

**Prirodno-matematički fakultet / Računarstvo i informacione tehnologije (2017) /**  
**KRIPTOGRAFIJA**

<b>Naziv predmeta:</b>	KRIPTOGRAFIJA			
<b>Šifra predmeta</b>	<b>Status predmeta</b>	<b>Semestar</b>	<b>Broj ECTS kredita</b>	<b>Fond časova (P+V+L)</b>
3444	Obavezan	6	4	2+0+0
<b>Studijski programi za koje se organizuje</b>	Računarstvo i informacione tehnologije (2017)			
<b>Uslovljenost drugim predmetima</b>	Polaganje ispita nije uslovljeno polaganjem drugih ispita.			
<b>Ciljevi izučavanja predmeta</b>	Cilj kursa je upoznavanje studenata sa osnovama simetrične i asimetrične kriptografije			
<b>Ishodi učenja</b>	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			
<b>Ime i prezime nastavnika i saradnika</b>	prof. dr Vladimir Božović			
<b>Metod nastave i savladanja gradiva</b>	Predavanja, vježbe, konsultacije, projektni zadaci			
<b>Plan i program rada</b>				
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 logaritam na eliptičnoj krivoj.					
XIV nedjelja, vježbe	Abelova grupa eliptične krive. Eliptična kriva nad konačnim poljem. Diskretni logaritam 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.					
<b>Opterećenje studenta</b>						
<b>Nedjeljno</b>	<b>U toku semestra</b>					
<b>4 kredita x 40/30=5 sati i 20 minuta</b> 2 sat(a) teorijskog predavanja 0 sat(a) praktičnog predavanja 0 vježbi <b>3 sat(a) i 20 minuta</b> samostalnog rada, uključujući i konsultacije	Nastava i završni ispit: <b>5 sati i 20 minuta x 16 =85 sati i 20 minuta</b> Neophodna priprema prije početka semestra (administracija, upis, ovjera): <b>5 sati i 20 minuta x 2 =10 sati i 40 minuta</b> Ukupno opterećenje za predmet: <b>4 x 30=120 sati</b> 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) <b>24 sati i 0 minuta</b> Struktura opterećenja: <b>85 sati i 20 minuta (nastava), 10 sati i 40 minuta (priprema), 24 sati i 0 minuta (dopunski rad)</b>					
<b>Obaveze studenta u toku nastave</b>	Studenti su obavezni da pohađaju nastavu, rade i predaju sve projektne zadatke i rade kolokvijum i završni ispit.					
<b>Konsultacije</b>	U dogovoru sa studentima.					
<b>Literatura</b>	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.					
<b>Oblici provjere znanja i ocjenjivanje</b>	Kolokvijum - 30 poena Projektni zadatak - 30 poena Završni ispit - 30 poena Prisustvo nastavi - 10 poena					
<b>Posebne naznake za predmet</b>						
<b>Napomena</b>						
<b>Ocjena:</b>	F	E	D	C	B	A
<b>Broj poena</b>	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