

FIȘA DISCIPLINEI

Criptografie cu cheie publica

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	Licență
1.6. Programul de studii / Calificarea	Informatică
1.7. Forma de învățământ	Cu frecvență

2. Date despre disciplină

2.1. Denumirea disciplinei	Criptografie cu cheie publica	Codul disciplinei	MLE0049		
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	3	2.5. Semestrul	5	2.6. Tipul de evaluare	Colocviu
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
Distribuția fondului de timp pentru studiul individual (SI) și activități de autoinstruire (AI)					ore
Studiul după manual, suport de curs, bibliografie și notițe (AI)					14
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					8
Pregătire seminare/ laboratoare/ proiecte, teme, referate, portofolii și eseuri					14
Tutoriat (consiliere profesională)					14
Examinări					8
Alte activități					0
3.7. Total ore studiu individual (SI) și activități de autoinstruire (AI)				58	
3.8. Total ore pe semestru				100	
3.9. Numărul de credite				4	

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)¹

¹ 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

Competențe profesionale	
Codul competenței	Competență
CP1	crează softuri
CP3	analizează specificații software
CP10	utilizează biblioteci de software
Competențe transversale	
Codul competenței	Competență
CT2	Soluționează probleme
CT3	Gândește analitic

6.2. Rezultatele învățării specifice programului de studii (se preiau din planul de învățământ)²

Rezultatele învățării vizate prin disciplină		
Codul competenței	Cunoștințe și înțelegere (Knowledge and understanding)	Abilități academice specifice (Specific academic skills)
CP5	Studentul/absolventul alege, explică și specifică fundamentele matematice aplicate în informatică, inclusiv logica formală, algebra, probabilitățile și statisticile.	Studentul/absolventul aplică, evaluează, propune metodele matematice pentru modelarea, simularea și rezolvarea problemelor informatice.

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 ³
1. Criptografie clasică, exemple	Expunere interactivă, explicație, demonstrație didactică	
2. Complexitatea algoritmilor, elemente de teoria numerelor	Expunere interactivă, explicație, demonstrație didactică	
3. Criptografie cu cheie publică. RSA	Expunere interactivă, explicație, demonstrație didactică	
4. Algoritmi pentru testarea primalității	Expunere interactivă, explicație, demonstrație didactică	

învățământ, fără modificări. Dacă nu se preia nici o competență din oricare din cele două categorii, se șterge linia din tabel aferentă acelei categorii.

² 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.

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

5. Algoritmi de factorizare a intregilor	Expunere interactiva, explicatie, demonstratie didactica	
6. Resturi patratice. Criptosistemul cu cheie publica Rabin	Expunere interactiva, explicatie, demonstratie didactica	
7. Polinoame. Corpuri finite	Expunere interactiva, explicatie, demonstratie didactica	
8. Criptosistemul cu cheie publica ElGamal	Expunere interactiva, explicatie, demonstratie didactica	
9. Algoritmi de calcul al logaritmilor discreti	Expunere interactiva, explicatie, demonstratie didactica	
10. Factorizarea polinoamelor: algoritmul lui Berlekamp	Expunere interactiva, explicatie, demonstratie didactica	
11. Semnături digitale	Expunere interactiva, explicatie, demonstratie didactica	
12. Protocoale legate de chei	Expunere interactiva, explicatie, demonstratie didactica	
13. Aspecte practice ale criptosistemelor cu cheie publica	Expunere interactiva, explicatie, demonstratie didactica	
14. Criptografie pe curbe eliptice	Expunere interactiva, explicatie, demonstratie didactica	

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. Classical cryptography	interactive exposure, algorithmization	The lab is scheduled as 2 hours every second week
2. Algorithm complexity	interactive exposure, algorithmization	
3. Modular arithmetics	interactive exposure, algorithmization	
4. Algorithms for testing primality	interactive exposure, algorithmization	
5. Algorithms for factoring integers	interactive exposure, algorithmization	
6. Public-key cryptography	interactive exposure, algorithmization	
7. Practical aspects of public-key cryptosystems	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 ⁴	9.2 Metode de evaluare ⁵	9.3 Pondere din nota finală
9.4 Curs	Folosirea unor concepte si metode de baza in exemple	Teme	1/2 din nota
9.5 Seminar/laborator	Implementarea de concepte si algoritmi	Examinare practica	1/2 din nota
9.6 Standard minim de promovare			
Nota finala cel putin 5.			

10. Etichete ODD (Obiective de Dezvoltare Durabilă / Sustainable Development Goals)⁶

	<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

⁴ 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.

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

⁶ 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