

## 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	INTELIGENTA ARTIFICIALA

### 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	Coloțiu	2.7 Regimul disciplinei	Optional

### 3. Timpul total estimat (ore pe semestru al activităților 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 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					15
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					15
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					15
Tutoriat					-
Examinări					5
Alte activități: evaluari lucrari de control					8
3.7 Total ore studiu individual	58				
3.8 Total ore pe semestru	100				
3.9 Numărul de credite	4				

### 4. Preconții (acolo unde este cazul)

4.1 de curriculum	Nu e cazul
4.2 de competențe	Nu e cazul

### 5. Conții (acolo unde este cazul)

5.1 De desfășurare a cursului	Nu e cazul
5.2 De desfășurare a seminarului/laboratorului	Nu e cazul

### 6. Competențele specifice acumulate

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

### 7. Obiectivele disciplinei (reieșind din grila competențelor acumulate)

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

### 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. Algoritmii lui Euclid extinsi.	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 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 algoritmi 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)	30%
10.5 Seminar/laborator	Implementarea algoritmilor invatati.	Evaluare in timpul fiecarui laborator.	35%
	Implementarea unei probleme complexe care implica adoptarea unor solutii computationale adecvate.	Prezentarea unui proiect final.	35%
10.6 Standard minim de performanță			
<ul style="list-style-type: none"> <li>• Dintre cele 5 teme de laborator pe care le vor primi studentii sunt obligati sa predea minimum 4.</li> <li>• Este obligatorie obtinerea unei note de trecere la prezentarea proiectului, precum si la discutia axata pe probleme teoretice de la colocviul final.</li> </ul>			

Data completării

28.04.2023

Data avizării în departament

.....

Semnătura titularului de curs

Conf. Dr. George Ciprian Modoi

Semnătura directorului de departament

Semnătura titularului de laborator

Conf. Dr. George Ciprian Modoi

Prof. Dr. Andrei Marcus