- R. Moreno (UdL): Recuento de puntos de curvas elípticas sobre cuerpos finitos
- J. Guàrdia (UPC): Tests de primalidad basados en curvas elípticas
- E. Nart (UAB): Criptosistemas hiperelípticos
- A. Rio (UPC): Uso criptográfico de la restricción de Weil
- A. Quirós (UAM): Uso criptográfico de jacobianas de curvas de Picard

Cursos

CATCert (Agència catalana de certificació)
Curso de 20 horas. (Julio de 2005) Con F. Martínez
Objetivos:

- Conocer los principios básicos de las técnicas criptográficas más importantes: criptografía de clave secreta, criptografía de clave pública, funciones hash y firma digital
- Familiarizarse con los protocolos basados en criptografía de clave pública y firma digital, y su sintaxis

Proyectos financiados

Red Temática española de Investigación en el campo de la Seguridad de las Tecnologías de la Información

CICYT TIC2002-12487-E

13 entidades participantes

Investigador responsable: E. Fernández-Medina

European FP6 Research and Training Network: Galois Theory and Explicit Methods 12 nodos

The total budget of 2.5 MEuro is provided by the European Commission under contract MRTN-CT-2006-035495

- May 20 2007: **Eurocrypt 2007**. Responsible partner: Barcelona

European FP6 Research and Training Network: Galois Theory and Explicit Methods

Training module T4: cryptography and coding theory

- T4.1 Mathematics for digital content (Workshop)
- T4.2 Cryptography or coding theory training at International conference
- T4.3 Overview course on cryptography or coding theory to gain acquaintance with existing techniques in the prospective application areas of the project

European FP6 Research and Training Network: Galois Theory and Explicit Methods

Milestones (Nodo de Essen)

- Report: construction of curves suitable for cryptography with discrete logarithms, index calculus and pairings
- Report: construction of curves with RM and CM curves of genus 2; pairing-friendly curves of genus 2; resistance against side-channel attacks
- Report: use of Quadratic sieve in Brauer group index calculus; application of Brauer group methods to discrete logs Result of task

Prof. G. Frey, Matematisches Institut der Universität zu Essen