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

Tantárgy kód	**BMETE91AM18**

Tantárgy azonosító adatok													
1.	A tárgy címe	**Matematikai kriptográfia és kódelmélet**											
2.	A tárgy angol címe	**Mathematical Cryptography and Coding Theory**											
3.	A tárgy rövid címe	**MatKriptKódelm**	Követelmény	**3**	+	**0**	+	**0**	**v**	Kredit			**3**
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	BMETE91AM02	Algebra1										
	4.2												
	4.3												
5.	Kizáró tantárgyak												
6.	A tantárgy felelős tanszéke	**Algebra Tanszék**											
7.	A tantárgy felelős oktatója	**Dr. Rónyai Lajos**		beosztása	**egyetemi tanár**								

Akkreditációs adatok				
8.	Akkreditációra benyújtás időpontja	**2006.02.01.**	Akkreditációs bizottsági döntés időpontja	2006.09.20.

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* a dékáni hivatal adja.
1-2. sorok: A *tárgy címének* (max. 60 karakter) legalább egy karakterben különböznie kell minden más, Neptunban regisztrált tárgy címétől.
3. sor: A *rövid cím* jellegzetes, legfeljebb 16 karakter hosszúságú rövidítés. A *követelmény* előadás+gyakorlat+labor formátumú, *az utolsó mező* a félév végi számonkérés típusa (v,f,a vagy s, részletes információ az F1 gombra). 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 2001* c. dokumentum 9.1 fejezete tartalmazza.

Tematika				
7.	A tantárgy az alábbi témakörök ismeretére épít			
	Algebra, lineáris algebra, valószínűségszámítás alapjai, algoritmusokkal kapcsolatos alapismeretek.			
8.	A tantárgy célkitűzése, feladata a szakképzés céljának megvalósításában			
	TTK Matematika (BSc) képzés Aklkalmazott szakirányának kötelező tárgya.			
9.	A tantárgy részletes tematikája			
	Klasszikus kripotgráfia elemei. A modern kripotgráfia alapjai: a bonyolultságelmélet, számelmélet, valószínűségszámítás kriptográfiában felhasznált fogalmainak rövid áttekintése. Kiszámíthatóság - egyirányú függvények (diszkrét logaritmus, RSA-függvény, Rabin négyzetre emelés függvénye, prím faktorizációval való kapcsolatuk). Álvéletlen generátorok, álvéletelen függvények. Nemfeltáró bizonyítások, és létezésük NP-problémákra. Kódolás és hitelesítés módszerei (privát kulcsú rendszerek, szimmetrikus titkosítási sémák, nyilvános kulcsú rendszerek: RSA-, Rabin-, hátizsák rendszerek, digitális aláírás), kulcs csere (Diffie-Hellman). Kriptográfiai protokollok: két résztvevős protokollok (oblivious transzfer, bit rábízás, ..), több résztvevős protokollok, titokmegosztás, elektronikus választás, digitális pénz. Alapvető kommunikációs-és hibamodellek. A bináris szimmetrikus csatorna. Kódolás, dekódolás, Hamming-távolság. A (blokk)kódok alapvető paraméterei. Ismétlés: véges testek aritmetikájának rövid áttekintése, létezés, bázisok, primitív elemek, polinomok véges testek felett, számolás véges testekben. Lineáris kódok, generátormátrix, paritás-ellenőrző mátrix. Szindrómákon alapuló dekódolás. A Hamming-kód. Ciklikus kódok, generátor-polinom, ellenőrző polinom. Ciklikus kódok és ideálok. BCH-kódok. Korlát hibajavító képességükre. Berlekamp-Massey-algoritmus. 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.			
10.	Követelmények, az osztályzat (aláírás) kialakításának módja			
	szorgalmi időszakban	Órákon való részvétel.	vizsgaidőszakban	Szóbeli vizsga.
11.	Pótlási lehetőségek			
	A Tanulmányi és vizsgaszabályzatban előírtaknak megfelelően.			
12.	Konzultációs lehetőségek			
	Igény szerint a vizsgák előtt.			
13.	Jegyzet, tankönyv, felhasználható irodalom			
	Buttyán L. -- Vajda I. Kriptográfia és alkalmazásai. Typotex Kiadó, 2004.			
	F.J. MacWilliams --- N.J.A. Sloane. The Theory of Error-Correcting Codes.			

14.	A tantárgy elvégzéséhez átlagosan szükséges tanulmányi munka mennyisége órákban (a teljes szemeszterre számítva)			
		14.1	Kontakt óra	**42**
		14.2	Félévközi felkészülés órákra	**24**
		14.3	Felkészülés zárthelyire	**0**
		14.4	Zárthelyik megírása	**0**
		14.5	Házi feladat elkészítése	**0**
		14.6	Kijelölt írásos tananyag elsajátítása (beszámoló)	**0**
		14.7	Egyéb elfoglaltság	**0**
		14.8	Vizsgafelkészülés	**24**
		14.9	**Összesen**	**90**
15.	Ellenőrző adat		**Kredit * 30**	**90**

A tantárgy tematikáját kidolgozta			
16.	Név	beosztás	Munkahely (tanszék, kutatóintézet stb.)
	Dr. Rónyai Lajos	**egyetemi tanár**	**Algebra Tanszék**

A tanszékvezető		
17.	Neve	aláírása
	Dr. Rónyai Lajos	

Megjegyzések
14.1 sor: Értéke automatikusan kitöltődik az űrlap elektronikus változatában, a *„Követelmény”* címszónál megadott óraszám értékek alapján, az (előadás+gyakorlat+labor) * (14 oktatási hét) formula szerint. **14.4 sor:** Értéke 0, ha a zárthelyik íratása kontakt órákon történik, egyébként pedig a minimálisan szükséges számú zárthelyi megírásához felhasználandó idő (a pót zárthelyik nélkül). **14.7 sor:** Az *„Egyéb elfoglaltság”* szöveg helyére a tevékenység konkrét megnevezését kell írni.
15. sor: Az itt szereplő értéknek és a **14.9 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.