FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Babes-Bolyai
1.2 Facultatea	Facultatea de Matematica si Informatica
1.3 Departamentul	Departamentul de matematica
1.4 Domeniul de studii	Matematica
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 activităţilor de curs	Lect. dr. George Ciprian Modoi						
2.3 Titularul activităţilor de seminar	Lect. dr. George Ciprian Modoi						
2.4 Anul de studiu	2	2.5 Semestrul	2	2.6. Tipul de evaluare	Colocviu	2.7 Regimul disciplinei	optional

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

3.1 Număr de ore pe săptămână	3	Din care: 3.2 curs	2	3.3 seminar/laborator	1
3.4 Total ore din planul de învăţământ	42	Din care: 3.5 curs	28	3.6 seminar/laborator	14
Distribuţia fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie şi notiţe					20
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					20
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					20
Tutoriat					-
Examinări					6
Alte activităţi: evaluari					17
3.7 Total ore studiu individual	83				
3.8 Total ore pe semestru	125				
3.9 Numărul de credite	5				

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	• Nu este cazul
4.2 de competenţe	• Nu este cazul

5. Condiţii (acolo unde este cazul)

5.1 De desfăşurare a cursului	• Nu este cazul
5.2 De desfăşurare a seminarului/laboratorului	• Nu este cazul

6. Competenţele specifice acumulate

Competenţe profesionale	• Determinarea gradului de complexitate al unui algoritm. • Dobandirea unor cunostiintelor referitoare la notiuni de aritmetica modulara (invers modular, radacina patrata modulara, logaritm discret) precum si a unor cunostiinte de algebra abstracta care sa permita intelegerea adecvata a notiunilor respective. • Implementare unor algoritmi eficienti din punct de vedere computational pentru rezolvarea unor probleme utile in sistemele criptografice moderne (determinarea inversului modular, exponentierea modulara etc.). • Realizarea de conexiuni intre algebra si algoritmi.
Competenţe transversale	• Manevrarea obiectelor matematice în diverse situaţii practice in vederea elaborarii unor algoritmi eficienti. • Dobândirea de abilităţi practice legate de studiul individual. • Abilităţi de a aplica rezultate matematice specifice unui domeniu în alte domenii teoretice sau practice.

7. Obiectivele disciplinei (reieşind din grila competenţelor acumulate)

7.1 Obiectivul general al disciplinei	• Prezentarea unor metode specifice algebrei computationale si exemplificarea lor prin aplicatii in dezvoltarea unor algoritmi folositi in criptografie.
7.2 Obiectivele specifice	• Compararea algoritmilor din punct de vedere al complexitatii lor. • Prezentarea unuor notiuni de aritmetica modulara (invers modular, radacina patrata modulara, logaritm discret). • Prezentarea unor exemple de demonstratie algebrica a corectitudinii unui algoritm. • Abordarea problemelor legate de numere prime si factorizarea intregilor in produs de numere prime din punct de vedere computational. • Prezentarea unor protocoale folosite in criptografie (RSA, Rabin, Diffie-Hellman, ElGamal) si evidentierea problemelor computationale pe care acestea le reclama.

8. Conţinuturi

8.1 Curs	Metode de predare	Observaţii
1. Sisteme clasice de criptare.	Prelegrea, conversatia, demonstratia, problematizarea.	
2. Complexitatea algoritmilor. Notatia O.	Prelegrea, conversatia, demonstratia, problematizarea.	
3.Criptografia cu cheie publica. Functii one-way si trap-door. Protocolul RSA.	Prelegrea, conversatia, demonstratia, problematizarea.	
4. Probleme computationale puse de RSA. Clase de resturi si aritmetica modulara. Algoritmul lui Euclid extins.	Prelegrea, conversatia, demonstratia, problematizarea.	
5. Exponentierea modulara prin ridicare repetata la	Prelegrea, conversatia,	

patrat. Corectitudinea si securitatea algoritmului RSA.	demonstratia, problematizarea.	
6. Numere prime si grupuri ciclice. Resturi patratice si simbolurile Legendre si Jacobi.	Prelegrea, conversatia, demonstratia, problematizarea.	
7. Teste de primalitate.	Prelegrea, conversatia, demonstratia, problematizarea.	
8. Metode de factorizare a intregilor.	Prelegrea, conversatia, demonstratia, problematizarea.	
9. Sistemul criptografic Rabin si radacina patrata modulara.	Prelegrea, conversatia, demonstratia, problematizarea.	
10.Schimbul de chei Diffie-Hellman si problema logaritmului discret.	Prelegrea, conversatia, demonstratia, problematizarea.	
11. Sistemul criptografic ElGamal. Corpuri finite.	Prelegrea, conversatia, demonstratia, problematizarea.	
12. Factorizarea polinoamelor cu coeficienti intr-un corp finit.	Prelegrea, conversatia, demonstratia, problematizarea.	
13. Metode de rezolvarea a problemei logaritmului discret.	Prelegrea, conversatia, demonstratia, problematizarea.	
14. Semnatura digitala bazata pe un sistem criptografic cu cheie publica.	Prelegrea, conversatia, demonstratia, problematizarea.	

Bibliografie

1. S. Crivei, A. Mărcuş, 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.

8.2 Seminar / laborator	Metode de predare	Observaţii
1. Sisteme clasice de criptare.	Conversatia, problematizarea.	
2. Algoritmul lui Euclid extins si probleme conexe.	Conversatia, problematizarea.	
3. Sistemul RSA.	Conversatia, problematizarea.	
5. Metode de factorizare a intregilor.	Conversatia, problematizarea.	
6. Semnatura digitala	Conversatia, problematizarea.	
7. Evaluare	Evaluare.	

Bibliografie (aceeasi ca si la curs)

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatori reprezentativi din domeniul aferent programului

- Studentii vor dobandi cunostinte teoretice de algebra computationala ceea ce le va permite sa aprecieze gradul de complexitate al unui algoritm, iar in activitatea de programare se indrepte spre solutiile adecvate din acest punct de vedere.
- Studentii se vor familiariza cu notiunile si problemele care apar in criptografie si vor invata principiile pe care sunt construite sistemele criptografice moderne.
- Studenţii vor fi capabili sa implementeze algoritmii folositi 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	Insusirea notiunilor teoretice, a rezultatelor (cu demonstratii),.	Colocviu (oral)	1/3
10.5 Seminar/laborator	Implementarea algoritmilor invatati.	Evaluare in timpul fiecarui laborator.	1/3
	Implementarea unei probleme complexe care implica adoptarea unor solutii computationale adecvate.	Prezentarea unui proiect final.	1/3
10.6 Standard minim de performanţă			
• Dintre cele 5 teme de laborator pe care le vor primi studentii sunt obligati sa predea minimum 4. • Este obligatorie obtinerea notei 5 la prezentarea proiectului, precum si la discutia axata pe probleme teoretice de la colocviul final.			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
30.04.2014	Lect. dr. George Ciprian Modoi	Lect. dr. George Ciprian Modoi

Data avizării în departament	Semnătura directorului de departament
.....	Prof. dr. Octavian Agratini