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

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	http://moodle.srce.hr/2020-2021/	
Mogućnost izvođenja nastave na engleskom jeziku	DA	
Bodovna vrijednost i način izvođenja nastave	***ECTS koeficijent opterećenja studenata***	6
	Broj sati (P+V+S)	30+15+15
Nositelj predmeta	***Ime i prezime***	Marija Maksimović
	Ured	O-504
	Vrijeme za konzultacije	konzultacije po dogovoru e-mailom
	Telefon	051/584-665
	e-adresa	mmaksimovic@math.uniri.hr
Nositelj predmeta	***Ime i prezime***	Nina Mostarac
	Ured	O-525
	Vrijeme za konzultacije	konzultacije po dogovoru e-mailom
	Telefon	051/584-666
	e-adresa	nmavrovic@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:

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

1.2. Korelativnost i korespondentnost predmeta

1.3. Očekivani ishodi učenja za predmet

Nakon odslušanog kolegija i položenog ispita studenti će:

- analizirati i razlikovati različite vrste kodova te da mogu argumentirano primijeniti odgovarajući postupak u rješavanju problema,
- 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

- biti u stanju matematički dokazati utemeljenost svih postupaka i tvrdnji kojima se služe u okviru ovog kolegija,
- razlikovati i analizirati kriptografske sustave i argumentirano primijeniti odgovarajući postupak u rješavanju problema.

1.4. Okvirni sadržaj predmeta

Uvod u teoriju kodiranja. Linearni kodovi. Ciklički kodovi. BCH kodovi. Reed-Solomonovi kodovi. Savršeni kodovi. Uvod u kriptografiju. Klasična kriptografija. Kriptografski standardi. Kriptografija javnog ključa.

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

1.7. Oblici praćenja studenata i način vrednovanja rada studenata tijekom nastave

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

2. SUSTAV OCJENJIVANJA

2.1. Ocjenjivanje i vrednovanje rada studenata tijekom nastave te način polaganja ispita

Rad studenta na predmetu će se vrednovati i ocjenjivati tijekom nastave i na završnom ispitu. Ukupan broj bodova koje student može ostvariti tijekom nastave je 70 (ocjenjuju se opisane aktivnosti studenata). Kroz sve oblike kontinuiranog praćenja i vrednovanja studenata tijekom nastave treba ukupno skupiti barem 50% ocjenskih bodova da bi se moglo pristupiti ispitu. Također, student mora ispuniti minimalne uvjete za pristup ispitu. Na ispitu je moguće ostvariti maksimalno 30 bodova**.** Prag prolaznosti na završnom ispitu ne može biti manji od 50% uspješno riješenog ispita. Ispit se polaže kao usmena provjera znanja.

Studenti koji tijekom nastave ostvare od 0% do 49,9% ocjenskih bodova koje je bilo moguće steći kroz oblike kontinuiranog praćenja i vrednovanja studenata ocjenjuju se ocjenom F (neuspješan), ne mogu steći ECTS bodove i moraju ponovno upisati predmet. Isto vrijedi i za studente koji u tri ponuđena ispitna roka ne polože završni ispit.

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 (30 bodova)
Organizirat će se dva testa kojima će se ispitivati poznavanje i razumijevanje osnovnih pojmova iz teorije (sadržaj predavanja) i provjera znanja stečenih rješavanjem domaćih zadaća.
Na svakom testu student može ostvariti najviše 15 bodova.

DOMAĆE ZADAĆE (10 bodova)
Tijekom semestra izrađivat će se domaće zadaće te će se u terminu vježbi održati dvije provjere zadaće u trajanju od 15-20 minuta sa zadacima sličnim zadacima iz zadaće. Provjere će se najaviti najkasnije tjedan dana ranije. Na svakoj provjeri student može ostvariti najviše 5 bodova.

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

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%.

2.2. Minimalni uvjeti za pristup ispitu/prolaznu ocjenu

AKTIVNOST KOJA SE BODUJE	MINIMALNI BROJ BODOVA
Seminar	15
Testovi	15
Domaće zadaće	5
UKUPNO:	35
OSTALI UVJETI:	

2.3. Formiranje konačne ocjene

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

OCJENA	BODOVI
5 (A)	od 90 do 100 ocjenskih bodova
4 (B)	od 75 do 89,9 ocjenskih bodova
3 (C)	od 60 do 74,9 ocjenskih bodova
2 (D)	od 50 do 59,9 ocjenskih bodova
1 (F)	od 0 do 49,9 ocjenskih bodova

3. LITERATURA

3.1. Obvezna literatura

1. Dujella: Kriptografija (skripta dostupna online: http://web.math.hr/~duje/kript/kriptografija.html
2. J.I. Hall, Notes on Coding Theory, 2010 (skripta dostupna online: http://www.math.msu.edu/~jhall/classes/codenotes/coding-notes.html)
3. Igor S. Pandžić, Alen Bažant, Željko Ilić, Zdenko Vrdoljak, Mladen Kos, Vjekoslav Sinković: Uvod u teoriju informacija i kodiranja, Element, 2009

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

Studenti smiju izostati s najviše 30% predavanja i s najviše 30% vježbi te su dužni informirati se o nastavi s koje su izostali. Ne tolerira se nikakav oblik remećenja nastave te korištenje mobitela za vrijeme nastave.

4.2. Način informiranja studenata

Svi relevantni podaci i obavijesti o kolegiju bit će objavljeni u okviru online kolegija. Osobna odgovornost studenta je biti redovito informiran.

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

4.3. Ostale relevantne informacije

Od studenata se očekuje visok stupanj samostalnosti i odgovornosti u radu. Tijekom rada na kolegiju poticat će se aktivni pristup učenju.
Prilikom izrade zadataka predviđenih planom i programom 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! Uratke koje studenti budu slali putem sustava Merlin trebaju pripremiti prema uputi koju će dobiti na nastavi. Ako 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. 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. Krajem semestra provodit će se anonimna anketa u kojoj će studenti evaluirati kvalitetu održane nastave iz ovog predmeta. Nakon završetka semestra provest će se analiza uspješnosti studenata iz ovog predmeta.

4.5. Ispitni rokovi

Ljetni	21.6.2021. u 10 sati 5.7.2021. u 10 sati
Jesenski izvanredni	2.9.2021. u 10 sati

5. SATNICA IZVOĐENJA NASTAVE I ODRŽAVANJA KOLOKVIJA U AKADEMSKOJ GODINI 2020./2021.

DATUM	*VRIJEME*	*OBLIK NASTAVE*	*NAZIV TEME*	*GRUPA*	*PROSTORIJA*
2.3.2021.	11:15-12:45	P	Uvod u kolegij. Osnovni pojmovi kriptografije.	svi	O-S31
4.3.2021.	10:15-11:45	V	Uvod u program GAP	svi	O-363
9.3.2021.	11:15-12:45	P	Klasična kriptografija	svi	O-S31
11.3.2021.	10:15-11:45	V	Klasična kriptografija	svi	O-363
16.3.2021.	11:15-12:45	P	Klasična kriptografija	svi	O-S31
18.3.2021.	10:15-11:45	S	Studentska izlaganja	svi	O-363
23.3.2021.	11:15-12:45	P	Kriptografski standardi.	svi	O-S31
25.3.2021.	10:15-11:45	V	Kriptografski standardi.	svi	O-363
30.3.2021.	11:15-12:45	P	Kriptografski standardi.	svi	O-S31
1.4.2021.	10:15-11:45	S	Studentska izlaganja	svi	O-363
6.4.2021.	11:15-12:45	P	Kriptografija javnog ključa.	svi	O-S31
8.4.2021.	10:15-11:45	S	Studentska izlaganja	svi	O-363
13.4.2021.	11:15-12:45	P	Kriptografija javnog ključa.	svi	O-S31
15.4.2021.	10:15-11:45	V	Kriptografija javnog ključa.	svi	O-363
20.4.2021.	11:15-12:45	P	Uvod u teoriju kodiranja.	svi	O-S31
22.4.2021.	**10:15-11:45**	**V**	**1. test**	**svi**	**O-363**
27.4.2021.	11:15-12:45	P	Linearni kodovi	svi	O-S31
29.4.2021.	10:00-12:00	S	Studentska izlaganja	svi	O-363
4.5.2021.	11:15-12:45	P	Linearni kodovi	svi	O-S31
6.5.2021.	10:15-11:45	V	Linearni kodovi	svi	O-363
11.5.2021.	11:15-12:45	P	Ciklički kodovi	svi	O-S31
13.5.2021.	10:00-12:00	S	Studentska izlaganja	svi	O-363
18.5.2021.	11:15-12:45	P	Ciklički kodovi. BCH kodovi	svi	O-S31
20.5.2021.	10:15-11:00	V	Ciklički kodovi	svi	O-363

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

20.5.2021.	11:00-11:45	S	Studentska izlaganja	svi	O-363
25.5.2021.	11:15-12:45	P	Savršeni kodovi	svi	O-S31
27.5.2021.	**10:15-11:45**	**V**	**2. test**	**svi**	**O-363**
01.06.2021.	11:15-12:45	P	Savršeni kodovi	svi	O-S31
08.6.2021.	11:00-13:00	S	Studentska izlaganja	svi	O-S31
10.6.2021.	10:15-11:45	P	Popravne aktivnosti	svi	O-363

Moguća su manja odstupanja u realizaciji izvedbenog plana.

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