جمهوری اسلامی ایران

وزارت علوم، تحقیقات و فناوری

شورای گسترش و برنامه‌ریزی آموزش عالی

برنامه درسی رشته

جرم یابی دیجیتال

Digital Forensic

مقطع کارشناسی ارشد ناپیوسته

گروه علوم انسانی

پیشنهادی دانشگاه تربیت مدرس

باسمه تعالی

نام رشته: جرم یابی‌دیجیتال | **عنوان گرایش:**

گروه: علوم‌انسانی | **دوره تحصیلی: کارشناسی ارشدناپیوسته**

کارگروه تخصصی:حقوق | **نوع مصوبه:تدوین**

پیشنهادی: دانشگاه تربیت مدرس | **تاریخ تصویب: ۱۴۰۰/۱۱/۰۳**

برنامه درسی تدوین شده دوره کارشناسی ارشد ناپیوسته رشته جرم یابی دیجیتال، در جلسه شماره ۹۵۰ به تاریخ ۱۴۰۰/۱۱/۰۳ شورای گسترش و برنامه‌ریزی آموزش عالی به شرح زیر تصویب شد:

ماده یک- این برنامه درسی برای دانشجویانی که پس از تصویب این برنامه درسی در دانشگاه‌ها و موسسات آموزش عالی پذیرفته می‌شوند، قابل اجرا است.

ماده دو- این برنامه درسی در سه فصل: مشخصات کلی، جدول‌های واحدهای درسی و سرفصل دروس تنظیم شده است و برای اجرا در دانشگاه‌ها و موسسات آموزش عالی پس از اخذ مجوز پذیرش دانشجو از شورای گسترش و برنامه‌ریزی آموزش عالی و سایر ضوابط و مقررات مصوب وزارت علوم، تحقیقات و فناوری، ابلاغ می‌شود.

ماده سه- این برنامه درسی از شروع سال تحصیلی ۱۴۰۲-۱۴۰۳ به مدت ۵ سال قابل اجرا است و پس از آن، در صورت تشخیص کارگروه تخصصی مربوطه، نیاز به بازنگری دارد.

دکتر محمدرضا آهنچیان
دبیر کمیسیون برنامه‌ریزی آموزشی

دکتر علی خاکی‌صدیق
دبیر شورای گسترش و برنامه‌ریزی آموزش عالی

وزارت علوم، تحقیقات و فناوری
شورای عالی برنامه‌ریزی و آموزشی

فهرست مطالب

۱- مقدمه

دانش میان‌رشته‌ای[1] اشاره به حوزه‌های نوینی در علوم دارد که بیش از یک زمینه‌ی محض دانشی را مورد مطالعه قرار می‌دهد. رویکرد میان‌رشته‌ای فرصت عبور از مرزهای سنتی رشته‌های گوناگون دانش را در راه رسیدن به نتیجه‌ی مطلوب در یک رشته فراهم می‌سازد. به عبارت دیگر، حوزه‌ی میان‌رشته‌ای، تلفیق دانش، روش و تجارب دو یا چند حوزه‌ی علمی و تخصصی است که به منظور شناخت و حل یک مسئله‌ی پیچیده و یا معضل اجتماعی چندوجهی صورت می‌گیرد. بنابراین، فعالیت‌های علمی میان‌رشته‌ای زمانی معنا پیدا می‌کنند که شناخت و فهم علمی و دقیق پدیده یا مسئله‌ای پیچیده یا ناشناخته که از ظرفیت و دانش یک رشته و یا تخصص خارج است، هدف باشد.

زمانی‌که حوزه‌ی مساله مرتبط با علوم اجتماعی باشد پیچیدگی این مساله دوچندان می‌شود و نیاز به همکاری تخصص-های میان رشته‌ای اهمیت بیشتری پیدا می‌کند. یکی از این مسائل، جرائم حوزه دیجیتال است که با گسترش شبکه‌های کامپیوتری و شبکه‌های اجتماعی به یک معضل روز تبدیل شده است. در این حوزه ما نیاز به دانشی داریم که پیشگیری، تشخیص و پیگیری این جرائم را تسهیل نموده و همزمان با ارائه ادله مستند و مستدل برخورد با این تخلفات را از جنبه قانونی هموار سازد. چنین دانشی با همکاری متخصصان در دانش‌هایی نظیر مهندسی کامپیوتر، علوم کامپیوتر، فناوری اطلاعات، حقوق جزا و جرم‌شناسی، حقوق خصوصی و حقوق مالیکت فکری تحقق می‌یابد. به عبارت دیگر، این همکاری موجب هم‌افزایی شده و در نتیجه شناخت و حل مساله را ساده‌تر می‌کند

در این راستا، گروه مهندسی کامپیوتر دانشکده مهندسی برق و کامپیوتر در نظر دارد با همکاری گروه‌های مرتبط از دانشکده حقوق (گروه حقوق جزا)، دانشکده ریاضی (گروه علوم کامپیوتر) و دانشکده صنایع برنامه‌ای برای برگزای دروه کارشناسی‌ارشد در حوزه جرم‌یابی دیجیتال برگزار کند. قابل ذکر است که این گروه به لحاظ آموزشی و پژوهشی سابقه‌ی خوبی در حوزه جرائم دیجیتال دارد. اول اینکه در وضعیت فعلی، گروه مهندسی کامپیوتر گرایش رایانش امن (امنیت اطلاعات) را برگزار می‌کند که به لحاظ محتوایی همپوشانی حدود ۳۰ درصدی با جرم‌یابی دیجیتال دارد. ثایناً، تحقیقات ارزشمندی در حوزه جرائم دیجیتال در قالب پایان‌نامه‌های کارشناسی‌ارشد و دکترای این گروه انجام گرفته است. در این گزارش برنامه درسی دوره کارشناسی‌ارشد رشته جرم‌یابی دیجیتال ارائه شده است. در ابتدا ضرورت این امر تبیین می‌شود. در ادامه تاریخچه این رشته مرور می‌شود. در پایان برنامه‌ی درسی پیشنهادی ارائه می‌گردد.

---

[1] Interdisciplinary

۲- ضرورت راه اندازی رشته جرم یابی دیجیتال

جرم یابی دیجیتال به عنوان یک دانش میان رشته‌ای تمرکز بر گردآوری، شناسایی، مستندسازی و تحلیل شواهد و ادله دیجیتال مرتبط با رویدادهای واقع در شبکه‌های کامپیوتری یا ابزارهای الکترونیکی نظیر کامپیوتر، تلفن‌های همراه هوشمند و غیرهوشمند دارد. با توجه به گسترش روز افزون استفاده از این ابزارها در قالب سرویسهایی نظیر خدمات مالی، دولتی و شبکه‌های اجتماعی امکان جعل، سوء استفاده و کلاهبرداری نیز برای نفوذگرها فراهم گردیده است. عدم توجه به این جرائم می‌تواند امنیت فضای سایبری را به خطر انداخته و حس ناامنی را به جامعه القاء کند. از اینرو پیگیری جرائم و فراهم سازی امنیت در فضای دیجیتال نیازمند مکانیزم‌های قوی جرم‌یابی و پیشگیری از آن است که می‌بایست در طیف وسیعی از سازمانها و نهادها نظیر پلیس فتا، قوه قضائیه، کانون وکلا، کارشناسان دادگستری و شورای عالی فضای مجازی عملیاتی گردد.

۳- اهدف راه‌اندازی رشته جرم‌یابی دیجیتال

- ایجاد دوره آموزش عالی در زمینه اصول و مبانی کاربردی جرم یابی دیجیتال به لحاظ مفاهیم فنی فضای دیجیتال همراه با مباحث حقوقی و قابل استناد در محاکم بین المللی یا داخل کشور
- آشنایی فارغ التحصیلان با دانش و مهارتهای لازم جهت هدایت یا همکاری با تیم‌های تحقیقاتی که دررابطه با جرائم روی داده در فضای دیجیتال پژوهش می کنند.
- تربیت نیروی متخصص جهت مشاغل پیشرفته‌ای نظیر توسعه نرم‌افزارهای جرم‌یابی، وارسی و ارزیابی نرم افزارهای موجود، برگزاری آزمون و مدیریت امنیت فضای سایبری
- تربیت نیروی انسانی برای پلیس فتا در معاونت ادله دیجیتال، معاونت مبارزه با جرائم سازمان یافته دیجیتال و معاونت پیشگیری از جرائم
- برگزاری دوره‌های تخصصی ادله دیجیتال برای کارشناسان و وکلای دادگستری
- تربیت نیروی متخصص در زمینه‌های قانونگذاری و یا اصلاح قوانین مربوط به حوزه دیجیتال
- تربیت نیروی متخصص جهت بررسی مزایا و معایب عضویت کشور در کنوانسیون‌های بین المللی دیجیتال و تشخیص تعارض این کنوانسیونها با قوانین داخلی کشور

٤- تاریخچه رشته جرم یابی دیجیتال

مرور این رشته در دانشگاههای مطرح جهان نشام می‌دهد که این رشته از پیشینه‌ای نزدیک به ۱۰ سال برخوردار است. معمولا این رشته در قالب یک دوره کارشناسی ارشد با عنوان جرم یابی دیجیتال[۲] ارائه شده است. در سایر موارد نیز این رشته به عنوان یک گرایش[۳] از دوره‌ای با عنوان کلی‌تری نظیر امنیت اطلاعات یا امنیت فضای سایبری[۴] ارائه شده است. در جدول ۱ فهرستی از دانشگاههای مطرح انگلستان و آمریکا که در زمینه جرم‌یابی دیجیتال فعالیت دارند، آورده شده است. نکته قابل توجه این است که در دو مورد، دانشگاه مریلند و دانشگاه فلوریدای مرکزی، این رشته به عنوان یک رشته‌ی میان‌رشته‌ای با همکاری چندین دانشکده یا موسسه برگزار شده است. در موارد دیگر نیز با اینکه این رشته در یک دانشکده خاص برگزار می‌شود، ولی ارتباط تنگاتنگی با موسسات حقوقی و امنیتی دارند.

جدول ۱ : فهرست دانشگاههای مطرح خارجی که در زمینه جرم یابی دیجتال فعالیت دارند

No.	University	Country	Department/School	Program Title	Tracks
1	Cranfield	UK	Computer Science	MSc in Digital Forensics	
2	WestMinster	UK	Faculty of Science and Technology, School of Computer Science & Software Engineering	MSc in Cyber Security and Forensics	1.Digital Forensics 2.Cyber Security
3	Edunburg Napier University	UK	School of Computing	MSc in Advanced Security & Digital Forensics	
4	South Wales	UK	Information Security Research Group	MSc in Computer Forensics MSc in Computer System Security MSc in Cyber Security	
5	Royal Holloway, University of London	UK	Information Security Group	MSc in Information Security	1.Cyber Security 2.Security Testing 3.Digital Forensics 4.Secure Digital Business
6	Central Florida	US	Collaborative between: 1.Computer Science 2.Forensic Science of Chemistry 3.Criminal Justice and Legal Studies 4.The National Center for Forensic Science	MSc in Digital Forensics	

[2] Digital Forensic
[3] Track/Pathway/Concentration
[4] Cyber Security

7	John Hopkins	US	Whiting School of Engineering	MSc in Cybersecurity	1.Analysis (Forensic related) 2.Network 3.System
8	Maryland	US	Collaboration of: 1.ECE Department 2.Computer Science 3. Maryland Cybersecurity Center	Master of Engineering in Cybersecurity	
9	Texas-San Antonio	US	College of Business, Department of Information Systems and Cyber Security	MSc in Information Technology	Cyber Security Concentration
10	Norwich	US	The College of Graduate and Continuing Studies	MSc in Information Security & Assurance	1. Computer Forensic Investigation /Incident Response Team Management 2.Critical Infrastructure Protection & Cyber Crime 3.Cyber Law & International Perspectives on Cyberspace
11	Carnegie Mellon	US	College of Engineering	MSc in Information Security	Cyber Forensics and Incident Response (CyFIR) Track

۵- برنامه رشته جرم‌یابی دیجیتال

طول دوره و شکل نظام واحدی

در این مرحله رشته جرم‌یابی دیجیتال با یک گرایش جرم‌یابی دیجیتال تعریف می‌شود. نظام کارشناسی‌ارشد شامل دو بخش آموزشی و پژوهشی (سمینار و پایان‌نامه کارشناسی‌ارشد) می‌باشد. طول این دوره چهار نیمسال تحصیلی خواهد بود.

شرایط پذیرش دانشجو

دانشجویان این رشته از طریق آزمون ورودی و از بین دانش‌آموختگان کارشناسی مهندسی کامپیوتر یا رشته‌های مرتبط با آن مطابق با ضوابط وزارت علوم، تحقیقات و فناوری انتخاب می‌شوند.

آزمون ورودی

دانشجویان این رشته از طریق آزمون ورودی متمرکز و مطابق با ضوابط وزارت علوم، تحقیقات و فناوری انتخاب برگزیده می‌شوند. مواد درسی که معیار انتخاب و تعیین اولویت برای این دانشجویان خواهد بود، به شرح زیر است:

مواد درسی آزمون ورودی				
ردیف	عنوان	تعداد واحد	نوع درس	ضریب
۱	سیستم‌عامل	۳	نظری-مهندسی	۳
۲	سیستم وساختار فایلها	۳	نظری-مهندسی	۳
۳	شبکه‌های کامپیوتری	۳	نظری-مهندسی	۳
۴	پیشگیری از جرم	۱	نظری-حقوق	۲
۵	آیین دادرسی کیفری (۱)	۲	نظری-حقوق	۲

تعداد واحدهای درسی و پژوهشی

تعداد دروس آموزشی و پژوهشی این دوره **۳۲** واحد است. بخش آموزشی این دوره در گروه‌های درسی ۱، ۲ و ۳ سازماندهی شده است. هر دانشجو می‌بایست معادل **۲۴** واحد از این گروه‌های درسی را اخذ نماید. در بخش پژوهشی نیز دانشجو موظف به گذراندن **۲** واحد سمینار و **۶** واحد پایان‌نامه خواهد بود.

دروس جبرانی

در صورتی که دانشجو از گرایشهایی غیر مرتب پذیرش شده باشد، با تشخیص گروه موظف به اخذ تعدادی از دروس جبرانی زیر خواهد بود :

جدول دروس جبرانی						
ردیف	**عنوان**	**تعداد واحد**	**نوع واحد**	**ساعات تدریس**	**پیش‌نیاز**	**هم‌نیاز**
۱	سیستم‌عامل	۳	نظری-مهندسی	۴۸		
۲	سیستم وساختار فایلها (ذخیره و بازیابی اطلاعات)	۳	نظری-مهندسی	۴۸		
۳	شبکه‌های کامپیوتری	۳	نظری-مهندسی	۴۸		
۴	کلیات حقوق جزا	۱	نظری-حقوق	۱۶		
۵	پیشگیری از جرم	۱	نظری-حقوق	۱۶		
۶	آیین دادرسی کیفری (۱)	۲	نظری-حقوق	۳۲		
۷	ادله اثبات دعوی	۲	نظری-حقوق	۳۲		
۸	حقوق جزای عمومی (۱)	۲	نظری-حقوق	۳۲		
۹	حقوق جزای اختصاصی (۱): جرایم علیه اموال و مالکیت	۲	نظری-حقوق	۳۲		
۱۰	حقوق جزای اختصاصی (۴) جرایم علیه شخصیت معنوی اشخاص	۲	نظری-حقوق	۳۲		
حداکثر ۶ واحد درسی به تشخیص گروه عنوان دروس جبرانی ارائه شده و دانشجویان بر اساس تشخیص ملزم به گذراندن آن خواهند بود.						

گروه ۱ : دروس الزامی حوزه‌ی جرم‌یابی دیجیتال

جدول دروس گروه۱ : دروس الزامی حوزه‌ی جرم‌یابی دیجیتال						
ردیف	**عنوان**	**تعداد واحد**	**نوع واحد**	**ساعات تدریس**	**پیش‌نیاز**	**هم‌نیاز**
۱	اصول جرم یابی دیجیتال	۳	نظری-عملی	۴۸		
۲	جرم‌یابی دیجیتال پیشرفته	۳	نظری-عملی	۴۸	اصول جرم یابی دیجیتال	
۳	گردآوری و ردیابی شواهد	۳	نظری-عملی	۴۸		اصول جرم یابی دیجیتال
۵	جرائم سایبری	۳	نظری	۴۸		
اخذ حداقل سه درس از چهار درس گروه ۱ برای دانشجویان الزامی است.						

گروه ۲ : دروس الزامی حوزه حقوق

جدول دروس گروه۲ : دروس الزامی حوزه حقوق						
ردیف	**عنوان**	**تعداد واحد**	**نوع واحد**	**ساعات تدریس**	**پیش‌نیاز**	**هم‌نیاز**
۱	آیین دادرسی جرائم دیجیتال	۳	نظری	۴۸		گردآوری و ردیابی شواهد
۲	حقوق اینترنت و فضای سایبری	۳	نظری	۴۸	اصول جرم یابی دیجیتال	
اخذ هر دو درس گروه ۲ (معادل ۶ واحد) برای دانشجویان الزامی است.						

گروه ۳ : دروس اختیاری

جدول دروس گروه۳: دروس اختیاری جرم‌یابی دیجیتال					
ردیف	عنوان	تعداد واحد	نوع واحد	ساعات تدریس	پیش‌نیاز
۱	طراحی سیستم های امنیتی تحمل پذیر اشکال	۳	نظری-مهندسی	۴۸	
۲	طراحی و ارزیابی سیستم‌های بی‌درنگ نهفته	۳	نظری-مهندسی	۴۸	
۳	معماری سامانه‌های ذخیره سازی داده	۳	نظری-مهندسی	۴۸	
۴	سیستم عامل پیشرفته	۳	نظری-مهندسی	۴۸	
۵	رمزنگاری کاربردی	۳	نظری-مهندسی	۴۸	
۶	امنیت شبکه پیشرفته	۳	نظری-مهندسی	۴۸	
۷	توسعه امن نرم‌افزار	۳	نظری-مهندسی	۴۸	امنیت شبکه پیشرفته
۸	پروتکل های امنیتی	۳	نظری-مهندسی	۴۸	امنیت شبکه پیشرفته
۹	روشهای صوری در امنیت اطلاعات	۳	نظری-مهندسی	۴۸	
۱۰	امنیت و اعتماد سخت‌افزار-رانه	۳	نظری-مهندسی	۴۸	
۱۱	امنیت سیستم‌های نوین ارتباطی	۳	نظری-مهندسی	۴۸	امنیت شبکه پیشرفته
۱۲	یادگیری ماشین	۳	نظری-مهندسی	۴۸	
۱۳	سیستم های توزیع شده	۳	نظری-مهندسی	۴۸	
۱۴	الگوریتم های هوش جمعی	۳	نظری-مهندسی	۴۸	
۱۵	الگوریتم های تقریبی	۳	نظری-مهندسی	۴۸	
۱۶	توصیف و وارسی برنامه‌ها	۳	نظری-مهندسی	۴۸	
۱۷	پنهان‌سازی اطلاعات	۳	نظری-مهندسی	۴۸	
۱۸	شبکه‌های دینامیکی پیچیده	۳	نظری-مهندسی	۴۸	
۱۹	وارسی و راستی آزمایی پروتکل‌های امنیتی	۳	نظری-مهندسی	۴۸	
۲۰	مباحث ویژه	۳	نظری-مهندسی	۴۸	
۲۱	حقوق رایانه و ارتباطات جدید	۲	نظری-حقوق	۳۲	
۲۲	حقوق اینترنت و تجارت الکترونیک	۲	نظری-حقوق	۳۲	
۲۳	حقوق انتقال تکنولوژی و دانش فنی	۲	نظری-حقوق	۳۲	
۲۴	جرم شناسی	۲	نظری-حقوق	۳۲	
۲۵	متون حقوقی	۲	نظری-حقوق	۳۲	
۲۶	حقوق کیفری اقتصادی و جرائم سازمان یافته بین المللی اقتصادی	۱	نظری-حقوق	۱۶	

اخذ حداقل ۹ واحد درس از گروه ۳ برای دانشجویان الزامی است.

٦- سر فصل دروس

سرفصل دروس جبرانی

سیستم عامل

نام درس به فارسی	سیستم‌های عامل		
نام درس به انگلیسی	**Operating Systems**		
نوع درس	جبرانی	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم‌یابی	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	هدف از این درس، آشنا نمودن دانشجویان کارشناسی با اصول سیستمهای عامل است .در این درس ضمن معرفی بخشهای مختلف یک سیستم‌عامل و معماریهای متداول آن، معماری چندین سیستم‌عامل نیز بیان میگردد ..در این درس تلاش می‌شود تا نمونه‌های مختلفی از سیستم های عامل از شرکت MacOS ، سیستم‌عامل SUN شرکت Solaris ، سیستم‌عامل IBM شرکت Z/OS شرکتهای مختلف مطرح شود .در این میان سیستمهای عامل مطرح شود .این درس دارای چند پروژه برنامه نویسی است که در آنها مفراهیم اولیه Symbian و سیستم‌عامل Unix ، بعضی نسخه‌های Apple،Linux سیستم های عامل آموزش داده می شود		
نتایج درس			
فهرست مباحث	**بخش نخست: مقدمه ای برمعماری سیستم های عامل** • سیستم‌های عامل،ساختار واجزای تشکیل دهنده آن • معرفی ماشین‌های مجازی از قبیل J AVA , V M wa r e, I B M Z V M **بخش دوم : مدیریت فرایندها** • فرایندها،برنامه‌ریزی وشیوه ارتباط بین آنها • نخ‌ها،مدلهای پیاده سازی نخ‌هاومعرفی کتابخانه‌های مربوط به نخ جاوا و برنامه‌ریزی پردازنده • پیاده سازی بخش مدیریت فرایند ومدیریت منابع یک سیستم عامل کوچک • همگام سازی فرایندها، معرفی نواحی بحرانی، معرفی روشهای سخت افزاری ونرم افزای همگام سازی شامل سمافور،مانیتور و عبارت‌های مسیر • بن بست		

	بخش سوم : مدیریت حافظه • مدیریت حافظه،شامل :فرازحافظه،صفحه‌بندی،قطعه‌بندی،ترکیب صفحه بندی وقطعه-بندی،معرفی بخش مدیریت حافظه چند پردازنده از قبیل پنتیوم، UltraSparc و IBM Z System • معرفی بخش Thrashing،مدیریت حافظه مجازی،شامل :درخواست صفحه،جایگزینی صفحه،تخصیص حافظه سیستم عامل • مدیریت حافظه چندسیستم‌عامل • بخش چهارم : مبانی محافظت وامنیت • مبانی محافظت وامنیت سیستم های عامل **بخش پنجم : مبانی سیستم عامل های بیدرنگ** • مبانی سیستم عامل های بیدرنگ،مدیریت پردازنده پردازنده ومعرفی چندسیستم عامل بیدرنگ نمونه **بخش ششم : مدیریت حافظه جانبی** • واسطه سیستم فایل • پیاده سازی سیستم فایل • حافظه های جانبی و برنامه ریزی دیسک • زیرسیستم ورودی وخروجی سیستم عامل
نرم افزارهای مورد نیاز	سیستم‌عاملهای ویندوز، لینوکس و MAC-OS
تکالیف پیشنهادی	۵ تمرین که در طول نیمسال داده می‌شود.
پروژه های پیشنهادی	
کتاب (های) مرجع	[1] P. Silberschatz, B. Galvin, G. Gagne, *Operating System Concepts*, 8th Edition, John Wiley, 2010. [2] R. Elmasri, A. G. Carrick, D. Levine, *Operating Systems: A Spiral Approach*, Mcgraw-Hill, 2009.
سایر مراجع	[1]

سیستم وساختار فایل‌ها

نام درس به فارسی	سیستم و ساختار فایل‌ها		
نام درس به انگلیسی	**File System Design**		
نوع درس	جبرانی	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم‌یابی	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	هدف از این درس، آشنا نمودن دانشجویان کارشناسی با اصولطراحی و پیاده‌سازی سیستم‌های ذخیره-ساز است. سیستم‌اهای ذخیره‌ساز یکی از فیلدهای مهم با رشد سریع در علوم کامپیوتر است. سیستم ذخیره سازی در هسته اکثر سیستم های کامپیوتری قرار دارد و عملکرد آن معمولا بر کارآیی کل سیستم تاثیرگذار است. همچنین مسئول نگهداری از ارزشمندترین دارایی های یک سازمان یعنی اطلاعات است.		
نتایج درس			
فهرست مباحث	• Uniprocessor file systems • File systems performance analysis • Distributed file systems (including peer-to-peer storage) • Archival storage and backup • Security and reliability (fault tolerance) in file systems and storage • Indexing and naming in file systems • File systems for next-generation storage technologies o flash, NVRAM • Large-scale storage systems • Special-purpose file systems		
نرم افزارهای مورد نیاز	سیستم‌عاملهای ویندوز، لینوکس و MAC-OS		
تکالیف پیشنهادی			
پروژه های پیشنهادی			
کتاب (های) مرجع	[1] Giampaolo, D., & Giampaolo, D. (1998). *Practical File System Design*. Morgan Kaufmann Publishers.		
سایر مراجع			

شبکه‌های کامپیوتری

نام درس به فارسی	شبکه‌های کامپیوتری		
نام درس به انگلیسی	**Computer Networks**		
نوع درس	جبرانی	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم‌یابی	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز	آشنایی با معماری کامپیوتر و مفاهیم سیستم عامل، آشنایی با مفاهیم آمار و احتمال مهندسی، آشنایی با یک زبان برنامه نویسی		
اهداف درس	این درسی به بررسی اصول، طراحی، پیاده‌سازی و کارآیی شبکه‌های کامپیوتری می-ردازد. دانشجویان در این درس با معماری وسرویس‌های شبکه‌های کامپیوتری و مدل لایه‌ای آشنا می‌شوند. این درس با تاکید بر شبکه‌های اینترنت و مدل TCP/IP به بررسی پروتکل‌های لایه کاربرد، لایه حمل، لایه شبکه ولایه پیوند داده می‌پردازد.		
نتایج درس			
فهرست مباحث	۱. مروری بر سرویس‌های شبکه‌های کامپیوتری ۲. شبکه اینترنت و اجزای تشکیل دهنده‌ی آن ۳. معماری لایه‌ای شبکه‌های کامپیوتری ۴. لایه کاربرد ۵. لایه حمل ۶. لایه شبکه ۷. لایه پیوند داده		
نرم افزارهای مورد نیاز	محیط یکی از زبانهای متداول برنامه نویسی و کتابخانه‌های مربوطه		
تکالیف پیشنهادی	۵ تمرین که در طول نیمسال داده می‌شود.		
پروژه های پیشنهادی	۶ تکلیف و یک تمرین برنامه نویسی سوکت		
کتاب (های) مرجع	[1] Kurose, James F., and Keith W. Ross. "Computer networking: a top-down approach." *Addison Wesley Computing* (2013). [2] Tanenbaum, Andrew S., and David Wetherall. *Computer networks*. Boston: Pearson Prentice Hall,, 2011.		
سایر مراجع			

کلیات حقوق جزا

نام درس به فارسی	کلیات حقوق جزا		
نام درس به انگلیسی	Principles of Criminal Law		
نوع درس	جبرانی	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۱ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها	ندارد		
مطالب پیش نیاز			
اهداف درس	آشنایی دانشجویان با عمومات مسائل حقوق کیفری و ساختار و تقسیمات عمده کیفری ایران		
نتایج درس			
فهرست مباحث	۱.محتوا و موضوع حقوق جزایی -آشنایی با مفاهیم جزایی، جرم، مجازات، اقدامات تأمینی و تربیتی، بزهکاری، بزه دیدهگی، مسئولیت جزایی -قواعد ناظر به اختیارات و وظایف دولت در مبارزه با بزهکاری و تحولات آن(جرم انگاری، کیفرگذاری، تعقیب و مجازات بزهکاران) ۲.منابع حقوق جزا در حقوق ایران- -منابع الزامی(قانون اساسی، قانون عادی، مصوبات مجمع تشخیص مصلحت نظام و آراء وحدت رویه (رویه قضایی به معنای خاص) -منابع معتبر اسلامی و فتاوای فقهی -منابع ارشادی(رویه قضایی به معنای عام، نظریات علمی حقوق و فقه، عرف و عادت) ۳. جایگاه حقوق جزایی و ارتباط آن با رشته های حقوقی دیگر و سایر علوم -جایگاه و اهمیت -ارتباط آن با شاخه های دیگر حقوقی و سایر علوم ۴.پدیده مجرمانه و واکنش اجتماعی علیه آن- -پدیده مجرمانه -واکنش اجتماعی -انواع واکنش اجتماعی(مجازات :سالب حیات، سالب آزادی، محدود کننده آزادی، سالب حقوق، مالی، جایگزین های حبس و اقدامات تأمینی) - -تحولات ناظر به واکنش ها(مکتب کلاسیک، مکتب تحققی، مکتب دفاع اجتماعی)		

کتاب (های) مرجع	منابع فارسی [۱]بکاریا، سزار ، رساله جرایم و مجازات ها، ترجمه دکتر محمد علی اردبیلی، تهران، نشر میزان، آخرین سال انتشار. [۲]جعفری، مجتبی، مقدمه علم حقوق کیفری، تهران، نشر میزان، آخرین سال انتشار. [۳]حیدر علامه، غلام، اصول راهبردی حقوق کیفری، نشر میزان، آخرین سال انتشار. [۴]فلچر، جورج پی، مفاهیم بنیادین حقوق کیفری، ترجمه سید مهدی سیدزاده ثانی، گروه پژوهشی ترجمه دانشگاه علوم [۵]اسلامی رضوی، مشهد، دانشگاه علوم اسلامی رضوی، آخرین سال انتشار. [۶]گلدوزیان، ایرج، محشای قانون مجازات اسلامی، تهران، انتشارات مجد، آخرین سال انتشار. [۷]نوربها، رضا، نگاهی به قانون مجازات اسلامی، تهران، نشر میزان، آخرین سال انتشار- . [۸]هرینگ، جاناتان، مبانی حقوق کیفری انگلستان، ترجمه امیر اعتمادی، انتشارات جنگل، آخرین سال انتشار- . [۹]مقالات علمی معتبر مرتبط با سرفصل درس در مجلات حقوقی داخلی و خارجی
سایر مراجع	منابع انگلیسی [1] A.Ashworth, Principles of Criminal Law, Oxford University Press, 1thed, 3332. [2]J.Dressler, Understanding Criminal Law, LexisNexis, 6thed, 3313. [3]P.Carlan, L.Nored and R.Downey, An Introduction to Criminal Law, Jones and Bartlett Publishers, 3311. [4]N.Lacey, C.Wells and O.Quick, Reconstructing Criminal Law: Text and Materials, Cambridge University Press, 2rded, 3336. [5]J.Hall, General Principles of Criminal Law, The Lawbook Exchange, 3nded, 3339. [6]G.P.Fletcher, Basic Concepts of Criminal Law, Oxford University Press, 1553. منابع فرانسه [7]Patrick Kolb, Laurence Leturmy, L'essentiel du droit pénal général, Gualino- 2115. [8]PRADEL, Jean. Droit penal general. Cujas, 2118.

پیشگیری از جرم

نام درس به فارسی	پیشگیری از جرم		
نام درس به انگلیسی	Crime Prevention		
نوع درس	جبرانی	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۱ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها	کلیات حقوق جزا		
اهداف درس	آشنایی با مفهوم پیشگیری به عنوان یکی از مفاهیم حوزه جرم شناسی و تبیین اصول حاکم بر پیشگیری و بیان اهداف و توجیهات آن، بررسی مبانی نظری پیشگیری از جرم و تشریح و توضیح انواع(گونه‌های)پیشگیری و در پایان توجه و تمرکز بر جایگاه پیشگیری در سیاست جنایی ایران، برخی کشورها و نیز در سطح بین المللی از جمله سازمان ملل متحد.		
فهرست مباحث	۱.مفهوم پیشگیری، اصول و مبانی آن • .مفهوم جرم شناختی و پیشگیری کیفری •اصول حاکم بر پیشگیری(حضور همه جانبه ی دولت، مشارکتی بودن، قابلیت محاسبه و پایداری، حقوق بشر مدار بودن) •مبانی نظری پیشگیری ۲.گونه‌های پیشگیری و جایگاه آن در سیاست گذاری جنایی •گونه‌ها (فردمدار، موقعیت مدار) • سیاست گذاری جنایی (در سیاست جنایی ایران، در رویکرد تطبیقی)		
کتاب (های) مرجع	[۱]دفتر تحقیقات کاربردی پلیس پیشگیری، فصلنامه مطالعات پیشگیری از جرم، تاکنون ۳۳ شماره. [۲]دفتر تحقیقات کاربردی پلیس و پیشگیری، مجموعه مجلدات) ۱مجلد(مقالات پیشگیری از جرم، آخرین سال انتشار [۳]شهرام ابراهیمی(مترجم)، مجموعه رویه های بین المللی پیشگیری از جرم، تهران، نشر میزان، آخرین سال انتشار. [۴]شهرام ابراهیمی، جرم شناسی پیشگیری، تهران، نشر میزان، آخرین سال انتشار. [۵]غلامرضا، محمدنسل، کلیات پیشگیری از جرم، تهران، نشر میزان، آخرین سال انتشار. [۶]غلامرضا، محمدنسل، مبانی پیشگیری از جرم، تهران، نشر میزان، آخرین سال انتشار. [۷]کسن، ریموند، جرم شناسی پیشگیری، ترجمه دکتر مهدی کی نیا، تهران، انتشارات مجد، آخرین سال انتشار [۸]معاونت اجتماعی و پیشگیری از وقوع جرم قوه قضاییه، رهیافتهای نوین پیشگیری از جرم، تهران، نشر میزان، آخرین [۹]سال انتشار. [۱۰]نجفی ابرند آبادی، علی حسین)زیر نظر(، دانشنامه بزه دیده شناسی و پیشگیری از جرم، دو جلد، تهران، نشر میزان، [۱۱] آخرین سال انتشار. [۱۲] مقالات علمی معتبر مرتبط با سرفصل درس در مجلات حقوقی داخلی و خارجی		

آیین دادرسی کیفری (۱)

نام درس به فارسی	آیین دادرسی کیفری (۱)		
نام درس به انگلیسی	Code of Criminal Procedure		
نوع درس	جبرانی	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۲ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	توجیه درس :نظر به اینکه مراجع تعقیب نقش مهمی در اجرای حقوق جزا دارند، آشنایی دانشجویان با تشکیلات و اختیارات و فرایند رسیدگی در این مراجع ضروری است. هدف :آشنایی دانشجویان با سازوکارهای اجرای عدالت کیفری، مبانی و لوازم آن شامل بررسی کلیات؛ مرحله کشف، تعقیب و تحقیقات مقدماتی.		
نتایج درس			
فهرست مباحث	کلیات :تاریخچه، موضوع آیین دادرسی کیفری و معرفی مهم ترین نظام های دادرسی کیفری ۱.تعقیب کیفری a.نهاد دادسرا؛ تشکیلات و اختیارات ●ویژگی های دادسرا به عنوان مرجع تعقیب ●تشکیلات دادسرا در نظام قضایی کنونی ●اختیارات دادسرا در امر تعقیب کیفری b.به جریان انداختن تعقیب ●جهات شروع به تعقیب ●شرایط و موانع تعقیب ●موارد سقوط تعقیب ●حقوق متهم و شاکی در مرحله تعقیب ۲.تحقیقات مقدماتی a.مقام تحقیق؛ صلاحیت و جهات شروع به تحقیق ●ویژگی های تحقیقات مقدماتی و جهات شروع به آن ●صلاحیت مقام تحقیق ●جهات شروع به تحقیق ●حقوق متهم و شاکی در مرحله تحقیقات مقدماتی b.اقدام به تحقیق و قرارهای این مرحله ●اقدام به تحقیق در جرایم عادی، رایانهای و اشخاص حقوقی ●قرارها(اعدادی و نهایی) ●کیفرخواست و مندرجات آن		

کتاب (های) مرجع	[۱] استفانی. گاستون. آیین دادرسی کیفری فرانسه. جلد دوم. ترجمه حسن دادبان. تهران، انتشارات دانشگاه علامه طباطبایی، آخرین سال انتشار [۲] آخوندی. محمود, آیین دادرسی کیفری. جلد اول. تهران، انتشارات وزارت فرهنگ و ارشاد اسلامی. آخرین سال انتشار [۳] آخوندی. محمود. آیین دادرسی کیفری. جلد دوم . تهران، انتشارات وزارت فرهنگ و ارشاد اسلامی. آخرین سال انتشار [۴] آشوری. محمد. آیین دادرسی کیفری. جلد اول. تهران، انتشارات سمت. آخرین سال انتشار [۵] آشوری، محمد، آیین دادرسی کیفری. جلد دوم . تهران، انتشارات سمت. آخرین سال انتشار [۶] آشوری، محمد، جایگزین های زندان یا مجازات های بینابین. تهران، نشر گرایش. آخرین سال انتشار [۷] تدین. عباس. ترجمه قانون آیین دادرسی کیفری فرانسه . تهران، انتشارات روزنامه رسمی جمهوری اسلامی ایران، آخرین سال انتشار [۸] جلالی فراهانی. در آمدی بر آیین دادرسی کیفری جرایم سایبری. تهران، انتشارات خرسندی. آخرین سال انتشار [۹] خالقی. علی،آیین دادرسی کیفری. تهران، انتشارات شهر دانش، آخرین سال انتشار [۱۰] خالقی، علی، نکته ها در قانون آیین دادرسی کیفری، تهران، انتشارات شهردانش، آخرین سال انتشار [۱۱] خزانی. منوچهر. فرآیند کیفری)مجموعه مقالات.(تهران، انتشارات گنج دانش، آخرین سال انتشار [۱۲] زراعت، عباس ، آیین دادرسی کیفری)جلد اول(، تهران ، نشر میزان، آخرین سال انتشار [۱۳] سلیمی، صادق و بخشی زاده اهری، امین، تحلیل ماده به ماده قانون آیین دادرسی کیفری ۹۲۱۳ در مقایسه با قوانین سابق، تهران، انتشارات جنگل، آخرین سال انتشار [۱۴] گلدوست جویباری، رجب، آیین دادرسی کیفری، تهران، انتشارات جنگل، آخرین سال انتشار [۱۵] گلدوست جویباری، رجب، کلیات آیین دادرسی کیفری، تهران، انتشارات جنگل ، آخرین سال انتشار [۱۶] لارگیه. ژان. آیین دادرسی کیفری فرانسه. ترجمه حسن کاشفی اسماعیل زاده. تهران، نشر کتابخانه گنج دانش، آخرین سال انتشار [۱۷] معاونت آموزش قوه قضاییه. دفتر آموزش روحانیون و تدوین متون فقهی. مجموعه نظریات فقهی در امور کیفری . جلد ششم، تهران، .نشر قضا، آخرین سال انتشار [۱۸] مسائل آیین دادرسی کیفری ۹, مجموعه نشست های قضایی. تهران، انتشارات جاودانه: آخرین سال انتشار [۱۹] مسائل آیین دادرسی کیفری ۳, مجموعه نشست های قضایی. تهران، انتشارات جاودانه: آخرین سال انتشار

	[۲۰] نیازپور، امیرحسن، توافقی شدن آیین دادرسی کیفری، تهران، نشر میزان، آخرین سال انتشار [۲۱] مقالات علمی معتبر مرتبط با سرفصل درس در مجلات حقوقی داخلی و خارجی.
سایر مراجع	منابع انگلیسی: 1.Y.Kamisar and Others, Basic Criminal Procedure: Cases, Comments and Questions, West Academic Publishing, ۱۱thed, ۲۰۱۵. 2.J.Dressler and G.Thomas, Criminal Procedure: Investigating Crime, West Academic Publishing, ۹thed, ۲۰۱۲. 3.R.V.Del Carmen, Criminal Procedure: Law and Practice, Cengage Learning, ۵thed, ۲۰۱۳. 4.M.Lippman, Criminal Procedure, SAGE Publications, ۲۰۱۰. 5.S.G.Coughlan, Criminal Procedure, Irwin Law, 2008. 6.J.Ingram, Criminal Procedure: Theory and Practice, Prentice Hall, 2005. منابع فرانسه: 1. Evelyne Bonis-Garçon, Virginie Peltier, Droit de la peine, LexisNexis,2115. 2. Emmanuel Dreyer, Droit pénal général, LexisNexis,2114. 3. Etienne Vergès, Procédure pénale, LexisNexis, 2114. 4. Cesare Beccaria,Des délits et des peines, Payot et Rivages, 2114. 5. Jean Larguier, Philippe Conte,Procédure pénale, Dalloz, 2114 6. Thierry Garé, Catherine Ginestet, Droit pénal - Procédure pénale, Dalloz, 2114.

حقوق جزای عمومی (۱)

نام درس به فارسی	حقوق جزای عمومی (۱)		
نام درس به انگلیسی	Criminal Law		
نوع درس	جبرانی	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۲ واحد
مقطع	تحصیلات تکمیلی		
اهداف درس	توجیه درس :از آنجا که جرم موضوع اصلی کلیه دروس حقوق جزایی است، ضروری است پس از آشنایی با قواعد واصول کلی در این درس، دانشجویان با مفهوم جرم و ارکان و طبقه بندی آن آشنا شوند. هدف :آشنایی دانشجویان با تعریف جرم و ارکان آن و طبقه بندی جرایم.		
نتایج درس			
فهرست مباحث	۱. جرم و اصل قانونی بودن آن a. تعریف جرم(جرم در حقوق جزا، جرم در جرمشناسی) b. اصل قانونی بودن i. کاربرد اصل قانونی بودن ii. آثار اصل قانونی بودن(تفسیر مضیق قانون کیفری، عطف به ماسبق نشدن قانون کیفری) c. علل موجهه جرم(اضطرار، حکم قانون و امر آمر قانونی، رضایت بزه دیده، دفاع مشروع) ۲. ارکان تشکیل دهنده جرم a. رکن مادی i. اجزای رکن مادی(رفتار مرتکب، شرایط و اوضاع و احوال لازم، نتیجه، رابطه علیت و سببیت) ii. شروع به جرم(شروع به جرم در مفهوم خاص، جرم محال و اقسام آن، جرم عقیم و مقایسه آن با جرم محال) b. رکن معنوی یا روانی i. مفاهیم، پیشینه و لزوم احراز رکن روانی ii. اشکال عنصر روانی(عمد(اجزاء و شرایط)، خطا(مفهوم و اقسام خطا)) ۳. طبقه بندی جرایم a. طبقه بندی تقنینی جرایم i. جرایم سیاسی و جرایم عمومی)ضابطه تشخیص و فواید حاصل از تشخیص آن) ii. جرایم نظامی و جرایم عمومی)ضابطه تشخیص جرم نظامی فواید حاصل از تشخیص آن) b. طبقه بندی جرایم بر حسب رکن مادی i. ه اعتبار رفتار فیزیکی(مادی و غیر مادی، آنی و مستمر، ساده و مرکب)		

	ii. به اعتبار شرایط و اوضاع و احوال (از لحاظ شیوه ارتکاب، از لحاظ ویژگی های مرتکب و قربانی، ساده و بهعادت) به اعتبار نتیجه(مطلق، مقید) c. طبقه بندی جرایم بر حسب رکن روانی i. جرایم عمدی و غیر عمدی ii. جرایم ساده و مرتبط iii. جرایم مادی صِرف
کتاب‌های مرجع	[۱] اردبیلی، محمد علی، حقوق جزای عمومی، ج ۱، تهران، نشر میزان، آخرین سال انتشار [۲] ساکی، محمدرضا، حقوق جزای عمومی، جلد اول(جرم و پدیده جنایی)، تهران، انتشارات جنگل، آخرین سال انتشار. [۳] -سلیمی، صادق، چکیده حقوق جزای عمومی، تهران، انتشارات جنگل، آخرین سال انتشار. [۴] شمس ناتری، محمد ابراهیم و همکاران، قانون مجازات اسلامی در نظم حقوقی کنونی، جلد اول(حقوق جزای [۵] عمومی)، تهران، نشر میزان، آخرین سال انتشار [۶] عوده، عبدالقادر، حقوق جنایی اسلام، مشهد، بنیاد پژوهش های اسلامی، آخرین سال انتشار [۷] گلدوزیان، ایرج، بایسته های حقوق جزای عمومی، تهران، نشر میزان، آخرین سال انتشار. [۸] مصدق، محمد، شرح قانون مجازات اسلامی مصوب ۱۳۹۲ ، تهران، انتشارات جنگل، آخرین سال انتشار [۹] نجفی توانا، علی و ملکی، ایوب،حقوق جزای عمومی، ج ۱، تهران، انتشارات جنگل، آخرین سال انتشار. [۱۰] نوربها، رضا، زمینه حقوق جزای عمومی، تهران، انتشارات گنج دانش، آخرین سال انتشار. [۱۱] مقالات علمی معتبر مرتبط با سرفصل درس در مجلات حقوقی داخلی و خارجی. [۱۲] قانون مجازات اسلامی، جدید مصوب ۱۳۹۲

حقوق جزای اختصاصی (۱) :جرایم علیه اموال و مالکیت

نام درس به فارسی	حقوق جزای اختصاصی (۱) :جرایم علیه اموال و مالکیت		
نام درس به انگلیسی	Criminal Law (Crimes against Property)		
نوع درس	جبرانی	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۲ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	توجیه درس :نظر به اینکه جرایم علیه اموال و مالکیت بخش بزرگی از جرایم ارتکابی در بسیاری از کشورهای جهان از جمله ایران را تشکیل میدهند، آشنایی دانشجویان با این جرایم ضروری است. هدف : آشنا کردن دانشجویان با ماهیت، اهمیت و ارکان تشکیل دهنده جرایم علیه اموال و مالکیت در قوانین ایران و مقایسه مختصر با یکی از نظامهای حقوقی معتبر.		
نتایج درس			
فهرست مباحث	کلیات : تعریف، ویژگیها، اهمیت و انواع جرایم علیه اموال و مالکیت ۱. کلاهبرداری a. مقدمه :تعریف، تاریخچه، ویژگیها b. ارکان i. رکن مادی(رفتار فیزیکی، شرایط و اوضاع و احوال لازم برای تحقق جرم و نتیجه حاصله)شروع به جرم کلاهبرداری. ii. رکن روانی c. واکنش در برابر جرم کلاهبرداری(کیفرهای اصلی، تبعی و تکمیلی) d. مباحث حقوق جزای عمومی ناظر به کلاهبرداری(موارد تخفیف یا تشدید مجازات، معاونت یا شرکت در جرم- کلاهبرداری و تعدد یا تکرار آن) e. صور خاص کلاهبرداری(انتقال مال غیر، تبانی و مواضعه برای بردن مال غیر و معرفی مال دیگری به عوض مال- خود، کلاهبرداری رایانه‌ای و).... ۲. خیانت در امانت a. مقدمه :تعریف، تاریخچه، ویژگیها b. ارکان– i. رکن مادی(رفتار فیزیکی، شرایط و اوضاع و احوال لازم برای تحقق جرم و نتیجه ی حاصله)شروع به جرم- خیانت در امانت. ii. رکن روانی c. واکنش در برابر جرم خیانت در امانت(کیفرهای اصلی، تبعی و تکمیلی-) d. مباحث حقوق جزای عمومی ناظر به جرم خیانت در امانت(موارد خفیف یا تشدید مجازات، معاونت یا- e. شرکت در جرم خیانت در امانت و تعدد و تکرار آن) f. صور خاص خیانت در امانت(اختلاس، سوء استفاده از ضعف نفس اشخاص، سوء استفاده از سفید مهر یا سفیدامضاء، خیانت مستخدمان دولت در اسناد دولتی و)... g. ۳. سرقت		

	a. مقدمه :تعریف، تاریخچه، ویژگیها و جایگاه آن در فقه اسلامی و سایر نظامهای حقوقی b. ارکان- i. رکن مادی(رفتار فیزیکی، شرایط و اوضاع و احوال لازم برای تحقق جرم و نتیجه حاصله)شروع به جرم سرقت. ii. رکن روانی c. اقسام سرقت و شرایط و احکام آن i. سرقت حدی(شرایط، راههای ثبوت و شرایط اجرای حد و)... ۱. مباحث حقوق جزای عمومی ناظر به سرقت حدی(موارد تخفیف، تشر، ...شرکت، تعدد و تکرار) ii. سرقت تعزیری ۱. شرایط و راههای ثبوت ۲. مباحث حقوق جزای عمومی ناظر به سرقت تعزیری(موارد تخفیف یا تشدید مجازات، معاونت یا شرکت در جرم سرقت حدی و تعدد و تکرار) ۳. انواع سرقتهای تعزیری(مقرون به آزار، سرقت مسلحانه، راهزنی، سرقت از موزه‌ها یا اماکن تاریخی، کیف زنی یا جیب بُری، سرقت از محل تصادفات رانندگی یا مناطق حادثه زده، سرقت یا استفاده غیر مجاز از آب، رق، گاز و تلفن، سرقت رایانه ای(سایبری)، سرقت ساده تعزیری) ۴. مداخله در اموال مسروق- ۴. صدور چک پرداخت نشدنی a. مقدمه : مفهوم، تعریف، تاریخچه، ویژگی ها و مبانی جرم انگاری b. ارکان– i. رکن مادی(رفتار فیزیکی، شرایط و اوضاع و احوال لازم برای تحقق جرم؛ موارد سلب جنبه کیفری چک ونتیجه حاصله.) ii. رکن روانی c. مسائل مربوط به شکایت و دادرسی در جرم صدور چک پرداخت نشدنی- d. واکنش نسبت به جرم صدور چک پرداخت نشدنی- e. مباحث حقوق جزای عمومی ناظر به جرم صدور چک پرداخت نشدنی(موارد تخفیف، تشدید، معاونت، شرکت، تعدد و تکرار) ۵. تخریب کیفری a. مقدمه : تعریف، تاریخچه، ویژگیها b. ارکان– i. رکن مادی(رفتار فیزیکی، شرایط و اوضاع و احوال لازم برای تحقق جرم نتیجه حاصله به اضافه شروع به جرم) ii. رکن روانی c. واکنش در برابر جرم تخریب(کیفرهای اصلی، تبعی و تکمیلی-) d. مباحث حقوق جزای عمومی ناظر به تخریب(موارد تشدید، تخفیف، معاونت، شرکت، تعدد و تکرار-) e. صور خاص تخریب(تخریب آثار فرهنگی، رایانه‌ای(سایبری)و سایر موارد)
کتاب (های) مرجع	منابع فارسی:

	[۱] زراعت، عباس، حقوق جزای اختصاصی(۱) جرایم علیه اموال و مالکیت، تهران، انتشارات جنگل، آخرین سال انتشار [۲] شامبیاتی، هوشنگ، حقوق جزای اختصاصی، جلد دوم(جرایم علیه اموال و مالکیت)، تهران، انتشارات مجد، آخرین سال انتشار [۳] گلدوزیان، ایرج، بایسته های حقوق جزای اختصاصی، تهران، نشر میزان، آخرین سال انتشار [۴] میرمحمدصادقی، حسین، حقوق کیفری اختصاصی(۱)، جرایم علیه اموال و مالکیت، تهران، نشر میزان، آخرین سال انتشار [۵] میرمحمدصادقی، حسین، حقوق جزای اختصاصی انگلستان و نقش حقوق جزا در جامعه، تهران، انتشارات جنگل،آخرین سال انتشار [۶] مقالات علمی معتبر مرتبط با سرفصل درس در مجلات حقوقی داخلی و خارجی.
سایر مراجع	**منابع انگلیسی:** [1] J.C.Smith and B.Hogan, Criminal Law, Oxford University Press, ۱۱thed, ۲۰۰۵. [2] T.J.Gardner and T.M.Anderson, Criminal Law, Wadsworth Publishing, ۱۳thed, ۲۰۱۴. [3] C.M.V.Clarkson, Understanding Criminal Law, Sweet & Maxwell, ۱thed, ۲۰۰۵. [4] A.P.Simester and G.R.Sullivan, Criminal Law: Theory and Doctrine, Oxford: Portland Oregon, ۲۰۰۳. [5] A.Read and P.Seago, Criminal Law, Sweet & Maxwell, ۲۰۰۲. [6] M.Jefferson, Criminal Law, Pearson/Longman, ۹thed, ۲۰۰۱. **منابع فرانسه:** [1] Thierry Fossier ,Droit pénal spécial. Affaires, entreprises et institutions publiques,۲e édition , Larcier , ۲۰۱۵. [2] Thierry Garé ,Droit pénal spécial. Personnes et biens,۱e édition ,Larcier ,۲۰۱۵ . [3] Coralie Ambroise-Casterot ,Droit pénal spécial et des affaires. ۱۳ exercices corrigés,۳e édition , Gualino Editeur, ۲۰۱۴ . [4] Coralie Ambroise-Casterot ,Droit pénal spécial et des affaires,۱e édition , Gualino Editeur,۲۰۱۴ .

حقوق جزای اختصاصی (٤) جرایم علیه شخصیت معنوی اشخاص

نام درس به فارسی	حقوق جزای اختصاصی (۴) جرایم علیه شخصیت معنوی اشخاص		
نام درس به انگلیسی	Criminal Law (Crimes against Humanity)		
نوع درس	جبرانی	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۱ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	نظر به اینکه انسان از دو بعد مادی و معنوی برخوردار است، آشنایی دانشجویان با جرایم علیه حیثیت و کرامت انسانی علاوه بر جرایم علیه تمامیت جسمانی، ضروری است. هدف :آشنا کردن دانشجویان با ماهیت، اهمیت و ارکان تشکیل دهنده ی جرایم علیه آزادی و حیثیت معنوی افراد درقوانین ایران و مقایسه مختصر با یکی از نظامهای حقوقی معتبر		
نتایج درس			
فهرست مباحث	کلیات : ۱. تعریف و ویژگیها، اهمیت و تقسیم بندی ۲. جرایم علیه آزادی تن شامل توقیف، اخفاء و حبس غیر قانونی • ارکان • واکنشها ۳. جرایم علیه آزادی روان شامل سلب حقوق و آزادی مردم، تهدید، ایجاد مزاحمت تلفنی، هتک حرمت ۴. منازل، مراسلات، مخابرات، مکالمات تلفنی و افشای اسرار • ارکان • واکنش ۵. جرایم علیه حیثیت شامل توهین، افتراء، قذف، نشر اکاذیب • ارکان • واکنش‌ها		
کتاب (های) مرجع	**منابع فارسی:** [۱] آقایی نیا، حسین، جرایم علیه اشخاص(شخصیت معنوی)، تهران، نشر میزان، آخرین سال انتشار [۲] شامبیاتی،هوشنگ، حقوق جزای اختصاصی، جلد اول(جرایم علیه اشخاص)، تهران، انتشارات مجد، آخرین سال انتشار [۳] زراعت، عباس، حقوق جزای اختصاصی(۱)جرایم علیه اشخاص، تهران، انتشارات جنگل جاودانه، آخرین سال انتشار [۴] گلدوزیان، ایرج، بایسته های حقوق جزای اختصاصی، تهران، نشر میزان، آخرین سال انتشار		

	[۵] میرمحمدصادقی، حسین، حقوق جزای اختصاصی (۱)، جرایم علیه اشخاص، تهران، نشر میزان، آخرین سال انتشار [۶] میرمحمدصادقی، حسین، حقوق جزای اختصاصی انگلستان و نقش حقوق جزا در جامعه، تهران، انتشارات جنگل جاودانه، آخرین سال انتشار [۷] مقالات علمی معتبر مرتبط با سرفصل درس در مجلات حقوقی داخلی و خارجی.
سایر مراجع	**منابع انگلیسی:** ۱. J.C.Smith and B.Hogan, Criminal Law, Oxford University Press, ۱۱thed, ۲۰۰۵. ۲. T.J.Gardner and T.M.Anderson, Criminal Law, Wadsworth Publishing, ۱۳thed, ۲۰۱۴. ۳. C.M.V.Clarkson, Understanding Criminal Law, Sweet & Maxwell, ۱thed, ۲۰۰۵. 4.A.P.Simester and G.R.Sullivan, Criminal Law: Theory and Doctrine, Oxford: Portland Oregon, ۲۰۰۳. ۵. A.Read and P.Seago, Criminal Law, Sweet & Maxwell, ۲۰۰۲. ۶. M.Jefferson, Criminal Law, Pearson/Longman, ۹thed, ۲۰۰۱. **منابع فرانسه:** ۱. Michel Véron ,Droit pénal spécial,۱۹e édition , Dalloz-Sirey , ۲۰۱۵. ۲. Sylvain Jacopin ,Droit pénal spécial. Les atteintes aux personnes,۳e édition ,Hachette Supérieur ,۲۰۱۳ . ۳. Thierry Garé ,Droit pénal spécial. Personnes et biens,۱e édition ,Larcier ,۲۰۱۵. ۴. Michel Véron ,Droit pénal spécial,۱۹e édition , Dalloz-Sirey , ۲۰۱۵.

سرفصل دروس گروه ۱ (الزامی جرم‌یابی دیجیتال)

اصول جرم یابی دیجیتال

نام درس به فارسی	اصول جرم یابی دیجیتال		
نام درس به انگلیسی	Concepts of Digital Forensics		
نوع درس	الزامی –گروه ۱	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم‌یابی	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها	سیستم عامل، ساختار سیستم فایل‌ها		
مطالب پیش نیاز			
اهداف درس	هدف از این درس آشنایی دانشجویان با مفاهیم، اصول و کابردهای جرم‌یابی دیجیتال است. در این درس تمرکز به لحاظ فنی بر روی یک سیستم ایزوله از نوع Desktp بوده و به معرفی ساختار سیستم فایل در سیستم‌عاملهای ویندوز و لینوکس پرداخته می‌شود. به لحاظ عملی دانشجویان با ابزارهای شاخص جرم‌یابی آشنا شده و تمرینهایی را با آنها انجام خواهند داد. همچنین مراحل بازپرسی دیجیتال با هدف جمع‌آوری شواهد و ادله قابل استناد از سیستم‌ها تشریح شده و در ادامه مستندسازی و گزارش رسمی ادله تبیین می‌گردد.		
نتایج درس	دانشجویان با اصول و کابردهای جرم‌یابی دیجیتال آشنا می‌شوند. همچنین فرآیند بازپرسی دیجیتال شامل جمع‌آوری شواهد و ادله قابل استناد با استفاده از ابزارهای مختلف و مستندسازی و گزارش نویسی تشریح می‌گردد.		
فهرست مباحث	**مفاهیم پایه** • نگاه کلی به جرم یابی دیجیتال ○ ساختار و روند جرم‌یابی دیجیتال (در قالب یک روش علمی کشف جرائم) • قوانین تاثیرگذار بر تحقیقات دیجیتال ○ حریم خصوصی ○ ادله تخصصی **مفاهیم مدیریت سیستم فایل** • ساختار دیسک، پارتیشن، سیستم فایل لینوکس و ویندوز • تحلیل سیستم فایل NTFS، EXT و HFS و بحث‌های لایه فیزیکی • تحلیل برنامه‌های کاربردی در سیستم‌عاملهای مختلف • تشخیص برنامه‌هایی که از دید ابزارهای کاوشگری نظیر زیر از دید سیستم عامل پنهان می‌مانند. ○ Event-Viewer ○ Task-Manager • تحلیل رویدادها، جستجو بر اساس کلیدواژه و مشخصات زمانی • امضای فایل، جستجوی متنی ○ عبارات منظم، ابزارهای لینوکسی grep، egrep و fgrep **روشهای بنهان‌سازی داده‌ها** • تشخیص داده‌های پنهان • بازیابی فایلهای حذف شده، • رمزنگاری، رمزگشایی • برش فایلهای تصویر و چندرسانه‌ای • پنهان‌نگاری : تشخیص اصالت و بازیابی تصاویر و فایلهای چندرسانه‌ای ○ جرم‌یابی در حوزه چندرسانه‌ای		

	• بازیابی فایلهای swap • فایلهای موقت و فایلهای کش شده **آشنایی با ابزارهای برتر جرم‌یابی** ○ تهیه تصویر، تحلیل و گزارش ادله دیجیتال ▪ Encase ▪ Helix ▪ FTK (Forensic Toolkit) ▪ Autopsy ▪ FIRE ▪ Found stone Forensic ToolKit ▪ SANS SIFT ○ تحلیل سیستم فایل ▪ Sleuth kit Forensic Browser ▪ WinHex ○ تحلیل حافظه ▪ Volatility ▪ Linux dd **بازپرسی دیجیتال : روشهای وارسی، تحقیق و کشف ادله** • اولین پاسخ در بازپرسی دیجیتال ○ کنترل صحنه و وضعیت جرم ○ پردازش، مدیریت و جستجوی ادله دیجیتال • مفاهیم مربوط به Data Carving و File Carving • استحصال داده‌ها (Data Acquisition) • گرفتن تصویر از دیسک (disk-image) • رونوشت (dump) از حافظه RAM • رونوشت (dump) از حافظه نهان (Cache) • جرم‌یای حافظه‌های SD • فایلهای رجیستری ویندوز • جرم‌یابی برخط و پاسخگویی به رخدادها • تحلیل ایستا و پویای کدهای اجرایی • طراحی و اجرای عملیات جستجو و ضبط با هدف یافتن ادله دیجیتال • معرفی ابزارها و تکنیک‌های مورد استفاده در تحلیل ادله دیجیتال • مستندسازی و گزارش
نرم افزارهای مورد نیاز	در بخش آشنایی با ابزارهای جرم‌یابی آمده است.
تکالیف پیشنهادی	حداقل یک تکلیف عملی شامل تحلیل با ابزارهای جرم‌یابی تدریس شده
پروژه های پیشنهادی	بررسی موردی یک جرم دیجیتال واقعی
کتاب (های) مرجع	[1] *Digital archaeology: the art and science of digital forensics*. By Graves, Michael W. , Pearson Education, 2013. [2] *Guide to Computer Forensics and Investigations* 5th Edition, Nelson, Phillips, Steuart, Cengage Learning, 2015 [3] *File System Forensic Analysis*, by Brian Carrier, Addison-Wesley, 2005
سایر مراجع	

جرم‌یابی دیجیتال پیشرفته

نام درس به فارسی	جرم یابی دیجیتال پیشرفته		
نام درس به انگلیسی	Advanced Digital Forensics		
نوع درس	الزامی – گروه ۱	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم‌یابی	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها	مقاهیم جرم یابی دیجیتال، شبکه پیشرفته، امنیت شبکه		
مطالب پیش نیاز			
اهداف درس	در این درس جرم‌یابی در بستر شبکه و دستگاههای همراه با هدف جمع‌آوری ادله و شواهد وتحلیل آنها مورد توجه قرار می‌گیرد. در هر دو مورد چالشها بیان شده و راهکارهای مختلف تبیین می‌گردد. در ادامه به دو جرم خاص دیجینال، جعل و سرقت ادبی پرداخته می‌شود و راهکارهای تشخیص و جمع‌آوری شواهد برای آنها معرفی می‌گردد.		
نتایج درس			
فهرست مباحث	**جرم یابی در بستر شبکه** • طرح بازجویی و ضبط از شبکه‌های خانگی تا شبکه‌های سازمانی • فناوریها و پروتکلهای مربوط به شبکه‌های محلی LAN • ساختار و مدیریت شبکه • تحلیل شبکه‌های بی‌سیم • آشنایی با ابزارهای دریافت و شنود بسته‌های داده (Packet sniffer) • تحلیل بسته‌های شبکه به لحاظ پروتکل و داده • ابزارهای تشخیص و جلوگیری از نفوذ • شناسایی شبکه‌های مشکوک • شناسایی و بازیابی عاملهای سرور و کلاینت مظنون • دسترسی راه دور • جمع‌آوری و تحلیل ادله‌های مبتنی بر شبکه • بازسازی عملیات مرور وب • فعالیت‌های پست الکترونیک (ایمیل) • جرم یابی در شبکه‌های SDN • تغییر رجیستری ویندوز، رهگیری مهاجم **جرم‌یابی دستگاههای همراه** • اصول جرم‌یابی دستگاههای همراه • چالشهای جرم‌یبای دستگاههای همراه • حافظه‌های خاص دستگاه همراه ○ استحصال، دریافت و ذخیره داده‌ها • جرم‌یابی شبکه‌ی خاص دستگاههای همراه ○ تفسیر ادله دیجیتال گردآوری شده از بستر شبکه موبایل • بدافزارهای خاص بسترهای موبایل		

	• جمع‌آوری ادله‌ی دیجیتال از دستگاههای همراه • جنبه‌های حقوقی جرم‌یابی دستگاههای همراه **جعل در حوزه‌ی دیجیتال** • مقدمه‌ای بر بازپرسی جعل، مهارت‌های لازم برای کارشناس و بازپرس جعل • ماهیت و دامنه جعل (قانون بنفورد) • مطالعه موردی : تحلیل مجموعه داده‌های مالی با استفاده از قانون بنفورد **سرقت ادبی (Plagiarism)** • تشخیص سرقت و تعیین کیفیت مولف **مهندس معکوس** ○ رویکردهای دفاع از نرم‌افزارهایی که هدف حملات مهندسی معکوس قرار دارند ○ مبهم‌سازی (obfuscation) در سخت‌افزار، میان‌افزار و نرم‌افزار ▪ برای مقابله با مهندسی معکوس ابزار ○ ارتقای امنیت با کتابخانه‌ی نرم‌افزاری طرف سوم مورد اعتماد **رویکردها، تکنیک‌ها و ابزارهای ضدجرم‌یابی (Antiforensics)** • پنهان سازی داده‌های سیستم • تخریب ابزار، تخریب داده‌ها و امحاء اطلاعات • داده‌های کانال جنبی (Covert Data) **سایر مباحث فنی** • جرم‌یابی حوزه پردازش ابری • ساختار وتحلیل فرمت‌های دیسک نوری • تحلیل جرم‌یابی ماشین‌های مجازی • آشنایی با مفاهیم دیسک پویا، دیسک spanned و دیسک striped در ویندوز • تحلیل جرم‌یابی کپی‌های در سایه (shadow copy)
نرم افزارهای مورد نیاز	ابزارهای مرتبط با جرم‌یابی دیجتال در حوزه شبکه و دستگاههای همراه
تکالیف پیشنهادی	حداقل یک تکلیف عملی شامل تحلیل با ابزارهای جرم‌یابی تدریس شده
پروژه های پیشنهادی	بررسی موردی یک جرم دیجیتال واقعی
کتاب (های) مرجع	[1] *Digital archaeology: the art and science of digital forensics*. By Graves, Michael W. , Pearson Education, 2013. [2] *Guide to Computer Forensics and Investigations*, by Nelson, Phillips, Enfinger, and Steuart, Thomson Course Technology, 2004 [3] *Hacking Exposed Computer Forensics*, by Davis, Cowen, and Philipp, McGraw-Hill/Osborne, 2005 [4] *Real Digital Forensics*, by Jones, Bejtlich, and Rose, Addison-Wesley, 2006
سایر مراجع	

گردآوری و ردیابی شواهد و ادله دیجیتال

نام درس به فارسی	گردآوری و دریابی شواهد و ادله دیجیتال		
نام درس به انگلیسی	Digital Evidence Trace and Collection		
نوع درس	الزامی-گروه۱	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم‌یابی	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها	اصول جرم‌یابی دیجیتال		
مطالب پیش نیاز			
اهداف درس	هدف از این درس آشنایی دانشجویان با فرایند طراحی و اجرای عملیات بازپرسی دیجیتال است که مشتمل بر شناسایی و حفظ ادله، گرداوری، جستجو، ضبط و مصادره، وارسی، تحلیل، تنظیم گزارش و تصمیم گیری نهایی می‌باشد. در این راستا قوانین موضوعه داخلی که در این فرآیند تاثیر دارد نیز تبیین خواهد شد..		
نتایج درس			
فهرست مباحث	• پایه و اساس راهبرد جرم یابی • انتخاب و گرد آوری ادله وشواهد • پیشینه و تاریجچه علم جرم یابی دیجیتال • بازپرسی جرائم دیجیتال • طراحی و اجرای عملیات بازپرسی دیجیتال ○ شناسایی و حفظ ادله ○ گرداوری ادله ○ جستجو و یافتن ادله ○ ضبط و مصادره ادله ○ وارسی ادله ○ تحلیل ادله ○ ارائه و تنظیم گزارش ○ تصمیم گیری • آشنایی با ابزارها و روشهای وارسی ادله دیجیتال • روند انتخاب و گردآوری ادله دیجیتال از رایانه‌های شخصی • روند انتخاب و گردآوری ادله دیجیتال از دستگاههای همراه • روند انتخاب و گردآوری ادله دیجیتال از بستر شبکه • گردآوری زنده (Live) ادله بر حسب پایداری داده‌ها از: ○ حافظه نهان، پردازنده و ثبات ها ○ جدول مسیریابی، حافظه ARP، حافظه پردازده ها ○ حافظه اصلی (رم)		

	○ فایل سیستم موقت – فضای سواپ ○ داده‌های روی دیسک سخت ○ داده‌های لاگ شده راه دور ○ داده‌های پشتیبان روی رسانه‌های آرشیو • قوانین موضوعه داخلی در مورد بازپرسی دیجیتل
نرم افزارهای مورد نیاز	نرم افزارهای معرفی شده در دروس اصول جرم یابی دیجیتال و جرم یابی دیجیتال پیشرفته
تکالیف پیشنهادی	کار با ابزراهای جرم یابی و کشف ادله
پروژه های پیشنهادی	یک پروژه عملی شامل گردآوری ادله دیجیتال
کتاب (های) مرجع	[1] Kyung-shick Choi, Cybercriminology and Digital InvestigationOct , 2015 [2] Thomas K. Clancy, Cyber Crime and Digital Evidence: Materials and Cases, First Edition 2011, LexisNexis, ISBN: 9781422494080 [3] E Casey, Digital evidence and computer crime: Forensic science, computers, and the internet, 2011
سایر مراجع	[2] Ian Walden, Computer Crimes and Digital Investigations, Oxford University Press, May 2007

جرائم سایبری

نام درس به فارسی	جرائم سایبری		
نام درس به انگلیسی	Cyber Crimes		
نوع درس	الزامی-گروه۱	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها	شبکه‌های کامپیوتری		
مطالب پیش نیاز	شبکه، امنیت شبکه		
اهداف درس	در این درس جرائم مربوط به فضای دیجتال معرفی می‌گردد. در این بخش نگاه کلی به قضیه خواهیم داشت و تمامی عملیاتی که می‌تواند از دید بعضی قوانین (داخلی، سایر کشورها وبین المللی) جرم انگاشته شود، تشریح می‌شود. در ادامه به قانون جرائم رایانه‌ای ایران مصوب خرداد ماه ۱۳۸۸ پرداخته شده و جرائم از دید این قانون بازبینی می‌شود. همچنین به طور خاص جرائم مرتبط با مالکیت فکری، تجارت الکترونیک و پولشویی به طور مشروح مورد توجه قرار می‌گیرد. در ادامه رویکردهای پیشگیری از جرم شامل راهبردها، تدوین دستورالعمل‌ها، توسعه‌ی ابزارها و کنترلهای فنی و آموزش افراد مطالعه شده و مورد بررسی و نقد قرار خواهد گرفت.		
نتایج درس			

فهرست مباحث	**مقدمه**
	• کامپیوتر، اینترنت و تاثیرات اجتماعی آن
	• نیاز به قوانین سایبری
	• سیستم قضایی فضای سایبری در جهان و ایران
	
	جرائم سایبری و چارچوب قانونی
	• جرائم سایبری علیه افراد، سازمانها و کشورها
	• هک کردن سیستم‌ها
	• جعل در فضای دیجیتال (Digital Forgery)
	• سرقت شناسه و کلاهبرداری (Fraud)
	  ○ Spyware
	  ○ Phishing
	  ○ Spam
	• شنود، رهگیری و آزاررسانی سایبری (Stalking/Harassment)
	• هرزه‌نگاری(در کل و به ویژه کودکان) در فضای سایبری
	  ○ تولید، توزیع، نگهداری و تماشای محتوای هرزه
	  ○ اثبات واقعی بودن تصاویر هرزه
	• شبکه‌ها ی اجتماعی و شکارچی کودکان (Child predator)
	• تروریسم سایبری
	• تهمت و افتراء در فضای سیایبری (Cyber Defamation)		

- آسیب‌رسانی دیجیتالی(Tort)
- قوانین CFAA (Computer Fraud and Abuse Act)

قانون جرائم رایانه ای ایران مصوب خرداد ۱۳۸۸

- جرائم
  - جرائم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی
  - جرائم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی
  - سرقت و کلاهبرداری مرتبط با رایانه
  - جرائم علیه عفت و اخلاق عمومی
  - هتک حیثیت و نشر اکاذیب
- آئین‌دادرسی
  - صلاحیت دادرسی
  - جمع‌آوری ادله الکترونیکی
  - تفتیش و توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی
  - شنود محتوای ارتباطات رایانه‌ای
  - استناد پذیری ادله الکترونیکی

جرائم مرتبط با مالکیت فکری در فضای سایبری

- ارتباط با قوانین کپی رایت
- ارتباط با قوانین ثبت اختراع (Patent Law)
- جنبه‌های مرتبط با علائم و نشان‌های تجاری (Trademarks)

جرائم مرتبط با تجارت الکترونیک

- مفاهیم و رویکردهای تجارت برخط نظیر B2B، B2C و C2C
- قراردادهای برخط امن
- کاربرد مرتبط با قانون تجارت الکترونیکی مصوب دی ماه ۱۳۸۲

جرائم مرتبط با پولشویی

- روشها و تکنیک‌های پولشویی
- رویکزدهای مقابله با پپولشویی
- شبکه مالی تروریسم

پیشگیری از جرائم

- توسعه و ارتقاء ابزارهای فنی نرم افزاری و سخت افزاری
  - ابزارهای تشخیص و جلوگیر از نفوذ
  - ابزارهای شناساسیی بدافزار
  - ابزارهای Anti-phishing
- آموزش افراد
- تدوین قوانین، آیین نامه و سیاست‌های امنیتی

	• مدیریت ریسک و ارزیابی امنیتی
پروژه های پیشنهادی	یک پروژه پژوهشی شامل بررسی آماری، تحلیلی جرمهای دیجیتال
کتاب (های) مرجع	[1] Justice Yatindra Singh, *Cyber Laws*, Universal Law Publishing Co, New Delhi, (2012). [2] Thomas K. Clancy, Cyber Crime and Digital Evidence: Materials and Cases, First Edition 2011, LexisNexis, ISBN: 9781422494080 [3] McQuade III, Samuel C. 2006. Understanding and Managing Cybercrime. ISBN 0-205-43973-X [4] Moore, Robert, (2011). Cybercrime, investigating high-technology computer crime (2nd Ed.). Elsevier
سایر مراجع	۱. قوانین جرائم رایانه ای مصوب خرداد ماه ۱۳۸۸، مرکز پژوهشهای مجلس شورای اسلامی ۲. قانون تجارت الکترونیکی مصوب دی ماه ۱۳۸۲، مرکز پژوهشهای مجلس شورای اسلامی

سرفصل دروس کروه ۲ (دروس الزامی حقوق)

آیین دادرسی جرائم دیجیتال

نام درس به فارسی	آیین دادرسی جرائم دیجیتال		
نام درس به انگلیسی	Courtroom Skills for Digital Crimes		
نوع درس	الزامی-گروه۲	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم‌یابی	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز	اصول جرم‌یابی دیجیتال		
اهداف درس	• آشنایی با ادله دیجیتال شامل گردآوری، اصالت و استنادپذیر بودن • زنجیره امانتداری، اصالت ادله و صحت جرم‌یابی • آشنایی با نقش و مسوولیتهای کارشناس جرم یابی دیجیتال • تنظیم گزارش تخصصی حاوی ادله دیجیتال • ارائه شواهد دیجیتال در دادگاه • آمادگی برای دفاع یا وارسی و به چالش کشیدن ادله دیجیتال		
نتایج درس			
فهرست مباحث	**بحث‌های حقوقی ادله دیجیتال** • ادله دیجیتال : گردآوری، اصالت و استنادپذیر بودن • زنجیره امانتداری، اصالت ادله و صحت جرم‌یابی • قوانین مربوط به ادله و شواهد، انتخاب بهترین شاهد، شواهد و دلایل علمی **جنبه‌های اجتماعی جرم‌یابی دیجیتال** • ساختار سیستم قضایی • شواهد و ادله‌ها و عاملهای تصمیم‌گیر (از قاضی تا هیات منصفه) • سیستم دادرسی • ایجاد پروفایلی رواشناسانه از هکرها و نویسنده‌های بدافزار **بازپرسی دیجیتال : روشهای وارسی، تحقیق و کشف ادله** ○ اولین پاسخ در بازپرسی دیجیتال ○ کنترل صحنه و وضعیت جرم ○ پردازش، مدیریت و جستجوی ادله دیجیتال ○ نقش و مسوولیتهای قانونی کارشناس جرم‌یابی دیجیتال ○ روند قانونی مربوط به جرائم مدنی و جنائی ○ ذکر شواهد و ادله دیجیتال در یک گزارش رسمی ○ تنظیم گزارش تخصصی حاوی ادله دیجیتال ○ مهارتهای مربوط به ارائه شواهد و ادله دیجیتال در دادگاه ○ وارسی اولیه ادله دیجیتال با حضورخوانده (in-chief-examination)		

	○ امکان وارسی مجدد ادله دیجیتال(re-examination) ○ مهارت لازم برای وارسی و مطابقت دادن ادله‌های دیجیتال متفاوت (cross-examination) **جرائم سایبری** • قوانین CFAA (Computer Fraud and Abuse Act) • مثالهای خاص نظیر هک سیستم‌ها، سرقت شناسه و شنود سایبری
پروژه های پیشنهادی	حداقل یک پروژه عملی شامل تهیه ادله دیجیتال، تحلیل و گزارش جهت ارائه به دادگاه برای یک جرم واقعی
کتاب (های) مرجع	[1] *Digital archaeology: the art and science of digital forensics*. By Graves, Michael W. , Pearson Education, 2013. [2] Jarrett, H. Marshall; Bailie, Michael W. (2010). "Prosecution of Computer Crimes" (PDF). justice.gov. Office of Legal Education Executive Office for United States Attorneys. Retrieved June 3, 2013.
سایر مراجع	[1] Atchinson, Brian K.; Fox, Daniel M. (May–June 1997). "The Politics Of The Health Insurance Portability And Accountability Act" (PDF). Health Affairs. 16 (3): 146–150. doi:10.1377/hlthaff.16.3.146 [2] H.R. 4718 (99th): Computer Fraud and Abuse Act of 1986

قوانین اینترنت و فضای سایبری

نام درس به فارسی	قوانین اینترنت و فضای سایبری		
نام درس به انگلیسی	Internet and Cyber-space Laws		
نوع درس	الزامی-گروه۲	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها	شبکه‌های کامپیوتری		
مطالب پیش نیاز			
اهداف درس	آشنایی دانشجویان با : • مبانی حقوق بشری و حقوق اساسی در فضای سایبری • قوانین سایبری از منظر حقوق بین الملل • قوانین حریم خصوصی در حوزه سلامت • قوانین مرتبط با تجارت الکترونیک • قوانین مرتبط با پولشویی • فرایندهای حل اختلاف در فضای سایبری		
نتایج درس			
فهرست مباحث	**قوانین اینترنت و فضای سایبری** **مقدمه** • کامپیوتر، اینترنت و تاثیرات اجتماعی آن • نیاز به قوانین سایبری • سیستم قضایی فضای سایبری در جهان و ایران **مبانی حقوق بشری و حقوق اساسی در فضای سایبری** • حقو آزادی بیان در فضای سایبری • حق دسترسی آزاد به اطلاعات، فضای سایبری و اتصال به اینترنت • حفظ حریم خصوصی ○ مصادیق و محدودیت‌ها (رعایت در حد معقول و پذیرفته شده) ○ شرایط استثناء (همانند شرایط بحرانی، رضایت و شهادت) • حق محافظت از اطلاعات **قوانین سایبری از منظر حقوق بین الملل** • ابتکارات سازمان ملل و اتحادیه جهانی ارتباطات راه دور (ITU) • معاهده (کنوانسیون) بوداپست در مورد فضای سایبری (مصوب پارلمان اتحادیه اروپا) • سازمان همکاریهای اقتصادی آسیا-اقیانوسیه (APEC) • سازمان همکاری و توسعه‌ی اقتصادی (OECD) • بانک جهانی •		

	قوانین مرتبط با مالکیت فکری در فضای سایبری • ارتباط با قوانین کپی رایت • ارتباط با قوانین ثبت اختراع (Patent Law) • جنبه‌های مرتبط با علائم و نشان‌های تجاری (Trademarks) **قوانین حریم خصوصی در حوزه سلامت** • آشنایی با استاندارد سلامت HIPPA، FERPA و ECPA • قوانین موضوعه‌ی داخلی در حوزه دیجیتال و تشخیص تعارض آنها با قوانین بین‌المللی **قوانین مرتبط با تجارت الکترونیک** • مفاهیم و رویکردهای برخط تجارت نظیر B2B، B2C و C2C • قراردادهای برخط امن • کاربرد مرتبط با قانون تجارت الکترونیکی مصوب دی ماه ۱۳۸۲ **قوانین مرتبط با پولشویی** • روشها و تکنیک‌های پولشویی • رویکزدهای مقابله با پولشویی • قوانین مقابله با پولشویی و شبکه مالی تروریسم در سطح جهان و ایران • آشنایی با FATF **فرایندهای حل اختلاف در فضای سایبری** • مکانیزم‌های حل اختلاف ○ سیستم دادرسی با صدور رای از طرف داور، قاضی یا هیات منصفه ○ سیستم مشارکتی مبتنی بر همکاری، میانجیگری، مذاکره و مصالحه طرفها • سیستم قضایی و صلاحیت دادرسی • قوانین بین المللی و صلاحیت‌های دادرسی در جرائم سایبری
پروژه های پیشنهادی	یک پروژه پژوهشی شامل بررسی موضوعی قوانین دیجیتال سایر کشورها
کتاب (های) مرجع	[1] Chris Reed & John Angel, *Computer Law*, OUP, New York, (2007). [2] Justice Yatindra Singh, *Cyber Laws*, Universal Law Publishing Co, New Delhi, (2012).
سایر مراجع	۱. قوانین جرائم رایانه ای مصوب خرداد ماه ۱۳۸۸، مرکز پژوهشهای مجلس شورای اسلامی ۲. قانون تجارت الکترونیکی مصوب دی ماه ۱۳۸۲، مرکز پژوهشهای مجلس شورای اسلامی

سرفصل دروس اختیاری

طراحی سیستم های امنیتی تحمل پذیر اشکال

نام درس به فارسی	طراحی سیستم های امنیتی تحمل پذیر اشکال		
نام درس به انگلیسی	Fault-Tolerant Systems Design		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	سیستمهای کامپیوتری در بسیاری از امور زندگی ما دخالت و تاثیر دارند. برای مثال می‌توان از کنترل نیروی هوایی، کنترل قطار و مترو، کنترل نیروگاههای اتمی، مخابرات، شبکه، دستگاههای پزشکی، ارتباطات بانکی، اتوماسیون صنایع و سیستم‌های تعبیه شده (موبایل، اتومبیل و ماهواره) نام برد. اطمینان به کارکرد صحیح چنین سیستم‌ها یک امر اجتناب ناپذیر است. این سیستم‌ها بایستی به گونه‌ای طراحی شوند که بتوانند اشکال‌هایی را که در حین کار آنها رخ می‌دهد تحمل کرده و سرویس مورد نظر را ارائه نمایند. این درس به طور کلی به روش‌های تحمل پذیری اشکال‌هایی که در قسمت‌های سخت‌افزاری یک سیستم رخ می‌دهد، به طور مختصر نیز اشاره می‌کند.		
نتایج درس	توجه و ترغیب مهندسان و طراحان سیستم‌های کامپیوتری به حساسیت و امنیت به کارگیری ساز و کارهای تحمل پذیری اشکال		
فهرست مباحث	۱.مقدمه‌ی تحمل پذیری اشکال ●چرا به تحمل پذیری اشکال نیاز داریم؟ ●کاربردهای سیستم‌های تحمل پذیری اشکال ●مفاهیم مهم و اساسی : قابلیت اطمینان، دسترس پذیری، ایمنی، قابلیت نگهداری، محرمانگی، تمامیت، امنیت، آزمون پذیری و اتکا پذیری ●تعاریف مهم و اساسی : اشکال، خطا و خرابی ●مشخصات و ویژگیهای اشکال ●مدلهای اشکال/خطا ●اشکال شدن اشکال و خطا ۲.روش‌های طراحی در تحمل پذیری اشکال ●افزونگی سخت‌افزاری رأی‌گیری سه‌پیمانه‌ای، رأی گیری n پیمانه‌ای ●افزونگی اطلاعات : کدهای توازن، کدهای m-of-n ●افزونگی زمانی : اجرای مجدد، محاسبه‌ی مجدد ●افزونگی نرم‌افزاری : وارسی‌های سازگاری، چند نسخه برنامه‌نویسی ۳.روش‌های ارزیابی		

	●روش‌های کمی: تخمین نرخ اشکال، تابع قابلیت اطمینان، پوشش اشکال، زمان متوسط تا خرابی، زمان متوسط تا تعمیر، زمان متوسط بین خرابی ●مدلسازی قابلیت اطمینان : مدلسازی ترکیبی، مدلسازی m+of+n، مدلسازی مارکوف ●محاسبه قابلیت اطمینان چند سیستم با یک نرم‌افزار ۴.محاسبه نرخ اشکال با استفاده از مدلهای تجربی ۵.طراحی سیستم های تحمل پذیر اشکال ۶.بررسی چند نمونه از سیستم‌های تحمل‌پذیر اشکال
نرم افزارهای مورد نیاز	استفاده از یک نرم‌افزار برای محاسبه قابلیت اطمینان، محاسبه دسترس‌پذیری، محاسبه ایمنی
تکالیف پیشنهادی	این درس دارای ۱۰ تمرین است که تمامی مباحث درس را می‌پوشاند.
پروژه های پیشنهادی	این درس یک پروژه دارد. هر دانشجو باید در خصوص یک موضوع مرتبط با تحمل‌پذیری اشکال پژوهش نماید.
کتاب (های) مرجع	[1] Elena Dubrova, “Fault Tolerant Design: An Introduction", Department of Micro-electronics and Information Technology, Royal Institute of 'Technology, Stockholm, Sweden, 2008. [2] B. W. Johnson. “Design and analysis of Fault tolerant Systems. Addison Wesley, 1989.
سایر مراجع	

طراحی و ارزیابی سیستم‌های بی‌درنگ نهفته

نام درس به فارسی	طراحی و ارزیابی سیستم‌های بی‌درنگ نهفته		
نام درس به انگلیسی	Design and Analysis of Real-Time Embedded Systems		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها	گذراندن درس‌های مرتبط با سیستم‌های نهفته،درسطح کارشناسی می‌تواند مفید باشد اما ضروری نیست.		
مطالب پیش نیاز	آشنایی با موضوعات درس‌های معماری کامپیوتر، ریزپردازنده، سیستم‌های عامل، زبان‌های برنامه-نویسی و ریاضیات مهندسی در دوره کارشناسی		
اهداف درس	آشنایی عمیق دانشجویان تحصیلات تکمیلی با اهمیت سیستم‌های نهفته بی‌درنگ، پیچیدگی‌ها و ملاحظات ویژه در مدلسازی، طراحی و ارزیابی این سیستم‌ها.		
نتایج درس	در پایان این درس دانشجویان می‌بایست درک عملیاتی نسبت به موضوعات درس یافته باشند و توانایی قابل ملاحظه‌ای در خصوص مدلسازی، طراحی و ارزیابی سیستم‌های نهفته بی‌درنگ در دنیای واقعی به دست آورده باشند. علاوه بر این، این درس باید به گونه‌ای تنظیم شود که مهارت دانشجویان در زمینه پژوهش و نگرش منتقدانه را نیز تقویت نماید.		
فهرست مباحث	۱.مقدمه تعریف و اهمیت سیستم‌های بی‌درنگ نهفته ۲.مدلسازی سیستم‌های بی‌درنگ نهفته ۳.زمان‌بندی کارهای ۴.مدیریت منابع ۵.مدیریت حافظه در سیستم‌های نهفته بی‌درنگ ۶.مدیریت توان مصرفی در حرارت ۷.طراحی سیستم‌های نهفته چندتراشه‌ای ۸.مدلسازی و تحلیل کارایی و قابلیت اتکا ۹.سیستم‌های نهفته بی‌درنگ توزیع شده ۱۰.تحلیل و ارزیابی سیستم‌های نهفته بی‌درنگ ۱۱.سیستم‌های سایبر فیزیکال ۱۲.بهینه‌سازی سیستم‌های نهفته بی‌درنگ		
نرم افزارهای مورد نیاز	نرم‌افزارها و ابزارهای مدل‌سازی، ارزیابی، تخمین کارایی، تخمین با اندازه‌گیری توان مصرفی در سیستم‌های نهفته‌ی بی‌درنگ		
کتاب (های) مرجع	[1] H. Kopetz, Real-Time Systems: Design Principles for Distributed Embedded Applications, Springer, 2011. [2] A. M. K. Cheng, Real-Time Systems: Scheduling, Analysis and Verification, John Wiley & Sons, 2002		
سایر مراجع	مقالات علمی ژورنال‌های و کنفرانس‌های معتبر		

معماری سامانه‌های ذخیره سازی داده

نام درس به فارسی	معماری سامانه‌های ذخیره سازی داده		
نام درس به انگلیسی	Architecture of Data Storage Systems		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	• معرفی و لزوم استفاده از سامانه‌های ذخیره‌سازی • معماری روش ذخیره‌سازی مبتنی بر سامانه ذخیره‌ساز داده • معماری و پیکربندی ورودی و خروجی در زیرسامانه دیسک • معیارهای کیفی و کمی در سامانه‌های ذخیره‌سازی داده • معرفی پیکربندی های RAID1, RAID10, RADID5, RAID6 • روند جریان داده در سامانه‌های ذخیره‌ساز داده • حافظه نهان در سامانه‌های ذخیره‌ساز داده • بررسی معماری‌های متداول سامانه‌های ذخیره‌ساز داده (IBM, HP, EMC)		
نتایج درس			
فهرست مباحث	۱.معرفی و لزوم استفاده از سامانه‌های ذخیره‌سازی ●تاریخچه‌ی روشهای ذخیره‌سازی داده ●مقایسه کارآیی دیسک‌ها و پردازنده‌ها ●بررسی قانون amdhal در سامانه‌های ذخیره‌ساز ●معماری روش ذخیره‌سازی مبتنی بر کارگزار ۲.معماری روش ذخیره‌سازی مبتنی بر سامانه ذخیره‌ساز داده ۳.معماری و پیکربندی ورودی و خروجی در زیرسامانه دیسک ۴.معیارهای کیفی و کمی در سامانه‌های ذخیره‌سازی داده ●پهنای باند، زمان پاسخ، دسترس پذیری، قابلیت سرویس و قابلیت توسعه‌پذیری ۵.انواع پیکربندی دیسک‌ها در سامانه‌های ذخیره‌سازی داده ●RAID1, RAID10, RADID5, RAID6 ●بررسی کارآیی خواندن، کارآیی نوشتن و دسترس‌پذیری ۶.طراحی یک سامانه پیشرفته ذخیره‌ساز داده ●طراحی منطق پسین ●طراحی منطق پیشین ●طراحی سامانه حافظه ۷.روند جریان داده در سامانه‌های ذخیره‌ساز داده ●خواندن و نوشتن و گپی داده		

	۸.بررسی ویژگی‌های پیشرفته سامانه‌های ذخیره‌سازی داده • Remote Mirroring • Instant Copies • Data Migration • LUN Masking ۹.حافظه نهان در سامانه‌های ذخیره‌ساز داده • بررسی ساختار حافظه نهان در سامانه‌های ذخیره‌ساز داده • مقایسه ساختار حافظه نهان در سامانه‌های ذخیره‌ساز داده یا ساختار حافظه نهان در ریزپردازنده‌ها • الگوریتم‌های حافظه نهان در سامانه‌های ذخیره‌ساز داده ۱۰.بررسی معماری‌های متداول سامانه‌های ذخیره‌ساز داده (IBM, HP, EMC) ۱۱.تکنیک‌های ورودی-خروجی در سامانه‌های ذخیره‌ساز داده ۱۲.طراحی و معماری دیسک‌های نیمه‌هادی(Solid-State Disk Drivers) • تکنولوژی‌های ذخیره‌سازی نوین مبتنی بر حافظه‌های ماندگار • معماری دیسک‌های نیمه هادی • معماری لایه‌ی انتقال دیسک نیمه‌هادی(Solid-State Disk Device) • الگوریتمهای Wear Leveling در دیسکهای نیمه‌هادی • روش‌های افزایش طول عمر دیسک نیمه هادی • روش‌های زمان‌بندی ورودی/خروجی در دیسک‌های نیمه‌هادی
کتاب (های) مرجع	[1] U. Troppens, R. Erkens, W. Mucller-Fricdt, and R. Wolafka، Storage Networks Explained: Basics and Application of Fibre Channel SAN, NAS, iSCSI,InfiniBand and FCoE.2nd Edition, John Wiley & Sons Inc., 2009. [2] Storage Technologies and Sy5tcms, IBM Journal of Research & Development, Special Issue. November 2008, [3] R. Barker and P. Massigalia, Storage Area Networks Essentials. John Wiely & Sons Inc, 2002. [4] J. Tate, F. Lucchese, and R. Moore, Introduction to Storage Area Networks, IBM Redbooks(eBook), July 2006. [5] John L. Hennessy and David A. Patterson, Computer Architecutre: A Quantitative Apporeach, Third Edition, Morgan Kaufmann Publication, May 2002 [6] John William Toigo, The Holy Grail of Data Storage Management. Prentice-Hall, 2000. [7] G. Somasundaram and A. Shrivastava, Information Storage and Management, Wiley Publishing Inc., EMC Education Services 2009.
سایر مراجع	

سیستم عامل پیشرفته

نام درس به فارسی	سیستم عامل پیشرفته		
نام درس به انگلیسی	Advanced Operating Systems		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز	مطالب درس سیستم‌های عامل کارشناسی		
اهداف درس	در این درس مطالب پیشرفته در زمینه سیستم‌های عامل و پژوهشهای مرتبط بحث می‌شوند. مطالب مطروحه شامل سیستم‌های توزیع شده، شبکه‌سازی، قابلیت اتکا، امنیت، حفاظت و سیستم‌های نهفته خواهد شد.		
نتایج درس			
فهرست مباحث	1.Challenges in the New OS Research a.Dependability، Security, Configuration, Extension, and Multiprocessors 2.Designing OS for new Computer Architectures (Multi-core as networked distributed systems) 3.OS Architecture for Reliability and Security 4.Virtualization a.Isolation b.Hardware-rooted Security Problems c.Nested Virtualization 5.OS Performance Improvement a.Microkernel/Multikernel/Linux for Manycores 6.Architecture for Massively Parallel Data Access 7.OS-level Management of GPUs for Computation Speedup 8.Resource Sharing in Cloud/Large Clusters/Data Centers 9.Network Operating Systems 10.Extra-Large File Systems 11.Resource Efficient OS Design (Energy Management)		
نرم افزارهای مورد نیاز	محیط کار با برنامه‌های MPI, OpenMP, and Cuda		
تکالیف پیشنهادی	هشت تکلیف یک هفته در میان دستی و کامپیوتری		
پروژه های پیشنهادی	سه پروژه بر روی سه قالب برنامه نویسی موازی مطرح شونده		
کتاب (های) مرجع	[1] A. Silberschatz, P.B، Galvin, and G. Gange, Operating System Concepts.9ه Edition, John Wiley & Sons, 2013 (Chapters 14-19) [2] Selected papers from HotOS, SOSP, and some USENIX conferences		
سایر مراجع	Proceedings of related conferences and ACM/IEEE journals.		

رمزنگاری کاربردی

نام درس به فارسی	رمزنگاری کاربردی		
نام درس به انگلیسی	Applied Cryptography		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	هدف درس ارائه مفاهیم اولیه‌ی و اصول رمزنگاری مدرن از دیدگاه کاربردی است. در این درس، چگونگی تعریف امنیت دز الگوریتم‌ها و پروتکل‌های رمزنگاری مشخص می‌شود. و بیان می‌شود که تعریف فرمال امنیت اولین قدم برای طراحی هر پروتکل رمزنگاری است. تأکید این درس بر چگونگی استفاده از سازوکارهای رمزنگاری در سیستم‌های امنیتی است. همچنین، امکان وقوع آسیب‌پذیری در سیستم‌های امنیتی به خاطر استفاده اشتباه از ساز و کارهای رمزنگاری مورد بررسی قرار می‌گیرد.		
نتایج درس			
فهرست مباحث	۱.مدلهای امنیت ●رمزنگاری بدون شرط ●امنیت پیچیدگی (Complexity theory) ●امنیت اثبات پذیر ●امنیت محاسباتی ●امنیت اقتضائی ۲.تعریف فرمال رمزنگاری ۳.ساختارهای پایه ●توابع یکطرفه ●توابع یکطرفه دریچه‌دار ●مولد شبه تصادفی ●توابع شبه تصادفی ●جایگشت‌های تصادفی ۴.توابع رمزنگاری ●رمزنگاری متقارن : رمز قالبی و رمز دنباله‌ای ●رمزنگاری کلید عمومی : رمزگذاری الجمال، تبادل کلید دیفی-هلمن ●محل حملات : حمله متن رمزی انتخابی، حمله متن اصلی انتخابی ۵.جامعیت داده ●توابع چکیده‌ساز ●کدلهای تصدیق اصالت پیام (MAC, HMAC)		

	●امضای دیجیتال ۶.مفاهیم جدید ۷.اثبات‌های هیچ‌دانش ●رمزنگاری همریخت ●رمزنگاری مبتنی بر ویژگی (Attribute-based) ●بازیابی محرمانه اطلاعات (Private Information Retrieval) ۸.رمزنگاری مبتنی بر pairing ●رمزنگاری کوانتومی ●انتقال فراموشکارانه ۹.تسهیم راز ۱۰.محاسبات چندطرفه‌ی امن ۱۱.رأی گیری الکترونیکی
کتاب (های) مرجع	[1] Jonathan Katz, Yehuda Lindcll. “Introduction to Modem Cryptography" (Chapman & Hall/Crc cryptography and Network Security Series), Chapm & Hall/CRC, 2007.
سایر مراجع	[1] Alfred J. Menezes, Paul C. Oorschot, and Scott A. Vanstone, Handbook of applied cryptography, CRC Press, 2010 [2] Oded Goldreich. “Foundations of Cryptography; Volume 2, Basic Application", Vol. 2, Cambridge university press, 2009.

امنیت شبکه پیشرفته

نام درس به فارسی	امنیت شبکه پیشرفته		
نام درس به انگلیسی	Advanced Network Security		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	این درس مباحث پیشرفته در امنیت شبکه و حملات موجود در این حوزه را مطرح می کند. در این درس با بررسی مقالات علمی مختلف موجود در شبکه‌های کامپیوتری معرفی می گردد و راه‌کارهای دفاعی مثل فایروال‌ها، سیستم‌های تشخیص نفوذ، تله عسل‌ها برای مقابله با این حملات بیان می‌شود. تهدیدات و حملاتی مثل DoS، کرمها/بدافزارها، بات‌نت‌ها، حملات phishing نیز در این درس بررسی می‌شود. همچنین پروتکلهای مورد استفاده برای تامین امنیت در فضای تبادل اطلاعات و پروتکل‌های گمنامی معرفی می‌شود.		
نتایج درس			
فهرست مباحث	۱.حملات و تهدیدات •DoS: تشریح حمله و راه‌کارهای مقابله Anomaly Filtering، Pushback، Client Puzzle •Worms/Malware: الگوریتمهای پخش، راهکارهای مقابله، آسیب-پذیری‌ها •Botnets: چوپان بات، روشهای کنترل شبکه بات و تشخیص آن •Adware Spyware، Keyloggers ، Browser Hijackers •Phsihing : تشریح حمله و راه‌کارهای مقابله ۲.فایروال‌ها : محل قرارگیری در توپولوژی شبکه، DMZ، Stateful/Stateless ۳.سیستم‌های تشخیص نفوذ، محل قرارگیری در توپولوژی شبکه، false positive/negative •NIDS/HIDS •Hybrid NIDS and HIDS •Correlation Engine ۴.تله عسل : طراحی و معماری تله عسل، حمله به تله عسل‌ها ۵.تحلیل ترافیک عادی و رمز شده ۶.گمنامی در شبکه •شبکه‌های Mixnet •Onion Routing و شبکه گمنامی Tor ۷.پروتکل‌های امن در شبکه‌های کامپیوتری		

	●رای‌گیری الکترونیکی ○معرفی مفاهیم و ویژگیهای سیستم‌های رأی‌گیری الکترونیکی ○گمنانی در رأی گیری و شبکه‌های Mixnet ●پرداخت الکترونیکی ○معرفی مفاهیم، ویژگیها و انواع روشهای پرداخت الکترونیکی ۸.امنیت مسیریابی : امنیت AS ها، امنیت پروتکل BGP، Prefix Hijacking و S-BGP ۹.Network Forensics ●فیلترهای بلوم ۱۰.امنیت شبکه‌های بی‌سیم WPA/WEP ۱۱.امنیت VoIP
کتاب (های) مرجع	[1] S.M. Bellovin. ''Security Problems in the TCP/IP Protocol Suite." Computer [2] Communication Review, Vol. 19TXo.ة pp. 32*48, 1989. [3] Hervc Debar. "An Introduction t0 Intrusion-Detection Systems." Proceedings of Conncct'2000, Qatar, 2000. [4] A. Kuzmanovic, E. Knightly. "Low-Rate TCP-Targeted Denial of Service Attacks (I'he Shrew vs. the Mice and Elephants)." In Proceedings of ACM SIGCOMM 2003. Germany, 2003. [5] s. Singh. c. Estan, G. Varghesc, s. Savage. "Automated Worm Fingerprinting." Proceedings of ١٦أ ACM'/USENIX Symposium on Operating System Design and Implementation, San Francisco, 2004.
سایر مراجع	

توسعه امن نرم افزار

نام درس به فارسی	توسعه امن نرم افزار		
نام درس به انگلیسی	Secure Software Development		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
اهداف درس	با توجه به اینکه بسیاری از مشکلات امنیتی نرم‌افزارهای تولیدی به عدم توجه به مساله امنیت در فرآیند تولید نرم افزار برمی‌گردد، در مباحث این درس به طور ویژه، به مسائل امنیتی و توصیه‌های امنیتی که در مراحل تولید یک نرم افزار (در مراحل تحلیل نیاز، تدوین معماری، طراحی، پیاده‌سازی و آزمون آن) در جهت حصول یک نسخه امن نرم افزاری مطرح است، پرداخته می‌شود. دانشجویان می‌بایست با انواع آسیب پذیریها و مشکلات امنیتی حاصل از برنامه‌نویسی نادرست آشنا گردند و نکات، روش‌ها و تکنیک‌های مختلف در تولید یک برنامه امن به آنها معرفی شود.		
نتایج درس			
فهرست مباحث	۱.امنیت نرم افزار ●تهدیدات نرم افزاری ●منابع ناامنی نرم افزاری ●مدیریت توسعه امن نرم افزاری ۲.تحلیل نیازمندیهای امنیتی نرم افزار ●موارد سوء استفاده و سوء کاربرد (Misuse and Abuse Cases) ●مدلهای فرآیندی امنیت محور ●استخراج نیازمندیهای امنیتی ●اولویت دهی به نیازمندیهای امنیتی ۳.معماری و طراحی امن نرم افزار ●تحلیل ریسک معمارانه ●اصول و راهنماهای امنیتی و الگوهای حمله در تدوین معماری و طراحی نرم افزار ۴.ملاحظات امنیتی در پیاده‌سازی و آزمون نرم افزار ●تحلیل امنیتی کد ●آزمون امنیتی نرم افزار ۵.مدیریت تولید نمر افزار امن ●امنیت، پیچیدگی و کارآیی ●امنیت و مدیریت پروژه ۶.مقدمه‌ای بر برنامه سازی امن ●اهمیت کدنویسی امن ●چرایی خطاهای امنیتی در کد نویسی		

	●انواع آسیب پذیریها ۷.اصول برنامه‌نویسی امن ●کنترل ورودی ●حداقل دسترسی ●دفاع چندلایه ●طراحی باز (عدم برقراری امنیت از طریق پنهان کاری) ۸.آسیب پذیریهای متداول ●انواع تزریق کد ●اسکریپت نویسی بین سایتی و جعل درخواست بین سایتی ●احراز هویت و مدیریت نشست معیوب ●مجاز شماری و کنترل دسترسی معیوب ●پیکربندی ناامن ●استفاده نادرست از رمزنگاری (تولید اعداد تصادفی ضعیف، مدیریت کلید ضعیفف استفاده ناردست از سیستم‌های مبتنی بر گذرواژه) ●انواع سرریز بافر ●نشت اطلاعات (عدم حفاظت از اطلاعات حساس مدیریت نامناسب، پیام‌های خطا) ●استفاده ناکافی از مکانیزم‌های غیرخودکارسازی (نظیر CAPTCHA) ۹.چارچوب‌های تحلیل امنیتی نرم افزار ●آزمون‌های نفوذ جعبه سفید، جعبه سیاه و جعبه خاکستری ●فازی سازی (Fuzzing) ۱۰.معرفی چارچوب‌های آزمون (همانند OWASP)
سایر مراجع	[1] Julia H. Allen. Software Security Engineering, A Guide for Project Manners, 1st Edition، Addison-Wesley Professional, 2008. [2] Cary McGraw, Software Security: Building Security ,Addison-Wesley Professional, 2006. [3] J. Viega, M. Messier, Secure Programming Cookbook, O'Reilly, 2005. [4] M. Howard, D. LeBlone, Writing Secure Code, Microsoft, Addison Wesley 2002. [5] J. Viega, G. McGraw, Building Secure Software, Addison Wesley 2002. [6] OWASP Top 10, 2010, http:://owasptop10.googlecode.com/filter/OWASPTop10-2010.pdf [7] The WASC Threat Classification, v2.0, http://files.pbwords.com

پروتکل های امنیتی

نام درس به فارسی	پروتکل های امنیتی		
نام درس به انگلیسی	Security Protocols		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
اهداف درس	درک آسیب پذیهای کلیدی که در پروتکل‌های امنیتی رخ می‌دهد و راه‌هایی برای رفع این آسیب پذیری‌ها از مباحث اصلی این درس به شمار می‌روند. تکنیکهای طراحی پروتکل‌های امنیتی مختلف نظیر SSL، WEP/WPA، IPSec و «Kerberos و همچنین مباحث آسیب پذیریهای اینگونه پروتکل‌ها در این درس مورد توجه قرار می‌گیرند.		
نتایج درس			
فهرست مباحث	۱.پیش نیازهای رمزنگاری ●رمزنگاری کلید متقارن ●رمزنگاری کلید عمومی ●الگوریتم های توابع درهمسازی یکطرف ۲.انواع پروتکل ●پروتکل‌های تصدیق هویت ●پروتکل‌های توزیع کلید ●پروتکل‌های تجارت الکترونیک ۳.مدل کردن پروتکل‌های امنیتی ۴.ویژگیهای امنیتی ●تصدیق هویت ●محرمانگی، تمامیت، دسترسی ●ویژگیهای دیگر ۵.تکینک‌هایی برای تصدیق پروتکل‌های امنیتی، منطق BAN و روش قیاسی inductive ۶.ابزارهایی برای تصدیق اتوماتیک پروتکل‌های امنیتی ۷.رده بندی رخنه ●حملات تکرار ●حملات نشست موازی ●حملات وابسته اجرایی ●حملات نرم افزار ●حمیلات کپسولی کردن ۸.توصیف پروتکل رمزنگاری ●زبان های صوری چند منظوره ●زبان‌های منطقی		

	●زبان‌های عملیاتی ●مدل حساب SPC ۹.توصیف ویژگی امنیتی ●منطق‌های امنیتی ●منطق ADM ●ساختار نحوی ●ساختار معنایی ۱۰.تحلیل پروتکل‌های رمزنگاری ●تحلیل منطقی ●تحلیل جبری مبتنی بر مدل ●تحلیل جبری فرآیند ●تحلیل مبتنی بر نوع ●چارچوب DYMNA ۱۱.پیچیدگی تحلیل پروتکل‌های امنیتی
سایر مراجع	[1] .PRyan, s. Schneider and M. H. Goldsmith: Modelling and Analysts of Security Protocols, Addision-Wesley, 2001 [2] M. Debbabi. Design and Analysis of Security Protocols. Lecture notes. CIISE, Concordia University, 2004. [3] B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, John Wiley and Sons Inc. 1996.

روشهای صوری در امنیت اطلاعات

نام درس به فارسی	روشهای صوری در امنیت اطلاعات		
نام درس به انگلیسی	Formal Methods in Information Security		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها	امنیت پایگاه داده		
مطالب پیش نیاز			
اهداف درس	در این درس روشهای صوری و رمزنگارانه برای مدل نمودن و تحلیل سیستم‌های امنیتی مورد بررسی قرار می‌گیرد. تعیین مسشخصه‌های صوری الزامات امنیتی، تحلیل امنیتی صوری سیستم‌ها و همچنین مبانی تئوری برای توسعه امن نرم افزاری با استفاده از پالایش گام به گام از موضوعات اصلی این درس به شمار می‌روند.		
نتایج درس			
فهرست مباحث	۱.نظریه مجموعه‌ها و منطق ۲.مدلهای کنترل دسترسی ●مدلهای کنترل دسترسی اختیاری و اجباری ●حالت‌های صوری DAC، MAC، RBAC و مدلهای قاعده مند ۳.مدلهای کنترل جریان اطلاعات ●کانالهای ارتباطی (کانالهای آشکار و پنهان) ●جریان اطلاعات در داخل یک برنامه ●رویه تئوری گونه اطلاعات در جریان اطلاعات امن ●مشخصه صوری جریان اطلاعات امن ۴.مقدمه‌ای بر مشخصه پروتکل صوری و تحلیل ●پروتکل‌های رمزنگاری ●مدلهای صوری بجای مدلهای محاسباتی ●مدلهایی برای عناصر رمزنگاری پایه ۵.منطق برای پروتکل‌های امنیتی ●منطق باور، منطق BAN برای تصدیق هویت، منطق دانایی برای پروتکل‌های رمزنگاری ۶.تحلیل خودکاربرای پروتکل‌های امنیتی ●اثبات قضیه ●وارسی مدل ●ابزارهای اثبات قضیه و وارسی مدل		

کتاب (های) مرجع	[1] P. Ryan. Steve Schneider and M. H. Goldsmith; Modeling and Analysis of Security Protocols, Addison-Wesley, 2.000 [2] M. Bishop: "Computer Security", Pearson Education, 2002 [3] C. Boyd, Anish Mathuria, Protocols for Authentication and Key Establishment. Springer, 2003. [4] G. Bella, Formal Verification of Security Protocols, Springer, 2007. [5] A.J. Menezes, P.C van Oorschot, and S. A. Vanstonc, Handbook of Applied Cryptography, CRC Press, 1996 (available online) [6] D. Gollmann, "Computer Security", Willy 2010 [7] J. Viega, G. McGraw, "Building Secure Software", Addison-Wesley, 2011
سایر مراجع	

امنیت و اعتماد سخت‌افزار-رانه

نام درس به فارسی	امنیت و اعتماد سخت‌افزار-رانه		
نام درس به انگلیسی	Hardware-Driven Security and Trust		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	در این درس به معرفی پیشرفتهای اخیر در طراحی و ارزیابی امنیت سخت‌افزار و اعتمادپذیر بودن آن پرداخته می‌شود. در چرخه‌ی عمر سخت‌افزار از طراحی تا تولید و در طول استفاده از آن لازم است تا امنیت سخت‌افزار و اعتماد به آن حفظ شود. لذا به عنوان مثال، در مرحله‌ی طراحی نیازمندیهایی چون غیرقابل دست‌کاری بودن و عدم نشت اطلاعات مطرح شده، و در مرحله‌ی تولید می‌بایست تطابق با طراحی بررسی شود، تا تغییری منجر به یک اسب تروا یا یک درپشتی انجام نشود. در ضمن ترفندهایی برای کشف چنین تهدیداتی لازم است. به علاوه، برای تأمین امنیت و اعتماد در سیستم‌های کامپیوتری نیاز به پشتیبانی توسط سخت‌افزار است. مثلاً در برخی کاربردها نیاز به تولید کلید خصوصی در سخت‌افزار اختصاصی می‌باشد و یا برای مقابله با حفظ مالکیت معنوی برنامه‌ها و اندازه‌گیری میزان استفاده از آنها، این نیاز وجود دارد. تأمین اعتماد برای برخی کاربردها نیز، نیازمند سخت‌افزارهای وارسی کننده است.		
فهرست مباحث	۱.مقدمه‌ای بر رمزنگاری و طراحی و تست VLSI ۲.پردازنده‌های رمزنگاری ۳.محاسبات مورد اعتماد (Trusted Computing) و TPM ها ۴.حملات فیزیکی و مقاومت در برابر دست‌کاری ۵.حمله‌ی کانال جنبی و حمله تزریق عیب ۶.توابع غیرقابل همانندسازی فیزیکی (PUFs) ۷.مولدهای عدد تصادفی مبتنی بر سخت افزار ۸.ته‌نقش نگاری (Watemarking) بلوک‌های IP (Intellectual Property) ۹.طراحی مورد اعتماد در FPGA ها ۱۰.امنیت سیستم‌های نهفته ۱۱.امنیت برچسب‌های RFID ۱۲.کنترل دسترسی و حفظ مالکیت معنوی برنامه با استفاده از سخت افزار (به طور منفعل و فعال) ۱۳.کشف و ایزوله کردن تروجان سخت‌افزاری در بلوک‌های IP و مدارهای مجتمع FIPS-140-2 : استاندارد مازول‌های رمزنگاری		
کتاب (های) مرجع	[1] M. Tehranipoor and C. Wang, Introduction to Hardware Security and Trust, Springer, 2011		
سایر مراجع			

امنیت سیستم‌های نوین ارتباطی

نام درس به فارسی	امنیت سیستم‌های نوین ارتباطی		
نام درس به انگلیسی	Security of Modem Communication Systems		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
اهداف درس	در این درس امنیت سیستم‌های ارتباطی و چگونگی به کارگیری رمزنگاری برای تأمین امنیت در این سیستم‌ها مورد بحث قرار می‌گیرد. بدین منظور جنبه‌های فنی امنیت و نیز کاربردها و مسائل خاص‌شان مطالعه می‌گردند.		
نتایج درس			
فهرست مباحث	۱.تهدیدات و راه‌حل‌ها ●شامل تهدیدات به امینت ارتباطات، تداخل، jamming، تشخیص توسط دشمن، استخراج اطلاعات از روی شکل موج، تصدیق اصالت، صحت، دسترس‌پذیری و مقابله با تهدیدات تشعشعی ۲.امنیت صوت در کاربردهای نظامی ●رمزنگاری آنالوگ برای ارتباطات رادیویی HF برد بلند دریایی، واحد رمزنگاری دیجیتال در عملیات زمینی، مدول رمزنگاری رادیویی ۳.سیستم‌های GSM امن ●معماری پایه GSM، ویژگیهای امنیتی GSM استاندارد، جنبه‌های امینت خاص برای کاربران GSM، مدیریت کلید و ابزارها، عملیات و امنیت GSM ۴.امنیت شبکه‌های رادیویی VHF/UHF خصوصی ●کاربری، ویژگیها، تهدیدات، افدامات مقابله، معماری و طراحی شبکه ارتباطی، اجزاء سخت افزاری، مدیریت کلید، بعضی ویژگیهای امنیتی خاص مانند حذف کلید از دوردست، انسداد از راه دور و ردگیری ساکت ۵.اقدامات حفاظت الکترونیک خیزش فرکانسی EPM، EA و ESM، کاربردهای نظامی، معماری شبکه، مراحل مأموریت، مشخصه‌های فرکانسی، شبکه‌های خیزشی COMSEC و TRANSEC، ابزارها و مدیریت داده‌ها و کلید اجزاء سخت‌افزاری ۶.رمزنگاری لینک، تکنولوژی پایه رمزنگاری لینک، پروسه‌ی رمزنگاری، پارامترهای رمزنگاری، مدیریت شبکه، امنیت لینک نظامی ۷.سیستم‌های امن (شبکه‌های فکسیمیلی امن، امنیت PC، امنیت E-mail، شبکه‌های اجتماعی مجازی امن، انتقال داده‌های نظامی)		
سایر مراجع	**[1]** .R. VSutton, Secure Communications: Applications and Management, John-Wiley *Inc., 2002* [2] D. J. Torrieri, Principle of Secure Communication Systems, Artech House, 1992		

یادگیری ماشین

نام درس به فارسی	یادگیری ماشین		
نام درس به انگلیسی	Machine Learning		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
اهداف درس	یادگیری ماشین بر اکتشاف و تجمیع دانش به صورت خودگردان اشاره دارد. هدف اصلی این درس، فراهم آوردن یک مقدمه جامع بر یادگیری ماشین است. برای این کار رویکردهای اصلی بحث خواهد شد و اصول، تکنیک‌ها و کاربردهای پایه یادگیری ماشین مطرح می‌شوند. این درس ایده‌های پایه و دید لازم را در خصوص یادگیری ماشین مدرن به دانشجویان می‌دهد و تا حدودی نیز به مباحث رسمی مرتبط با یادگیری ماشین می‌پردازد.		
فهرست مباحث	۱.مقدمه ۲.یادگیری درخت بیزی (بزارش بیش از حد روشهای هرس) ۳.یادگیری بیزی ۴.یادگیری بر پایه مثال ۵.ارزیابی فرضیه ۶.الگوریتم انتشار خطا به عقب ۷.ماشین برداز پشتیبان ۸.رگرسیون خطی و لاجیستیک ۹.نظریه یادگیری محاسباتی ۱۰.ترکیب دسته‌بندها ۱۱.مدل اختلاط ۱۲.یادگیری برخط ۱۳.یادگیری نیمه نظارتی ۱۴.یادگیری فعال ۱۵.یادگیری چند برچسبی ۱۶.یادگیری از داده‌های غیرکامل		
نرم افزارهای مورد نیاز	Matlab, SVMLight, Weka		
کتاب (های) مرجع	**[1]** Mehryar Mohri, Afshin Rostamizadeh, and Ainect Talwalkar, Foundations of Machine Learning. MIT Press**, 2012** **[2]** Kevin Murphy, Machine Learning: a Probabilistic Prespective, 2012 [3] Tom M. Mitchell, Machine Learning, McGraw Hill, 1997 [4] Christopher M. Bishop, Pattern Recognition and Machine Learning, Springer 2006		
سایر مراجع			

سیستم های توزیع شده

نام درس به فارسی	سیستم های توزیع شده		
نام درس به انگلیسی	Distributed Systems		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
اهداف درس	هدف از این درس آشنایی دانشجویان با مفاهیم سیستم‌های توزیع شده می‌باشد. در پایان آموزش این درس دانشجو می‌بایست درک خوبی از چالش‌ها و پیچیدگی‌های سیستم‌های توزیع شده و راه‌حل‌های کلی داشته باشد.		
نتایج درس			
فهرست مباحث	۱.مقدمات ۲.تعریف‌ها، اهداف، مفاهیم اساسی، نرم افزار وسخت‌افزار، مدل محاسباتی خادم و مخدوم ۳.ارتباطات ۴.پروتکل‌ها، فراخوانی‌های راه دور، تبادل پیغام و جریان‌ها ۵.پردازش‌ها ۶.ریسمان‌ها، خادم‌هاف مخدوم‌ها و مهاجرت ۷.نام‌گذاری ۸موجودیت‌های نام‌گذاری، محل‌یابی موجودیت‌های متحرک و زباله‌رویی موجودیت‌های بلااستفاده ۹.هنگام سازی ۱۰.همگام سازی زمان، زمان منطقی، الگوریتم‌های انتخابات، مانعه‌الجمعی و تراکنش‌های توزیعی ۱۱.سازگاری و کپی‌سازی ۱۲.مدلهای سازگاری، پروتکل‌های توزیعی، پروتکل‌های سازگاری و نمونه‌های عملی ۱۳.تحمل‌پذیری خطا ۱۴.مفاهیم ارتباطات مطمئن گروهی و نقطه به نقطه و بازسازی ۱۵.امنیت ۱۶.کانالهای امن، کنترل دستیابی، مدیریت امنیت و نمونه‌های عملی ۱۷.مطالعه موردی ۱۸.سیستم‌های توزیعی شیء‌گرا، سیستم‌های توزیعی بر پایه مستندات و سیستم‌های توزیعی فایل‌ها		
کتاب (های) مرجع	[1] Tanenbaum, Andrew **S۶.** and Maarten Van Steen. Distributed Systems, Principles & Paradigms, 2nd Edition, Prentice Hall, 2007. [2] Coulouis, George F., Distributed Systems: Concepts and Design, ***5th*** Edition, Pearson Education, **2012**		
سایر مراجع			

الگوریتم های هوش جمعی

نام درس به فارسی	الگوریتم های هوش جمعی		
نام درس به انگلیسی	Swarm Intelligence Algorithms		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	هدف از این درس یادگیری الگوریتم‌های الهام گرفته از زیست است. در این راستا دو رویکرد مهم شامل اگلوریتم کلونی مورچگان و کلونی زنبورها تشریح می‌شود.		
نتایج درس			
فهرست مباحث	۱.مقدمه ۲.بهینه‌سازی گروه ذرات، بهینه‌سازی استاتیک، بهینه‌سازی دینامیک، بهینه‌سازی چند هدفه ۳.الگوریتم کلونی مورچگان، خوشه‌بندی، بهینه‌سازی استاتیک، بهینه‌سازی دینامیک، بهینه-سازی چندهدفه، ۴.الگوریتم کلونی زنبورها : بهینه‌سازی استاتیک، بهینه‌سازی دینامیک، بهینه‌سازی چندهدفه، ۵.سیستم ایمنی مصنوعی، بهینه‌سازی استاتیک، بهینه‌سازی دینامیک، بهینه‌سازی چندهدفه، تشخیص و نفوذ و ویروس ۶.الگوریتم‌های دیگر مبتنی بر زیست		
کتاب (های) مرجع	[1] Bijaya Ketaya, Panigrahi, Yuhui Shi, Meng-Hiot, Lim , Handbook of Swarm Intelligence Concepts,، Principles and Applications. Springer 2011. [2] Andries P. Enggelbreehl, Computational Intelligence An Introduction. Wiley 2nd edition, 2007 [3] Marco Dorigo, Thomas Stuzle, Ant Colony Optimization, A Bradford book, First Edition, First Printing edition [4] Lendro Numes De Castro, Artifical Immune Systems : A New Computational Intelligence Approach, Springer 2002, edition		
سایر مراجع			

الگوریتم های تقریبی

نام درس به فارسی	الگوریتم های تقریبی		
نام درس به انگلیسی	Approximation Algorithm		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	بسیاری از مسائل بهینه‌سازی در ریاضیات، علوم کامپیوتر و مهندسی NP-سخت هستند و بنابراین به دست آوردن جواب‌های بهینه برای این دسته از مسائل در زمان چندجمله‌ای با فرض $P \neq NP$ امکان پذیر نیست. الگوریتم‌های تقریبی امکان دست‌یابی به جواب‌هایی نزدیک بهینه با ضریب تقریب قابل اثبات را برای این دسته از مسائل فراهم می‌کنند. هدف از این درس، آشنایی دانشجویان با مفاهیم و تکنیک‌های متداول در طراحی الگوریتم‌های تقریبی حول محور مسائل بنیادی در بهینه‌سازی ترکیبیاتی و نی آشنایی با روش‌های اثبات سختی تقریب برای برخی از این مسائل است.		
نتایج درس			
فهرست مباحث	۱.مقدمات مسائل NP، بهینه‌سازی، درجه‌ی تقریب پذیری ۲.روشهای ترکیبیاتی، الگوریتم‌های حریصانه، جست‌وجوی محلی، تکنیک لایه‌بندی، برنامه‌ریزی پویا ۳.روشهای مبتنی بر برنامه‌ریزی خطی، گرد کردن قطعی، گردکردن تصادفی، روش اولیه-دوگان، روش برازش دوگان، برنامه‌ریزی بردازی و نیمه‌معین ۴.مسائل بهینه‌سازی ●مسائل پوششی، پوشش رأسی، پوشش مجموعه‌ای ●مسائل شبکه‌ای درخت‌های اشتاینر، مسیرهای با کم‌ترین اشتراک ●مسائل عددی، کوله‌پشتی، بسته‌بندی ●مسائل گشت‌ها : فروشنده‌ی دوره گرد، فروشنده‌ی دوره‌گرد اقلیدسی ●مسائل برش‌ها : برش بیشینه، k-برش، برش چند مسیره، برش چندگانه ●مسائل صدق پذیری : k-صدق پذیری بیشینه ●مسائل خوشه‌بندی : k-مرکز، k-میانه، مکان‌یابی تسهیلات ●مسائل زمان‌بندی : زمان بندی با پردازنده‌های موازی ۵.سختی تقریب : اثبات‌های اولیه، کاهش با حفظ درجه‌ی تقریب		
کتاب (های) مرجع	[1] D. Williamson and D. Shmoya, The Design of Approximation Algorithms, Cambridge University Press, 2011. [2] V. Vazirani, Approximation Algorithms, Springer-Verlag, 2001.		
سایر مراجع			

توصیف و وارسی برنامه‌ها

نام درس به فارسی	توصیف و وارسی برنامه‌ها		
نام درس به انگلیسی	Program specification and Verification		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	این درس برای دانشجویان کارشناسی ارشد و دکتری ارائه می گردد و هدف از آن پرداختن به روش‌های صوری برای توصیف و وارسی سیستم‌ها است. در این درس ابزارهای لازم برای به کارگیری این روش‌ها معرفی و در مورد رابطه بین توصیف صوری و پیاده‌سازی به طور اختصار بحث می گردد.		
نتایج درس			
فهرست مباحث	۱.مقدمه‌ای بر توصیف سیستم‌ها ●چرا توصیف صوری؟ ●توصیف صوری و مهندسی نرم‌افزار ●تولید برنامه از توصیف (پالایش) ۲.جبر گزاره‌ها، جبر مستندات ۳.تئوری مجموعه‌ها و زبان Z ●تساوی ●انواع داده‌گونه‌ها، مجموعه‌ها و عملیات روی آنها ●تعاریف ●روابط و عملیات روی آنها ۴.واحدهای ساختاری توصیف ●شما (schema) و نحوه مدل کردن سیستم ●استفاده از شما به عنوان اعلان، نوع و همبند ●شمای ژنریک ●نحوه بیان اصول (Axiomatic Description) ۵.جبر شماها (Schema Calculus) ●تغییر متغیر (Renaming and Decoration) ●ترکیب شماها با استفاده از عملگرهای منطقی(و، یا، نقیض)، صورهای وجودی و عام، شمول ۶.ابزارگان ریاضی Z ●ردیف‌ها و Bagها و عملیات روی آنها ●نوع آزاد (Free Type)		

	۷.توصیف با استفاده از ارتقاأ (Promotion) ۸.امکان پذیری توصیف و محاسبه پیش‌شرط‌ها (Precondition) ۹.وارسی (Verification) ●اصول تئوری مجموعه‌ها ●قوانین استنتاج ●قضیه حالت اولیه سیستم ●ساده‌سازی پیش‌شرطها ●اثبات خصوصیات توصیف ۱۰.تولید برنامه از توصیف صوری Z، استفاده از پالایش (Refinement) ●پالایش ساختارهای داده‌ای ●پالایش عملیات
پروژه های پیشنهادی	●دانشجویان به گروه‌های ۲ یا ۳ نفری تقسیم شده و هر گروه سه صورت برنامه در اندازه‌های کوچک، متوسط و بزرگ را پیشنهاد می‌نماید. پس از تصویب برنامه‌ها، هر گروه تمرینات (حداقل ۳ تمرین) را در طول ترم بر اساس مسائل پیشنهادی خود پاسخ خواهند دارد. ●برنامه بزرگ صورت پروژه هر گروه را مشخص می کند که یک ماه پس از پایان امتحانات فرصت دارند تا توصیف صوری کامل پروژه را تحویل دهند. ●دانشجویان باید با استفاده از نرم‌افزارهای کنترل کننده جامعیت و عدم تناقض و اثبات قضیه خصوصیات توصیف صوری خود را مورد ارزیابی قرار دهند. ●دانشجویان به طور اختیاری سمیناری را در ارتباط با مطالب درس پس از گرفتن تایید ارائه می‌نمایند.
کتاب (های) مرجع	[1] J. Woodcock, J. Davies. Using Z Specifications, Refinement and Proof, Prcnticc IHalHurope, 1996. [2] D. Gries, F.B. Schneider, A Logical Approach to Discrete Math, Springer Verlag, 1993 [3] C. Morgan, Programming from Specifications, Prentice Hall, 1990
سایر مراجع	

پنهان‌سازی اطلاعات

نام درس به فارسی	پنهان‌سازی اطلاعات		
نام درس به انگلیسی	Information Hiding		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	آشنایی با مبانی، اصول، تکنیک‌ها و کاربردهای • نشانه‌گذاری (watermarking) • تشخیص، نشانه، پوشینه‌نگاری (Steganography) • پوشینه‌کاوی (Steg-analysis) در رسانه‌های مختلف		
نتایج درس			
فهرست مباحث	۱.مقدمه، معرفی زمینه پنهان‌سازی اطلاعات، نشانه‌گذاری و پوشینه‌کاری، تاریخچه، پنهان‌سازی اطلاعات ۲.کاربردها و خصوصیات سیستم‌های پنهان‌سازی اطلاعات، نشانه‌گذاری، پوشینه‌نگاری و پوشینه‌کاوی ۳.اصول و روش‌های نشانه‌گذاری : مدلهای نشانه‌گذاری، نشانه‌گذاری با اطلاعات جنبی، تحلیل خطاها، استفاده از مدل‌های ادراکی، نشانه‌گذاری مقاوم، امنیت نشانه، قالب بیت‌های نشانه (طیف گسترده، کدهای تصحیح خطا، طرح نشانه فرکانسی پایین)، انتخاب جایگاه نشانه در پوشش (الگوریتم patchwork، بازیابی عمومی نشانه)، انتخاب فضای کاری نشانه‌گذاری (فضای پیکسل‌ها، تبدیل فوریه گسسته، تبدیل کسینوسی گسسته، تبدیل موجک)، نحوه درج نشانه در پوشش (مدولاسیون فاز، مدولاسیون دامنه، قرار دادن نشانه بر اساس کواتیزاسیون)، آشکارسازهای بیشینه درست‌نمایی. ۴.اصول پوشینه‌نگاری ارتباط بر مبنای پوشینه‌نگاری، تئوری اطلاعات در پوشینه‌نگار، روش‌های عملی پوشینه-نگاری، چارچوب‌های ممکن برای ارتباطات سری، امنیت سیستم‌های پوشینه‌نگاری، پنهان‌سازی اطلاعات در داده‌های دارای نویز، الگوریتم‌های تطبیقی و غیر تطبیقی ۵.روش‌های پوشینه‌نگاری : تعاریف اولیه، سیستم‌های جایگزینی در پیکسل‌ها، روش‌های حوزه تبدیل، طیف گسترده و پنهان‌سازی اطلاعات، پوشینه‌نگاری آماری، روش‌های اعوجاج، روشهای تولید پوشش (cover)، پوشینه‌نگاری صورت ۶.پوشینه‌کاوی : صورت‌بندی رسمی مسأله پوشینه‌کاوی، آشکارسازی پوشینه‌نگاری(آشکارسازی کور، آشکارسازی هدفمند)، پوشینه‌کاوی فورنژیک، تاثیر پوشش در پوشینه کاوی، روشهای مهم موجود، حمله هیستوگرام، تحلیل جفت نمونه‌ها، استفاده از معیارهای کیفیت تصویر، استفاده از آمارگان درجه بالای تصویر، استفاده از حوزه موجک، استفاده ازماتریسهای رخداد توأم و مدلهای مارکوف، کالیبراسیون		
کتاب (های) مرجع	[1] I.J. Cox, M. A. Miller, J. A. Bloom, J. Fridrich, and T. Kalkar, Digital Watermarking and Steganography, Second Edition, Elsevier, 2008 [2] K S. katzcnbeisser, F. A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, 2000 [3] R. Bohme, Advanced Statistical Steganalysis, Springer, 2010.		

شبکه‌های دینامیکی پیچیده

نام درس به فارسی	شبکه‌های دینامیکی پیچیده		
نام درس به انگلیسی	Complex Data Networks		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	• آشنایی با مسائل و مشکلات و راه‌حل‌ها و مزایای شبکه‌های دینامیکی • آشنایی با شاخص‌های شبکه در قالب مدلسازی گراف • خوشبه بندی، برچسب زنی و همکاری درشبکه‌ها		
نتایج درس			
فهرست مباحث	۱.مقدمه‌ای بر تئوری شبکه‌های پیچیده ۲.اندازه‌گیری شبکه ۳.شاخص‌های اندازه‌گیری شبکه‌ها ●کوتاهترین مسیرها ●ضریب کلاسترینگ ●پل ●ایجاد یال ●همسان بودن ۴.تحلیل طیف شبکه ۵.ساختار motif ها در شبکه‌ها ۶.اندازه‌گیری مرکزیت در شبکه‌ها ۷.ساختار سلسله مراتبی و خوشه‌بندی شبکه‌ها ۸.گشت‌های تصادفی و شبکه‌های تصادفی ۹.شبکه‌های small-world ۱۰.شبکه‌های مقیاس آزاد ۱۱.تکامل شبکه‌ها ۱۲.جستجو در شبکه‌ها ۱۳.شبکه‌های علامت‌دار ۱۴.هم‌ارزی اجتماعی ۱۵.دینامیک اجتماعی ۱۶.همکاری در شبکه‌ها ۱۷.اقوام وقابلیت اطمینان در شبکه‌ها ۱۸.رفتار آبشاری در شبکه‌ها		

	۱۹.انتشار اپیدمی در شبکه‌ها ۲۰.مقدمه‌ای بر سیستمهای دینامیکی ۲۱.سنکرونی و همگامی در شبکه‌ها
نرم افزارهای مورد نیاز	شبیه‌سازهای کامپیوتری شبکه از قبیل ns-2/3 و Opnet
تکالیف پیشنهادی	چندین تکلیف در طول ترم برای فهم بهتر مفاهیم و الگوریتمهای ارائه شده در درسی و یک پروژه نهایی
کتاب (های) مرجع	[1] Newman, M., A.-L, Barabasi, etal.(2006), The structure and dynamics of networks, Princeton University Press. [2] Osipov, G. V.J ،Kurths,et. Al. (2007), Synchronization in Oscillatory Networks, springer [3] Albert, R. and A.-L. Barabasi (2002). "Statistical mechanics of complex networks." Reviews of Modern Physics 74(l): 47-97 [4] Boccaletti, S. V. latora, et al (2006), "Complex networks:structure and dynamics.", Physics Reports 424:175-308 [5] Newman, M. E. J. (2003), "The structure and function of complex networks" SIAM Review 45(2):167-256 [6] J. Cox, M. A. Miller, J. A. Bloom, J. Fridrich, and T. Kalkar, Digital Watermarking and Steganography, Second Edition, Elsevier, 2008 [7] K S. katzcnbeisser, F. A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, 2000 [8] R. Bohme, Advanced Statistical Steganalysis, Springer, 2010.

وارسی و راستی آزمایی پروتکل های امنیتی

نام درس به فارسی	وارسی و راستی آزمایی پروتکل های امنیتی		
نام درس به انگلیسی	Verification of Security Protocols		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها	شبکه‌های کامپیوتری، پروتکل‌های امنیتی		
مطالب پیش نیاز			
اهداف درس	• راستی آزمایی ایستای پروتکل‌های امنیتی • آشنایی با ابزارهای تحلیل و وارسی • بررسی پروتکل‌ها از جنبه ویژگیهایی نظیر احراز اصالت و گمنامی		
نتایج درس			
فهرست مباحث	• تعریف پروتکل‌های ارتباطی، تعریف پروتکل‌های امنیتی، تعریف اهداف امنیتی، تعریف مفاهیم پایه امنیتی، • تبیین اهداف تحلیل پروتکل های امنیتی، نقد روش های سنتی (غیر صوری) شبیه سازی و آزمون برنامه، • معرفی چند پروتکل امنیتی، معرفی آسیب پذیری های پروتکل‌های امنیتی، حمله به پروتکل‌های امنیتی، روش های صوری در تحلیل پروتکل‌های امنیتی، چالش های روشهای صوری • معرفی روش های تحلیل پروتکل، معرفی نقاط قوت و ضعف روش های تحلیل پروتکل‌های ایمنی • معرفی پروتکل های احراز اصالت و تبادل کلید، انعقاد قرارداد، جا به جایی پول، رای گیری، • معرفی مدل عمومی مهاجم (Dolev-Yao) • معرفی pi-calculus در بیان پروتکل‌های امنیتی، معرفی spi-calculus : توسعه pi-calculus با دستوراترمزنگاری • بیان پروتکل امنیتی با زبان spi-calculus، تعریف ویژگی محرمانگی(secrecy) : جریان اطلاعات مستقیم (direct information flow)،تعریف حملات داخلی و خارجی، • آشنایی با ابزار اثبات قضیه ProVerif : ابزار وارسی پروتکل‌های امنیتی • تعریف ویژگی احراز اصالت (Authenticity)، تعریف مفاهیم Timeliness و injective در احراز اصالت • استفاده از سیستم نوع (type system) در اثبات محرمانگی قوی (robust Secrecy)، اثبات خوش نوعی (well-typed)، استفاده از برچسب گذاری (tagging)، تحلیل آسیب پذیری در sign-then-encrypt و encrypt-then-sign، نشان دادن صحت و ناکامل بودن type theory • ProVerif وارسی احراز اصالت با استفاده از ابزار		

	• بیان دیگری از ویژگی محرمانگی (secrecy) : جریان اطلاعات ضمنی (implicit information flow) ، ویژگی non-interference or strong secrecy: (پیش‌گیری از هر دو جریان اطلاعات مستقیم و ضمنی)، • تخطی از ویژگی non-interference، رمزنگاری نامعین (Non-deterministic Encryption)، • آزمون این همانی (Equivalence)، سیستم نوع برای non-interference، • وارسی پروتکل رای گیری الکترونیکی با استفاده از ابزار ProVerif • وارسی پروتکل پیام الکترونیکی تایید شده (certified E-mail) با استفاده از ابزار ProVerif • گمنامی/ بخش اول : تعریف گمنامی، بررسی گمنامی در پروتکل dining cryptographers، ویژگی‌های گمنامی، گمنامی قوی • گمنامی/ بخش دوم : سنجش کمی گمنامی، وارسی پروتکل Crowds و Probable Innocence • گمنامی/ بخش سوم : وارسی پروتکل Mix، معرفی رویکرد بررسی مدل (Model Checking)، بیان ویژگی‌های امنیتی به زبان CTL و CTL احتمالاتی (PCTL)، معرفی ابزار بررسی مدل احتمالاتی PRISM، بررسی مدل پروتکل MIX
نرم افزارهای مورد نیاز	
تکالیف پیشنهادی	یک پروژه عملی شامل وارسی یک پروتکل امنیتی با ابزارهای گفته شده در کلاس
پروژه های پیشنهادی	یک پروژه پژوهشی شامل وارسی امنیتی یک پروتکل جدید
نمره دهی پیشنهادی (درصد نمره دهی پیشنهادی)	امتحان (۵۰٪) تکلیف (۲۰٪) پروژه (۳۰٪)
کتاب (های) مرجع	[1] Bella G., Formal Correctness of Security Protocols, Springer, 2007 [2] Baier C. and J-P. Katoen, Principles of Model Checking, MIT Press, 2008. [3] Clarke E.M., Henzinger T.A. and Veith H. (Editors), Handbook of Model Checking, Springer, 2015 [4] M. Abadi, B. Blanchet Computer-assisted Verification for Certified E-mail. In Science of Computer Programming, 58(1-2):3-27, 2005 [5] S. Kremer, M. Ryan. Analysis of an Electronic Voting Protocol in the Applied Pi Calculus. In 14th European Symposium on Programming (ESOP), pp. 186-200, 2005
سایر مراجع	[1] B. Blanchet, M. Abadi, C. Fournet. Automated Verification of Selected Equivalences for Security Protocols. In 20th IEEE Symposium on Logic in Computer Science (LICS), pp. 331-340, 2005 [2] Sassone V, ElSalamouny E, Hamadou S. Trust in Crowds: probabilistic behaviour in anonymity protocols. In Trustworthly Global Computing 2010 Jan 1 (pp. 88-102). Springer Berlin Heidelberg

حقوق رایانه و ارتباطات جدید

نام درس به فارسی	حقوق رایانه و ارتباطات جدید		
نام درس به انگلیسی	Computer and Communications Law		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۲ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	• آشنایی با مبانی و نظریه‌های مختلف در مورد حقوق پدیدآوردندگان نرم‌افزارهای رایانه‌ای • بررسی قانون حمایت از پدیدآورندگان نرم‌افزارهای رایانه‌ای • مقررات بین‌المللی حمایت از نرم‌افزارهای کامپیوتری • حقوق اینترنت و فن‌آوری اطلاعات		
نتایج درس			
فهرست مباحث	۱.مبانی و نظریه‌های مختلف در مورد نظام حمایت از حقوق پدیدآوردندگان نرم‌افزارهای رایانه-ای •شرایط حقوق مالکیت ادبی، هنری، نظام حق اختراع و نظام خاص ۲.بررسی قانون حمایت از پدیدآورندگان نرم‌افزارهای رایانه‌ای •شرایط حمایت،نرم‌افزار رایانه‌ای و اختراع، •حقوق مادی و معنوی، مدت حمایت، •نمرافزارهای ناشی از رایانه‌ای، ضمانت اجرای مدنی و کیفری ۲.مقررات بین‌المللی حمایت از نرم‌افزارهای کامپیوتری ۳.حقوق اینترنت ۴.حقوق فن‌آوری اطلاعات		
کتاب (های) مرجع	[۱] کاتوزیان ناصر، حقوق مدنی : قواعد عمومی قراردادها، جلد اول تا پنجم، شرکت انتشار با همکاری شرکت بهمن برنا، انتشارات مدرس، ۱۳۷۶ [۲] آیتی- حمید، حقوق آفرینشهای فکری، نشر حقوقدان، ۱۳۷۵ [۳] لایقی، غلامرضا، کپی رایت در کشورهای اسلامی، خانه کتاب ۱۳۸۱		
سایر مراجع	[1] S.Von Lewinski- J.Reinbothe, WIPO Treaties 1996, Butterworths, London, 1999. [2] Chisum-Nard-Schwartz-Neumann-Kief, "Principles of Patent Law", Foundation Press, New York, 1998 [3] R.P.Merges, "Patent Law and Policy", Lexis Law Publishing, Charlottesville, 1997 [4] T.Cook, "A User's Guide to Patents", Butterworths, London, 1999 [5] W.R.Comish, "Intellectual Property, Patent, Copyright, Trademarks and Allied Rights", Sweet and Maxwell, London, 1999 (PRIV 1639) [6] Terrell on the Law of Patents, Sweet and Maxwell, London, 1994 [7] E.J.Van Den Graaf, Patent Law and Modern Biotechnology, Kluwer, Deventer, Gouda Quint, 1997 [8] Uma suthersanen, Design Law in Europe. Sweet and Maxwell, 2000 [9] R.Toulson- C.Phipss, Confidentialty, Sweet and Maxwell, London, 1996 [10] A.Coleman, The legal Protection of Trade Secret, Sweet and Maxwell, London, 1992		

[11] R.Annand, Blackstones Guide to the Community Trade Mark, Blackstone Press Ltd., London, 1999
[12] P.Van Der Kooij, The Community Trademark Regulation, Sweet and Maxwell, London,2000
[13] T.M.Jordan, D.J.Teece (eds.) Antitrust Innovation Oxford University Press, New York, 1997
[14] Sanders, Unfair Competition Law, Oxford University Press, Oxford, 1997 60- R.S.Perlmutter- W.O.Hennessey- G.Dinwoodie, International Intellectual Property Law, Matthew Bender, N.Y., 2000
[15] K. Beresford, "Patenting Software under the European Convention", Sweet and Maxwell, London, 1999
[16] Mihaly Ficsor, The Law of Copyright and Internet, Oxford, 2002 63- Jonathan Posenoer, Cyber Law, The Internet, Springer, 1997
[17] J.Boyle, Shamans, Software and Spleens: Law and the Construction of Information Society, Hardvard University Press, Combridge, 1996
[18] L.Lessig, Code and other Laws of Cyberspace, Basic Book, New York, 2000 66- F.L.Street- M.P.Grant, Law ofthe Internet, Matthew Bender, New York, 1999 67- M.Chissick- A.Kelman, Electronic Commerce Law and Practice, Sweet and Maxwell, London, 1999
[19] S.York, £-Commerce: A Guide to the Law of Electronic Business, Butterworths,London, 1999
[20] Roger J.Smiky, Property Law, Pearson Eduation, 2000.
[21] WIPO. Guide to the International Registration of Marks under the Madrid Agreement and the Madrid Protocol, WIPO, 2002.
[22] M.Chissick- A.Kelman, Electronic Commerce Law and Practice, Sweet and Maxwell, London, 1999.

حقوق اینترنت و تجارت الکترونیک

نام درس به فارسی	حقوق اینترنت و تجارت الکترونیک		
نام درس به انگلیسی	Internet and E-Commerce Law		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۲ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	• کپی رایت و اینترنت • قراردادهای الکترونیکی و امضاهای دیجیتالی • جرائم اینترنتی • حمایت از تجارت الکترونیک : مطالعه حقوق آمریکا • حمایت از تجارت الکترونیک : مطالعه حقوق انگلیس • مطالعه مقررات کمیسیون حقوق تجارت بین‌الملل		
نتایج درس			
فهرست مباحث	۱.کپی رایت و اینترنت ۲.اینترنت و اخلاق ۳.هتک حرمت از طریق اینترنت ۴.مسوولیت مدنی ۵.قراردادهای الکترونیکی و امضاهای دیجیتالی •تجارت الکترونیک •حیف و میل/ اختلاس / دزدی اطلاعات ۶.جرائم اینترنت •جرائم مربوط به داده‌ها : شنود الکترونیکی، تغییر داده‌ها، سرقت داده‌ها، تقلب در حراج اینترنتی •جرائم شبکه : اختلال در شبکه، خرابکاری در شبکه، تهدید یا مزاحمت پست الکترونیکی •نفوذ : دسترسی غیرمجاز، انتشار ویروس •سایر موارد : همکاری در ارتکاب جرم، جعل رایانه‌ای، کلاهبرداری، سرقت کدشناسایی، تقاضای متقلبانه برای کالاها یا خدمات، معامله متقلبانه به وسیله کارت اعتباری، بازی قمار در شبکه ۷.بحث در انجمن بین‌المللی کامپیوتر ۸.حمایت از تجارت الکترونیک : مطالعه حقوق آمریکا •قانون ۱۹۶۴-۱۹۸۶، قوانین آراء دادگاهها در مسائل مربوط به حمایت از نرم-افزارهای برای تجارت الکترونیکی		

	۹.حمایت از تجارت الکترونیک : مطالعه حقوق انگلیس ●قوانین حمایتی ۱۹۴۹-۱۹۷۷ ، قوانین حمایتی اتحادیه اروپا (کنوانسیون اروپایی ۱۹۷۳ وبعد) ۱۰.مطالعه مقررات کمیسیون حقوق تجارت بین‌الملل ●حمایت از پیام‌های اطلاعاتی راجع به کالاها و خدمات ●حمایت از عرضه از طریق سیستم رسانه‌های گروهی ●دستور 2000/31/EC اتحادیه اروپایی ●مطالعه اجمالی کنوانسیون بیع بین‌المللی ●مطالعه دستورالعمل UNCTTERAL ●قراردادهای الکترونیکی راجع به اعطای امتیاز ●قلمرو اجرائی ●مبادلات الکترونیکی اسناد تجارتی (نظیر برات و سفته) ●کاربرد پیام‌های داده‌ای در عقد قرارداد ●زمان و مکان ارسال و دریافت پیام‌های داده‌ای (مدل حقوق تجارت الکترونیکی)
کتاب (های) مرجع	[۱] کاتوزیان ناصر، حقوق مدنی : قواعد عمومی قراردادها، جلد اول تا پنجم، شرکت انتشار با همکاری شرکت بهمن برنا، انتشارات مدرس، ۱۳۷۶ [۲] صفائی-سید حسین، دوره مقدماتی حقوق مدنی، قواعد عمومی قراردادها، نشر میزان، ۱۳۸۲ [۳] آیتی- حمید، حقوق آفرینشهای فکری، نشر حقوقدان، ۱۳۷۵ [۴] لایقی، غلامرضا، کپی رایت در کشورهای اسلامی، خانه کتاب ۱۳۸۱ [۵] صفائی-سید حسین، دوره حقوق مدنی و حقوق تطبیقی، نشر میزان، ۱۳۷۵
سایر مراجع	[1] S.Von Lewinski- J.Reinbothe, WIPO Treaties 1996, Butterworths, London, 1999. [2] Chisum-Nard-Schwartz-Neumann-Kief, "Principles of Patent Law", Foundation Press, New York, 1998 [3] R.P.Merges, "Patent Law and Policy", Lexis Law Publishing, Charlottesville, 1997 [4] T.Cook, "A User's Guide to Patents", Butterworths, London, 1999 [5] W.R.Comish, "Intellectual Property, Patent, Copyright, Trademarks and Allied Rights", Sweet and Maxwell, London, 1999 (PRIV 1639) [6] Terrell on the Law of Patents, Sweet and Maxwell, London, 1994 [7] E.J.Van Den Graaf, Patent Law and Modern Biotechnology, Kluwer, Deventer, Gouda Quint, 1997 [8] Uma suthersanen, Design Law in Europe. Sweet and Maxwell, 2000 [9] R.Toulson- C.Phipss, Confidentialty, Sweet and Maxwell, London, 1996 [10] A.Coleman, The legal Protection of Trade Secret, Sweet and Maxwell, London, 1992 [11] R.Annand, Blackstones Guide to the Community Trade Mark, Blackstone Press Ltd., London, 1999 [12] P.Van Der Kooij, The Community Trademark Regulation, Sweet and Maxwell, London,2000 [13] T.M.Jordan, D.J.Teece (eds.) Antitrust Innovation Oxford University Press, New York, 1997 [14] Sanders, Unfair Competition Law, Oxford University Press, Oxford, 1997 60-R.S.Perlmutter- W.O.Hennessey- G.Dinwoodie, International Intellectual Property Law, Matthew Bender, N.Y., 2000

[15] K. Beresford, "Patenting Software under the European Convention", Sweet and Maxwell, London, 1999
[16] Mihaly Ficsor, The Law of Copyright and Internet, Oxford, 2002 63- Jonathan Posenoer, Cyber Law, The Internet, Springer, 1997
[17] J.Boyle, Shamans, Software and Spleens: Law and the Construction of Information Society, Hardvard University Press, Combridge, 1996
[18] L.Lessig, Code and other Laws of Cyberspace, Basic Book, New York, 2000 66- F.L.Street- M.P.Grant, Law ofthe Internet, Matthew Bender, New York, 1999 67- M.Chissick- A.Kelman, Electronic Commerce Law and Practice, Sweet and Maxwell, London, 1999
[19] S.York, £-Commerce: A Guide to the Law of Electronic Business, Butterworths,London, 1999
[20] Roger J.Smiky, Property Law, Pearson Eduation, 2000.
[21] WIPO. Guide to the International Registration of Marks under the Madrid Agreement and the Madrid Protocol, WIPO, 2002.
[22] M.Chissick- A.Kelman, Electronic Commerce Law and Practice, Sweet and Maxwell, London, 1999.

حقوق انتقال تکنولوژی و دانش فنی

نام درس به فارسی	حقوق انتقال تکنولوژی و دانش فنی		
نام درس به انگلیسی	Technology Transfer Law		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۳ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	• آشنایی دانشجویان با: • ماهیت حقوقی انتقال تکنولوژی • جنبه‌های بین‌المللی حقوق انتقال تکنولوژی • مقررات ناظر به حق اختراع و ه نام تجاری • مقررات ناظر به حقوق مولف و دانش فنی • طریق مشارکتی و طریق قراردادی محض • قراردادهای معاضدت فنی و قراردادهای ناقل		
نتایج درس			
فهرست مباحث	۱.ماهیت حقوقی انتقال تکنولوژی •جنبه‌های بین‌المللی حقوق انتقال تکنولوژی • حقوق بین‌المللی اقتصادی • حقوق تطبیقی •جنبه‌های حقوق داخلی با مقتضیات و تنگناها • مقررات ناظر به حق اختراع • مقررات ناظر به نام تجاری • مقررات ناظر به حقوق مولف • مقررات ناظر به دانش فنی ۲.طرق قرادادی انتقال تکنولوژی • طریق مشارکتی و طریق قراردادی محض • قراردادهای معاضدت فنی • قراردادهای ناقل		
کتاب (های) مرجع	[۱] کاتوزیان ناصر، حقوق مدنی : قواعد عمومی قراردادها، جلد اول تا پنجم، شرکت انتشار با همکاری شرکت بهمن برنا، انتشارات مدرس، ۱۳۷۶ [۲] صفائی-سید حسین، دوره مقدماتی حقوق مدنی، قواعد عمومی قراردادها، نشر میزان، ۱۳۸۲ [۳] آیتی- حمید، حقوق آفرینشهای فکری، نشر حقوقدان، ۱۳۷۵ [۴] لایقی، غلامرضا، کپی رایت در کشورهای اسلامی، خانه کتاب ۱۳۸۱ [۵] صفائی-سید حسین، دوره حقوق مدنی و حقوق تطبیقی، نشر میزان، ۱۳۷۵		

[1] S.Von Lewinski- J.Reinbothe, WIPO Treaties 1996, Butterworths, London, 1999. [2] Chisum-Nard-Schwartz-Neumann-Kief, "Principles of Patent Law", Foundation Press, New York, 1998 [3] R.P.Merges, "Patent Law and Policy", Lexis Law Publishing, Charlottesville, 1997 [4] T.Cook, "A User's Guide to Patents", Butterworths, London, 1999 [5] W.R.Comish, "Intellectual Property, Patent, Copyright, Trademarks and Allied Rights", Sweet and Maxwell, London, 1999 (PRIV 1639) [6] Terrell on the Law of Patents, Sweet and Maxwell, London, 1994 [7] E.J.Van Den Graaf, Patent Law and Modern Biotechnology, Kluwer, Deventer, Gouda Quint, 1997 [8] Uma suthersanen, Design Law in Europe. Sweet and Maxwell, 2000 [9] R.Toulson- C.Phipss, Confidentialty, Sweet and Maxwell, London, 1996 [10] A.Coleman, The legal Protection of Trade Secret, Sweet and Maxwell, London, 1992 [11] R.Annand, Blackstones Guide to the Community Trade Mark, Blackstone Press Ltd., London, 1999 [12] P.Van Der Kooij, The Community Trademark Regulation, Sweet and Maxwell, London,2000 [13] T.M.Jordan, D.J.Teece (eds.) Antitrust Innovation Oxford University Press, New York, 1997 [14] Sanders, Unfair Competition Law, Oxford University Press, Oxford, 1997 60- R.S.Perlmutter- W.O.Hennessey- G.Dinwoodie, International Intellectual Property Law, Matthew Bender, N.Y., 2000 [15] K. Beresford, "Patenting Software under the European Convention", Sweet and Maxwell, London, 1999 [16] Mihaly Ficsor, The Law of Copyright and Internet, Oxford, 2002 63- Jonathan Posenoer, Cyber Law, The Internet, Springer, 1997 [17] J.Boyle, Shamans, Software and Spleens: Law and the Construction of Information Society, Hardvard University Press, Combridge, 1996 [18] L.Lessig, Code and other Laws of Cyberspace, Basic Book, New York, 2000 66- F.L.Street- M.P.Grant, Law ofthe Internet, Matthew Bender, New York, 1999 67- M.Chissick- A.Kelman, Electronic Commerce Law and Practice, Sweet and Maxwell, London, 1999 [19] S.York, £-Commerce: A Guide to the Law of Electronic Business, Butterworths,London, 1999 [20] Roger J.Smiky, Property Law, Pearson Eduation, 2000. [21] WIPO. Guide to the International Registration of Marks under the Madrid Agreement and the Madrid Protocol, WIPO, 2002. [22] M.Chissick- A.Kelman, Electronic Commerce Law and Practice, Sweet and Maxwell, London, 1999.	**سایر مراجع**

جرم شناسی

نام درس به فارسی	جرم شناسی		
نام درس به انگلیسی	Criminology		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۲ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	آموزش نظری یکی از مباحث درس جرم‌شناسی به صورت تحقیقی و تطبیقی آشنایی با اصول جرم‌شناسی کاربردی و روشهای اصلاح و درمان بالینی		
نتایج درس			
فهرست مباحث	یک یا چند مبحث از موارد زیر به انتخاب استاد تعیین و تدریس می‌شود: ۱.جرم‌شناسی نظری ●نظریه اولیه در جرم‌شناسی (اوایل سده نوزدهم تا اوایل سده بیستم) ●نظریه‌های جدید در جرم‌شناسی (از اوایل سده بیستم تا به امروز) ۲.جرم‌شناسی کاربردی (بالینی) ●اصول جرم‌شناسی کاربردی ●روشهای اصلاح و درمان بالینی		
کتاب (های) مرجع	[1] Weisburd, David. "The law of crime concentration and the criminology of place." Criminology 53, no. 2 (2015): 133-157. [2] Barnes, J. C., John Paul Wright, Brian B. Boutwell, Joseph A. Schwartz, Eric J. Connolly, Joseph L. Nedelec, and Kevin M. Beaver. "Demonstrating the validity of twin research in criminology." Criminology 52, no. 4 (2014): 588-626. [3] Ferrell, Jeff. Cultural criminology. Springer New York, 2014.		
سایر مراجع			

حقوق کیفری اقتصادی و جرائم سازمان یافته بین المللی اقتصادی

نام درس به فارسی	حقوق کیفری اقتصادی و جرائم سازمان یافته بین المللی اقتصادی		
نام درس به انگلیسی	International Cooperation against Transnational Financial Organized Crime		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۱ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	جرائم سازمان یافته اقتصادی در سطوح مختلف ملی، منطقه‌ای و جهانی که نظم و امنیت بین‌المللی را در معرض مخاطره جدی قار داده است، یکی از عناوین حدید در حقوق است که به لحاظ اهمیت و توسعه روز افزون حرائم اقتصادی و مالی، همکاری دولتها را در مبارزه با اینگونه جرائم طلب می‌نماید. آشنایی دانش آموختگان حقوق با این رشته به لحاظ روبرو شدن جوامع با این حرائم و چگونگی مبارزه و جلوگیری از آثار زیانبار آن نه تنها لازم، بلکه ضروری و مهم می‌باشد. لذا در این درس، ضمن معرفی انواع اینگونه جرائم، سازمانهای مبارزه با حرائم اقتصادی برای دانشجویان معرفی و مورد بحث قرار می گیرد.		
نتایج درس			
فهرست مباحث	۱.اقدامات سازمان ملل متحد در خصوص مبارزه با جرائم سازمان‌یافته ●کنوانسیون پالرمو (این کنوانسیون در شهر پالرمو-جزیره سیسیل ایتالیا به امضای ۱۲۴ کشور رسیده است) ●کنوانسیون سازمان ملل متحد علیه فساد مالی ۲.کنوانسیون‌های مرتبط با جرائم سازمان‌یافته فراملی ●کنوانسیون سازمان ملل مرتبط با مواد مخدر مصوب ۱۹۶۱ ●کنوانسیون سازمان ملل در رابطه با مواد مخدر و داروهای روانگردان مصوب ۱۹۸۸ ●کنوانسیون بین‌المللی کمکهای متقابل اداری به منظور پیشگیری، تجسس و جلوگیری از تخلفات گمرکی مصوب ۱۹۹۵ ۳.برنامه‌های موسسات حسابرسی بین‌المللی و منطقه‌ای مبارزه با تقلب و فساد از قبیل INTOSAI، ASOSAI، ECOSAI و EUROSAI ●مقررات بین‌المللی مبارزه با پولشویی ●مقررات داخلی جهت مبارزه با پولشویی و دیگر جرائم اقتصادی ۴.جرائم سازمان یافته اقتصادی و نقض اطلاعات تکنولوژی در توسعه و مقابله با آن ۵.سازمان بین‌المللی اقدام مالی و مبارزه با پولشویی FATF ●توصیه‌ها و استانداردها ●متدولوژی برای ارزیابی و تطبیق ●اقدامات اجرایی		

[1] Berdal, Mats R., and Mónica Serrano, eds. Transnational organized crime and international security: business as usual?. Lynne Rienner Publishers, 2002. [2] Sanderson, Thomas M. "Transnational terror and organized crime: blurring the lines." SAIS Review of International Affairs 24, no. 1 (2004): 49-61. [3] Masciandaro, Donato, ed. Global financial crime: terrorism, money laundering and offshore centres. Taylor & Francis, 2017. [4] Leong, Angela Veng Mei. The disruption of international organised crime: an analysis of legal and non-legal strategies. Routledge, 2016.	**کتاب (های) مرجع**
	سایر مراجع

متون حقوقی

نام درس به فارسی	متون حقوقی		
نام درس به انگلیسی	Legal Literature Review		
نوع درس	اختیاری	میان رشته‌ای جرم یابی دیجیتال-گرایش جرم یابی دیجیتال	۲ واحد
مقطع	تحصیلات تکمیلی		
پیش نیازها			
مطالب پیش نیاز			
اهداف درس	هدف از این درس آشنایی دانشجویان با متون تخصصی انگلیسی در زمینه جرم‌یابی دیجیتال و توانایی استفاده از آنهاست.		
نتایج درس			
فهرست مباحث	در این درس متون حقوقی شامل کتب، اسناد بین‌المللی، منطقه‌ای و قوانین موضوعه کشورهای توسعه یافته، دکترین و آرای قضایی در زمینه جرائم دیجیتال مورد مطالعه قرار می‌گیرد.		
کتاب (های) مرجع	[1] S.Von Lewinski- J.Reinbothe, WIPO Treaties 1996, Butterworths, London, 1999. [2] W.R.Comish, "Intellectual Property, Patent, Copyright, Trademarks and Allied Rights", Sweet and Maxwell, London, 1999 (PRIV 1639) [3] Terrell on the Law of Patents, Sweet and Maxwell, London, 1994 [4] E.J.Van Den Graaf, Patent Law and Modern Biotechnology, Kluwer, Deventer, Gouda Quint, 1997 [5] Uma suthersanen, Design Law in Europe. Sweet and Maxwell, 2000 [6] R.Toulson- C.Phipss, Confidentialty, Sweet and Maxwell, London, 1996 [7] A.Coleman, The legal Protection of Trade Secret, Sweet and Maxwell, London, 1992 [8] R.Annand, Blackstones Guide to the Community Trade Mark, Blackstone Press Ltd., London, 1999 [9] P.Van Der Kooij, The Community Trademark Regulation, Sweet and Maxwell, London,2000 [10] T.M.Jordan, D.J.Teece (eds.) Antitrust Innovation Oxford University Press, New York, 1997 [11] S.York, £-Commerce: A Guide to the Law of Electronic Business, Butterworths,London, 1999 [12] Roger J.Smiky, Property Law, Pearson Eduation, 2000. [13] WIPO. Guide to the International Registration of Marks under the Madrid Agreement and the Madrid Protocol, WIPO, 2002.		
سایر مراجع			