جمهوری اسلامی ایران

وزارت علوم، تحقیقات و فناوری

شورای عالی برنامه ریزی آموزشی

برنامه درسی

دوره: دکتری

رشته: ریاضی

با زمینه های تخصصی

۱-گراف و ترکیبیات ۲-منطق ریاضی ۳-ریاضیات تصادفی ۴-آنالیز عددی

۵-رمز ۶-کد ۷-ریاضی مالی

گروه برنامه ریزی علوم ریاضی

مصوب جلسه شماره ۸۸۷ مورخ ۱۳۹۶/۰۹/۰۴ شورای عالی برنامه ریزی آموزشی

بسم الله الرّحمن الرّحیم

عنوان برنامه: دوره دکتری رشته ریاضی

با زمینه های تخصصی:۱- گراف و ترکیبیات(تدوین) ۲-منطق ریاضی(تدوین) ۳-ریاضیات تصادفی(تدوین)

۴-آنالیز عددی(بازنگری) ۵-رمز(بازنگری) ۶-کد (تدوین) ۷-ریاضی مالی(تدوین)

۱- برنامه درسی دوره دکتری رشته ریاضی در زمینه های ۱-گراف و ترکیبیات ۲-منطق ریاضی ۳-ریاضیات تصادفی ۴-آنالیز عددی ۵-رمز ۶-کد ۷-ریاضی مالی در جلسه شماره ۸۸۷ مورخ ۱۳۹۶/۰۹/۰۴ شورای عالی برنامه ریزی آموزشی به تصویب رسیده است.

۲ـ برنامه درسی مذکور در سه فصل: مشخصات کلی، جدول واحد های درسی و سرفصل دروس تنظیم شده وبرای تمامی دانشگاه ها ومؤسسه های آموزش عالی و پژوهشی کشور که طبق مقررات مصوب وزارت علوم، تحقیقات و فناوری فعالیت می کنند، برای اجرا ابلاغ می شود.

۳ـ این برنامه درسی از شروع سال تحصیلی ۱۳۹۸ـ۱۳۹۷ به مدت ۵ سال قابل اجراست و پس از آن نیازمند بازنگری می باشد.

مجتبی شریعتی نیاسر

نایب رئیس شورای عالی برنامه‌ریزی آموزشی

عبدالرحیم نوه‌ابراهیم

دبیر شورای عالی برنامه‌ریزی آموزشی

برنامه و سرفصل درس‌های دکترای ریاضی

- ریاضی - زیر برنامه آنالیز (آماده تصویب)
- ریاضی - زیر برنامه جبر
- ریاضی - زیر برنامه هندسه و توپولوژی
- ریاضی - زیر برنامه گراف و ترکیبیات (مصوب)
- ریاضی - زیر برنامه منطق ریاضی (مصوب)
- ریاضی - زیر برنامه ریاضیات تصادفی (مصوب)
- ریاضی - زیر برنامه آنالیز عددی (مصوب)
- ریاضی - زیر برنامه بهینه سازی (آماده تصویب)
- ریاضی - زیر برنامه رمز (مصوب)
- ریاضی - زیر برنامه کد (مصوب)
- ریاضی - زیر برنامه ریاضی مالی (مصوب)
- ریاضی - زیر برنامه معادلات دیفرانسیل و سیتم های دینامیکی

مقررات عمومی برنامه دکترای ریاضی

دانش آموختگان این دوره در هر یک از زمینه‌های تخصصی اخذ شده این رشته با رعایت مقررات برنامه مربوطه در برنامه فعلی **بدون قید زمینه تخصصی** دانش‌آموخته می‌شوند.

کلیه دانشگاه‌هایی که قبلاً مجوز اجرای رشته را به صورت کلی اخذ کرده کماکان می‌توانند با پذیرش دانشجو در تمام کد رشته‌های "ریاضی" نسبت به پذیرش دانشجو اقدام کنند. این دانشگاه‌ها نیز می‌توانند با پذیرش دانشجو در کد رشته‌های "ریاضی" به صورت تجمعی اقدام به پذیرش دانشجو کرده و هر یک از دانشجویان پذیرفته شده را با در نظر گرفتن تخصص اعضای هیأت علمی و امکانات موجود در هر یک از زمینه‌های تخصصی اخذ شده این رشته با رعایت مقررات برنامه مربوطه در برنامه فعلی دانش‌آموخته کنند.

اگر دانشگاهی دریکی از زمینه‌های تخصصی خاص"ریاضی" قبلا مجوز گرفته باشد، در همان زمینه تخصصی می‌تواند کماکان اقدام به پذیرش دانشجو نماید. چنانچه این نوع دانشگاه‌ها تمایل داشته باشند در سایر زمینه های تخصصی رشته"ریاضی" که قبلاً مجوز اجرای آن را نداشته است، با کد رشته محل مجزا دانشجو پذیرد، لازم است که نسبت به اخذ مجوز اجرا اقدام کرده و فقط در صورت احراز شرایط و پس از اخذ مجوز از وزارت عتف نسبت به پذیرش دانشجو با کد رشته محل مختص زمینه تخصصی مربوطه اقدام کنند.

طول دروه و شکل نظام

دوره دکترای ریاضی مطابق با آیین‌نامه جاری دوره‌ی دکترای وزارت عتف است.

تعداد واحدهای دوره

تعداد واحدهای درسی دوره دکترای ریاضی ۳۶ واحد و به قرار زیر است.

درس‌های الزامی:

۶ واحد، شامل دروس اصلی زمینه تخصصی یا زیر زمینه تخصصی با نظر استاد راهنما و دانشکده.

درس‌های تخصصی- انتخابی:

۹ واحد، شامل حداقل یک درس و حداکثر دو درس از جدول شماره ۲ درس‌های تخصصی- انتخابی و حداقل یک درس با نظر استاد راهنما و تأیید گروه از درس‌های انتخابی یکی از دوره‌های تحصیلات تکمیلی مرتبط.

رساله: ۲۱ واحد

دانشجویان دوره دکترای ریاضی با اخذ دست کم ۶ واحد تمام وقت محسوب می‌شوند.

با توجه به پایه‌ای بودن دروس الزامی زمینه‌های تخصصی وتنوع ورودی‌های دوره‌های دکترای ریاضی به پیشنهاد گروه آموزشی مربوط و تصویب دانشگاه این دروس به جای ۳ واحد می‌توانند ۴ واحدی اجرا شوند. در این صورت سقف واحدهای این دوره با این تغییر به ۱۷ واحد درسی و ۱۹ واحد رساله تغییر خواهد یافت.

گروه‌های مجری می‌توانند درس‌های جدیدی را به عنوان درس اختیاری مطابق با روال جاری دانشگاه مصوب و ارایه دهند.

دانشجو در طول تحصیل خود نمی‌تواند بیش از یک درس با عنوان مباحث ویژه اختیار کند.

دانشجو می‌تواند با نظر استاد راهنما یا دانشکده، از مجموعه درس‌های دوره کارشناسی ارشد که قبلا نگذرانده است انتخاب نماید.

دکتری ریاضی

فصل اول

مشخصات دوره دکتری ریاضی – زیر برنامه رمز

مقدمه:

رشته دکتری ریاضی با تخصص رمز یک دوره تحصیلی میان رشته‌ای است که در راستای تربیت دانش‌آموختگانی طراحی شده‌است که بتوانند در عین حال با آگاهی مناسبی از جنبه‌های کاربردی و عملی سامانه‌های رمزنگاری، با تسلط بر مبانی و اصول نظری مرتبط به مدلسازی، طراحی و تحلیل دقیق این سامانه‌ها بپردازند.

هدف:

اهداف اصلی این دوره عبارتند از:

۱. تربیت متخصصین در حوزه رمز با توانایی طراحی، تحلیل و مدلسازی سامانه‌های رمزنگاری با استفاده از دانش نظری پیشرفته و به روز در این رشته.
۲. تامین نیازهای نهادها، سازمان‌ها یا شرکت‌های فعال در این حوزه در سطوح تحلیل، طراحی و توسعه با توجه به الویت‌های کشور
۳. توسعه علم رمز و دستیابی به مرزهای دانش در این رشته با تاکید بر مبانی بنیادی و ریاضی در به روز ترین سطح بین‌المللی آن

کلیات برنامه:

در این برنامه دروسی در دو جدول، شامل درس‌های اصلی(الزامی) دکتری ریاضی زمینه تخصصی رمز (جدول ۱) و درس‌های تخصصی-انتخابی این دوره (جدول ۲) آورده شده‌است.

اخذ حداقل دو درس (۶ واحد) از جدول ۱ الزامی است. اخذ حداقل یک درس و حداکثر دو درس (۶ واحد) از جدول ۲ یا مابقی دروس اخذ شده از جدول ۱ الزامی است. ۳ واحد باقی‌مانده دوره یک درس کاملاً اختیاری است که با نظر استاد راهنما و تائید گروه اخذ خواهد شد.

عنوان دوره: دکترای ریاضی

پیش‌نیاز ورود:

سه درس «الگوریتم و محاسبه»، «نظریه اطلاع و کاربردها» و «رمز۱» از دروس مقطع کارشناسی ارشد رمز، پیش‌نیاز درسی این دوره هستند و انتظار می‌رود دانشجو در مقطع کارشناسی ارشد آنها را گذرانده باشد. در غیر این صورت بنا به تشخیص استاد راهنما و گروه این دروس می‌توانند به عنوان دروس جبرانی و خارج از تعداد واحدهای مصوب دوره اخذ شوند، در این صورت یک نیمسال به سنوات مجاز تحصیلی دانشجو اضافه خواهد شد.

مواد آزمون تخصصی ورودی(کنکور):

سه درس «الگوریتم و محاسبه»، «نظریه اطلاع و کاربرد» و «رمز۱» از مقطع کارشناسی ارشد

فصل دوم

جدول دروس دکتری ریاضی - زیر برنامه رمز

جدول شماره۱: درس‌های اصلی دکتری ریاضی - زیر برنامه رمز

شماره درس	نام درس	تعداد واحد	پیش‌نیاز
۱	رمزنگاری پیشرفته	۳	
۲	پروتکل‌های رمزنگاشتی پیشرفته	۳	
۳	تحلیل رمز متقارن	۳	

جدول۲: درس‌های تخصصی-انتخابی دکتری ریاضی - زیر برنامه رمز

شماره درس	نام درس	تعداد واحد	پیش‌نیاز و هم‌نیازها
۱	رمزنگاری مبتنی بر خم‌های بیضوی	۳	
۲	رمزنگاری مشبکه مبنا	۳	
۳	حریم خصوصی داده	۳	
۴	محاسبات روی داده رمزشده	۳	
۵	ابزارهای رمزنگاشتی در رایانش ابری	۳	
۶	اثبات‌های نا تراوا	۳	
۷	محاسبه امن چندعاملی	۳	
۸	طرح‌های تسهیم راز	۳	
۹	رای‌گیری الکترونیکی	۳	
۱۰	پول‌دیجیتال	۳	
۱۱	مبهم‌سازی برنامه	۳	
۱۲	طرح‌های امضای دیجیتال	۳	
۱۳	رمزنگاری و پیچیدگی محاسبه	۳	
۱۴	تصادفی‌سازی در رمزنگاری	۳	
۱۵	مباحث ویژه در رمزنگاری	۳	

فصل سوم

سر فصل دروس دکتری ریاضی – زیر برنامه رمز

عنوان درس	فارسی	رمزنگاری پیشرفته									
	انگلیسی	Advanced Cryptography									
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز	
پایه		اصلی		تخصصی		اختیاری		۳	۴۸		
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین:		نیاز به اجرای پروژه عملی:									

هدف:مقدمه‌ای بر مفاهیم پایه‌ای رمزنگاری، معرفی مولدهای شبه‌تصادفی و توابع یک‌طرفه، طرح‌های رمزنگاری کلید عمومی

سرفصل‌های درس:

- **مرور و تعریف دقیق مفاهیم پایه‌ای:** فرضیات و مسائل سخت در رمزنگاری، مسئله لگاریتم گسسته، مسئله تجزیه، مسئلهRSA، توابع یک‌طرفه (one-way function)، جایگشت یک‌طرفه (one-way permutation)، جایگشت یک‌طرفه دریچه دار (trapdoor)، توابع شبه‌تصادفی (pseudo-random functions)، مولدهای‌شبه‌تصادفی (pseudo-random generators)، استدلال پیوندی (hybrid argument)
- **مفاهیم پایه‌ای پیشرفته:** تابع یکطرفهclaw-free، تابع یکطرفه enhanced، تابع یکطرفه ضعیف و قوی، قضیه تقویت سختی (hardness amplification) و اثبات آن، تابع hardcore و اثبات وجود آن برای هر تابع یکطرفه، ساخت تابع و جایگشت شبه تصادفی از روی مولد شبه تصادفی به همراه اثبات، تابع یک طرفه جهانی (universal one-way function)، تابع چکیده‌ساز یک طرفه جهانی (universal one-way hash function)
- **مباحث پیشرفته امضای دیجیتال:** تعریف انواع امنیت امضای دیجیتال، طرح امضای دیجیتال Naor-Yung، طرح امضای دیجیتال Dolev-Dwork-Naor
- **مباحث پیشرفته رمزنگاری کلید عمومی:** تعریف امنیتCCA-1، CCA-2،Non-Malleability و ارتباط آنها، طرح مبتنی بر جایگشت یک طرفه دریچه دار، طرح رمز کلید عمومی Naor-Yung با امنیت CCA-1، طرح رمز کلیدعمومی Dolev-Dwork-Naor با امنیت CCA-2، طرح Cramer-Shoup با امنیت در مدلCCA-2 در مدل استاندارد
- **سایر موارد به انتخاب مدرس:** طرح‌های همریخت Pallier و Goldwasser-Micali، سامانه رمزنگاری کلید عمومی آستانه‌ای، سامانه‌های با قابلیت اضافی مانند: رمزنگاری باقابلیت جستجو (PKE with Keyword Search)، رمزنگاری شناسه بنیاد (IBE) ، رمزنگاری ویژگی مبنا (ABE)، رمزنگاری تابعی (FE)

مراجع پیشنهادی

- **Books**

1. O. Goldreich: Foundations of Cryptography: Volume 1, New York, NY: Cambridge University Press, 2006. (Chapters 1-3)

2. O. Goldreich: Foundations of Cryptography: Volume 2, Basic Applications, New York, NY: Cambridge University Press, 2006.Y. Lindell, J. Katz: Introduction to Modern Cryptography, Chapman Hall/CRC, 2007.
3. Jonathan Katz and Yehuda Lindell. 2014. Introduction to Modern Cryptography, Second Edition (2nd ed.). Chapman & Hall/CRC. (Chapters 5-6)

- **Lecture notes**

4. Jonathan Katz. Advanced topics in cryptography.http://www.cs.umd.edu/~jkatz/gradcrypto2/scribes.html
5. 6. Rafael Pass and Abi Shelat. A Course in Cryptography. https://www.cs.cornell.edu/courses/cs4830/2010fa/lecnotes.pdf
6. Shafi Goldwasser and Mihir Bellare. Lecture Notes on Cryptography. https://cseweb.ucsd.edu/~mihir/papers/gb.html

- **Papers**

7. Mihir Bellare, Anand Desai, David Pointcheval, Phillip Rogaway: Relations Among Notions of Security for Public-Key Encryption Schemes. CRYPTO 1998: 26-45.

عنوان درس	فارسی	پروتکل‌های رمزنگاشتی پیشرفته									
	انگلیسی	Advanced Cryptographic Protocols									
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز	
پایه		اصلی		تخصصی		اختیاری		۳	۴۸		
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین:		نیاز به اجرای پروژه عملی:									

هدف: آشنایی با پروتکل‌های مختلف رمزنگاری

سر فصل های درس:

- **پروتکل‌های تعهد(commitment schemes)**: تعریف ویژگی‌های انقیاد (binding) و پنهان سازی (hiding)، طرح‌های تعهد Feldman و Pedersen و اثبات ویژگی‌های آنها
- **اثبات‌های ناتراوا (zero-knowledge proofs)**: تعریف اثبات‌های تعاملی (interactive proofs) و اثبات‌های ناتراوا، اثبات‌های ناتراوای با وارسی کننده صادق (honest verifier) و ارائه چند مثال
- **پرتکل‌های سیگما** (Σ-protocols): تعریف پروتکل سیگما و ارتباط آن با پروتکل‌های اثبات‌های ناتراوا، پروتکل Schnorr، پروتکل Chaum-Pederson ، ترکیب AND و OR پروتکل‌های سیگما
- **پروتکل‌های تبادل کلید**: تعریف پروتکل، یادآوری پروتکل Diffie-Hellman و اثبات امنیت آن، پروتکل تبادل کلید احراز اصالت شده
- **پروتکل‌های احراز هویت**: روش‌های مبتنی بر کلیدواژه (password)، روشهای مبتنی بر چالش-پاسخ (challenge-response)، روش‌های مبتنی بر اثبات ناتروا مانند پروتکل‌های Guillou-Quisquater و Schnorr
- **پروتکل‌های تسهیم راز**: تسهیم راز Shamir، تسهیم راز تصدیق‌پذیر (Verifiable)، پروتکل‌های تسهیم راز تصدیق پذیر Feldman و Pedersen
- **محاسبه امن دوعاملی و چندعاملی**: پروتکل انتقال بی‌اعتنا (oblivious transfer)، پروتکل دوعاملی Yao و پروتکل-های چندعاملی GMW و BGW
- **سایر پروتکل‌ها و مباحث به انتخاب مدرس**: رای-گیری الکترونیکی، حراجی (auction)، امضای قرارداد (contract signing)، پرتاب سکه (coin-tossing)، اثبات امنیت پروتکل‌ها و ...

مراجع پیشنهادی

- **Books**

1. Oded Goldreich. 2006. Foundations of Cryptography: Volume 1. Cambridge University Press, New York, NY, USA. (Chapter 4)

2. Oded Goldreich. 2004. Foundations of Cryptography: Volume 2, Basic Applications. Cambridge University Press, New York, NY, USA. (Chapter7).
3. Berry Schoenmakers, Cryptographic Protocols, 2004, Technische Univer- siteit Eindhoven. (Chapter 5)
4. Carmit Hazay and Yehuda Lindell. Efficient Secure Two-Party Protocols: Techniques and Constructions (1st). 2010, Springer-Verlag New York, Inc., New York, NY, USA. (Chapters 5, 6, 7)

- **Lecture Notes**

1. Shafi Goldwasser and Mihir Bellare. Lecture Notes on Cryptography. https://cseweb.ucsd.edu/~mihir/papers/gb.html

عنوان درس	فارسی	تحلیل رمز متقارن								دروس پیش‌نیاز	تعداد ساعت	تعداد واحد
	انگلیسی	Symmetric Cryptanalysis										
نوع واحد												
پایه		اصلی		تخصصی		اختیاری					۴۸	۳
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی					
حل تمرین:		نیاز به اجرای پروژه عملی:										

هدف:آشنایی با حملات معروف به سامانه‌های رمزنگاری متقارن

سرفصل‌های درس:

- **یادآوری پیش‌نیازها:** مفاهیم اصلی موردنیاز از نظریه میدان‌های متناهی و توابع بولی مانند فرم نرمال جبری، تبدیل Hadamard-Walsh، احتمال و آزمون‌های فرض، ثبات‌های انتقال خطی(LFSR)
- **یادآوری حملات عام:** آزمون های آماری، حمله جستجوی فراگیر (brute-force)، حملات بده‌بستان حافظه-زمان-داده (tome-memory-data tradeoff)، ملاقات در میانه (meet-in-the-middle)، حملات خطی و تفاضلی، الگوریتم Berlekamp-Massey
- **حملات رمزهای جریانی:** تحلیل همبستگی (سریع)، جبری، تحلیل حل و تقسیم، حدس و تعیین، مکعبی (cube)، خطی‌سازی، تمایز
- **حملات رمزهای قالبی:** تحلیل های پیشرفته خطی چندگانه (multiple)، چندبعدی (multidimensional)) و تحلیل-های پیشرفته تفاضلی چندگانه، منقطع (truncated)، بومرنگ (boomerang) و مستطیلی (rectangular)، حملات خطی- تفاضلی (linear-differential)
- **حملات توابع چکیده‌ساز:** حملات بر اساس پارادوکس روز تولد، حملات عمومی مانند چند برخوردی (multi-collision)، herding و long message second preimage، حملات ساختاری مانند حمله Rebound و Biclick.
- **حملات به اولیه‌های مرتبط:** حمله بهطرح های احراز اصالت (MAC) و طرح های رمزنگاری احراز اصالت‌شده (authenticated encryption)
- **مباحث دیگر به انتخاب مدرس:** کاربرد محاسبات کوانتومی در تحلیل رمزهای متقارن، طراحی اولیه‌های متقارن با رویکرد امنیت اثبات‌پذیر و ...

مراجع پیشنهادی

- **Books**

1. Wu, Chuan-Kun, and D. Feng. Boolean Functions and Their Applications in Cryptography. Springer, 2016.
2. A. Joux, Algorithmic Cryptanalysis, Chapman & Hall/CRC, 2009.
3. J. Katz, Introduction to Modern Cryptography, Chapman Hall/CRC, 2007.

4. Kazuo Sakiyama, Li Yang, and Yu Sasaki, Security of Block Ciphers: From Algorithm Design to Hardware Implementation" wiley 2015
5. L R. Knudsen and M. Robshaw, The Block Cipher Companion. Springer, 2011.

- **Theses**

6. Preneel, Bart. Analysis and design of cryptographic hash functions. Diss. PhD thesis, Katholieke Universiteit Leuven, 1993.
7. Mennink, Bart. Provable security of cryptographic hash functions. Diss. University of Bristol, UK, 2013.
8. Lauridsen, Martin Mehl, Christian Rechberger, and Lars Ramkilde Knudsen. Design and Analysis of Symmetric Primitives. Diss. Technical University of DenmarkDanmarks Tekniske Universitet, Department of Applied Mathematics and Computer ScienceInstitut for Matematik og Computer Science, CryptologyKryptologi, 2015.

- **Papers**

9. Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, María Naya-Plasencia: Breaking Symmetric Cryptosystems Using Quantum Period Finding. CRYPTO (2) 2016: 207-237.

عنوان درس	فارسی	رمزنگاری مبتنی بر خم‌های بیضوی									
	انگلیسی	Elliptic Curve Cryptography									
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز	
پایه		اصلی		تخصصی		اختیاری		۳	۴۸		
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین:		نیاز به اجرای پروژه عملی:									

هدف: معرفی خم‌های بیضوی و برخی از مفاهیم مرتبط با آن، مسئله لگاریتم گسسته خم بیضوی، سامانه‌های رمزنگاری بر روی خم بیضوی، زوج‌نگارها و کاربردهای آن در رمزنگاری

سر فصل‌های درس:

- **مفاهیم مرتبط با خم‌های بیضوی:** تعریف خم‌های بیضوی، قانون گروه، j–پایا (j-invariant)، درون‌ریختی‌ها (endomorphisms)
- **خم‌های بیضوی بر روی میدان‌های متناهی:** نقاط تاب(torsion)، درون‌ریختی فروبنیوس(Frobenius)، ساختار گروه و مرتبه گروه، قضیه Hasse، خم‌های super singular، مسئله لگاریتم گسسته خم بیضوی(ECDLP)
- **زوج‌نگارها بر روی خم‌های بیضوی:** نقاط از مرتبه متناهی بر روی خم بیضوی، بخشیاب‌ها(divisors)، زوج‌نگار ویل(Weil pairing)، الگوریتم Miller، زوج‌نگار تیت(Tate pairing)
- **تولید خم‌های بیضوی برای رمزنگاری:** الگوریتم Schoof ، تولید خم‌های زوج‌نگار- پسند (pairing-friendly)
- **مسئله دیفی‌هلمن دوخطی و مسایل مربوطه:** مسئله دیفی‌هلمن دوخطی(BDH)، مسئله دیفی‌هلمن دوخطی کلی(GBDH)، مسئله دیفی‌هلمن دوخطی تصمیمی(DBDH)، مسئله دیفی‌هلمن دوخطی چکیده ساز تصمیمی(DHBDH)
- **کاربردهای زوج‌نگارها در رمزنگاری**
  - طرح‌های رمزنگاری: رمزنگاری شناسه بنیاد(IBE) و تعریف امنیت، IBE سلسه مراتبی(HIBE)، رمزنگاری همریخت BGN
  - پروتکل‌های توافق کلید: پروتکل توافق کلید سه نفره، توافق کلید شناسه بنیاد (identifier-based)
  - طرح‌های امضا: امضای BLS، طرح امضای آستانه‌ای(threshold)، طرح‌های رمز امضا شناسه بنیاد (ID-based signcryption)
- **مباحث دیگر به انتخاب مدرس:** حمله MOV، حمله Frey-Rück، خم‌های غیرعادی(anomalous)، خم‌های ابربیضوی(hyper elliptic)، کاربردهای دیگر از زوج‌نگارها (مانند: امضای گروهی شناسه بنیاد(ID-based group signature)، امضای شناسه بنیاد سلسه مراتبی(HIDS)، طرح چند امضایی(multi-signature)، امضای کل(aggregate)، رمزنگاری کلید عمومی جستجو پذیر (searchable)، رمزنگاری همه‌پخشی (broadcast)

مراجع پیشنهادی

- **Books**

1. S. V. D. Hankerson and A. Menezes: Guide to Elliptic Curve Cryptography, 2004, Springer.
2. J. Hoffstein, J. Pipher and J. H. Silverman: An Introduction to Mathematical Cryptography, 2014, Springer.
3. N. Mrabet, M. Joye: Guide to Pairing-Based Cryptography. Chapman & Hall/CRC (2016).
4. L. Washington: Elliptic Curves: Number Theory and Cryptography, 2nd edition, 2003, Taylor & Francis.

- **Papers**

1. D. Boneh, M. Franklin: Identity-Based Encryption from the Weil Pairing. SIAM J. Comput. 32(3), 586-615 (2003).
2. D. Boneh, H. Shacham, and B. Lynn: Short Signatures from the Weil Pairing. J. Cryptology 17(4), 297-319 (2004).
3. A. Joux: A one Round Protocol for Tripartite Diffie–Hellman. J. Cryptology 17, 263–276 (2004).

عنوان درس	فارسی	رمزنگاری مشبکه مبنا									
	انگلیسی	Lattice-based cryptography									
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز	
پایه		اصلی		تخصصی		اختیاری		۳	۴۸		
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین:						نیاز به اجرای پروژه عملی:					

هدف:آشنایی با مفاهیم و تعاریف اولیه، مسائل محاسباتی مطرح و الگوریتم های رمزنگاری مدرن مشبکه بنیاد

سر فصل‌های درس:

- مقدمات: مروری بر فضاهای برداری و زیرفضا، متعامدسازی و الگوریتم گرام- اشمیت، تعریف مشبکه (lattice)، ماتریس‌های یونی‌مدولار، خواص جبری زیرگروه ماتریس‌های یونی‌مدولار و مولدهای گروه، پایه‌ها و متوازی‌السطوح بنیادین (fundamental parallelepiped)، نامساوی هادامارد، جسم محدّب و قضیهٔ مینکوفسکی، قضیهٔ هرمیت و شهود گاوسی (Gaussian heuristic)
- مسائل محاسباتی در مشبکه: «مسئلهٔ کوتاه‌ترین بردار» در مشبکه (SVP)، «مسئلهٔ نزدیک‌ترین بردار» در مشبکه (CVP)، «مسئلهٔ تقریب کوتاه‌ترین بردار» (SVP)، مسئلهٔ تصمیم‌گیری تقریب کوتاه‌ترین بردار (Gap-SVP)، مسئلهٔ کوتاه‌ترین بردارهای مستقل خطی (SIVP)، مسئلهٔ تقریب کوتاه‌ترین بردارهای مستقل خطی (SIVP)، مسئلهٔ BDD (bounded-distance decoding)، صور دیگر مسائل محاسباتی مشبکه
- الگوریتم‌های کاهش مشبکه، پیچیدگی و کران تقریب آنها: الگوریتم enumeration، الگوریتم LLL، الگوریتم BKZ، الگوریتم Babai
- مشبکه و رمزنگاری: خانوادهٔ توابع یک‌طرفه، خانوادهٔ توابع مقاوم به برخورد (collision resistant)، مفهوم امنیت معنایی (semantic security)، مفاهیم IND-CPA و IND-CCA، رمزنگاری مبتنی بر هویت (IBE)
- الگوهای سنّتی در رمزنگاری مبتنی بر مشبکه: رمزنگاری Ajtai-Dwork، رمزنگاری GGH و امضاهای دیجیتالی، رمزنگاری NTRU و گونه‌های متفاوت آن، رمزنگاری مبتنی بر حلقه‌های چندجمله‌ای
- الگوهای مدرن در رمزنگاری مبتنی بر مشبکه: تشریح مسئلهٔ SIS (shortest integer solution)، تشریح مسئلهٔ LWE (learning with error)، تشریح مسئلهٔ Ring-LWE، تشریح مسئلهٔ تصمیم‌گیری decision R-LWE، خانوادهٔ توابع درهم‌سازی مبتنی بر مشبکه، مطالعهٔ روش‌های رمزنگاری مبتنی بر هویت مشبکه‌مبنا (Lattice-based IBE)، توابع شبه‌تصادفی در مشبکه
- رمزنگاری کاملا همریخت مبتنی بر مشبکه: مفاهیم پایه، رمزنگاری کاملا همریخت مبتنی بر مشبکه
- رمزنگاری ABE (abased encryption)
- مروری بر مسائل باز در مشبکه

مراجع پیشنهادی

- **Books**

1. J. Hoffstein, J. Pipher, and J. H. Silverman, An introduction to mathematical cryptography. Vol. 1. New York: springer, 2008.

2. D. Micciancio, S. Goldwasser:Complexity of lattice problems: a cryptographic erspective. Vol. 671. Springer Science & Business Media, 2012.

- **Lecture Notes**

1. D. Micciancio: Lattices in cryptography and cryptanalysis, 2002. Lecture notes of a course given in UC San Diego.

- **Theses**

1. C. Gentry. A fully homomorphic encryption scheme. Ph.D. thesis, Stanford University, 2009

- **Papers**

1. D. Boneh and D. M. Freeman: Linearly Homomorphic Signatures over Binary Fields and New Tools for Lattice-Based Signatures.Public Key Cryptography 2011: 1-16.
2. P. Q. Nguyen, J. Stern: The Two Faces of Lattices in Cryptology. CaLC 2001, 146-180.
3. C. Peikert:A Decade of Lattice Cryptography. Foundations and Trends in Theoretical Computer Science 10(4): 283-424 (2016).

عنوان درس	فارسی	حریم خصوصی داده										دروس پیش‌نیاز	تعداد ساعت	تعداد واحد
	انگلیسی	Data Privacy												
	نوع واحد													
	پایه		اصلی		تخصصی		اختیاری							
	نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی					۴۸	۳
حل تمرین:	نیاز به اجرای پروژه عملی:													

هدف: بررسی میزان حریم خصوصی از دست رفته، زمانی که اطلاعاتی از یکپایگاه داده منتشر می‌شود.

سرفصل‌های درس:

- **تعریف حریم خصوصی داده و اهمیت آن**: بیان اهمیت حریم خصوصی داده با چند مثال و تعریف دقیق حریم خصوصی داده
- **مکانیسم حریم خصوصی داده:** مکانیسم لاپلاس، مکانیسم ضربی، محدودیت مکانیسم لاپلاس و مکانیسم نمایی، مکانیسمی برای تعداد درخواست‌هایشمارشی(Counting Queries) خیلی زیاد
- **انتشار تعاملی داده**: روش‌های وجودی حریم خصوصی و محدودیت آن‌ها، مکانیسم آستانه‌ای، کنترل تعاملی میزان حریم خصوصی از دست رفته، به روز رسانی ضربی وزن‌ها، مکانیسم تعاملی برای درخواست‌های شمارشی
- **مکانیسم‌هایی برای داده‌های حساس**: درخواست میانه (median query) و مکانیسم میانه پایدار، subsample و مکانیسم aggregate
- **محدودیت‌هایی آماری انتشارخصوصی داده**: نویز و درخواست‌های شمارشی، پایگاه‌های داده با سطرهای بزرگ کم
- **محدودیت محاسباتی برای داده‌های مصنوعی**: سختی تولید پایگاه‌های داده مصنوعی، مکانیسم sanitization
- **سختی مکانیسم‌های کارا برای درخواست‌های شمارشی**: کدهای اثر انگشت، سطرهای کوتاه و انتشار خصوصی داده، سختی پاسخ خصوصی به درخواست به درخواست‌های شمارشی
- **امنیت و حق‌گویی**: حراج کالاهای دیجیتال، مکانیسم Vickrey-Clarke-Groves برای پرداخت و رفاه اجتماعی، بهینه‌سازی خصوصی رفاه اجتماعی
- **امنیت در یادگیری**: یادگیری در مدل PAC و حریم خصوصی، یادگیری برخط با experts
- **پیاده‌سازی‌هایحریم خصوصی**: مکانیسم‌های محلی، مشاهده‌ی دائمی، پیاده‌سازی‌های پان-خصوصی و مکانیسم مجموع‌های تجمعی پان خصوصی
- **تعاریف مختلف حریم خصوصی**: ترکیب جمعیت، حریم خصوصی تفاضلی از ترکیب جمعیت، حریم خصوصی داده‌های خارج از محدوده

مراجع پیشنهادی

- **Books**

1. Dwork, Cynthia, and Aaron Roth. "The algorithmic foundations of differential privacy." Foundations and Trends® in Theoretical Computer Science 9, no. 3–4 (2014): 211-407
2. Hundepool, Anco, Josep Domingo-Ferrer, Luisa Franconi, Sarah Giessing, Eric Schulte Nordholt, Keith Spicer, and Peter-Paul De Wolf. Statistical disclosure control. John Wiley & Sons, 2012.
3. Wiley Duncan et al (2011) Statistical Confidentiality: Principle and Practice. Springer

- **Lecture Notes**

4. Andrej Bogdanov. Lecture notes on Data Privacy. www.cse.cuhk.edu.hk/~andrejb/csci5520/
5. Tal Malkin. Advanced Cryptography (Data Privacy). Spring 2010. http://www.cs.columbia.edu/~tal/6261/SP10/

عنوان درس	فارسی	محاسبات روی داده رمز شده										دروس پیش‌نیاز
	انگلیسی	Computing on Encrypted Data										
نوع واحد										تعداد واحد	تعداد ساعت	
پایه		اصلی		تخصصی		اختیاری				۳	۴۸	
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی					
حل تمرین:		نیاز به اجرای پروژه عملی:										

هدف: آشنایی با تکنیک‌های محاسبه روی داده رمزشده، محاسبات امن چندعاملی، رمزنگاری همریخت و تمام- همریخت (FHE)، رمزنگاری تابعی

سر فصل‌های درس:

- مقدمه: برون‌سپاری امن محاسبات، طرح‌های رمزگذاری همریخت: RSA، الجمال، گلدواسر- میکالی، Paillier، مساله LWE
- مبانی ریاضی مشبکه‌ها، توابع دریچه‌ای روی مشبکه‌ها و رمزنگاری شناسه بنیاد
- مساله یادگیری با خطا (نسخه تصمیمی و جست‌وجویی)، روش‌های کاهش جست‌وجویی به تصمیمی، کاهش مساله LWE از بدترین حالت به حالت متوسط، رمزگذاری کلید خصوصی و کلید عمومی مبتنی بر LWE
- نمونه‌گیری از توزیع گاوسی گسسته و رمزنگاری شناسه بنیاد
- تعویض بعد و رمزگذاری نسبتا همریخت
- تعویض پیمانه‌ای، FHE سطح‌بندی‌شده، قضیه بوت استرپ (Bootstrapping theorem) و FHE، امنیت مدور طرح‌های رمزگذاری
- برون‌سپاری وارسی‌پذیر محاسبات و معرفی چند پروتکل معروف برای محاسبات با زمان چندجمله‌ای
- مدار درهم ریخته (Garbled Circuit)، حالت دوگان سامانه رمز Regev
- رمزگذاری تابعی، مدارهای درهم ریخته یائو و رمزگذاری تابعی تک‌کلیده
- ساختن رمزنگاری خصیصه بنیاد و رمزنگاری تابعی روی مشبکه

مراجع پیشنهادی

- **Books**

1. Boneh, Dan, Amit Sahai, and Brent Waters. "Functional encryption: Definitions and challenges." Theory of Cryptography Conference. Springer Berlin Heidelberg, 2011.
2. Yi, Xun, Russell Paulet, and Elisa Bertino. Homomorphic encryption and applications. Vol. 3. Berlin: Springer, 2014.

- **Theses**
  1. C. Gentry. A fully homomorphic encryption scheme. Ph.D. thesis, Stanford University, 2009
- **Papers**
  1. Regev, Oded. "The learning with errors problem." Invited survey in CCC (2010): 15.

عنوان درس	فارسی	ابزارهای رمزنگاشتی در رایانش ابری									
	انگلیسی	Cryptographic Tools in Cloud Computing									
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز	
پایه		اصلی		تخصصی		اختیاری		۳	۴۸		
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین:						نیاز به اجرای پروژه عملی:					

هدف: در این درس به طور ویژه نگرانی های امنیتی و حریم خصوصی مربوط به داده‌های حجیم مورد بحث و بررسی قرار می گیرد. هدف این درس آشنایی دانشجویان با چالش های اساسی امنیتی مربوط به مدیریت داده با توجه به چرخه حیات آن می باشد.

سر فصل‌های درس:

- **مقدمه‌ای بر برون سپاری و رایانش ابری:** ضرورت مسئله، مزایا و معایب، معماری و انواع مدل‌های سرویس ابری، تاکید بر امنیت به عنوان چالش در سرویس‌های ابری.
- **انواع سرویس‌های داده:** شامل معرفی سرویس‌های جستجو، محاسبات و ذخیره سازی، مقدمات مورد نیاز خاص این سرویس‌ها همچون رمزگذاری مشبکه مبنا (lattice-based encryption)، رمزگذاری حافظ فرمت (format-preserving encryption)، نگاشت‌های دو خطی، جداول مراجعه، روش‌های ذخیره و بازیابی اطلاعات، نمایه سازی و جستجو، مدارهای بولی و....
- **تهدیدات و ملزومات امنیتی در سرویس‌های داده:** حفظ محرمانگی داده، کنترل دسترسی، یکپارچگی، حفظ حریم خصوصی
- **راه حل‌های امنیتی:**
  - معرفی رمزگذاری‌های متناسب با سرویس، جهت حفظ محرمانگی داده شامل: رمزگذاری جستجو پذیر (searchable encryption)، رمزگذاری حافظ ترتیب (order-preserving encryption) و رمزگذاری همریخت (homomorphic encryption).
  - معرفی مکانیسم‌های کنترل دسترسی شامل: رمزگذاری ویژگی-بنیاد(ABE) ، رمزگذاری تابعی(FE) و رمزگذاری انتخابی (selective-encryption)
  - معرفی ابزارهای تضمین یکپارچگی: امضای دیجیتال، درخت مرکل، اثبات‌های تعاملی و غیر تعاملی و....
  - معرفی مکانیسم‌های حفظ حریم خصوصی: انواع حریم خصوصی (کاربر، داده، جواب) و مکانیسم‌های وابسته نظیرروش‌های گمنام‌سازی، امضای گروهی، امضای کور، سامانه‌های صدور گواهی گمنام، k-گمنامی، PIR و ORAMوl-diversity و ....
- **سرویس‌های جستجو:** تمرکز بر جزییات رمزگذاری جستجوپذیر، معرفی و مقایسه روش‌های متقارن و نامتقارن، تعریف امنیت (IND-CKA)، بیان مفهوم جستجوی دقیق و تک کلمه‌ای و طرح رمزهای موجود. توصیف طرح رمزهای مرتبط با جستجوی فازی، جستجوی رتبه بندی شده، جستجوی وارسی‌پذیر، پرسمان‌های غنی و در نهایت تشریح حملات موجود.

- **سرویس‌های ذخیره‌سازی:** تمرکز بر روش‌های تضمین یکپارچگی خاص این سرویس‌ها نظیر مالکیت اثبات‌پذیر داده(provable data possession)، اثبات قابلیت بازیابی(proof of retrievability)، مقایسه این روش‌ها، روش‌های حذف داده تکراری (data deduplication)، روش‌های حذف داده مورد نظر (data destruction).
- **سرویس‌های محاسبه:** تمرکز بر رمزگذاری تمام همریخت، همریخت ضربی و جمعی و نحوه محاسبه توابع مختلف، روش‌های تضمین صحت محاسبات شامل، انواع روش‌های محاسبات وارسی‌پذیر (verifiable computation)، اثبات‌های بررسی احتمالی (PCP) ، روش‌های رمزگذاری جهت تضمین صحت، اثباتهای تعاملی و غیر تعاملی.

مراجع پیشنهادی

- **Books:**
  1. Stefan Rass , Daniel Slamanig. Cryptography for security and privacy in cloud computing. Artech House publication. 2013.

- **Oline Course**

  1. Encrypted Search: http://cs.brown.edu/~seny/2950-v/

- **Theses**

  1. Muhamad Naveed, secure and practical computation on encrypted data, University of Illinois at Urbana-Champaign, 2016.
  2. Justin R. Thaler, Practical Verified Computation with Streaming Interactive Proofs. Harvard University Cambridge, Massachusetts. May 2013.
  3. Raluca Ada Popa, Building Practical Systems That Compute on Encrypted Data. Massachusetts Institute of Technology, 2014; 0830542.

- **Papers**
  1. Jun Tang, Yong Cui, Qi Li, Kui Ren, Jiangchuan Liu, Rajkumar Buyya: Ensuring Security and Privacy Preservation for Cloud Data Services. ACM Comput. Surv. 49(1): 13:1-13:39 (2016).
  2. Christoph Bösch, Pieter H. Hartel, Willem Jonker, Andreas Peter: A Survey of Provably Secure Searchable Encryption. ACM Comput. Surv. 47(2): 18:1-18:51 (2014).

عنوان درس	فارسی	اثبات‌های نا تراوا									
	انگلیسی	Zero-Knowledge Proofs									
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز	
پایه		اصلی		تخصصی		اختیاری		۳	۴۸		
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین:						تیاز به اجرای پروژه عملی:					

هدف: معرفی اثبات‌های تعاملی، اثبات‌های ناتراوا، پروتکل‌های سیگما، و معرفی تعریف امنیت با استفاده از شبیه‌ساز

سر فصل های درس:

- **مرور مفاهیم پایه‌ای:** اثبات‌های تعاملی (interactive proofs)، اثبات‌های ناتراوا (zero-knowledge proofs)، اثبات‌های ناتراوای با وارسی کننده صادق (honest verifier)، معرفی طرح‌های تعهد (commitment schemes)
- **مفاهیم پیشرفته‌تر:** اثبات برابری IP=PSPACE، معرفی کلاس‌های ناتراوای کامل (PZK)، آماری (SZK) و محاسباتی (CAK) و ارتباط آنها، استدلال‌های ناتروا (zero-knowledge arguments)، اثبات‌های ناتراوای غیرتعاملی(Non-Interactive Zero-Knowledge)، الگوی فیات- شامیر(Fiat-Shamir Paradigm)، اثبات‌های با ویژگی تمایز ناپذیری شاهد (witness indistinguishable) و مخفی‌سازی شاهد (witnesshiding)، ویژگی ترکیب سری و موازی در اثبات‌های ناتراوا.
- **پرتکل‌های سیگما** (Σ-protocols): تعریف و ارتباط آن با پروتکل‌های اثبات‌های ناتراوا، پروتکلSchnorr، پروتکل Chaum-Pederson، ترکیب AND و OR پروتکل‌های سیگما
- **سایرموارد به انتخاب مدرس:**ساخت طرح‌های امضای دیجیتال با استفاده پروتکل‌های سیگما، اشاره به مفهوم پروتکل دوعاملی، مفاهیم اولیه پروتکل‌های انتقال بی‌اعتنا (Oblivious Transfer)، مدار بهم‌ریخته یائو و پروتکل چندعاملی GMW

مراجع پیشنهادی

- **Books**

5. Oded Goldreich. 2006. Foundations of Cryptography: Volume 1. Cambridge University Press, New York, NY, USA. (Chapter 4)
6. Oded Goldreich. 2004. Foundations of Cryptography: Volume 2, Basic Applications. Cambridge University Press, New York, NY, USA. (Chapter7).
7. Berry Schoenmakers, Cryptographic Protocols, 2004, Technische Univer- siteit Eindhoven. (Chapter 5)
8. Carmit Hazay and Yehuda Lindell. Efficient Secure Two-Party Protocols: Techniques and Constructions (1st). 2010, Springer-Verlag New York, Inc., New York, NY, USA. (Chapters 5, 6, 7)

9. Rosen, Alon. Concurrent Zero-Knowledge: With Additional Background by Oded Goldreich. Springer Science & Business Media, 2007. Harvard

- **Lecture notes**

10. Damgård, I. "On Sigma protocols. Notes for Cryptographic Protocol Theory course."
11. Helger Lipmaa. Lecture course on Zero-knowledge and some applications. http://kodu.ut.ee/~lipmaa/teaching/Bergen2004.pdf

- **Papers**

12. Uriel Feige, Adi Shamir: Witness Indistinguishable and Witness Hiding Protocols. STOC 1990: 416-426
13. Oded Goldreich, Hugo Krawczyk: On the Composition of Zero-Knowledge Proof Systems. SIAM J. Comput. 25(1): 169-192 (1996)

- **Theses**

14. Vadhan, Salil Pravin. "A study of statistical zero-knowledge proofs." PhD diss., Massachusetts Institute of Technology, 1999.

عنوان درس		فارسی	محاسبه امن چندعاملی							
		انگلیسی	Secure Multi-Party Computation							
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
پایه		اصلی		تخصصی		اختیاری		۳	۴۸	
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی			
حل تمرین:				نیاز به اجرای پروژه عملی:						

هدف: آشنایی با انواع پروتکل‌های محاسبات امن دوعاملی و چندعاملی و اثبات امنیت آنها بالاخص در چارچوب ترکیب سراسری

سر فصل‌های درس:

- **مفاهیم پایه:** معرفی انواع مهاجم‌های فعال (active) و غیرفعال (passive)، مهاجم‌های ایستا (static) و پویا (adaptive)، پروتکل انتقال بی‌اعتنا (Oblivious Transfer) و گسترش آن، پروتکل‌های طرح‌های تسهیم راز
- **پروتکل‌های دوعاملی:** معرفی پروتکل دو عاملی یائو و مدار درهم ریخته یائو (Yao's garbled circuit)، امنیت پروتکل یائو در حضور انواع مهاجم و اثبات امنیت آن، معرفی روش‌های Cut and Choose برای امنیت پروتکل یائو در حضور حمله‌کننده‌های فعال.
- **پروتکل‌های چندعاملی:** معرفی پروتکل‌های GMW، BGW و BMR، کامپایلر GMW
- **سایر پروتکل‌ها:** پروتکل‌های همه‌پخشی (Broadcast)، توافق بیزانتین (Byzantine agreement)
- **مدل‌های اثبات امنیت:** امنیت تنها (stand-alone)، امنیت در چارچوب ترکیب سراسری (Universally Composable Framework)، الگوی دنیای واقعی و دنیای مجازی، عملکرد ایده‌آل.
- **سایر مباحث به انتخاب مدرس:** گسترش OT و انواع پروتکل‌های مختلف برای آن، انواع پروتکل‌های خاص‌منظوره مانند محاسبه امن اشتراک دو مجموعه، محاسبه امن حاصلضرب داخلی دو بردار، رای‌گیری الکترونیکی، حراجی (Auction)، مدل رشته مرجع مشترک ((Common Reference String (CRS)

مراجع پیشنهادی

- **Books**
  1. Ronald Cramer, Ivan Bjerre Damgrd, and Jesper Buus Nielsen. 2015. Secure Multiparty Computation and Secret Sharing (1st ed.). Cambridge University Press, New York, NY, USA.(Chapters 2,3,11).
  2. Yehuda Lindell, Composition of Secure Multi-Party Protocols, 2003, 1st, Springer-Verlag Berlin Heidelberg (Chapters 2,3,4).

3. Carmit Hazay and Yehuda Lindell. Efficient Secure Two-Party Protocols: Techniques and Constructions (1st). 2010, Springer-Verlag New York, Inc., New York, NY, USA. (Chapters 5,6,7).
4. Oded Goldreich. 2006. Foundations of Cryptography: Volume 1. Cambridge University Press, New York, NY, USA. (Chapter 4).
5. Oded Goldreich. 2004. Foundations of Cryptography: Volume 2, Basic Applications. Cambridge University Press, New York, NY, USA. (Chapter 5).
6. Yehuda Lindell. Composition of Secure Multi-Party Protocols, A Comprehensive Study. Lecture Notes in Computer Science 2815, Springer 2003, ISBN 3-540-20105-X

- **Online Course**

http://drona.csa.iisc.ernet.in/~arpita/SecureComputation15.html

- **Papers**

7. Yehuda Lindell and Benny Pinkas. 2011. Secure two-party computation via cut-and-choose oblivious transfer. Springer-Verlag, Berlin, Heidelberg
8. Yehuda Lindell: How To Simulate It - A Tutorial on the Simulation Proof Technique. IACR Cryptology ePrint Archive 2016: 46 (2016)
9. R. Canetti. 2001. Universally Composable Security: A New Paradigm for Cryptographic Protocols. IEEE Computer Society, Washington, DC, USA, 136-.
10. Mihir Bellare, Viet Tung Hoang, Phillip Rogaway: Foundations of garbled circuits. ACM Conference on Computer and Communications Security 2012: 784-796.

عنوان درس	فارسی	طرح‌های تسهیم راز									
	انگلیسی	Secret Sharing Schemes									
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز	
پایه		اصلی		تخصصی		اختیاری		۳	۴۸		
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین:		نیاز به اجرای پروژه عملی:									

هدف: مقدمه‌ای بر طرح‌های تسهیم راز، معرفی طرح‌های تسهیم راز تصدیق‌پذیر،ارائه مفاهیم نرخ اطلاعات و میانگین‌نرخ اطلاعات برای ساختارهای دسترسی و بیان روش‌هایی برای بدست آوردن کران‌های بالایی و پایینی بر روی آن

سر فصل‌های درس:

- **مفاهیم پایه‌ای:** تسهیم راز آستانه‌ای، تسهیم راز شامیر، ساختارهای دسترسی، ساختارهای دسترسی ناتمام (incomplete/non-perfect)، اثبات وجود طرح‌تسهیم راز برای هر ساختار دسترسی، مفهوم monotone Boolean formula و ارتباط آن با ساختار دسترسی، طرح‌های تسهیم راز خطی، طرح تسهیم راز ramp
- **تعریف انواع امنیت:** طرح‌های تسهیم راز کامل (PSS)، طرح‌های تسهیم رازآماری (SSS)، طرح‌های تسهیم راز محاسباتی (CSS)، تعریف معادل امنیت کامل با استفاده از مفهوم آنتروپی
- **طرح‌های تسهیم راز تصدیق‌پذیر (VSS):** معرفی مهاجم فعال (active) و غیر فعال (passive)، پروتکل-های با قابلیت کشف و شناسایی متخلف، طرح‌های با امنیت محاسباتی Feldman و Pedersen
- **نرخ اطلاعات طرح‌های تسهیم راز:** تعریف نرخ اطلاعات (information rate) و میانگین‌نرخ اطلاعات ساختارهای دسترسی، تعیین کران بالایی بر روی (میانگین)نرخ اطلاعات با استفاده از نامساوی‌های اطلاعاتی شانون و غیرشانون، معرفی روش‌های ارائه کران پایینی برای (میانگین) نرخ اطلاعات با استفاده از راهکارهای کلی تجزیه ساختارهای دسترسی مانند λ- تجزیه، $\bar{\lambda}$- تجزیه وزن‌دار و $(\bar{\lambda}, \omega)$-تجزیه
- **ساختارهای دسترسی ایده‌آل:** ساختارهای دسترسی گرافی ایده‌آل،ساختارهای دسترسی القا شده از ماتروییدها، قضیه Brickell-Davenport و تعمیم آن
- **مباحث پیشرفته:** مدل‌های ارتباطی همزمان (synchronous) و غیرهمزمان (asynchronous)، پیچیدگی دور طرح‌های VSS، طرح‌های تصدیق‌پذیر عمومی (publicly verifiable)،تابع دسترسی، ارتباط بین پلی ماتروییدها با طرح‌های تسهیم راز، طرح‌های تسهیم راز غیر خطی، رفتار مجانبی نرخ اطلاعات، تسهیم راز مبتنی بر کد
- **مروری بر مسائل مطرح در زمینه تسهیم راز**

مراجع پیشنهادی:

- **Books**

1. J. B. Nielsen, I. Damgård, R. Cramer: Secure Multiparty Computation and Secret SharingCambridge University Press, 2015. (Part II, Secret Sharing)

2. D.R. Stinson: Cryptography. Theory and practice. Third edition. Discrete Mathematics and its Applications. Chapman & Hall/CRC, 2006. (Chapter 13)

- **Lecture Notes**

3. C. Padró: Lecture notes in secret sharing. Cryptology ePrint Archive 2012/674.

- **Theses**

4. Gennaro, Rosario. "Theory and practice of verifiable secret sharing." PhD diss., Massachusetts Institute of Technology, 1996.
5. O. Farràs. Multipartite Secret Sharing Schemes. PhD diss.UPC (2010)
6. K. M. Martin, Discrete Structures in the Theory of Secret Sharing. Ph. D. Thesis, University of London, (1991).
7. Patra, Arpita. "Studies on Verifiable Secret Sharing, Byzantine Agreement and Multiparty Computation." PhD diss., INDIAN INSTITUTE OF TECHNOLOGY, MADRAS, 2010.
8. Kumaresan, Ranjit. Broadcast and Verifiable Secret Sharing: New Security Models and Round Optimal Constructions. Diss. 2012.
9. A. Yang. Secret Sharing Schemes and Polymatroids. PhD diss ,NTU (2014).

- **Papers**

10. A. Beimel, Y. Ishai: On the Power of Nonlinear Secret Sharing Schemes, SIAM J. Discrete Math. 19 (2005) 258–280.
11. A. Beimel: Secret-Sharing Schemes: A Survey. IWCC 2011: 11-46.
12. O. Farràs, T. B. Hansen, T. Kaced, and C. Padró: On the Information Ratio of Non-Perfect Secret Sharing Schemes. Cryptology ePrint Archive, Report 2014/124, 2014.

عنوان درس	فارسی	رای‌گیری الکترونیکی									
	انگلیسی	Digital Democracy									
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز	
پایه		اصلی		تخصصی		اختیاری		۳	۴۸		
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین:		نیاز به اجرای پروژه عملی:									

هدف: آشنایی با تاریخچه رای‌گیری، معرفی سامانه‌های رای‌گیری الکترونیکی و کاربردهای آن، معرفی ابزارهای رمزنگاری، ارائه تعاریف و اثبات امنیت در این حوزه

سر فصل‌های درس:

- **تاریخچه:** رای‌گیری سنتی، رای‌گیری الکترونیکی، الزامات امنیتی در رای‌گیری الکترونیکی
- **ابزارهای رمزنگاری:** رمزنگاری هوموروفیک، رمزنگاری توزیع‌شده، اثبات‌های ناتراوا، تسهیم راز، رمزگذاری مجدد (reencryption)
- **میکس‌نت:** میکس‌نت Chaum، میکس‌نت Park-Ito-Kurosawa، میکس‌نت RPC، میکس‌نت Neff، میکس-نت Verificatum
- **تعاریف:** تعریف پروتکل رای‌گیری الکترونیکی، تعریف امنیت، مدل کردن الزامات امنیتی رای‌گیری الکترونیکی
- **سامانه‌های متمرکز و غیر متمرکز:** سامانه‌های مبتنی بر میکس‌نت، سامانه‌های مبتنی بر شمارش هوموروفیک، طرح‌های مبتنی بر امضای کور
- **پروتکل‌های پیاده‌سازی‌شده:** پروتکل وی‌ووت (vVote)، پروتکل هلیوس (Helios)، پروتکل پرته‌وتر (Pret a voter)، پروتکل Scantegrity، پروتکل scratch and vote

مراجع پیشنهادی

- **Lecture notes**
  1. Ron Rivest. Selected Topics in Cryptography (Lectures 17-27 on mixnets). http://courses.csail.mit.edu/6.897/spring04/materials.html

- **Online Course**
  1. J. Alex Halderman. "Securing Digital Democracy.": www.coursera.org

- **Theses**
  2. Adida, Ben. "Advances in cryptographic voting systems." PhD diss., Massachusetts Institute of Technology, 2006.Stathakidis, Efstathios. Formal modelling and analysis of mix net implementations. Diss. University of Surrey, 2015.
  3. Essex, Alexander. "Cryptographic End-to-end Verification for Real-world Elections." (2012).

4. Kempka, Carmen. Matters of Coercion-Resistance in Cryptographic Voting Schemes. Diss. Karlsruhe, Karlsruher Institut für Technologie (KIT), Diss., 2014, 2014.
5. Terelius, Björn. Some aspects of cryptographic protocols: with applications in electronic voting and digital watermarking. Diss. KTH Royal Institute of Technology, 2015.

- **Papers**

6. Ben Adida: Helios: Web-based Open-Audit Voting. USENIX Security Symposium 2008: 335-348
7. Chris Culnane, Peter Y. A. Ryan, Steve A. Schneider, Vanessa Teague: vVote: A Verifiable Voting System. ACM Trans. Inf. Syst. Secur. 18(1): 3:1-3:30 (2015)
8. David Chaum, Richard Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L. Rivest, Peter Y. A. Ryan, Emily Shen, Alan T. Sherman: Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems using Invisible Ink Confirmation Codes. EVT 2008
9. Ben Adida, Ronald L. Rivest: Scratch & vote: self-contained paper-based cryptographic voting. WPES 2006: 29-40

عنوان درس	فارسی	پول دیجیتال										
	انگلیسی	Digital Currency										
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
پایه		اصلی		تخصصی		اختیاری		۳	۴۸	
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی			
حل تمرین:				نیاز به اجرای پروژه عملی:						

هدف: آشنایی با پول دیجیتال (Digital Cash) و رمزپول (Crypto-Currencies)، فراگیری مبانی رمزنگاری آن‌ها، آشنایی با مسائل امنیتی و حفظ حریم خصوصی در حوزه پول دیجیتال، آشنایی با رمزپول بیت‌کوین (Bitcoin) و سایر رمزپول‌های مشابه، آشنایی با تکنولوژی زنجیره بلوکی (Block chain)

سر فصل‌های درس:

- **تاریخچه:** پول به عنوان یک واسطه، پول با پشتوانه، پول بدون پشتوانه، پیشرفت‌های رمزنگاری در دهه‌های اخیر، ایده و فلسفه پول دیجیتال
- **سامانه‌های متمرکز و غیرمتمرکز:** فرآیند غیرمتمرکزسازی، مساله جنرال‌های بیزانس، مفهوم اجماع، نظریه بازی‌ها و طراحی مکانیزم، اهمیت توجه به انگیزه‌مندی عامل‌ها در سامانه‌های غیرمتمرکز
- **سامانه‌های متمرکز و غیرمتمرکز مالی:** پول دیجیتال به عنوان یک سامانه مالی متمرکز، رمزپول به عنوان یک سامانه مالی غیرمتمرکز، رمز پول بیت‌کوین، پول اینترنتی، نهادهای نظارتی، قوانین و نظارت‌ها
- **پیشنیازهای رمزنگاری:** رمزنگاری کلیدعمومی، امضای دیجیتال، امضای کور، توابع چکیده‌ساز، مفهوم اثبات‌کار (proof of work)
- **مبانی پول دیجیتال:** عرضه پول دیجیتال، تکنیک‌های رمزنگاری، تعریف امنیت، آشنایی با پروتکل‌های معروف و اثبات امنیت آن‌ها، حفظ حریم خصوصی، چالش‌ها و نوآوری‌های حوزه پول دیجیتال
- **معرفی رمزپول بیت‌کوین:** اصول بیت‌کوین، معدن‌کاوی (mining) و عرضه‌پول در بیت‌کوین، تراکنش‌ها (transaction) و نحوه تایید آن‌ها، حساب‌های بیت‌کوینی (address)، امنیت و حفظ حریم خصوصی، گمنامی، قابلیت ردیابی، زنجیره بلوکی
- **کاربردهای بیت‌کوین:** استفاده‌های متنوع از زنجیره بلوک‌ها، آشنایی با سایر رمزپول‌های مشابه بیت‌کوین، قراردادهای هوشمند غیرمتمرکز (smart contract)

مراجع پیشنهادی

- **Books**

1. Delfs, Hans, Helmut Knebl, and Helmut Knebl. Introduction to cryptography. Vol. 2. Berlin etc.: Springer, 2002. (chapter 5)
2. Franco, Pedro. Understanding Bitcoin: Cryptography, engineering and economics. John Wiley & Sons, 2014.

3. Narayanan, Arvind, et al. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, 2016.
4. Rosenberg, Burton, ed. Handbook of financial cryptography and security. Chapman and Hall/CRC, 2010.

- **Online courses**

5. Arvind NarayananBitcoin and Cryptocurrency Technologies. https://www.coursera.org/learn/cryptocurrency
6. Bitcoin and Cryptocurrencies. Stanford course. https://crypto.stanford.edu/cs251/

عنوان درس	فارسی	مبهم‌سازی برنامه											
	انگلیسی	Program Obfuscation											
نوع واحد										تعداد واحد	تعداد ساعت	دروس پیش‌نیاز	
پایه		اصلی		تخصصی		اختیاری				۳	۴۸		
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی						
حل تمرین:						نیاز به اجرای پروژه عملی:							

هدف: آشنایی باتعاریف و مفاهیم امنیتی مربوط به این حوزه، روش‌های مبهم سازی، ابزارهای رمزنگاری، بررسی محدودیت‌ها، مرور پژوهش های اخیر، کاربردهای مبهم‌سازی برنامه در رمزنگاری

سر فصل‌های درس:

- **تعریف مبهم‌سازی:** آشنایی با پیش‌زمینه‌های بحث، نمادگذاری، تعاریف، مبهم‌سازی مبتنی بر مسند (predicate)، مبهم‌سازی مبتنی بر تمایزدهنده (Distinguisher)، مبهم‌سازی Best-Possible
- **مفاهیم رمزنگاری مرتبط:** رمزنگاری متقارن، رمزنگاری نامتقارن، رمزنگاری خصیصه-مبنا، رمزنگاری شناسه- مبنا، رمزگذاری تابعی، محاسبات امن چندعاملی، رمزگذاری شاهددار(witness encryption)
- **تعریف امنیت:** امنیت خوش‌تعریف (Well-Defined) و مبهم‌سازی کد، امنیت فازی، راحت‌کردن خاصیت پنهان سازی، تعاریف ضعیف‌تر مبهم‌سازی
- **نتایج بدست‌آمده:** نتایج مثبت (positive result)، نتایج منفی (negative result)،
- **کاربردهای مبهم‌سازی کد:** ساخت رمزگذاری انکار پذیر، ساخت تابع یک‌طرفه، ساخت محاسبات امن چند عاملی با حداکثر دو دور، ساخت رمزگذاری تابعی تطبیقی (adaptively)، ساخت تسهیم راز برای NP، ساخت رمزگذار شاهددار
- **مبهم‌سازی در عمل:** چارچوب مفسر مبهم‌سازی‌شده، مبهم‌سازی خلاقانه (heuristic)، مبهم‌سازی واژه‌گانی(lexical)، مبهم سازی داده، مبهم‌سازی کنترل، مبهم‌سازی ، مبهم‌سازی call-flow، یکی‌سازی فرمت فراخوانی، روش ادغام Inter-classes، روش ساختی استخر شیء (Object pool)، افزایش مبهم‌سازی (Obfuscating enhancement)، نتایج عملی

مراجع پیشنهادی

- **Theses**
  1. Varia, Mayank Mayank Harshad. Studies in program obfuscation. Diss. Massachusetts Institute of Technology, 2010.
  2. Telang, Sidharth Durgesh. On Program Obfuscation. Diss. Cornell University, 2016.

- **Papers**

3. Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, Brent Waters:Candidate Indistinguishability Obfuscation and Functional Encryption for all circuits. IACR Cryptology ePrint Archive 2013: 451 (2013)
4. Collberg, Christian, Clark Thomborson, and Douglas Low. A taxonomy of obfuscating transformations. Department of Computer Science, The University of Auckland, New Zealand, 1997.
5. Goldwasser, Shafi, and Guy N. Rothblum. "On best-possible obfuscation." Theory of Cryptography Conference. Springer Berlin Heidelberg, 2007
6. Lynn, Benjamin, Manoj Prabhakaran, and Amit Sahai. "Positive results and techniques for obfuscation." International conference on the theory and applications of cryptographic techniques. Springer Berlin Heidelberg, 2004.

عنوان درس	فارسی	طرح‌های امضای دیجیتال									
	انگلیسی	Digital Signature Schemes									
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز	
پایه		اصلی		تخصصی		اختیاری					
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی	۳	۴۸		
حل تمرین:		نیاز به اجرای پروژه عملی:									

هدف: مقدمه‌ای بر مفاهیم امضای دیجیتال و تعریف امنیت آنها، آشنایی با انواع امضاها و معرفی امضاهایی با قابلیت‌های اضافی

سر فصل‌های درس

- **مفاهیم پایه‌ای:** مقدمه‌ای بر امضاهای دیجیتال، تعریف امنیت برای امضاهای دیجیتال، تعریف امنیت در مقابل حمله پیام‌تصادفی(RMA)، حمله پیام‌معلوم(KMA) و حمله پیام انتخابی انطباقی(ACM)
- **طرح‌های بدون اوراکل‌های تصادفی:**
  - امضای یک‌بار مصرف ((one-time(OTS)؛ امضای Lamport
  - امضاهای با استفاده از امضاهای OTS؛ امضاهای chain-based، امضاهای tree-based
  - امضاهای با استفاده از توابع یک‌طرفه
  - امضاهای مبتنی بر فرض RSA: امضای Dwork-Naor، امضای Cramer-Damgard
  - امضاهای مبتنی بر فرض RSA قوی: امضای Cramer-Shoup، امضای Fischlin
  - امضاهای مبتنی بر نگاشت‌های دوخطی(bilinear)؛ امضای Boneh-Boyen، امضای Waters
- **طرح‌های در مدل اوراکل تصادفی:**
  - امضای چکیده‌ساز تمام‌دامنه((full-domain hash (FDH)، FDH احتمالاتی
  - امضاهای مبتنی بر اثبات‌های ناتروا و پروتکل‌های سیگما: امضای Schnorr
- **طرح‌های امضا با قابلیت‌های اضافی:** طرح چندامضایی(multi-signature)، امضای آستانه‌ای (threshold)، امضای on-line/off-line، امضای افزایشی (incremental signature)، امضای کور(blind)، امضای وکالتی (proxy)، امضای جوهر نامرئی (magic ink)، امضای خودتصدیق‌شده (self-certified)، امضای امن پیشرو (forward-secure)، امضای ایست‌خرابی(fail-stop)، امضای پایا (invariant)، امضای غیرقابل انکار (undeniable)، امضای با بازیابی پیام (message recovery)، امضای دسته‌ای(batch)، امضای گروهی (group)، امضای حلقه‌ای (ring)

مراجع پیشنهادی

- **Books**

1. O. Goldreich: Foundations of Cryptography: Volume 1, New York, NY: Cambridge University Press, 2006.
2. O. Goldreich: Foundations of Cryptography: Volume 2, Basic Applications, New York, NY, Cambridge University Press, 2006. (Chapter 2)
3. J. Katz, Digital Signatures, Springer, 2010.

- **Papers**

1. D. Chaum: Blind Signatures for Untraceable Payments. CRYPTO 1982, 199-203.
2. D. Chaum, H. V. Antwerpen: Undeniable Signatures. CRYPTO 1989, 212-216.
3. K. Nyberg, R. A. Rueppel: Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem. Des. Codes Cryptography 7(1-2), 61-81 (1996).

عنوان درس	فارسی	رمزنگاری و پیچیدگی محاسبه										دروس پیش‌نیاز
	انگلیسی	Cryptography and Complexity										
نوع واحد										تعداد واحد	تعداد ساعت	
پایه		اصلی		تخصصی		اختیاری				۳	۴۸	
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی					
حل تمرین:						نیاز به اجرای پروژه عملی:						

هدف: روش های پیچیدگی محاسبه در رمزنگاری و برعکس، محدودیت در اثبات های رمزنگاری، نحوه غلبه بر محدودیت‌های روش‌های معمول

سر فصل‌های درس:

- **مروری بر مدل‌های محاسبه:** مدل یکنواخت (ماشین تورینگ)، مدل غیر یکنواخت(مدارها، ماشین‌های تورینگ غیر خطی)
- **مروری بر تعاریف و تحویل‌های اولیه رمزنگاری:** توابع یک‌طرفه، توابع شبه‌تصادفی، مولدهای شبه تصادفی و hardness amplification.
- **مدل کردن تحویل مساله:** مدل کاملا جعبه سیاه، مدل نیمه جعبه سیاه، مدل جعبه سیاه ضعیف، مدل relativized، مدل دو اراکلی
- **نتایج منفی برای مدل‌های یکنواخت** : غیرممکن بودن تحویل مسائل زیر
  - توافق کلید به تابع یک‌طرفه و توابع درهم‌ساز برخورد تاب
  - تابع یک‌طرفه برخود تاب به جایگشت یک‌طرفه
  - توافق کلید ۲ نفره با k-pass، به توافق کلید ۲ نفره با (k-1)-pass.
- **نتایج منفی برای مدل‌های غیریکنواخت:** لم بازسازی Gennaro-Trevisan، محدودیت در بهینه‌سازی مولدهای شبه تصادفی ساخته شده از جایگشت یک‌طرفه، محدودیت در بهینه‌سازی توابع درهم ساز یکطرفه جهانی ساخته شده از جای‌گشت یک‌طرفه، محدودیت در بهینه‌سازی امضای دیجیتال ساخته شده از جایگشت یک‌طرفه دریچه دار، محدودیت در بهینه‌سازی رمزنگاری کلید عمومی ساخته شده از جایگشت یک‌طرفه دریچه‌دار
- **تحویل‌های جبری و محدودیت‌ها:** مدل عمومی گروه‌ها. سختی مسائل لگاریتم گسسته و دیفی- هلمن محاسباتی و تصمیمی در مدل عمومی گروه‌ها، سختی تحویل لگاریتم گسسته به دیفی- هلمن محاسباتی در مدل عمومی گروه‌ها، میدان‌های جعبه سیاه و تحویل زیرنمایی (sub-exponential) مساله لگاریتم گسسته به دیفی- هلمن محاسباتی، مدل‌های مدرج، برنامه‌های خط مستقیم (straight line programs)، مساله‌ی Low Exponent RSA، RSA و تجزیه‌ی اعداد، رده‌بندی اولیه‌های رمزنگاری، تعیین جایگاه و قدرت اولیه‌های رمزنگاری نسبت به یکدیگر و جایگاه گزاره‌های $P \neq NP$ و $BPP \neq NP$، مولدهای شبه‌تصادفی، عصاره‌گیری از متغیرهای تصادفی و Derandomization، جایگزین کردن بیت‌های تصادفی در الگوریتم‌های تصادفی با

خروجی مولدهای شبه تصادفی، مولدهای شبه تصادفی با زمان اجرای بیشتر از حمله کننده، ساختن مولدهای شبه تصادفی از توابع یکطرفه و عصاره‌گیری از متغیرهای تصادفی

- **مباحث انتخابی توسط مدرس:** پیچیدگی بدبینانه (worst case complexity) و رمزنگاری: Worst case. EXP و مولدهای شبه تصادفی. Worst case EXP و ZK argumentهای جهانی، اثبات اینکه هر ساختار کاملا جعبه سیاه مولد شبه تصادفی از توابع یکطرفه یک عصاره‌گیر است، محدودیت رمزنگاری مبتنی بر NP-hardness. مبهم‌سازی برنامه‌ها، غلبه بر محدودیت‌های روش‌های جعبه سیاه با استفاده از روش‌های غیر جعبه سیاه و کاربرد در رمزنگاری resettable.

مراجع پیشنهادی

- **Books**
  1. Talbot, John, and Dominic James Anthony Welsh. Complexity and cryptography: an introduction. Vol. 13. Cambridge University Press, 2006.

- **Theses**
  1. Barak, Boaz. Non-black-box techniques in cryptography. Diss. Weizmann Institute of Science, 2004.
  2. Dachman-Soled, Dana. On Black-Box Complexity and Adaptive, Universal Composability of Cryptographic Tasks. Columbia University, 2011.
  3. Jager, Tibor. Black-Box Models of Computation in Cryptology. Springer Science & Business Media, 2012.
  4. Mohammad Mahmoody Studies in the Efficiency and (versus) Security of Cryptographic Tasks Ph.D. Thesis, Princeton University, 2010.

- **Lecture Notes**
  1. Vadhan, Salil P. "Pseudorandomness." Foundations and Trends® in Theoretical Computer Science 7.1–3 (2012): 1-336.
  2. Bogdanov, Andrej, and Luca Trevisan. "Average-case complexity." Foundations and Trends® in Theoretical Computer Science 2.1 (2006): 1-106.

- **Papers**
  1. Omer Reingold, Luca Trevisan, Salil P. Vadhan:Notions of Reducibility between Cryptographic Primitives. TCC 2004: 1-20
  2. Iftach Haitner, Jonathan J. Hoch, Omer Reingold, Gil Segev:Finding Collisions in Interactive Protocols - Tight Lower Bounds on the Round and Communication Complexities of Statistically Hiding Commitments. SIAM J. Comput. 44(1): 193-242 (2015)
  3. Dan Boneh, Richard J. Lipton:Algorithms for Black-Box Fields and their Application to Cryptography (Extended Abstract). CRYPTO1996: 283-297

عنوان درس	فارسی	تصادفی‌سازی در رمزنگاری										دروس پیش‌نیاز
	انگلیسی	Randomness in cryptography										
	نوع واحد								تعداد واحد	تعداد ساعت		
	پایه		اصلی		تخصصی		اختیاری		۳	۴۸		
	نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی				
	حل تمرین:		نیاز به اجرای پروژه عملی:									

هدف: هدف اصلی درس بررسی لزوم، به کارگیری و تحلیل منابع مولد تصادفی در علم رمزنگاری است.

سر فصل‌های درس:

- یاد آوری مفاهیم اصلی احتمال، تعریف منبع مولد تصادفی و مفاهیم اولیه از نظریه محاسبه و نظریه اطلاعات
- کاربردهای مولدهای تصادفی در رمزنگاری: وابستگی امنیت به کاربرد مولد تصادفی، نقش تصادف در تولید کلید، نقش مولدهای تصادفی درMasking . نقش توزیع احتمال مولد تصادفی در امنیت و امنیت توزیع یکنواخت یا تاکید در اینکه در عمل توزیع احتمال یکنواخت در دسترس نیست.
- بحث در مورد امنیت نظریه اطلاعاتی و امنیت محاسباتی و بررسی نقش تصادف در این دو امنیت، مفهوم آنتروپی در تحلیل منابع تصادفی و امنیت
- نقش مولدهای تصادفی در طراحی الگوریتم‌های تصادفی و امنیت آن در طراحی حملات (با مثال)، بحث مختصر در نقش تصادف در امنیت از نظر پیچیدگی محاسبه، کلاس‌هایBPP ، NP و اثبات‌هایZK
- کاربرد و طراحیExtractor ها: روش‌های ساخت کلاسیک و نحوه استفاده از leftover hash lemma مقایسه با سناریوی امنیت شانون(نظریه اطلاعاتی) و کاربرد آنتروپی
- ارائه روش ساخت حداقل یک یا دو اولیه رمزنگاری مبتنی برExtractor ها
- بحث خاص: در حد زمان باقی‌مانده
- منابع غیر ایده‌آل در رمزنگاری و انواع آن‌ها (از لحاظ مدل) مشکلات
- بررسی امنیت مبتنی بر منابع غیرایده‌آل و نشان‌دادن عدم کفایت آن‌ها (حداقل چند مدل)
- بحث در مورد رابطه Extractability با اولیه‌های رمزنگاری
- امنیت منابع در حملات کانال جانبی و رمزنگاری نشت‌تاب(Leakage resilient)

مراجع پیشنهادی

1. **Online course**
   Yevgeniy Dodis. Randomness in Cryptography.
   http://cs.nyu.edu/~dodis/randomness-in-crypto/

2. Papers

1. D. Dachman-Soled, R. Gennaro, H. Krawczyk, T. Malkin. Computational Extractors and Pseudorandomness in TCC 2012.
2. Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. In EUROCRYPT 2004.
3. J. Kamo, D. Zuckerman. Deterministic Extractors for Bit-Fixig Sources and Exposure-Resilient Cryptography. In SICOMP 2006.

عنوان درس	فارسی	مباحث ویژه در رمز نگاری
	انگلیسی	Special Topics in Cryptography

نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
پایه		اصلی		تخصصی		اختیاری		۳	۴۸	
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی			
حل تمرین:				نیاز به اجرای پروژه عملی:						

درسی است در سطح دکتری در زمینه رمز که سرفصل آن بر حسب امکانات و نیاز درنیم‌سال مورد نظر توسط استادمربوطه پیشنهاد شده وپس از تصویب شورای تحصیلات تکمیلی گروه و دانشکده ارایه می‌شود.

دکتری ریاضی

(زیر برنامه منطق ریاضی)

فصل اول

مشخصات دوره دکتری ریاضی - زیر برنامه منطق ریاضی

مقدمه

منطق ریاضی در اواخر قرن نوزدهم و اوایل قرن بیستم میلادی ضمن کوشش فیلسوف- ریاضیدانانی چون فرگه و راسل برای حل مسائل موجود در مبانی ریاضیات به وجود آمد و با تلاش ریاضیدانان بزرگی چون هیلبرت، گودل و تارسکی شکوفا شد. دهه ۱۹۴۰ میلادی شاهد رشد شاخه‌های اصلی منطق ریاضی مانند نظریه برهان، نظریه محاسبه‌پذیری، نظریه مدل و نظریه مجموعه بود.

یک محصول جانبی ولی بسیار با ارزش این تلاش‌ها که در راستای بررسی تصمیم‌پذیری دستگاه‌های مختلف منطقی و ریاضی به دست آمد، معرفی نخستین ماشین‌های محاسب صوری از قبیل ماشین تورینگ بود. این موضوع نه تنها منجر به شکل‌گیری بخش مهم نظریه محاسبه‌پذیری (نظریه بازگشت) از منطق ریاضی شد، بلکه موجب ساخت کامپیوترهای امروزی و پیدایش علوم کامپیوتر نظری نیز شد. در سال‌های اخیر کاربردهای منطق در علوم کامپیوتر آنچنان فراگیر شده که اهمیت آن را با اهمیت حساب دیفرانسیل و انتگرال در علم فیزیک مقایسه می‌کنند.

هدف:

هدف از این دوره رسیدن به مرزهای دانش در یکی از بخش‌های منطق یا کاربردهای آن و انجام پژوهش اصیل در آن قسمت است.

نقش وتوانایی :

منطق ریاضی یکی از شاخه‌های مهم ریاضیات است و قسمت‌های مختلف آن کاربردها و ارتباط‌های اساسی با بخش‌های مختلف ریاضیات و همچنین علوم نظری کامپیوتر دارند. فارغ‌التحصیلان این دوره علاوه بر توانایی جذب شدن به عنوان عضو هیئت علمی در گروه‌های آموزشی یا پژوهشی ریاضی، با توجه به دروس اخذ کرده و زمینه پژوهشی رساله خود، امکان کار به عنوان عضو هیئت علمی در گروه‌های علوم کامپیوتر را نیز دارند.

ضرورت واهمیت:

منطق ریاضی یکی از شاخه‌های ریاضیات است که علاوه بر داشتن کاربردهای مختلف در قسمت‌های دیگر ریاضیات، در بررسی بنیادهای ریاضیات و سوال‌های مربوط به مبانی آن نقش اساسی دارد. به علاوه استفاده از منطق در علوم کامپیوتر امروزه به ابزاری غیر قابل صرف نظر کردن تبدیل شده است. به این ترتیب انتظار می‌رود فارغ‌التحصیلان این دوره بتوانند سهم مهمی در تحقق هدف اساسی تقویت تأثیرگذاری ریاضیات در خارج از این رشته ایفا کنند.

کلیات برنامه:

برنامه آموزشی دوره دکتری ریاضی (منطق ریاضی) شامل پنج درس متشکل از دو درس الزامی و سه درس تخصصی- اختیاری است. درس‌های الزامی شامل دو درس از میان چهار درس نظریه برهان، نظریه محاسبه‌پذیری، نظریه مدل و نظریه مجموعه خواهد بود. این چهار درس، چهار بخش مختلف منطق ریاضی را پوشش می‌دهند و انتظار می‌رود که فارغ‌التحصیلان دکتری ریاضی (منطق ریاضی) در حداقل دو تا از این گرایش‌ها درس گذرانده باشند. در صورت اخذ این دو درس در دوره کارشناسی ارشد، دانشجویان می‌توانند به جای آنها از میان دیگر دروس تخصصی - انتخابی این گرایش درس‌هایی را با نظر استاد راهنما بگذرانند. برنامه پژوهشی این دوره ۲۱ واحد است که به نگارش یک رساله اختصاص دارد. رساله شامل پژوهش اصیل در یکی از بخش‌های منطق ریاضی یا کاربردهای آن خواهد بود.

عنوان دوره : دکترای ریاضی

پیشنیاز ورود: دارا بودن مدرک کارشناسی ارشد در یکی از رشته‌های مجموعه علوم ریاضی

مواد آزمون ورودی(کنکور): درس منطق ریاضی و یکی دیگر از دروس الزامی دوره کارشناسی ارشد رشته ریاضیات و کاربردها

فصل دوم

جدول دروس دکتری ریاضی – زیر برنامه منطق ریاضی

جدول شماره ۱: درس های اصلی – زیر برنامه منطق ریاضی

شماره درس	نام درس	تعداد واحد	پیش نیاز و هم نیازها
۱	نظریه برهان	۳	منطق ریاضی
۲	نظریه محاسبه‌پذیری	۳	منطق ریاضی
۳	نظریه مدل	۳	اجازه گروه
۴	نظریه مجموعه	۳	اجازه گروه

- انتخاب ۶ واحد از جدول فوق به عنوان دروس اصلی زمینه تخصصی با نظر استاد راهنما و دانشکده.
- دانشجو می تواند سایر دروس جدول فوق را به عنوان درس تخصصی – انتخابی خود انتخاب کند

جدول شماره ۲: درس‌های تخصصی- انتخابی دکتری ریاضی – زیر برنامه منطق ریاضی

شماره درس	نام درس	تعداد واحد	پیش نیاز و هم نیازها
۱	آنالیز نااستاندارد	۳	اجازه گروه
۲	منطق محاسباتی	۳	منطق ریاضی
۳	نظریه مجموعه‌های فازی و منطق فازی	۳	ندارد
۴	آنالیز محاسبه‌پذیر	۳	نظریه محاسبه‌پذیری
۵	جبر جامع	۳	ندارد
۶	نظریه رسته و توپوس	۳	ندارد
۷	نظریه مشبکه	۳	ندارد
۸	ساختارهای جبری مرتب	۳	ندارد
۹	منطق شهودی	۳	منطق ریاضی
۱۰	منطق وجهی	۳	منطق ریاضی
۱۱	منطق فازی پیشرفته	۳	منطق ریاضی
۱۲	فلسفه ریاضی	۳	منطق ریاضی
۱۳	نظریه پیشرفته مدل	۳	نظریه مدل
۱۴	نظریه پیشرفته مجموعه	۳	نظریه مجموعه
۱۵	مدل‌های نااستاندارد حساب	۳	منطق ریاضی، نظریه مدل
۱۶	منطق و محاسبه	۳	منطق ریاضی
۱۷	نظریه پیشرفته محاسبه‌پذیری	۳	نظریه محاسبه‌پذیری
۱۸	نظریه پیشرفته برهان	۳	نظریه برهان
۱۹	منطق جبری	۳	اجازه گروه
۲۰	مباحث ویژه در منطق ریاضی	۳	اجازه گروه

فصل سوم

سر فصل دروس دکتری ریاضی – زیر برنامه منطق ریاضی

عنوان درس	فارسی	نظریه برهان							
	انگلیسی	Proof Theory							
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی			۳	۴۸	منطق ریاضی
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد				**نیاز به اجرای پروژه عملی:** ندارد					

هدف درس:

هدف از این درس آشنایی با مقدمات نظریه برهان که یکی از قسمت‌های اصلی منطق ریاضی است، می‌باشد.

سرفصل‌های درس:

مروری بردستگاه‌های مختلف اثباتی نظیرهیلبرتی، استنتاج طبیعی و حساب رشته‌ای، حساب رشته‌ای برای منطق کلاسیک، قضیه حذف برش، خاصیت زیرفرمولی، حساب رشته‌ای برای منطق شهودی، قضیه هربراند، قضیه درون‌یابی، قضیه سازگاری گنتزن، مقدمه‌ای بر نظریه برهان حساب مرتبه اول.

مراجع پیشنهادی:

1. Jean-Yves Girard, **Proof Theory and Logical Complexity**, Volume 1, Bibliopolis, 1987.
2. Sara Negri and Jan van Plato, **Structural Proof Theory**, Cambridge University Press, 2001.
3. G. Takeuti, **Proof Theory**, 2nd ed., Dover Publications, 2013(ISBN: 9780486490731)

عنوان درس	فارسی	نظریه محاسبه‌پذیری							
	انگلیسی	Computability Theory							
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی			۳	۴۸	منطق ریاضی
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد				نیاز به اجرای پروژه عملی: ندارد					

هدف درس:

هدف از این درس آشنایی مقدماتی با نظریه محاسبه‌پذیری (نظریه بازگشت) است. نظریه محاسبه‌پذیری یکی از شاخه‌های اصلی منطق ریاضی است و بعلاوه کاربردهای فراوانی در علوم کامپیوتر دارد.

سرفصل‌های درس:

مفهوم شهودی محاسبه‌پذیری و الگوریتم، مدل‌های ریاضی الگوریتم مانند ماشین تورینگ و ماشین رجیستری، توابع بازگشتی ابتدایی، توابع بازگشتی (جزئی)، فرضیه چرچ، مجموعه‌های شماره‌پذیر کارآمد، تصمیم‌ناپذیری مسأله توقف، تحویل‌های چند به یک و تورینگ، درجات حل‌ناپذیری، قضیه نقطه ثابت، قضیه رایس، مجموعه‌های خلاق، مجموعه‌های ساده و m-ناکامل بودن آن‌ها، سلسله مراتب حسابی و برخی مثال‌ها، عملگر جهش.

مراجع پیشنهادی:

1. S. B. Cooper, **Computability Theory**, Chapman & Hall/CRC Mathematics Series, 2004.
2. H.B. Enderton, **Computability Theory: an introduction to recursion theory**, Academic Press, 2010 (ISBN: 9780123849588)

3- A. Shen and N.K. Vereshchagin, **Computable Functions**, American Mathematical Society, 2002. (ISBN: 9780821827321)

عنوان درس	فارسی	نظریه مدل							
	انگلیسی	Model Theory							
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی			۳	۴۸	اجازه گروه
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد		نیاز به اجرای پروژه عملی: ندارد							

هدف درس:

هدف از این درس آشنایی با نظریه مدل که یکی از شاخه‌های اصلی منطق ریاضی است، می‌باشد. نظریه مدل کاربردهای زیادی در سایر شاخه‌های ریاضیات دارد.

سرفصل‌های درس:

زبان، فرمول، مدل، صدق(satisfaction) ، قضیه فشردگی با روش ساختن هنکین، فراضرب، قضیه‌های لوونهایم- اسکولم فروسو و فراسو، آزمون تارسکی، کامل بودن، جازم بودن، آزمون وات، تعریف‌پذیری، چنداگر (quantifier)، نظریه‌های مجموعه‌های مرتب چگال، گراف‌های تصادفی، میدان‌های بسته جبری و میدان‌های بسته حقیقی، کمینگی قوی، ترتیب- کمینگی.

مراجع پیشنهادی:

1. K. Tent, M. Ziegler, **A Course in Model Theory**, Cambridge University Press, 2012
2. C.C. Chang, H. Jerome Keisler, **Model Theory**, North-Holland, 1990
3. D. Marker, **Model Theory: An Introduction**, Springer-Verlag, 2002
4. A. Marcja, C. Toffalori, **A Guide to Classical and Modern Model Theory**, Kluwer Academic Publishers, 2003
5. M. Manzano, **Model Theory**, Oxford University Press, 1999
6. P. Rothmaler, **Introduction to Model Theory**, Taylor and Francis, 2000.

عنوان درس	فارسی	نظریه مجموعه							
	انگلیسی	Set Theory							
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی			۳	۴۸	اجازه گروه
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد				نیاز به اجرای پروژه عملی: ندارد					

هدف درس:

هدف از این درس آشنایی با نظریه مجموعه می‌باشد که علاوه بر این که یکی از شاخه‌های اصلی منطق ریاضی است و کاربردهای متفاوتی در ریاضیات دارد، نقش مهمی نیز در مطالعه بنیادهای ریاضیات ایفا می‌کند.

سرفصل‌های درس:

پنداشت‌های ZFC، حساب اردینال‌ها، حساب کاردینال‌ها، کاردینال‌های دست نیافتنی و برهان‌ناپذیری وجود و سازگاری آن‌ها، فروپاشی (collapsing) موستاوسکی، اصل بازتاب، عمل‌های گودل، مدل‌های ترایایی، اَوَستی (absoluteness)، جهان ساخت‌پذیر، سازگاری ZFC با V=L و GCH.

مراجع پیشنهادی:

1. K. Ciesielski, **Set Theory for Working Mathematicians**, Cambridge, 1997
2. T. Jech, **Set theory**, Springer, 2013
3. K. Kunen, **Set Theory, an Introduction to Independence Proofs**, North-Holland, 1992
4. R.M. Smullyan, M. Fitting, **Set Theory and the Continuum Problem**, Oxford, 1996.

عنوان درس	فارسی	آنالیز نااستاندارد							
	انگلیسی	Nonstandard Analysis							
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی			۳	۴۸	اجازه گروه
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد		نیاز به اجرای پروژه عملی: ندارد							

هدف درس:

هدف از این درس آشنایی با آنالیز نااستاندارد و کاربردهای آن در آنالیز ریاضی استاندارد می‌باشد.

سرفصل‌های درس:

هم‌ساختن فراتوانی عددهای ابر حقیقی، عددهای بی‌نهایت بزرگ و بی‌نهایت کوچک، اصل تراوژ (transfer)، همگرایی دنباله‌ها و سری‌های عددی و تابعی، پیوستگی، مشتق و انتگرال از دیدگاه نااستاندارد، مجموعه‌ها و تابع‌های درونی در R، جهان نااستاندارد، مجموعه‌های درونی، برونی و ابر متناهی، ماندگاری (permanence)، اندازه لوب.

مراجع پیشنهادی:

1- J. L. Bell, **A Primer of Infinitesimal Analysis**, Cambridge University Press, 2008. (ISBN: 9780521887182)
2- M. Davis, **Applied Nonstandard Analysis**, Dover Publications, 2005. (ISBN: 9780486442297)
3- V. Kanovei and M. Reeken, **Nonstandard Analysis - Axiomatically**, Springer, 2010. (ISBN:9783642060779)

عنوان درس	فارسی	منطق محاسباتی							
	انگلیسی	**Computational Logic**							
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی			۳	۴۸	منطق ریاضی
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد				**نیاز به اجرای پروژه عملی:** ندارد					

هدف درس:

هدف از این درس آشنایی با جنبه‌های محاسباتی منطق و روش‌های اثبات خودکار است.

سرفصل‌های درس:

منطق گزاره‌ها، شکل‌های نرمال، مسأله ارضاپذیری، قواعد دیویس و پاتنام، رزولوشن، شکل‌های پیشوندی، اسکولمی کردن فرمول‌ها، قضیه هربراند، یکسان‌سازی، قضایای ناتمامیت گودل.

مراجع پیشنهادی:

1. M. Fitting, **First- order Logic and Automated Theorem Proving**, Springer-Verlag, 1996.
2. M. Ben-Ari, **Mathematical Logic for Computer Science**, 3rd ed., Springer, 2012. (ISBN: 9781447141280)
4- M. Tarver, **Logic, Proof and Computation**, Upfront Publishing, 2014. (ISBN: 9781784561277)

عنوان درس	فارسی	نظریه مجموعه‌های فازی و منطق فازی								
	انگلیسی	Fuzzy Set Theory and Fuzzy Logic								
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی				۳	۴۸	ندارد
نظری	عملی	نظری	عملی	نظری	عملی					
حل تمرین: ندارد				نیاز به اجرای پروژه عملی: ندارد						

هدف درس:

هدف از این درس آشنایی با نظریه مجموعه‌ها و منطق فازی به معنای عام است که دارای کاربردهای متنوعی در شاخه‌های مختلف مهندسی است.

سرفصل‌های درس:

مجموعه‌های فازی، برش‌های مجموعه‌های فازی، نمایش‌های مختلف مجموعه‌های فازی، اعداد فازی، متغیرهای زبانی، رابطه‌های فازی، تابع‌های فازی، منطق فازی مقدماتی، استدلال تقریبی، شرطی‌های فازی، مقدمه‌ای بر کنترل فازی و برخی کاربردهای دیگر منطق فازی.

مراجع پیشنهادی:

1. H. T-Nguyen, E. A. Walker, **A First Course in Fuzzy Logic**, Third Edition, Chapman & Hall/CRC Taylor Francis Groups, 2006.
2. G. J. Klir, Bo Yuan, **Fuzzy Sets and Fuzzy Logic (Theory and Applications)**, Prentice Hall, 1995.
3. Kwang H. Lee, **First Course on Fuzzy Theory and Applications**, Springer, 2005.

عنوان درس	فارسی	آنالیز محاسبه‌پذیر							
	انگلیسی	Computable Analysis							
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی			۳	۴۸	نظریه محاسبه‌پذیری
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد				**نیاز به اجرای پروژه عملی:** ندارد					

هدف درس:

هدف از این درس آشنایی با آنالیز محاسبه‌پذیر یا بازگشتی است. این شاخه نظریه محاسبه پذیری استاندارد را که به اعداد طبیعی مرتبط می شود به اعداد حقیقی گسترش می دهد.

سرفصل‌های درس:

محاسبه‌پذیری در آنالیز کلاسیک، دنباله‌های بازگشتی از تابع‌های حقیقی، محاسبه‌پذیری روی فضاهای باناخ، تابع‌های حقیقی بازگشتی پاره‌ای، نظریه بازگشتی اندازه، پیچیدگی محاسبه‌ای تابع‌های حقیقی.

مراجع پیشنهادی:

1. M. B. Pour-el and J. I. Richards, **Computability in Analysis**, Springer, 1989.
2. K. Weihrauch, **A Simple Introduction to Computable Analysis**, 1995.

عنوان درس	فارسی	جبرجامع							
	انگلیسی	**Universal Algebra**							
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی			۳	۴۸	ندارد
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد		**دنیاز به اجرای پروژه عملی:** ندارد							

هدف درس:

هدف از این درس آشنایی با کلاس‌های معادله‌ای و ساختارهای کلی جبری است. جبر جامع با نظریه مدل در منطق ریاضی مرتبط است.

سرفصل‌های درس:

جبرجامع، زیرجبر و مشبکه زیرجبرها، همریختی بین جبرهای جامع، رابطه همنهشتی، ضرب مستقیم جبرها، زیرضرب مستقیم، واریته، جبرآزاد، معادله وجبرهای معادله‌ای، قضیه بیرخوف برای ارتباط بین واریته وکلاس‌های جبرهای معادله‌ای.

مراجع پیشنهادی:

1. Burris and Sankapanavar, **A Course in Universal Algebra**, Springer-Verlag, 1981.
2. G. Gratezer, **Universal Algebra**, Second edition, Springer, 2008.
3. P. M. Cohn, **Universal Algebra**, D. Reidel Publication Company, 1981.

عنوان درس	فارسی	نظریه رسته و توپوس							
	انگلیسی	Category Theory and Topos							
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی				۳	۴۸	ندارد
نظری	عملی	نظری	عملی	نظری	عملی					
حل تمرین: ندارد				نیاز به اجرای پروژه عملی: ندارد						

هدف درس:

هدف از این درس آشنایی با نظریه رسته ونظریه توپوس است. یکی از کاربردهای مهم این مبحث فراهم نمودن مدلی برای منطق شهودی است.

سرفصل‌های درس:

معرفی رسته، تابع‌گون، تبدیل طبیعی، پیکان‌ها واشیای خاص، زیررسته، دوگان رسته، رسته تابع‌گون‌ها، پیکان جهانی، لم یوندا، حدو هم حد، الحاقی، رسته بسته دکارتی، شبه توپوس، توپوس، تجزیه در توپوس، مشبکه و جبر هیتینگ در توپوس، توپوس‌های خاص (بولی، دومقداری، موضعی) ، اصل انتخاب، شیءاعدادطبیعی.

مراجع پیشنهادی:

1. Goldblatt,Topoi: **The Categorical Analysis of Logic**, North-Holland, 1984.
2. Lambek and Scott, **Introduction to higher Order Logic**, Cambridge University Press, 1986
3. P. T. Johnston, **Topos Theory**, Dover Publications, 2014.

عنوان درس	فارسی	نظریه مشبکه							
	انگلیسی	Lattice Theory							
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی			۳	۴۸	ندارد
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد		نیاز به اجرای پروژه عملی: ندارد							

هدف درس:

هدف از این درس آشنایی با نظریه مشبکه است که در مطالعه مدل‌های جبری دستگاه‌های مختلف منطقی نقش اساسی ایفا می‌کند.

سرفصل‌های درس:

مشبکه، همریختی مشبکه، مشبکه کامل، مشبکه مدولار، مشبکه توزیع‌پذیر مشبکه هایتینگ، رابطه همنهشتی، جبربول، نمایش‌های مجموعه‌ای وتوپولوژیکی جبر بول (قضیه استون)، مشبکه جبری، مشبکه پیوسته، توپولوژی اسکات، توابع اسکات پیوسته، فضاهای سوبر و دوگانی جبر هیتینگ پیوسته.

مراجع پیشنهادی:

1. Gratzer, Birkhauser, **General Lattice Theory**, 1998.
2. Davey, Priestloy, **Introduction to Lattice and Order**, Cambridge University Press, 2002.
3. Blyth, **Lattices and Ordered Algebraic Structures**, Springer-Verlag, 2005.

عنوان درس	فارسی	ساختارهای جبری مرتب							
	انگلیسی	Ordered Algebraic Structures							
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی					
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد				نیاز به اجرای پروژه عملی:ندارد			۳	۴۸	ندارد

هدف درس:

هدف از این درس آشنایی با ساختارهای جبری مرتب است که در مطالعه مدل‌های جبری دستگاه‌های مختلف منطقی نقش ایفا می کند.

سرفصل‌های درس:

مفهوم ترتیب، نگاشت‌های حافظ ترتیب، نگاشت‌های باقیمانده‌ای، پستارها، یکریختی‌های مجموعه‌های مرتب، نیم‌گروه‌های نگاشت‌های باقیمانده‌ای، مشبکه‌ها و زیرمشبکه‌ها، زیرگروه‌های بثر، مجموعه‌های خارج‌قسمتی مرتب، هم‌ارزی‌های قویاً منظم بالایی، همنهشتی‌های مشبکه، زوج‌های مدولار، شرط‌های زنجیر، تحویل‌ناپذیری‌های الحاقی، مشبکه‌های پخشی، زیرگروه‌های بثر و مدولاریتی، عضوهای متمم‌دار،مشبکه‌های متمم‌دار منحصر بفرد، جبرها و حلقه‌های بولی، عضوهای مرکزی و خنثی، قضیه نمایشی Stone، متمم جبرهای بولی، شبه متمم‌ها، جبرهای Stone، جبرهای هیتینگ،زیرگروه‌های بثر و باقیمانده‌ای، همنهشتی‌ها و جبرهای تحویل‌ناپذیر زیر مستقیم، گروه‌های مرتب، زیرگروه‌های محدب، L-زیرگروه‌های مرتب، گروه‌های نمایش‌پذیر، حلقه‌ها و میدان‌های کلاً مرتب، زیرگروه‌های باقیمانده‌ای و زیرگروه مرتب، زیرگروه‌های منظم.

مراجع پیشنهادی:

1.T. S.Blyth, **Lattices and Ordered Algebraic Structures**, Springer-verlag, 2005.

2. G. Birkhoff, **Lattice Theory**, American Mathematical Society, 1973.

عنوان درس	فارسی	منطق شهودی							
	انگلیسی	**Intuitionistic Logic**							
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی			۳	۴۸	منطق ریاضی
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد				**نیاز به اجرای پروژه عملی:** ندارد					

هدف درس:

هدف از این درس آشنایی با منطق شهودی (شهودگرایی) است که یکی از مهم‌ترین رهیافت‌های ساختنی به منطق و ریاضیات است.

سرفصل‌های درس:

تاریخچه مختصری از ساخت‌گرایی در ریاضیات با تاکید بر شهودگرایی برآوری، تعبیر BHK (برآور- هیتینگ- کولموگوروف) از ثوابت منطقی، تعبیرهای توپولوژیک و جبری، دستگاه‌های صوری اثباتی برای منطق شهودگرایی گزاره‌ای و محمولات، معناشناسی جهان‌های ممکن (مدل‌های کریپکی)، قضایای درستی و تمامیت نسبت به مدل‌های کریپکی، خواص DP و EP.

مراجع پیشنهادی:

1. A. S. Troelstra and D. Van Dalen, **Constructivism in Mathematics**, Vol. I, North-Holland, 1988.
2. A. G. Dragalin, **Mathematical Intuitionism, Introduction to Proof Theory**, AMS, Providence, RI, 1988.
3- G. Mints, **A Short Introduction to Intuitionistic Logic**, Springer, 2013. (ISBN: 9781475773194)

عنوان درس	فارسی	منطق وجهی							
	انگلیسی	Modal Logic							
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی				۳	۴۸	منطق ریاضی
نظری	عملی	نظری	عملی	نظری	عملی					
حل تمرین: ندارد				**نیاز به اجرای پروژه عملی:** ندارد						

هدف درس:

هدف از این درس آشنایی با منطق وجهی است که یکی از مهم‌ترین منطق‌های غیر کلاسیک می‌باشد و کاربردهای مهمی در بخش روش‌های صوری (رسمی) از علوم کامپیوتر دارد.

سرفصل‌های درس:

زبان منطق وجهی، قاب‌ها و مدل‌های کریپکی، منطق وجهی نرمال، تناظر دوسویه، قضیه هنسی-میلنر، ترجمه استاندارد، قضیه مشخص‌سازی فن بنتم، تعریف‌پذیری قاب‌ها، مدل‌های کانونی، دستگاه‌های اثباتی و تمامیت، جبری کردن منطق وجهی، جبرهای بولی با عملگر، قضیه ینسن-تارسکی.

مراجع پیشنهادی:

1. P. Blackburn, M. de Rijke and Y.Venema, **Modal Logic**, Cambridge University Press, 2002.
2. A. Chagrov and M. Zakharyaschev, **Modal Logic**, Clarendon Press, Oxford, 1997.
3. J. van Benthem, **Modal Logic for Open Minds**, CSLI Publications, 2010.
4- B.F. Chellas, **Modal Logic: An Introduction**, Cambridge University Press, 2012. (ISBN: 9780511621192)

عنوان درس	فارسی	فلسفه ریاضی							
	انگلیسی	Philosophy of Mathematics							
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی				۳	۴۸	منطق ریاضی
نظری	عملی	نظری	عملی	نظری	عملی					
حل تمرین: ندارد				نیاز به اجرای پروژه عملی: ندارد						

هدف درس:

هدف از این درس آشنایی با برخی فلسفه‌های مشهور ریاضی است.

سرفصل‌های درس:

افلاطون‌گرایی، واقع‌گرایی، نام‌گرایی، کانت، منطق‌گرایی، صورت‌گرایی، برنامه هیلبرت، قضیه‌های ناتمامیت گودل، شهودگرایی (برآور، دامت)، طبیعی‌گرایی، ساختارگرایی، حوزه‌های جدید در فلسفه ریاضی.

مراجع پیشنهادی:

1. James Robert Brown, **Philosophy of Mathematics: A Contemporary Introduction to the World of Proofs and Pictures**, 2nd Edition, Routledge, 2008.
2. **The Oxford Handbook of Philosophy of Mathematics and Logic**, Stewart Shapiro (Editor), 2007.
3. Stewart Shapiro, **Philosophy of mathematics: Structure and ontology**, Oxford, Oxford University Press, 1997.
4- P. Benaceraf & H. Putnam, **Philosophy of Mathematics**, Cambridge University Press, 1984. (ISBN: 9780521296489)

عنوان درس	فارسی	نظریه پیشرفته مدل							
	انگلیسی	**Advanced Model Theory**							
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی			۳	۴۸	نظریه مدل
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد				**نیاز به اجرای پروژه عملی:** ندارد					

هدف:

سرفصل‌های درس:

مدل‌های اول، همگن، جهانی و آکنده ، زدایش تایپ، قضیه Ryll-Nardzewski، آکندگی، همگنی و جهانی بودن، کاربردهای آکندگی، دنباله‌ها و مجموعه‌های تمایزناپذیر، مدل‌های اِرنفویخت- موستاوسکی، جفت‌ها واتی، قضیه دو- کاردینال وات، پایداری وω-پایداری، قضیه جازمیت مورلی، رتبه ودرجه مورلی، آشنایی با ناوابستگی و فورکینگ درنظریه‌های ω-پایدار، آشنایی با گروه‌های ω-پایدار.

مراجع پیشنهادی:

1. K. Tent, M. Ziegler, **A Course in Model Theory,** Cambridge University Press, 2012.
2. S. Buechler, **Essential Stability Theory,** Springer, 1996.
3. C.C. Chang, H. Jerome Keisler, **Model Theory,** North-Holland, 1990.
4. A. Marcja, C. Toffalori, **A Guide to Classical and Modern Model Theory,** Kluwer Academic Publishers, 2003.
5. D. Marker, **Model Theory, An Introduction**, Springer, 2002.
6. A. Pillay, **Geometric Stability Theory**, Clarendon Press-Oxford, 1996.
7. B. Poizat, **A Course in Model Theory**, Springer, 2000.

عنوان درس	فارسی	نظریه پیشرفته مجموعه							
	انگلیسی	Advanced Set Theory							
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی			۳	۴۸	نظریه مجموعه
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد				نیاز به اجرای پروژه عملی: ندارد					

هدف:

سرفصل‌های درس:

ازمیان موردهای زیرگزیده خواهد شد:

۱. نیرش (forcing) و دستاوردهای ناوابستگی، نیرش ومدل‌های هرویک (generic)، بنداشت مارتین، ناوابستگی بنداشت انتخاب و بنداشت پیوستار،کاردینال های بزرگ

۲. نظریه توصیفی مجموعه ها: فضای بئر، فضاهای لهستانی، پایاگان بورل، مجموعه‌های واکاویک(analytic) و همواکاویک، کاردینال یک مجموعه واکاویک، پایگان افکنشی.

مراجع پیشنهادی:

1.K. Ciesielski, **Set Theory for Working Mathematicians,** Cambridge, 1997.

2. T. Jech, **Set Theory**, Springer, 2013.

3. A.S. Kechris**, Classical Descriptive Set Theory, Springer**, 1995.

4. K. Kunen, **Set theory, An Introduction to Independence Proofs**, North-Holland, 1992.

5. R.M. Smullyan, M. Fitting**, Set Theory and the Continuum Problem**, Oxford, 1996.

عنوان درس	فارسی	مدل‌های نااستاندارد حساب							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
	انگلیسی	Non-Standard Models of Arithmetic									
		نوع واحد									
		الزامی		اختیاری		جبرانی			۳	۴۸	منطق ریاضی، نظریه مدل
		نظری	عملی	نظری	عملی	نظری	عملی				
		حل تمرین: ندارد				نیاز به اجرای پروژه عملی: ندارد					

هدف:

سرفصل‌های درس:

حساب پئانو، قالب‌های درهازش (induction)، اصل کوچکترین عدد و اصل گردایه، شکاف (cut)، سرریز و پایین ریز، گسترش‌های دربایان و هم‌پایان، سامانه استاندارد، تایپ‌ها و شمارا آکندگی، قضیه نشاندن فریدمن، قضیه MacDowel-Specker، ژیر نظریه‌های حساب‌ها، ارتباط با نظریه بازگشت، پیچیدگی محاسبه، نظریه برهان، ریاضیات همساختی و برهان‌پذیری .

مراجع پیشنهادی:

1. R. Kossak, J. Schmerl, **The Structure of Models of Peano Arithmetic**, Clarendon Press, Oxford, 2006
2. P. Hajek and P. Pudlak, **Meta mathematics of first order arithmetic**, Springer, 1998
3. R. Kaye, **Models of Peano Arithmetic**, Oxford, 1991
4. C. Smorynski, **Logical Number Theory**, Springer, 1992
5. A. S. Troelstra and D. van Dalen, **Constructivism in Mathematics**, Northh-Holland, 1998.

عنوان درس	فارسی	منطق و محاسبه							
	انگلیسی	Logic and Computation							
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی				۳	۴۸	منطق ریاضی
نظری	عملی	نظری	عملی	نظری	عملی					
حل تمرین: ندارد				**نیاز به اجرای پروژه عملی:** ندارد						

هدف:

سرفصل‌های درس:

در این درس از میان موارد زیر یا دیگر موضوع‌های مرتبط به کاربردهای منطق در علوم کامپیوتر پرداخته می‌شود:

۱. منطق و نظریه پیچیدگی: شامل پیچیدگی اثبات گزاره‌ای، حساب محدود، نظریه مدل‌های متناهی.

۲. منطق و روش‌های صوری (رسمی): شامل منطق زمانی، شناختی و پویا، بررسی مدل (Model Checking)، درست‌یابی برهان (Proof Verification).

۳. ساختارهای محاسبه‌پذیر، نظریه مدل محاسبه‌پذیر.

۴. تناظر برهان‌ها و برنامه‌ها: شامل منطق شهودی، حساب λ، تناظر Curry-Howard.

مراجع پیشنهادی:

1. Jan Krajicek, **Bounded Arithmetic, Propositional Logic and Complexity Theory**, Cambridge University Press, 1995.
2. H. van Ditmarsch, W. van der Hoek, B. Kooi, **Dynamic Epistemic Logic**, Springer, 2008.
3. F. Kröger and S. Merz, **Temporal Logic and State Systems**, Springer, 2008.
4. M. H. Sørensen and P. Urzyczyn, **Lectures on Curry-Howard Isomorphism**, Elsevier, 2006.

عنوان درس	فارسی	منطق فازی پیشرفته							
	انگلیسی	Advanced Fuzzy Logic							
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی			۳	۴۸	منطق ریاضی
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد		نیاز به اجرای پروژه عملی: ندارد							

هدف درس:

هدف از این درس آشنایی با منطق فازی به عنوان بخشی از منطق ریاضی است.

سرفصل‌های درس:

t- نرم‌ها، منطق گزاره‌ای BL، منطق لوکاسیویچ گزاره‌ای، منطق ضرب گزاره‌ای، منطق گودل گزاره‌ای، ساختارهای جبری مرتبط با منطق‌های یاد شده، قضیه تمامیت، منطق پایه محمولی، منطق لوکاسیویچ محمولی، منطق گودل محمولی، نظریه مدل منطق‌های یاد شده، قضیه‌های تمامیت مرتبط.

مراجع پیشنهادی:

1. P. Hájek, **Metamathematics of Fuzzy Logic**, Kluwer Academic Publishers, 1998.
2- J. T. Starczewski, **Advanced Concepts in Fuzzy Logic and Systems with Membership Uncertainty**, Springer, 2014. (ISBN: 9783642448522)
3- H. J. Zimmerman, **Fuzzy Set Theory and Its Applications**, Springer, 2012. (ISBN: 9789401038706)

عنوان درس	فارسی	نظریه پیشرفته محاسبه پذیری							
	انگلیسی	Advanced Computability Theory							
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی			۳	۴۸	نظریه محاسبه پذیری
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد				**نیاز به اجرای پروژه عملی:** ندارد					

هدف:

سرفصل های درس:

اوراکل ها و محاسبات نسبی، درجات محاسبه(نا)پذیری، سلسله مراتب تحلیلی و تصویری، اوردینال های محاسبه پذیر، سلسله مراتب فراحسابی، توابع محاسبه پذیر روی اعداد حقیقی، اندازه و نیرش (forcing)، حساب لامبدا.

مراجع پیشنهادی:

1- P. Odifreddi, **Classical Recursion Theory: The Theory of Functions and Sets of Natural Numbers**, *Vol. 1*, North-Holland, 1992. (ISBN: 9780444894830)

2- P. Odifreddi, **Classical Recursion Theory: The Theory of Functions and Sets of Natural Numbers**, *Vol. 2*, North-Holland, 1999. (ISBN: 9780444502056)

3- J.R. Shoenfield, **Recursion Theory**, Springer, 2013. (ISBN: 9783540570936)

4- G.E. Sacks, **Higher Recursion Theory**, Springer, 1990. (ISBN: 9783540193050)

عنوان درس	فارسی	نظریه پیشرفته برهان							
	انگلیسی	**Advanced Proof Theory**							
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی				۳	۴۸	نظریه برهان
نظری	عملی	نظری	عملی	نظری	عملی					
حل تمرین: ندارد				**نیاز به اجرای پروژه عملی:** ندارد						

هدف:

سرفصل‌های درس:

برهان گنتزن برای سازگاری حساب پئانو، توابع تعریف پذیر تام در نظریه های حسابی، آنالیز اوردینالی، طول برهان و پیچیدگی آن، منطق اثبات پذیری، ریاضیات معکوس، نظریه تایپ، تناظر Curry-Howard.

مراجع پیشنهادی:

1- S.R. Buss (ed.) **Handbook of Proof Theory**, Elsevier Science, 1998. (ISBN: 9780444898401)

2- S. Negri and J. von Plato, **Proof Analysis: A Contribution to Hilbert's Last Problem**, Cambridge University Press, 2014. (ISBN: 9781107417236)

3- W. Pohlers, *Proof Theory:* **The First Step into Impredicativity**, Springer, 2010. (ISBN: 9783540693185)

عنوان درس	فارسی	منطق جبری							
	انگلیسی	Algebraic Logic							
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی				۳	۴۸	اجازه گروه
نظری	عملی	نظری	عملی	نظری	عملی					
حل تمرین: ندارد				نیاز به اجرای پروژه عملی: ندارد						

هدف:

سرفصل‌های درس:

عملگرهای نتیجه در منطق ها، ماتریس های منطقی، جبرهای لیندنبام، تارسکی، منطق های جبرپذیر، نظریه منطق جبری مجرد، اصول نظریه عمومی جبرجامع، دستگاه های گنتزن وتعمیم آن ها، سیستم های بستاری، جبرهای آزاد، جبرهای بولی، واریته ها، چارچوب عمومی مطالعه منطق ها، چارچوب جدید برای مطالعه منطق ها، پل بین جهان منطق ها وجهان جبرها، همتای جبری منطق ها، سیستم استنتاجی هیلبرت وتعمیم آن ها، جبری کردن خواص تامیت و فشردگی منطق ها، منطق های جدید، جبر رابطه ها.

مراجع پیشنهادی:

1. Hajnal Andreka, Istran Nemati, Ildiko Sain, **Universal Algebraic Logic**, Springer Bassel, 20017.
2. J.M. Font, R. Jansana, D. Pigozzi, **A Survey of Abstract Algebraic Logic**, Hand Book of Algebraic Logic.

عنوان درس	فارسی	مباحث ویژه در منطق ریاضی								
	انگلیسی	Special Topics in Logic								
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
الزامی		اختیاری		جبرانی				۳	۴۸	اجازه گروه
نظری	عملی	نظری	عملی	نظری	عملی					
حل تمرین: ندارد		نیاز به اجرای پروژه عملی: ندارد								

درسی است در سطح دکتری در زمینه منطق ریاضی که سرفصل آن بر حسب امکانات و نیاز درنیم‌سال مورد نظر توسط استادمربوطه پیشنهاد شده وپس از تصویب شورای تحصیلات تکمیلی گروه و دانشکده ارایه می‌شود.

دکتری ریاضی

(زیر برنامه گراف و ترکیبیات)

فصل اول

مشخصات دوره دکتری ریاضی – زیر برنامه گراف و ترکیبیات

مقدمه:

برنامه حاضر حاصل تخصص، تجربه و هم‌فکری اعضای زیر کمیته تخصصی گراف و ترکیبیات، منتخب کمیته تخصصی برنامه-ریزی علوم ریاضی در وزارت علوم است که متشکل از متخصصین از دانشگاه‌های مختلف کشور با سابقه تدریس و تحقیق در مقاطع مختلف و تجربه تربیت دانشجویان دکتری در زمینه گراف و ترکیبیات است.

هدف:

در این برنامه اهداف زیر مورد نظر قرار گرفته است.

۱. پوشش مفاهیم دسته‌بندی شده در رده‌بندیMSC 2010 در زمینه تخصصی گراف و ترکیبیات
۲. کتاب‌های استاندارد و به روز دنیا در زمینه تخصصی گراف و ترکیبیات
۳. در حد ممکن همخوانی با دروس موجود در دانشگاه‌های مطرح دنیا در زمینه تخصصی گراف و ترکیبیات
۴. حفظ استاندارد بالا و داشتن عمق کافی

کلیات برنامه:

در این برنامه دروس در دوجدول، شامل درس‌های اصلی دکتری ریاضی (زمینه تخصصی نظریه گراف و ترکیبیات) (جدول ۱)و درس‌های تخصصی- انتخابی دکتری ریاضی (زمینه تخصصی نظریه گراف و ترکیبیات) (جدول ۲) آورده شده است. هر دانشجو بایستی ۶ واحد الزامی خود را از دروس جدول ۱ و ۶ واحد انتخابی خود را از بین دروس جدول شماره ۲ یا درس اخذ نشده از جدول ۱ اخذ نماید. ۳ واحد باقیمانده یک درس کاملا اختیاری است که با نظر استاد راهنما و تأیید گروه اخذ خواهد شد. مجری این دوره می تواند گروه ریاضیات و کاربردها یا گروه ریاضی کاربردی باشند.

عنوان دوره: دکترای ریاضی

پیش‌نیاز ورود:

دو درس نظریه گراف و آنالیز ترکیبیاتی از دروس مقطع کارشناسی ارشد، پیش‌نیاز سایر دروس می‌باشند و انتظار می‌رود دانشجو در مقطع کارشناسی‌ارشد آنها را گذرانده باشد. در غیر این‌صورت بنا به تشخیص استاد راهنما و گروه می‌تواند به عنوان درس جبرانی خارج از تعداد واحدهای الزامی دوره در نظر گرفته شود و در این صورت به سنوات تحصیلی دانشجو یک نیم‌سال اضافه خواهد شد.

مواد آزمون تخصصی ورودی(کنکور):

دو درس نظریه گراف و آنالیز ترکیبیاتیاز دروس مقطع کارشناسی ارشد

فصل دوم

جدول دروس دکتری ریاضی – زیر برنامه گراف و ترکیبیات

جدول ۱: درس‌های اصلی دکتری ریاضی – زیر برنامه گراف و ترکیبیات

شماره درس	نام درس	تعداد واحد	پیش‌نیاز
۱	نظریه گراف پیشرفته	۳	نظریه گراف
۲	آنالیز ترکیبیات پیشرفته	۳	آنالیز ترکیبیاتی
۳	روش‌های پایه در ترکیبیات	۳	نظریه گراف و آنالیز ترکیبیاتی

- انتخاب ۶ واحد از جدول فوق به عنوان دروس اصلی زمینه تخصصی با نظر استاد راهنما و دانشکده.
- دانشجو می‌تواند سایر دروس جدول فوق را به عنوان درس تخصصی – انتخابی خود انتخاب کند

جدول۲: درس‌های تخصصی-انتخابی دکتری ریاضی –زیر برنامه گراف و ترکیبیات

شماره درس	نام درس	تعداد واحد	پیش‌نیاز و هم‌نیازها
۱	نظریه جبری گراف	۳	نظریه گراف
۲	نظریه طیفی گراف	۳	نظریه جبری گراف
۳	روش‌های احتمالاتی در ترکیبیات	۳	نظریه گراف
۴	ترکیبیات شمارشی	۳	
۵	ترکیبیات تحلیلی	۳	
۶	ترکیبیات جمعی	۳	
۷	ترکیبیات حدی	۳	
۸	روش‌های توپولوژیک در ترکیبیات	۳	
۹	هندسه ترکیبیاتی	۳	
۱۰	نظریه الگوریتمی گراف	۳	
۱۱	بهینه‌سازی ترکیبیاتی	۳	
۱۲	پیچیدگی محاسباتی	۳	
۱۳	مباحث ویژه در نظریه گراف	۳	اجازه گروه
۱۴	مباحث ویژه در ترکیبیات	۳	اجازه گروه

فصل سوم

سر فصل دروس دکتری ریاضی– زیر برنامه گراف و ترکیبیات

عنوان درس	فارسی	نظریه گراف پیشرفته						
	انگلیسی	Advanced Graph Theory						
نوع واحد								
	اصلی		انتخابی		جبرانی		تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
	نظری	عملی	نظری	عملی	نظری	عملی			
	✓		✓			✓	۳	۴۸	نظریه گراف
حل تمرین: ندارد					**نیاز به اجرای پروژه عملی:** ندارد				

هدف: آشنایی با مفاهیم پیشرفته نظریه گراف.

سرفصل‌های درس:

- **همبندی:** ساختار گراف‌های ۲، ۳و ۴- همبند، قضیه Mader، قضیه Nashwilliams- Tutteدر مورد درخت-های فراگیر مجزا.
- **رنگ‌آمیزی:** مباحث تکمیلی در رنگ‌آمیزی رأسی به ویژه قضیه گراف‌های بی‌نقص، مباحث تکمیلی در رنگ‌آمیزی یالی به ویژه مسأله رده‌بندی کلاس‌های ۱ و ۲، رنگ‌آمیزی لیستی و اثبات قضیه گالوین.
- **گراف‌ها روی رویه‌ها:** رسم گراف‌های مسطح، عدد تقاطعی گراف، گونه گراف‌ها، رسم گراف‌ها بر روی سطوح با شرایط خاص.
- **عرض درختی و مسیری و برخی از کاربردهای آن.**
- **ماینورهای گراف:** قضیه ۴-رنگ، حدس Hadwiger در حالت‌های کوچک، بیان قضیه Graph Minor و اثبات آن برای درخت‌ها.
- **جریان‌های صحیح گراف:** قضایای وجودیk- جریان برای kهای کوچک، قضایای مربوط به معادل بودن وجود k-جریان‌ها، دوگانی جریان و رنگ‌آمیزی و بیان حدس‌های تات.
- **فضاهای برداری متناظر با گراف:** فضاهای دوری، فضاهای برشی، تعریف مترویدد، شبکه‌های الکتریکی، قدم زدن تصادفی.
- **چندجمله‌ای‌های گراف:** چندجمله‌ای تات و تعریف‌های معادل آن و ارتباط آن با سایر چندجمله‌ای‌ها. بحث در مورد چندجمله‌ای‌های دیگر مانند چندجمله‌ای تطابقی.
- **گراف‌ها، گروه‌ها و ماتریس‌ها:** گراف‌های کیلی و شرایر، ماتریس مجاورت، لاپلاسین و مقادیر ویژه آنها، گراف‌های قویا منظم، گروه خودریختی‌ها و مسایل یکریختی و همریختی در گراف‌ها.

مراجع پیشنهادی:

1. Bondy J.A., Murty U.S.R., Graph Theory, Springer, 2008.
2. West, Douglas B.Introduction to Graph Theory, Second edition, 2001.
3. Diestel R., Graph Theory, Fourth edition, 2010.
4. Bollobás B., Modern Graph Theory, 1998.

عنوان درس	فارسی	آنالیز ترکیبیاتی پیشرفته						
	انگلیسی	Advanced Combinatorial Analysis						

نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
اصلی		انتخابی		جبرانی			۳	۴۸	آنالیز ترکیبیاتی
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد				**نیاز به اجرای پروژه عملی:** ندارد					

هدف:آشنایی با مفاهیم پیشرفته آنالیز ترکیبیاتی.

سرفصل‌های درس:

- **نظریه اکسترمال مجموعه‌ها:**مجموعه‌های جزئی مرتب، قضیه دیلورث، قضیه اسپرنر، قضیه اردوش-کو- رادو
- **جریان در شبکه‌ها:** قضیه صحیح بودن، تعمیمی از قضیه بیرکهف
- **دنباله‌های دبروین:** تعداد آنها
- **کدها و طرحها:** تعریف اولیه کدگذاری **انواع کران‌ها ، قضیه مک ویلیامز ،** قضیه اسموس- متسون ، کدهای گولی، کد از صفحات تصویری
- **گراف‌های قویا منتظم و هندسه‌های جزئی:** جبر بز- منسر، مقادیر ویژه، کران ،سه‌های جزئی
- **مشبکه‌ها و وارون موبیوس:** جبر وقوعی مجموعه‌های جزئی مرتب تابع موبیوس ،جمله‌ای رنگی گراف، کدهای MDS
- **مجموعه‌های تفاضلی:** انواع آن
- **روش‌های جبری در نظریه گراف:** مقادیر ویژه، ظرفیت شنون، کران هافمن، قضیه پرون-فروبنیوس، در هم بافتگی
- **قضیه بارانیای:** افراز طرح‌های کامل

مراجع پیشنهادی:

1. Van Lint, J.H. and Wilson, R.M., A Course in Combinatorics, 2003.
2. Cameron, Peter J., Combinatorics; Topics, Techniques, Algorithms, 1996.

عنوان درس	فارسی	روش‌های پایه در ترکیبیات							
	انگلیسی	Basic Methods in Combinatorics							
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
اصلی		انتخابی		جبرانی			۳	۴۸	نظریه گراف و آنالیز ترکیبیاتی
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد		نیاز به اجرای پروژه عملی: ندارد							

هدف: آشنایی با کلیات مفاهیم و روش‌های مهم و مورد نیاز در زمینه تخصصی گراف و ترکیبیات.

سرفصل‌های درس:

- **یادآوری روش‌های شمارش دوگانه و روش شمارش استفاده از انواع توابع مولد**
- **لم منظم زمردی (Regularity Zemeredy Lemma): اثبات و برخی کاربردها.**
- **جنبه‌های الگوریتمی: معرفی کلاس‌های پیچیدگی P و NP.**
- **برنامه‌ریزی خطی و الگوریتم‌های تقریب برای حل مسایل نظریه گراف.**
- **روش‌های احتمالاتی**
- **نظریه رمزی**
- **مترویدها**
- **روش دشارژ کردن**

مراجع پیشنهادی:

1. Bondy J.A., Murty U.S.R., Graph Theory, Springer, 2008.
2. West, Douglas B.Introduction to Graph Theory, Second edition, 2001.
3. Diestel R., Graph Theory, Fourth edition, 2010.
4. Bollobás B., Modern Graph Theory, 1998.
5. Cranston, D.W., West Douglas B., A Guide for the Discharging Method, 2013.

عنوان درس	فارسی	نظریه جبری گراف						
	انگلیسی	Algebraic Graph Theory						
نوع واحد						تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
اصلی		انتخابی		جبرانی		۳	۴۸	نظریه گراف
نظری	عملی	نظری	عملی	نظری	عملی			
حل تمرین: ندارد		**نیاز به اجرای پروژه عملی:** ندارد						

هدف: آشنایی با گروه خودریختی‌های گراف‌ها و ارتباط آنها با خواص گراف‌ها.

سرفصل‌های درس:

- **مطالعه طیف ماتریس‌های متناظر با گراف‌ها مانند ماتریس مجاورت و لاپلاسین و ارتباط آنها با خواص گراف‌ها.**
- **یافتن طیف برخی از گراف‌هایخاص.**
- **قضیه پرون- فریبنیوس.**
- **روابط درهم پیچیدگی.**
- **گراف‌های هم طیف.**
- **افرازهای منصفانه، گراف‌های قویا منظم و مقادیر ویژه آنها، NEPS گراف‌ها.**
- **قضیه درخت- ماتریس.**
- **عدد همبندی جبری گراف‌ها، Expansion و نامساوی چیگر.**
- **Associated Schemes.**
- **همریختی بین گراف‌ها، انقباض گراف‌ها، یکریختی بین گراف‌ها، گروه خودریختی‌های گراف‌ها.**
- **گراف‌های راس ترایا، گراف‌های یال ترایا، گراف‌های کمان ترایا، گراف‌های فاصله ترایا.**
- **گراف‌های فاصله منظم، گراف‌های کیلی. گرافهای شرایر و گراف‌های هم مجموعه.**
- **گراف‌های اولیه و غیر اولیه.**

مراجع پیشنهادی:

1. Cvetkovic, D., Rowlinson P. and Simic S., Introduction to the Theory of Graph Spectra, 2010.
2. Biggs,N., Algebraic Graph Theory, 1993.
3. Cvetkovic, D., Doob M. and Sachs, Spectra of Graphs, 1995.
4. Brouwer A.E. and Haemers, W.H., Spectra of Graphs, Springer, 2011.
5. Godsil G. and Royle G., Algebraic Graph Theory, 2001.
6. Beineke L.W. and Wilson R.J., Topics in Algebraic Graph Theory, 2004.

عنوان درس	فارسی	نظریه طیفی گراف						
	انگلیسی	Spectral Graph Theory						
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
اصلی		انتخابی		جبرانی			۳	۴۸	نظریه جبری گراف
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد				نیاز به اجرای پروژه عملی: ندارد					

هدف: آشنایی با طیف و فضای ویژه گراف‌ها و ارتباطات خواص جبری و ترکیبیاتی آن‌ها.

سرفصل‌های درس:

- **طیف‌های ماتریس مجاورت و ماتریس لاپلاسین.**
- **رده بندی به کمک طیف.**
- **همبندی:** همبندی جبری، رسانایی و تنک‌ترین برش.
- **مسائل ایزوپریمتری:** نامساوی چیگر، توسیع راسی و یالی گراف‌ها.
- **گراف‌های توسیعی و کاربردهای آن در علوم کامپیوتر و کدینگ.**
- **فضای ویژه:** قضیه پرون فروبینوس، قضیه فیدلر و دامنه‌های نودال.
- **گشت تصادفی روی گراف‌ها و زمان اختلاط.**
- **افراز ستاره‌ای، تکنیک‌های زاویه، بازسازی.**
- **مقادیر ویژه گراف‌های تصادفی.**
- **تخمین گراف‌ها و تنک سازی.**
- **مقادیر ویژه زیرگراف‌ها با شرایط مرزی.**

مراجع پیشنهادی:

1. Chung, F.R.K.,Spectral Graph Theory, 1997.

2. Cvetkovic, D., Rowlinson P., Simic S., Eigenspaces of Graphs (Encyclopedia of Mathematics and its Applications) 1st Edition, 1997.

3. Hoory S., Linial N. and Wigderson, A., Expanders and their Applications, 2006.

عنوان درس	فارسی	روش‌های احتمالاتی در ترکیبیات						
	انگلیسی	Probabilistic Methods in Combinatorics						
نوع واحد								
اصلی		انتخابی		جبرانی		تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
نظری	عملی	نظری	عملی	نظری	عملی	۳	۴۸	نظریه گراف
حل تمرین: ندارد			نیاز به اجرای پروژه عملی: ندارد					

هدف:

آشنایی با روش‌ها و ابزارهای احتمالاتی در حل مسایل ترکیبیاتی.

سرفصل‌های درس:

- یادآوری برخی اثبات‌ها و مفاهیم اولیه احتمالاتی اولیه برای مساله‌های نظریه گراف و ترکیبیات.
- روش اولین گشتاور، نامساوی مارکف و کاربردهای آن.
- استفاده از خطی بودن امید ریاضی.
- روش دومینگشتاور، نامساوی چبیشف و کاربردهای آن.
- لم موضعی لواس و کاربردهای آن.
- مارتینگل‌ها، نامساوی آزوما و کاربردهای آن.
- نامساوی ین سن.
- تالاگراند.
- نتایجی در مورد گراف‌های تصادفی.

مراجع پیشنهادی:

1. Alon, A. and Spencer J.I., The Probabilistic Method, John Wiley & Sons Inc., Third edition, 2008.
2. Molloy, M and Reed B., Graph Coloring and Probabilistic Method, Springer, 2002.

عنوان درس	فارسی	ترکیبیات شمارشی							
	انگلیسی	Enumerative Combinatorics							
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
اصلی		انتخابی		جبرانی			۳	۴۸	
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد			نیاز به اجرای پروژه عملی: ندارد						

هدف: آشنایی با روش‌های پیشرفته و تکمیلی شمارشی در ترکیبیات.

سرفصل‌های درس:

- **یادآوری مفاهیم پایه در شمارش:** ترتیب، ترکیب، اصل شمول و عدم شمول، شمارش جایگشت‌ها با محدودیت مکانی.
- **روش‌های شمارش پیشرفته:** شمارش دوگانه، جدول Twelvefold، روش شمارش پولیا، روش‌های غربال.
- **مجموعه‌های مرتب جزیی:** شبکه‌ها، شبکه‌های توزیعی، زنجیرها، مجموعه‌های مرتب جزیی اویلری، مجموعه‌های مرتب جزیی دو جمله‌ای، فرمول معکوس موبیوس، روش‌های محاسبه تابع موبیوس، چندجمله‌ای زتا.
- **توابع مولد و توابع مولد گویا.**

مراجع پیشنهادی:

1- Stanley R.P., Enumerative Combinatorics Vol 1, CUP, 1997.

2- Aigner M., A Course in Enumeration. Springer, 2007.

عنوان درس	فارسی	ترکیبیات تحلیلی							
	انگلیسی	Analytic Combinatorics							
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
اصلی		انتخابی		جبرانی			۳	۴۸	
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد				نیاز به اجرای پروژه عملی: ندارد					

هدف: آشنایی با روش‌های تحلیلی برای مطالعه ساختارهای ترکیبیاتی بزرگ.

سرفصل‌های درس:

- **ساختارهای ترکیبیاتی و توابع مولد عادی:** روش‌های شمارش صوری، ترکیبات و افرازها، کلمات و زبان‌های منظم، ساختارهای درختی.
- **ساختارهای برچسب‌دار و توابع مولد نمایی:** ساختارهای برچسب‌دار، توابع پوشا، افرازها، کلمات، جایگشت‌ها، درخت‌های برچسب‌دار و گراف‌های برچسب‌دار.
- **پارامترهای ترکیبیاتی و توابع مولد چند متغیره:** توابع مولد دو متغیره و توزیع‌های احتمال، پارامترهای موروثی و توابع مولد، پارامترهای بازگشتی.
- **آنالیز مختلط و آنالیز مجانبی:** توابع مولد و توابع تحلیلی مختلط، نقاط تکین و رشد نمایی ضرایب، طرح کلی آنالیز مجانبی با ارائه مثال از دنباله‌های تودرتو، کسرهای مسلسل و مسیرها در گراف‌ها.
- **آنالیز تکینگی توابع مولد و کاربردها:** ارائه اصول نظریه تکینگی و رفتار مجانبی ضرایب با ارائه مثال‌های مناسب ترکیبیاتی به عنوان مثال از ساختارهای درختی یا ساختارهای مستقل از متن و نظایر آن.

مراجع پیشنهادی:

1- Philippe Flajolet and Robert Sedgewick, Analytic Combinatorics, Cambridge University Press, 2009.

عنوان درس	فارسی	ترکیبیات جمعی						
	انگلیسی	Additive Combinatorics						
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
اصلی		انتخابی		جبرانی			۳	۴۸	
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد				نیاز به اجرای پروژه عملی: ندارد					

هدف: آشنایی با ترکیبیات محاسباتی.

سرفصل‌های درس:

- یادآوری مفاهیم اصلی از روش‌های احتمالاتی و قضایای اصلی.
- بحث در مورد ایده‌های اصلی موضوع درس (discrepancy و ارتباط با نظریه Ramsey).
- ارائه ایده‌های اصلی ترکیبیات جمعی با مثال.
- قضیه van der Warden.
- قضیه‌های Hales-Jewett و Erdös-Turan.
- طرح ایده چگونگی استفاده از روش‌های آنالیز فوریه و اثبات قضیه Roth.
- بحث در مورد روش Gowers و اثبات قضیه Szemerèdi، قضیه Freiman و قضیه Green-Tao.
- جمع‌بندی نتایج و تکنیک‌های درس.

مراجع پیشنهادی:

1- Tao, T., Van H. Vu, Additive Combinatorics, Cambridge University Press, 2006.

2. Gowers, T., Additive and Combinatorial Number Theory, Lecture Notes, 2006.

عنوان درس	فارسی	ترکیبیات حدی (اکسترمال)							
	انگلیسی	**Extremal Combinatorics**							
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
اصلی		انتخابی		جبرانی			۳	۴۸	
نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد				**نیاز به اجرای پروژه عملی:** ندارد					

هدف: معرفی قضایای اصلی ترکیبیات اکسترمال، همچنین آشنایی با روش‌ها و ابزارهای گوناگون برای حل مسایل اکسترمال در ترکیبیات.

سرفصل‌های درس:

- نظریه رمزی، قضیه توران و اردوش-استون، مساله‌های توران دوبخشی.
- Regularity Lemma و کاربردهای آن (همچنین Lemma Counting و Lemma Embedding).
- Method Stability.
- نظریه مجموعه‌های اکسترمال و روش‌های جبرخطی شامل قضیه اردوش-کو-رادو، لم اسپرنر، قضیه کروسکال-کاتونا، قضیه فیشر، قضیه فرانکل-ویلسون و ....
- Choice Dependent Random، روش‌های آنالیز فوریه.
- حد گراف‌ها و Algebra Flag.
- روش‌های توپولوژی جبری در مساله‌های اکسترمال.

مراجع پیشنهادی:

1. Jukna, S., *Extremal Combinatorics with Applications in Computer Science*, 2011.
2. Bollobás, B., *Modern Graph Theory*, 1998.
3. Babai, L. and Frankl P., *Linear Algebra Methods in Combinatorics with Applications to Geometry and Computer Science*, 1992.
4. Matoušek, J., *Thirty-three Miniatures: Mathematical and Algorithmic Applications of Linear Algebra*, 2010.

عنوان درس	فارسی	روش‌های توپولوژیکی در ترکیبیات						
	انگلیسی	Topological Methods in Combinatorics						
نوع واحد						تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
اصلی		انتخابی		جبرانی		۳	۴۸	
نظری	عملی	نظری	عملی	نظری	عملی			
حل تمرین: ندارد		**نیاز به اجرای پروژه عملی:** ندارد						

هدف: آشنایی با چگونگی به کار گیری ابزار و نتایج توپولوژی در حل مسایل ترکیبیات.

سرفصل‌های درس:

- مقدمه‌ای بر مجتمع‌های سادکی.
- صورت‌های مختلف قضیه بورساک- اولام و کاربردهای آن، معادل‌ها و تعمیم‌های قضیه بورساک- اولام.
- لم‌های تاکر، کی- فن و تاکر کی- فن.
- قضیه ساندویچ ژامبون.
- افراز گردنبند.
- حدس کنسر و تعمیم آن.
- عدد همبندی مجتمع‌های سادکی و قضیه لواز.
- قضیه نقطه ثابت براور.
- لم اشپرنر و چند کاربرد آن، ضرب حذفی، اتصال حذفی.
- قضیه ون کمپن، قضیه فلور.
- کران‌های پایین برای عدد رنگی، قضایای توپولوژیکی و رنگی تیوربرگ.

مراجع پیشنهادی:

1. Matousek, J., Using the Borsuk –Ulam Theorem, Springer 2003.
2. Kozlov, D., Combinatorial Algebraic Topology, Springer 2008.
3. Longueville, M. de, A Course in Topological Combinatorics, 2013.

عنوان درس	فارسی	هندسه ترکیبیاتی						
	انگلیسی	Combinatorial Geometry						
نوع واحد						تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
اصلی		انتخابی		جبرانی				
نظری	عملی	نظری	عملی	نظری	عملی			
حل تمرین: ندارد		نیاز به اجرای پروژه عملی: ندارد						

هدف: بررسی و مطالعه ساختار و خواص ترکیبیاتی مجموعه ای از اشیاء هندسی

سرفصل های درس :

۱. مجموعه محدب، پوش محدب یک مجموعه، قضایای مهم هلی، رادون و کاراتئودوری و کاربردهای آنها، مفهوم ترنسورسال هندسی و قضیه ترنسورسال هادویگر
۲. مشبکه‌ها و قضایای پیک و مینکوفسکی
۳. بررسی خواص ترکیبیاتی مجموعه‌ای متناهی از نقاط: مسایل وقوع، قضایایی از نوع سیلوستر، مجموعه‌های چند فاصله‌ای، بررسی گراف‌های متناظر با مجموعه نقاط
۴. تعریف چندضلعی ساده، چندضلعی محدب، مثلث‌بندی چندضلعی و محاسبه تعداد مثلث‌بندی‌های یک چندضلعی محدب و مساله گالری هنر
۵. قضیه اسپرنر و نتایج مهم آن
۶. معرفی گراف‌های هندسی و بررسی خواص آنها
۷. دیاگرام Dirichlet-Voronoi
۸. مثلث‌بندی دلونی (Delaunay)
۹. مساله هادویگر- نلسون(Hadwiger-Nelson Problem) درباره رنگ‌آمیزی نقاط صفحه
۱۰. اعداد رمزی هندسی

مراجع پیشنهادی:

1. Matousek, j., Lectures on Discrete Geometry, Springer-Verlag, 2002.
2. Jacob E. Goodman, Joseph O'Rourke, Handbook of Discrete and Computational Geometry, Chapman & Hall, CRC, 2004.
3. Mark de Berg, Otfried Cheong, Marc van Kreveld, Mark Overmars, Springer Computational Geometry, Algorithms and Applications, Verlag Berlin Heidelberg, 2008.
4. Stefan Felsner, Geometric Graphs and Arrangements, Vieweg and Teubner Verlag, 2004.
5. János Pach, Pankaj K. Agarwal, Combinatorial Geometry, Wiley-Interscience, 1995.

عنوان درس	فارسی	نظریه الگوریتمی گراف						
	انگلیسی	Algorithmic Graph Theory						
نوع واحد						تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
اصلی		انتخابی		جبرانی		۳	۴۸	
نظری	عملی	نظری	عملی	نظری	عملی			
حل تمرین: ندارد		نیاز به اجرای پروژه عملی: ندارد						

هدف: آشنایی با الگوریتم‌های مسایل نظریه گراف.

سرفصل‌های درس:

- **یادآوری پیش‌نیازها:** معرفی مقدمات الگوریتم‌ها و پیچیدگی محاسباتی الگوریتم‌ها.
- **اثبات NP- سخت بودن مسایل معروف مانند:** مسایل پوشش رأسی، مجموعه مستقل رأسی، 3-SAT،3- رنگ‌پذیری ، ماکزیمم خوشه.
- **درخت‌ها و جنگل‌ها:** درخت فراگیر کمینه، پیمایش درخت‌ها، q-درخت‌ها و اهیمت آن‌ها.
- **ساختمان‌داده‌های درختی:** صف مرتب، انواع heap، جستجوی دودویی.
- **فاصله، جریان در شبکه و همبندی:** الگوریتم‌های مربوط به همبندی رأسی و یالی و جریان در شبکه.
- **الگوریتم‌های انواع پیمایش در گرافها:** الگوریتم‌های مربوط به گراف‌های اویلری، هامیلتونی و مساله فروشنده دوره گرد.
- **گراف‌های مسطح:** الگوریتم‌های مربوط به مسطح بودن گراف‌ها.
- **رنگ‌آمیزی گراف‌های:** تحلیل الگوریتمی مسئله رنگ‌آمیزی گراف‌ها، بحث در مورد الگوریتم‌های مختلف، مفهوم انتقال فاز.
- **گراف‌های تصادفی:** الگوریتم‌های مربوط به تولید گراف‌های تصادفی و گراف‌های تصادفی منتظم.
- **الگوریتم‌های پارامتری:** الگوریتم‌های وابسته به پارامتر با مثال منتخب استاد.
- **الگوریتم‌های برخط:** طراحی و تحلیل الگوریتم‌های برخط (online) و الگوریتم‌های sequential با مثال‌های منتخب استاد.

مراجع پیشنهادی:

1- David Joyner, Minh Van Nguyen, Nathann Cohen, Algorithmic Graph Theory, 2010.
2- Kloks, T., Advanced Graph Algorithms, 2012.
3- Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein, Introduction to Algorithms, 2009.