	Naziv predmeta:	Zaštita podataka i sistema		
Šifra predmeta	**Status predmeta**	**Semestar**	**Broj ECTS kredita**	**Fond časova**
	Obavezni	**V**	**6**	**3P+0V+1L**

Ime i prezime nastavnika i saradnika:
Prof. dr Vladan Vujičić - nastavnik, Doc. dr Zoran Miljanić, dr Martin Ćalasan - saradnici

Plan rada:

I nedjelja (26.09.2017.)	Uvodno predavanje. Osnovni pojmovi u kriptografiji. Supstitucijska šifra;
II nedjelja (03.10.2017.)	Klasične šifre i sprave za šifrovanje;
III nedjelja (10.10.2017.)	**Prvi ciklus laboratorijskih vježbi;**
IV nedjelja (17.10.2017.)	DES kriptosistem: opis algoritma i svojstva; Načini rada simetričnih kriptosistema;
V nedjelja (24.10.2017.)	Pregled ostalih simetričnih kriptosistema; AES kriptosistem: opis algoritma i svojstva;
VI nedjelja (31.10.2017.)	**Drugi ciklus lab. vježbi;**
VII nedjelja (**07.11.2017.**)	*I kolokvijum;*
VIII nedjelja (14.11.2017.)	Osnovni principi kriptosistema sa javnim ključem. Diffie Helman-ov protokol; RSA kriptosistem;
IX nedjelja (21.11.2017.)	Pregled kriptosistema sa javnim ključem;Funkcije za sažimanje, digitalni potpis i digitalni sertifikat;
X nedjelja (28.11.2017.)	Zlonamjerni softver, upadi sa Interneta i elementi zaštite; (Sigurnosni protokoli;)
XI nedjelja (05.12.2017.)	**Treći ciklus lab. vježbi;**
XII nedjelja (12.12.2017.)	(Sigurnosni protokoli;), Četvrti-popravni ciklus lab. vježbi;
XIII nedjelja (**19.12.2017.**)	*II kolokvijum;*
XIV nedjelja (26.12.2017.)	Popravni kolokvijum; Prezentacija seminarskih radova*;
XV nedjelja (02.01.2018.)	-
	Završni i popravni ispit - tokom januara

Literatura: Behrouz A. Forouzan: Introduction to cryptography and network security, McGraw-Hill, 2008.
Skripta (fotokopirnica, www.zastita.ac.me)
Uputsvo za laboratorijske vježbe i dopunska literatura (elektronska oglasna tabla)

Oblici provjere znanja i ocjenjivanje:

- 3 testa iz laboratorijskih vježbi po 2 poena (ukupno 6 poena)
- Dva kolokvijuma po 22 poena (ukupno 44 poena)
- Završni ispit 50 poena

Prelazna ocjena se dobija ako se kumulativno sakupi najmanje 51 poen

Napomena:

* U dogovoru sa nastavnikom studenti mogu pristupiti izradi seminarskog rada. Prijavljivanje se vrši najkasnije do kraja VII nedjelje nastave. U slučaju uspješne odbrane seminarskog rada, uz uslov da je prethodno na kolokvijumima kumulativno sakupio minimum 22 poena, student se oslobađa od izlaska na završni ispit.