SVEUČILIŠTE U RIJECI
FAKULTET ZA MATEMATIKU

Sveučilište u Rijeci •Fakultet 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 KOLEGIJA

Opće informacije		
Naziv kolegija	**Teorija kodiranja i kriptografija**	
Studijski program	Sveučilišni diplomski studij Diskretna matematika i primjene	
Godina	1.	
Status kolegija	Obvezatan	
Web stranica kolegija	https://moodle.srce.hr	
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 kolegija	***Ime i prezime***	**Nina Mostarac**
	Ured	O-525
	Vrijeme za konzultacije	Četvrtak, 8:30-10:00
	Telefon	051/584-666
	e-adresa	nmavrovic@math.uniri.hr
Suradnici na kolegiju	***Ime i prezime***	**Tin Zrinski**
	Ured	O-319
	Vrijeme za konzultacije	Četvrtak, 8:30-10:00
	Telefon	051/584-679
	e-adresa	tin.zrinski@math.uniri.hr

1. OPIS PREDMETA

1.1. Ciljevi kolegija

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 kolegija

1.3. Očekivani ishodi učenja za kolegij

Nakon odslušanog kolegija i položenog ispita studenti će biti u stanju:

I1. razlikovati i analizirati kriptografske sustave i argumentirano primijeniti odgovarajući postupak u rješavanju problema (A7,B7,C7,D7,E5,F7,G7), ...

I2. analizirati i razlikovati različite vrste kodova te argumentirano primijeniti odgovarajući postupak u rješavanju problema (A7,B7,C7,D7,E5,F7,G7),
I3. razlikovati načine detektiranja greške u prijenosu podataka pojedinom metodom kodiranja i analizirati uvjete u kojima je moguće ispraviti tu pogrešku (A7,B7,C5,D5,E5,F5,G5),
I4. matematički dokazati utemeljenost svih postupaka i tvrdnji kojima se služe u okviru ovog kolegija (B7,F4).

1.4. Okvirni sadržaj kolegija

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

1.5. Vrste izvođenja nastave	☒ predavanja ☒ seminari i radionice ☒ vježbe ☒ e-učenje ☐ terenska nastava ☐ praktična nastava ☒ praktikumska nastava	☒ samostalni zadaci ☒ multimedija i mreža ☐ laboratorijski rad ☐ projektna nastava ☐ mentorski rad ☐ konzultativna nastava ☐ ostalo _____
1.6. Komentari	Vježbe iz ovog kolegija izvodit će se na računalima.	

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

KOLOKVIJI (40 bodova)
Organizirat će se dva kolokvija na računalima kojima će se ispitivati poznavanje i razumijevanje gradiva sa predavanja i vježbi. Svaki student na kraju semestra ima pravo pristupiti popravku najviše jednog kolokvija. Bodovi ostvareni na kolokviju kojeg se želi popravljati se brišu te se mjerodavnim smatraju bodovi ostvareni na ponovljenom (popravnom) kolokviju

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.

SEMINAR (20 bodova)
Svaki student obavezan je izraditi barem jedan seminar na zadanu temu. Za svaki seminar student predaje pisani rad, održava izlaganje u trajanju od 40 minuta i priprema zadatke na temu seminara.

ZAVRŠNI ISPIT (30 bodova)
Završni ispit se sastoji od pisanog i usmenog dijela te nosi najviše 30 bodova. Ispitni prag je 50%.

1.8. Konstruktivno povezivanje

ISHODI UČENJA	SADRŽAJ	NASTAVNE AKTIVNOSTI	METODE VREDNOVANJA
I1	Kriptografija	Kroz predavanja, seminare, vježbe na računalima, rasprave i samostalni rad primjenjivat će se sljedeće metode učenja i poučavanja: metoda demonstracije, metoda usmenog izlaganja, metoda razgovora, metoda pisanja, metoda čitanja i rada na tekstu.	pisane provjere znanja, seminarski rad, zadaće, usmeni ispit
I2	Teorija kodiranja		
I3	Teorija kodiranja		
I4	Cjelokupni sadržaj kolegija.		

SVEUČILIŠTE U RIJECI
FAKULTET ZA MATEMATIKU

Sveučilište u Rijeci •Fakultet 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

2. SUSTAV OCJENJIVANJA

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

Rad studenata 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**.** Završni ispit se sastoji od pisanog i usmenog dijela. Prag prolaznosti na završnom ispitu ne može biti manji od 50% uspješno riješenog ispita.

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.

2.2. Minimalni uvjeti za pristup ispitu/prolaznu ocjenu

AKTIVNOST KOJA SE BODUJE	MINIMALNI BROJ BODOVA
Kolokviji	20
Seminar	10
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, http://web.math.hr/~duje/kript/kriptografija.html
2. J.I. Hall, Notes on Coding Theory, 2010, skripta, 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. E.F. 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 KOLEGIJU

4.1. Pohađanje nastave

Studenti su dužni informirati se o nastavi s koje su izostali. Ne tolerira se nikakav oblik remećenja nastave te korištenje mobitela za vrijeme nastave, na kolokvijima, testovima i ispitima. Studenti su dužni poštovati norme Etičkog kodeksa Sveučilišta u Rijeci.

4.2. Način informiranja studenata

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

4.3. Ostale relevantne informacije

Od studenata se očekuje visok stupanj samostalnosti i odgovornosti u radu.
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 kolegija

Kvaliteta održane nastave prati se u skladu s aktima Fakulteta za matematiku i Sveučilišta u Rijeci. Krajem semestra provodit će se anonimna anketa u kojoj će studenti evaluirati kvalitetu održane nastave iz ovog kolegija. Nakon završetka semestra provest će se analiza uspješnosti studenata iz ovog kolegija.

4.5. Ispitni rokovi

Ljetni	19.6.2024. 10h u 355 3.7.2024. 10h u 355
Jesenski	13.9.2024. 10h u 355

5. SATNICA IZVOĐENJA NASTAVE U AKADEMSKOJ GODINI 2023/2024.

DATUM	*VRIJEME*	*OBLIK NASTAVE*	*NAZIV TEME*	*GRUPA*	*PROSTORIJA*
4.3.2024.	10:15-11:45	P	Uvod u kolegij. Osnovni pojmovi kriptografije.	Svi	360
7.3.2024.	10:15-11:45	VP	Uvod u program GAP	Svi	363
11.3.2024.	10:15-11:45	P	Klasična kriptografija	Svi	360
14.3.2024.	10:15-11:45	VP	Klasična kriptografija	Svi	363
18.3.2024.	10:15-11:45	P	Klasična kriptografija	Svi	360
21.3.2024.	10:15-11:45	VP	Klasična kriptografija	Svi	363
25.3.2024.	10:15-11:45	P	Kriptografski standardi	Svi	360
28.3.2024.	10:15-11:45	S	Studentska izlaganja	Svi	363
4.4.2024.	10:15-11:45	S	Studentska izlaganja	Svi	363
8.4.2024.	10:15-11:45	P	Kriptografski standardi	Svi	360
11.4.2024.	10:15-11:45	P	Kriptografija javnog ključa	Svi	363
15.4.2024.	10:15-11:45	P	Kriptografija javnog ključa	Svi	360

SVEUČILIŠTE U RIJECI
FAKULTET ZA MATEMATIKU

Sveučilište u Rijeci •Fakultet 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

18.4.2024.	10:15-11:45	VP	Kriptografija javnog ključa	Svi	363
22.4.2024.	10:15-11:45	P	Uvod u teoriju kodiranja	Svi	360
25.4.2024.	10:15-11:45	S	Studentska izlaganja	Svi	363
29.4.2024.	10:15-11:45	P	Linearni kodovi	Svi	360
2.5.2024.	10:15-11:45	VP	Prvi kolokvij	Svi	363
6.5.2024.	10:15-11:45	P	Linearni kodovi	Svi	360
9.5.2024.	10:15-11:45	VP	Linearni kodovi	Svi	363
13.5.2024.	10:15-11:45	P	Ciklički kodovi	Svi	360
16.5.2024.	10:15-11:45	S	Studentska izlaganja	Svi	363
20.5.2024.	10:15-11:45	P	Ciklički kodovi	Svi	360
23.5.2024.	10:15-11:45	VP	Ciklički kodovi	Svi	363
27.5.2024.	10:15-11:45	P	BCH kodovi. Savršeni kodovi	Svi	360
3.6.2024.	10:15-11:45	S	2.kolokvij	Svi	363
6.6.2024.	10:15-11:45	S	Studentska izlaganja	Svi	363
10.6.2024.	10:15-11:45	P	Popravni kolokvij	Svi	363
13.6.2024.	10:15-11:45	S	Studentska izlaganja	Svi	363

Moguća su manja odstupanja u realizaciji izvedbenog plana.
Do 40% planirane nastave može biti održano online.

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