FIŞA 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 ROMANA

2. Date despre disciplină

2.1 Denumirea disciplinei	ALGEBRA COMPUTATIONALA						
2.2 Titularul activităților de curs	Conf. Dr. George Ciprian Modoi						
2.3 Titularul activităților de seminar	Conf. Dr. George Ciprian Modoi						
2.4 Anul de studiu	3	2.5 Semestrul	5	2.6. Tipul de evaluare	Coloviu	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 şi notițe					20
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					15
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					15
Tutoriat					-
Examinări					6
Alte activități: evaluari lucrari de control					2
3.7 Total ore studiu individual	58				
3.8 Total ore pe semestru	100				
3.9 Numărul de credite	4				

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 desfăşurare a cursului	• Nu e cazul
5.2 De desfăşurare a seminarului/laboratorului	• Nu e cazul

6. Competențele specifice acumulate

Competențe profesionale	Utilizarea bazelor teoretice ale informaticii si a modelelor formale • Interpretarea de modele matematice şi informatice (formale) • Identificarea modelelor si metodelor adecvate pentru rezolvarea unor probleme reale • Utilizarea simulării pentru studiul comportamentului modelelor realizate si evaluarea performantelor • Încorporarea de modele formale în aplicații specifice din diverse domenii
Competențe transversale	• **CT1** Aplicarea regulilor de muncă organizată şi eficientă, a unor atitudini responsabile față de domeniul didactic-ştiințific, pentru valorificarea creativă a propriului potențial, cu respectarea principiilor şi a normelor de etică profesională • Utilizarea unor metode şi tehnici eficiente de învățare, informare, cercetare şi dezvoltare a capacităților de valorificare a cunoştințelor, de adaptare la cerințele unei societăți dinamice şi de comunicare în limba română şi într-o limbă de circulație internațională

7. Obiectivele disciplinei (reieşind din grila competențelor 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. 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 *one-way* si *trap-door*. 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	Prelegeri; Conversatii; Demonstratia;	

patrat. Corectitudinea si securitatea algoritmului RSA.	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. 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.

8.2 Laborator	Metode de predare	Observații
1. Sisteme clasice de criptare.	Conversatii; Problematizarea	
2. Protocolul RSA.	Conversatii; Problematizarea	
3. Algoritmul lui Euclid si cel de ridicare la o putere	Conversatii; Problematizarea	
4. Teste de primalitate	Conversatii; Problematizarea	
5. Schimbul de chei Diffie Hellman.	Conversatii; Problematizarea	

6. Protocolul ElGamal. .	Conversatii; Problematizarea	
7. Semnatura digitala..	Conversatii; Problematizarea	

9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și 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.
- Studenții 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 final (oral)	20%
10.5 Seminar/laborator	Implementarea algoritmilor invatati.	Evaluare in timpul fiecarui laborator.	40%
	Implementarea unei probleme complexe care implica adoptarea unor solutii computationale adecvate.	Prezentarea unui proiect final.	40%
10.6 Standard minim de performanță			
• Dintre cele 5 teme de laborator pe care le vor primi studentii sunt obligati sa predea minimum 4. • Este obligatorie obtinerea unei note de trecere 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
29.04.2018	Conf. Dr. George Ciprian Modoi	Conf. Dr. George Ciprian Modoi

Data avizării în departament ..... Semnătura directorului de departament ….....