FAKULTETI I SHKENCAVE TË NATYRËS

DEPARTAMENTI I MATEMATIKËS

CIKLI II MASTER I SHKENCAVE NË MATEMATIKË PROGRAMI I LËNDËS: KRIPTOGRAFI DHE TEORIA E KODIMIT

Aktiviteti mësimor	**Leksione**	**Ushtrime**	**Laboratore**	**Praktike**	**Totale**
Detyrimi i studentit	Jo të detyrueshëm	75%			
Orë mësimore	30	30	0	0	60
Studim individual	90				
Gjuha e zhvillimit të mësimit	Shqip				
Tipologjia e lëndës / Lloji i lëndës/ Kodi i lëndës	E / E detyrueshme /				
Kodi i etikës	Referuar Kodit të etikës së UT, miratuar me Vendim Nr. 12, datë 18.04.2011				
Mënyra e shlyerjes	Provim				
Kredite	6				
Zhvillimi i Mësimit	Viti II, Semestri III, 15 javë: 2 orë leksione, 2 orë ushtrime/javë				
Zhvillimi i Provimit	Me shkrim e zë				
Vlerësimi, Nota, Provim	Pjesëmarrja dhe aktivizimi	6%			
	Kontrolle të ndërmjetme				
	Detyra kursi				
	Laboratore				
	Praktika në terren				
	Provimit final	94%			
	Gjithsej	**100%**			

Konceptet themelore	Lënda përbëhet nga dy pjesë kryesore: e para është një hyrje në teorinë e kodeve gabim-ndreqës dhe në kriptografi. Pjesa e parë hapet zakonisht me disa plotësime të nevojshme të algjebrës, që kanë synim të konsolidojnë kulturën algjebrike me strukturën e fushave të fundme. Pjesa kryesore e saj përbëhet nga një paraqitje koncize e teorisë së kodeve linearë, me theks te kodet Hamming dhe te kodet ciklikë. Pjesa e fundit paraqet disa nga konceptet dhe teknikat e kriptografisë si shkencë, në këndvështrimin e zbatimeve të njohurive matematike.
Objektivat	Për pjesën e parë, një nga objektivat kryesore është pajisja e studentëve me parimet dhe njohuritë bazë të teorisë së kodeve gabim-ndreqës. Një synim tjetër është njohja me disa nga grupet kryesore të kodeve, karakteristikat e parametrat e tyre, si dhe vetitë e tyre algjebrike. Njohja me disa kode konkretë e më të përdorshëm është gjykuar si mjet jo vetëm tërheqës por dhe formues për studentët. Ndërsa, për pjesën e dytë, objektiv kryesor është njohja e studentëve me problemet kryesore që zgjidh kriptografia, si: vërtetësia, autenticiteti, ndërtimi i çelësave, ndarja e sekretit, etj., me anë të disa kriptosistemeve realizues të tyre, duke paraqitur problemet përkatës. Një nga objektivat kryesorë është dhe njohja me disa standarde kriptografikë më të përdorshëm.
Njohuritë paraprake	Kurs fillestar algjebre abstrakte dhe lineare, kuptime bazë të teorisë së numrave, kurs fillestar analize reale, kuptime bazë të probabilitetit.