Studijski program	Vrsta studija (ciklus)	I ciklus		
	Naziv studijskog programa	Opći smjer, Teorijska kompjuterska nauka, Primijenjena matematika		
PREDMET				
Naziv predmeta	**Kriptologija**			
Šifra predmeta	Semestar	Status predmeta	ECTS	Kontakt sati (P+AV+LV)
AMAT 230	III/V	Obavezni/Izborni	3	2+1+0
Nosilac programa				
Cilj predmeta	Kriptografija se bavi zaštitiom podataka na komjuteru i zaštitom istih prilikom prenosa kroz mrežu. Cilj predmeta je da se studenti upoznaju sa teorijskim osnovama kriptologije, kriptologijskim metodama, tehnikama i algoritmima, tako da na budućem radnom mjestu mogu pravilno odabrati i po potrebi isprogramirati kriptosistem u cilju uspješne zaštite podataka.			
Ishod učenja	Nakon uspješnog završetka modula student će: - poznavati savremene načine zaštite podataka; - stečena znanja veoma uspješno primjenjivati u praksi.			

Sadržaj predmeta

- Pojam kriptologije. Svrha kriptologije. Istorijat, dometi i budućnost kriptologije.Teorijske osnove.
- Prosti šifarski sistemi, moderne protočne šifre i konačna polja.
- Pojam sigurnosti kriptosistema, napadi na blokovske šifre.
- Simetrični kriptosistemi, AES, DES, triple-DES.
- Kriptosistemi sa javnim ključem: RSA.
- Heš funkcije, MD5, kodovi za autentifikaciju, potpisi za autentifikaciju.
- Kriptoanaliza. Linearna i diferencijalna kriptoanaliza.
- Ispitivanje prostosti broja, faktorizacija brojeva. Načini odabira tajnog ključa
- Permutacioni polinomi, kriptologije upotrebom eliptičkih krivih. Booleove funkcije.

LITERATURA

[1] Richard A. Mollin, An Introduction to cryptography, 2nd edition, (2007), Taylor & Francis Group.
[2] Jonathan Katz, Yehuda Lindel, Introduction to Modern Cryptography, (2008), Taylor & Francis Group.
[3] Lidl, Niederriter, Finite Fields, Encyclopedia of Mathematics and its Applications, (2008).
[4] ByWenbo Mao Helwett-Pacard Company, Modern Cryptography: Theory and Practice, (2003) Prentice Hall.

OPTEREĆENJE STUDENTA (sati u semestru)

Predavanje	30	Vježbe	15	Samostalan rad	30	U k u p n o	75

PROVJERA ZNANJA I OCJENJIVANJA			**NAPOMENA**
Kriterij	Maksimalan broj bodova	Bodovi za prolaz	
Testovi tokom kursa	40	23	
Zadaće	5	2	
Projekti	15	8	
Završni ispit	40	22	
U k u p n o	100	55	