SVEUČILIŠTE U RIJECI
ODJEL ZA MATEMATIKU

# DETALJNI IZVEDBENI NASTAVNI PLAN PREDMETA

| Opće informacije | | |
|---|---|---|
| ***Naziv predmeta*** | Teorija kodiranja i kriptografija | |
| ***Studijski program*** | Diplomski studij Diskretna matematika i primjene; Diplomski studij Matematika; Diplomski studij Matematika i informatika | |
| ***Godina*** | 1. | |
| ***Status predmeta*** | Obvezatan/Izborni | |
| ***Web stranica predmeta/MudRi*** | Mudri, Odjel za matematiku, Teorija kodiranja i kriptografija | |
| ***Mogućnost izvođenja nastave na engleskom jeziku*** | DA | |
| ***Bodovna vrijednost i način izvođenja nastave*** | ***ECTS koeficijent opterećenja studenata*** | 5 |
| | ***Broj sati (P+V+S)*** | 30+0+15 |
| ***Nositelj predmeta*** | ***Ime i prezime*** | Vedrana Mikulić Crnković |
| | ***Ured*** | 503 |
| | ***Vrijeme za konzultacije*** | konzultacije po dogovoru e-mailom |
| | ***Telefon*** | 584-667 |
| | ***e-adresa*** | vmikulic@math.uniri.hr |
| ***Suradnik na predmetu*** | ***Ime i prezime*** | Marija Maksimović |
| | ***Ured*** | 526 |
| | ***Vrijeme za konzultacije*** | Ponedjeljak 16-18 |
| | ***Telefon*** | 584-665 |
| | ***e-adresa*** | mmaksimovic@math.uniri.hr |

## 1. OPIS PREDMETA

### 1.1. *Ciljevi predmeta*

Cilj kolegija je upoznati studente s osnovnim kriptografskim sustavima i osnovnim metodama u teoriji kodiranja. U tu će se svrhu u okviru kolegija:

- opisati, usporediti i primijeniti različite kriptografske sustave,
- analizirati osnovna načela kriptoanalize,
- analizirati osnovna načela teorije kodiranja,
- definirati, razlikovati i primijeniti različite metode kodiranja,
- analizirati metode detektiranja grešaka pri kodiranju,
- opisati metode ispravljanja grešaka pri kodiranju.

### 1.2. *Korelativnost i korespondentnost predmeta*

### 1.3. *Očekivani ishodi učenja za predmet*

Očekuje se da nakon odslušanog kolegija i položenog ispita studenti:

- budu sposobni razlikovati i analizirati kriptografske sustave i argumentirano primijeniti odgovarajući postupak u rješavanju problema,
- mogu analizirati i razlikovati različite vrste kodova te da mogu argumentirano primijeniti odgovarajući postupak u rješavanju problema,
- mogu razlikovati načine detektiranja greške u prijenosu podataka pojedinom metode kodiranja i analizirati uvjete u kojima je moguće ispraviti tu pogrešku,

SVEUČILIŠTE U RIJECI
ODJEL ZA MATEMATIKU

***Sveučilište u Rijeci • Odjel za matematiku***
Radmile Matejčić 2 • 51 000 Rijeka • Hrvatska
T: (051) 584-650 • F: (051) 584-699
*http://www.math.uniri.hr* • e-adresa: math@math.uniri.hr

- budu sposobni matematički dokazati utemeljenost svih postupaka i tvrdnji kojima se služe u okviru ovog kolegija.

### 1.4. *Okvirni sadržaj predmeta*

Uvod u kriptografiju. Klasična kriptografija. Data Encryption Standard. International Data Encrpytion Algorithm. Advanced Encryption Standard. Kriptografija javnog ključa. RSA i primijene. Uvod u teoriju kodiranja. Golayevi kodovi. Ciklički kodovi. BCH kodovi. Hadamardovi kodovi. Reed-Solomonovi kodovi i CD.

| | | |
|---|---|---|
| 1.5. ***Vrste izvođenja nastave*** | X predavanja<br>X seminari i radionice<br>☐ vježbe<br>X e-učenje<br>☐ terenska nastava<br>☐ praktična nastava<br>☐ praktikumska nastava | X samostalni zadaci<br>X multimedija i mreža<br>☐ laboratorijski rad<br>X projektna nastava<br>X mentorski rad<br>X konzultativna nastava<br>☐ ostalo<br>_____ |
| 1.6. ***Komentari*** | | |

### 1.7. *Obveze studenata i način vrednovanja obveza*

Studenti su obavezni prisustvovati nastavi, aktivno sudjelovati u svim oblicima nastave, ostvariti određeni broj bodova na svakoj aktivnosti te položiti završni ili popravni ispit.

## 2. SUSTAV OCJENJIVANJA

### 2.1. *Ocjenjivanje i vrednovanje rada studenata tijekom nastave i na završnom ispitu*

Rad studenta na predmetu će se vrednovati i ocjenjivati tijekom nastave i na završnom/popravnom ispitu.
Ukupan broj bodova koje student može ostvariti tijekom nastave je 70 (ocjenjuju se opisane aktivnosti studenata). Kroz sve aktivnosti tijekom nastave treba ukupno skupiti odgovarajući broj ocjenskih bodova da bi se moglo pristupiti završnom/popravnom ispitu.
Studenti koji tijekom nastave ostvare iznos ocjenskih bodova koji ih svrstavaju u kategoriju FX (30 do 39,9 na preddiplomskom/40 do 49,9 na diplomskom) imaju mogućnost tri izlaska na popravni ispit i mogu ukupno dobiti samo ocjenu E.
Popravni/završni ispit se sastoji od pisanog i usmenog dijela. Na završnom ispitu moguće je ostvariti najmanje 10, a najviše 30 bodova. Na popravnom ispitu moguće je ostvariti najviše 10 bodova. Ispitni praga na svakom pojedinom dijelu završnog/popravnog ispita je 50%.

SEMINAR (30 bodova)
Svaki student obavezan je izraditi na zadanu temu. Za svaki seminara studente predaje pisani rad, održava izlaganje u trajanju od 40 minuta i priprema zadatke na temu seminara.
TEST (20 bodova)
Organizirat će se dva testa kojima će se ispitivati poznavnaje i razumijevanje osnovnih pojmova iz teorije (sadržaj predavanja) i provjera znanja stećenih rješavanjem domaćih zadaća.
Na svakom testu student može ostvariti najviše 10 bodova.
DOMAĆE ZADAĆE (20 bodova)
Nakon predavanja u 6 navrata bit će objavljeni zadaci iz područja koje je obrađeno na predavanjima.

POPRAVNI ISPIT (10 bodova)
Popravni ispit nosi najviše 10 bodova. Sastoji se od pisanog i usmenog dijela, a ispitni prag na svakom pojedinom dijelu je 50%.
ZAVRŠNI ISPIT (30 bodova)
Završni ispit se sastoji od pisanog i usmenog dijela te nosi najviše 30 bodova. Ispitni prag na svakom pojedinom dijelu je 50%. Student koji pređe ispitni prag ostvarit će minimalno 10 bodova.

### 2.2. *Minimalni uvjeti za pristup ispitu*

| AKTIVNOST KOJA SE BODUJE | MINIMALNI BROJ BODOVA ZA IZLAZAK NA ZAVRŠNI ISPIT | MINIMALNI BROJ BODOVA ZA IZLAZAK NA POPRAVNI ISPIT |
|---|---|---|
| Seminar | 15 | 12 |
| Domaće zadaće | 10 | 8 |

***Sveučilište u Rijeci • Odjel za matematiku***
Radmile Matejčić 2 • 51 000 Rijeka • Hrvatska
T: (051) 584-650 • F: (051) 584-699
*http://www.math.uniri.hr* • e-adresa: math@math.uniri.hr

| | | |
|---|---|---|
| Tetsovi | 10 | 8 |
| **UKUPNO:** | 50 | 40 |
| **OSTALI UVJETI:** | | |

### 2.3. *Formiranje konačne ocjene*

Na temelju ukupnog zbroja ocjenskih bodova stečenih tijekom nastave i na popravnom/završnom ispitu određuje se konačna ocjena prema sljedećoj raspodjeli:

| OCJENA | PREDDIPLOMSKI STUDIJ | DIPLOMSKI STUDIJ |
|---|---|---|
| 5 (A) | od 80 do 100 ocjenskih bodova | od 90 do 100 ocjenskih bodova |
| 4 (B) | od 70 do 79,9 ocjenskih bodova | od 80 do 89,9 ocjenskih bodova |
| 3 (C) | od 60 do 69,9 ocjenskih bodova | od 70 do 79,9 ocjenskih bodova |
| 2 (D) | od 50 do 59,9 ocjenskih bodova | od 60 do 69,9 ocjenskih bodova |
| 2 (E) | od 40 do 49,9 ocjenskih bodova | od 50 do 59,9 ocjenskih bodova |
| 1 (FX) | od 30 do 39,9 ocjenskih bodova | od 40 do 49,9 ocjenskih bodova |
| 1 (F) | od 0 do 29,9 ocjenskih bodova | od 0 do 39,9 ocjenskih bodova |

## 3. LITERATURA

### 3.1. *Obvezna literatura*

Dujella: Kriptografija (skripta dostupna online: http://web.math.hr/~duje/kript/kriptografija.html
J.I. Hall, Notes on Coding Theory, 2010 (skripta dostupna online: http://www.math.msu.edu/~jhall/classes/codenotes/coding-notes.html)

### 3.2. *Dodatna literatura*

1. Assmus, J.D. Key, Designs and their codes, Cambridge University Press, London, 1992.
2. A. Dujella, M. Maretić, Kriptografija, Element, Zagreb, 2007.
3. N. Koblitz, A Course in Number Theory and Cryptography, Springer Verlag, New York, 1994.
4. J.H. van Lint, Introduction to Coding Theory, Springer-Verlag, Berlin, 1982.
5. F.J. MacWilliams, N.J.A. Sloane, The theory of error-correcting codes, North-Holland, 1977.
6. B.Schneiner, Applied Cryptography, Wiley, NY 1995.
7. J. Seberry, J. Pieprzyk, Cryptography: an introduction to computer security, Prentice-Hall, 1989.
8. D.R.Stinson, Cryptography. Theory and Practice, CRC Press, Boca Raton, 1996.
9. D. Welsh, Codes and cryptography, Oxford: Clarendon Press, 1988.

## 4. DODATNE INFORMACIJE O PREDMETU

### 4.1. *Pohađanje nastave*

### 4.2. *Način informiranja studenata*

Studenti će obavijesti o kolegiju dobivati na sustavu Mudri (forumi, private poruke i sl.). Na sustavu Mudri će također biti objavljene sve obaveze (uključujući i zadatke za domaću zadaću) koje student moraju izvršavati tijekom semestra i na završnom/popravnom ispitu kao i bodovi ostvareni na svim aktivnostima.
Odgovornost je studenta da redovito provijerava online kolegij na Mudrom te elektorničku poštu kako bi bio pravovremeno informiran.

### 4.3. *Ostale relevantene informacije*

- Od studenata se očekuje visok stupanj samostalnosti i odgovornosti u radu. Tijekom rada na kolegiju poticat će se poučavanje usmjereno studentu i aktivni pristup učenju.
- Prilikom izrade zadataka predviđenih planom i programom kolegija te izvedebnim planom kolegija studenti se ne smiju služiti tuđim tekstom kao svojim. Svako neovlašteno preuzimanje tuđega teksta bez navođenja izvora smatra se intelektualnom krađom i podložno je sankcijama predviđenim važećim aktima! Ukoliko student ne zna objasniti rješenje zadatka koji je predao kao domaću zadaću ili na kolokviju, smatrat će se da ga student nije samostalno izradio te se rješenje neće bodovati.

SVEUČILIŠTE U RIJECI
ODJEL ZA MATEMATIKU

***Sveučilište u Rijeci • Odjel za matematiku***
Radmile Matejčić 2 • 51 000 Rijeka • Hrvatska
T: (051) 584-650 • F: (051) 584-699
*http://www.math.uniri.hr* • e-adresa: math@math.uniri.hr

- Uratke koje studenti budu slali putem sustava MudRi trebaju pripremiti prema uputi koju će dobiti na predavanjima odnosno seminarima. Kopije svojih radova studenti trebaju zadržati dok ne polože završni ispit iz kolegija.
- Za uspješan rad na kolegiju od studenta se očekuje poznavanje engleskog jezika (čitanje i razumijevanje teksta na engleskom jeziku).

### 4.4. *Način praćenja kvalitete i uspješnosti izvedbe predmeta*

Kvaliteta održane nastave prati se u skladu s aktima Odjela za matematiku i Sveučilišta u Rijeci. U zadnjem tjednu nastave tekućega semestra provodit će se anonimna anketa u kojoj će studenti evaluirati kvalitetu održane nastave iz ovog predmeta. Na kraju semestra provest će se analiza uspješnosti studenata na održanim ispitima iz ovog predmeta.

### 4.5. *Ispitni rokovi*

| | |
|---|---|
| ***Ljetni*** | 26.6.2017.<br>10.7.2017. |
| ***Jesenski izvanredni*** | 4.9.2017. |

## 5. RASPORED IZVOĐENJA NASTAVE I ODRŽAVANJA KOLOKVIJA U AKADEMSKOJ GODINI 2016./2017.

| *DATUM* | *VRIJEME* | *VRSTA NASTAVE* | *NAZIV TEME* | *GRUPA* | *PROSTORIJA* |
|---|---|---|---|---|---|
| 6.3. | 10.15-12.45 | P | Uvod u program GAP | | O-334 |
| 13.3. | 10.15-12.45 | P | Klasična kriptografija | | O-334 |
| 20.3. | 10.15-12.45 | P | Klasična kriprografija. Kriptografski standardi. | | O-334 |
| 27.4. | 10.15-12.45 | P | Kriptografski standardi. Kriptografija javnog ključa. | | O-334 |
| 3.4. | 10.15-12.45 | S | Kriptografija javnog ključa. | | O-334 |
| 10.4 | 10.15-12.45 | P | Uvod u teoriju kodiranja. Linerani kodovi. | | O-334 |
| nadoknada u dogovoru sa studentima | | S | Studentska izlaganja | | O-334 |
| 24.4. | 10.15-12.45 | | 1. test | | O-334 |
| nadoknada u dogovoru sa studentima | | P | Linearni kodovi | | O-334 |
| 8.5. | 10.15-12.45 | S | Studentska izlaganja | | O-334 |
| 15.5. | 10.15-12.45 | P | Ciklički kodovi | | O-334 |
| 22.5. | 10.15-12.45 | P | BCH kodovi | | O-334 |
| 29.5. | 10.15-12.45 | P | Savršeni kodovi | | O-334 |
| 5.6. | 10.15-12.45 | P | Kodovi u programu Magma | | O-334 |
| 12.6 | 10.15-12.45 | S | 2. test/Studentska izlaganja | | O-334 |

**Moguća su manja odstupanja u realizaciji izvedbenog plana.*

P – predavanja
AV – auditorne vježbe
VP – vježbe u praktikumu
MV – metodičke vježbe
S - seminari