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
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	Szántó Csaba egyetemi docens						
2.3 A szemináriumért felelős tanár neve	Șuteu Szöllősi Ștefan Lucian adjunktus						
2.4 Tanulmányi év	3	2.5 Félév	5	2.6. Értékelés módja	Kollokvium	2.7 Tantárgy típusa	Választható szaktárgy
2.8 A tantárgy kódja	MLM5085						

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

3.1 Heti óraszám	3	melyből: 3.2 előadás	2	3.3 szeminárium/labor	1
3.4 Tantervben szereplő összóraszám	42	melyből: 3.5 előadás	28	3.6 szeminárium/labor	14

A tanulmányi idő elosztása:	óra
A tankönyv, a jegyzet, a szakirodalom vagy saját jegyzetek tanulmányozása	14
Könyvtárban, elektronikus adatbázisokban vagy terepen való további tájékozódás	8
Szemináriumok / laborok, házi feladatok, portfóliók, referátumok, esszék kidolgozása	14
Egyéni készségfejlesztés (tutorálás)	14
Vizsgák	4
Más tevékenységek: projekt	4

3.7 Egyéni munka összóraszáma	58
3.8 A félév összóraszáma	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	• Vetítő
5.2 A szeminárium / labor lebonyolításának feltételei	• Vetítő

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 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 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	[1], 1, 2.1.1 fejezet
2.Mátrixos rendszerek	Előadás	[1], 2.1.2 fejezet
3.Kódkönyv, átrendezéses kódok, rejtjelező gépek	Előadás	[1], 2.1.3,4,5,6 fejezet
4. Folyamtitkosítók.	Előadás	[1], 2.2.1 fejezet
5. Bonyolultság-elméleti alapfogalmak. Véges testek	Előadás	[1], Appendix
6. Tömbtitkosítók 1 (DES,AES)	Előadás	[1], 2.2.2 fejezet
7. Tömbtitkosítók 2 (differenciális kriptoanalízis)	Előadás	[6]
8. One-way és trapdoor függvények. Knapsack rendszerek	Előadás	[1], 3,3.1 fejezet
9. RSA	Előadás	[1], 3.2 fejezet

10. Diszkrét logaritmáláson alapuló rendszerek	Előadás	[1], 3.3,4 fejezet
11. Hash függvények	Előadás	[1], 4 fejezet
12. Egyéb kriptográfiai protokollok (Digitális aláírás, hitelesítés)	Előadás	[1], 5,6 fejezet
13. Egyéb kriptográfiai protokollok (TLS)	Előadás	[1], 5,6 fejezet
14. Bitcoin kriptográfiai háttere	Előadás	[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., 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] https://esirc.emporia.edu/bitstream/handle/123456789/3317/Sophia%20Crossen.pdf?sequence=1		
8.2 Szeminárium / Labor	Didaktikai módszerek	Megjegyzések
1.Kriptográfiai alapfogalmak, Caesar-kód és variációi	Példák	Klasszikus kriptorendszerek implementációja és kriptoanalízise Pythonban 1
2.Mátrixos rendszerek	Implementációk, alkalmazások	Klasszikus kriptorendszerek implementációja és kriptoanalízise Pythonban 2
3.Kódkönyv, átrendezéses kódok, rejtjelező gépek	Implementációk, alkalmazások	Klasszikus kriptorendszerek implementációja és kriptoanalízise Pythonban 3
4. Folyamtitkosítók	Implementációk, alkalmazások	Álvéletlenszám-generátorok tesztelése 1
5. Bonyolultság-elméleti alapfogalmak. Véges testek	Implementációk, alkalmazások	Álvéletlenszám-generátorok tesztelése 2
6. Tömbtitkosítók 1 (DES,AES)	Implementációk, alkalmazások	
7. Tömbtitkosítók 2 (differenciális kriptoanalízis)	Implementációk, alkalmazások	
8. One-way és trapdoor függvények. Knapsack rendszerek	Implementációk, alkalmazások	
9. RSA	Implementációk, alkalmazások	
10. Diszkrét logaritmáláson alapuló rendszerek	Implementációk, alkalmazások	
11. Hash függvények	Implementációk, alkalmazások	Biztonságos hálózati kommunikáció Javaban 1 (hash függvények)
12. Egyéb kriptográfiai protokollok (Digitális aláírás, hitelesítés)	Implementációk, alkalmazások	Biztonságos hálózati kommunikáció Javaban 2 (digitális aláírás)

13. Egyéb kriptográfiai protokollok (TLS)	Implementációk, alkalmazások	Biztonságos hálózati kommunikáció Javaban 3 (TLS/SSL)
14. Bitcoin kriptográfiai háttere	Implementációk, alkalmazások	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., 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] 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 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	Egyéni feladatlap 12 órás munkaidőre, majd másnap szóbeli	50%
10.5 Szeminárium / Labor	Kriptorendszerek implementálásának és feltörésének képessége	Konkrét implementációs és feltörési feladatok	50%

10.6 A teljesítmény minimumkövetelményei

Minimális átmenő jegy 5. Ezt mind elméleti, mind laborvizsgán el kell érni az átmenethez. Ehhez szükséges az alapfogalmak ismerete és egyszerű implementációk megvalósítási képessége.

Kitöltés dátuma	Előadás felelőse	Szeminárium felelőse
25.04.2023	Szántó Csaba egyetemi docens	Szántó Csaba egyetemi docens
Az intézeti jóváhagyás dátuma		Intézetigazgató
30.04.2023		András Szilárd egyetemi docens