

## FIȘA DISCIPLINEI

### Aritmetica modulara si criptografie

Anul universitar 2026-2027

#### 1. Date despre program

1.1. Instituția de învățământ superior	Universitatea Babeș-Bolyai
1.2. Facultatea	Matematică și Informatică
1.3. Departamentul	Matematică
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Master
1.6. Programul de studii / Calificarea	Baze de date
1.7. Forma de învățământ	Cu frecvență

#### 2. Date despre disciplină

2.1. Denumirea disciplinei	<b>Aritmetica modulara si criptografie</b>			Codul disciplinei	<b>MME3051</b>
2.2. Titularul activităților de curs	Prof. dr. Septimiu Crivei				
2.3. Titularul activităților de seminar	Prof. dr. Septimiu Crivei				
2.4. Anul de studiu	1	2.5. Semestrul	1	2.6. Tipul de evaluare	Examen
2.7. Regimul disciplinei	Opțional	2.8. Tipul disciplinei		Disciplină de specializare (DS)	

#### 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/ proiect	1
3.4. Total ore din planul de învățământ	42	din care: 3.5. curs	28	3.6 seminar/laborator	14
<b>Distribuția fondului de timp pentru studiul individual (SI) și activități de autoinstruire (AI)</b>					<b>ore</b>
Studiul după manual, suport de curs, bibliografie și notițe (AI)					28
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					28
Pregătire seminare/ laboratoare/ proiecte, teme, referate, portofolii și eseuri					28
Tutoriat (consiliere profesională)					10
Examinări					14
Alte activități					0
<b>3.7. Total ore studiu individual (SI) și activități de autoinstruire (AI)</b>				<b>108</b>	
<b>3.8. Total ore pe semestru</b>				<b>150</b>	
<b>3.9. Numărul de credite</b>				<b>6</b>	

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

4.1. de curriculum	
4.2. de competențe	

#### 5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	
5.2. de desfășurare a seminarului/ laboratorului	

### 6.1. Competențele dobândite în urma absolvirii programului de studii (se preiau din planul de învățământ)<sup>1</sup>

Competențe profesionale	
Codul competenței	Competență
CP1	Cunoașterea aprofundată a dezvoltărilor teoretice, metodologice și practice specifice informaticii.
CP3	Elaborarea și conducerea de proiecte software complexe, de natură practică sau de cercetare, utilizând un spectru larg de metode cantitative și calitative
Competențe transversale	
Codul competenței	Competență
CT1	Utilizarea sistematică a cunoștințelor de specialitate în informatică la modelarea și interpretarea unor situații noi, în contexte de aplicare mai largi decât cele cunoscute
CT4	Capacitate de lucru în echipă, asumarea de roluri de execuție și de conducere, realizarea sarcinilor profesionale în condiții de autonomie și responsabilitate

### 6.2. Rezultatele învățării specifice programului de studii (se preiau din planul de învățământ)<sup>2</sup>

Rezultatele învățării vizate prin disciplină		
Codul competenței	Cunoștințe și înțelegere (Knowledge and understanding)	Abilități academice specifice (Specific academic skills)
CF1	Absolventul/a posedă cunoștințe fundamentale de modelare prin care analizează probleme din viața reală, le transpune în cerințe concrete și elaborează un model software corespunzător	Absolventul/a demonstrează abilități avansate de programare care vor permite acumularea de cunoștințe solide și înțelegerea rapidă a tehnologiilor moderne din domeniu

### 7. Rezultatele învățării specifice disciplinei

Cunoștințe și înțelegere (Knowledge and understanding)
1. Studentul a dobândit competențele specifice disciplinelor legate de matematică și algoritmică necesare pentru realizarea temelor.
2. Studentul cunoaște noțiuni fundamentale legate de criptografie, precum și metode de aplicare a acestora în domenii ale științei legate de matematică și informatică.
Abilități academice specifice (Specific academic skills)
1. Studentul are abilitatea de a dezvolta gândirea matematică și algoritmică, progresând de la o înțelegere procedurală/computațională a matematicii la o înțelegere largă care să cuprindă raționamentul logic, generalizarea, abstractizarea și demonstrația formală.

### 8. Conținuturi

8.1 Curs	Metode de predare - învățare	Observații <sup>3</sup>
1. Complexitatea algoritmilor, aritmetica modulara	expunere, algoritmicizare	
2. Primalitate și factorizare	expunere, algoritmicizare	
3. Corpuri finite și logaritmi discreți	expunere, algoritmicizare	

<sup>1</sup> Se vor prelua din Planul de învățământ al programului de studii acele competențe profesionale și/sau transversale la dezvoltarea cărora contribuie disciplina pentru care se elaborează fișa disciplinei. Pentru fiecare competență se va prelua întregul enunț, inclusiv codul competenței, cu formularea care apare în planul de învățământ, fără modificări. Dacă nu se preia nici o competență din oricare din cele două categorii, se șterge linia din tabel aferentă acelei categorii.

<sup>2</sup> Se menționează rezultatele învățării specifice programului de studiu la dezvoltarea cărora contribuie disciplina pentru care se elaborează fișa. Enunțurile, preluate fără modificări din Planul de învățământ în funcție de tipul disciplinei (DF/DS/DC) se trec în dreptul competenței asociate.

<sup>3</sup> De exemplu aspecte organizatorice, recomandări pentru studenți, aspecte specifice legate de curs/seminar cum ar fi invitarea unor practicieni în domeniu etc.

4. Criptografie clasica	expunere, algoritmizare	
5. DES, AES	expunere, algoritmizare	
6. Cifruri fluide	expunere, algoritmizare	
7. Cifruri pe blocuri	expunere, algoritmizare	
8. Criptosistemul RSA	expunere, algoritmizare	
9. Criptosistemul ElGamal	expunere, algoritmizare	
10. Funcții hash	expunere, algoritmizare	
11. Semnături digitale	expunere, algoritmizare	
12. Protocoale legate de chei	expunere, algoritmizare	
13. Criptografie pe curbe eliptice	expunere, algoritmizare	
14. Criptografie cuantica	expunere, algoritmizare	

#### Bibliografie

1. M. Cozzens, S.J. Miller, The Mathematics of Encryption: An Elementary Introduction, American Mathematical Society, 2013.
2. S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to coding theory and cryptography, Editura EFES, Cluj-Napoca, 2006.
3. C. Gherghe, D. Popescu, Criptografie. Coduri. Algoritmi, Editura Univ. Bucuresti, 2005.
4. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1997. [<http://www.cacr.math.uwaterloo.ca/hac>]
5. C. Paar, J. Pelzl, Understanding Cryptography, Springer, 2009.

8.2 Seminar / laborator	Metode de predare - învățare	Observații
1. Complexitatea algoritmilor, aritmetica modulara	interactive exposure, algorithmization	Seminarul are 2 ore la 2 saptamani.
2. Primalitate si factorizare	interactive exposure, algorithmization	
3. Corpuri finite și logaritmi discreti	interactive exposure, algorithmization	
4. Criptografie clasica	interactive exposure, algorithmization	
5. Cifruri pe blocuri	interactive exposure, algorithmization	
6. Criptografie cu cheie publica	interactive exposure, algorithmization	
7. Semnături digitale	interactive exposure, algorithmization	






#### Bibliografie

1. M. Cozzens, S.J. Miller, The Mathematics of Encryption: An Elementary Introduction, American Mathematical Society, 2013.
2. S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to coding theory and cryptography, Editura EFES, Cluj-Napoca, 2006.
3. C. Gherghe, D. Popescu, Criptografie. Coduri. Algoritmi, Editura Univ. Bucuresti, 2005.
4. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1997. [<http://www.cacr.math.uwaterloo.ca/hac>]
5. C. Paar, J. Pelzl, Understanding Cryptography, Springer, 2009.

## 9. Evaluare

Tip activitate	9.1 Criterii de evaluare <sup>4</sup>	9.2 Metode de evaluare <sup>5</sup>	9.3 Pondere din nota finală
9.4 Curs	Folosirea unor concepte si metode de baza in exemple	Teme	1/3 din nota
9.5 Seminar/laborator	Rezolvare de probleme, prezentare de proiecte	Test, examinare practica	2/3 din nota
9.6 Standard minim de promovare			
Nota finala cel putin 5.			

### 10. Etichete ODD (Obiective de Dezvoltare Durabilă / Sustainable Development Goals)<sup>6</sup>

	<input type="radio"/>	Eticheta generală pentru Dezvoltare durabilă						
								
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X
								Nu se aplică nici o etichetă
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Data completării:  
15.04.2026

Semnătura titularului de curs  
.Prof. dr. Septimiu Crivei

Semnătura titularului de seminar  
Prof. dr. Septimiu Crivei

<sup>4</sup> Criteriile de evaluare trebuie să reflecte direct rezultatele învățării vizate la nivel de program de studii, respectiv la nivel de disciplină. Mai concret, se evaluează achizițiile de învățare menționate în rezultatele anticipate ale învățării.

<sup>5</sup> Se recomandă stabilirea atât a metodelor de evaluare finală, cât și a strategiei de evaluare pe parcurs.

<sup>6</sup> Selectați o singură etichetă, cea care, în conformitate cu [Procedura de aplicare a etichetelor ODD în procesul academic](#), se potrivește cel mai bine disciplinei. Dacă disciplina tratează tema dezvoltării durabile la modul general (de ex. prin prezentarea/introducerea cadrului general al dezvoltării durabile etc.) atunci se poate alocă eticheta generală de Dezvoltare Durabilă. Dacă niciuna dintre etichete nu descrie disciplina, selectați ultima opțiune: „Nu se aplică nici o etichetă”.

Data avizării în departament:  
23.04.2026

Semnătura directorului de departament  
Prof. dr. Andrei Mărcuș