PODIPLOMSKI ŠTUDIJSKI PROGRAM 2. STOPNJE MATEMATIČNE ZNANOSTI
OPISI PREDMETOV

TEMELJNI PREDMETI ŠTUDIJSKEGA PROGRAMA

Ime predmeta: **IZBRANA POGLAVJA IZ ALGEBRE (1)**
Število ECTS kreditnih točk: **6**

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: **6**

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: **6**

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,
- Teorija velikih omrežij in analiza,
- Učenje na omrežjih,
- Slučajni sprehodi na grafih,
- Svetovni splet kot graf.

Ime predmeta: **IZBRANA POGLAVJA IZ FINANČNE MATEMATIKE (1)**
Število ECTS kreditnih točk: **6**

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: **6**

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: **6**

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: **6**

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: **6**

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.

Ime predmeta: **MATEMATIČNI PRAKTIKUM**
Število ECTS kreditnih točk: **6**

Vsebina:
Pokrite bodo vsebine, ki spadajo med spodaj naštete:

1. Wolfram Mathematica
- osnove programa, elementarni izračuni, grafi funkcij,
- reševanje standardnih problemov iz analize, linearne algebre, diferencialnih enačb itd.
- risanje (ekplicitne, implicitne, parametrične prezentacije objektov),

- ustvarjanje interaktivnih in dinamičnih risb.
- grafična predstavitev rešitev NDE in PDE.
- izbrana poglavja.

2. MATLAB oziroma Octave
- osnove programa
- vgrajene funkcije
- delo z matrikami
- uvažanje in izvažanje podatkov med MATLABom/Octavom in ostalimi formati
- vizualizacija (risanje različnih objektov)
- programiranje (pisanje funkcij)
- obravnava napak
- Orodja v MATLABu
- reševanje realnih problemov z MATLABom ali Octavom

3. Blender
- osnove programa
- spoznavanje uporabniškega vmesnika
- 3D modeliranje
- osnove animacije
- pretvorbe v video

OBVEZNI PREDMETI

Ime predmeta: **SEMINAR (1. LETNIK)**
Število ECTS kreditnih točk: **12**

Vsebina:
Pri seminarju bodo študenti samostojno študirali poglavja in članke na področjih, ki jih bo določil izvajalec. Vsebino poglavij in člankov bodo morali predstaviti v obliki seminarja pred izvajalcem predmeta in ostalimi študenti in oddati seminarsko delo v zaključeni pisni obliki.

Ime predmeta: **SEMINAR (2. LETNIK)**
Število ECTS kreditnih točk: **12**

Vsebina:
Pri seminarju bodo študenti samostojno študirali poglavja in članke na področjih, ki jih bo določil izvajalec. Vsebino poglavij in člankov bodo morali predstaviti v obliki seminarja pred izvajalcem predmeta in ostalimi študenti in oddati seminarsko delo v zaključeni pisni obliki. Študenti bodo na seminarju predstavili temo svoje načrtovane magistrske naloge. Poudarek bo na izboljšanju komunikacije raziskovalnih rezultatov, pripravi predstavitve (v Beamerju) ki bo vsebovala več vizualnih predstavitvah, grafov, tabel ipd.

Ime predmeta: **MAGISTRSKO DELO (PRIPRAVA IN ZAGOVOR)**
Število ECTS kreditnih točk: **24**

Vsebina:
Celovita obravnava vsebine izbranega predmetnega področja študijskega programa druge stopnje in/ali interdisciplinarna povezava z drugimi predmetnimi področji.

Študenti izberejo temo glede na njihove interese in v dogovoru z mentorjem, predmetnim področjem, s katerim se želijo podrobneje ukvarjati.

Dolžina naloge je točno navedena v fakultetnem pravilniku, ki ureja to področje.

Z izdelavo magistrske naloge študent razvije raziskovalne metode: ustreznost teme, razvoj delovnega načrta, oblikovanje ciljev in hipotez, dokumentarnega in bibliografskega iskanja, vzpostavitev strukture raziskave itd. in se izkaže poznavanje, izbira in aplikacija ustreznih teoretskih podlag.

IZBIRNI PREDMETI

Ime predmeta: **ALGEBRAIČNA KOMBINATORIKA**
Število ECTS kreditnih točk: **6**

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: **6**

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: **FILOZOFIJA**
Število ECTS kreditnih točk: **3**

Vsebina:
- Izhodišča zahodne filozofske misli: vzroki za nastanek filozofije v antični Grčiji; glavne značilnosti filozofije in razlike med filozofijo, religijo in znanostjo ter med zahodno filozofijo in azijskimi in drugimi refleksijami o svetu in človeku; različnost glavnih zahodnih filozofskih in kulturnih tradicij. **Kaj je filozofija?**
- *Antika:* Izhodišča antične kulture; predsokratiki, Sokrat, Platon, Aristotel in helenizem. **Doktrina biti in teorija vednosti.**
- *Srednji vek, renesansa in humanizem:* Družbena in idejna izhodišča srednjega veka in njegov zgodovinski okvir. Avrelij Avguštin, Tomaž Akvinski in pozna sholastika. Nikolaj Kopernik, Johannes Kepler, Francis Bacon, Erazem Rotterdamski in Michel de Montaigne. **Zgodovinski tipi filozofije.**
- *Novoveška filozofija in razsvetljenstvo:* René Descartes, Thomas Hobbes in David Hume. Filozofski in zgodovinski temelji razsvetljenstva ter njegove družbene posledice: Voltaire, Jean-Jacques Rousseau in Immanuel Kant. **Socialna filozofija.**
- *Romantika in 19. stoletje:* Pomen umetnosti in kulture; nacionalna kultura. G.W.F. Hegel, Arthur Schopenhauer; August Comte; Karl Marx; Friedrich Nietzsche. **Filozofska aksiologija in antropologija.**
- Filozofski in kulturni tokovi 20. stoletja: eksistencialna fenomenologija (Martin Heidegger in Maurice Merleau-Ponty) in eksistencializem (Jean-Paul Sartre); psihoanaliza in nadrealizem. Logika in analitična filozofija (Ludwig Wittgenstein). Frankfurtska šola; hermenevtika; strukturalizem. Karl Popper in njegovi kritiki. **Filozofija in znanost.**

Ime predmeta: **FINANCIRANJE ZDRAVSTVENEGA VARSTVA**
Število ECTS kreditnih točk: **6**

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: **GEOMETRIJA IN TOPOLOGIJA**
Število ECTS kreditnih točk: **3**

Vsebina:
Geometrija in topologija mnogoterosti:
i) splošna topologija (odprta in zaprta podmnožica, povezljivost, aksiomi ločljivosti, kompaktnost);
ii) topološke mnogoterosti, gladke mnogoterosti, gladke funkcije in preslikave;
iii) Tangentni vektor, tangentni prostor, diferencial; regularne preslikave
iv) Lokalna struktura regularnih preslikav, vložitve, Whitneyov izrek;
v) Orientacija in usmerjenost;
vi) Klasifikacija 2-dimenzionalnih zaprtih mnogoterosti;
vii) Tenzorska algebra;
viii) Diferencialne forme;
ix) De Rham cohomologije;
x) Affina povezanost, kovariantni odvod, vzporedni transport, geodeziki;
xi) Riemanova geometrija.

Ime predmeta: **GEOMETRIJSKA TEORIJA MERE**
Število ECTS kreditnih točk: **3**

Vsebina:
- Pozitivne mere na sigma algebrah: Pregled/ponovitev lastnosti merljivih množic in pozitivnih mer. Napolnitev mere/sigma algebre. Borelova sigma algebra
- Caratheodoryjeve zunanje mere, Borelova mera, regularne mere, Lebesgueova mera: Caratheodoryjev izrek, Lebesgue-Stieltjesove mere in naraščajoče desno-zvezne funkcije
- Merljjive funkcije: Pregled/ponovitev lastnosti merljivih funkcij
- Lebesgueov integral, Fubinijev izrek: Pregled/ponovitev lastnosti Lebesgueovega integrala pozitivne/kompleksne funkcije. Produktna mera in Fubinijev izrek. Večrazsežna Lebesgueova mera
- Izreki o pokritjih: Vitalijev in Besicovitchev izrek
- Odvodi mer: odvod kompleksne mere v točki glede na Lebesgueovo mero; funkcije z omejeno varianco; absolutno zvezne funkcije; Newton–Leibnizova formula
- Hausdorffova mera in Hausdorffova dimenzija: osnovne lastnosti, povezava med Hausdorffovo in Lebesgueovo mero
- Lipschitzove preslikave: osnovne lastnosti, povezava s Hausdorffovo mero
- Daniellov integral: konstrukcija mere s pomočjo integrala

Ime predmeta: **GEOMETRIJSKI ASPEKTI DISKRETNIH DINAMIČNIH SISTEMOV**
Število ECTS kreditnih točk: **6**

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

1. Osnove diskretne dinamike. Diferenčne enačbe. Logistična enačba. Klasifikacija fiksnih točk. Linearizacija in izrek Hartman Grobman. Funkcija Ljapunova in eksponent Ljapunova, Stabilna in nestabilna mnogoterost.
2. Podvajanje period in kaos. Hiperbolični sistemi in Arnoldova mačka. Heteroklinične orbite in Smalova podkev.

3. Polinomska iteracija v kompleksni ravnini in na Riemannovi sferi. Juliajeva, Fatoujeva in Mandelbrotova množica. Fatou-Bieberbachova območja.
4.Morsova teorija, nedegenerirane kritične točke, gradientni tok in topologija nivojnic. Mnogoterosti kot CW kompleksi, kompleksne mnogoterosti, Steinove mnogoterosti in njihova CW struktura.
5.Riemannove mnogoterosti, povezave in geodetke. Ukrivljenostni tenzor, sekcijska in Riccijeva ukrivljenost, geodezični tok.

Ime predmeta: **GEOMETRIJSKI OPTIMIZACIJSKI PROBLEMI**
Število ECTS kreditnih točk: **3**

Vsebina:
(1) Teorija grafov. Drevesa, vpeta drevesa, Kirchhoff-ov izrek, minimalna vpeta drevesa, Kruskal-ov algoritem.

(2) Problem dosegljivosti in problem najkrajših poti, algebraični pristop. Idempotentni pol-kolobarji, induktivno urejene množice, Izrek o fiksni točki, Zaprti pol-kolobarji, linearne enačbe v pol-kolobarjih, uporaba pri problemih optimizacije v grafih.

3) Euklidska minimalna vpeta drevesa, Delaunay-eve triangulacije in Voronoi-evi diagrami.

(4) Najkrajša drevesa v euklidski ravnini. Fermat-ov problem. Lokalna struktura, Melzak-Weng-ov algoritem. Gilbert-Pollack-ova domneva in Steiner-jevo razmerje.

(5) Relacije med možnimi strukturami minimalnih mrež in “boundary set geometry”.

(6) Ravninski grafi. Izrek Pontryagin-Kuratowskii, Wagner-jev izrek. Linearne vložitve z danimi koti.

Ime predmeta: **GRUPE, KROVI IN ZEMLJEVIDI**
Število ECTS kreditnih točk: **6**

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: **6**

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 PARCIALNIH DIFERENCIALNIH ENAČB**
Število ECTS kreditnih točk: **6**

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

- Parcialne diferencialne enačbe (Parcialne diferencialne enačbe 1. reda in metoda karakteristik, Valovna enačba v eni in dveh krajevnih spremenljivkah. Fourierева metoda. D'Alembertova rešitev. Toplotna enačba in toplotno jedro. Laplaceova enačba v dveh dimenzijah. Fourierева metoda. Klasifikacija parcialnih diferencialnih enačb drugega reda.)
- Distribucije (definicija, primeri distribucij, reševanje DE in PDE z distribucijami)

Ime predmeta: **IZBRANA POGLAVJA IZ DINAMIČNIH SISTEMOV**
Število ECTS kreditnih točk: **6**

Vsebina:
1. Linearni in nelinearni sistemi, osnovni izreki o enoličnosti in eksistenci, maksimalni interval eksistence, reparametrizacija, odvisnost od parametrov.

2. Fazni portreti avtonomnih sistemov, klasifikacija kritičnih točk, teorija stabilnosti, metoda Ljapunova, periodične rešitve v ravnini, nehiperbolične točke analitičnih sistemov v ravnini, kritične točke Hamiltonskih sistemov.

Ime predmeta: **IZBRANA POGLAVJA IZ DISKRETNE MATEMATIKE (2)**
Število ECTS kreditnih točk: **6**

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

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

Ime predmeta: **IZBRANA POGLAVJA IZ KOMPLEKSNE ANALIZE**
Število ECTS kreditnih točk: **6**

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

- Holomorfne, harmonične, subharmonične funkcije (Cauchyjeva formula za holomorfne in neholomorfne funkcije. Taylorjeva in Laurentova vrsta, Izrek o ostankih, Schwarzeva lema, Avtomorfizmi diska. Konvergenca v prostoru holomorfnih funkcij Normalne družine in Montelov izrek. Hurwitzev izrek. Riemannov upodobitveni izrek. Princip zrcaljenja. Konvergenca produktov. Weierstrassov faktorizacijski izrek. Rungejev izrek.Mittag-Lefflerjev izrek. Interpolacija. Harmonične in subharmonične funkcije. Laplacov operator. Poissonovo jedro in rešitev Dirichletovega problema na krogu.)
- Holomorfne funkcije več spremenljivk (definicija in zgledi, Reinhardtova območja in Hartogsov izrek, analitična nadaljevanja, holomorfna konveksnost in aproksimacija s celimi funkcijami)

Ime predmeta: **IZBRANA POGLAVJA IZ MATEMATIČNE STATISTIKE (2)**
Število ECTS kreditnih točk: **6**

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: **6**

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

- Aproksimacija funkcij.
- Numerično reševanje navadnih diferencialnih enačb.
- Numerično reševanje parcialnih diferencialnih enačb.
- Numerična optimizacija.
- Numerično reševanje velikih linearnih sistemov in računanje lastnih vrednosti velikih sistemov.
- Bezierove krivulje in ploskve.

Ime predmeta: **IZBRANA POGLAVJA IZ TEORIJE ASOCIATIVNIH SHEM**
Število ECTS kreditnih točk: **6**

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 TEORIJE KONČNIH GEOMETRIJ**
Število ECTS kreditnih točk: **6**

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: **6**

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: **6**

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: **6**

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

Ime predmeta: **KAOTIČNI DINAMIČNI SISTEMI**
Število ECTS kreditnih točk: **6**

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: **6**

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: **KOMBINATORIČNE IN KONVEKSNE GEOMETRIJE**
Število ECTS kreditnih točk: **6**

Vsebina:
Predavajo se najpomembnejše raziskovalno aktualne teme iz kombinatorične in konveksne gemetrije, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja
- konveksne množice, ki podpirajo hiperravnine, izreki separacije
- Hellyov izrek in uporabe
- Struktura lic konveksnih politopov, ciklični polytopi
- Euler-Poincarejeva formula, regularni politopi
- Sferično pakiranje, problemi gostote
- Izrek Erdősa in Szekeresa
- Razdelitev ${\ bf R}^d $ s hiperravninami
- Problemi svetlobe, povezava s teorijo kodiranja
- Borsukov problem particije

Ime predmeta: **KOMBINIRANE METODE ZA KVANTNO-KLASIČNE SIMULACIJE**
Število ECTS kreditnih točk: **6**

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: **KRIPTOGRAFSKE RAZPRŠILNE FUNKCIJE IN VERIŽENJE BLOKOV**
Število ECTS kreditnih točk: **6**

Vsebina:
Kriptografske razpršilne (hash) funkcije so uporabni kriptografski primitivi, ki omogočajo učinkovito implementacijo številnih kriptografskih protokolov. Na prvem mestu so obvezna komponenta generiranja tako imenovanega povzetka sporočila, (»message digest«), kar je kompresirana binarna slika fiksne velikosti za dano poljubno sporočilo. Tipična aplikacija, ki vsebuje razpršilne funkcije, je generiranje digitalnih podpisov, ki vežejo podpisano sporočilo na podpisnika. Pred nedavnim so bile razpršilne funkcije deležne velike pozornosti tudi zaradi uporabe v tehnologiji veriženja blokov (blockchain technology) in še posebej pri implementaciji bitcoina.
Cilj predmeta je poglobljeno razumevanje načrtovanja in varnosti razpršilnih funkcij. To vključuje njihovo uporabnost v tako imenovanih MAC (Message authentication Codes), ki so v svojem bistvu razpršilne funkcije s ključem. Na bolj splošnem nivoju si bomo ogledali tudi uporabo razpršilnih funkcij v tehnologiji veriženja blokov.
Vsebino predmeta lahko opišemo s sledečim:
- Glavne lastnosti kriptografskih razpršilnih funkcij
- Splošen model za iterirane/drevesne razpršilne funkcije
- Načrtovalske metode razpršilnih funkcij in aspekti njihove implementacije
- Varnostna analiza razpršilnih funkcij in nekateri splošni kriptoanalitični pristopi
- Moderno načrtovanje razpršilnih funkcij in standardov
- MAC – načrtovanje in varnost

Ime predmeta: **LIEJEVE GRUPE IN LIEJEVE ALGEBRE**
Število ECTS kreditnih točk: **3**

Vsebina:
1. Koncept Liejevih grup, glavni primeri. Liejeve algebra, Liejeva algebra Liejeve grupe.
2. Morfizmi Liejevih grup in inducirani morfizmi Liejevih algeber. Podgrupe. Cartanov izrek.
3. Delovanja Liejevih grup. Izrek o delovanjih. Posledice. Orbite in stabilizatorji.
4. Reprezentacije Liejevih grup, inducirane reprezentacije Liejevih algeber.
5. Godemski izrek. Kvocienti Liejevih grup. Posledice: tranzitivna delovanja, praslika podgrup, presek podgrup.
6. Prvi Liejev izrek.
7. Enoparametrične podgrupe. Eksponentno preslikovanje. Relacije do eksponentnih preslikav skozi diferencialne geometrije.
8. Splošne lastnosti povezanih in enostavno povezanih Liejevih grup. Izrek o enostavno povezani

krovih Liejevih grup.
9. Drugi Liejev izrek.
10. Pol-enostavne Liejeve algebre.
11. Konstrukcija poldirektnih produktov Liejevih grup in Liejevih algeber.
12. Bottov in Gurevichov izrek iz algebraične topologije. Tretji Liejev izrek.
13. Klasifikacija kompaktnih Liejevih grup.

Ime predmeta: **MATEMATIČNA MODELIRANJA**
Število ECTS kreditnih točk: **6**

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: **6**

Vsebina:
Stohastične diferencialne enačbe

- Formulacije in definicija rešitve.
- Obstoj in enoličnost rešitev.

Vrednotenje z arbitražo

- Modeli za gibanje cen vrednostnih papirjev.
- Pogojne terjatve.
- Varovanje v zveznem času.
- Izrek Girsanova in zamenjava mere.
- Izrek o martingalski reprezentaciji.
- Vrednotenje v Black-Sholesovem modelu.
- Grki.
- Ameriške opcije.

Modeli obrestnih mer.

- Osnovni modeli za obrestne mere.
- Opcije na obrestne mere.

Ime predmeta: **MATEMATIČNE VSEBINE V TUJEM JEZIKU**
Število ECTS kreditnih točk: **6**

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: **6**

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: **6**

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: **RAČUNALNIŠKO PODPRTO GEOMETRIJSKO OBLIKOVANJE**
Število ECTS kreditnih točk: **3**

Vsebina:

- Polinomi in zlepki
- Bézierove krivulje
- Bézierove ploskve
- Racionalne Bézierove krivulje in ploskve
- B-zlepki in NURBS-i

- Druge oblike prezentacije krivulj in ploskev v računalniško podprtem geometrijskem oblikovanju

Ime predmeta: **SIMETRIJA IN PREHODNOST NA GRAFIH**
Število ECTS kreditnih točk: **6**

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:

- Kratka ponovitev algebraične teorije grafov in teorije permutacijskih grup
- 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: **6**

Vsebina:
- Predhodna sredstva iz analize, Stieltjesov integral, funkcije s končno totalno variacijo.
- Martingali, izrek o opcijskem ustavljanju, maksimalne neenakosti, Doobova neenakost.
- Brownovo gibanje: konstrukcija Brownovega gibanja, lastnosti trajektorij, markovska lastnost, princip zrcaljenja, martingali povezani z Brownovim gibanjem.
- Itôv integral, Itôva izometrija, lastnosti integrala, Itôva formula, izrek o lokalizaciji, lokalni martingali, kvadratična variacija, posplošitev na splošne integrande.

Ime predmeta: **TEORIJA IGER**
Število ECTS kreditnih točk: **6**

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: **6**

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: **6**

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: **6**

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: **6**

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: **UPRAVLJANJE PROJEKTOV**
Število ECTS kreditnih točk: **3**

Vsebina:
Vsebina predmeta bo sestavljena iz treh vsebinskih sklopov:

Nacionalni in EU programi financiranja temeljnih in aplikativnih raziskav

- Vrste in načini financiranja nacionalnih in mednarodnih projektov
- Iskanje razpisov
- Vključevanje v mednarodne mreže in iskanje partnerjev

Pridobivanje, vodenje in izvajanje projektov

- Projektni cikel
- Projektno vodenje
- Načrtovanje aktivnosti projekta
- Izvedba projekta
- Evalvacija projekta

Od projektne ideje do projekta

- Projektna ideja
- Splošni in specifični cilji
- Aktivnosti
- Projektni partnerji
- Načrt aktivnosti – cilji, trajanje,vključeni partnerji,rezultati, mejniki, odvisnosti
- Gantogram
- Opredelitev stroškov
- Konzorcijske pogodbe projektnih partnerjev

Ime predmeta: **UVOD V KRIPTOGRAFIJO JAVNIH KLJUČEV**
Število ECTS kreditnih točk: **6**

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: **6**

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: **VERJETNOST Z MERO (1)**
Število ECTS kreditnih točk: **6**

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: **6**

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: **VERJETNOSTNI RAČUN**
Število ECTS kreditnih točk: **6**

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: **ZGODOVINA IN METODOLOGIJA PODROČJA**
Število ECTS kreditnih točk: **3**

Vsebina:
1. Predmet zgodovine in metodologije matematike in uporabljenih metod v njem.
   - Problem komunikacije matematičnega znanja, komunikacijskih sredstev (kamnitih gravogramov, pisem, knjig, člankov, blogov, posnetih predavanj itd.), problemi – rešitve. Odprte težave, domneve, aksiomi, definicije, izreke, dokazi.
   - Abstrakcija, logika, osnova matematiko.
   - Kontinuirano in diskretno, dve paradigmi, ki vozita matematiko.

2. Matematika v predgrških civilizacijah.
   - Egipt, Mezopotamija.

3. Matematika antične Grčije.
   - Thales, Pythagoras, Euclid's Elements, Archimedes.
   - Ptolemey, Heron, Diophantus, Pappus.

4. Zgodnja matematika izven Evrope.
   - Kitajska.
   - Japonska.
   - Islam.
   - Indija.
   - Južna Amerika.

5. Matematika v Evropi v srednjem veku in renesansa.
   - Prevod iz arabščine v latinico (12., 13. stoletje). Kubične in kvadratne enačbe.
   - Trigonometrija, logaritmi.

6. Matematika in znanstvena in tehnološka revolucija XVI-XVII. stoletja.
   - Descartes, Bernoulli, Huygens,Fermat, Cavlieri.

7. Rojstvo matematične analize.
   - Newton, Leibniz.

8. Razvoj matematične analize v XVIII. stoletju.
   - Euler.

9. Algebra XVIII. stoletja.
   - Lagrange, Laplace, Vandermonde.

10. Matematika XIX. stoletja.
    - Gauss, Galois ...

11. Matematika XIX-XX. stoletja.
    - Lobachevsky, Chebyshev, Riemann, Hilbert ...
    - Teorija grup.
    - Teorija množic.

12. Matematika v Vzhodni Evropi, Rusiji in USSR.
    - Pomembnost matematikov, ki so pogosto spregledani v zahodnih kurikulumih: Bolyai, Lobachevsky, Chebyshev, Alexandrov, Kolmogorov …

13. Matematika XX. stoletja.
    - Velike težave in njihove rešitve, kot so štiri barvne težave, problem Fermata itd.
    - rojstvo in razvoj izbranih področij matematike, kot so topologija, kombinatorika, teoretična računalništvo itd.
    - Vzpon diskretne paradigme za račun rojstva računalništva in informacijske znanosti, informacijske tehnologije, kodiranja in kriptografije, razumevanja človeškega genoma prek DNK, računalnika, prometa in socialnih omrežij ter logistike.