Budapesti Műszaki és Gazdaságtudományi Egyetem **Természettudományi Kar**	**TANTÁRGY ADATLAP**

Tantárgy kód	**BMETE91AM48**

Tantárgy azonosító adatok													
1.	A tárgy címe	**Az adatbiztonság matematikai alapjai**											
2.	A tárgy angol címe	**Mathematical Foundations of Data Security**											
3.	Heti óraszámok (ea + gy + lab) és a félévvégi követelmény típusa	**2**	+	**0**	+	**0**	**v**	Kredit	**2**				
4.	Ajánlott/kötelező előtanulmányi rend												
	vagy	Tantárgy kód 1		Rövid cím 1		Tantárgy kód 2		Rövid cím 2		Tantárgy kód 3		Rövid cím 3	
	4.1	**BMETE91AM38**		**Algebra1**									
	4.2												
	4.3												
5.	Kizáró tantárgyak												
6.	A tantárgy felelős tanszéke	**Algebra Tanszék**											
7.	A tantárgy felelős oktatója	**Dr. Wettl Ferenc**						beosztása	**egyetemi docens**				

Akkreditációs adatok				
8.	Akkreditációra benyújtás időpontja	**2015.02.16.**	Akkreditációs bizottsági döntés időpontja	**2016.04.18.**

Megjegyzések

Csak az űrlap fehéren hagyott mezőibe írjunk és a mezők között a **tabulátor** billentyűvel haladjunk! Ha egy kitöltött mezőből tabulátor billentyűvel lépünk ki, több más mező értéke automatikusan megváltozhat. Egy adott mezőre lépve, az állapotsorban megjelenő rövid, ill. az F1 gomb megnyomásakor kapható hosszabb leírás ad segítséget a kitöltéshez. A *tantárgy kódot* és a *tárgy rövid címét* a dékáni hivatal adja.

1-2. sorok: A *tárgy címének* (max. 85 karakter) célszerű legalább egy karakterben különböznie minden más, Neptunban regisztrált tárgy címétől.

3. sor: A *követelmény* előadás+gyakorlat+labor formátumú, *az utolsó mező* a félév végi számonkérés típusa (v,f,a vagy s, részletes információ F1). A *kredit* megadásánál ügyelni kell arra, hogy az alább részletezett, *a tantárgy elvégzéséhez átlagosan szükséges tanulmányi munka* mennyiségével összhangban legyen (összes óraszám = kredit*30 óra).

4. sor: Legfeljebb 3, már korábban hallgatott tárgy adható meg a 4.1 sorban. A 4.2 és 4.3 sorok *vagylagos* lehetőségek megadására szolgálnak, például abban az esetben, ha az egyik tárgynak korábban oktatott változatai is megfelelőek. **5. sor:** A *kizáró tantárgyaknál* azokat a tárgyakat kell felsorolni, amelyek tematikái a most akkreditálandó tárggyal 75% vagy annál nagyobb átfedést mutatnak.

6-7. sorok: A felelős tanszék és oktató hatáskörét, ill. kijelölésének feltételeit a *Képzési Kódex 2010* c. dokumentum 4.§-a tartalmazza.

Tematika				
9.	A tantárgy az alábbi témakörök ismeretére épít			
	Lineáris algebra, véges testek			
10.	A tantárgy szerepe a képzés céljának megvalósításában (szak, kötelező, kötelezően választható, szabadon választható)			
	TTK matematika (BSC) képzés Adattudományi sávjának kötelezően választható tárgya.			
11.	A tantárgy részletes tematikája			
	A tárgy célja a kódelmélet és a kriptográfia matematikai alapjainak megismerése. A tárgy a bizonyítható biztonság modern fogalmára épít. **Tematika: A kódelmélet és a kriptográfia információelméleti alapjai. Alapvető kommunikációs- és hibamodellek. A bináris szimmetrikus csatorna. Kódolás, dekódolás, Hamming-távolság. A (blokk) kódok alapvető paraméterei. Véges testek aritmetikája, polinomok véges testek felett. Lineáris kódok, generátormátrix, ellenőrző mátrix. Szindróma dekódolás. A Hamming-kód. Ciklikus kódok és ideálok. BCH-kódok. Reed-Solomon- és Justensen-kódok. Az MDS-korlát, optimális kódok. Golay-kódok, perfekt kódok. Korlátok a kódparaméterekre: Varshamov-Gilbert, Delsarte, gömbkitöltési. Reed-Muller-kódok. Kapcsolatuk a Boole-függvényekkel. Goppa-kódok, nem lineáris kódok, konvolúciós kódok.** **Klasszikus kripotgráfia elemei. A modern kriptográfia alapjai: a bonyolultságelmélet, számelmélet, a bizonyítható biztonság. Kiszámíthatóság – egyirányú és egyirányú kiskapufüggvények (diszkrét logaritmus, RSA-függvény, Rabin négyzetre emelés függvénye, prím faktorizációval való kapcsolatuk). Álvéletlen generátorok, álvéletlen függvények. Nemfeltáró bizonyítások, és létezésük NP-problémákra. Kódolás és hitelesítés módszerei (privát kulcsú rendszerek, szimmetrikus titkosítási sémák, nyilvános kulcsú rendszerek, kulcs csere (Diffie-Hellman). Kriptográfiai protokollok: két résztvevős protokollok (oblivious transzfer, bit rábízás,...), több résztvevős protokollok, titokmegosztás, elektronikus választás, digitális pénz.**			
12.	Követelmények, az osztályzat (aláírás) kialakításának módja			
	szorgalmi időszakban	**házi feladatok**	vizsga-időszakban	**szóbeli vizsga**
13.	Pótlási lehetőségek			
	TVSZ szerint			
14.	Konzultációs lehetőségek			
	TVSZ szerint			
15.	Jegyzet, tankönyv, felhasználható irodalom			
	Wettl Ferenc: Online jegyzet a tárgy honlapján			
	Hall: Notes on Coding theory, http://users.math.msu.edu/users/jhall/classes/codenotes/coding-notes.html			
	Katz, Lindell: Introduction to Modern Cryptography, Chapman & Hall, 2008			

16.	A tantárgy elvégzéséhez átlagosan szükséges tanulmányi munka mennyisége órákban (a teljes szemeszterre számítva)			
		16.1	Kontakt óra	**28**
		16.2	Félévközi felkészülés órákra	**8**
		16.3	Felkészülés zárthelyire	**0**
		16.4	Zárthelyik megírása	**0**
		16.5	Házi feladat elkészítése	**8**
		16.6	Kijelölt írásos tananyag elsajátítása (beszámoló)	**0**
		16.7	Egyéb elfoglaltság	**0**
		16.8	Vizsgafelkészülés	**16**
		16.9	**Összesen**	**60**
17.	Ellenőrző adat		**Kredit * 30**	**60**

A tantárgy tematikáját kidolgozta			
18.	Név	beosztás	Munkahely (tanszék, kutatóintézet stb.)
	Dr. Wettl Ferenc	**egyetemi docens**	**Algebra Tanszék**

A tanszékvezető		
19.	Neve	aláírása
	Dr. Nagy Attila	

Megjegyzések

16.1 sor: Értéke automatikusan kitöltődik az űrlap elektronikus változatában, a *„Követelmény”* címszónál megadott óraszám értékek alapján, az (előadás+gyakorlat+labor) * (14 oktatási hét) formula szerint. **16.4 sor:** Értéke 0, ha a zárthelyik íratása kontakt órákon történik, egyébként pedig a minimálisan szükséges számú zárthelyi megírásához felhasználandó idő (a pót zárthelyik nélkül). **16.7 sor:** Az *„Egyéb elfoglaltság”* szöveg helyére a tevékenység konkrét megnevezését kell írni.

17. sor: Az itt szereplő értéknek és a **16.9 sorban** automatikusan megjelenő tanulmányi óraszám összegnek hozzávetőlegesen meg kell egyeznie! Tájékoztatásul azt vegyük figyelembe, hogy a hallgatók által egy szemeszterben átlagosan 30 kreditnyi munkamennyiséget kell teljesíteni, azaz a szorgalmi és vizsgaidőszak során elvárt terhelés összesen kb. 900 munkaóra.