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	Nyilvános kulcsú kriptográfia						
2.2 Az előadásért felelős tanár neve	Conf. Dr. Szántó Csaba						
2.3 A szemináriumért felelős tanár neve	Asist.Dr. Szöllősi István						
2.4 Tanulmányi év	3	2.5 Félév	5	2.6. Értékelés módja	kollokvium	2.7 Tantárgy típusa	kötelező-alap

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 össz-óraszám	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	33
Könyvtárban, elektronikus adatbázisokban vagy terepen való további tájékozódás	11
Szemináriumok / laborok, házi feladatok, portofóliók, referátumok, esszék kidolgozása	30
Egyéni készségfejlesztés (tutorálás)	14
Vizsgák	6
Más tevékenységek: projekt	14

3.7 Egyéni munka össz-óraszáma	108
3.8 A félév össz-óraszáma	150
3.9 Kreditszám	6

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	• Kriptorendszerek felépítésének és működésének megértése • Kriptorendszerek implementálásának és használatának képessége • Kriptorendszerek biztonsági elemzése
Transzverzális kompetenciák	• Programozási és algoritmikai képességek elmélyítése

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 pedig új nyilvános kulcsú kriptorendszerek szerkesztési elveinek, szabályainak a megismertetése.
7.2 A tantárgy sajátos célkitűzései	• A szemináriumok 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	Előadás	[1], 1 fejezet
2.Caesar-kód és variációi	Előadás	[1], 2.1.1 fejezet
3.Mátrixos rendszerek	Előadás	[1], 2.1.2 fejezet
4.Kódkönyv, átrendezéses kódok, rejtjelező gépek	Előadás	[1], 2.1.3,4,5,6 fejezet
5. Folyamtitkosítók	Előadás	[1], 2.2.1 fejezet
6. Tömbtitkosítók 1	Előadás	[1], 2.2.2 fejezet
7. Tömbtitkosítók 2	Előadás	[1], 2.2.2 fejezet
8. One-way és trapdoor függvények	Előadás	[1], 3 fejezet
9. Knapsack rendszerek	Előadás	[1], 3.1 fejezet
10. RSA	Előadás	[1], 3.2 fejezet
11. Diszkrét logaritmáláson alapuló rendszerek 1	Előadás	[1], 3.3,4 fejezet
12. Diszkrét logaritmáláson alapuló rendszerek 1	Előadás	[1], 3.3,4 fejezet
13. Hash függvények	Előadás	[1], 4 fejezet
14. Egyéb kriptográfiai protokollok	Előadás	[1], 5,6 fejezet
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.

8.2 Szeminárium / Labor	Didaktikai módszerek	Megjegyzések
1.Kriptográfiai alapfogalmak	Példák	
2.Caesar-kód és variációi	Implementációk, alkalmazások	
3.Mátrixos rendszerek	Implementációk, alkalmazások	
4.Kódkönyv, átrendezéses kódok, rejtjelező gépek	Implementációk, alkalmazások	
5. Folyamtitkosítók	Implementációk, alkalmazások	
6. Tömbtitkosítók 1	Implementációk, alkalmazások	
7. Tömbtitkosítók 2	Implementációk, alkalmazások	
8. One-way és trapdoor függvények	Implementációk, alkalmazások	
9. Knapsack rendszerek	Implementációk, alkalmazások	
10. RSA	Implementációk, alkalmazások	
11. Diszkrét logaritmáláson alapuló rendszerek 1	Implementációk, alkalmazások	
12. Diszkrét logaritmáláson alapuló rendszerek 1	Implementációk, alkalmazások	
13. Hash függvények	Implementációk, alkalmazások	
14. Egyéb kriptográfiai protokollok	Implementációk, alkalmazások	

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.

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	Pótólagos dokumentálódás	Referátum	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.			

Kitöltés dátuma	Előadás felelőse	Szeminárium felelőse
2015. április 30	.....	.....

Az intézeti jóváhagyás dátuma	Intézetigazgató
2015. április 30	Conf. Dr. Szenkovits Ferenc