

Fișa disciplinei

1. Date despre program

1.1 Instituția de învățământ superior	UNIVERSITATEA BABES-BOLYAI
1.2 Facultatea	MATEMATICA SI INFORMATICA
1.3 Departamentul	MATEMATICA
1.4 Domeniul de studii	INFORMATICA
1.5 Ciclul de studii	LICENTA
1.6 Programul de studiu / Calificarea	INFORMATICA

2. Date despre disciplină

2.1 Denumirea disciplinei	ALGEBRA COMPUTATIONALA
---------------------------	------------------------

2.2 Titularul activităților de curs	Lect. Dr. George Ciprian Modoi
2.3 Titularul activităților de seminar	Lect. Dr. George Ciprian Modoi

2.4 Anul de studiu	2	2.5 Semestrul	2	2.6. Tipul de Coloviu evaluare	2.7 Regimul disciplinei	optional
--------------------	---	---------------	---	-----------------------------------	----------------------------	----------

3. Timpul total estimat (ore pe semestru al activităților didactice)

3.1 Număr de ore pe săptămână	4	Din care: 3.2 curs	2	3.3 seminar/laborator	2
3.4 Total ore din planul de învățământ	42	Din care: 3.5 curs	28	3.6 seminar/laborator	14
Distribuția fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie și notițe					20
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					20
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					20
Tutoriat					-
Examinări					6
Alte activități: evaluari lucrari de control					17

3.7 Total ore studiu individual	83
3.8 Total ore pe semestru	125
3.9 Numărul de credite	5

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	Nu e cazul
-------------------	------------

4.2 de competențe	Nu e cazul
-------------------	------------

5. Condiții (acolo unde este cazul)

5.1 De desfășurare a cursului	<ul style="list-style-type: none"> Nu e cazul
5.2 De desfășurare a seminarului/laboratorului	<ul style="list-style-type: none"> Nu e cazul

6. Competențele specifice acumulate

Competențe profesionale	<ul style="list-style-type: none"> Determinarea gradului de complexitate al unui algoritm. Dobândirea unor cunoștințe referitoare la noțiuni de aritmetică modulară (invers modular, rădăcina pătrată modulară, logaritm discret) precum și a unor cunoștințe de algebra abstractă care să permită înțelegerea adecvată a noțiunilor respective. Implementare unor algoritmi eficienți din punct de vedere computațional pentru rezolvarea unor probleme utile în sistemele criptografice moderne (determinarea inversului modular, exponențierea modulară etc.); Realizarea de conexiuni între algebra și algoritmi.
Competențe transversale	<ul style="list-style-type: none"> Manevrarea obiectelor matematice în diverse situații practice în vederea elaborării unor algoritmi eficienți; Dobândirea de abilități practice legate de studiul individual; Abilități de a aplica rezultate matematice specifice unui domeniu în alte domenii teoretice sau practice.

7. Obiectivele disciplinei (reieșind din grila competențelor acumulate)

7.1 Obiectivul general al disciplinei	<ul style="list-style-type: none"> Prezentarea unor metode specifice algebrei computaționale și exemplificarea lor prin aplicații în dezvoltarea unor algoritmi folosiți în criptografie.
7.2 Obiectivele specifice	<ul style="list-style-type: none"> Compararea algoritmilor din punct de vedere al complexității lor. Prezentarea unor noțiuni de aritmetică modulară (invers modular, rădăcina pătrată modulară, logaritm discret). Prezentarea unor exemple de demonstrație algebrică a corectitudinii unui algoritm. Abordarea problemelor legate de numere prime și factorizarea întregilor în produs de numere prime din punct de vedere computațional. Prezentarea unor protocoale folosite în criptografie (RSA, Rabin, Diffie-Hellman, ElGamal) și evidențierea problemelor computaționale pe care acestea le reclama.

8. Conținuturi

8.1 Curs	Metode de predare	Observații
1. Sisteme clasice de criptare.	Prelegeri; Conversatii; Demonstratia; Problematizarea	
2. Complexitatea algoritmilor. Notatia O.	Prelegeri; Conversatii; Demonstratia; Problematizarea	
3. Criptografia cu cheie publica. Functii <i>one-way</i> si <i>trap-door</i> . Protocolul RSA.	Prelegeri; Conversatii; Demonstratia; Problematizarea	
4. Probleme computationale puse de RSA. Clase de resturi si aritmetica modulara. Algoritmul lui Euclid extins.	Prelegeri; Conversatii; Demonstratia; Problematizarea	
5. Exponentierea modulara prin ridicare repetata la patrat. Corectitudinea si securitatea algoritmului RSA.	Prelegeri; Conversatii; Demonstratia; Problematizarea	
6. Numere prime si grupuri ciclice. Resturi patratice si simbolurile Legendre si Jacobi.	Prelegeri; Conversatii; Demonstratia; Problematizarea	
7. Teste de primalitate.	Prelegeri; Conversatii; Demonstratia; Problematizarea	
8. Metode de factorizare a intregilor.	Prelegeri; Conversatii; Demonstratia; Problematizarea	
9. Sistemul criptografic Rabin si radacina patrata modulara.	Prelegeri; Conversatii; Demonstratia; Problematizarea	
10. Schimbul de chei Diffie-Hellman si problema logaritmului discret.	Prelegeri; Conversatii; Demonstratia; Problematizarea	
11. Sistemul criptografic ElGamal. Corpuri finite.	Prelegeri; Conversatii; Demonstratia; Problematizarea	
12. Factorizarea polinoamelor cu coeficienti intr-un corp finit.	Prelegeri; Conversatii; Demonstratia; Problematizarea	
13. Metode de rezolvarea a problemei logaritmului discret.	Prelegeri; Conversatii; Demonstratia; Problematizarea	
14. Semnatura digitala bazata pe un sistem criptografic cu cheie publica.	Prelegeri; Conversatii; Demonstratia; Problematizarea	

Bibliografie

1. S. Crivei, A. Mărcuș, C. Săcărea, C. Szanto, Computational Algebra with applications to cryptography and coding theory, Efes 2006.
2. W. Bosma, A. van der Porten, Computational Algebra and Number Theory, Kluwer 1995.
3. D. Bressoud, S. Wagon, A Course in Computational Number Theory, Springer-Verlag 2000.
4. H. Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag, 2000.
5. H. Cohen, A.M. Cuypers, H. Sterk, Some Tapas of Computer Algebra, Springer-Verlag, 1999.
6. R. Crandall, C. Pomerance, Prime Numbers. A Computational Perspective, Springer-Verlag, 2001.
7. K. Ireland, M. Rosen, A Classical Introduction to Number Theory, Springer-Verlag, 1990.
8. N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 1994.
9. R. Lidl, G. Pilz, Applied Abstract Algebra, Springer-Verlag, 1998.
10. H. S. Wilf, Algorithmes et complexite, Masson, Paris, 1989.

9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului

- Studentii vor dobândi cunoștințe teoretice de algebra computațională ceea ce le va permite să aprecieze gradul de complexitate al unui algoritm, iar în activitatea de programare se îndreaptă spre soluțiile adecvate din acest punct de vedere.
- Studentii se vor familiariza cu noțiunile și problemele care apar în criptografie și vor învăța principiile pe care sunt construite sistemele criptografice moderne.
- Studenții vor fi capabili să implementeze algoritmi folosiți de un sistem criptografic.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Însușirea noțiunilor teoretice, a rezultatelor (cu demonstrații),	Colocviu final (oral)	30%
10.5 Seminar/laborator	Implementarea algoritmilor învățați.	Evaluare în timpul fiecărui laborator.	35%
	Implementarea unei probleme complexe care implică adoptarea unor soluții computaționale adecvate.	Prezentarea unui proiect final.	35%
10.6 Standard minim de performanță			
<ul style="list-style-type: none">• Dintre cele 5 teme de laborator pe care le vor primi studenții sunt obligați să predea minimum 4.• Este obligatorie obținerea unei note de trecere la prezentarea proiectului, precum și la discuția axată pe probleme teoretice de la colocviul final.			

Data completării

30.04.2013

Semnătura titularului de curs

Lect. Dr. George Ciprian Mădoi

Semnătura titularului de seminar

Lect. Dr. George Ciprian Mădoi

Data avizării în departament

.....

Semnătura directorului de departament

.....