Tantárgy neve: **Kriptográfia és biztonság**	**Kreditértéke: 5 kredit**
A tantárgy **besorolása**: **kötelező**	
A tantárgy elméleti vagy gyakorlati jellegének mértéke: **40/60** (kredit%)	
A **tanóra típusa**: ea. / konz és **óraszáma**: 2 / 2 / 1 az adott **félévben**,	
A **számonkérés** módja (koll. / gyj. / **egyéb**[1]): **koll / gyj**	
A tantárgy **tantervi helye** (hányadik félév): **4. félév, 5. félév**	
Előtanulmányi feltételek *(ha vannak)*: **Diszkrét Matematika I**	

Tantárgy-leírás: az elsajátítandó **ismeretanyag tömör, ugyanakkor informáló leírása**

A tantárgy keretében elméleti oldaról az egyszerűbb kriptográfiai primitívekhez szükséges matematikai és számításelméleti hátteret sajátíthatják el az érdeklődők. Gyakorlati oldalról alapvető kriptográfiai protokollokat, valamint komplex rendszereket mutatunk be számos alkalmazási területen keresztül.
Tematika: kriptográfiai biztonság alapjai, fenyegetésmodell, nehéz problémák, faktorizáció, diszkrét logaritmus; prímtesztek és támadások; szimmetrikus kulcsú kriptográfia, one-time pad, blokktitkosítók és folyamtitkosítók; nyilvános kulcsú kriptográfia, RSA, Diffie-Hellman kulcscsere, hash-függvények, MAC-ek, digitális aláírások.

A legfontosabb *kötelező,* illetve *ajánlott* irodalom (jegyzet, tankönyv) felsorolása bibliográfiai adatokkal (szerző, cím, kiadás adatai, (esetleg oldalak), ISBN)

Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein: Új algoritmusok, ISBN: 9789639193901

Buttyán Levente, Vajda István: Kriptográfia és alkalmazásai, ISBN: 978-963-2796-96-3

Bruce Schneier: Applied Cryptography – Protocols, Algorithms, and Source Code in C, ISBN 978-1-119-09672-6

Azoknak az előírt szakmai kompetenciáknak, kompetencia-elemeknek *(tudás, képesség* stb., *KKK 8. pont*) a felsorolása, amelyek kialakításához a tantárgy jellemzően, érdemben hozzájárul

pl.:

a) tudása

- Ismeri az informatikai szakterület tudásanyagát megalapozó általános és specifikus matematikai, számítástudományi elveket, tényeket, szabályokat, összefüggéseket, és eljárásokat.
- Ismeri az informatikai szakterület tervezési, fejlesztési, működtetési és irányítási folyamatainak alapvető feladatmegoldási elveit, módszereit és eljárásait, különösen a következő területen: információbiztonság.
- Rendelkezik az informatikai szakterület megfelelő szakspecifikus eszközeinek ismeretével az eszközök kiválasztásához és a feladatok elvégzéséhez, különösen alábbi területen: információbiztonság.

b) képességei

- Képes az általános és specifikus matematikai, számítástudományi elveket, tényeket, szabályokat, összefüggéseket alkalmazni informatikai szakterületen.
- Képes az informatikai szakterület tudásanyagát alkalmazni algoritmusok tervezésére, elemzésére és implementálására a legfontosabb programozási paradigmák figyelembe vételével.
- Képes az informatikai szakterület tudásanyagát alkalmazni információbiztonsági és kriptográfiai problémák esetében.
- Képes informatikai tudását az elsajátított matematikai, számítástudományi elvek, tények, szabályok, eljárások alapján folyamatosan fejleszteni.

Tantárgy felelőse (*név, beosztás, tud. fokozat*)**: Ligeti Péter, egyetemi adjunktus, PhD**

Tantárgy oktatásába bevont oktató(k), ha van(nak) (*név, beosztás, tud. fokozat*)**:**
Nagy Ádám, egyetemi tanársegéd
Tóth Viktória, egyetemi adjunktus, PhD