SYLLABUS

1. Puni naziv nastavnog predmeta:

Kriptografija

2. Skraćeni naziv nastavnog predmeta / šifra:

3. Ciklus studija:

1

4. Bodovna vrijednost ECTS:

6

5. Status nastavnog predmeta:

○ Obavezni ◉ Izborni

6. Preduslovi za polaganje nastavnog predmeta:

nema

7. Ograničenja pristupa:

8. Trajanje / semestar:

1 8

9. Sedmični broj kontakt sati:

9.1. Predavanja: 3

9.2. Auditorne vježbe: 1

9.3. Laboratorijske / praktične vježbe: 1

10. Fakultet:

Prirodno-matematički fakultet

11. Odsjek / Studijski program:

Matematika/Matematika

12. Odgovorni nastavnik:

dr.sc. Mirela Garić-Demirović, vanredni profe

13. E-mail nastavnika:

14. Web stranica:

15. Ciljevi nastavnog 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.

16. Ishodi učenja:

Po završetku kursa, studenti će biti u mogućnosti isprogramirati kriptosistem u cilju uspješne zaštite podataka.

17. Indikativni sadržaj nastavnog 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.

18. Metode učenja:

Planirane su sljedeće aktivnosti uspješnog učenja: konkretno iskustvo, promatranje i promišljanje, stvaranje apstraktnih koncepata. Kao stilovi učenja preferiraju se: vizuelni stil, logičko-matematički i samostalni.
Najznačanije metode učenja na predmetu su:
- Predavanja, tehnika aktivnog učenja i uz aktivno učešće i diskusije studenata;
- Auditorne vježbe;

19. Objašnjenje o provjeri znanja:

Ocjena na ispitu zasnovana je na ukupnom broju bodova koje je student stekao ispunjavanjem predispitnih obaveza i polaganjem ispita, a prema kvalitetu stečenih znanja i vještina, i sadrži maksimalno 100 bodova, te se utvrđuje prema slijedećoj skali:
Sistem bodovanja:

1. Test - Zadaci 25%
2. Test - Zadaci 25%

Domaće zadaće 5%
Aktivnost 5%
Predispitne obaveze ukupno: 60%
Završni ispit 40%
UKUPNO: 100%

20. Težinski faktor provjere:

Ocjenjivanje

Osvojen broj bodova	Ocjena (BiH)	(ECTS ocjena)
< 54	5	F
54 – 63	6	E
64 – 73	7	D
74 – 83	8	C
84 – 93	9	B
94 – 100	10	

21. Osnovna literatura:

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

22. Internet web reference:

23. U primjeni od akademske godine:

2018/2019

24. Usvojen na sjednici NNV/UNV:

03.04.2018.