Studijski program	Vrste studija (ciklus)		III ciklus	
	Naziv studijskog programa		Matematičke nauke u jugoistočnoj Evropi	
PREDMET				
Naziv predmeta	**Izabrana poglavlja iz kriptografije**			
Šifra predmeta	Semestar	Status predmeta	ECTS	Kontakt sati
AMAT 670	II	izborni	10	30
Cilj predmeta	Cilj predmeta je dati solidnu osnovu studentima iz moderne kriptografije sa aspektom na dizajniranje, kriptoanalizu i implementaciju kriptografskih algoritama i protokola			

SADRŽAJ PREDMETA

- Enkriptički algoritmi sa simetričnim ključem
- Matematičke strukture u tekućim i bločnim šiframa
- Kriptografija javnih ključeva-Hash funkcije i MAC algoritmi
- Autentifikacijski i identifikacijskialgoritmi i protokoli
- Kriptografski algoritmi u praksi i standardi

LITERATURA

[1] Daglas R. Stinson " Cryptography: Theory and Practice"

[2] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone"Handbook of applied cryptography"

OCJENJIVANJE

Kriterij		Poeni	Uslov
1.	Zadaće	20	10
2.	Projekt	20	10
3.	Završni ispit	60	35
Ukupno		100	55