11868 - CRIPTO - CRIPTOGRAFIA

Unitat responsable: 200 - FME - Facultat de Matemàtiques i Estadística

Unitat que imparteix: 726 - MA II - Departament de Matemàtica Aplicada II
743 - MA IV - Departament de Matemàtica Aplicada IV

Curs: 2008

Titulació: LLICENCIATURA DE MATEMÀTIQUES (Pla 1992). (Unitat docent Optativa)
MÀSTER EN MATEMÀTICA APLICADA (Pla 2006). (Unitat docent Optativa)
DOCTORAT EN MATEMÀTICA APLICADA, PLA 2005 (Pla 2007). (Unitat docent Optativa)

Crèdits: 7,5 Idiomes docència: Català

Professors

Responsable: RIO DOVAL, ANA

Altres: ROTGER CERDÀ, VICTOR

Objectius generals de l'assignatura

Adquirir una visió general dels conceptes i mètodes de la criptografia clàssica i de la criptografia de clau secreta. Conèixer a fons el funcionament dels sistemes criptogràfics de clau pública d'ús generalitzat, entenent els resultats matemàtics en què es basen la seva eficiència i la seva seguretat. Capacitar tant per a l'exercici professional com per a la incorporació a algunes de les línies de recerca més actives en aquest camp.

* Conèixer el caràcter conjecturalment intractable dels problemes de factorització i logaritme discret. Identificar l'ús que fa la criptografia d'aquestes hipòtesis provinents de la teoria de la complexitat algorísmica.
* Conèixer els algoritmes involucrats en el criptosistema RSA i en els estàndards de signatura digital DSA i ECDSA.
* Conèixer la teoria de corbes el·líptiques rellevant per al disseny de criptosistemes el·líptics.
* Preparar i comunicar oralment i/o per escrit un treball matemàtic realitzat de forma autònoma a partir d'un guió i referències bibliogràfiques.
* Utilitzar eines informàtiques de càlcul simbòlic o numèric per experimentar amb l'aplicació criptogràfica dels resultats matemàtics estudiats.

Capacitats a adquirir:

* Conèixer els principals resultats matemàtics involucrats en els sistemes criptogràfics utilitzats actualment en les TIC.
* Incorporar el punt de vista de la complexitat algorítmica en la valoració d'un resultat matemàtic teòric.
* Implementar tests de primalitat.
* Manipular corbes el·líptiques sobre cossos finits. Conèixer mètodes per calcular el cardinal del grup de punts.
* Preparar un tema fent la recerca bibliogràfica necessària, que pot incloure articles recents en revistes especialitzades.

Continguts

Criptografia de clau secreta

Conceptes bàsics. Criptosistemes clàssics. Teoria de Shannon. L'advanced encryption standard.

11868 - CRIPTO - CRIPTOGRAFIA

Aritmètica computacional

Aspectes computacionals dels grups abelians. Exponenciació, extracció d'arrels i logaritme discret.

Primalitat i factorització

Distribució dels nombres primers. Primalitat. Criteris probabilístics. Certificats de primalitat. Mètodes clàssics de factorització: rho de Pollard, mètode p-1 i variants. Mètodes de factorització subexponencials.

Criptografia de clau pública

La idea de Diffie i Hellman. Funcions unidireccionals. Portes trampa.
El problema de factorització. Criptosistema RSA. El problema del logaritme discret. Signatura digital DSA.
Criptografia amb corbes el·líptiques.
Criptografia amb corbes hiperel·líptiques.

Sistema de qualificació

S'entregarà un treball (30 %) i es realitzarà un examen final (70 %).

Capacitats prèvies

* Les de les assignatures obligatòries de la llicenciatura de Matemàtiques.

11868 - CRIPTO - CRIPTOGRAFIA

Bibliografia

Bàsica:

Cohen, H.. *A course in computational algebraic number theory*. Springer-Verlag, 1993.

Koblitz, N.. *A course in number theory and cryptography*. Springer-Verlag, 1994.

Blake, I.F.; Seroussi, G.; Smart , N.P.. *Elliptic curves in cryptography*. Cambridge University Press, 1999.

Mollin, R. A.. *RSA and public-key cryptography*. Chapman & Hall, 2003.

Yan. S.Y.. *Number theory for computing*. Springer-Verlag, 2000.

Complementària:

Menezes, A.J.; Oorsschot, P.C. van; Vanstone, S.A.. *Handbook of Applied Criptography*. CRC Press, 1997.

Schneier, B.. *Applied cryptography. Protocols, algorithms, and source code in C*. John Wiley & Sons, 1996.

Stinson, D.R.. *Cryptography. Theory and practice*. CRC Press, 2006.

Mollin, R. A.. *Fundamental number theory with applications*. CRC Press, 1998.