

A TANTÁRGY ADATLAPJA

Bevezetés a kriptográfiába

Egyetemi tanév 2025-2026

1. A képzési program adatai

1.1. Felsőoktatási intézmény	Babeş–Bolyai Tudományegyetem
1.2. Kar	Matematika és Informatika Kar
1.3. Intézet	Magyar Matematika és Informatika Intézet
1.4. Szakterület	Informatika
1.5. Képzési szint	Alapképzés
1.6. Tanulmányi program / Képesítés	Informatika
1.7. Képzési forma	Nappali

2. A tantárgy adatai

2.1. A tantárgy neve		Introducere în criptografie/Bevezetés a kriptográfiába/Introduction to Cryptography				A tantárgy kódja	MLM5085
2.2. Az előadásért felelős tanár neve			Şuteu-Szöllősi Ştefan Lucian				
2.3. A szemináriumért felelős tanár neve			Şuteu-Szöllősi Ştefan Lucian				
2.4. Tanulmányi év	3	2.5. Félév	5	2.6. Értékelés módja	K	2.7. Tantárgy típusa	Választható, szaktárgy

3. Teljes becsült idő (az oktatási tevékenység féléves óraszama)

3.1. Heti óraszám	4	melyből: 3.2 előadás	2	3.3 szeminárium/labor/projekt	2
3.4. Tantervben szereplő összóraszám	56	melyből: 3.5 előadás	28	3.6 szeminárium/labor	28
Az egyéni tanulmányi idő (ET) és az önképzési tevékenységekre (ÖT) szánt idő elosztása:					óra
A tankönyv, a jegyzet, a szakirodalom vagy saját jegyzetek tanulmányozása					8
Könyvtárban, elektronikus adatbázisokban vagy terepen való további tájékozódás					2
Szemináriumok / laborok, házi feladatok, portfóliók, referátumok, esszék kidolgozása					24
Egyéni készségfejlesztés (tutorálás)					4
Vizsgák					4
Más tevékenységek:					2
3.7. Egyéni tanulmányi idő (ET) és önképzési tevékenységekre (ÖT) szánt idő összóraszama					44
3.8. A félév összóraszama					100
3.9. Kreditszám					4

4. Előfeltételek (ha vannak)

4.1. Tantervi	Nincsen
4.2. Kompetenciabeli	Algebrai, számelméleti, programozási ismeretek

5. Feltételek (ha vannak)

5.1. Az előadás lebonyolításának feltételei	Vetítővel (videoprojektorral) felszerelt tanterem
5.2. A szeminárium / labor lebonyolításának feltételei	Vetítővel (videoprojektorral) felszerelt tanterem

6.1. Elsajátítandó jellemző kompetenciák¹

¹ Választhat kompetenciák vagy tanulási eredmények között, illetve választhatja mindkettőt is. Amennyiben csak az egyik lehetőséget választja, a másik lehetőséget el kell távolítani a táblázatból, és a kiválasztott lehetőség a 6. számot kapja.

Szakmai/kulcs-kompetenciák	- C1.5 A programegységek fejlesztése és a kapcsolódó dokumentáció megvalósítása - C3.2 Az alkalmazási területnek megfelelő alapvető informatikai modellek azonosítása és magyarázata - C3.3 Számítógépes és matematikai modellek és eszközök használata az alkalmazási területre specifikus feladatok megoldására - C3.5 Interdiszciplináris projektek számítógépes elemeinek kidolgozása
Transzverzális kompetenciák	- CT2 Interdiszciplináris csoportban szervezett tevékenységek hatékony lebonyolítása és az interperszonális kommunikáció, a különféle csoportokhoz való viszony és együttműködés empátikus - CT3 Hatékony módszerek és technikák használata tanulásra, információszerzésre, kutatásra és a tudásszerzési kapacitások fejlesztésére, egy dinamikus társadalom igényeinek való megfelelésre, román és egy nemzetközi nyelven történő kommunikáció-képesség fejlesztése

7. A tantárgy célkitűzései (az elsajátítandó jellemző kompetenciák alapján)

7.1 A tantárgy általános célkitűzése	Az előadás célja egyrészt különböző (titkos és nyilvános kulcsú) kriptorendszerek bemutatása és ezek matematikai hátterének és biztonságának elemzése (kriptoanalízise), másrészt új nyilvános kulcsú kriptorendszerek szerkesztési elveinek, szabályainak a megismertetése, harmadrészt egyéb kriptográfia protokollok bemutatása (hash függvények, digitális aláírás, TLS, kriptovaluták).
7.2 A tantárgy sajátos célkitűzései	A laborok célja az említett kriptorendszerek számítógépes implementációja, illetve konkrét használatának bemutatása, fejlesztve ezáltal programozási készségeket is.

8. A tantárgy tartalma

8.1 Előadás	Didaktikai módszerek	Megjegyzések
1. Kriptográfiai alapfogalmak, Caesar-kód és variációi	Előadás, magyarázat, példák	[1], 1, 2.1.1 fejezet
2. Mátrixos rendszerek, Vigenère- és Playfair-rendszer	Előadás, magyarázat, példák	[1], 2.1.2 fejezet
3. Kódkönyv, átrendezéssel kódok, rejtjelező gépek	Előadás, magyarázat, példák	[1], 2.1.3, 4, 5, 6 fejezet
4. One time pad, átvétel-számok generálása	Előadás, magyarázat, példák	[1], 2.2.1 fejezet
5. Bonyolultságelméleti alapfogalmak. véges testek	Előadás, magyarázat, példák	[1], Appendix
6. Feistel típusú rendszerek 1 (DES, AES)	Előadás, magyarázat, példák	[1], 2.2.2 fejezet
7. Feistel típusú rendszerek 2 (differenciális kriptoanalízis)	Előadás, magyarázat, példák	[6]
8. Egyirányú és csapóajtó függvények. A Knapsack rendszer	Előadás, magyarázat, példák	[1], 3, 3.1 fejezet
9. RSA	Előadás, magyarázat, példák	[1], 3.2 fejezet
10. Diszkrét logaritmáláson alapuló rendszerek	Előadás, magyarázat, példák	[1], 3.3, 4 fejezet

11. Hash függvények	Előadás, magyarázat, példák	[1], 4 fejezet
12. Kriptográfiai protokollok 1 (Digitális aláírás, hitelesítés)	Előadás, magyarázat, példák	[1], 5, 6 fejezet
13. Kriptográfiai protokollok 2 (TLS)	Előadás, magyarázat, példák	[1], 5, 6 fejezet
14. A Bitcoin kriptográfiai háttere. Egy blokklánc felépítése	Előadás, magyarázat, példák	[7]
Könyvészet [1] Szántó Cs., Şuteu Szöllősi I.: <i>Kriptográfia</i> , Presa Universitară Clujeană, 2009. [2] Koblitz N.: <i>A Course in Number Theory and Cryptography</i> (Second Edition), Springer, 1994. [3] Salomaa A.: <i>Public-Key Cryptography</i> (Second Edition), Springer, 2000. [4] Crivei S., Marcus A., Sacarea Ch., Szántó Cs.: <i>Computational algebra with applications to coding theory and cryptography</i> , EFES, 2006. [5] Heiko Knospe: <i>A Course in Cryptography</i> , AMS Pure and Applied Undergraduate Texts, 2019 [6] https://www.ukma.edu.ua/~yubod/teach/coding/crypto/diffanalysis.pdf [7] Nakamoto, S., <i>Bitcoin: A Peer-to-Peer Electronic Cash System</i> , https://bitcoin.org/bitcoin.pdf , 2009		
8.2 Szeminárium / Labor	Didaktikai módszerek	Megjegyzések
1. Verziókövető rendszerek (Git) használata programozásban. Python programozás	Magyarázat, példák	[1], [2], [3]
2. Klasszikus kriptográfiai rendszerek (CAESAR-rendszer és változatai, mátrixrendszerek, átrendeztetési kódok stb.) implementációja Pythonban	Magyarázat, példák, implementálás	[4], [5]
3. Klasszikus kriptográfiai rendszerek kriptóanalízise	Magyarázat, gyakorlatok, implementálás	[6]
4. Álvéletlen-számok generálására szolgáló algoritmusok. Folyamtitkosítók implementálása Pythonban. Alkalmazások (programok közötti biztonságos kommunikáció)	Magyarázat, implementálás	[7]
5. Nyilvános kulcsú infrastruktúrák (PKI). Implementáció/szimuláció Pythonban	Magyarázat, példák, implementálás	
6. SSL/TLS a gyakorlatban. Implementáció Java nyelvben (OpenSSL, java.security). Alkalmazások (tanúsítványok generálása és ellenőrzése, biztonságos kliens-szerver kommunikáció stb.)	Magyarázat, implementálás	[8]
7. Webszerverek biztonságossá tétele. Általános tudnivalók a szerverek biztonságáról	Magyarázat, gyakorlatok, implementálás	[9]
Könyvészet [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, <i>A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications</i> , https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf [8] Oracle, <i>Package java.security</i> , 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. Az episztemikus közösségek képviselői, a szakmai egyesületek és a szakterület reprezentatív munkáltatói elvárásainak összhangba hozása a tantárgy tartalmával.

- A tantárgy tartalma megegyezik az egyetemi oktatásban a fontosabb egyetemeken oktatott kriptográfia tárgy hagyományos tartalmával.
- A különféle kriptorendszer-implementációk jelentős mértékben tesztelik és fejlesztik a programozási készségeket.

10. Értékelés

Tevékenység típusa	10.1 Értékelési kritériumok	10.2 Értékelési módszerek	10.3 Aránya a végső jegyben
10.4 Előadás	Elméleti anyag alkalmazási képessége	Írásbeli vizsga (szükség esetén szóbeli kérdésekkel kiegészítve)	50%
10.5 Szeminárium / Labor	Kriptográfiai rendszerek megvalósításának (implementálásának) és elemzésének képessége	Feladatok (implementálás, elemzés)	50%
10.6 A teljesítmény minimumkövetelményei			
• Minimális átmenő jegy 5. A minimumkövetelményeket írásbeli vizsgán és gyakorlaton (laboron) is teljesíteni kell az átmenőhöz.			

11. SDG ikonok (Fenntartható fejlődési célok/ Sustainable Development Goals)²



Kitöltés időpontja:
2025. 04. 30.

Előadás felelőse:

Dr. Şuteu-Szöllősi Ştefan Lucian,
egyetemi docens

Szeminárium felelőse:

Dr. Şuteu-Szöllősi Ştefan Lucian,
egyetemi docens

Az intézeti jóváhagyás dátuma:

...

Intézetigazgató:

Dr. András Szilárd Károly, egyetemi docens

² Csak azokat az ikonokat tartsa meg, amelyek az [SDG-ikonoknak az egyetemi folyamatban](#) történő alkalmazására vonatkozó eljárás szerint illeszkednek az adott tantárgyhoz, és törölje a többit, beleértve a fenntartható fejlődés általános ikonját is – amennyiben nem alkalmazható. Ha egyik ikon sem illik a tantárgyra, törölje az összeset, és írja rá, hogy „Nem alkalmazható”.