

Eines de càlcul simbòlic

Codi	Tipus	Curs/Semestre	Crèdits
24984	Obligatòria Semestral	3er / 1er	4,5

Objectius

Competències específiques

Coneixements

- Conèixer un sistema de càlcul simbòlic: MAPLE.
- Conèixer una metodologia de programació basada en càlculs amb objectes matemàtics.
- Repassar coneixements previs d'aritmètica, combinatòria i teoria de grafs, utilitzant paquets específics de MAPLE.
- Aprendre diferents mètodes criptogràfics bàsics com una aplicació de l'aritmètica, mitjançant el MAPLE.

Habilitats

- Fer servir el MAPLE a nivell general per manipular objectes estructurals.
- Saber utilitzar les comandes de MAPLE per resoldre problemes d'aritmètica, combinatòria, criptografia i grafs.
- Manipular i programar dominis simbòlics de MAPLE.
- Saber programar procediments i funcions en un sistema de càlcul simbòlic.
- Ser capaç d'implementar sistemes criptogràfics aprofitant la potència de MAPLE.
- Saber implementar algorismes bàsics de teoria de grafs utilitzant el paquet *Networks* de MAPLE.

Competències genèriques

- Capacitat d'anàlisi i síntesi.
- Capacitat de resolució de problemes.
- Capacitat d'organització i planificació.
- Treball en equip.
- Aprenentatge autònom.
- Motivació per la qualitat.
- Coneixement d'anglès.

Capacitats prèvies

Encara que no hi ha prerequisits establerts en la titulació, és convenient que l'estudiant repassi (tingui aprovades) les següents assignatures:

- Fonaments de Matemàtica Discreta (1r curs, 2n semestre)
- Grafs i Complexitat (2n curs, 1r semestre)
- Combinatòria i Optimització (2n curs, 2n semestre)

Continguts

1- Introducció al càlcul simbòlic: MAPLE	
Funcionament de MAPLE a nivell general. Introducció al llenguatge de programació de MAPLE. Procediments.	
2. Aritmètica i Combinatòria (Pràctica 1)	
Resolució de problemes d'aritmètica i combinatòria utilitzant alguns paquets específics de MAPLE.	
3. Introducció a la Criptografia (Pràctica 2)	
Resolució de problemes relacionats amb la criptografia utilitzant el MAPLE. Criptosistemes Cesar, matricial-afí i RSA.	
4. Grafs: fonaments i algorismes (Pràctica 3)	
Resolució de problemes relacionats amb la teoria de grafs utilitzant el paquet <i>Networks</i> de MAPLE. Fonaments de grafs i algorismes (Kruskal, Prim, Dijkstra, Floyd).	

Metodologia docent

L'assignatura no inclou classes teòriques, únicament s'impartiran de caràcter presencial classes pràctiques al laboratori (L). Aquestes estaran distribuïdes en sessions setmanals de 2,5 hores, durant 12 setmanes al llarg del semestre. L'estudiant haurà d'assistir obligatòriament a aquestes sessions i podrà realitzar en elles la major part dels apartats obligatoris de les pràctiques.

Altres activitats de caràcter no presencial seran la preparació i finalització de les pràctiques incloent els apartats opcionals (PP), així com l'À estudi i repàs dels conceptes teòrics necessaris per a la realització de les pràctiques (E).

S'hauran de realitzar i lliurar 3 pràctiques al llarg del curs. Per a realitzar-les es faran grups de dues persones. El/La professor/a supervisarà la feina feta al laboratori durant cadascuna de les sessions. Si no es comunica el contrari, els lliuraments de cada sessió es realitzaran a l'inici de la sessió següent. No s'acceptaran pràctiques fora de termini.

Avaluació

1a convocatòria (febrer/juny)		2a convocatòria (juliol/setembre)
Avaluació en grups	Avaluació individual	
60% de la nota final que es correspon a les notes de les tres pràctiques.	40% de la nota final corresponent a l'examen final.	No n'hi ha.

Bibliografia bàsica

- A. Heck. *Introduction to Maple*. Second Edition. Springer-Verlag, 1996.
- D. Redfern. *The Maple Handbook*. Springer-Verlag, 1996.
- J.M. Basart. *Programació lineal*. Col·lecció Materials n. 58. Servei de Publicacions de la UAB, 1998.
- J.M. Basart. *Grafs: Fonaments i algorismes*. Servei de Publicacions de la UAB, 1994.
- J.M. Basart, J. Rifà, M. Villanueva. *Fonaments de Matemàtica Discreta*. Col·lecció Materials n. 36. Servei de Publicacions de la UAB, 1997.
- J. Rifà, Ll. Huguet *Comunicación Digital*. Masson, 1991.

Bibliografia complementària

- T.H. Cormen, et al. *Introduction to Algorithms*. The MIT Press, 1990, 1992.
- K.Q. Geddes, et al. *Algorithms for Computer Algebra*. Kluwer Academic Publishers, 1992.
- M.B. Monagan, K.O. Geddes, G. Labahn, S. Vorkoetter. *Maple V. Programming Guide*. Springer-Verlag, 1996.
- D.G. Stinson. *Cryptography. Theory and Practice*. CRC Press, 1995.

Enllaços

[Tutorials, exemples,...](http://www.maplesoft.com/academic/students) <http://www.maplesoft.com/academic/students>

[Pàgina web de l'assignatura on es troben els enunciats de les pràctiques, així com informació complementària sobre cada pràctica.](http://www.deic.uab.es/) <http://www.deic.uab.es/>

[Tutorial de MAPLE.](http://www.math.fsu.edu/~quine/IntroMathBio_04/Maple_essent_tut/CourseStart.html) http://www.math.fsu.edu/~quine/IntroMathBio_04/Maple_essent_tut/CourseStart.html

[Recursos de MAPLE de domini públic.](http://www.maplesoft.com/applications) <http://www.maplesoft.com/applications>