A TANTÁRGY ADATLAPJA

1. A képzési program adatai

1.1 Felsőoktatási intézmény	Babeș-Bolyai Tudományegyetem
1.2 Kar	Matematika és Informatika
1.3 Intézet	Magyar Matematika és Informatika Intézet
1.4 Szakterület	informatika
1.5 Képzési szint	Alap
1.6 Szak / Képesítés	Informatika

2. A tantárgy adatai

2.1 A tantárgy neve (hu) (en) (ro)	Bevezetés a kriptográfiába Introduction to cryptography Introducere în criptografie						
2.2 Az előadásért felelős tanár neve	Prof. dr. habil. Szántó Csaba						
2.3 A laborért felelős tanár neve	Lect. dr. Șuteu Szöllősi Ștefan Lucian						
2.4 Tanulmányi év	3	2.5 Félév	5	2.6. Értékelés módja	Kollokvium	2.7 Tantárgy típusa	Opcionális szaktárgy
2.8 A tantárgy kódja	MLM5085						

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

3.1 Heti óraszám	4	melyből: 3.2 előadás	2	3.3 szeminárium/labor	1+1
3.4 Tantervben szereplő össz-óraszám	56	melyből: 3.5 előadás	28	3.6 szeminárium/labor	28
A tanulmányi idő elosztása:					óra
A tankönyv, a jegyzet, a szakirodalom vagy saját jegyzetek tanulmányozása					7
Könyvtárban, elektronikus adatbázisokban vagy terepen való további tájékozódás					7
Laborok, házi feladatok, portofóliók, referátumok, esszék kidolgozása					7
Egyéni készségfejlesztés (tutorálás)					7
Vizsgák					8
Más tevékenységek: gyakorlati projektek					8

3.7 Egyéni munka össz-óraszáma	44
3.8 A félév össz-óraszáma	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	• Videoprojektorral felszerelt előadó
5.2 A szeminárium / labor lebonyolításának feltételei	• Videoprojektorral felszerelt előadó

6. Elsajátítandó jellemző kompetenciák

Szakmai 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 empatikus 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 kommunikációra való képességének 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 a fenti 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, példák, párbeszéd	[1], 1, 2.1.1 fejezet
2.Mátrixos rendszerek	Előadás, példák, párbeszéd	[1], 2.1.2 fejezet
3.Kódkönyv, átrendezéses kódok, rejtjelező gépek	Előadás, példák, párbeszéd	[1], 2.1.3,4,5,6 fejezet
4. Folyamtitkosítók (ONE TIME PAD)	Előadás, példák, párbeszéd	[1], 2.2.1 fejezet
5. Bonyolultság-elméleti alapfogalmak. Véges testek	Előadás, példák, párbeszéd	[1], Appendix, [8] Sagemath alkalmazása
6. Tömbtitkosítók 1 (DES,AES)	Előadás, példák, párbeszéd	[1], 2.2.2 fejezet
7. Tömbtitkosítók 2 (differenciál kriptoanalízis)	Előadás, példák, párbeszéd	[6]
8. One-way és trapdoor függvények. Knapsack rendszerek	Előadás, példák, párbeszéd	[1], 3,3.1 fejezet
9. RSA	Előadás, példák,	[1], 3.2 fejezet

	párbeszéd	
10. Diszkrét logaritmáláson alapuló rendszerek	Előadás, példák, párbeszéd	[1], 3.3,4 fejezet, [8] Sagemath alkalmazása
11. Hash függvények	Előadás, példák, párbeszéd	[1], 4 fejezet
12. Egyéb kriptográfiai protokollok (Digitális aláírás, hitelesítés)	Előadás, példák, párbeszéd	[1], 5,6 fejezet
13. Egyéb kriptográfiai protokollok (TLS)	Előadás, példák, párbeszéd	[1], 5,6 fejezet
14. BITCOIN kriptográfiai háttere. BLOCKCHAIN felépítése	Előadás, példák, párbeszéd	[7]

Könyvészet

[1] Szántó Cs., Șuteu Szöllősi I.: *Kriptográfia*, Kolozsvári Egyetemi Kiadó 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., Săcărea Ch., Szántó Cs.: *Computational algebra with applications to coding theory and cryptography*, EFES, 2006.
[5] Knospe H.: *A Course in Cryptography*, AMS Pure and Applied Undergraduate Texts, 2019
[6] https://www.ukma.edu.ua/~yubod/teach/coding/crypto/diffanalysis.pdf
[7] https://esirc.emporia.edu/bitstream/handle/123456789/3317/Sophia%20Crossen.pdf?sequence=1
[8] https://www.sagemath.org

8.2 Labor	Didaktikai módszerek	Megjegyzések
1.Kriptográfiai alapfogalmak, Caesar-kód és variációi	Példák, párbeszéd	Klasszikus kriptorendszerek implementációja és kriptoanalízise Pythonban 1
2.Mátrixos rendszerek	Implementációk, alkalmazások, párbeszéd	Klasszikus kriptorendszerek implementációja és kriptoanalízise Pythonban 2
3.Kódkönyv, átrendezéses kódok, rejtjelező gépek	Implementációk, alkalmazások, párbeszéd	Klasszikus kriptorendszerek implementációja és kriptoanalízise Pythonban 3
4. Folyamtitkosítók.	Implementációk, alkalmazások, párbeszéd	Álvéletlenszám-generátorok tesztelése 1
5. Bonyolultság-elméleti alapfogalmak. Véges testek	Implementációk, alkalmazások, párbeszéd	Álvéletlenszám-generátorok tesztelése 2
6. Tömbtitkosítók 1 (DES,AES)	Implementációk, alkalmazások, párbeszéd	
7. Tömbtitkosítók 2 (differenciális kriptoanalízis)	Implementációk, alkalmazások, párbeszéd	
8. One-way és trapdoor függvények. Knapsack rendszerek	Implementációk, alkalmazások, párbeszéd	
9. RSA	Implementációk, alkalmazások, párbeszéd	
10. Diszkrét logaritmáláson alapuló rendszerek	Implementációk, alkalmazások, párbeszéd	
11. Hash függvények	Implementációk, alkalmazások, párbeszéd	Biztonságos hálózati kommunikáció Javaban 1 (hash függvények)
12. Egyéb kriptográfiai protokollok (Digitális aláírás, hitelesítés)	Implementációk, alkalmazások, párbeszéd	Biztonságos hálózati kommunikáció Javaban 2

		(digitális aláírás)
13. Egyéb kriptográfiai protokollok (TLS)	Implementációk, alkalmazások, párbeszéd	Biztonságos hálózati kommunikáció Javaban 3 (TLS/SSL)
14. Bitcoin kriptográfiai háttere	Implementációk, alkalmazások, párbeszéd	Biztonságos hálózati kommunikáció Javaban 4 (TLS/SSL)

Könyvészet

[1] Szántó Cs., Șuteu Szöllősi I.: *Kriptográfia*, Kolozsvári Egyetemi Kiadó 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., Săcărea Ch., Szántó Cs.: *Computational algebra with applications to coding theory and cryptography*, EFES, 2006.
[5] Knospe H.: *A Course in Cryptography*, AMS Pure and Applied Undergraduate Texts, 2019
[6] https://www.ukma.edu.ua/~yubod/teach/coding/crypto/diffanalysis.pdf
[7] https://esirc.emporia.edu/bitstream/handle/123456789/3317/Sophia%20Crossen.pdf?sequence=1

9. Az episztemikus közösségek képviselői, a szakmai egyesületek és a szakterület reprezentatív munkáltatói elvárásainak összhangba hozása a tantárgy tartalmával.

- A tantárgy tartalma megegyezik 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 „Take home” vizsga: egyéni feladatlap megoldása 8 órás határidővel	50%
10.5 Labor	Kriptorendszerek implementálásának és feltörésének képessége	Határidős, gyakorlati implementációs és feltörési feladatok	50%
10.6 A teljesítmény minimumkövetelményei			
Minimális átmenő jegy 5 (úgy, hogy ez mind az elméleti, mind a gyakorlati részből meg kell legyen). Ehhez szükséges az alapfogalmak ismerete és egyszerű gyakorlatok implementálási képessége.			

Kitöltés dátuma	Előadás felelőse	Szeminárium felelőse
10.03.2024	Prof. dr. habil. Szántó Csaba	Lect. dr. Șuteu Szöllősi Ștefan Lucian

Az intézeti jóváhagyás dátuma	Intézetigazgató
13.03.2024	András Szilárd egyetemi docens