

TANTÁRGYI TEMATIKA ÉS TELJESÍTÉSI KÖVETELMÉNYEK 2022/2023. ÉV TAVASZI FÉLÉV

Cím *Bevezetés a számítástudományba*

Tárgykód	IVB014MLMI
Óraszám:	5 alkalom, ebből ea/gy/lab: 2/0/0
Kreditpont	3
Szak(ok)/ típus	Mérnökinformatikus
Tagozat	levelező
Követelmény	vizsga
Meghirdetés féléve	2
Előzetes követelmény(ek)	nincs
Oktató tanszék(ek)	Mérnöki Matematika Tanszék
Tárgyfelelős	Pilgermájer Ákos
Oktatók	Gyöngy András

TÁRGYLEÍRÁS

A számfogalom kialakulása, Peano axiómák, helyiértékes számrendszerek, műveletek elvégzése helyiértékes számrendszerekben, az Euklideszi algoritmus, oszthatóság, legnagyobb közös osztó, legkisebb közös többszörös, osztók száma, prímszámok, a számelmélet alaptétele, kongruenciák, műveletek kongruenciákon, maradékosztályok, teljes és redukált maradékrendszer, Euler-Fermat tétel, Euler-féle függvény, lineáris kongruenciák és kongruencia-rendszerek, Kínai maradéktétel, kriptográfia, RSA kódolás.

TÁRGYTEMATIKA

1. AZ OKTATÁS CÉLJA

A hallgatók megismerkednek az RSA titkosítás matematikai alapjával; ennek érdekében meg kell tanulniuk a számelmélet ide vonatkozó fogalmait, tételeit.

2. A TANTÁRGY TARTALMA

TÉMAKÖRÖK

ELŐADÁS	1. Számelmélet elemei 2. Kriptográfia elemei
GYAKORLAT	nincs
LABOR- GYAKORLAT	nincs

RÉSZLETES TANTÁRGYI PROGRAM ÉS A KÖVETELMÉNYEK ÜTEMEZÉSE

ELŐADÁS

Konzu Itáció	Téma	Kötelező irodalom hivatkozás, oldalszám (-tól-ig)	Teljesítendő feladat (beadandó, zárthelyi, stb.)	Teljesítés ideje, határideje
1.	Kriptográfia alapjai Oszthatóság Számhalmazok és algoritmusok	[M] 1. lecke [M] 2. lecke [M] 3. lecke	Beadandó	Következő hét vége
2.	Indukció	[M] 4. lecke	Beadandó	Következő hét vége

	Számábrázolás Euklideszi algoritmus	[M] 5. lecke [M] 6. lecke		
3.	Rekurzív algoritmusok Diofantoszi egyenletek	[M] 7. lecke [M] 8. lecke	Beadandó	Következő hét vége
4.	Kongruenciák Kínai maradéktétel	[M] 9. lecke [M] 10. lecke	Beadandó	hét vége
5.	zh		zh	Tanóra idején

3. SZÁMONKÉRÉSI ÉS ÉRTÉKELÉSI RENDSZER

JELENLÉTI ÉS RÉSZVÉTELI KÖVETELMÉNYEK

A PTE TVSz 45.§ (2) és 9. számú melléklet 3§ szabályozása szerint a hallgató számára az adott tárgyból érdemjegy, illetve minősítés szerzése csak abban az esetben tagadható meg hiányzás miatt, ha levelező tagozaton egy tantárgy esetén a tantárgyi tematikában előírányzott foglalkozások több mint 50%-áról hiányzott.

A jelenlét ellenőrzésének módja

Teszt vagy jelenléti ív

SZÁMONKÉRÉSEK

Vizsgával záruló tantárgy

Félévközi ellenőrzések, teljesítményértékelések és részarányuk a vizsgára bocsájtás feltételének minősítésben

Típus	Értékelés	Részarány a vizsgára bocsájtás feltételének minősítésben
1. ZH	Kb 50 pont	80 %
2. Beadandók	Kb 100 pont	20 %

Az aláírás megszerzésének (vizsgára bocsájtás) feltétele

TVSZ szerinti mértékű jelenlét (nem pótolható), zárthelyi dolgozaton (pótolható, javítható) minimum 40%-os teljesítése, amelyről indokolt, előre jelzett, és utólagosan igazolt esetben hiányzás elfogadott, beadandók (rögzített elérhetőségük alatt többször is javíthatók) *határidőre* és *nullától különböző* eredménnyel történő teljesítése esetén legalább 40%-os évközi teljesítményt kell elérni a fenti táblázat szerinti súlyozás szerint.

Pótlási lehetőségek az aláírás megszerzéséhez (PTE TVSz 50§(2))

Amennyiben a hallgató a zárthelyi dolgozatát nem írta meg, vagy nem sikeres, azt a vizsgaidőszak első hetében, tervezetten az óra idejével egyező sávban pótolhatja, javíthatja egy alkalommal.

Vizsga típusa (írásbeli, szóbeli): írásbeli

A vizsga minimum 40 %-os teljesítés esetén sikeres.

Az érdemjegy kialakítása (TVSz 47§ (3))

- *Megajánlott jeggyel:* amennyiben a hallgató évközi teljesítménye legalább 60% (Neptunban el kell fogadnia!),
- *Vizsgajeggyel:* amennyiben a hallgató nem kaphat megajánlott jegyet, vagy nem fogadja azt el, ahol az értékelés **50** %-ban az évközi teljesítmény, **50** %-ban a vizsgán nyújtott teljesítmény alapján történik.

Az érdemjegy megállapítása az összesített teljesítmény alapján %-os bontásban

Érdemjegy	Teljesítmény %-ban kifejezve
jeles (5)	85 % ...
jó (4)	70 % ... 85 %
közepes (3)	55 % ... 70 %
elégséges (2)	40 % ... 55 %
elégtelen (1)	40 % alatt

Az egyes érdemjegyeknél megadott alsó határérték már az adott érdemjegyhez tartozik.

4. IRODALOM

KÖTELEZŐ IRODALOM ÉS ELÉRHETŐSÉGE

[M] Möbius rendszerben elérhető leckék

[MGy] Maróti György, *Előadások algoritmikus számelméletből*, Livermore, 2008, ISBN 978 963 06 3662 9

AJÁNLOTT IRODALOM ÉS ELÉRHETŐSÉGE

[ET] A kurzus Moodle és Teams csoportjaiban található anyagok