Óbudai Egyetem Neumann János Informatikai Kar	Biomatika és Alkalmazott Mesterséges Intelligencia Intézet

Tantárgy neve és kódja: Kriptográfia és kvantumkriptográfia *NBXKR1HMLF* **Kreditérték*: 5***
/
Jelöljön ki egy elemet. ***Esti tagozat 2025/26 tanév II. félév***

Tantárgy felelős: Prof. Dr. Kozlovszky Miklós				
Tantárgy oktató: Prof. Dr. Takács Márta				
Előtanulmányi feltételek: (kóddal)	Szöveg beírásához kattintson ide.			
Heti óraszámok:	Előadás: 1	Tantermi gyak.: 0	Laborgyakorlat: 1	Konzultáció: 0
Számonkérés módja (vizsga v. évközi jegy):	vizsga			

A tananyag

Oktatási cél: A tantárgy célja, hogy a hallgatók megismerjék a kriptográfiai primitívekhez szükséges matematikai hátteret és az ezekhez kapcsolódó algoritmusokat. Az előadásokon bemutatásra kerülnek olyan titkosítási eljárások, amelyek garanciát adnak a kriptográfiai algoritmusok biztonságára. Gyakorlati oldalról ezek megvalósítását ismerhetik meg a hallgatók.

Tematika: Történelmi áttekintés, mono- és polialfabetikus rendszerek rövid bemutatása, DES AES, oszthatóság, prímek, lnko, lkkt, relatív prím, maradékos osztás, lineáris kongruencia, maradékosztályok, elsőfokú kongruencia egyenletek, Euler-féle φ függvény, Euler tétel, kis Fermat tétel, Wilson prímteszt, Fermat-prímteszt, AKS-prímteszt testek algebrai struktúrája, véges testek, testbővítés, RSA, SSL/TLS, PGP, elliptikus görbék, művelet elliptikus görbékkel, elliptikus görbék véges test felett, Diffie-Helmann kulcscsere elektronikus aláírás tulajdonságai, aláírás logikája, aláírás tartalma, aláírás RSA-val, aláírás elliptikus görbékkel, a kvantumkriptográfia algoritmusai, Poszt kvantumkriptográfia, QKD, NIST PQC szabványosítás, kriptográfiai PQC-ben.

Féléves ütemezés:	
Oktatási hét szerinti témakörök (konzultáció)	Témakör
1.	Történelmi áttekintés, motiváció, Alapfogalmak, Klasszikus és modern titkosítási eljárások, gyakorlati használati példák: digitális aláírás, üzenet pecsét, kulcsgondozás, kriptográfia a kommunikációban
2.	Szimmetrikus kulcsú titkosítások (DES, AES)
3.	Számelméleti alapok
4.	Kongruenciák relációk, kongruencia egyenletek, prímtesztek
5	Műveletek véges testek felett, testbővítés
6.	Aszimmetrikus kulcsú titkosítások (RSA)
7.	Biztonságtechnikai protokollok (SSL/TLS, PGP)
8.	Elliptikus görbék
9.	Elektronikus aláírás
10.	A kvantuminformatika és a kvantumkriptográfia algoritmusai
11.	Poszt kvantumkriptográfia, A kvatumkriptográfia határai
12.	A QKD és szerepe a kvantumkriptográfiában, NIST PQC szabványosítás, Az OQS projekt, Kriptográfiai típusok PQC-ben,
13.	Zárthelyi dolgozat
14.	Zárthelyi dolgozat pótlása

Félévközi követelmények

Aláírás megszerzésének feltétele:
- az előadásokon feladott házi feladatok feltöltése a Moodle rendszerbe (50%-ban számítható be a vizsgajegy kialakításába)
- a ZH megírása legalább elégséges érdemjeggyel (beszámítható legfeljebb 50%-ban a vizsgajegybe).

2026. 01. 16.

Zárthelyi dolgozatok	
Oktatási hét (konzultáció)	Témakör
13	Labor és elméleti ZH
14	Labor és elméleti ZH(pót)

A *félévzáró érdemjegy* kialakításának módszere
A ZH pontszámai alapján. Ponthatárok: 0-49 elégtelen (1) 50-61 elégséges (2) 62-74 közepes (3) 75-85 jó (4) 86-100 jeles (5)
Pótlás módja
Az aláírás pótlásának módja a labor ZH pótlása a 14. héten és a házi feladatok utólagos beadása (pontlevonással jár). Aláíráspótlásra a vizsgaidőszak első hetében a meghirdetett időpontban van lehetőség.
Vizsga módja
-Évközi jegy a félévközi teljesítmény alapján
Vizsgajegy kialakítása
-lásd fentebb
Irodalom
Kötelező:
Liptai Kálmán: Kriptográfia, Digitális Tankönyvtár, 2011
Ajánlott:
Zhiyong Zheng: Modern Cryptography Volume 1: A Classical Introduction Springer; 1st ed. 2022 edition (2022); eBook (Creative Commons Licensed), **ISBN-10:** 9811909229, **ISBN-13:** 978-9811909221 Zhiyong Zheng , Kun Tian , Fengxia Liu: Modern Cryptography Volume 2: Post-Quantum Cryptography, Springer; 1st ed. (2023), **ISBN-10:** 9811976465, **ISBN-13:** 978-9811976469
Egyéb segédletek:
Az órákon javasolt és a Moodle rendszerben hivatkozott további internetes források