

Prirodno-matematički fakultet / MATEMATIKA I RAČUNARSKE NAUKE / KRIPTOGRAFIJA

Naziv predmeta:	KRIPTOGRAFIJA			
Šifra predmeta	Status predmeta	Semestar	Broj ECTS kredita	Fond časova (P+V+L)
12082	Obavezan	1	5	3+1+0
Studijski programi za koje se organizuje	MATEMATIKA I RAČUNARSKE NAUKE			
Uslovljenost drugim predmetima	Polaganje ispita nije uslovljeno polaganjem drugih ispita.			
Ciljevi izučavanja predmeta	Cilj kursa je upoznavanje studenata sa osnovama simetrične i asimetrične kriptografije			
Ishodi učenja	Nakon što student položi ovaj ispit, biće u mogućnosti da: 1. Razumije i primjenjuje definicije i tvrđenja Teorije brojeva 2. Razumije osnovna tvrđenja i algoritme klasične kriptografije 3. Razumije pojam asimetrične kriptografije i javnog i tajnog ključa 4. Razumije i primjenjuje algoritme asimetrične kriptografije 5. Razumije pojam elektronskog potpisa, i implementira digitalni potpis			
Ime i prezime nastavnika i saradnika	prof. dr Vladimir Božović			
Metod nastave i savladanja gradiva	Predavanja, vježbe, konsultacije, projektni zadaci			
Plan i program rada				
Pripremne nedjelje	Priprema i upis semestra			
I nedjelja, pred.	Uvod u kriptografiju. Istorija kriptografije. Jednostavni supstitucionni sistemi. Uvod u kriptanalizu.			
I nedjelja, vježbe	Uvod u kriptografiju. Istorija kriptografije. Jednostavni supstitucionni sistemi. Uvod u kriptanalizu.			
II nedjelja, pred.	Djeljivost. Euklidov algoritam.			
II nedjelja, vježbe	Djeljivost. Euklidov algoritam.			
III nedjelja, pred.	Prosti brojevi i faktorizacija. Modularna aritmetika.			
III nedjelja, vježbe	Prosti brojevi i faktorizacija. Modularna aritmetika.			
IV nedjelja, pred.	Kineska teorema o ostacima. Diofantove jednačine.			
IV nedjelja, vježbe	Kineska teorema o ostacima. Diofantove jednačine.			
V nedjelja, pred.	Osnovne algebarske strukture. Grupa, prsten, polje. Sistem ostataka kao prsten po modulu.			
V nedjelja, vježbe	Osnovne algebarske strukture. Grupa, prsten, polje. Sistem ostataka kao prsten po modulu.			
VI nedjelja, pred.	Aritmetičke funkcije. Fermaova i Ojlerova teorema.			
VI nedjelja, vježbe	Aritmetičke funkcije. Fermaova i Ojlerova teorema.			
VII nedjelja, pred.	Simetrična kriptografija. Primjeri simetričnih kriptosistema.			
VII nedjelja, vježbe	Simetrična kriptografija. Primjeri simetričnih kriptosistema.			
VIII nedjelja, pred.	Asimetrična kriptografija. Problem diskretnog logaritma u konačnom polju. Difi-Helman algoritam.			
VIII nedjelja, vježbe	Asimetrična kriptografija. Problem diskretnog logaritma u konačnom polju. Difi-Helman algoritam.			
IX nedjelja, pred.	Prvi kolokvijum. ElGamal algoritam. Kompleksnost problema diskretnog logaritma.			
IX nedjelja, vježbe	Prvi kolokvijum. ElGamal algoritam. Kompleksnost problema diskretnog logaritma.			
X nedjelja, pred.	Baby step-Giant step algoritam za traženje diskretnog logaritma. Kineska teorema o ostacima. Skica Polig-Helman algoritma.			
X nedjelja, vježbe	Baby step-Giant step algoritam za traženje diskretnog logaritma. Kineska teorema o ostacima. Skica Polig-Helman algoritma.			
XI nedjelja, pred.	Faktorizacija u kriptografiji. Ojlerova formula i korijeni modulo pq. Uvod u RSA algoritam.			
XI nedjelja, vježbe	Faktorizacija u kriptografiji. Ojlerova formula i korijeni modulo pq. Uvod u RSA algoritam.			
XII nedjelja, pred.	RSA implementacija. Sigurnosna pitanja RSA algoritma. Uticaj RSA algoritma na razvoj kriptografije.			
XII nedjelja, vježbe	RSA implementacija. Sigurnosna pitanja RSA algoritma. Uticaj RSA algoritma na razvoj kriptografije.			
XIII nedjelja, pred.	Testovi primalnosti. Polardovi algoritmi za faktorizaciju. Faktorizacija pomoću razlike kvadrata.			
XIII nedjelja, vježbe	Testovi primalnosti. Polardovi algoritmi za faktorizaciju. Faktorizacija pomoću razlike kvadrata.			

XIV nedjelja, pred.	Abelova grupa eliptične krive. Eliptična kriva nad konačnim poljem. Diskretni logaritmi na eliptičnoj krivoj.					
XIV nedjelja, vježbe	Abelova grupa eliptične krive. Eliptična kriva nad konačnim poljem. Diskretni logaritmi na eliptičnoj krivoj.					
XV nedjelja, pred.	Pojam i implementacija digitalnog potpisa. RSA digitalni potpis.					
XV nedjelja, vježbe	Pojam i implementacija digitalnog potpisa. RSA digitalni potpis.					
Opterećenje studenta						
Nedjeljno			U toku semestra			
5 kredita x 40/30=6 sati i 40 minuta 3 sat(a) teorijskog predavanja 0 sat(a) praktičnog predavanja 1 vježbi 2 sat(a) i 40 minuta samostalnog rada, uključujući i konsultacije			Nastava i završni ispit: 6 sati i 40 minuta x 16 =106 sati i 40 minuta Neophodna priprema prije početka semestra (administracija, upis, ovjera): 6 sati i 40 minuta x 2 =13 sati i 20 minuta Ukupno opterećenje za predmet: 5 x 30=150 sati Dopunski rad za pripremu ispita u popravnom ispitnom roku, uključujući i polaganje popravnog ispita od 0 do 30 sati (preostalo vrijeme od prve dvije stavke do ukupnog opterećenja za predmet) 30 sati i 0 minuta Struktura opterećenja: 106 sati i 40 minuta (nastava), 13 sati i 20 minuta (priprema), 30 sati i 0 minuta (dopunski rad)			
Obaveze studenta u toku nastave			Studenti su obavezni da pohađaju nastavu, rade i predaju sve projektne zadatke i rade kolokvijum i završni ispit.			
Konsultacije			U dogovoru sa studentima.			
Literatura			1. An Introduction to Mathematical Cryptography, Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, 2008, ISBN: 978-0-387-77993-5. 2. A Course in Number Theory and Cryptography, Neal Koblitz, 1994, ISBN: 0-387-94293-9.			
Oblici provjere znanja i ocjenjivanje			Kolokvijum - 30 poena Projektni zadatak - 30 poena Završni ispit - 30 poena Prisustvo nastavi - 10 poena			
Posebne naznake za predmet						
Napomena						
Ocjena:	F	E	D	C	B	A
Broj poena	manje od 50 poena	više ili jednako 50 poena i manje od 60 poena	više ili jednako 60 poena i manje od 70 poena	više ili jednako 70 poena i manje od 80 poena	više ili jednako 80 poena i manje od 90 poena	više ili jednako 90 poena