Prirodno-matematički fakultet / MATEMATIKA I RAČUNARSKE NAUKE / KRIPTOGRAFIJA

Uslovljenost drugim predmetima	Polaganje ispita nije uslovljeno polaganjem drugih ispita.
Ciljevi izučavanja predmeta	Cilj kursa je upoznavanje studenata sa osnovama simetrične i asimetrične kriptografije
Ime i prezime nastavnika i saradnika	prof. dr Vladimir Božović
Metod nastave i savladanja gradiva	Predavanja, vježbe, konsultacije, projektni zadaci
I nedjelja, pred.	Uvod u kriptografiju. Istorija kriptografije. Jednostavni supstitucioni sistemi. Uvod u kriptoanalizu.
I nedjelja, vježbe	Uvod u kriptografiju. Istorija kriptografije. Jednostavni supstitucioni sistemi. Uvod u kriptoanalizu.
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 kripto-sistema.
VII nedjelja, vježbe	Simetrična kriptografija. Primjeri simetričnih kripto-sistema.
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.
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.
Opterećenje studenta u casovima	

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	
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