| | Naziv predmeta: | Odabrana poglavlja iz kriptografije II | | |
|---|---|---|---|---|
| **Šifra predmeta** | **Status predmeta** | **Semestar** | **Broj ECTS kredita** | **Fond časova** |
| | **Izborni** | **II** | **10** | |

***Studijski programi za koje se organizuje :***
Doktorski studijski program Računarske nauke (studije traju 6 semestra, 180 ECTS kredita)

***Uslovljenost drugim predmetima:*** Nema uslovljenosti drugim predmetima

***Ciljevi izučavanja predmeta:***
Cilj predmeta je da upozna studenta sa teorijskim i praktičnim aspektima kriptologije, kriptoamalize i bezbednosnim konceptima

***Ime i prezime nastavnika i saradnika:*** Prof. dr Milo Tomašević

***Metod nastave i savladanja gradiva:*** Mentorska nastava, konsultacije, samostalno učenje i samostalna izrada zadataka

## *Sadržaj predmeta*

| | |
|---|---|
| Pripremna nedjelja | Priprema i upis semestra |
| I nedjelja | Heš funkcije |
| III nedjelja | Digitalni potpis |
| IV nedjelja | Kriptološki sistemi |
| V nedjelja | Infrastuktura sa javnim ključevima |
| VI nedjelja | Sistemi za sakrivanje informacija |
| VII nedjelja | Osnovni modeli autentifikacije |
| VIII nedjelja | Biometrijsk sistemi autentifikacije |
| IX nedjelja | Sistemi za autorizaciju |
| X nedjelja | Autentifikacioni protokoli |
| XI nedjelja | Elementi kriptoanalize |
| XII nedjelja | TMTO princip |
| XIII nedjelja | Bezbednosni aspekti razvoja softvera |
| XIV nedjelja | Primena paralelizacije u implementacije |
| XV nedjelja | Patenti i standardi |
| XVI nedjelja | *Završni ispit* |
| Završna nedjelja | *Ovjera semestra i upis ocjena* |
| XVIII-XXI nedjelja | *Dopunska nastava i popravni ispitni rok* |

***Obaveze studenta u toku nastave:*** Prisustvo predavanjima, izrada projektnog zadatka i zavšnog ispita

***Opterećenje studenta u časovima:***

| Nedjeljno | Rad u toku semestra |
|---|---|
| 10 kredita x 40/30 = 13 sati i 20 minuta.<br>Struktura: 4 sata predavanja 9 sati i 20 min. samostalnog rada, uključujući konsultacije | Nastava i završni ispit: (13 sati i 20 minuta) x16=213 sati i 20 minuta<br>Pripreme: ( nabavka literature, upis, ovjera) 2 x (13 sati 20 minuta) = 26 sati 40 minuta<br>Ukupno opterećenje za predmet: 10 x 30 = 300 sati<br>Dopunski rad: od 0 do 300 – 240 = 60 sati |

***Literatura:***


1. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone - Handbook of Applied Cryptography, 1996.
2. M. Stamp, R. Low – Aplied Cryptanalysis, J. Wiley & Sons, 2007.
3. B. Schneier, Applied Cryptography, J. Wiley & Sons, 1996.


***Oblici provjere znanja i ocjenjivanje:***
Projektni zadatak 50 poena
Završni ispit 50 poena