FIŞA DISCIPLINEI

Introducere în criptografie

Anul universitar 2025-2026

1. Date despre program

1.1. Instituţia de învăţământ superior	Universitatea Babeş-Bolyai din Cluj-Napoca
1.2. Facultatea	Facultatea de Matematică şi Informatică
1.3. Departamentul	Departamentul de Matematică şi Informatică al Liniei Maghiare
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Licenţă
1.6. Programul de studii / Calificarea	Informatică (în limba maghiară)
1.7. Forma de învăţământ	Învăţământ cu frecvenţă

2. Date despre disciplină

2.1. Denumirea disciplinei	**Introducere în criptografie/Bevezetés a kriptográfiába/Introduction to Criptography**					Codul disciplinei	**MLM5085**
2.2. Titularul activităţilor de curs	Şuteu-Szöllősi Ştefan Lucian						
2.3. Titularul activităţilor de seminar	Şuteu-Szöllősi Ştefan Lucian						
2.4. Anul de studiu	3	2.5. Semestrul	5	2.6. Tipul de evaluare	Colocviu (C)	2.7. Regimul disciplinei	Disciplină de specialitate (DS)

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

3.1. Număr de ore pe săptămână	**4**	din care: 3.2. curs	**2**	3.3. seminar/ laborator/proiect	**2**
3.4. Total ore din planul de învăţământ	**56**	din care: 3.5. curs	**28**	3.6 seminar/laborator/proiect	**28**
Distribuţia fondului de timp pentru studiul individual (SI) şi activităţi de autoinstruire (AI)					**ore**
Studiul după manual, suport de curs, bibliografie şi notiţe (AI)					8
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					2
Pregătire seminare/ laboratoare/ proiecte, teme, referate, portofolii şi eseuri					24
Tutorat (consiliere profesională)					4
Examinări					4
Alte activităţi					2
3.7. Total ore studiu individual (SI) şi activităţi de autoinstruire (AI)				**44**	
3.8. Total ore pe semestru				**100**	
3.9. Numărul de credite				**4**	

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	Nu e cazul
4.2. de competenţe	Cunoştinţe de bază de algebră, teoria numerelor, programare

5. Condiţii (acolo unde este cazul)

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

6.1. Competenţele specifice acumulate[1]

Competenţe profesionale/esenţiale	• C1.5 Dezvoltarea de unităţi de program şi elaborarea documentaţiilor aferente • C3.2 Descrierea de concepte, teorii şi modele folosite în domeniul de aplicare • C3.3 Utilizarea modelelor şi instrumentelor informatice şi matematice pentru rezolvarea problemelor specifice domeniului de aplicare • C3.5 Elaborarea componentelor informatice ale unor proiecte interdisciplinare
Competenţe transversale	• CT1 Aplicarea regulilor de muncă organizată şi eficientă, a unor atitudini responsabile fată de domeniul didactic-ştiinţific, pentru valorificarea creativă a propriului potenţial, cu respectarea principiilor şi a normelor de etică profesională • CT3 Utilizarea unor metode şi tehnici eficiente de învăţare, informare, cercetare şi dezvoltare a capacităţilor de valorificare a cunoştinţelor, de adaptare la cerinţele unei societăţi dinamice şi de comunicare în limba română şi într-o limbă de circulaţie internaţională

7. Obiectivele disciplinei (reieşind din grila competenţelor acumulate)

7.1 Obiectivul general al disciplinei	• Prezentarea, analiza siguranţei şi implementarea diferitelor sisteme criptografice (de la cele clasice la cele cu cheie publică) şi a diferitelor protocoale criptografice (funcţii hash, semnătura digitala, TLS, cripto-valute). Înţelegerea cadrului matematic asociat şi al principiilor de construcţie ale acestor sisteme.
7.2 Obiectivele specifice	• Scopul laboratoarelor este implementarea şi utilizarea specifică a sistemelor criptografice de mai sus, îmbunătăţind astfel şi abilităţile de programare.

8. Conţinuturi

8.1 Curs	**Metode de predare**	**Observaţii**
1. Noţiuni criptografice de bază. Sistemul CAESAR şi variantele lui	Prelegere, demonstraţie, exemple	[1], capitolul 1, 2.1.1
2. Sisteme matriceale, sistemele Vigenère, Playfair	Prelegere, demonstraţie, exemple	[1], capitolul 2.1.2
3. Codebook, sisteme de transpoziţie, aparate de criptare	Prelegere, demonstraţie, exemple	[1], capitolul 2.1.3, 4, 5, 6
4. One time pad, generarea numerelor pseudo-aleatoare	Prelegere, demonstraţie, exemple	[1], capitolul 2.2.1
5. Noţiuni din teoria complexităţii. Corpuri finite	Prelegere, demonstraţie, exemple	[1], Appendix
6. Sisteme Feistel 1 (DES, AES)	Prelegere, demonstraţie, exemple	[1], capitolul 2.2.2

[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.

7. Sisteme Feistel 2 (criptanaliză diferențială)	Prelegere, demonstrație, exemple	[6]
8. Funcţii one-way şi trapdoor. Sisteme cu cheie publică Knapsack	Prelegere, demonstrație, exemple	[1], capitolul 3, 3.1
9. Cifrul RSA	Prelegere, demonstrație, exemple	[1], capitolul 3.2
10. Sisteme bazate pe logaritmare discretă	Prelegere, demonstrație, exemple	[1], capitolul 3.3, 4
11. Funcţii hash	Prelegere, demonstrație, exemple	[1], capitolul 4
12. Protocoale criptografice 1 (semnătura digitală, autentificare)	Prelegere, demonstrație, exemple	[1], capitolul 5, 6
13. Protocoale criptografice 2 (TLS)	Prelegere, demonstrație, exemple	[1], capitolul 5, 6
14. Bazele criptografice ale criptovalutei Bitcoin. Structura unui blockchain	Prelegere, demonstrație, exemple	[7]

Bibliografie

[1] Szántó Cs., Şuteu Szöllősi I.: *Kriptográfia*, Presa Universitară Clujeană, 2009.
[2] Koblitz N.: *A Course in Number Theory and Cryptography* (Second Edition), Springer, 1994.
[3] Salomaa A.: *Public-Key Cryptography* (Second Edition), Springer, 2000.
[4] Crivei S., Marcus A., Sacarea Ch., Szántó Cs.: *Computational algebra with applications to coding theory and cryptography*, EFES, 2006.
[5] Heiko Knospe: *A Course in Cryptography*, AMS Pure and Applied Undergraduate Texts, 2019
[6] https://www.ukma.edu.ua/~yubod/teach/coding/crypto/diffanalysis.pdf
[7] Nakamoto, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf, 2009

8.2 Seminar / laborator	**Metode de predare**	**Observaţii**
1. Folosirea sistemelor de version control (Git) în programare. Programare în Python	Prelegere, exemple	[1], [2], [3]
2. Implementarea sistemelor criptografice clasice (sistemul CAESAR şi variantele lui, sisteme matriceale, sisteme de transpoziţie, etc.) în Python	Prelegere, exemple, implementare	[4], [5]
3. Criptanaliza sistemelor criptografice clasice	Exemple, exerciţii, implementare	[6]
4. Algoritmi pentru generarea numerelor pseudo-aleatoare. Implementarea cifrelor de flux în Python. Aplicaţii (comunicare securizată între programe)	Prelegere, implementare	[7]
5. Infrastructuri cu chei publice (PKI). Implementare/simulare în Python	Prelegere, exemple, implementare	
6. SSL/TLS în practică. Implementare în Java (OpenSSL, java.security). Aplicaţii (generarea şi verificarea certificatelor, comunicare securizată client-server, etc.)	Prelegere, implementare	[8]
7. Securizarea serverelor web. Bune practici de securitate	Prelegere, exemple, exerciţii	[9]

Bibliografie

[1] https://try.github.io/
[2] https://www.atlassian.com/git/tutorials
[3] https://www.vogella.com/tutorials/Git/article.html
[4] PEP 8 – Style Guide for Python Code, https://peps.python.org/pep-0008/
[5] PEP 20 – The Zen of Python, https://peps.python.org/pep-0020/
[6] https://www.cryptool.org
[7] NIST - National Institute of Standards and Technology, *A Statistical Test Suite for Random and Pseudorandom Number*

Generators for Cryptographic Applications, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf
[8] Oracle, *Package java.security*, https://docs.oracle.com/javase/8/docs/api/java/security/package-summary.html
[9] The Open Worldwide Application Security Project (OWASP), https://owasp.org

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

- Conținutul cursului coincide cu cel tradițional al unui curs de criptografie predat la universitățile majore din învățământul universitar.
- Diferitele implementări criptografice testează și dezvoltă în mod semnificativ abilitățile de programare.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Capacitatea de aplicare a noțiunilor teoretice	Examen scris și oral (dacă este cazul)	50%
10.5 Seminar/laborator	Abilitatea de a implementa și de a analiza sistemele criptografice	Probleme concrete de implementare și analiză	50%
10.6 Standard minim de performanță			
• Nota de trecere este 5 (care trebuie obținută atât la examenul scris cât și la laborator)			

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

Data completării:
30.04.2025

Semnătura titularului de curs

Conf. dr. Șuteu-Szöllősi Ștefan Lucian

Semnătura titularului de seminar

Conf. dr. Șuteu-Szöllősi Ștefan Lucian

Data avizării în departament:
...

Semnătura directorului de departament

Conf. dr. András Szilárd Károly

[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.*".