Studijski program	Vrsta studija (ciklus)	Treći ciklus
	Naziv studijskog programa	Doktorski studij matematičkih nauka u jugoistočnoj Evropi

PREDMET

Naziv predmeta	**Izabrana poglavlja iz kriptografije**

Šifra predmeta	Semestar	Status predmeta	ECTS bodovi	Kontakt sati
	II		10	30

Nastavnici i saradnici	Nosilac predmeta	Prof. dr. Enes Pasalic
	Učesnici u nastavi	
Ciljevi 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 identifikacijski algoritmi 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"

PROVJERA ZNANJA I OCJENJIVANJE

	Kriterij	Poeni	Uslov
1.	Zadaće	20	10
2.	Projekat	15	15
3	Završni ispit	65	30
	U k u p n o	100	55