PODIPLOMSKI ŠTUDIJSKI PROGRAM 2. STOPNJE MATEMATIČNE ZNANOSTI
OPISI PREDMETOV

TEMELJNI PREDMETI ŠTUDIJSKEGA PROGRAMA

Ime predmeta: **IZBRANA POGLAVJA IZ ALGEBRE (1)**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz področja algebre, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja:
- teorija grup,
- teorija kolobarjev,
- teorija obsegov.

Ime predmeta: **IZBRANA POGLAVJA IZ ANALIZE (1)**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz področja analize, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja
- Fourierova analiza
- analiza na mnogoterostih
- Vektorska analiza. Gaussov in Stokesov izrek.

Ime predmeta: **IZBRANA POGLAVJA IZ DISKRETNE MATEMATIKE (1)**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz področja diskretne matematike, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja
- Teorija konfiguracij
- Teorija grafov
- Algebraične metode v teoriji grafov

Ime predmeta: **IZBRANA POGLAVJA IZ FINANČNE MATEMATIKE (1)**
Število ECTS kreditnih točk: **9**

Vsebina:
Matematika življenjskih zavarovanj.
- Obresti, sedanja vrednost.

- Princip ekvivalence.
- Modeli preživetja.
- Določanje neto premij.
- Določanje neto matematičnih rezerv.
- Upravljanje s tveganji pri življenjskih zavarovanjih.

Modeli trgov.
- Tipi vrednostnih papirjev.
- Stohastični modeli trgov.
- Pojem strategije.

Upravljanje s premoženjem.
- Mere tveganja.
- Optimalna strategija za eno obdobje.
- Dinamične strategije.
- CAPM model.

Opcije.
- Tipi opcij.
- Princip arbitraže.
- Varovanje in osnovni izrek vrednotenja opcij.
- Evropske in ameriške opcije.
- Eksotične opcije.
- Praktični vidiki varovanja.

Modeli obrestnih mer.
- Pomen stohastičnega modeliranja.
- Osnovni modeli za trenutne obrestne mere.
- Opcije na obrestne mere.

Ime predmeta: **IZBRANA POGLAVJA IZ KRIPTOGRAFIJE (1)**
Število ECTS kreditnih točk: **9**

Vsebina:
Nahajamo se na pragu vsesplošnega komuniciranja in elektronskega trgovanja na Internetu. Preko Interneta so dostopne številne podatkovne baze. Na vseh koncih se pojavljajo tudi pametne (čip) kartice, ki predstavljajo tako rekoč računalnik v žepu. Z vsakim dnem bolj občutimo vpliv vsega tega na šolstvo, znanost ter družbo v širšem pomenu.
Kriptografija je veda, ki nam ponuja konkretne rešitve za varnost in zaščito na pravkar omenjenih področjih, ter s tem predstavlja osnovo informacijske družbe (cilji: zasebnost, celovitost podatkov, elektronsko overjanje/podpisovanje, elektronski denar, in drugi kriptografski protokoli; obseg: matematika, računalništvo, elektrotehnika, finance, politika, vojska, itd.). Bolj podrobno bomo študirali področja z naslednjega seznama.

(A) Simetrične šifre
(B) Kriptografija javnih ključev
(C) Digitalni podpisi
(D) Razni kriptografski protokoli
(E) Algoritmična teorija števil
(F) Zgoščevalne funkcije
(G) Napadi

(A) Simetrične šifre
- Splošna teorija tekočih šifer
- Analiza konkretne tekoče šifre, npr. RC4

- Splošna analiza bločnih šifer
- Analiza konkretne bločne šifre, npr. AES
- Primerjava bločnih in tokovnih šifer
- Psevdo-naključna zaporedja
- Analiza 3-DES-a in njegovih posplošitev
- Analiza DESX-a in njegovih posplošitev
- Analiza generatorjev psevdo-naključnih števil v različnih operacijskih sistemih.

(B) Kriptografija javnih ključev
- Napadi na RSA
- Napadi na ElGamalove kriptosisteme
- "Psevdo-naključno" generiranje števil v diskretnih algoritmih (če uporabljamo linearni kongruenčni psevdo-naključni generator števil v DSA, potem lahko zlahka določimo zasebni ključ takoj, ko dobimo nekaj podpisov)
- XTR (Lenstra et al.)
- NTRU (nov napad)
- LUC (kriptosistem z javnimi ključi, ki ne uporablja potenciranja)
- McEliecov sistem z Goppa kodami (predvsem nova varianta digitalnega podpisa)

(C) Digitalni podpisi
- Slepi podpisi
- Skupinski podpisi
- Enkratni podpisi

(D) Razni kriptografski protokoli
- Digitalni denar
- Anonimnost
- Deljenje skrivnosti
- Mentalni poker in vohuni
- Resiliant funkciji
- Kleptografija (študij varne kraje informacij)
- Key escrow (kako skonstruirati kriptosistem javnih ključev, v katerem bi vladalo ravnovesje med zasebnostjo posameznikov ter ustavnim redom)
- Vizualna kriptografija (in Hadamardjeve matrike)
- Dokazi brez razkritja znanja (angl. zero-knowledge proofs)
- Identifikacija in črtne kode

(E) Algoritmična teorija števil
- Optimalno računanje v končnih obsegih
- Polinomske baze
- Normalne baze (npr. optimalne normalne baze ali Chebisheve baze)
- Prehod med različnimi bazami v končnih obsegih GF(pn)
- Faktorizacija naravnih števil
- Pollardova rho-metoda za faktorizacijo
- Faktorizacija polinomov
- Generiranje praštevil
- Probabilistično testiranje praštevilskosti (npr. z EC)
- Problem Praštevilo je v P
- Problem diskretnega logaritma (DLP)
- Pollardova rho-metoda za DLP
- Floydov algoritem

(F) Zgoščevalne funkcije
- Opis in analiza zgoščevalne funkcije HMAC
- Opis in analiza zgoščevalne funkcije RIPEMD

(G) Napadi

Metoda napada s paradoksom rojstnih dni (angl. birthday attack) (uporabna je tako pri simetričnih kot tudi asimetričnih kriptosistemih)

Ime predmeta: **IZBRANA POGLAVJA IZ MATEMATIČNE STATISTIKE (1)**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz področja matematične statistike, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja :
Zadostne statistike
- Definicija zadostne statistike.
- Faktorizacijski izrek.

Teorija optimalnosti pri ocenjevanju parametrov
- Nepristranske cenilke.
- Koncept optimalne cenilke.
- Cramér-Raov izrek.
- Optimalne cenilke.

Ime predmeta: **OSNOVE MOLEKULARNEGA MODELIRANJA**
Število ECTS kreditnih točk: **9**

Vsebina:
- Osnovni koncepti molekularnega modeliranja
- Uvod v računsko kvantno mehaniko
- Moderne ab-initio in DFT kvantne metode
- Metode molekularne mehanike
- Potencialna polja in molekularna mehanika
- Metode računalniških simulacij
- Metode za simulacije molekulske dinamike
- Metode za Monte Carlo simulacije
- Uporaba metod molekularnega modeliranja v kemiji, farmaciji, biofiziki, pri odkrivanju in načrtovanju novih molekul, itd.

Ime predmeta: **IZBRANA POGLAVJA IZ FUNKCIONALNE ANALIZE**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz področja funkcionalne analize, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja
- Topološki vektorski prostori. Posplošena zaporedja.
- Šibka* kompaktnost.
- Operatorji na Banachovem in Hilbertovem prostoru.
- Banachove algebra, C* algebre in von Neumannove algebre.

IZBIRNI PREDMETI

Ime predmeta: **ALGEBRAIČNA KOMBINATORIKA**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz področja algebraične kombinatorike, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja

- Lastne vrednosti grafa;
- Grupa avtomorfizmov grafa;
- Simetrije grafa;
- Grafi s tranzitivno grupo avtomorfizmov (točkovno-tranzitivni grafi, povezavno-tranzitivni grafi, ločno-tranzitivni grafi, razdaljno-tranzitivni grafi);
- Krepko regularni grafi in algebraične metode.

Ime predmeta: **ELIPTIČNE KRIVULJE V KRIPTOGRAFIJI**
Število ECTS kreditnih točk: **9**

Vsebina:
Ta predmet predstavlja samostojen uvod v teorijo eliptičnih krivulj in kako jih uporabimo za konstrukcijo varnih kriptosistemov z javnimi ključi. Predstavili bomo osnovne ideje algoritmov za štetje točk in varnosti diskretnega algoritma. Pokrili bomo tako eliptične krivulje nad obsegi sode karakteristike (t.i. binarni obsegi), ki so posebej primerni za hardwarske implementacije, in eliptične krivulje nad obsegi lihe karakteristike, ki so imele tradicionalno več pozornosti. Bolj podrobno bomo študirali področja z naslednjega seznama.

- O kriptografiji v praksi
- Uporaba končnih obsegov
- Faktorizacija polinomov nad končnimi obsegi
- Rekurzivne in učinkovite konstrukcije nerazcepnih polinomov
- Nerazcepnost kompozitov polinomov
- Normalne baze in porazdelitev normalnih elementov
- Algoritmi za konstrukcijo normalnih elementov
- Optimalne normalne baze, uvod in konstrukcije
- Problem diskretnega logaritma
- Eliptične krivulje na končnimi obsegi
- Kriptosistemi z eliptičnimi krivuljami
- Problem diskretnega logaritma na eliptični krivulji in supersingularne krivulje
- Štetje točk na eliptični krivulji

Ime predmeta: **FINANCIRANJE ZDRAVSTVENEGA VARSTVA**
Število ECTS kreditnih točk: **9**

Vsebina:
Zdravje.

- opredelitev pojma;
- kazalniki zdravstvenega stanja prebivalstva.

Javno in zasebno.

- viri financiranja zdravstvenega varstva;
- vloga sobivanja javnega in zasebnega financiranja zdravstvenega varstva.

Sistemi zdravstvenega varstva.
- Bismarckov sistem obveznega zdravstvenega zavarovanja;
- Beveridgev sistem nacionalnega zdravstvenega varstva;
- tržni sistem zdravstvenega zavarovanja;
- klasifikacije zdravstvenih zavarovanj.

Javno obvezno zdravstveno zavarovanje.
- zgodovinski podatki o razvoju;
- vsebina javnega obveznega zdravstvenega zavarovanja;
- dileme in smeri razvoja.

Zasebna zdravstvena zavarovanja.
- zavarovalna dejavnost;
- dejavniki tveganja in določitev premije;
- dileme in smeri razvoja.

Študije primerov.
- rast izdatkov za zdravstveno varstvo in obvladovanje rasti;
- ponudba zasebnih zdravstvenih zavarovanj;
- odsotnost z dela zaradi bolezni ali poškodbe;
- financiranje zdravstvenega varstva in dolgoživosti;
- druge aktualne vsebine.

Ime predmeta: **GRUPE, KROVI IN ZEMLJEVIDI**
Število ECTS kreditnih točk: **9**

Vsebina:
- Delovanje grup (homomorfizmi in avtomorfizmi delovanj, ekvivariantna in invariantna grupa delovanja).
- Krovi, dvig avtomorfizmov in razširitev grup (krovna projekcija, rekonstrukcija prek delovanja napetostne grupe, regularna krovna projekcija, dvig in spust avtomorfizmov, potrebni in zadostni pogoji za dvig s pomočjo napetostne grupe, dvig avtomorfizmov v regularne abelske krove, zgledi za ciklične in $(\ZZ_p \times \ZZ_p)$-krove, razširitev grup in struktura dvigov grup, geometrične krepko razcepne razširitve).
- Akcijski grafi (homomorfizem delovanj in krovne projekcije akcijskih grafov).
- Zemljevidi (pojem zemljevida na kompaktni ploskvi, algebraični zemljevidi, trikotniške grupe in kartografske grupe orientabilnih algebraičnih zemljevidov, reprezentacija z akcijskim grafom in Schreierjeva reprezentacija, homomorfizmi in avtomorfizmi orientabilnih algebraičnih zemljevidov, topološka interpretacija, regularni homomorfizmi, Riemann-Hurwitzeva enakost in njena uporaba, dvig in spust avtomorfizmov).
- Zemljevidi z visoko stopnjo simetrije (regularni orientabilni zemljevidi, konstrukcije, problem klasifikacije, Cayleyevi orientabilni zemljevidi, potrebni in zadostni pogoji za regularnost, grupa avtomorfizmov kot rotacijski produkt, rod grupe, Hurwitzev izrek, grupe malega roda).

Ime predmeta: **IZBRANA POGLAVJA IZ ALGEBRE (2)**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz področja algebre, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja

- Upodobitve
- Neasociativne algebre
- Delovanje grup
- Grupni kolobarji
- Shurovi kolobarji

Ime predmeta: **IZBRANA POGLAVJA IZ DIFERENCIALNIH ENAČB**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz področja analize, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja

- Diferencialne enačbe.
- Parcialne diferencialne enačbe
- Distribucije
- Variacijski račun.

Ime predmeta: **IZBRANA POGLAVJA IZ TEORIJE ASOCIATIVNIH SHEM**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz področja asociativnih shem, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja

- Asociativne sheme (osnovne definicije, Bose-Mesnerjeva algebra, Kreinovi parametri, primitivne in neprimitivne asociativne sheme, metrične in kometrične asociativne sheme).
- Razdaljno-regularni grafi (osnovne definicije, razdaljno-regularni grafi kot metrične asociativne sheme, presečna števila, lastne vrednosti, primitivni in neprimitivni razdaljno-regularni grafi, Q-polinomski razdaljno-regularni grafi, klasične družine razdaljno-regularnih grafov).

Ime predmeta: **IZBRANA POGLAVJA IZ DISKRETNE MATEMATIKE (2)**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz področja diskretne matematike, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja

- Teorija načrtov
- Diskretne metode v geometriji
- Algebraične metode v diskretni matematiki

Ime predmeta: **IZBRANA POGLAVJA IZ KOMPLEKSNE ANALIZE**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz področja kompleksne analize, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja

- Holomorfne, harmonične, subharmonične funkcije.
- Holomorfne funkcije več spremenljivk

Ime predmeta: **IZBRANA POGLAVJA IZ MATEMATIČNE STATISTIKE (2)**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz področja matematične statistike, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja :

Teorija optimalnosti pri preizkušanju domnev

- Neyman-Personova lema.
- Enakomerno najmočnejši testi.

Asimptotske lastnosti cenilk

- Dosledne cenilke.
- Asimptotska normalnost MLE cenilk.

Ime predmeta: **IZBRANA POGLAVJA IZ NUMERIČNIH METOD**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz področja numeričnih metod, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja

- Aproksimacija funkcij.
- Numerično reševanje navadnih diferenci-alnih enačb.
- Numerično reševanje parcialnih diferenci-alnih enačb.
- Bezierove krivulje in ploskve.

Ime predmeta: **IZBRANA POGLAVJA IZ TEORIJE KONČNIH GEOMETRIJ**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz teorije končnih geometrij, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja

- afine ravnine
- projektivne ravnine
- Desarguesov ter Pappusov izrek
- kolineacije in korelacije
- krivulje druge stopnje, stožernice
- skoraj linearni prostori
- linearni prostori

- afini in projektivni prostori
- posplošeni štirikotniki

Ime predmeta: **IZBRANA POGLAVJA IZ TEORIJE ŠTEVIL**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz iz področja teorije števil, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja:

- Diofanske enačbe,
- Geometrija števil,
- Aditivna teorija števil,
- Algebraična teorija števil.

Ime predmeta: **IZBRANA POGLAVJA IZ TOPOLOGIJE**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz topologije, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja

- Mnogoterosti in Riemannove mnogoterosti
- Algebraična topologija

Ime predmeta: **IZBRANE TEME IZ RAČUNSKO INTENZIVNIH METOD**
Število ECTS kreditnih točk: **9**

Vsebina:

- Hamiltonski sistemi
- numerične integracijske metode in algoritmi
- Liejev formalizem
- simplektične integracijske metode
- numerični eksperimemnti

Ime predmeta: **KAOTIČNI DINAMIČNI SISTEMI**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz področja kaotičnih dinamičnih sistemov, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja

- Enodimenzionalni dinamični sistemi (osnovne definicije, strukturna stabilnost, izrek Šarkovskega, teorija bifurkacij, homoklinične točke, teorija gnetenja).
- Večdimenzionalni dinamični sistemi (atraktorji, Hopfova bifurkacija, Henonova preslikava).
- Juliajeva množica, Mandelbrotova množica.

Ime predmeta: **KARAKTERJI KONČNIH GRUP**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz teorije karakterjev končnih grup, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja

- algebre, moduli in predstavitve;
- karakterji grup;
- tenzorski produkt;
- inducirani karakterji;
- Frobeniusov ter Burnsidov izrek.

Ime predmeta: **KOMBINIRANE METODE ZA KVANTNO-KLASIČNE SIMULACIJE**
Število ECTS kreditnih točk: **9**

Vsebina:

- Osnove kvantne mehanike
- Ab-initio kvantno-kemijske metode
- Teorija gostotnih funkcionalov
- Kohn-Shamova teorija
- Obravnava atomov in molekul
- Osnove klasične mehanike
- Teorija potencialnega polja
- Metode za QM/MM simulacije
- Uporaba metod za kombinirane kvantno-klasične simulacije

Ime predmeta: **MATEMATIČNA MODELIRANJA**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz teorije matematičnega modeliranja, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja

- Optimizacija (Minimum, maksimum in sedlo. Taylorjeva formula za skalarna polja. Tip stacionarne točke. Vezani ekstremi. Diskretna verižnica. Newtonova metoda. Metoda zveznega nadaljevanja. Ravnotežje paličja.)
- Variacijski račun (Standardna variacijska naloga. Izoperimetrični problem. Nihanje paličja. Rotirajoča os. Oblika rotirajoče vrvi.)
- Torzija (Navierjeve enačbe. Obremenitev na nateg.)
- Statistika (Test $\chi 2$. Nepristransko ocenjevanje. Statistične simulacije.)
- Kombinatorična optimizacija (Optimizacijske naloge. Transportna naloga. Najkrajša pot po grafu. Naloga o maksimalnem pretoku. Naloga o trgovskem potniku. Kombinatorična optimizacija.)
- Linearno programiranje (Linearni program. Umetna krmila. Žaganje debel. Nestandardne oblike lineranih programov. Terminologija. Kombinatorična narava linearnega programiranja. Metoda simpleksov.
- Žaganje (Formulacija naloge. Algoritem. Problem nahrbtnika.)
- Teorija dualnosti (Definicija dualnosti. Izrek o dualnosti. Optimalnost metode simpleksov.)

- Algebraična teorija grafov (Pojem grafa. Omrežje. Izrek o podprostorih. Cikli in kocikli. Dimenzije podprostorov C in K. Baza v K. Reševanje enačbe $Ax=\chi$. Baza v C.)
- Out of Kilter (Naloga. Redukcija na krožne tokove. Dualnost. Mintyjev izrek.)

Ime predmeta: **MATEMATIČNE FINANCE V ZVEZNEM ČASU**
Število ECTS kreditnih točk: **9**

Vsebina:
Stohastični integrali.
- Brownovo gibanje.
- Martingali v zveznem času.
- Stohastični integral, Itôva izometrija.
- Itôva formula.
- Izrek Girsanova.
- Stohastične diferencialne enačbe.

Vrednotenje z arbitražo
- Modeli za gibanje cen vrednostnih papirjev.
- Izvedeni zahtevki.
- Opcije in Black-Sholesova formula.
- Nastanovitnost.
- Ameriške opcije

Popolnost trgov.
- Popolnost trgov.
- Popolnost Black-Sholesovega modela.

Nepopolni trgi.
- Definicije in primeri.
- Pojem dosegljivosti.
- Vrednotenje z dominacijo.

Modeli obrestnih mer.
- Pomen stohastičnega modeliranja.
- Osnovni modeli za trenutne obrestne mere.
- Opcije na obrestne mere.

Ime predmeta: **MATEMATIČNE VSEBINE V TUJEM JEZIKU**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz področja matematike, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja
- algebra,
- analiza,
- diskretna matematika,
- finančna matematika,
- kriptografija,
- računsko intenzivne metode in aplikacije,
- statistika.

Ime predmeta: **METODE ZA SIMULACIJE MOLEKULSKE DINAMIKE**
Število ECTS kreditnih točk: **9**

Vsebina:
- Modeli za molekulske simulacije
- Newtonova dinamika
- Hamiltonska dinamika
- Klasifikacija dinamičnih sistemov
- Numerične integracijske metode in algoritmi
- Liejev formalizem
- Simplektične metode za simulacije molekulske dinamike
- Simulacije molekulske dinamike pri konstatni temperaturi in pritisku
- Obravnava statičnih lastnosti molekulskih sistemov
- Obravnava dinamičnih lastnosti molekulskih sistemov
- Uporaba metod za simulacijo molekulske dinamike

Ime predmeta: **MOLEKULARNA GRAFIKA**
Število ECTS kreditnih točk: **9**

Vsebina:
- Pregled računalniških sistemov za molekularno modeliranje
- Pregled računalniške grafike
- Molekulska vizualizacija
- Geometrijska optimizacija
- Moderni računalniški programi za molekularno grafiko
- Grafična manipulacija molekul in molekulskih sistemov

Ime predmeta: **SIMETRIJA IN PREHODNOST NA GRAFIH**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz področja simetrij in prehodnosti na grafih. L.Lovasz (1969) se je vprašal ali ima vsak povezan točkovno tranzitiven graf Hamilonsko pot. Seznanili se bomo s tem se vedno odprtim problemom, ki povezuje navidez nepovezana pojma simetrije in prehodnosti grafov. Posebej se bomo dotaknili naslednjih tem:
- Problem potujočega trgovskega potnika: zgodovinski zorni kot.
- Hamiltonskost točkovno tanzitivnih grafov nekaterih posebnih redov.
- Hamiltonskost Cayleyevih grafov.
- Hamiltonskost kubičnih grafov
- Problem Lovasza: poskus pogleda v prihodnost.

Ime predmeta: **STOHASTIČNI PROCESI**
Število ECTS kreditnih točk: **9**

Vsebina:
- Markovske verige v diskretnem času, klasifikacija stanj, krepka lastnost Markova, verjetnosti zadetka, ergodične lastnosti.

- Markovske verige v zveznem času: definicije, krepka lastnost Markova, leve in desne enačbe, procesi rojevanja in umiranja, procesi razvejanja, ergodijske lastnosti, uporabe.
- Brownovo gibanje: konstrukcija Brownovega gibanja, lastnosti trajektorij, markovska lastnost, princip zrcaljenja, martingali povezani z Brownovim gibanjem.
- Poissonovi procesi: abstraktne definicije, transformacije Poissonovih procesov, teorija ekskurzij.

Ime predmeta: **TEORIJA IGER**
Število ECTS kreditnih točk: **9**

Vsebina:
- Problemi odločanja v strateških situacijah.
- Osnovni koncepti teorije iger: igralci, poteze, zaslužek, matrična igra z dvema igralcema.
- Igre v normalni obliki: dominirane poteze, najboljši odgovor, Nashevo ravnovesje, mešane poteze, obstoj Nashevega ravnovesja, pomembni primeri.
- Igre v normalni obliki v praksi: modeliranje, odločanje ljudi.
- Dinamične igre, igre v razvejeni obliki: strategije, Nashevo ravnovesje, povratna indukcija, podigre, popolno ravnovesje podiger, pomembni primeri.
- Ponavljane igre: neskončno ponavljanje, končno ponavljanje, Ljudski izrek.
- Dinamične igre v praksi: razlike med teorijo in človeškim odločanjem.
- Odločanje brez skupnega znanja: dinamične igre z nepopolno informacijo, sekvenčno ravnovesje.
- Evolucijska teorija iger.

Ime predmeta: **TEORIJA KODIRANJA**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz teorije kodiranja, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja
- matematične osnove (grupe, kolobarji, ideali, vektorski prostori, končni obsegi)
- osnovni pojmi iz teorije kodiranja
- algebraične metode za konstrukcijo kod za popravljanje napak
- Hammingove kode
- Linearne kode
- Binarne Golayeve kode
- Ciklične kode
- BCH kode
- Reed-Solomonove kode
- meje (Hammingova meja, Singletonova meja, Johnsonova meja, ...)

Ime predmeta: **TEORIJA KONČNIH OBSEGOV**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz teorije končnih obsegov, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja:
- Struktura končnih polj

- Polinomi nad končnimi polji
- Faktorizacija polinomov
- Enačbe nad končnimi polji
- Uporaba končnih polj.

Ime predmeta: **TEORIJA MERE**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz teorije mere, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja:

- Koncept merljivosti. σ-algebra merljivih množic. Merljive funkcije. Borelove množice in Borelovo merljive funkcije. Merljivost limitnih funkcij. Enostavne funkcije.
- Integral nenegativnih merljivih funkcij in kompleksnih merljivih funkcij.. Fatou-jeva lema. Lebesgue-ov izrek o monotoni in dominantni konvergenci. Vpliv množic z mero nič in koncept enakosti skoraj povsod. Lp prostori.
- Pozitivne Borelove mere. Nosilec funkcije. Rieszov izrek o reprezentaciji pozitivnega linearnega funkcionala na algebri zveznih funkcij z integralom. Regularnost Borelovih mer. Lebesgue-ova mera.
- Aproksimacija merljivih funkcij z zveznimi. Lusinov izrek
- Kompleksne mere. Totalna variacija. Absolutna zveznost. Lebesgue-Radon-Nikodym-ov izrek. Lp prostori kot refleksivni Banachovi prostori.
- Diferenciabilnost mer in simetrični odvod mere. Absolutno zvezne funkcije in osnovni integralski izrek. Izrek o vpeljavi novih spremenljivk.
- Produktne mere in Fubinnijev izrek. Napolnitev produktnih Lebesgue-ovih mer.

Ime predmeta: **TEORIJA PERMUTACIJSKIH GRUP**
Število ECTS kreditnih točk: **9**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz teorije permutacijskih grup, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja:

- delovanja grup;
- orbite in stabilizatorji;
- razširitev do večkratne tranzitiv-nosti;
- primitivnost in neprimitivnost.
- permutacijske grupe in grafi.
- avtomorfizmi grafov, Cayleyevi grafi.
- grafi z visoko stopnjo simetrije.
- permutacijske grupe in dizajni.

Ime predmeta: **UVOD V KRIPTOGRAFIJO JAVNIH KLJUČEV**
Število ECTS kreditnih točk: **9**

Vsebina:
Leta 1976 sta Diffie in Hellman predstavila koncept kriptografije javnih ključev, ki predstavlja nenadomestljivo orodje za poenostavitev upravljanja ključev ter realizacijo varne komunikacije.

Od takrat naprej smo priča izrednemu povečanju aktivnosti na tem področju (prej pa so bile aktivnosti običajno omejene na tako imenovane črne kabinete).
Kriptografske tehnike javnih ključev uporabljamo danes pri elektronski pošti, faksih, za zaščito proti virusom, pri elektronskem denarju, protokolih za internet, brezžičnih telefonih, kabelski televiziji, če omenimo samo nekaj primerov uporabe. Na vseh področjih komunikacij nastajajo standardi za kriptografsko zaščito (na primer IEEE, ANSI, ISO, IETF in ATM Forum).

Večina kriptografskih sistemov je zasnovana na teoriji števil, povzročila pa je tudi odkritja novih algoritmov za stare probleme. Na tem tečaju bomo preučevali te nove algoritme teorije števil. Pri preučevanju varnosti oziroma pri napadih na kriptografske protokole pa pogosto uporabljamo statistične principe. Spoznali bomo nekaj najbolj zvitih algoritmov in elegantne matematike nasploh. Namen tega tečaja je splošen uvod v kriptografijo javnih ključev in njeno zgodovino ter osvetlitev njenih pomembnejših dosežkov v zadnjih dvajsetih letih. Obravnavali bomo čim več tem z naslednjega seznama:

- koncept kriptografije javnih ključev
- končni obsegi, razširjen Evklidov algoritem
- javni kriptosistemi, enosmerne funkcije in z njimi povezani problemi iz teorije števil (testiranje praštevilskosti, faktorizacija števil, diskretni logaritem)
- digitalni podpisi
- zgoščevalne funkcije in celovitost (integriteta) podatkov
- protokoli za izmenjavo ključev in za identifikacijo.

Ime predmeta: **UVOD V KRIPTOGRAFIJO SIMETRIČNIH ŠIFER**
Število ECTS kreditnih točk: **9**

Vsebina:
Kriptografija ima dolgo in vznemirljivo zgodovino. Sledi prve uporabe segajo v Egipt pred 4000 leti. V današnjem času pa je postala moderna znanost, ki se opira na številne druge discipline kot so teorija informacij, računalništvo, diskretna matematika, teorija števil, itd. V moderni družbi je izmenjava in hranjenje informacij, ki ju opravimo učinkovito, zanesljivo in varno, osrednjega pomena.

Kriptologijo sestavljata prepleteni področji kriptografije in kriptoanalize. Kriptografske kode in šifre se uporabljajo za zaščito informacij pred branjem/snemanjem, nepooblašenim spreminjanjem in drugimi nezaželjenimi uporabami.

Po drugi strani pa kriptoanaliza preučuje / odkriva šibkosti kriptografskih sistemov. Varna komunikacija bo osrednjega pomena za Internet in mobilno komunikacijo, če hočemo realizirati ves njun potencial in omogočiti prenos občutljivih podatkov, npr. pri plačilnih sistemih, e-trgovanju, zdravstvenih sistemih itd. Kriptologija torej postaja vedno bolj pomembna tako za gospodarstvo kakor tudi za celotno družbo.

Šifrirna tehnika tekočih šifer predstavlja le del širšega razreda šifer s simetričnimi ključi, ki vsebuje tudi bločne šifre. Medtem, ko je pri bločnih šifrah vnaprej določeno število zaporednih simbolov čistopisa za šifriranih kot en blok, je pri tekočih šifrah vsak simbol čistopisa za šifriran ločeno. Znamenita moderna bločna šifra je AES (Advanced Encryption Standard), ki jo je ameriška vlada leta 2002 sprejela za standard in predstavlja varnostno močnejše nadomestilo za DES.

AES je nastal na iniciativo ameriškega NIST-a (National Institute of Standards and Technology), ki je leta 1997 naredil razpis za predloge novih šifer za standard. Podobno iniciativo za tekoče

šifre je izpeljala ECRYPT Stream Cipher Project, ki predstavlja večletni napor, da se identificira nova tekoča šifra, ki bo primerna za široko uporabo.

Pri tem predmetu bodo slušatelji pridobili poglobljeno znanje varnostne analize ter načrtovanja modernih šifer s simetričnimi ključi. Obravnavali bomo naslednje teme:

- zgodovina razvoja gradnikov šifer s simetričnimi ključi,
- fundamentalna logika načrtovanja bločnih in tekočih šifer,
- načini uporabe simetričnih šifer,
- kriptografski kriteriji šifrirnih shem,
- ocenjevanje varnosti in generični napadi,
- osnovni konstrukcijski bloki gradnikov šifer s simetričnimi ključi,
- sodobne (``State-of-art'') šifre in njihova varnost.

Ime predmeta: **VERJETNOSTNI RAČUN**
Število ECTS kreditnih točk: **9**

Vsebina:

- Izidi, dogodki, σ-algebre (Množica vseh možnih izidov. σ-algebre dogodkov, verjetnostne mere. Sistemi dogodkov, Dynkinova lema. Neodvisnost dogodkov in sistemov dogodkov.)
- Porazdelitve kot mere (Porazdelitev kot prenos verjetnostne mere. Diskretnost, gostota porazdelitve. Funkcije slučajnih spremenljivk. Večrazsežne porazdelitve, robne porazdelitve, neodvisnost.)
- Pričakovana vrednost (Pričakovana vrednost kot abstraktni integral. Pričakovana vrednost kot integral po porazdelitvi. Varianca in kovarianca.)
- Pogojna pričakovana vrednost (Pogojevanje na dogodke in diskretne slučajne spremenljivke. Pogojevanje na splošne slučajne spremenljivke in σ-algebre, obstoj. Lastnosti pogojne pričakovane vrednosti. Pogojna porazdelitev. Pogojni izrek o monotoni in dominirani konvergenci.)
- Transformacije slučajnih spremenljivk: Rodovne funkcije. Karakteristične funkcije, izrek o edinosti.
- Konvergenca slučajnih spremenljivk (Vrste konvergenc in povezave med njimi. Prva in druga Borel-Cantellijeva lema. Zakoni velikih števil. Konvergenca v porazdelitvi. Aproksimacija porazdelitev.)
- Martingali (Definicije in osnovne lastnosti. Izrek o opcijskem ustavljanju. Konvergenca martingalov. Maksimalne neenakosti.)

Ime predmeta: **VERJETNOST Z MERO (1)**
Število ECTS kreditnih točk: **9**

Vsebina:

Osnovni pojmi teorije mere

- Motivacija pojma mere, σ-algebre, konstrukcija mer.
- Merljive funkcije, Lebesgueov integral, konvergenčni izreki.
- L^p - prostori.
- Produktne mere, Fubinijev izrek.
- Radón-Nikodýmov izrek.

Verjetnostni prostori in slučajne spremenljivke

- Aksiomatska definicija verjetnosti.

- Slučajne spremenljivke in njihove porazdelitve.
- Neodvisnost slučajnih spremenljivk.

Matematično upanje
- Abstraktna definicija matematičnega upanja.
- Varianca, kovarianca.

Ime predmeta: **VERJETNOST Z MERO (2)**
Število ECTS kreditnih točk: **9**

Vsebina:
Pogojno matematično upanje in pogojne porazdelitve
- Abstraktna definicija pogojnega upanja, lastnosti.
- Obstoj pogojnega matematičnega upanja v splošnem.
- Primeri izračuna pogojnega matematičnega upanja.
- Pogojne porazdelitve.

Transformacije porazdelitev
- Rodovne funkcije.
- Proces razvejanja.
- Karakteristične funkcije.

Aproksimacija porazdelitev
- Tipi konvergence slučajnih spremenljivk.
- Šibki izreki velikih števil.
- Krepki izreki velikih števil.
- Konvergenca v porazdelitvi,
- Normalna aproksimacija.
- Poissonova aproksimacija.

Ime predmeta: **RAČUNALNIŠKA VARNOST**
Število ECTS kreditnih točk: **9**

Vsebina
- Uvod in osnovne definicije.
- Simetrični tajnopisni sistemi in asimetrični tajnospisni sistemi.
- Kriptografski protokoli in uvod v formalne metode.
- Infrastruktura javnih ključev.
- Elementi celovite varnostne infrastrukture (obrambni zidovi, sistemi za detekcijo vdorov, protokoli SSL, IPSec, in SET).
- Obvladovanje človeškega dejavnika (organizacijski in zakonski vidiki).