Tantárgy neve: **Cryptography and security**	**Kreditértéke: 5 kredit**
A tantárgy **besorolása**: **kötelezően választható**	
A tantárgy elméleti vagy gyakorlati jellegének mértéke, *„képzési karaktere”*: **2+3** (kredit%)	
A **tanóra típusa**: ea. / gyak. / konz. és **óraszáma**: 2 / 2 / 1 az adott **félévben**, (*ha nem (csak) magyarul oktatják a tárgyat, akkor a* **nyelve**:*)* Az adott ismeret átadásában alkalmazandó **további** (*sajátos*) **módok, jellemzők** *(ha vannak)*: -	
A **számonkérés** módja (koll. / gyj. / **egyéb**): **koll** Az ismeretellenőrzésben alkalmazandó **további** (*sajátos*) **módok** *(ha vannak)***: -**	
A tantárgy **tantervi helye** (hányadik félév): **4. félév, 5. félév**	
Előtanulmányi feltételek *(ha vannak)*: **Discrete mathematics I**	

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

From the theoretical point of view, this course gives introduction to the mathematical and computer science background necessary for simple cryptographic primitives. From the practical point of view, basic cryptographic protocols and complex systems were presented through several application areas.
Syllabus: security and privacy basics, risc modeling, hard problems, factorization, discrete logarithm problem; primality testing and attacks; symmetric crypto, one-time pad, blockcipher, streamcipher; public key crypto, RSA, Diffie-Hellman key exchange, hash functions, MAC, digital signatures.

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

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

Jonathan Katz, Yehuda Lindell: Introduction to Modern Cryptography: Principles and Protocols, ISBN-13: 978-1584885511

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*)**:**