Naziv predmeta	*KRIPTOGRAFIJA*					
Skraćeni naziv	**Status**	**Semestar**	**ECTS**	**Fond časova (P+A+L)**		
RN-KRI	izborni	7.	**8**	2	3	
Šifra predmeta	RN-KRI					

Vrsta i nivo studija, studijski program: Akademske studije prvog ciklusa studija; Studijski program Računarske nauke.

Uslovljenost drugim predmetima: Nema uslova prijavljivanja i slušanja predmeta.

Ciljevi izučavanja predmeta: Sticanje opštih znanja iz kriptografije. Upoznavanje studenata sa kriptografskim algoritmima i tehnikama. Upoznavanje studenata sa osnovama zaštite podataka i aplikacija, zaštite računarskih mreža, operativnih sistema i baza podataka. Studenti upoznaju razne klase kriptosistema, kao i tehnike za formiranje digitalnog potpisa i razmjenu ključa.

Ime i prezime nastavnika i saradnika:

Metod nastave i savladavanje gradiva: Nastava se izvodi u obliku predavanja i vježbi na računaru. Učenje, testovi, domaći radovi, seminarski rad i konsultacije.

Sadržaj predmeta po sedmicama:

1.	Uvod u kriptografiju.
2.	Gradivi elementi protokola.
3.	Osnovni protokoli.
4.	Protokoli srednje složenosti.
5.	Napredni protokoli.
6.	Ezoterični protokoli.
7.	Dužina ključa i upravljanje ključevima.
8.	Tipovi i režimi algoritama i njihova primjena.
9.	Prvi test
10.	Matematičke osnove kriptografskih algoritama.
11.	Data encryprion standard (DES).
12.	Ostale blokovske šifre.
13.	Generatori pseudoslučajnih sekvenci i šifre toka.
14.	Jednosmjerne heš funkcije.
15.	Algoritmi s javnim ključem i algoritmi za digitalno potpisivanje s javnim ključem.
16.	Primjena i realizacija kriptografskih algoritama. Politika kriptografije.
17.	Drugi test

Opterećenje studenta po predmetu:

Nedjeljno:	**U semestru:**
Kreditni koeficijent	**Ukupno opterećenje za predmet:**
8/30=0,26	8 kredita x 30 sati/kreditu=**240 sati**
Nedjeljno opterećenje:	Aktivna nastava: 5 x15=75 **sati** predavanja i vježbi,
= 0,26 x 40 sati	**Kontinualna provjera znanja: 10 sati**
= 10 sati	**Završna provjera znanja: 5 sati**
	Samostalan rad: učenje, seminarski, konsultacije **120 sati**

Obaveze studenta: Studenti su obavezni da: pohađaju nastavu, urade domaće radove, seminarski rad i testove, da rade kolokvije i posjećuju konsultacije.

Literatura: Stinson, D, (1995). Cryptography: Theory and Practice, CRC Press.; Menezes, A., Van Oorshot, P., Vanstone, S. (1996). Handbook of Applied Cryptography, CRC Pres; Schneier, B, (2007). Primenjena kriptografija, Mikro knjiga, Beograd.

Oblici provjere znanja i ocjenjivanje: Redovno prisustvo nastavi donosi do 10 bodova, kolokvijumi, testovi domaći radovi i seminarski rad donose do 40 bodova, završni ispit donosi do 50 bodova. Prolazna ocjena se dobije ako se sakupi 55 ili više bodova.

Posebna napomena za predmet: Nema