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

PREDMET				
Naziv predmeta	**Algoritamska teorija brojeva**			
Šifra predmeta	Semestar	Status predmeta	ECTS	Kontakt sati (P+AV+LV)
CS 525	III	Izborni	7	3+2+0
Nosilac programa				
Cilj predmeta	Cilj predmeta je da se studenti upoznaju sa nekim temama iz algoritamske teorije brojeva, s posebnim akcentom na one teme koje su relevantne za primjene u kriptografiji.			
Ishod učenja	Nakon uspješnog završetka predmeta očekuje se da će student: - Razumjeti osnovne pojmove i neke tehnike koje se primjenjuju u algoritmaskoj teoriji brojeva - Razumjeti i biti u mogućnosti implementirati i koristiti neke algoritme za određivanje prostih brojeva, faktorizaciju borjeva i diskretne logaritme			

Sadržaj predmeta

- Teorija brojeva i kompleksnost.
- Euklidov algoritam za NZD; Analiza najkompleksnijih slučajeva;
- Binarni NZD algoritam; Neprekidni razlomci;
- Računanje Legendreovog i Jakobievog simbola;
- Rješavanje jednačina nad konačnim poljima; Korijeni; Henselova lema;
- Algoritmi za određivanje prostih brojeva; Testovi prostosti za brojeve specijalnog oblika;
- Pseudoprosti i Carmichaelovi brojevi; Vjerovatnosni testovi prostosti;
- Testovi prostosti pomoću sita; Konstrukcija "slučajnih" prostih brojeva;
- Algoritmi za faktorizaciju brojeva;
- Algoritmi za izračunavanje diskretnog logaritma.

LITERATURA

[1] S. Y. Yan: Number theory for computing, Springer, 2002.
[2] W. Stein: Elementary Number Theory: Primes, Congruences, and Secrets, a computational approach, Springer, 2009.
[3] P.J. Giblin: Primes and programming, Cambridge University Press, 1993.
[4] E. Bach, J, Shallit: Algorithmic number theory, Volume I: Efficient Algorithms, MIT Press, 1996.

OPTEREĆENJE STUDENTA (sati u semestru)

Predavanje	45	Vježbe	30	Samostalan rad	100	Ukupno	175

PROVJERA ZNANJA I OCJENJIVANJA			**NAPOMENA**
Kriterij	Maksimalan broj bodova	Bodovi za prolaz	
Testovi tokom kursa	30	15	
Projekat	30	15	
Završni ispit	40	20	
Ukupno	100	55	