	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 Martin Ćalasan i Mihailo Micev, spec. sci - saradnici

Plan rada:

I nedjelja (24.09.2019.)	Uvodno predavanje. Osnovni pojmovi u kriptografiji. Supstitucijska šifra;
II nedjelja (01.10.2019.)	Klasične šifre i sprave za šifrovanje;
III nedjelja (08.10.2019.)	**Prvi ciklus laboratorijskih vježbi;**
IV nedjelja (15.10.2019.)	DES kriptosistem: opis algoritma i svojstva; Načini rada simetričnih kriptosistema;
V nedjelja (22.10.2019.)	Pregled ostalih simetričnih kriptosistema; AES kriptosistem: opis algoritma i svojstva;
VI nedjelja (29.10.2019.)	**Drugi ciklus lab. vježbi;**
VII nedjelja (**05.11.2019.**)	*I kolokvijum;*
VIII nedjelja (12.11.2019.)	Osnovni principi kriptosistema sa javnim ključem. Diffie Helman-ov protokol; RSA kriptosistem;
IX nedjelja (19.11.2019.)	Pregled kriptosistema sa javnim ključem;Funkcije za sažimanje, digitalni potpis i digitalni sertifikat;
X nedjelja (26.11.2019.)	Zlonamjerni softver, upadi sa Interneta i elementi zaštite; (Sigurnosni protokoli;)
XI nedjelja (03.12.2019.)	**Treći ciklus lab. vježbi;**
XII nedjelja (10.12.2019.)	(Sigurnosni protokoli;), Četvrti-popravni ciklus lab. vježbi;
XIII nedjelja (**17.12.2019.**)	*II kolokvijum;*
XIV nedjelja (24.12.2019.)	Popravni kolokvijum;
XV nedjelja (31.12.2019.)	Prezentacija seminarskih radova*;
	Završni i popravni ispit - tokom januara

Literatura:

- Skripta (fotokopirnica, www.zastita.ac.me), materijal i bilješke sa predavanja
- Uputsvo za laboratorijske vježbe

- Behrouz A. Forouzan: *Introduction to cryptography and network security*, McGraw-Hill, 2008.
- William Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed., Prentice Hall, 2017.

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 50 poena

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.