

Studijski program		Vrsta studija (ciklus)	Treći ciklus studija – doktorski studij		
		Naziv studijskog programa	Doktorski studij matematičkih i kompjuterskih nauka		
PREDMET					
Naziv predmeta		Odabrane oblasti kriptologije			
Šifra predmeta	Semestar	Status predmeta	ECTS bodovi	Kontakt sati	
AMAT 671	II	Izborni	10	30	
Ciljevi i ishodi predmeta	Osnovni cilj predmeta je da studenti steknu znanje i vještine u odabranim naprednim oblastima kriptologije.				
	Na kraju položenog ispita student treba da ima duboko razumijevanje teorije iz izučavane oblasti, te da posjeduje vještinu primjene tog znanja u različitim situacijama u oblasti kibernetičke sigurnosti. Također student treba da stekne sposobnost samostalnog istraživanja iz kriptografije i da stekne sposobnost donošenja naučnih zaključaka.				
Sadržaj predmeta					
• Enkriptički algoritmi sa simetričnim ključem • Matematičke strukture u tekućim i bločnim šiframa • Kriptografija javnih ključeva-Hash funkcije i MAC algoritmi • Autentifikacijski i identifikacijski algoritmi i protokoli • Kriptografski algoritmi u praksi i standardi • Napredna kriptanaliza					
LITERATURA		PROVJERA ZNANJA I OCJENJIVANJE			
[1] Daglas R. Stinson “ Cryptography: Theory and Practice” [2] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone“Handbook of applied cryptography”			Kriterij	Bodovi	Uslov
		1.	Zadaće	30	15
		2.	Projekat	30	15
		3	Završni ispit	40	25
		U k u p n o		100	55