

FIȘA DISCIPLINEI

Criptografie cu cheie publica

Anul universitar 2025-2026

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	C	2.7. Regimul disciplinei	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 specifice acumulate¹

¹ Se poate opta pentru competențe sau pentru rezultatele învățării, respectiv pentru ambele. În cazul în care se alege o singură variantă, se va șterge tabelul aferent celeilalte opțiuni, iar opțiunea păstrată va fi numerotată cu 6.

Competențe profesionale/ esențiale	C1.5 Dezvoltarea de unități de program și elaborarea documentațiilor aferente Abilitatea de a intelege si a aborda probleme de modelare din alte stiinte C3.3 Utilizarea modelelor si instrumentelor informatice si matematice pentru rezolvarea problemelor specifice domeniului de aplicare
Competențe transversale	CT2 Desfășurarea eficientă a activităților organizate într-un grup inter-disciplinar și dezvoltarea capacităților empatică de comunicare inter-personală, de relaționare și colaborare cu grupuri diverse

6.2. Rezultatele învățării

Cunoștințe	Studentul a dobândit competențele specifice disciplinelor legate de matematică și algoritmică necesare pentru realizarea temelor. Studentul cunoaște noțiuni fundamentale legate de criptografie, precum și metode de aplicare a acestora în domenii ale științei legate de matematică și informatică.
Aptitudini	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.
Responsabilități și autonomie	Studentul este capabil să exploreze în mod independent anumite conținuturi matematice aplicate, bazându-se pe ideile și instrumentele din însușite deja, pentru a-și extinde cunoașterea. Studentul este capabil să extindă în mod independent ideile și argumentele matematice aplicate deja însușite, la un subiect matematic/informatic care nu a fost studiat anterior.

7. Obiectivele disciplinei (reieșind din grila competențelor acumulate)

7.1 Obiectivul general al disciplinei	Prezentarea unor algoritmi matematici folosiți în criptografia cu cheie publică
7.2 Obiectivele specifice	Algoritmi numerici și algebrici vor fi studiați și implementați în proiecte

8. Conținuturi

8.1 Curs	Metode de predare	Observații
1. Criptografie clasică, exemple	Expunere interactivă, explicație, demonstrație didactică	

2. Complexitatea algoritmilor, elemente de teoria numerelor	Expunere interactiva, explicatie, demonstratie didactica	
3. Criptografie cu cheie publica. RSA	Expunere interactiva, explicatie, demonstratie didactica	
4. Algoritmi pentru testarea primalitatii	Expunere interactiva, explicatie, demonstratie didactica	
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 logaritmulor discreti	Expunere interactiva, explicatie, demonstratie didactica	
10. Factorizarea polinoamelor: algoritmul lui Berlekamp	Expunere interactiva, explicatie, demonstratie didactica	
11. Semnaturi 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	Observatii
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. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului

Continutul este orientat catre aspecte practice ale criptografiei. Subiectul este prezent in mai multe programe de studii in domenii ale informaticii ale universitatilor importante.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Folosirea unor concepte si metode de baza in exemple	Teme	1/2 din nota
10.5 Seminar/laborator	Implementarea de concepte si algoritmi	Examinare practica	1/2 din nota
10.6 Standard minim de performanță			
Nota finala cel putin 5.			

11. Etichete ODD (Obiective de Dezvoltare Durabilă / Sustainable Development Goals)²

	Eticheta generală pentru Dezvoltare durabilă							
								

Data completării:
11.04.2025

Semnătura titularului de curs
Prof. dr. Septimiu Crivei

Semnătura titularului de seminar
Prof. dr. Septimiu Crivei

Data avizării în departament:
25.04.2025

Semnătura directorului de departament
Prof. dr. Andrei Mărcuș

² Păstrați doar etichetele care, în conformitate cu [Procedura de aplicare a etichetelor ODD în procesul academic](#), se potrivesc disciplinei și ștergeți-le pe celelalte, inclusiv eticheta generală pentru *Dezvoltare durabilă* - dacă nu se aplică. Dacă nicio etichetă nu descrie disciplina, ștergeți-le pe toate și scrieți "Nu se aplică".

