Óbudai Egyetem **Alba Regia Kar**	

Tantárgy neve és kódja: Alkalmazott matematika, ATXAM1HMNF Kreditérték: 4
Nappali 2024/2025. tanév **őszi** félév

Szakok, melyeken a tárgyat oktatják: Mérnökinformatikus MSc

Tantárgyfelelős oktató:	Dr. Borbély József	Oktatók:	Dr. Borbély József

Előtanulmányi feltételek: (kóddal)		

Heti óraszámok:	Előadás: 3	Tantermi gyak.: 1	Laborgyakorlat: 0	Konzultáció: 0
Számonkérés módja (s,v,f):	vizsga			

A tananyag

Oktatási cél: Az algebra, különösen a számelmélet eszközeinek gyakorlati alkalmazásait bemutatni

Tematika:

Témakör	**Óraszám**
Előadások/Gyakorlatok:	
Egész számok tulajdonságai. Maradékos osztás. A számelmélet alaptétele. A prímszámok száma. Kongruenciák és tulajdonságaik. Teljes és redukált maradékrendszerek. Kis Fermat-tétel. Az Euler-féle φ-függvény. Euler-Fermat-tétel. Az RSA-eljárás.	4
Néhány gyakorlati kérdés (hatékony hatványozás, multiplikatív inverz keresése). Euklideszi algoritmus. Példák. A modulo p test. Bezout tétele tetszőleges test feletti polinomokra. Fokszámtétel.	4
A rend fogalma. Adott rendű elemek száma a p elemű testben. Generálóelemek, primitív gyökök. Összegképlet az Euler-féle φ-függvényre. A Diffie-Hellmann-féle titkosítási eljárás. ElGamal. Titkosítás elliptikus görbék segítségével.	4
Számonkérés	4

Félévközi követelmények

AZ ELŐADÁSOK LÁTOGATÁSA KÖTELEZŐ!

A pótlás módja:	írásbeli zh a félév végén

Aláírás feltétele:	a vizsgazh sikeres teljesítése
A vizsga módja (írásbeli, szóbeli, teszt, stb): szóbeli	

Irodalom:	
Kötelező:	a moodle-ba feltöltött elektronikus tananyagok
Ajánlott:	Freud Róbert; Gyarmati Edit: Számelmélet Liptai Kálmán: Kriptográfia Szalay Mihály: Számelmélet