FIȘA DISCIPLINEI

Criptografie

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	**Informatică**
1.4. Domeniul de studii	**Informatică**
1.5. Ciclul de studii	**Licență**
1.6. Programul de studii / Calificarea	**Informatică în limba germană**
1.7. Forma de învățământ	**Cu frecvență**

2. Date despre disciplină

2.1. Denumirea disciplinei	**Criptografie**					Codul disciplinei	**MLG0059**
2.2. Titularul activităților de curs	Lekt. dr. Thu Hang Bui						
2.3. Titularul activităților de seminar	Lekt. dr. Thu Hang Bui						
2.4. Anul de studiu	2	2.5. Semestrul	2	2.6. Tipul de evaluare	C	2.7. Regimul disciplinei	Optional

3. Timpul total estimat (ore pe semestru al activităților didactice)

3.1. Număr de ore pe săptămână	2	din care: 3.2. curs	2	3.3. seminar/ laborator/proiect	2+2
3.4. Total ore din planul de învățământ	52	din care: 3.5. curs	28	3.6 seminar/laborator/proiect	24
Distribuția fondului de timp pentru studiul individual (SI) și activități de autoinstruire (AI)					ore
Studiul după manual, suport de curs, bibliografie și notițe (AI)					20
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					20
Pregătire seminare/ laboratoare/ proiecte, teme, referate, portofolii și eseuri					20
Tutoriat (consiliere profesională)					10
Examinări					3
Alte activități					
3.7. Total ore studiu individual (SI) și activități de autoinstruire (AI)				73	
3.8. Total ore pe semestru				125	
3.9. Numărul de credite				5	

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	Fundamentele algebrice ale informaticii
4.2. de competențe	

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Sala de curs dotata cu tablă și videoproiector
5.2. de desfășurare a seminarului/ laboratorului	Laborator dotat cu tablă și videoproiector, laptopuri

6.1. Competențele specifice acumulate[1]

[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	C 4.1 Definirea conceptelor și principiilor de bază ale informaticii, precum și a teoriilor și modelelor matematice C 4.3 Identificarea modelelor si metodelor adecvate pentru rezolvarea unor probleme reale C 4.4 Utilizarea simulării pentru studiul comportamentului modelelor realizate si evaluarea performantelor C 4.5 Încorporarea de modele formale în aplicații specifice din diverse domenii C6.4 Efectuarea de măsurători de performanță pentru timpi de răspuns, consum de resurse; stabilirea drepturilor de acces.
Competențe transversale	CT1 Aplicarea regulilor de muncă organizată și eficientă, a unor atitudini responsabile față de domeniul didactic-științific, pentru valorificarea creativă a propriului potențial, cu respectarea principiilor și a normelor de etică profesională CT2 Desfășurarea eficientă a activităților organizate într-un grup inter-disciplinar și dezvoltarea capacităților empatice de comunicare inter-personală, de relaționare și colaborare cu grupuri diverse CT3 Utilizarea unor metode și tehnici eficiente de învățare, informare, cercetare și dezvoltare a capacităților de valorificare a cunoștințelor, de adaptare la cerințele unei societăți dinamice și de comunicare în limba română și într-o limbă de circulație internațională

6.2. Rezultatele învățării

Cunoștințe	Studentul este capabil să asigure formarea competențelor specifice disciplinelor din domeniul matematicii și algoritmicii, necesare pentru realizarea sarcinilor de lucru. Studentul cunoaște noțiunile fundamentale legate de criptografie și metodele de aplicare ale acestora în domenii științifice conexe matematicii și informaticii.
Aptitudini	Absolventul își va dezvolta gândirea matematică și algoritmică, evoluând de la o înțelegere procedurală/computațională a matematicii la o înțelegere amplă care include raționamentul logic, generalizarea, abstractizarea și demonstrația formală.
Responsabilități și autonomie	Studentul este capabil să exploreze în mod independent conținuturi matematice aplicate, bazându-se pe idei și instrumente dobândite anterior pentru a-și extinde înțelegerea. Studentul va extinde în mod independent idei și argumente matematice aplicate din cursurile anterioare către o temă de matematică/informatică care nu a fost studiată anterior.

7. Obiectivele disciplinei (reieșind din grila competențelor acumulate)

7.1 Obiectivul general al disciplinei	Kryptografiealgorithmen und Anwendungen der Kryptografie in der Praxis, z. B. in MAC, digitale Signatur, Steganografie, Netzwerksicherheit, Bitcoin, Post-Quanten usw.
7.2 Obiectivele specifice	Se studiaza algoritmi de teoria numerelor si algebra, fiind apoi implementati in proiecte concrete.

8. Conținuturi

8.1 **Curs**	Metode de predare	Observații
1. Criptografie clasica. Exemple. Sisteme de criptare.	expunerea, conversația, discutarea unor studii de caz	
2. Principiile criptografiei moderne. Scenarii de atac. Metode de criptanaliza.	expunerea, conversația, discutarea unor studii de caz	
3. Securitatea sistemelor criptografice.	expunerea, conversația, discutarea unor studii de caz	

4. Criptografia simetrica. Moduri de criptare.	expunerea, conversaţia, discutarea unor studii de caz	
5. Standardul de criptare a datelor: (DES) și AES	expunerea, conversaţia, discutarea unor studii de caz	
6. Funcționarea cifrării bloc	expunerea, conversaţia, discutarea unor studii de caz	
7. Criptografie cu cheie publică: RSA, Diffie-Hellman	expunerea, conversaţia, discutarea unor studii de caz	
8. Algoritmi de semnătură digitală: RSA folosind funcția hash, ElGamal DS, Schnoor DS, DSA	expunerea, conversaţia, discutarea unor studii de caz	
9. Funcții hash criptografice	expunerea, conversaţia, discutarea unor studii de caz	
10. Bitcoins	expunerea, conversaţia, discutarea unor studii de caz	
11. Post-cuantică	expunerea, conversaţia, discutarea unor studii de caz	
12. Algoritmi de criptare în rețelele telefonice și atacuri asupra rețelelor telefonice	expunerea, conversaţia, discutarea unor studii de caz	
13. Criptografie în securitatea rețelelor	expunerea, conversaţia, discutarea unor studii de caz	

In limba germana:

- Buchmann Johannes, Einführung in die Kryptographie, Springer, 2001.
- Klein, Andreas, Visuelle Kryptographie, Springer 2007.
- Schwenk, J., Sicherheit und Kryptographie im Internet, Vieweg, 2005.

In limba engleza

- S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to cryptography and coding theory, Editura EFES, 2006.
- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography. CRC Press, Boca Raton, 1997. (http://www.math.uwaterloo.ca/~ajmeneze)
- B. Schneier, Applied Cryptography. John Wiley & Sons, 1996.

8.2 Seminar	Metode de predare	Observații

Seminarul 1: Criptografie clasică	problematizarea, exemplificarea	
Seminarul 2: Criptoanaliza pentru cifruri clasice	problematizarea, exemplificarea	
Seminarul 3: Cheie publică simetrică (DES şi AES)	problematizarea, exemplificarea	
Seminarul 4: Cheie asimetrică (RSA) și DSS	problematizarea, exemplificarea	
Seminarul 5: MAC și HMAC	problematizarea, exemplificarea	
Seminarul 6: Steganografie	problematizarea, exemplificarea	
Seminarul 7: Post-cuantic (Distribuirea cheilor cuantice QKD)	problematizarea, exemplificarea	

Bibliografie

1. S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to cryptography and coding theory, Editura EFES, 2006.

2. R. **Küsters,** Ralf, Th. **Wilke**, Thomas, Moderne Kryptographie - Eine Einführung, Leitfäden der Informatik , Springer-Vieweg, 2011

9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului

- Cursul respectă recomandările curiculare IEEE / ACM pentru programele de studii de informatică;
- Cursuri cu conţinut similar sunt predare la majoritatea universităţilor din România care au programe de studii similare;

Companiile de dezvoltare de software consideră foarte important conţinutul cursului pentru formarea viitorilor dezvoltatori de software

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Conceptele predate la curs şi metodologiile de modelare	Examen final	70%

10.5 Seminar/Laborator	Modalitatea de aplicare a metodologiilor de modelare pentru rezolvarea unor probleme concrete	3 miniproiecte de modelare prezenţa/activitatea de la seminar	30%
10.6 Standarde minime de performanţă			
minim nota 5 la fiecare dintre examene (parţial şi final) minim nota 5 la evaluarea miniproiectelor			

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

Nu se aplică.

Data completării:	Semnătura titularului de curs	Semnătura titularului de seminar
30.10.2025	Lect. dr. Bui Thang	Lect. dr. Bui Thang

Data avizării în departament:	Semnătura directorului de departament
... 30.10.2025	Conf.dr. Adrian STERCA

[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.*".