Univerzitet „UKSHIN HOTI“ PRIZREN
Fakultet kompjuterskih nauka

NASTAVNI PLAN-PROGRAM – SYLLABUS							
Nivo studija		BACHELOR	***Departament***	TIT BOS	***Akademska god.***	2017/2018	
PREDMET		**AUTHENTICATION AND CRYPTOGRAPHY AUTENTIFIKACIJA I KRIPTOGRAFIJA**					
Godina	II	***Status predmeta***	OBAVEZNI	***Kod***		***ECTS kred.***	6
Semestar	IV						
Nastavne nedjelje		15	***Nastavni časovi***		Predavanja	Vježbe	
					2	2	
Metodologija nastave		Predavanja, vježbe, seminarski radovi, konsultacije, testovi, e-learning, zadaci					
Konsultacije		Jedan sat prije i jedan sat posle predavanja					
Predavač		**Prof. Asoc. dr Muzafer Saračević**		e-mail	**muzafer.saracevic@uninp.edu.rs**		
				tel.	**+381648891544**		
Asistent		**Msc. Haris Bibuljica**		e-mail			
				tel.			

Cilj studija i sadržaj predmeta	**Dobit studenta**
Na ovom predmetu studenti stiču neophodna znanja iz osnova kriptologije uz primenu matematičkog aparata koji je potreban za analizu i sintezu savremenih šifarskih sistema. Savladavaju se osnovni servisi zaštite informacija: tajnost, integritet, autentifikacija i neporecivost. Detaljno se razmatraju svojstva simetričnih i asimetričnih šifarskih sistema.	Studenti će biti osposobljeni da samostalno procenjuju kvalitet zadatog šifarskog sistema i razumeju njegovo mesto i ulogu u savremenom integrisanom računarskom okruženju.

Metodologija za realizaciju nastavnih tema:

- Studentski slučaj ili zadatak (tokom vježbi) povezano sa predavanom temom
- Obnavljanje predvidjene teme od odredjene grupe studenata, analiza i diskusija
- Prezentacije, forumi, konceptualne mape, wiki, google dokumenti, interaktivni posteri

Uslovi za realizaciju nastavne teme:

- Sala opremljena sa kompjuterom i projektorom

Način vrednovanja studenta (u %) :

- Redovnost na predavanjima 0-5%
- Aktivnost 0-5%
- Seminarski rad 0-10%
- Test I 0-10 %
- Test II 0-10%
- Završni ispit 0- 50%
- Učestvovanje u vježbama 0 - 5%
- Grupni rad na zadacima i slučajevima studija 0- 5%

Vrednovanje u %	**Konačna ocjena**
91-100	10 (deset)
81-90	9 (devet)
71-80	8 (osam)
61-70	7 (sedam)
51-60	6 (šest)
0-50	5 (pet)

Obaveza studenta:

Predavanja	**Vježbe**
• Redovnost na predavanjima • Aktivno učestvovanje u diskusijama tokom predavanja • Seminarski rad • Učestvovanje na testu • Završni ispit	• Aktivno učestvovanje na vježbama • Grupni rad u slučajevima studija i zadacima • Učestvovanje u diskusijama na temu slučajeva studija

Dužnosti studenta za predmet

Aktivnost	**Časovi**	**Dana/Nedjelja**	**Ukupno**
Predavanja	**2**	**15**	**30**
Vježbe	**2**	**15**	**30**

Praktičan rad	**2**	**05**	**10**
Kontakti sa predavačima/konsultacije	**1**	**15**	**15**
Vježbe na terenu	**-**	**-**	**-**
Kolokviumi, seminari	**2**	**10**	**20**
Domaći zadaci	**-**	**-**	**-**
Samostalni rad	**2**	**15**	**30**
Završne pripreme za ispit	**2**	**15**	**30**
Protekli period , uspjeh (testovi, kviz, finalni ispit, itd.)	**1**	**05**	**05**
Projekti, prezentacije, itd.	**5**	**2**	**10**
Napomena: 1 ECTS kred. = 30 čas. angažovanja, npr. ako predm. ima 6 ECTS kred. student treba biti angažovan tokom semestra 180 čas.		**Total:**	**180**

Nedja:	**Predavanja**		**Vježbe**	
	Tema	**Čas**		**Čas.**
1.	**Tema: Osnovni pojmovi u oblasti kriptologije i autentifikacija** Literatura: M.Veinović, S.Adamović, Kriptologija 1, Univerzitet Singidunum, 2013	2	Vezbe – Uvod u Cryptool alat za kriptografiju Literatura: S. Adamović, Zaštita informacionih sistema, Univerzitet Singidunum, 2015.	2
2.	**Tema: Kriptografija, Kriptoanaliza i steganografija** Literatura: M.Veinović, S.Adamović, Kriptologija 1, Univerzitet Singidunum, 2013	2	Vezbe – Uvod u Cryptool alat za kriptografiju Literatura: S. Adamović, Zaštita informacionih sistema, Univerzitet Singidunum, 2015.	2
3.	**Tema: Tri faktora autentifikacije** Literatura: M.Veinović, S.Adamović, Kriptologija 1, Univerzitet Singidunum, 2013	2	Vezbanje – Cryptool – primer sifrovanja Literatura: S. Adamović, Zaštita informacionih sistema, Univerzitet Singidunum, 2015.	2
4.	**Tema: Klasični šifarski sistemi** Literatura: M.Veinović, S.Adamović, Kriptologija 1, Univerzitet Singidunum, 2013	2	Vezbe - Cryptool – primer sifrovanja Literatura: M.Veinović, S.Adamović, Kriptologija 1, Univerzitet Singidunum, 2013	2
5.	**Tema: Apsolutno tajni šifarski sistemi** Literatura: M.Veinović, S.Adamović, Kriptologija 1, Univerzitet Singidunum, 2013	2	Vezbe - Cryptool – primer OTP sifrovanja Literatura: M.Veinović, S.Adamović, Kriptologija 1, Univerzitet Singidunum, 2013	2
6.	**Tema: Simetrični sekvencijalni šifarski sistemi** Literatura: M.Veinović, S.Adamović, Kriptologija 1, Univerzitet Singidunum, 2013	2	Vezbanje - Apsolutno tajni šifarski sistemi Literatura: M.Veinović, S.Adamović, Kriptologija 1, Univerzitet Singidunum, 2013	2
7.	**Tema: Simetrični blokovski šifarski sistemi** Literatura: M.Veinović, S.Adamović, Kriptologija 1, Univerzitet Singidunum, 2013	2	Vezbanje - Simetrični šifarski sistemi Literatura: S. Adamović, Zaštita informacionih sistema, Univerzitet Singidunum, 2015.	2
8.	**Tema: Diffie-Helman razmena tajnih ključeva** Literatura: M.Veinović, S.Adamović, Kriptologija 1, Univerzitet Singidunum, 2013	2	Vezbanje - sekvencijalni šifarski sistemi u Java jeziku Literatura: S. Adamović, Zaštita informacionih sistema, Univerzitet Singidunum, 2015.	2
9.	**Tema: Asimetrični šifarski sistemi** M.Veinović, S.Adamović, Kriptologija 1, Univerzitet Singidunum, 2013	2	Vezbanje - blokovski šifarski sistemi u Java jeziku Literatura: S. Adamović, Zaštita informacionih sistema, Univerzitet Singidunum, 2015.	2
10.	**Tema: Infrastruktura sistema sa javnim ključevima** Literatura: M.Veinović, S.Adamović, Kriptologija 1, Univerzitet Singidunum, 2013	2	Vezbanje - Diffie-Helman razmena tajnih ključeva Literatura: S. Adamović, Zaštita informacionih sistema, Univerzitet Singidunum, 2015.	2
11.	**Tema: Heš funkcije. Primena heš funkcija** M.Veinović, S.Adamović, Kriptologija 1, Univerzitet Singidunum, 2013	2	Vezbanje - Asimetrični šifarski sistemi Literatura: S. Adamović, Zaštita informacionih sistema, Univerzitet Singidunum, 2015.	2
12.	**Tema: Kontrola pristupa - autentifikacija** Literatura: M.Veinović, S.Adamović, Kriptologija 2, Univerzitet Singidunum, 2013	2	Vezbanje - Infrastruktura sa javnim ključevima Literatura: S. Adamović, Zaštita informacionih sistema, Univerzitet Singidunum, 2015.	2
13.	**Tema: Autentfikacioni protokoli** Literatura: M.Veinović, S.Adamović, Kriptologija 2, Univerzitet Singidunum, 2013	2	Vezbanje - Heš funkcije Literatura: S. Adamović, Zaštita informacionih sistema, Univerzitet Singidunum, 2015.	2
14.	**Tema: Kriptografski protokoli** Literatura: M.Veinović, S.Adamović, Kriptologija 2, Univerzitet Singidunum, 2013	2	Vezbanje - autentifikacija Literatura: S. Adamović, Zaštita informacionih sistema, Univerzitet Singidunum, 2015.	2
15.	**Tema: Kontrola pristupa - autorizacija** Literatura: M.Veinović, S.Adamović, Kriptologija 2, Univerzitet Singidunum, 2013	2	Vezbanje - autentifikacija Literatura: S. Adamović, Zaštita informacionih sistema, Univerzitet Singidunum, 2015.	2

LITERATURA:

Osnovna literatura :

- M.Veinović, S.Adamović, Kriptologija 1, Univerzitet Singidunum, 2013.
- M.Veinović, S.Adamović, Kriptologija 2, Univerzitet Singidunum, 2013.
- S. Adamović, Zaštita informacionih sistema, Univerzitet Singidunum, 2015.

Dodatna literatura :

- M.Stamp, Information Security, Principles and Practice, John Wiley&Sons, 2011.
- Bruce Schneier, Primenjena kriptografija, prevod Mikro Knjiga, 2007.

NAPOMENA:

- *Za svaku nastavnu temu, studentima mora biti dostupan materijal na bosanskom jeziku.*
- *Na kraju svakog nastavnog časa odredjene grupe studenata će se angažovati na studijskom slučaju ili zadatku na osnovu predavane teme .*
- *Postignute rezultatete sa datog zadatka, studentske grupe trebaju prezentovati i prodiskutovati na časovima vježbi.*

Napomena za studente:

- Student treba biti odgovoran i poštovati instituciju i pravila školovanja.
- Treba poštovati raspored predavanja , vježbi i biti pažljiv na nastavnom času.
- Obavjezan je posjedovati i prikazati indeks na testovima i ispitu .
- Tokom izrade seminarskog rada , student se treba pridržavati datih uputstava od predavača o realizaciji istraživanja i tehničkoj izradi.