FIŞA DISCIPLINEI

Criptografie cu cheie publica

Anul universitar 2025-2026

1. Date despre program

1.1. Instituţia de învăţământ superior	Universitatea Babeş-Bolyai
1.2. Facultatea	Matematică şi Informatică
1.3. Departamentul	Matematică
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Licenţă
1.6. Programul de studii / Calificarea	Informatică
1.7. Forma de învăţământ	Cu frecvenţă

2. Date despre disciplină

2.1. Denumirea disciplinei	**Criptografie cu cheie publica**					Codul disciplinei	**MLE0049**
2.2. Titularul activităţilor de curs	Prof. dr. Septimiu Crivei						
2.3. Titularul activităţilor 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 activităţilor 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 învăţământ	42	din care: 3.5. curs	28	3.6 seminar/laborator	**14**
Distribuţia fondului de timp pentru studiul individual (SI) şi activităţi de autoinstruire (AI)					**ore**
Studiul după manual, suport de curs, bibliografie şi notiţe (AI)					14
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					8
Pregătire seminare/ laboratoare/ proiecte, teme, referate, portofolii şi eseuri					14
Tutoriat (consiliere profesională)					14
Examinări					8
Alte activităţi					0
3.7. Total ore studiu individual (SI) şi activităţi de autoinstruire (AI)				**58**	
3.8. Total ore pe semestru				**100**	
3.9. Numărul de credite				**4**	

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	
4.2. de competenţe	

5. Condiţii (acolo unde este cazul)

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

6.1. Competenţele specifice acumulate[1]

[1] Se poate opta pentru competenţe sau pentru rezultatele învăţării, respectiv pentru ambele. În cazul în care se alege o singură variantă, se va şterge tabelul aferent celeilalte opţiuni, iar opţiunea păstrată va fi numerotată cu 6.

Competențe profesionale/esențiale	C1.5 Dezvoltarea de unităţi de program şi elaborarea documentaţiilor 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 Desfăşurarea eficientă a activităţilor organizate într-un grup inter-disciplinar şi dezvoltarea capacităţilor empatice de comunicare inter-personală, de relaţionare şi colaborare cu grupuri diverse

6.2. Rezultatele învăţării

Cunoștințe	Studentul a dobândit competenţele specifice disciplinelor legate de matematică şi algoritmica necesare pentru realizarea temelor. Studentul cunoaşte noţiuni fundamentale legate de criptografie, precum şi metode de aplicare a acestora în domenii ale ştiinţei legate de matematică şi informatică.
Aptitudini	Studentul are abilitatea de a dezvolta gândirea matematică şi algoritmică, progresând de la o înţelegere procedurală/computaţională a matematicii la o înţelegere largă care să cuprindă raţionamentul logic, generalizarea, abstractizarea şi demonstraţia formală.
Responsabilități și autonomie	Studentul este capabil să exploreze în mod independent anumite conţinuturi matematice aplicate, bazându-se pe ideile şi instrumentele din însuşite deja, pentru a-şi extinde cunoaşterea. Studentul este capabil să extindă în mod independent ideile şi argumentele matematice aplicate deja însuşite, la un subiect matematic/informatic care nu a fost studiat anterior.

7. Obiectivele disciplinei (reieşind din grila competenţelor acumulate)

7.1 Obiectivul general al disciplinei	Prezentarea unor algoritmi matematici folositi in criptografia cu cheie publica
7.2 Obiectivele specifice	Algoritmi numerici si algebrici vor fi studiati si implementati in proiecte

8. Conţinuturi

8.1 Curs	**Metode de predare**	**Observaţii**
1. Criptografie clasica, exemple	Expunere interactiva, explicatie, demonstratie didactica	

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 logaritmilor 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**	**Observaţii**
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 conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi 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 performanţă			
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 Mărcuş

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