Studijski program	Vrsta studija (ciklus)	II ciklus
	Naziv studijskog programa	Teorijska kompjuterska nauka

PREDMET				
Naziv predmeta	**Odabrana poglavlja kriptologije**			
Šifra predmeta	Semestar	Status predmeta	ECTS	Kontakt sati (P+AV+LV)
CS 530	II	Izborni	7	3+2+0
Nosilac programa				
Cilj predmeta	Cilj predmeta je upoznati studente sa funkcijama nad konačnim poljima, Boolevim funkcijama i njihovoj upotrebi u kriptologiji.			
Ishod učenja	Sticanje sposobnosti upotrebe naprednih matematičkih alata u kriptologiji koji su neophodni za pračenje najnovijih naučnih doprinosa u ovoj oblasti.			

Sadržaj predmeta

- Boolevove funkcije.
- Pristup u vektorskim prostorima.
- Pristup u konačnim poljima.
- Normalna baza u konačnim poljima.
- Permutacioni polinomi.
- Bent funkcije, Walshov spektrum.
- Otporne funkcije
- Algebarski imune funkcije.
- Simetrične funkcije.

LITERATURA

[1] Claude Carlet, Boolean functions in Cryptography and Error correcting Codes, http://www.math.univ-paris13.fr/~carlet/chap-fcts-Bool-corr.pdf

[2] Thomas E. Cusick, Pantelimon Stănică, Cryptographic Boolean functions and Applications, Anademic Press Elsivier, 2009

[3] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley, Reading, Massachussetts (1983)

OPTEREĆENJE STUDENTA (sati u semestru)							
Predavanje	45	Vježbe	30	Samostalan rad	100	U k u p n o	175

PROVJERA ZNANJA I OCJENJIVANJA			**NAPOMENA**
Kriterij	Maksimalan broj bodova	Bodovi za prolaz	
Testovi tokom kursa	50	25	
Završni ispit	50	25	
U k u p n o	100	55	