جمهوری اسلامی ایران
وزارت علوم، تحقیقات و فناوری
شورای عالی برنامه‌ریزی آموزشی

دانشگاه اصفهان

برنامه درسی رشته

امنیت اطلاعات

INFORMATION SECURITY

مقطع دکتری مهندسی فناوری اطلاعات– امنیت اطلاعات

اعضای کمیته تدوین و بازنگری برنامه:

دکتر مائده عاشوری	**عضو هیات علمی دانشگاه اصفهان**
دکتر حمید مَلا	**عضو هیات علمی دانشگاه اصفهان**
دکتر مجتبی مهدوی	**عضو هیات علمی دانشگاه اصفهان**
دکتر احسان مهدوی	**عضو هیات علمی دانشگاه اصفهان**
دکتر بهروز ترک لادانی	**عضو هیات علمی دانشگاه اصفهان**

فهرست..... شماره صفحه

جدول تغییرات

	عنوان درس در برنامه قبلی	تعداد واحد		عنوان درس در برنامه بازنگری شده	تعداد واحد		استاد بازنگری درس	توضیحات
		نظری	عملی		نظری	عملی		
۱				امنیت کامپیوتر	۳	۰	دکتر عاشوری	این درس به مجموعه دروس اضافه شده و سرفصل آن تدوین شده است.
۲	رمزنگاری کاربردی	۳	۰	رمزنگاری کاربردی	۳	۰	دکتر ملا	سرفصل درس بازنگری شده است
۳	امنیت شبکه پیشرفته	۳	۰	امنیت شبکه	۳	۰	دکتر عاشوری	عنوان درس تغییر داده شده و سرفصل درس بازنگری شده است
۴	توسعه امن نرم‌افزار	۳	۰	امنیت نرم‌افزار	۳	۰	دکتر لادانی	عنوان درس تغییر داده شده و سرفصل آن بازنگری شده است.
۵	مدیریت امنیت اطلاعات	۳	۰	مدیریت امنیت اطلاعات	۳	۰	دکتر ملا	سرفصل درس بازنگری شده است.
۶	امنیت پایگاه داده	۳	۰	امنیت پایگاه داده	۳	۰	دکتر عاشوری	سرفصل درس بازنگری شده است.
۷				محاسبات امن	۳	۰	دکتر ملا	این درس به مجموعه دروس اضافه و سرفصل آن تدوین شده است.
۸				حریم خصوصی	۳	۰	دکتر عاشوری	این درس به مجموعه دروس اضافه و سرفصل آن تدوین شده است.
۹				امنیت در رایانش ابری	۳	۰	دکتر عاشوری	این درس به مجموعه دروس اضافه و سرفصل آن تدوین شده است.
۱۰	پروتکل‌های امنیتی	۳	۰	پروتکل‌های امنیتی	۳	۰	دکتر ملا	سرفصل درس بازنگری شده است.
۱۱	روش‌های صوری در امنیت اطلاعات	۳	۰	تحلیل و وارسی صوری امنیت	۳	۰	دکتر لادانی	عنوان درس تغییر داده شده و سرفصل آن بازنگری شده است.
۱۲				جرم یابی کامپیوتری	۳	۰	دکتر احسان مهدوی	این درس به مجموعه دروس اضافه و سرفصل آن تدوین شده است.

۱۳			رمزنگاری پیشرفته	۳	۰	دکتر ملا		این درس به مجموعه دروس اضافه و سرفصل آن تدوین شده است.
۱۴			مبانی فناوری بلاکچین	۳	۰	دکتر مجتبی مهدوی		این درس به مجموعه دروس اضافه و سرفصل آن تدوین شده است.
۱۵			طراحی سامانه های مبتنی بر بلاکچین	۳	۰	دکتر مجتبی مهدوی		این درس به مجموعه دروس اضافه و سرفصل آن تدوین شده است.
۱۶			تحلیل بدافزار	۳	۰	دکتر لادانی		این درس به مجموعه دروس اضافه و سرفصل آن تدوین شده است.
۱۷	نهان‌سازی اطلاعات	۳	پنهان‌سازی اطلاعات	۳	۰	دکتر عاشوری		نام درس تغییر یافته و سرفصل درس بازنگری شده است.
۱۸			سامانه‌های تشخیص نفوذ	۳	۰	دکتر احسان مهدوی		این درس به مجموعه دروس اضافه و سرفصل آن تدوین شده است.
۱۹	امنیت و اعتماد سخت‌افزار	۳	امنیت و اعتماد سخت‌افزار	۳	۰	دکتر عاشوری		سرفصل درس بازنگری شده است.
۲۰			امنیت سیستم های سایبرفیزیکی	۳	۰	دکتر احسان مهدوی		این درس به مجموعه دروس اضافه و سرفصل آن تدوین شده است.
۲۱	ریاضیات رمزنگاری	۳	ریاضیات رمزنگاری	۳	۰	دکتر ملا		سرفصل درس بازنگری شده است.
۲۲	تئوری اطلاعات و کدینگ	۳	تئوری اطلاعات و کدینگ	۳	۰	دکتر ملا		سرفصل درس بازنگری شده است.
۲۳			تحلیل رمز	۳	۰	دکتر ملا		این درس به مجموعه دروس اضافه و سرفصل آن تدوین شده است.
۲۴	امنیت تجارت الکترونیک	۳	امنیت تجارت الکترونیکی	۳	۰	دکتر عاشوری		سرفصل درس بازنگری شده است.
۲۵			پروتکل‌های امنیتی پیشرفته	۳	۰	دکتر ملا		این درس به مجموعه دروس اضافه و سرفصل آن تدوین شده است.

۲۶			امنیت شبکه-های سیار		۳	۰	دکتر عاشوری	این درس به مجموعه دروس اضافه و سرفصل آن تدوین شده است.
۲۷			امنیت اینترنت اشیا		۳	۰	دکتر عاشوری	این درس به مجموعه دروس اضافه و سرفصل آن تدوین شده است.
۲۸	نظریه الگوریتمی بازی ها	۳	۰	نظریه الگوریتمی بازی ها	۳	۰	دکتر ملا	سرفصل درس بازنگری شده است.
۲۹	نظریه پیچیدگی	۳	۰	نظریه پیچیدگی	۳	۰	دکتر عاشوری	سرفصل درس بازنگری شده است.
۳۰				آزمون نرم افزار پیشرفته	۳	۰	دکتر عاشوری	این درس به مجموعه دروس اضافه و سرفصل آن تدوین شده است.
۳۱				شبکه‌های کامپیوتری پیشرفته	۳	۰	دکتر عاشوری	این درس به مجموعه دروس اضافه و سرفصل آن تدوین شده است.
۳۲				فرایندهای تصادفی	۳	۰	دکتر عاشوری	این درس به مجموعه دروس اضافه و سرفصل آن تدوین شده است.
۳۳				سیستم‌های سایبرفیزیکی	۳	۰	دکتر احسان مهدوی	این درس به مجموعه دروس اضافه و سرفصل آن تدوین شده است.
۳۴				تعامل امنیت سایبری و یادگیری ماشین	۳	۰	دکتر احسان مهدوی	این درس به مجموعه دروس اضافه و سرفصل آن تدوین شده است.
۳۵	درستی‌یابی سیستم‌های واکنشی	۳	۰				اعضای گروه	این درس بدلیل نامرتبط‌بودن حذف شده است.
۳۶	امنیت سیستم‌های نوین ارتباطی	۳	۰				اعضای گروه	این درس بدلیل نامرتبط‌بودن حذف شده است.

فصل اول

مشخصات کلی برنامه درسی

الف) مقدمه: معرفی کلی و تبیین برنامه درسی

همزمان با رشد روزافزون کاربردهای کامپیوتر، فناوری اطلاعات و ارتباطات در عرصه‌های مختلف، تهدیدات و تهاجمات علیه سامانه‌های اطلاعاتی و ارتباطی نیز به سرعت رشد نموده‌اند. به همین علت تربیت نیروی انسانی متخصص در زمینه امنیت اطلاعات از نیازهای اصلی کشور به شمار می‌رود. در همین راستا تدوین دوره دکتری با هدف تربیت نیروی متخصص و محقق در زمینه‌ی امنیت اطلاعات و امنیت سامانه‌های اطلاعاتی و ارتباطی مورد توجه قرار گرفته است.

امنیت اطلاعات شاخه‌ای بین رشته‌ای از علوم فنی و مهندسی است که راهبردها، خط مشی‌ها، روال‌ها، سازوکارها، ابزارها، راهکارها و روش‌های محافظت از اطلاعات و مقابله با تهدیدات سامانه‌ها و شبکه‌های اطلاعاتی و ارتباطی در آن مورد مطالعه قرار می‌گیرد. دانش آموختگان این رشته قادر خواهند بود برای فراهم نمودن امنیت اطلاعات و ارتباطات بخش‌های مهم اقتصادی، نظامی، علمی و اجتماعی کشور راه‌حل‌های کاربردی و محصولات امنیتی ارائه دهند و به این ترتیب کشور را در راستای بومی‌سازی صنعت امنیت سایبری یاری دهند.

ب) اهداف

در تدوین این دوره ضمن آنکه برنامه‌ی دوره‌های دکتری در دانشگاه‌های معتبر دنیا و دیگر دانشگاه‌های ایران و نیز برنامه‌ی سایر گروه‌های آموزشی در دانشگاه اصفهان مورد بررسی قرار گرفت، با نظرخواهی از همکاران و متخصصین داخلی سعی شده است بر نقاط قوت این دوره افزوده و از نقاط ضعف دوره‌ی موجود کاسته شود. از آنجایی که امکان ورود دانشجویان به مقطع دکتری امنیت اطلاعات، از رشته‌ها و گرایش‌های متعدد، همچون نرم‌افزار، شبکه، مخابرات و علوم کامپیوتر وجود دارد، دانشجویان ورودی این دوره از پیش‌زمینه‌ی علمی یکسان برخوردار نیستند. برای رفع این چالش تلاش شده است دروس این دوره انعطاف مناسبی هم از لحاظ ارایه‌ی دروس برای گروه مجری و هم از لحاظ اخذ دروس برای دانشجویان فراهم آورد. از سوی دیگر، ورود دانشجویان از گرایش‌های مختلف به دوره‌ی دکتری امنیت اطلاعات از این مزیت برخوردار است که با توجه به ماهیت بین‌رشته‌ای امنیت اطلاعات می‌تواند منجر به نتایج علمی مناسبی شود. برنامه‌ی حاضر به دنبال تقویت مزیت مذکور در عین رفع اشکالات محتمل می‌باشد.

پ) اهمیت و ضرورت

همان‌گونه که بیان شد، با وجود تهدیدات و تهاجمات علیه سامانه‌های اطلاعاتی و ارتباطی نیاز به تربیت نیروی متخصص و پژوهشگر در زمینه امنیت اطلاعات و ارتباطات از نیازهای اصلی کشور به شمار می‌رود. در همین راستا دوره تحصیلات تکمیلی امنیت سایبری با هدف تربیت نیروی متخصص در زمینه‌ی امنیت سامانه‌های اطلاعاتی و ارتباطی مورد توجه قرار گرفته است.

ت) تعداد و نوع واحدهای درسی (بر اساس جدول شماره ۱ تا ۳ آیین‌نامه تدوین و بازنگری برنامه‌های درسی)

تعداد کل واحدهای در نظر گرفته شده برای دوره‌ی دکتری ۳۶ واحد می‌باشد که شامل دروس گروه ۱، گروه ۲ و رساله می‌باشد. فهرست دروس جبرانی دوره‌ی دکتری در فصل دوم ارائه می‌شود.

نوع دروس و توزیع واحدهای درسی دکتری مهندسی فناوری اطلاعات- گرایش امنیت اطلاعات به شرح جدول ۱ است:

جدول (۱)- نوع دروس و توزیع واحدهای درسی
دکتری مهندسی فناوری اطلاعات - امنیت اطلاعات

ردیف			نوع واحد درسی	تعداد واحد
۱	قسمت آموزشی	دروس تخصصی الزامی	دروس تخصصی گروه ۱	۹
		دروس تخصصی اختیاری	دروس تخصصی گروه ۲	۹
۲	قسمت پژوهشی		رساله	۱۸
	جمع			۳۶

ث) نقش، توانایی و شایستگی مورد انتظار از دانش‌آموختگان:

از فارغ التحصیلان دوره دکتری مهندسی فناوری اطلاعات-گرایش امنیت اطلاعات انتظار می‌رود در طراحی، تحقیق، توسعه، به روزرسانی و بهینه‌سازی صنعت امنیت کشور فعال شوند. از ایشان انتظار می‌رود با تأمین قابلیت رقابت‌پذیری بین‌المللی در سیستم‌های کامپیوتری، شبکه‌ای و هوشمند مورد استفاده در کلیه صنایع، سازمان‌های دولتی و خصوصی، زیرساخت‌های محاسباتی و ارتباطی در صنعت و خدمات و مدیریت و دفاع و امنیت کشور نقش تعیین کننده داشته باشند و ضمن اشراف بر کلیه روش‌های علمی و فنی طراحی و اجرا و نگهداری در پروژه‌ها، بتوانند بهترین گزینه موجود طراحی و ساخت و اجرا و حفظ امنیت اطلاعات در موارد مورد نیاز جامعه و کشور را انتخاب و زیر ساخت پروژه‌های مورد نیاز ایران را در بهترین کیفیت جهانی طراحی و اجرا و مدیریت نمایند.

ج) شرایط و ضوابط ورود به دوره (اطلاعات این بند به صورت پیشنهادی می‌باشد و شرایط و ضوابط ورود به دوره‌های تحصیلی، تابع سیاست‌های بالادستی می‌باشد).

دانشجویان پذیرفته شده در دوره دکتری مهندسی فناوری اطلاعات- گرایش امنیت اطلاعات می‌توانند بر اساس ضوابط موضوعه از بین دانش‌آموختگان کارشناسی ارشد مهندسی فناوری اطلاعات، مهندسی کامپیوتر، علوم کامپیوتر و مهندسی برق انتخاب شوند.

چ) شرایط، ضوابط و الزامات اجرا و گسترش رشته؛

برای اجرای رشته امنیت اطلاعات، علاوه بر نیاز به آزمایشگاه‌های تحقیقاتی، نیاز به آزمایشگاه امنیت و سیستم‌های کامپیوتری جهت نصب نرم افزارهای تست و ارزیابی امنیت است. جهت گسترش رشته می‌توان شاخه‌های مختلف بین رشته‌ای مانند جرم‌شناسی رایانه‌ای را نیز راه اندازی کرد.

ه) زمینه‌های شغلی حال و آینده

در شرایط کنونی و با گسترش سیستم‌های کامپیوتری، رشته امنیت اطلاعات بازار کار داغ و موقعیت‌های شغلی گسترده‌ای را در دانشگاه‌ها، سازمان‌های دولتی و شرکت‌های خصوصی برای فارغ التحصیلان به وجود آورده‌است. به علاوه با رشد و توسعه فناوری انتظار می‌رود این روند همچنان ادامه یابد. بازار کار برای جذب متخصصان امنیت سایبری به دلیل کمبود نیروی متخصص حتی برای تازه‌کاران این حوزه به شدت بالا می باشد. گزارش‌ها از ESG، که همواره نتایج نظرسنجی سالانه در مورد وضعیت فناوری اطلاعات را منتشر می‌کند، به وضوح بر تقاضای بالا در حوزه امنیت سایبری دلالت می نماید، به طوری که بر طبق گزارش سال ۲۰۱۸، نیاز به کارکنان متخصص در حوزه امنیت سایبری بیشترین تقاضا را نشان می دهد.

همچنین بر اساس این گزارش ، نیاز به مهارت‌های سایبری، سالیانه در حال افزایش می باشد چنانچه در سال ۲۰۱۴، ۲۵ درصد از پاسخ دهندگان، کمبود مهارت‌های سایبری و در سال ۲۰۱۸، ۵۱ درصد از پاسخ دهندگان ، نیاز به کارکنان بیشتر با مهارت‌های سایبری را به عنوان یکی از مشکلات مهم امنیتی اعلام کردند. گزارش اخیر (ISC2) از پیش بینی یک شکاف بزرگ ۱/۸ میلیونی بین مشاغل و تعداد کارکنان مورد نیاز امنیت سایبری تا سال ۲۰۲۲ خبر می‌دهد.

با نگاهی به پیش‌بینی‌های مطرح شده در خصوص روندهای امنیت سایبری سال ۲۰۲۵، می‌توان دریافت که دولت‌ها و جامعه متخصصان امنیت سایبری، در حال آماده‌سازی امکانات و قابلیت‌های خود برای مقابله با تغییرات قابل توجه ناشی از ظهور فناوری‌های نوظهور، در حوزه تهدیدات سایبری هستند. همزمان با افزایش پیچیدگی حملات سایبری در نتیجه گسترش فناوری‌های دیجیتال و توسعه هوش مصنوعی و رایانش کوانتومی، دولت‌ها، سازمان‌ها و متخصصان امنیت سایبری در پی تقویت موقعیت امنیتی، کاهش خطرات و حفاظت از دارایی‌های دیجیتال خود هستند.

به گزارش theinsightpartners، کووید- ۱۹ علاوه‌بر اینکه کشورهای متعددی را تحت تاثیر قرار داد، اقتصاد و صنایع برخی کشورها را نیز تا حد ورشکستگی پیش برد و وضعیت تجاری بسیاری از آنها را با رکورد مواجه کرد. به همین منوال، به دلیل برخط شدن بسیاری از کسب‌وکارها و پررنگ‌تر شدن نقش اینترنت در دوران همه‌گیری و به دنبال آن بالا رفتن خطر تهدید نفوذ حملات سایبری، حوزه‌های امنیت سایبری در سیستم‌های رباتیک رنگ و بوی دیگری پیدا کرد و اهمیت دوچندانی برای مراقبت از فضاهای اینترنتی به خود گرفت.

به گزارش futuremarketinsights، انتظار می‌رود بازار امنیت سایبری در حوزه رباتیک با میانگین رشد پایدار سالانه ۱۱/۶ درصدی همراه باشد. این بازار در سال ۲۰۲۳ درآمدی بالغ بر ۳ میلیارد و ۸۰۰ میلیون دلار را به خود اختصاص داده و پیش‌بینی می‌شود این درآمد تا ۱۰ سال آینده یعنی ۲۰۳۳ به ۱۱ میلیارد و ۶۰۰ میلیون دلار برسد. مطالعاتی که روی این

بازار انجام شده نشان می‌دهد که هرچه بهره‌مندی از فناوری‌های حوزه رباتیک و ماشین‌آلات خودکار بالاتر رود، کاربران بیشتر به یافتن راه‌حل‌های امنیت سایبری رو می‌آورند. علاوه‌بر این هوش‌مصنوعی در ادغام با حوزه رباتیک برای خودکار کردن بسیاری از صنایع مورد استفاده قرار می‌گیرد. رشد استفاده از حوزه‌های رباتیک و ابزارهای خودکار در جمعیت سالمندان دنیا هم درحال افزایش است. کاربرد قابل‌توجه امنیت سایبری در حوزه رباتیک و سیستم‌های خودکار با افزایش حملات سایبری در این سیستم‌ها درحال ارتقاست. حملات سایبری در حوزه رباتیک با فناوری‌های هوشمند، نفوذ بالاتری پیدا کرده است. حوزه رباتیک در سطوح سخت‌افزاری و سیستم‌عاملی مستعد حملات سایبری است. بنابراین نیاز به سرویس‌های مدیریت امنیت سایبری در این حوزه درحال افزایش است. همچنین نفوذ بیشتر هوش‌مصنوعی، یادگیری ماشینی، رباتیک و سیستم‌های خودکار، تقاضا برای استفاده از امنیت سایبری را در حوزه‌های رباتیک بالا می‌برد. به‌عنوان مثال شرکت‌ها دیوار امنیتی خود را با راهکارهای رباتیک امنیت سایبری تقویت می‌کنند و همچنین ایمنی و امنیت سایبری از طریق سیستم‌های داخلی، رشد این بازار را دچار تحول کرده است.

طبق تجزیه و تحلیل‌های صورت‌گرفته، بازار امنیت سایبری در حوزه رباتیک از ۲میلیارد و ۱۸۰ میلیون دلار در سال ۲۰۱۸ به ۳ میلیارد و ۵۰۰ میلیون دلار در ۲۰۲۰ رسید. یکی از اتفاقاتی که در این بازار شاهد هستیم، رشد کوتاه‌مدت آن است که بین سال‌های ۲۰۲۳ تا ۲۰۲۶ رخ می‌دهد. این حملات اغلب در نتیجه کاهش امنیت داده‌ها رخ می‌دهد، برای مواجهه با آن، تقاضا برای سرویس‌های مدیریت نوآورانه‌ی امنیت سایبری باید به سرعت وارد عمل شود. بااین‌اوصاف انتظار می‌رود رشد این بازار تا ۲۰۲۶ به رقمی بالغ بر ۵ میلیارد و ۳۰۰ میلیون دلار برسد. اتفاق دیگر رشد میان‌مدت بین سال‌های ۲۰۲۶ تا ۲۰۲۹ است که در این برهه زمانی افزایش سیستم‌های خودکار و رباتیک در بخش مراقبت‌های سلامت، موادغذایی، معدن و سایر برنامه‌های اکتشافات فضایی رخ خواهد داد. علاوه‌بر این چنین سیستم‌هایی که داده‌های محرمانه را ذخیره می‌کنند، شرکت‌ها را به سمت پذیرش راهکارهای امنیت سایبری برای حوزه‌های رباتیک سوق می‌دهند. این روند، ارزش بازار امنیت سایبری در حوزه‌های رباتیک را از ۵ میلیارد و ۳۰۰ میلیون دلار در ۲۰۲۶ به ۷ میلیارد و ۳۹۰ میلیون دلار خواهد رساند اما در دوره‌های رشد درازمدت، بسیاری از سیستم‌های دفاعی، سیستم‌های خودکار و رباتیک را برای مهندسی و ایمنی مورد استفاده قرار می‌دهند. درصورتی‌که کاربری نادرستی از سیستم‌های رباتیک به عمل بیاید، کنترل آن از دست می‌رود. بنابراین دولت و مراکز نظامی از راهکارهای امنیت سایبری در این سیستم‌ها بهره می‌برند. انتظار می‌رود میانگین رشد سالانه امنیت سایبری در حوزه‌های رباتیک در درازمدت یعنی بین سال‌های ۲۰۲۳ تا ۲۰۳۳ حدود ۱۱/۶ درصد باشد.

دلایل ذکر شده به خوبی عطش بازار برای جذب متخصصان امنیت سایبری را نشان می دهد. بر اساس گزارش نشریه فوربس، انتظار می رود تقاضا برای مشاغل امنیت سایبری در آینده‌ی نزدیک به طور قابل توجهی افزایش یابد و این مسیر شغلی را جذاب کند. اداره آمار کار ایالات متحده افزایش ۳۲ درصدی مشاغل امنیت سایبری از سال ۲۰۲۲ تا ۲۰۲۳ را پیش بینی می‌کند که به طور قابل توجهی بالاتر از نرخ رشد متوسط ۳ درصدی برای همه مشاغل ایالات متحده است. به طور خاص، BLS پیش‌بینی می‌کند که نقش‌های تحلیلگران امنیت اطلاعات پنجمین رشد سریع را در میان تمام مشاغل ایالات متحده در این دوره تجربه خواهد کرد.

برخی از حوزه های شغلی امنیت سایبری عبارتند از:

- تستر نفوذ (Penetration Tester): افراد فعال در این حوزه، همواره در حال تست شبکه‌های سازمان‌ها برای شناسایی و کشف آسیب‌پذیری‌ها هستند، این نقش گاهی اوقات با عنوان "هکر اخلاقی" شناخته می‌شود. انجام وظایف معمولاً به تنهایی انجام نشده و نیاز به تیم وسیعی برای بررسی و پوشش همه آسیب‌پذیری‌های احتمالی و مهمترین بخش‌های نفوذپذیر یک سیستم می‌باشد.
- توسعه دهنده‌ی نرم افزارهای امنیتی(Security Software Developer): توسعه نرم افزارهای امنیتی یک حوزه بسیار عالی با افقی وسیع و روشن به منظور کسب مهارت و سرمایه‌گذاری در آن می باشدکه امکان اشتغال بالایی را برای متخصصان این حوزه در بسیاری از شرکت‌های جهان فراهم می‌نماید.
- حسابرس امنیتی(Security Auditor): حسابرس امنیتی مسئولیت کنترل، اندازه‌گیری میزان امنیت کامپیوترهای سازمان، ثبت و نگهداری آنها را بر عهده دارد. حسابرس، گزارش‌های منظمی را از میزان اثربخشی اقدامات امنیتی و ایجاد معیارهایی را برای سنجش اثبات کارایی شیوه‌های امنیتی فوق در سازمان ارائه می‌نماید. آنها همچنین پیشنهاداتی را در مشورت با مدیران سازمان‌ها به منظور بهبود این اقدامات ارائه می‌دهند. در کنار مهارت به عنوان مشخصه اصلی حسابرسان امنیتی، داشتن دانش کافی در مورد مقررات مربوط به امنیت اطلاعات نیز از ضروریات شغلی آنها به حساب می‌آید.
- معمار امنیتی (Security Architect): معماران امنیت در زمینه طراحی بنیادین معماری سیستم‌های سازمانی فعالیت می‌کنند و تضمین امنیت مشخصات فنی معماری مربوطه را برعهده دارند.
- مدیر تولید (Product Manager): نقش مدیران تولید، مدیریت محصولات شرکت‌های امنیت سایبری می‌باشد. نیاز به دانش عمیق و گسترده از محصول و مدل‌های آن ، دید راهبردی نسبت به توسعه محصول به منظور پیشروی در بازار رقابتی از الزامات تصدی این شغل می باشد.
- مدیر ارشد امنیت اطلاعات ((Chief Information Security Officer (CISO)): این شغل یک جایگاه راهبردی در سازمان به حساب می‌آید که بر روی کاهش تهدیدات سایبری از طریق اقدامات هوشمندانه تمرکز دارد. CISO ها غالباً به عنوان سخنگوی سازمان به ویژه در زمان مواجه شرکت با یک حادثه امنیتی جدی در زمینه امنیت سایبری مطرح می باشند. CISO مسئولین تصمیم‌گیری در مورد مسائل امنیت سایبری سازمان خود هستند زیرا آنها به عنوان سرپرست امنیت سایبری در سرتاسر سازمان فعالیت می‌نمایند.

ی) جایگاه تمدنی، فرهنگی و اجتماعی (جایگاه رشته تحصیلی در حوزه تمدنی گذشته، حال و آینده و بافت فرهنگی و اجتماعی کشور)

این رشته در ایران از قدمت نسبتا خوبی برخوردار است، شرکت‌ها و سازمان‌هایی وجود دارند که به‌طور تخصصی در حوزه امنیت سایبری و زیرشاخه‌های آن از جمله امنیت شبکه، امنیت اینترنت اشیا و امنیت اطلاعات مشغول فعالیت هستند و محصولات تجاری امنیتی خود را توسعه داده‌اند. همچنین بررسی اسناد آمایش کشور، مصوب ۱۳۹۹، نشان می‌دهد امنیت سایبری یکی از رشته‌های ضروری در راستای پیشبردراهبردهای پابرجای کشور در حوزه‌های آموزش، علم و فناوری و همچنین دفاعی–امنیتی می‌باشد. علاوه بر این متخصصان امنیت سایبری، نقشهای اساسی در برنامه‌های اجرایی

آمایش استان اصفهان در حوزه‌های آموزش، علم و فناوری، صنعت، بازرگانی، دفاعی، امنیتی و پدافند غیرعامل برعهده خواهند داشت.

فصل دوم

جدول عناوین و مشخصات دروس

جدول (۲)- عنوان و مشخصات کلی دروس گروه ۱ (تخصصی الزامی)

ردی ف	عنوان درس	تعداد واحد	تعداد واحد به تفکیک نوع			تعداد جلسات	تعداد ساعات*		پیش نیاز	هم نیاز
			نظری	عملی	عملی - نظری		نظری	عملی		
۱	امنیت کامپیوتر (Computer Security)	۳	۳	۰	۰	۳۲	٤٨		–	–
۲	امنیت پایگاه داده (Database Security)	۳	۳	۰	۰	۳۲	٤٨		–	–
۳	امنیت نرم‌افزار (Software Security)	۳	۳	۰	۰	۳۲	٤٨		–	–
٤	مدیریت امنیت اطلاعات (Information Security Management)	۳	۳	۰	۰	۳۲	٤٨		–	–
٥	پروتکل‌های امنیتی (Security Protocols)	۳	۳	۰	۰	۳۲	٤٨		–	–
٦	امنیت شبکه (Network Security)	۳	۳	۰	۰	۳۲	٤٨		–	–

*: ساعت آموزش برای هر واحد نظری ۱۶ ساعت، عملی ۳۲ ساعت، عملی (از نوع کارگاهی) ۴۸ ساعت، کارآموزی و کارورزی ۶۴ یا ۱۲۸ ساعت است.

جدول (۳)- عنوان و مشخصات کلی دروس گروه ۲ (تخصصی اختیاری)

ردیف	عنوان درس	تعداد واحد	تعداد واحد به تفکیک نوع			تعداد جلسات	وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)		تعداد ساعات*		پیش نیاز	هم نیاز
			نظری	عملی	نظری – عملی		مرتبط با آمایش/مأموریت موسسه نیست.	مرتبط با آمایش/مأموریت موسسه است.	نظری	عملی		
۱	محاسبات امن (Secure Computing)	۳	۳			۳۲	✓		۴۸			
۲	حریم خصوصی (Privacy)	۳	۳			۳۲	✓		۴۸			
۳	امنیت رایانش ابری (Cloud Computing Security)	۳	۳			۳۲	✓		۴۸			
٤	رمزنگاری کاربردی (Applied Cryptography)	۳	۳			۳۲	✓		۴۸			
٥	تحلیل و وارسی صوری امنیت (Formal Security Analysis and Verification)	۳	۳			۳۲	✓		۴۸			
٦	جرم‌یابی کامپیوتری (Computer Forensics)	۳	۳			۳۲	✓		۴۸			
۷	رمزنگاری پیشرفته (Advanced Cryptography)	۳	۳			۳۲	✓		۴۸			
۸	مبانی فناوری بلاکچین (Foundation of Blockchain Technology)	۳	۳			۳۲	✓		۴۸			
۹	طراحی سامانه‌های مبتنی بر بلاکچین (Design of Blockchain-based Systems)	۳	۳			۳۲	✓		۴۸			

۱۰	تحلیل بدافزار (Malware Analysis)	۳	۳			۳۲	✓		٤٨			
۱۱	پنهان‌سازی اطلاعات (Information Hiding)	۳	۳			۳۲	✓		٤٨			
۱۲	سامانه‌های تشخیص نفوذ (Intrusion Detection Systems)	۳	۳			۳۲	✓		٤٨			
۱۳	امنیت و اعتماد سخت افزار (Hardware Security and Trust)	۳	۳			۳۲	✓		٤٨			
١٤	امنیت سیستم‌های سایبرفیزیکی (Cyberphysical Systems Security)	۳	۳			۳۲	✓		٤٨			
۱۵	ریاضیات رمزنگاری (Cryptography Mathematics)	۳	۳			۳۲	✓		٤٨			
١٦	تئوری اطلاعات و کدینگ (Coding and Information Theory)	۳	۳			۳۲	✓		٤٨			
۱۷	تحلیل رمز (Cryptanalysis)	۳	۳			۳۲	✓		٤٨			
۱۸	پروتکل‌های امنیتی پیشرفته (Advanced Security Protocols)	۳	۳			۳۲	✓		٤٨			
۱۹	امنیت شبکه‌های سیار (Mobile Network Security)	۳	۳			۳۲		✓	٤٨			
۲۰	امنیت اینترنت اشیا (IoT Security)	۳	۳			۳۲		✓	٤٨			
۲۱	نظریه الگوریتمی بازی‌ها (Algorithmic Theory of Games)	۳	۳			۳۲	✓		٤٨			

۲۲	نظریه پیچیدگی (Complexity Theory)	۳	۳			۳۲	✓			٤٨		
۲۳	امنیت تجارت الکترونیکی (Electronic Commerce Security)	۳	۳			۳۲	✓			٤٨		
۲٤	آزمون نرم‌افزار پیشرفته (Advanced Software Testing)	۳	۳			۳۲	✓			٤٨		
۲۵	شبکه‌های کامپیوتری پیشرفته (Advanced Computer Networks)	۳	۳			۳۲	✓			٤٨		
۲٦	فرایندهای تصادفی (Stochastic Processes)	۳	۳			۳۲	✓			٤٨		
۲۷	سیستم‌های سایبرفیزیکی (Cyberphysical Systems)	۳	۳			۳۲	✓			٤٨		
۲۸	تعامل امنیت سایبری و یادگیری ماشین (Cybersecurity and Machine Learning Interaction)	۳	۳			۳۲	✓			٤٨		
۲۹	مباحث ویژه در امنیت سایبری (۱) (Special Topics in Cybersecurity 1)	۳	۳			۳۲	✓			٤٨		
۳۰	مباحث ویژه در امنیت سایبری (۲) (Special Topics in Cybersecurity 2)	۳	۳			۳۲	✓			٤٨		
۳۱	یک درس از سایر دوره‌های تحصیلات تکمیلی دانشکده به پیشنهاد استاد راهنما و تایید گروه آموزشی	۳	۳			۳۲				٤٨		

*: ساعت آموزش برای هر واحد نظری ۱۶ ساعت، عملی ۳۲ ساعت، عملی (از نوع کارگاهی) ۴۸ ساعت، کارآموزی و کارورزی ۶۴ یا ۱۲۸ ساعت است.

جدول (٤)- دروس جبرانی دکتری

ردیف	نام درس	واحد	نوع درس
۱	پایگاه داده‌ها	۳	نظری
۲	سیستم عامل	۳	نظری
۳	شبکه‌های کامپیوتری	۳	نظری
٤	ریاضیات گسسته	۳	نظری
در صورت عدم گذراندن درس در دوره کارشناسی و با تشخیص گروه مهندسی فناوری اطلاعات.			

فصل سوم

ویژگی‌های دروس

الف: عنوان درس به فارسی: امنیت کامپیوتر			
عنوان درس به انگلیسی:	Computer Security		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☑ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☐ نظری-عملی ☐
			پروژه/ رساله / پایان‌نامه ☐
تعداد ساعت:	٤٨		مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☐ / مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- تبیین مفاهیم اصلی امنیت کامپیوتر و روش‌های طراحی و پیاده‌سازی سیستم‌های کامپیوتری امن
- معرفی انواع خط‌مشی‌ها و مدل‌های امنیتی و روش‌های اعمال آن‌ها

اهداف ویژه:

۱. معرفی فنون مختلف کنترل دسترسی

۲. راهکارهای تصدیق اصالت در سیستم‌های کامپیوتری

۳. تضمین امنیت سیستم و استانداردهای موجود

پ) سرفصل‌ها:

۱. مفاهیم پایه
   - امنیت کامپیوتر، محرمانگی، صحت، دسترس‌پذیری، تهدید، آسیب‌پذیری، حمله
   - خط‌مشی و مدل امنیتی، مکانیزم امنیتی
   - دسته‌بندی تهدیدها و حمله‌های امنیتی
   - نرم‌افزار بدخواه: اسب تِروا، ویروس، کِرم

۲. خط‌مشی‌ها و مدل‌های امنیتی
   - انواع خط مشی‌های امنیتی
   - مدل محرمانگی بل-لاپاجولا
   - امنیت جریان اطلاعات، عدم تداخل
   - مدل صحت بیبا، مدل کِلارک ویلسون
   - مدل دیوار چینی

۳. هویت دیجیتال و نظام‌های هویت

- هویت دیجیتالی، هویت اشیا، کاربران، گروه‌ها، و نقش‌ها
- هویت در وب و اینترنت
- روش‌های تصدیق اصالت کاربر: گذرواژه، توکن، زیست‌سنجی
- حمله به سیستم‌های تصدیق اصالت
- مکانیزم‌های کنترل دسترسی
- لیست‌های کنترل دسترسی و لیست‌های شایستگی، پیاده سازی در سیستم‌های عامل یونیکس و ویندوز
- کنترل دسترسی مبتنی بر نقش (RBAC)
- کنترل دسترسی قفل و کلید، کنترل دسترسی مبتنی بر حلقه

۴. محاسبات قابل اعتماد
- اصول طراحی سیستم‌های امن
- مفهوم سیستمه‌ای قابل اعتماد
- مدول سکّوی قابل اعتماد
- معماری امنیتی FLASK
- سیستم عامل لینوکس با امنیت بهبود یافته (SELinux)

۵. هسته‌های امنیتی
- مفاهیم پایه
- انواع سیستم‌های عامل قابل اعتماد
- بررسی هسته امنیتی سیستم عامل مالتیکس

۶. کانال‌های نهان و تحلیل آنها
- جداسازی ماشین‌های مجازی و جعبه شنی
- تشخیص و تحلیل کانال‌های نهان
- حذف کانال‌های نهان

۷. تضمین و ارزیابی امنیت سیستم‌ها
- اصول طراحی سیستم‌های امن
- مفاهیم مرتبط با تضمین امنیت
- استانداردهای TCSEC و CC
- معرفی چند پروفایل حفاظت

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال ۳۰ درصد

آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. S. William and L. Brown. Computer security: principles and practice. Pearson, 2015.
2. M. Bishop, Computer Security, Art and Science, 2nd Edition, Addison-Wesley, 2019.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: امنیت پایگاه داده			
عنوان درس به انگلیسی:	Database Security		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☑ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☐ نظری-عملی ☐
تعداد ساعت:	٤٨		پروژه/ رساله / پایان‌نامه ☐
			مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☐ مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- بررسی نکات منطقی در مورد امنیت پایگاه داده‌ها

اهداف ویژه:

۱. بررسی مدل‌های کنترل دسترسی (اختیاری، اجباری و نقش-مبنا)

۲. بررسی مدل‌سازی سیستم‌های پایگاه داده‌ها همراه با نکات پیاده‌سازی مانند تجزیه ناپذیری ((atomicity، پی‌درپی سازی ((serialization، و کنترل مبتنی بر دیدگاه ((View

پ) سرفصل‌ها:

۱. مقدمه‌ای بر پایگاه داده‌ها و نیازهای امنیتی (یکپارچگی پایگاه داده و صحت، قابلیت بازرسی، کنترل دستیابی، تصدیق اصالت کاربر، دسترسی پذیری، قابلیت اعتماد)

۲. مدل‌های امنیتی
   - کنترل دسترسی
   - مسأله استنتاج و کانال‌های نهان
   - خط‌مشی باز در مقابل بسته
   - کنترل دسترسی اختیاری در مقابل اجباری

۳. مدل‌های کنترل دسترسی اختیاری

۴. مدل‌های کنترل دسترسی اجباری
   - مدل‌های حفظ محرمانگی عمومی
   - مدل‌های حفظ صحت عمومی
   - مدل‌های کنترل دسترسی پایگاه‌داده‌های چند سطحی (از بُعد محرمانگی و صحت)
   - معماری DBMS امن چندسطحی

۵. مدل‌های کنترل دسترسی نقش-مبنا و مدیریت آنها

- کنترل دسترسی در پایگاه‌داده‌های شیئ‌گرا

۶. معماری‌های امن پایگاه داده

۷. برونسپاری امن پایگاه داده‌ها

۸. مطالعه موردی (مکانیزم‌های امنیتی در نسخ مختلف اوراکل)

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. G. Blokdyk, Database Security A Complete Guide, 5STARCooks, 2019.
2. S. Castano, M. G. Fugini, G. Martella, and P. Samarati, "Database Security," Addison-Wesley, 1996.
3. E. Bertino and R.. Sandhu, "Database Security – Concepts, Approaches, and Challenges," IEEE Transaction on Dependable and Secure Computing, vol. 2, no. 1, 2005.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: امنیت نرم افزار			
عنوان درس به انگلیسی:	Software Security		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☑ عملی ☐
تعداد واحد:	۳	حل تمرین: ☑	تخصصی اختیاری ☐ نظری-عملی ☐
			پروژه/ رساله / پایان‌نامه ☐
تعداد ساعت:	٤٨		مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☐ / مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- بررسی مفاهیم روش‌ها و ابزارهای ایجاد ناامنی در سامانه‌های نرم‌افزاری توسط نفوذگران
- بررسی روش‌های مقابله با تهدیدات امنیتی

اهداف ویژه:

۱. بررسی چالش‌هایهای امنیتی اصلی در نرمافزارها و دلائل ریشه‌ای آن‌ها

۲. بررسی روش‌ها، رهیافت‌ها، اصول و ابزارهای لازم برای تشخیص و جلوگیری از چالش‌های امنیتی در نرم افزارها

پ) سرفصل‌ها:

۱. مقدمه، تعریف مفاهیم و تبیین اهمیت امنیت نرم افزار
۲. حمله به حافظه: چرا و چگونه؟
۳. حملات و دفاع‌های پایه سرریز بافر
۴. حملات و دفاع‌های پیشرفته سرریز بافر
۵. سایر حملات و دفاع‌های حافظه (ROP، JOP، Action scrip و...)
۶. تشخیص و جلوگیری از حملات حافظه
۷. انواع حملات و دفاع‌های وب
۸. تامین امنیت وب از طریق خط مشی هم منشأی
۹. ردیابی کاربران در وب
۱۰. کلیک ربائی

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. M. Payer, Software Security: Principles, Policies, and Protection (SS3P)- https://nebelwelt.net/SS3P/softsec.pdf
2. R. J Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems 3rd Edition 2020, ISBN-13: 978-0470068526 (https://www.cl.cam.ac.uk/~rja14/book.html)
3. P. Oorschot, Computer Security and the Internet: Tools and Jewels 2020, ISBN-13: 978-0134085043 (https://people.scs.carleton.ca/~paulv/toolsjewels.html)
4. K. Kaspersky, Hacker Disassembling Uncovered, 2nd Edition, ISBN 978-1931769648
5. A. Hoffman, Web Application Security: Exploitation and Countermeasures for Modern Web Applications 2020, O'Reilly Media

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: مدیریت امنیت اطلاعات			
عنوان درس به انگلیسی:	Information Security Management		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☑ عملی ☐
تعداد واحد:	۳	حل تمرین: ☑	تخصصی اختیاری ☐ نظری-عملی ☐
			پروژه/ رساله / پایان‌نامه ☐
تعداد ساعت:	٤٨		مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☐ / مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- شناخت مفاهیم امنیت و اطلاعات در سه سطح تصمیم‌سازی (راهبردی)، مدیریتی (تاکتیکی) و فنی (تکنیکی)

اهداف ویژه:

۱. تبیین روش‌های نوین طرح‌ریزی امنیت اطلاعات
۲. اشراف بر مفهوم پروتکل و نقش و جایگاه بی‌بدیل آن در تأمین امنیت اطلاعات
۳. شناخت تحلیلی پروتکل‌های ISO 27000 در حوزه‌ی امنیت اطلاعات

پ) سرفصل‌ها:

۱. نگاهی کلی به سیستم مدیریت امنیت اطلاعات
۲. استانداردهای سیستم مدیریت امنیت اطلاعات
۳. تبیین استاندارد ISO/IEC 27001
۴. مدیریت مخاطرات در سیستم مدیریت امنیت اطلاعات
۵. الزامات مستندسازی سیستم مدیریت امنیت اطلاعات
۶. ممیزی سیستم مدیریت امنیت اطلاعات

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. M Ibrahim, Securing Excellence: A Guide to ISO 27001:2022 Information Security Standards: A Leader's Roadmap to Success with Simplified ISO 27001 and Information Security Management System Requirements, Kindle Edition, 2023
2. M. E. Whitman and H. J. Mattord, Management of Information Security, Cengage Learning, 6th ed., 2018.
3. ISO/IEC 27000, information security management systems - overview and vocabulary
4. ISO/IEC 27001, information security management systems – Requirements
5. ISO/IEC 27002, good practice for information security controls
6. ISO/IEC 27003, guidance for implementing an ISMS based on ISO 27001
7. ISO/IEC 27004, information security management – measurement
8. ISO/IEC 27005, information security risk management
9. ISO/IEC 27031, guidelines for information and communication technology (ICT) readiness for Business Continuity

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: پروتکل‌های امنیتی			
عنوان درس به انگلیسی:	Security Protocols		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☑ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☐ نظری-عملی ☐
تعداد ساعت:	٤٨		پروژه/ رساله / پایان‌نامه ☐
			مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☐ مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- معرفی انواع پروتکل‌های امنیتی
- ممعرفی حمله به پروتکل و دفاع از آن
- **اهداف ویژه:**

۱. معرفی پروتکل‌های تبادل کلید
۲. معرفی پروتکل‌های تصدیق اصالت و امضا
۳. حقوق الکترونیکی
۴. رای گیری الکترونیکی

پ) سرفصل‌ها:

۱. مقدمه
- تعریف پروتکل امن
- انواع پروتکل‌های امن
- حمله به پروتکل

۲. بلوک‌های سازنده پروتکل‌های امن
- استفاده از توابع امنیتی
- رمزنگاری متقارن
- توابع یک طرفه
- توابع نامتقارن
- امضای رقمی
- امضای رقمی کور
- امضای رقمی یکبارمصرف

- طرح‌های امضای رقمی غیر قابل انکار
- طرح‌های امضای رقمی رد- توقف

۳. پروتکل‌های ساده
- پروتکل‌های مبادله کلید
- تصدیق اصالت
- تصدیق اصالت رمزشده
- رمزنگاری با کلید عمومی چندگانه
- تقسیم و اشتراک راز

۴. پروتکل‌های متوسط
- سرویس‌های مهر زمانی
- کانال نهان
- امضای رقمی با قابلیت عدم انکار
- امضای با تاییدکننده مشخص
- امضای نیابتی و گروهی
- محاسبه با اطلاعات رمزشده
- تعهد به مقدار بیت
- طرح‌های سکه‌اندازی منصفانه

۵. پروتکل‌های پیشرفته
- طرح‌های تصدیق هویت
- اثبات صفردانش
- امضای پول
- رمزنگاری کلید عمومی مبتنی بر هویت
- انتقال بی‌خبر
- امضای بی‌خبر
- امضای قرارداد به صورت توأمان
- نامه سفارشی

۶. پروتکل‌های خاص
- انتخابات امن
- محاسبات چندطرفه امن
- پخش بی‌نام پیام
- پول دیجیتال
- ریزپرداخت

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1- G. Blokdyk, Security Protocol A Complete Guide, 2021.
2- D. R. Stinson, *Cryptography: theory and practice*. Chapman and Hall/CRC, 2018
3- B. Schnider, *Applied cryptography protocols, algorithms and source code in C*, Wiely, 20th Anniversary Edition, 2015.
4- J. Seberry, and J. Pieprzyk, *Cryptography: An Introduction to Computer Security*, Prentice-Hall, 1992.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: امنیت شبکه			
عنوان درس به انگلیسی:	Network Security		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی☑ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☐ نظری-عملی ☐
تعداد ساعت:	٤٨		پروژه/ رساله / پایان‌نامه ☐
			مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☐ مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- درک عمیق‌تر دانشجویان از شبکه‌های اطلاعاتی

اهداف ویژه:

۱. بررسی جنبه‌های عملی امنیت شبکه

۲. تبیین راهکارهای برقراری امنیت در لایه‌های مختلف شبکه

پ) سرفصل‌ها:

۱. مقدمه مشتمل بر تعاریف و اصطلاحات، مولفه‌های امنیت، انواع و ماهیت حملات، مکانیزم‌ها و سرویس‌های امنیتی

۲. کاربردهای رمزنگاری در پروتکل‌های امنیت شبکه، روش‌های توزیع کلید در شبکه‌های ثابت، سیار، و موردی، روش‌های بینامی و ناشناسی، زنجیره بلوکی و کاربردهای آن در امنیت شبکه

۳. کنترل دسترسی در سیستم و شبکه (NAC) و معماری‌های آن

۴. روش‌های جلوگیری از نشت و از بین رفتن اطلاعات (DLP)

۵. امنیت مسیریابی

۶. امنیت در لایه‌ی پیوند داده و لایه‌ی شبکه مشتمل بر شنود و روش‌های مقابله در سوئیچ‌ها، جعل آدرس، شبکه های اختصاصی مجازی، IPSEC، L2TP

۷. امنیت در لایه‌ی انتقال، SSL، NAT

۸. پویش، حملات از کاراندازی سرویس، دیواره‌های آتش حالتمند

۹. امنیت لایه‌ی کاربرد، امنیت وب، پست الکترونیکی، ساختار PKI

۱۰. آشنایی با سامانه‌های کشف و مقابله با نفوذ و انواع آنها

۱۱. تحمل پذیری خطا در تجهیزات شبکه

۱۲. کانال‌های پنهان و روش‌های جلوگیری از آنها

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. W. Stallings, Cryptography and Network Security: Principles and Practice, Global edition, Pearson, 2022.
2. M. Stamp, Information Security: Principles and Practice, 3rd edition, John Wiley and Sons, 2021.
3. W. Stallings, Network Security Essentials: Applications and Standards, 6th edition, Prentice Hall, 2017.
4. M. Ciampa, Security+ Guide to Network Security Fundamentals, Cengage Learning, 2015.
5. S. McClure, J. Scambray and G. Kurtz, Hacking Exposed 7: Network Security Secrets & Solutions, 7th edition, 2012.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: محاسبات امن			
عنوان درس به انگلیسی:	Secure Computations	نوع درس و واحد	
دروس پیش‌نیاز:	رمزنگاری کاربردی	پایه ☐	نظری ☑
دروس هم‌نیاز:		تخصصی الزامی ☐	عملی ☐
تعداد واحد:	۳	تخصصی اختیاری ☑	نظری-عملی ☐
	حل تمرین: ☐	پروژه/ رساله / پایان‌نامه ☐	
تعداد ساعت:	٤٨	مهارتی-اشتغال پذیری ☐	
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)		مرتبط با آمایش/مأموریت موسسه نیست ☑	مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- بررسی انواع روش‌های انجام محاسبات به صورت امن و کاربردهای آن‌ها

اهداف ویژه:

۱. پیاده‌سازی امن حراج امن
۲. رای گیری الکترونیکی امن
۳. داده‌کاوی امن

پ) سرفصل‌ها:

۱. معرفی پروتکل‌های مقدماتی رمزنگاری
۲. معرفی پروتکل‌ها و روش‌های صفر دانش
۳. پروتکل‌های محاسبات دوسویه‌ی امن: روش مبتنی بر تسهیم راز، روش استفاده از مدارهای آشفته
۴. پروتکل‌های محاسبات چندسویه‌ی امن
۵. مدل امنیتی شبه‌درستکار در محاسبات چندسویه‌ی امن
۶. مدل امنیتی بدخواه در محاسبات چندسویه‌ی امن
۷. معرفی انواع مسایل موجود در حوزه‌ی محاسبات چندسویه‌ی امن
۸. راه حل‌های عمومی برای محاسبات چندسویه‌ی امن، مسئله‌ی میلیونرها و روش‌های عمومی حل آن
۹. محاسبه‌ی اشتراک و اجتماع مجموعه‌های محرمانه
۱۰. راه حل های خاص برخی دیگر از مسایل موجود در حوزه‌ی محاسبات چندسویه ی امن

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1- A. Choudhury and A. Patra, Secure Multi-Party Computation Against Passive Adversaries, Springer, 2022
2- M. M. Prabhakaran and A. Sahai, Secure Multi-Party Computation IOS Press, 2013.
3- I. Damagard, R. Cramer, and J. B. Nielsen. "Secure multiparty computation and secret sharing." (2015).
4- C. Hazay and Y. Lindell, Efficient Secure Two-Party Protocols, Techniques and Constructions, Springer, 2013.
5- Y. Lindell, Composition of Secure Multiparty Protocols: A Comprehensive Study, Springer, 2003

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

<table>
<tr><td colspan="5">الف: عنوان درس به فارسی: حریم خصوصی</td></tr>
<tr><td>عنوان درس به انگلیسی:</td><td colspan="2">Privacy</td><td colspan="2">نوع درس و واحد</td></tr>
<tr><td>دروس پیش‌نیاز:</td><td colspan="2"></td><td colspan="2">پایه ☐ نظری ☑</td></tr>
<tr><td>دروس هم‌نیاز:</td><td colspan="2"></td><td colspan="2">تخصصی الزامی ☐ عملی ☐</td></tr>
<tr><td rowspan="3">تعداد واحد:</td><td rowspan="3">۳</td><td rowspan="3">حل تمرین: ☐</td><td colspan="2">تخصصی اختیاری ☑ نظری-عملی ☐</td></tr>
<tr><td colspan="2">پروژه/ رساله / پایان‌نامه ☐</td></tr>
<tr><td colspan="2">مهارتی-اشتغال پذیری ☐</td></tr>
<tr><td rowspan="2">تعداد ساعت:</td><td rowspan="2">۴۸</td><td rowspan="2"></td><td colspan="2" rowspan="2"></td></tr>
<tr><td colspan="3">وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)</td><td>مرتبط با آمایش/مأموریت موسسه نیست ☑</td><td>مرتبط با مأموریت/آمایش موسسه است ☐</td></tr>
</table>

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- ارائه چالش‌ها و تهدیدهای مختلف مرتبط با حریم خصوصی کاربران در محیط‌های رایانشی و کاربردهای مختلف

اهداف ویژه:

۱. تبیین حریم خصوصی و نیازمندی‌های آن
۲. بررسی تکنیک‌های حفظ حریم خصوصی

پ) سرفصل‌ها:

۱. معرفی حریم خصوصی و نیازمندی‌های حریم خصوصی
۲. معرفی پروتکل‌های رمزنگاری تامین‌کننده حریم خصوصی
۳. آشنایی با کاربردهای مختلف مبتنی بر حریم خصوصی: عملیات مجموعه‌ای (مانند اجتماع و اشتراک) با حفظ حریم خصوصی، تحلیل آماری با حفظ حریم خصوصی، محاسبات هندسی با حفظ حریم خصوصی، تشخیص نفوذ با حفظ حریم خصوصی، داده‌کاوی با حفظ حریم خصوصی، محاسبات علمی با حفظ حریم خصوصی، پرس‌وجو از پایگاه داده‌ها با حفظ حریم خصوصی و غیره
۴. امنیت و حریم خصوصی در کاربردهای اینترنت
۵. حریم خصوصی در کاربردهای آگاه از اطلاعات زمینه (Context-aware application)
۶. حریم خصوصی در سرویس‌های مبتنی بر مکان (Location-based services)
۷. معرفی فناوری‌های تامین‌کننده حریم خصوصی (PET: Privacy Enhancing Technology)
۸. حریم خصوصی در مانیتورینگ ترافیک جاده‌ها
۹. حریم خصوصی در کاربردهای داده‌کاوی و تکنیک‌های تامین‌کننده حریم خصوصی در داده‌کاوی
۱۰. مدل‌های گمنامی برای حریم خصوصی داده
۱۱. حملات استنتاج در انتشار داده
۱۲. مدل گمنامی مرتبه k

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. K. Jarmul, Practical Data Privacy, O'Reilly Media, 2023.
2. M. Mokbel, Privacy Preserving Location Services, Tutorial, ICDM 2008.
3. D. B. Rawat, B. B. Bista and G.Yan, Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications, 2013.
4. M. Hay, G. Miklau, D. Jensen and D. Towsley, Resisting Structural Re-identification in Anonymized Social Networks, 2010.
5. S. Gritzalis, T. Karygiannis and C. Skianis, Security and Privacy in Mobile and Wireless Networking, 2009.
6. J. Joshi, Network Security: Know It All, Elsevier, 2008.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: امنیت رایانش ابری			
عنوان درس به انگلیسی:	Cloud Computing Security		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☐ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☑ نظری-عملی ☐
تعداد ساعت:	٤٨		پروژه/ رساله / پایان‌نامه ☐
			مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☑ / مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- معرفی چالش‌ها، مسائل و ویژگی‌های اساسی رایانش ابری
- **اهداف ویژه:**

۱. بررسی مسائل امنیتی و حریم خصوصی مرتبط و راهکارهایی برای رسیدگی به این مسائل

۲. بررسی مساله کنترل دسترسی به داده‌های ابری

پ) سرفصل‌ها:

۱. مقدمه‌ای بر رایانش ابری
۲. مدل‌های ابر و مدل‌های تهدید
۳. امنیت زیرساخت (Infrastructure Security)
۴. امنیت داده و حافظه (Data Security and Storage)
۵. مدیریت دسترسی و شناسه‌ها
۶. حریم خصوصی
۷. راه‌حل‌های موجود
۸. کنترل دسترسی در رایانش ابری

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. J. R. Vacca, Cloud Computing Security: Foundations and Challenges, CRC Press, 2020.
2. R. L. Krutz and R. D. Vines, Cloud security a comprehensive guide to secure cloud computing. Wiley, 2010.
3. B. Bhargava, A. Kim and Y. Cho, Research in Cloud Security and Privacy, Computer Science. Purdue University, last visit on August 2023.
4. منابع الکترونیکی

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: رمزنگاری کاربردی			
عنوان درس به انگلیسی:	Applied Cryptography		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☐ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☑ نظری-عملی ☐
تعداد ساعت:	٤٨		پروژه/ رساله / پایان‌نامه ☐
			مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست☑ / مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- مطالعه توابع محافظت از اطلاعات
- اصول طراحی و تحلیل توابع محافظت از اطلاعات

اهداف ویژه:

۱. استفاده از توابع محافظت از اطلاعات به منظور حفظ محرمانگی پیام
۲. استفاده از توابع محافظت از اطلاعات به منظور تصدیق اصالت پیام
۳. استفاده از توابع محافظت از اطلاعات به منظور حفظ صحت پیام

پ) سرفصل‌ها:

۱. مقدمه
   - نیاز به خدمت‌های امنیتی در سیستم‌های کامپیوتری و ارتباطی
   - مفاهیم پایه :امنیت مطلق، امنیت عملی، سناریوهای حمله
۲. پیش زمینه‌های لازم
   - نظریه اطلاعات، نظریه اعداد، و نظریه پیچیدگی
   - ایهام کلید، فاصله یگانگی، و مدل رمز تصادفی (random cipher)
۳. رمزنگاری کلاسیک
   - سیستم‌های رمز چندالفبایی و تحلیل آن‌ها
۴. سیستم‌های رمزنگار مدرن
   - سیستم‌های رمزنگاری دنباله‌ای و قالبی
   - انواع سیستم‌های رمز دنباله‌ای
   - ساختار سیستم‌های رمزنگار قالبی
   - معرفی سیستم‌های رمزنگار مدرن DES و ویژگی‌های آن

- معرفی AES، RC5، Blowfish، IDEA، FEAL و Serpent

۵. تحلیل الگوریتم‌های رمز قالبی و روش‌های تحلیل خطی و تفاضلی
- مقدمه‌ای بر تحلیل
- تحلیل خطی و تحلیل تفاضلیDES

۶. ویژگی‌ها و طراحی S-box مطلوب الگوریتم‌های رمزنگاری

۷. رمزنگاری با کلید عمومی
- توصیف الگوریتم‌های با کلید عمومی، دیفی هلمن، RSA و بررسی امنیت آن، رمز ویلیامز، رمز الجمال
- سیستم‌های رمز با مسئله کوله‌پشتی
- رمزهای با کدهای جبری، رمزنگاری خم بیضوی و تحلیل آن‌ها

۸. تولید اعداد اول
- روش‌های قطعی و احتمالاتی
- آزمون ضعیف
- آزمون قوی
- الگوریتم تجزیه اعداد

۹. تصدیق اصالت و صحت داده‌ها
- مفاهیم پایه
- طرح تصدیق اصالت فیات -شامیر، الجمال،RSA
- مسئله زندانبان و کانال نهان، طرح‌های کانال نهان، توابعMAC
- طرح‌های تصدیق اصالت

۱۰. امضای رقمی
- انواع پروتکل‌های امن، مفاهیم پایه امضای رقمی، طرح‌های امضای رقمی ساده، طرح رابین، طرح ماتیاس، امضای RSA و انواع آن و نقاط ضعف
- طرح امضایDSS

۱۱. طرح‌های توابع چکیده‌ساز امن
- طرح‌های ساده
- پارادوکس روز تولد و تحلیل توابع چکیده‌ساز
- حمله تلاقی در میان و راهکارهای مقاوم‌سازی
- توابع MD5 ، SHA ، RIPEMD ، توابع چکیده‌ساز کلیددار و بی‌کلید
- استفاده از توابع چکیده‌ساز به صورت موازی و سریال

۱۲. مدیریت کلید، مدول امن، کلیدگذاری چندلایه، دفترچه راهنمای کلید عمومی، گواهی و مرجع گواهی

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. T. Himanshu and S. Watanabe, Information-theoretic Cryptography. Cambridge University Press, 2023.
2. S. Douglas R, Cryptography: theory and practice. Chapman and Hall/CRC, 2018
3. J. Seberry and J. Pieprzyk, Cryptography: An Introduction to Computer Security, Prentice-Hall, 1992.
4. B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, John-Wiley & Sons Inc., 20th Anniversary Edition, 2015.
5. C. H. Meyer and S. M. Metyas, Cryptography: A New Dimension in Computer Data Security, John-Wiley & Sons Inc., 1982.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: تحلیل و وارسی صوری امنیت			
عنوان درس به انگلیسی:	Formal Security Analysis and Verification		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☐ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☑ نظری-عملی ☐
			پروژه/ رساله / پایان‌نامه ☐
تعداد ساعت:	٤٨		مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☑ / مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- بررسی روش‌های مدل‌سازی، تحلیل و وارسی ویژگی‌های امنیتی به ویژه با رویکرد صوری در سامانه‌های اطلاعاتی
- **اهداف ویژه:**

۱. معرفی نحوه استفاده از روش‌های صوری در تحلیل و وارسی صوری پروتکل‌های امنیتی

۲. مدل‌سازی و تحلیل آسیب‌پذیری‌های امنیتی نرم افزار

پ) سرفصل‌ها:

۱. تبیین مفاهیم، ضرورت و جایگاه وارسی صوری در امنیت سامانه‌ها
۲. مروری بر منطق ریاضی و اثبات خودکار قضیه
۳. بررسی مدل (مدل‌های حالت محدود، منطق زمانی، الگوریتم‌های جستجو، بررسی مدل نمادی)
۴. توصیف و وارسی پروتکل‌های امنیتی
۵. توصیف و وارسی خط مشی‌های کنترل دسترسی
۶. مدل سازی نرم افزار و وارسی ویژگی‌های امنیتی برنامه‌ها
۷. تحلیل امنیت جریان اطلاعات
۸. آشنائی با برخی ابزارهای وارسی صوری امنیت

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. M. Kaufmann, P. Manolios and J. S. Moore, Computer Aided Reasoning: An Approach, Kluwer Academic Publishers, 3rd edition, 2011.
2. A. Datta, S. Jha, N. Li, D. Melski, and T. Reps, Analysis Techniques for Information Security, Morgan & Claypool, 2010.
3. C. Baier and J. Katoen, Principles of Model Checking, MIT Press, 2008.
4. M. Bishop, Computer Security: Art and Science, Addison-Wesley, 2018.
5. P. Ryan, S. Schneider, M. Goldsmith, G. Lowe and B. Roscoe, Modeling and Analysis of Security Protocols, Addison-Wesley, 2001.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

<table>
<tr><td colspan="5">الف: عنوان درس به فارسی: جرم‌یابی کامپیوتری</td></tr>
<tr><td colspan="2">عنوان درس به انگلیسی:</td><td colspan="2">Computer Forensics</td><td rowspan="2">نوع درس و واحد</td></tr>
<tr><td colspan="2">دروس پیش‌نیاز:</td><td colspan="2"></td></tr>
<tr><td colspan="2">دروس هم‌نیاز:</td><td colspan="2"></td><td>پایه ☐ نظری ☑</td></tr>
<tr><td rowspan="3">تعداد واحد:</td><td rowspan="3">حل تمرین: ☐</td><td>۳</td><td>تخصصی الزامی ☐</td><td>عملی ☐</td></tr>
<tr><td rowspan="2">تعداد ساعت:</td><td rowspan="2">۴۸</td><td>تخصصی اختیاری ☑</td><td>نظری-عملی ☐</td></tr>
<tr><td colspan="2">پروژه/ رساله / پایان‌نامه ☐</td></tr>
<tr><td colspan="3">وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)</td><td colspan="2">مهارتی-اشتغال پذیری ☐</td></tr>
<tr><td colspan="3">مرتبط با آمایش/مأموریت موسسه نیست☑</td><td colspan="2">مرتبط با مأموریت/آمایش موسسه است ☐</td></tr>
</table>

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- بررسی مفاهیم و روش‌های تحلیل رسانه‌های دیجیتال
- **اهداف ویژه:**

۱. تحلیل نرم‌افزارهای بدخواه
۲. تحلیل لاگ‌های شبکه
۳. تحلیل حافظه
۴. پیجویی نفوذهای یافته شده بر روی سیستم عامل ویندوز و متدولوژی‌های رهیابی آنها

پ) سرفصل‌ها:

۱. مقدمه
   - منابع و انواع شواهد دیجیتال
   - مباحث حقوقی فورنسیک کامپیوتری
۲. جمع‌آوری شواهد کامپیوتری از رسانه‌های مختلف

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. E. Casey, Digital evidence and computer crime, Academic Press, 2011.
2. R. P. J. Evans, Windows 10 forensic analysis, Blurb, 2017.
3. P. Polstra, Linux forensics, Penster Academy, 2015.
4. C. Chad Tilbury, R. Lee and M. Pilkington, FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics, SANS Institute, 2022.
5. P. Hagen and M. Oldham, FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response, SANS Institute, 2022.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

<table>
<tr><td colspan="5">الف: عنوان درس به فارسی: رمزنگاری پیشرفته</td></tr>
<tr><td colspan="2">عنوان درس به انگلیسی:</td><td colspan="2">Advanced Cryptography</td><td rowspan="2">نوع درس و واحد</td></tr>
<tr><td colspan="2">دروس پیش‌نیاز:</td><td colspan="2"></td></tr>
<tr><td colspan="2">دروس هم‌نیاز:</td><td colspan="2"></td><td>پایه ☐ نظری ☑</td></tr>
<tr><td rowspan="3">تعداد واحد:</td><td rowspan="3">۳</td><td rowspan="3">حل تمرین: ☐</td><td>تخصصی الزامی ☐</td><td>عملی ☐</td></tr>
<tr><td>تخصصی اختیاری ☑</td><td>نظری-عملی ☐</td></tr>
<tr><td colspan="2">پروژه/ رساله / پایان‌نامه ☐</td></tr>
<tr><td>تعداد ساعت:</td><td>۴۸</td><td colspan="3">مهارتی-اشتغال پذیری ☐</td></tr>
<tr><td colspan="3">وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)</td><td>مرتبط با آمایش/مأموریت موسسه نیست ☑</td><td>مرتبط با مأموریت/آمایش موسسه است ☐</td></tr>
</table>

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- تبیین مباحث پیشرفته در حوزه رمزنگاری
- **اهداف ویژه:**

۱. تعریف صوری رمزنگاری و مدل‌های امنیت

۲. ساختارهای پایه

۳. مباحث مربوط به رمزنگاری کوانتومی

پ) سرفصل‌ها:

۱. ریاضیات رمزنگاری
   - مروری بر نظریه پیچیدگی اطلاعات و کاربردهای آن در رمزنگاری
   - نظریه اعداد :دستگاه معادلات همنهشتی و قضایای مربوط به آن، اعداد اول، ریشه‌های اولیه، نمادهای لژاندر و ژاکوبی، مسئله لگاریتم گسسته
   - نظریه گروه :هم‌مجموعه‌ها و روابط هم‌ارزی در گروه‌ها، زیرگروه‌های نرمال، گروه‌های خارج قسمتی
   - نظریه حلقه و میدان :حلقه چندجمله‌ای‌ها، حلقه‌های خارج قسمتی، میدان‌های متناهی، توسعه میدان‌ها و چند جمله‌ای‌ها
۲. تعریف صوری رمزنگاری و مدل‌های امنیت
   - رمزنگاری بدون شرط
   - امنیت پیچیدگی
   - امنیت قابل اثبات
   - امنیت محاسباتی
۳. ساختارهای پایه
   - توابع یک طرفه

- توابع دریچه‌ای یک طرفه
- مولد شبه تصادفی
- توابع شبه تصادفی
- جایگشت‌های یک طرفه

۴. اثبات‌های صفردانش
- رمزنگاری همریخت
- رمزنگاری مبتنی بر ویژگی
- بازیابی محرمانه اطلاعات

۵. رمزنگاری پساکوانتومی
- مقدمه‌ای بر محاسبات کوانتومی
- مسئله پاسخ صحیح کوتاه (SIS)
- توابع چکیده‌ساز مبتنی برSIS
- امضاهای مبتنی بر مشبکه
- مسئله یادگیری با وجود خطا (LWE)

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. D. Boneh, and V. Shoup, A Graduate Course in Applied Cryptography, Stanford University, 2023.
2. D. R. Stinson, Cryptography: Theory and Practice, 4rd edition, CRC Press, 2018.
3. J. A. Anderson and J. M. Bell, Number Theory with Applications, Prentice Hall, 1997.
4. Selected Papers

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: مبانی فناوری بلاکچین			
عنوان درس به انگلیسی:	Foundations of Blockchain Technology		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☐ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☑ نظری-عملی ☐
تعداد ساعت:	٤٨		پروژه/ رساله / پایان‌نامه ☐
			مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☑ / مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- ارائه مبانی نظری قوی در حوزه بلاکچین
- **اهداف ویژه:**

۱. ارائه یک درک جامع از مفاهیم بنیادی بلاکچین

۲. پروتکل بیت کوین

۳. ساختارهای داده

۴. مکانیزم های اجماع

پ) سرفصل‌ها:

۱. مقدمه ای بر فناوری بلاکچین، تاریخچه و کاربردها

۲. پروتکل بیت کوین

۳. ساختارهای داده در بلاکچین (زنجیره‌های خطی، درخت مرکل، گراف‌های غیرمتمرکز)

۴. انواع سازوکارهای اجماع (PoW, PoS, DPoS, BFT)

۵. پروتکل‌های شبکه، گره‌ها و توپولوژی شبکه در بلاکچین

۶. انواع کیف پول‌های سخت‌افزاری، نرم‌افزاری، کاغذی، سلسله مراتبی، (SPV)

۷. چالش‌های مقیاس پذیری و راهکارهای ارائه شده

۸. تراکنش‌های خارج از زنجیره و کانال‌های پرداخت

۹. مقایسه تطبیقی ارزهای دیجیتال مطرح

۱۰. توکن‌ها، ایردراپ ها و عرضه اولیه سکه(ICO)

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. A. M. Antonopoulos, Mastering Bitcoin: Programming the Open Blockchain, O'Reilly Media, 2017.
2. A. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 2016.
3. D. Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, Apress, 2017.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: طراحی سامانه‌های مبتنی بر بلاکچین			
عنوان درس به انگلیسی:	Design of Blockchain-based Systems	نوع درس و واحد	
دروس پیش‌نیاز:		پایه ☐	نظری ☑
دروس هم‌نیاز:		تخصصی الزامی ☐	عملی ☐
تعداد واحد: ۳	حل تمرین: ☐	تخصصی اختیاری ☑	نظری-عملی ☐
		پروژه/ رساله / پایان‌نامه ☐	
تعداد ساعت: ٤٨		مهارتی-اشتغال پذیری ☐	
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)		مرتبط با آمایش/مأموریت موسسه نیست ☑	مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- تقویت توانایی دانشجویان در طراحی و پیاده سازی سیستم های غیرمتمرکز مبتنی بر فناوری بلاکچین با تمرکز بر پلتفرم اتریوم
- **اهداف ویژه:**

۱. تبیین جزئیات معماری اتریوم
۲. مفاهیم پیشرفته قراردادهای هوشمند
۳. چالش‌های طراحی سیستم‌های بلاکچینی در مقیاس وسیع

پ) سرفصل‌ها:

۱. معرفی پلتفرم اتریوم و تفاوت‌های آن با بیت‌کوین
۲. معماری اتریوم، ماشین مجازی (EVM) و مفهوم گس(Gas)
۳. زبان Solidity و آموزش برنامه نویسی قراردادهای هوشمند
۴. الگوهای طراحی و معماری در توسعه قراردادهای هوشمند
۵. مدل های دسترسی و کنترل در سیستم‌های بلاکچینی
۶. چارچوب‌های حاکمیتی غیرمتمرکز (DAO) و مکانیزم‌های رأی‌گیری
۷. مقیاس‌پذیری لایه اول و دوم (Sharding, Plasma, State Channels)
۸. قابلیت همکاری بین زنجیره‌ای و ارتباط با سیستم‌های سنتی
۹. سازوکارهای حفظ حریم خصوصی تراکنش‌ها
۱۰. پروژه عملی: طراحی معماری یک سیستم غیرمتمرکز مبتنی بر اتریوم

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. A. M. Antonopoulos and G. Wood, Mastering Ethereum: Building Smart Contracts and DApps, O'Reilly Media, 2019.
2. X. Xu, I. Weber and M. Staples, Architecture for Blockchain Applications, Springer, 2019.
3. K. Solorio, R. Kanna and D. Hoover, Hands-On Smart Contract Development with Solidity and Ethereum: From Fundamentals to Deployment, O'Reilly Media, 2019.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: تحلیل بدافزار			
عنوان درس به انگلیسی:	Malware Analysis		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☐ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☑ نظری-عملی ☐
تعداد ساعت:	٤٨		پروژه/ رساله / پایان‌نامه ☐
			مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☑ / مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- بررسی مفاهیم، معماری و روش‌های مورد استفاده در بدافزارها
- معرفی رویکردها و ابزارهای تشخیص و تحلیل بدافزارها
- **اهداف ویژه:**

۱. تبیین ساختار و انواع بدافزارها و روش‌های بدخواهانه مورد استفاده در آنها

۲. انواع روش‌های تشخیص و تحلیل بدافزارها

پ) سرفصل‌ها:

۱. تاریخچه، تعاریف، دسته بندی و مفاهیم بدافزار
۲. بررسی معماری و تکنیک‌های مورد استفاده در بدافزارها
۳. تشریح موردی چند نمونه بدافزار
۴. روش‌های تشخیص بدافزار
۵. تحلیل ایستا (مهندسی معکوس)
۶. تحلیل پویا (زمان اجرا)
۷. روش‌های ضدتحلیل بدافزار و مقابله با آنها
۸. تکنیک های پیشرفته در بدافزارهای مدرن و روش های مقابله با آنها
۹. تشخیص الگو و کاربرد آن در تشخیص بدافزار

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. M. Sikorski and A. Honig, "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software", No Starch Press, 2012.
2. M. Ligh, S. Adair, B. Hartstein and M. Richard, "Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code", First Edition, Wiley Publications, 2010
3. A. Kleymenov and A. Thabet, Mastering Malware Analysis, Packt Publishing, 2022.
4. P. Szor, "The Art of Computer Virus Research and Defense", Addison-Wesley Professional, 2005
5. J. Aycock, "Computer Viruses and Malware" , Springer, 2006
6. E. Skoudis and L. Zeltser , "Malware: Fighting Malicious Code", Prentice Hall Publications, 2003

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: پنهان‌سازی اطلاعات			
عنوان درس به انگلیسی:	Information Hiding		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☐ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☑ نظری-عملی ☐
تعداد ساعت:	٤٨		پروژه/ رساله / پایان‌نامه ☐
			مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☑ / مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- ایجاد درک صحیح در ارتباط با موضوع اختفای اطلاعات و نکات امنیتی مطرح در آن
- **اهداف ویژه:**

۱. معرفی فنون نشانه‌گذاری و نهان‌نگاری و نیز کاربردهای مختلف آنها

۲. معرفی روش‌های مختلف نهان‌کاوی

پ) سرفصل‌ها:

۱. مقدمات و تعاریف اولیه
   - تعریف اختفای اطلاعات، نشانه‌گذاری، و نهان‌نگاری
   - تاریخچه و اهمیت

۲. کاربردها و شاخص‌های ارزیابی

۳. مرور مطالب پیش نیاز درس
   - آمار و احتمال
   - جبر خطی
   - امنیت

۴. نشانه‌گذاری
   - مدلسازی سیستم‌های نشانه‌گذاری
   - نشانه‌گذاری با اطلاعات جانبی
   - تحلیل خطا
   - استفاده از مدل‌های ادراکی
   - امنیت نشانه‌گذاری
   - تکنیک‌های نشانه‌گذاری مقاوم

- تأیید محتوا

۵. نهان‌نگاری
- اصول نهان‌نگاری و امنیت
- سیستم‌های جانشینی
- تکنیک‌های حوزه تبدیل
- طیف گسترده
- نهان‌نگاری آماری
- معرفی مهمترین روش‌های نهان‌نگاری

۶. نهان‌کاوی
- مفاهیم اولیه و انواع روش‌ها
- نهان‌کاوی در حوزه مکان و حوزه تبدیل
- نهان‌کاوی حین کدگذاری
- معرفی مهمترین روش‌های تحلیل نهان‌کاوی

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. I. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, Elsevier, Morgan Kaufmann Publishers, 2008.
2. H. T. Sencar, M. Ramkumar, and A. N. Akansu, Data Hiding Fundamentals and Applications Content Security in Digital Media, Elsevier Academic Press, 2004.
3. S. Katzenbeisser and F. A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, 2000.
4. I. Ahmad A. V. Bajaj, Data Hiding Fundamentals and Applications Content Security in Digital Media, IOP Science, 2021.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: سامانه‌های تشخیص نفوذ			
عنوان درس به انگلیسی:	Intrusion Detection Systems		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☐ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☑ نظری-عملی ☐
			پروژه/ رساله / پایان‌نامه ☐
تعداد ساعت:	٤٨		مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☑ / مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- تبیین سیستم‌های تشخیص و جلوگیری از نفوذ یا IDPS
- **اهداف ویژه:**

۱. معرفی روش‌های شناسایی و تشخیص و انواع روش‌های پیشگیری

۲. معرفی نحوه‌ی عملکرد و معماری سامانه‌های تشخیص و پیشگیری از نفوذ

پ) سرفصل‌ها:

۱. مروری بر انواع حملات

۲. مفاهیم و تعاریف سامانه‌های تشخیص نفوذ

۳. رهیافت‌های تشخیص نفوذ (مبتنی بر امضا، مبتنی بر ناهنجاری، مبتنی بر تحلیل حالت پروتکل ارتباطی)

۴. سامانه‌های تشخیص و مقابله با نفوذ مبتنی بر شبکه (نحوه‌ی جمع‌آوری اطلاعات، نحوه‌ی ثبت رویداد، قابلیت تشخیص، قابلیت پیشگیری

۵. سامانه‌های تشخیص و مقابله با نفوذ مبتنی بر میزبان

۶. سامانه‌های تشخیص و مقابله با نفوذ توزیع شده

۷. مدیریت هشدارها و همبستگی داده‌ها

۸. استفاده و مجتمع‌سازی فناوری‌های مختلف IDPS

۹. فناوری‌های دیگر با قابلیت IDPS شامل آنتی‌ویروس، دیواره آتش، ظرف عسل

۱۰. ارزیابی سیستم‌های تشخیص نفوذ
   - معیارهای ارزیابی
   - مجموعه‌های داده

۱۱. حملات علیه سامانه‌های تشخیص و مقابله با نفوذ (مانندکشف IDS، منع سرویس، دور زدن IDS)

۱۲. آشنایی با ابزارهایی مانند Snort و Bro

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. D. Hoelzer, Network Monitoring and Threat Detection In-Depth, SANS Institute, 2021.
2. K. Scarfone and P. Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), NIST Special Publication 800-94, Revision 1, 2012.
3. A. Ghorbani, W. Lu and M. Tavallaee, Network Intrusion Detection and Prevention: Concepts and Techniques, Springer, 2010.
4. R. Trost, Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century, Addison-Wesley Professional, 2009

۵. ا. ملکیان، نفوذگری در شبکه و روشهای مقابله، انتشارات نص، ۱۳۹۸.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: امنیت و اعتماد سخت افزار			
عنوان درس به انگلیسی:	Security and Trust of Hardware		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☐ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☑ نظری-عملی ☐
تعداد ساعت:	٤٨		پروژه/ رساله / پایان‌نامه ☐
			مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☑ / مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- تبیین محاسبات رمزنگاری و نحوه پیاده سازی کارآ، امن و قابل اعتماد آنها
- معرفی پیشرفت‌های اخیر در طراحی و ارزیابی امنیت سخت افزار و قابل اعتماد بودن آن
- **اهداف ویژه:**

۱. معرفی حملات فیزیکی

۲. معرفی راهکارهای مقابله با حملات فیزیکی

پ) سرفصل‌ها:

۱. تبیین مفاهیم رمزنگاری و امنیت

۲. بررسی حملات فیزیکی و مقابله‌ها
   - حملات تهاجمی
   - حملات نیمه‌تهاجمی
   - حملات غیرتهاجمی

۳. بررسی حملات کانال جانبی و مقابله‌ها
   - حملات کانال جانبی ساده
   - حملات کانال جانبی تفاضلی
   - حملات کانال جانبی همگرا

۴. تبیین تروجان‌های سخت‌افزاری
   - انواع تروجان‌ها
   - برخی روشهای کشف تروجان‌ها
   - برخی روش‌های مقاوم‌سازی (طراحی برای ایجاد قابلیت کشف)

۵. تبیین جعل سخت‌افزارها

- انواع جعل
- برخی روش‌های کشف و مقابله

۶. توابع غیرقابل همانندسازی فیزیکی (PUFs)
- انواع PUF
- مبتنی بر تاخیر
- مبتنی بر حافظه
- برخی کاربردها

۷. محاسبات مورد اعتماد (Trusted Computing) و TPM ها
۸. مولدهای عدد تصادفی مبتنی بر سختافزار
۹. تهنقش‌گذاری (Watermarking) بلوک‌های IP (Intellectual Property)
۱۰. طراحی مورداعتماد در FPGA ها
۱۱. امنیت سیستم‌های نهفته
۱۲. امنیت برچسب‌های Radio frequency identification (RFID)

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. N Sklavos, R. Chaves, G.D. Natale and F. Regazzoni, Hardware Security and Trust, Springer, 2017.
2. M. Tehranipoor and C. Wang, *Introduction to Hardware Security and Trust*, Springer, 2011.
3. H. Salmani, X. Zhang and M. Tehranipoor, *Integrated Circuit Authentication: Hardware Trojans and Counterfeit*, Springer, 2013
4. Selected journal or conference papers

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد

الف: عنوان درس به فارسی: امنیت سیستم‌های سایبرفیزیکی			
عنوان درس به انگلیسی:	Cyberphysical Systems Security	نوع درس و واحد	
دروس پیش‌نیاز:		پایه ☐	نظری ☑
دروس هم‌نیاز:		تخصصی الزامی ☐	عملی ☐
تعداد واحد: ۳	حل تمرین: ☐	تخصصی اختیاری ☑	نظری-عملی ☐
		پروژه/ رساله / پایان‌نامه ☐	
تعداد ساعت: ٤٨		مهارتی-اشتغال پذیری ☐	
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)		مرتبط با آمایش/مأموریت موسسه نیست ☑	مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- پرداختن به مباحث مربوط به امنیت سیستم‌های سایبرفیزیکی
- **اهداف ویژه:**

۱. معرفی تهدیدها و حمله‌های سیستم‌های سایبر فیزیکی

۲. معرفی روش‌های مقابله با حملات در سیستم‌های سایبرفیزیکی

پ) سرفصل‌ها:

۱. مقدمه

۲. تاریخچه و مروری بر سیستم‌های سایبرفیزیکی (CPS)

۳. تهدیدهای مانای پیشرفته (APT)

۴. معرفی سیستم‌های سایبرفیزیکی
   - انواع و دسته‌بندی سیستم‌های سایبرفیزیکی
   - مثال‌هایی از حملات به سیستم‌های سایبرفیزیکی

۵. ارزیابی امنیتی سیستم‌های سایبرفیزیکی
   - فرآیند تحلیل امنیت و تحلیل مخاطره
   - روش‌های تحلیل خسارت، مدلسازی تهدید و ارزیابی مخاطره
   - استانداردهای ارزیاب

۶. امنیت سیستم‌های کنترل صنعتی(ICS) و زیرساخت‌های حیاتی
   - معماری سیستم‌های کنترل صنعتی (لایه‌ها، اجزا و پروتکل‌ها)
   - حمله‌ها و تهدیدها
   - معرفی استانداردهای امنیتی
   - راهبردها و راهکارهای مقاوم سازی

۷. امنیت و حریم خصوصی در IoT
۸. سیستم‌های سایبرفیزیکی و جنگ‌های سایبری

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. H. Karimipour, H. Farag, J. Wei-Kocsis and P. Srikantha, Security of Cyber-Physical Systems, Vulnerability and Impact, Springer, 2020.
2. H. Song, G. A. Fink, and S, Jeschke, Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications, John Wiley, 2017.
3. R. Alur, Principles of Cyber-Physical Systems, MIT Press, 2015.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: ریاضیات رمزنگاری			
عنوان درس به انگلیسی:	Cryptography Mathematics		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☐ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☑ نظری-عملی ☐
تعداد ساعت:	۴۸		پروژه/ رساله / پایان‌نامه ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مهارتی-اشتغال پذیری ☐
مرتبط با آمایش/مأموریت موسسه نیست ☑			مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- معرفی ریاضیات رمزنگاری
- **اهداف ویژه:**

۱. تبیین گستره وسیعی از مفاهیم رمزنگاری

۲. فراگیری ریاضیات رمز

۳. درک عمیق روش‌های اثبات در رمزنگاری

پ) سرفصل‌ها:

۱. مقدمه
- مفهوم امنیت اثبات‌پذیر
- مروری بر نظریه محاسبات
- مروری بر نظریه پیچیدگی
- مفاهیم «تعریف» و «مدل»

۲. ساختارهای اساسی رمزنگاری
- توابع و جایگشت‌های یک‌طرفه
- مولدها، توابع، و جایگشت‌های شبه تصادفی
- توابع درهم ساز
- کدهای تصدیق اصالت پیام

۳. رمزنگاری متقارن
- امنیت در برابر حملات متن آشکار انتخابی(CPA)
- امنیت در برابر حملات متن رمز انتخابی(CCA)

- ساخت رمزهای متقارن
- رمزنگاری تصادفی و رمزنگاری حالت‌دار
- سبک های رمزنگاری: مدل سازی و اثبات

٤. رمزنگاری کلید عمومی
- امنیت در برابر حملاتCPA ، CCA، وCCA2
- رمز انعطاف ناپذیر
- روابط میان گونه‌های مختلف رمزنگاری کلید عمومی
- بنا نمودن شماهای رمز نامتقارن

٥. امضای دیجیتال
- تعاریف و مدل سازی
- الگوی درهم‌سازی – معکوس‌گیری
- درهم‌سازی تمام دامنه
- امنیت دقیق
- امضای کور، امضای انکار ناپذیر، امضای گروهی، امضای دریچه‌دار، رمز امضا

٦. ریاضی رمز
- مقدمه‌ای بر نظریه گروه‌ها
- نظریه اعداد؛ قضیه باقیمانده چینی
- اعداد اول و مسئله تجزیه
- الگوریتم‌های تجزیه
- گروه‌های دوری، مسئله لگاریتم گسسته و مسائل مرتبط
- الگوریتم های حل لگاریتم گسسته
- خم های بیضوی

٧. تعاریف مبتنی بر شبیه‌سازی
- تعاریف مبتنی بر شبیه‌سازی در مقابل تعاریف مبتنی بر بازی
- انواع تمیز ناپذیری (کامل، آماری، محاسباتی)
- تعریف مبتنی بر شبیه‌سازی از رمز نامتقارن امن
- نا-آگاه‌سازی و کاربردهای آن
- مفاهیم اثبات دانش، تمیز ناپذیری گواه، و مخفی سازی گواه

٨. مدل پیشگوی تصادفی
- توابع درهم ساز آرمانی و مکاشفه فیات–شامیر
- تعریف پیشگوی تصادفی
- بنا نمودن انواع ساختارهای رمزنگاری در مدل پیشگوی تصادفی
- ساخت ناپذیری پیشگوهای تصادفی

۹. رمزنگاری کوانتومی
- ماشین‌های کوانتومی و قدرت آنها
- تبادل کلید کوانتومی
- نظریه مشبکه‌ها

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. W. Easttom, Modern Cryptography: Applied Mathematics for Encryption and Information Security 2nd ed, 2022
2. J. Katz and Y. Lindell, Introduction to Modern Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) 2nd Edition, 2014
3. O. Goldreich, Foundations of Cryptograph, Volume 1: Basic Tools. Cambridge University Press, 2001.
4. O. Goldreich, Foundations of Cryptograph, Volume 2: Basic Applications. Cambridge University Press, 2004.
5. A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

ح) ملاحظات برای افراد با نیازهای ویژه:

ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: تئوری اطلاعات و کدینگ			
عنوان درس به انگلیسی:	Coding and Information Theory		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☐ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☑ نظری-عملی ☐
			پروژه/ رساله / پایان‌نامه ☐
تعداد ساعت:	٤٨		مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☑ / مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- تبیین نظریه اطلاعات و کدینگ
- **اهداف ویژه:**

۱. معرفی اطلاعات و آنتروپی

۲. معرفی فشرده‌سازی

۳. معرفی کدینگ

پ) سرفصل‌ها:

۱. مفهوم اطلاعات و آنتروپی
   - آنتروپی
   - اطلاعات متقابل
   - نامساوی‌های اطلاعات متقابل
   - AEP
۲. الگوریتم‌های فشرده‌سازی منبع
   - نامساوی کرفت
   - کد هافمن
   - کد اریتمتیک
   - کد لمپل –زیف
   - کد کردن اعداد طبیعی
۳. فشرده‌سازی چند منبعی
   - روش اسلپین و ولف

٤. آمار و تئوری اطلاعات
   - روش نوعی
   - فشرده‌سازی جهانی
   - قضیه سانوف
   - آزمون فرض
٥. ظرفیت کانال
   - مفهوم ظرفیت کانال
   - اثبات وجود کد برای نرخ‌های کمتر از ظرفیت
   - اثبات عدم وجود کد برای نرخ‌های بالاتر از ظرفیت
٦. کدینگ‌های خطی
   - کد همینگ
   - کد رید و سولمون
   - کد کانولوشنال
   - کد LDPC
۷. تئوری اطلاعات و یادگیری ماشین

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. D. Ellerman, New Foundations for Information Theory: Logical Entropy and Shannon Entropy (SpringerBriefs in Philosophy), 1st ed, 2021
2. D.J.C. MacKay, Information theory, inference, and learning algorithms. Vol. 7. Cambridge: Cambridge university press, 2003.
3. T. M. Cover, and A. T. Joy, Elements of information theory. John Wiley & Sons, 2012.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: تحلیل رمز			
عنوان درس به انگلیسی:	Cryptanalysis		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☐ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☑ نظری-عملی ☐
			پروژه/ رساله / پایان‌نامه ☐
تعداد ساعت:	٤٨		مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☑ / مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- تحلیل و شکستن رمز
- **اهداف ویژه:**

۱. روش‌های پیشرفته تحلیل شکستن رمزهای متقارن

۲. روش‌های پیشرفته تحلیل شکستن رمزهای نامتقارن

پ) سرفصل‌ها:

۱. معرفی و دسته‌بندی روش‌های رمزشکنی

۲. روش‌های تحلیل رمزهای کلاسیک

۳. روش‌های تحلیل رمزهای قالبی: حملات خطی، تفاضلی، تفاضل ناممکن، تفاضل بریده، خطی-تفاضلی، انتگرال، اشباع، لغزشی، بومرنگ، تطابق در میانه، بایکلیک

۴. روش‌های تحلیل رمزهای جریانی: حمله‌ی تمایز، حمله‌ی همبستگی، حمله‌ی همبستگی سریع، حمله‌ی حدس و تعیین، حمله‌ی مکعب

۵. حمله‌ی معاوضه‌ی داده-زمان-حافظه

۶. حمله‌ی جبری و XSL

۷. انواع حملات به توابع درهم‌ساز

۸. حملات مبتنی بر ایده‌ی روز تولد

۹. حملات ساختاری علیه رمزهای کلید نامتقارن: حملات علیه RSA

۱۰. حملات مبتنی بر مشبکه

۱۱. حملات کانال جانبی: حمله‌ی زمانی، توانی، توانی تفاضلی، حمله بر اساس تزریق خطا، حمله بر اساس cache

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. G. Blokdyk, Cryptanalysis A Clear and Concise Reference, 2022
2. M. Joye and M. Tunstall, Fault Analysis in Cryptography, Springer, 2012.
3. L.R Knudsen and M. Robshaw, The Block Cipher Companion, Springer, 2011.
4. C. Paar and J. Pelzl, Undrastanding Cryptography, Springer, 2010.
5. A. Joux, Algorithmic Cryptanalysis, Chapman and Hall/CRC, 2009.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: پروتکل‌های امنیتی پیشرفته			
عنوان درس به انگلیسی:	Advanced Security Protocols		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☐ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☑ نظری-عملی ☐
			پروژه/ رساله / پایان‌نامه ☐
تعداد ساعت:	٤٨		مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☑ / مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- معرفی پروتکل‌های پیشرفته به منظور حفظ امنیت داده
- **اهداف ویژه:**

۱. معرفی پروتکل‌های حفظ امنیت داده در محاسبات

۲. معرفی پروتکل‌های حفظ امنیت داده در ذخیره‌سازی

پ) سرفصل‌ها:

۱. برون‌سپاری امن محاسبات
   - حریم خصوصی داده‌های برون‌سپاری
   - وارسی‌پذیری نتایج خروجی

۲. برون‌سپاری محاسبات سنگین‌وزن
   - برون‌سپاری نمارسانی پیمانه‌ای
   - برون‌سپاری زوج‌سازی دوخطی
   - برون‌سپاری ضرب ماتریس‌های بزرگ
   - برون‌سپاری معکوس ماتریس‌های بزرگ

۳. برون‌سپاری و ذخیره‌سازی داده‌های حجیم
   - ذخیره‌سازی امن داده‌ها
   - وارسی تغییرناپذیری داده‌های ذخیره شده
   - وارسی حذف ناپذیری داده‌های ذخیره‌شده
   - جستجوی امن داده‌های ذخیره‌شده

۴. رمزنگاری جستجوپذیر
   - روش‌های مبتنی بر رمزهای متقارن

- روش‌های مبتنی بر رمزهای نامتقارن

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. The Art of Service - Security Outsourcing Publishing, Security Outsourcing A Complete Guide, 2020
2. X. Chen, Introduction to Secure Outsourcing Computation, Springer, 2016

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

<table>
<tr><td colspan="5">الف: عنوان درس به فارسی: امنیت شبکه‌های سیار</td></tr>
<tr><td>عنوان درس به انگلیسی:</td><td colspan="2">Mobile Network Security</td><td colspan="2">نوع درس و واحد</td></tr>
<tr><td>دروس پیش‌نیاز:</td><td colspan="2"></td><td colspan="2">پایه ☐ نظری ☑</td></tr>
<tr><td>دروس هم‌نیاز:</td><td colspan="2"></td><td colspan="2">تخصصی الزامی ☐ عملی ☐</td></tr>
<tr><td rowspan="3">تعداد واحد:</td><td rowspan="3">۳</td><td rowspan="3">حل تمرین: ☐</td><td colspan="2">تخصصی اختیاری ☑ نظری-عملی ☐</td></tr>
<tr><td colspan="2">پروژه/ رساله / پایان‌نامه ☐</td></tr>
<tr><td colspan="2">مهارتی-اشتغال پذیری ☐</td></tr>
<tr><td>تعداد ساعت:</td><td>۴۸</td><td colspan="3"></td></tr>
<tr><td colspan="3">وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)</td><td>مرتبط با آمایش/مأموریت موسسه نیست ☐</td><td>مرتبط با مأموریت/آمایش موسسه است ☑</td></tr>
</table>

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- تعمیق دانش دانشجویان در زمینه‌ی روش‌های تأمین امنیت در شبکه‌های بی‌سیم و سیار
- **اهداف ویژه:**

۱. بررسی چالش‌های امنیتی در شبکه‌های تلفن سیار

۲. بررسی چالش‌های امنیتی در شبکه‌های بی‌سیم محلی و شهری

۳. بررسی چالش‌های امنیتی در شبکه‌های بی سیم اقتضایی و حسگر

۴. بررسی فناوری‌های ارتباطی کوتاه‌برد

پ) سرفصل‌ها:

۱. مقدمه ای بر ارتباطات سیار و انواع آن, معرفی استانداردهای ارتباطات بی سیم سیار

۲. تهدیدها و حملات رایج در شبکه‌های ارتباطی بی سیم, فناوری‌های پایه در تامین امنیت شبکه‌های بی‌سیم سیار، امنیت کارت‌های هوشمند و SIM/USIM

۳. آشنایی اجمالی با روش‌های تامین امنیت در ارتباطات بی‌سیم سنتی و آنالوگ

۴. آشنایی با شبکه‌های ارتباطات سیار نسل دوم و سوم (GSM/UMTS) و روش‌های تامین امنیت آن

۵. آشنایی با استانداردهای شبکه محلی WiFi و شبکه شهری WiMAX و روش‌های تامین امنیت در آنها

۶. امنیت ارتباطات در حین جابجایی (Roaming) و امنیت بین شبکه‌ای, بررسی مسائل امنیتی مربوط به دست به دست کردن (Handoff) و راهکارهای آن

۷. تامین امنیت خدمات در سامانه‌های بی‌سیم سیار و روش‌های آن

۸. امنیت در شبکه‌های بی سیم خصوصی, امنیت بلوتوث و Zigbee, امنیت در RFID و NFC

۹. امنیت در شبکه‌های بی‌سیم حسگر و اقتضایی

۱۰. امنیت در ارتباطات ماهواره‌ای

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. W. Osterhage, Wireless Network Security, CRC Press, 2018.
2. T. Wrightson, Wireless Network Security: A Beginner's Guide, McGraw-Hill, 2012.
3. A. Holt and C. Huang, 802.11 Wireless Networks: Security and Analysis, Springer, 2010.
4. N. Boudriga, Security of Mobile Communications, CRC Press, 2009.
5. M. Y. Rhee, Mobile Communication Systems and Security, Wiley-IEEE Press, 2009.
6. P. Chandra, Bulletproof Wireless Security: GSM, UMTS, 802.11, and Ad Hoc Security, Elsevier, 2005

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

<table>
<tr><td colspan="5">الف: عنوان درس به فارسی: امنیت اینترنت اشیا</td></tr>
<tr><td>عنوان درس به انگلیسی:</td><td colspan="2">IoT Security</td><td colspan="2">نوع درس و واحد</td></tr>
<tr><td>دروس پیش‌نیاز:</td><td colspan="2"></td><td>پایه ☐</td><td>نظری ☑</td></tr>
<tr><td>دروس هم‌نیاز:</td><td colspan="2"></td><td>تخصصی الزامی ☐</td><td>عملی ☐</td></tr>
<tr><td rowspan="2">تعداد واحد:</td><td rowspan="2">۳</td><td rowspan="3">حل تمرین: ☐</td><td>تخصصی اختیاری ☑</td><td>نظری-عملی ☐</td></tr>
<tr><td colspan="2">پروژه/ رساله / پایان‌نامه ☐</td></tr>
<tr><td>تعداد ساعت:</td><td>۴۸</td><td colspan="2">مهارتی-اشتغال پذیری ☐</td></tr>
<tr><td colspan="2">وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)</td><td>مرتبط با آمایش/مأموریت موسسه نیست ☐</td><td colspan="2">مرتبط با مأموریت/آمایش موسسه است ☑</td></tr>
</table>

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- تبیین چالش‌های امنیتی در محیط اینترنت اشیا و فناوری‌های تامین‌کننده امنیت
- **اهداف ویژه:**

۱. بررسی حفاظت از دستگاه‌ها در اینترنت اشیا

۲. بررسی حفاظت از شبکه‌های متصل در اینترنت اشیا

پ) سرفصل‌ها:

۱. امنیت اینترنت اشیا
۲. آسیب‌ها و خطرات امنیتی اینترنت اشیا (Sybil attck، بدافزارها، ...)
۳. چالش‌های ایمن‌سازی دستگاه‌های اینترنت اشیا
۴. نمونه‌هایی از بدترین حملات اینترنت اشیا
۵. راهکارهای جلوگیری از آسیب‌های اینترنت اشیا
۶. فناوری های تامین کننده حریم خصوصی در اینترنت اشیا
۷. اعتماد و احراز اصالت در اینترنت اشیا
۸. امنیت داده ها در اینترنت اشیا

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. M. Liyanage, A. Braeken, P. Kumar and M. Ylianttila, IoT Security, Wiley, February 2020.
2. S. Li and L. D. Xu, Securing the Internet of Things, Elsevier Science, 2017
3. F. Hu, Security and Privacy in Internet of Things (IoTs) Models, Algorithms, and Implementations, CRC Press, 2016
4. Selected papers

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: نظریه الگوریتمی بازی‌ها			
عنوان درس به انگلیسی:	Algorithmic Game Theory	نوع درس و واحد	
دروس پیش‌نیاز:		پایه ☐	نظری ☑
دروس هم‌نیاز:		تخصصی الزامی ☐	عملی ☐
تعداد واحد:	۳	تخصصی اختیاری ☑	نظری-عملی ☐
	حل تمرین: ☐	پروژه/ رساله / پایان‌نامه ☐	
تعداد ساعت:	۴۸	مهارتی-اشتغال پذیری ☐	
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)		مرتبط با آمایش/مأموریت موسسه نیست ☑	مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- بررسی نظریه بازی‌ها و سیستم‌های چندعاملی و معرفی ابزارهای لازم برای تحلیل آنها
- **اهداف ویژه:**

۱. معرفی نظریه بازی‌ها

۲. طراحی مکانیزم و راهکارهای طراحی بهینه

پ) سرفصل‌ها:

۱. بازی‌ها
- مقدمات و تعاریف
- نقطه تعادل نش و مباحث مربوط به محاسبه‌ی آن در حالت‌های مختلف
- هزینه آشوب

۲. طراحی مکانیزم
- مقدمه، قضایای انکارناپذیری، مکانیزم VCG و مثال‌ها
- مکانیزم‌های صادق و طراحی با پرداخت
- طراحی مکانیزم‌های بدون پرداخت
- مزایده‌های ترکیبیاتی
- شبکه‌های اجتماعی و مسائل مربوط به آن

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. E. N. Barron, Game theory: an introduction. John Wiley & Sons, 2024.
2. A. Espinola-Arredondo and F. Muñoz-Garcia, Game Theory: An Introduction with Step-by-Step Examples, 1st ed., 2023
3. N. Nisan, T. Rougharden, E, Tardos and V. Vaziran, Algorithmic Came Theory, Cambridge University Press, 2007.
4. Y. Shoham and K L. Brown, Multiagents Systems: Algorithmic, Game-Theoretic and Logical Foundations, Cambridge University Press, 2008.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: نظریه پیچیدگی			
عنوان درس به انگلیسی:	Complexity Theory		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☐ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☑ نظری-عملی ☐
			پروژه/ رساله / پایان‌نامه ☐
تعداد ساعت:	۴۸		مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☑ / مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- ارائه مدل‌های پایه برای پیچیدگی محاسبه
- **اهداف ویژه:**

۱. شناخت کلاس‌های پیچیدگی زمانی و فضایی

۲. محاسبات موازی

۳. محاسبات تصادفی

۴. محاسبات کوانتمی

پ) سرفصل‌ها:

۱. مروری بر نظریه ماشین‌های تورینگ، ماشین‌های تورینگ چند نواری و غیرقطعی(nondeterministic) ، تز تورینگ-چرچ، مسایل و زبان‌های بازگشتی و به طور بازگشتی شمارا. تعریف مفاهیم زمان اجرا و فضای مصرفی یک الگوریتم.

۲. مروری بر مسایل تصمیم ناپذیر، مساله توقف و انواع آن، قضیه رایس، روش قطری‌سازی(Diagonalization)

۳. مروری بر منطق گزاره‌ها و منطق مرتبه‌اول، مدل‌های حساب، قضایای صحت و تمامیت نظام استنتاجی منطق مرتبه‌اول، قضیه تصمیم‌ناپذیری منطق مرتبه‌اول، قضایای ناتمامیت گدل.

۴. تعریف کلاس‌های پیچیدگی زمانی و فضایی در حالت کلی و قضایای اساسی ارتباط آنها. قضیه سلسله مراتبی بودن (Hierarchy) و قضیه Gap در حوزه پیچیدگی زمانی و فضایی، مروری بر کلاس‌های زمانی P ، NP، EXP و NEXP و کلاس‌های مکمل آنها. مروری بر کلاس‌های فضایی L، NL، PSPACE، NPSPACE و کلاس‌های مکمل آنها و ارتباط آنها با کلاس‌های زمانی.

۵. تعریف تقلیل (Reduction) و مسایلی که برای یک کلاسC-تمام (C-Complete) هستند. بررسی کلاس‌های مسایل P-Completeو NP-Complete قضیه کوک-لوین و مباحث مرتبط با رابطه کلاس P و NP

۶. مروری بر برخی مسایل معروف NP-Complete

۷. کلاس coNP و مسایل توابع. کلاس PSPACE-Complete و مسایل مهم در آن

۸. کلاس‌های پیچیدگی الگوریتم‌های تصادفی، کلاس‌هایRP ، CoRP، ZPP، وBPP ، پیچیدگی مداری (Circuit Complexity)
۹. الگوریتم‌های موازی، ساختار درونی کلاس P
۱۰. کلاس‌های پیچیدگی الگوریتم‌های تقریبی، حدود تقریب پذیری و تقریب ناپذیری
۱۱. رابطه نظریه‌های پیچیدگی و رمزنگاری. اثبات تعاملی (Iinteractive Proof)
۱۲. مباحث ویژه مانند نظریه پیچیدگی در حضور ماشین‌های تورینگ پیشگو (Oracle TM)، ماشین تورینگ تناوبی (Alternating TM)، نظریه پیچیدگی محاسبات کوانتمی

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. C.H. Papadimitriou. Computational Complexity. Addison-Wesley, 1994.
2. S. Arora and B. Barak. Computational Complexity: A Modern Approach. Cambridge University Press, 2009.
3. D.Z. Du and K.I. Ko. Theory of Computational Complexity. Wiley, 2000.
4. I. Wegener. Complexity Theory: Exploring the Limits of Efficient Algorithms. Springer, 2005.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: امنیت تجارت الکترونیکی			
عنوان درس به انگلیسی:	Electronic Commerce Security		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☐ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☑ نظری-عملی ☐
			پروژه/ رساله / پایان‌نامه ☐
تعداد ساعت:	٤٨		مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☑ / مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- تبیین مفاهیم امنیت اطلاعات در تجارت الکترونیکی
- **اهداف ویژه:**

۱. معرفی تهدیدها و آسیب پذیری های رایج در فضای تجارت الکترونیک

۲. معرفی راهکارهای لازم را برای رفع و مواجهه با تهدیدها و آسیب پذیری‌ها

پ) سرفصل‌ها:

۱. سیستم‌های تجارت الکترونیکی

۲. نیازمندی‌های امنیتی در سیستم‌های تجارت الکترونیکی

۳. مروری بر سیستم‌های پرداخت شامل: پرداخت نقدی، پرداخت با چک و حواله، پرداخت با کارت پرداخت

۴. معماری انواع کارت‌های پرداخت

۵. سیستم‌های پرداخت حساب مرکزی

۶. سیستم‌ها و استانداردهای ریزپرداخت الکترونیکی

۷. سیستم‌ها و استانداردهای پرداخت چک الکترونیکی

۸. سیستم‌ها و استانداردهای پرداخت پول الکترونیکی

۹. سیستم‌ها و استانداردهای پرداخت سیار الکترونیکی

۱۰. زنجیره بلوکی و قراردادهای هوشمند

۱۱. اعتماد در سیستم‌های تجارت الکترونیکی

۱۲. مقدمه ای بر تهدیدات امنیتی در تجارت الکترونیکی

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. D. OMahony, M. Pierce and H. Tewori, Electronic Payment Systems for E-Commerce, Artech House, 2001.
2. C. Radu, Implementing Electronic Card Payment Systems, Artech House, 2003.
3. A. M. Antonopolis, Mastering Bitcoin, Programming the open blockchain, O'Reilly Press, 2017.
4. K. Balasubramanian, K. Mala and M. Rajakani, Cryptographic solutions for secure online banking and commerce, IGI Global, Hershey, PA, 2016.
5. M. H. Sherif, Protocols for secure electronic commerce (3rd edition), CRC Press, Boca Raton, FL, 2016.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: آزمون نرم‌افزار پیشرفته			
عنوان درس به انگلیسی:	Advanced Software Testing	نوع درس و واحد	
دروس پیش‌نیاز:		پایه ☐	نظری ☑
دروس هم‌نیاز:		تخصصی الزامی ☐	عملی ☐
تعداد واحد: ۳	حل تمرین: ☐	تخصصی اختیاری ☑	نظری-عملی ☐
		پروژه/ رساله / پایان‌نامه ☐	
تعداد ساعت: ٤٨		مهارتی-اشتغال پذیری ☐	
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)		مرتبط با آمایش/مأموریت موسسه نیست ☑	مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- بررسی روش‌های مدل‌رانه در طراحی آزمون و تولید داده آزمون
- **اهداف ویژه:**

۱. بررسی روش‌های مدل‌رانه در طراحی آزمون

۲. بررسی روش‌های مدل‌رانه در تولید داده

پ) سرفصل‌ها:

۱. مقدمه‌ای بر روش‌های آزمون
۲. آزمون مدل‌رانه
۳. معیارهای پوشش
۴. افراز فضای ورودی
۵. پوشش گراف
۶. پوشش منطق
۷. آزمون مبتنی بر نحو
۸. ملاحظات عملی در آزمون نرم‌افزار
۹. مباحث جدید در آزمون نرم‌افزار

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال ۳۰ درصد

آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. P. Amman and J. Offutt, Introduction to Software Testing, Cambridge University Press, 2017.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: شبکه‌های کامپیوتری پیشرفته			
عنوان درس به انگلیسی:	Advance Computer Networks		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☐ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☑ نظری-عملی ☐
			پروژه/ رساله / پایان‌نامه ☐
تعداد ساعت:	۴۸		مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☑ / مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- ارائه مطالب جدید در حوزه شبکه های کامپیوتری
- **اهداف ویژه:**

۱. بررسی معماری شبکه

۲. بررسی تعاملات و ارتباطات شبکه

۳. بررسی مدیریت منابع شبکه

پ) سرفصل‌ها:

۱. معرفی و تاریخچه

۲. معماری شبکه‌های کامپیوتری
- انواع مدل‌های لایه‌ای در شبکه‌های کامپیوتری
- معماری اینترنت و شبکه‌های سازمانی
- معماری شبکه‌های نسل جدید
- معماری شبکه‌های شهری
- معماری شبکه‌های دسترسی و بی‌سیم

۳. مدل سرویس در اینترنت
- مدل سرویس اینترنت اولیه و اینترنت نسل جدید
- معماری‌های تضمین کیفیت سرویس
- فناوری MPLS و سرویس‌های مبتنی بر آن
- سرویس‌های چندرسانه‌ای

۴. معماری و پروتکل‌های صفحه کنترل
- مسیریابی درون‌دامنه‌ای و برون‌دامنه‌ای

- مسیریابی حساس به کیفیت سرویس
- فناوری SDN و پروتکل‌های مربوط به آن

۵. مدیریت و مهندسی ترافیک
- دسته بندی انواع مکانیزم‌های مهندسی ترافیک
- مدل‌سازی ترافیک و کنترل دسترسی
- روش‌های کنترل ازدحام
- نوبت‌دهی عادلانه و مدیریت فعال صف

۶. پروتکل‌های طرف میزبان
- پروتکل‌های لایه حمل
- سیستم‌های نظیر به نظیر
- خدماتOTT

۷. تعاملات بین شبکه‌ای
- مفاهیم معماری
- نام ها
- آدرس ها
- مسیریابی بین دامنه‌ای

۸. مدیریت منابع
- کنترل ازدحام انتها به انتها
- صف بندی منصفانه
- کنترل ازدحام مسیریاب
- کیفیت خدمات
- طراحی مسیریاب

۹. ارتباطات بی‌سیم
- مروری بر شبکه‌های بی‌سیم و معماری آنها
- شبکه‌های بی‌سیم در دنیا واقعی
- مسیریابی در شبکه‌های موردی
- مسیریابی در شبکه‌های حسگر

۱۰. کاربردها، نامگذاری و اورلی
- شبکه اورلی
- جداول توزیع شده هش
- DNS و Web
- نام‌ها، معرف ها و معماری شبکه

۱۱. سنجش

- اندازه گیری
- شبکه‌سازی مبتنی بر داده و شبکه‌های تحمل پذیر تأخیر
- چندپخشی

۱۲. مباحث تکمیلی

- روندهای نو در شبکه سازی
- شبکه‌های رادیو شناختی
- شبکه های ICN ، NDN، DTN

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. B. Frouzan, Data Communications and Networking, 5th edition, McGraw Hill, 2012.
2. W. Stallings, Data and Computer Communications, Pearson, 10th edition, 2013.
3. W. Stallings, Foundations of Modern Networking, SDN, NFV, QoE, IoT, and Cloud, Pearson Education, 2016.
4. I. Marsic, Computer Networks, Performance and Quality Service, Rutgers University Press, 2013.
5. P. A. Morale and J. M. Anderson, Software Defined Networking: Design and Deployment, CRC Press, 2015.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: فرآیندهای تصادفی			
عنوان درس به انگلیسی:	Stochastic Processes		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☐ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☑ نظری-عملی ☐
			پروژه/ رساله / پایان‌نامه ☐
تعداد ساعت:	٤٨		مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☑ / مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- بررسی اصولی و مبنایی فرایندهای تصادفی و کاربرد آن در شبکه‌های کامپیوتری
- **اهداف ویژه:**

۱. شناخت مبانی و اصول فرایندهای تصادفی و ویژگی‌های آنها

۲. شناخت انواع کاربردهای فرایند تصادفی در سیستم‌های کامپیوتری

پ) سرفصل‌ها:

۱. مروری بر نظریه احتمال و متغیرهای تصادفی

۲. دنباله‌ای از متغیرهای تصادفی

۳. ایستایی در فرایندهای تصادفی

۴. سیستم‌های خطی تصادفی

۵. چگالی طیف توان

۶. ارگادیک بودن یک فرایندهای تصادفی

۷. فرایندهای تصادفی خاص (فرایند پوآسون، فرایند حرکت براونی و مانند آن)

۸. نظریه تخمین

۹. آزمون فرضیه

۱۰. فرآیندهای مارکوف

۱۱. نظریه صف

۱۲. مدل‌های مارکوف پنهان

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. A. Papoulis and S. U. Pillai, Probability, Random Variables, and Stochastic Processes, McGraw Hill, 2002.
2. S. Ross, Probability Models for Computer Science, Harcourt Academic Press, 2002.
3. R. G. Gallager, Stochastic Processes: Theory for Applications, Cambridge University Press, 2014.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

<table>
<tr><td colspan="5">الف: عنوان درس به فارسی: سیستم‌های سایبرفیزیکی</td></tr>
<tr><td>عنوان درس به انگلیسی:</td><td colspan="2">Cyberphysical systems</td><td colspan="2">نوع درس و واحد</td></tr>
<tr><td>دروس پیش‌نیاز:</td><td colspan="2"></td><td colspan="2">پایه ☐ نظری ☑</td></tr>
<tr><td>دروس هم‌نیاز:</td><td colspan="2"></td><td colspan="2">تخصصی الزامی ☐ عملی ☐</td></tr>
<tr><td rowspan="3">تعداد واحد:</td><td rowspan="3">۳</td><td rowspan="3">حل تمرین: ☐</td><td colspan="2">تخصصی اختیاری ☑ نظری-عملی ☐</td></tr>
<tr><td colspan="2">پروژه/ رساله / پایان‌نامه ☐</td></tr>
<tr><td colspan="2">مهارتی-اشتغال پذیری ☐</td></tr>
<tr><td>تعداد ساعت:</td><td>۴۸</td><td colspan="3"></td></tr>
<tr><td colspan="2">وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)</td><td>مرتبط با آمایش/مأموریت موسسه نیست ☑</td><td colspan="2">مرتبط با مأموریت/آمایش موسسه است ☐</td></tr>
</table>

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- تبیین مفهوم سیستم‌های سایبرفیزیکی و اینترنت اشیا به عنوان سیستمی متشکل از سه بخش محاسباتی، ارتباطات و فیزیکی

اهداف ویژه:

۱. بررسی چالش‌های مربوط به پویایی، گستردگی، پراکندگی و تنوع اجزای سیستم و نیازمندی‌های ارتباطی و محاسباتی

۲. بررسی حوه اطمینان از صحت عملکرد سیستم

۳. معرفی انواع مدل‌ها و پروتکل‌های ارتباطی

پ) سرفصل‌ها:

۱. مقدمه و تاریخچه
   - سیستم‌های سایبرفیزیکی و اینترنت اشیا
   - حوزه‌های کاربردی
   - اشتراکات و تمایزات با سیستم‌های نهفته
   - ویژگی‌ها، فرصت‌ها، چالش‌ها و محدودیت‌ها

۲. مشخصه‌ها و نیازمندی‌های سیستم‌های سایبرفیزیکی و اینترنت اشیا
   - بی‌درنگی، قابلیت اطمینان، ایمنی، دسترس‌پذیری، امنیت و مصرف انرژی
   - رویکردهای تأمین و تضمین آنها

۳. بی‌درنگی، زمان‌بندی و تخصیص منابع
   - انواع سیستم‌های بیدرنگ
   - الگوریتم‌های زمان‌بندی و تخصیص منابع در سیستم‌های بی‌درنگ توزیع‌شده

۴. ارتباطات در سیستم‌های سایبرفیزیکی و اینترنت اشیا
   - ارتباطات درون‌سیستم و پروتکل‌های ارتباطی در آنها

- ارتباطات برون‌سیستم و پروتکل‌های ارتباطی در آن‌ها

۵. بسترهای سخت‌افزاری و نرم‌افزاری سیستم‌های سایبرفیزیکی و اینترنت اشیا
- ساختار گره‌های پردازشی، حسگرها، عملگرها
- لایه‌های پردازشی، سیستم عامل و برنامه‌های کاربردی

۶. امنیت در تعامل با لایه بن‌سازه (Platform)

۷. فناوری‌های نوین مبتنی بر سیستم‌های سایبرفیزیکی و اینترنت اشیا
- معرفی چند مثال واقعی و تشریح و تحلیل ساختار و رفتار یک نمونه عملی

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. R. Alur, Principles of Cyber-Physical Systems, MIT Press, 2015.
2. A. Platzer, Foundations of Cyber-Physical Systems, Lecture Notes, Computer Science Department, Carnegie Mellon University. 2016.
3. E. A. Lee and S. A. Seshia, Introduction to Embedded Systems - A Cyber-Physical Systems Approach, The MIT Press; 2nd edition, 2017.
4. P. Marwedel, Embedded System Design: Embedded Systems Foundations of CyberPhysical Systems, and the Internet of Things, Springer, 2021.
5. W. M. Taha, A.E. M. Taha and J. Thunberg, Cyber-Physical Systems: A Model-Based Approach, Springer, 2021.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

الف: عنوان درس به فارسی: تعامل امنیت سایبری و یادگیری ماشین			
عنوان درس به انگلیسی:	Cybersecurity and Machine Learning Interaction		نوع درس و واحد
دروس پیش‌نیاز:			پایه ☐ نظری ☑
دروس هم‌نیاز:			تخصصی الزامی ☐ عملی ☐
تعداد واحد:	۳	حل تمرین: ☐	تخصصی اختیاری ☑ نظری-عملی ☐
			پروژه/ رساله / پایان‌نامه ☐
تعداد ساعت:	٤٨		مهارتی-اشتغال پذیری ☐
وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)			مرتبط با آمایش/مأموریت موسسه نیست ☑ / مرتبط با مأموریت/آمایش موسسه است ☐

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- استفاده از روش‌های یادگیری ماشین در حوزه امنیت سایبری
- **اهداف ویژه:**

۱. روش‌های استفاده از یادگیری ماشین در امنیت سایبری

۲. روش‌های ارتقای امنیت در مسایل هوش مصنوعی

پ) سرفصل‌ها:

۱. مقدمه
۲. تبیین انواع حملات
۳. تبیین روش‌های دسته‌بندی و خوشه‌بندی
۴. تشخیص ناهنجاری
۵. تحلیل ترافیک با یادگیری ماشین
۶. دفاع سایبری با هوش مصنوعی
۷. چالش‌های یادگیری ماشین در مسایل واقعی امنیت
۸. یادگیری ماشین تهاجمی

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

1. E. Tsukerman, Machine Learning for Cybersecurity Cookbook, Packt Publishing Ltd, 2019.
2. C. Chio and D. Freeman, Machine Learning and Security: Protecting Systems with Data and Algorithms, Sebastopol, CA: O'Reilly Media, 2018.
3. N. M. Shekokar, H. Vasudevan, S. S. Durbha, A. Michalas and T. P Nagarhalli, Intelligent Approaches to Cyber Security, Taylor & Francis, 2024.

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

<table>
<tr><td colspan="5">الف: عنوان درس به فارسی: مباحث ویژه در امنیت سایبری ۱</td></tr>
<tr><td colspan="2">عنوان درس به انگلیسی:</td><td colspan="2">Special Topics in Cybersecurity 1</td><td rowspan="2">نوع درس و واحد</td></tr>
<tr><td colspan="2">دروس پیش‌نیاز:</td><td colspan="2"></td></tr>
<tr><td colspan="2">دروس هم‌نیاز:</td><td colspan="2"></td><td>پایه ☐ نظری ☑</td></tr>
<tr><td rowspan="3">تعداد واحد:</td><td rowspan="3">۳</td><td rowspan="3">حل تمرین: ☐</td><td>تخصصی الزامی ☑</td><td>عملی ☐</td></tr>
<tr><td>تخصصی اختیاری ☐</td><td>نظری-عملی ☐</td></tr>
<tr><td colspan="2">پروژه/ رساله / پایان‌نامه ☐</td></tr>
<tr><td>تعداد ساعت:</td><td>۴۸</td><td colspan="3">مهارتی-اشتغال پذیری ☐</td></tr>
<tr><td colspan="2">وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)</td><td>مرتبط با آمایش/مأموریت موسسه نیست ☐</td><td colspan="2">مرتبط با مأموریت/آمایش موسسه است ☐</td></tr>
</table>

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- ارائه مطالب جدید مطرح در زمینه‌ی امنیت اطلاعات که هنوز به صورت درس استاندارد مطرح نشده‌اند
- **اهداف ویژه:**

پ) سرفصل‌ها:

برای ارایه این درس لازم است سرفصل پیشنهادی مدرس به تصویب شورای تحصیلات تکمیلی گروه برسد.

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

- ویدیو پرژکتور و پرده نمایش

چ) منابع علمی پیشنهادی:

-

ح) ملاحظات برای افراد با نیازهای ویژه:

- ملاحظات و شرایط خاصی ندارد.

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.

<table>
<tr><td colspan="5">الف: عنوان درس به فارسی: مباحث ویژه در امنیت سایبری ۲</td></tr>
<tr><td>عنوان درس به انگلیسی:</td><td colspan="2">Special Topics in Cybersecurity 2</td><td colspan="2">نوع درس و واحد</td></tr>
<tr><td>دروس پیش‌نیاز:</td><td colspan="2"></td><td colspan="2">پایه ☐ نظری ☑</td></tr>
<tr><td>دروس هم‌نیاز:</td><td colspan="2"></td><td colspan="2">تخصصی الزامی☑ عملی ☐</td></tr>
<tr><td rowspan="3">تعداد واحد:</td><td rowspan="3">حل تمرین: ☐</td><td>۳</td><td colspan="2">تخصصی اختیاری نظری-عملی ☐</td></tr>
<tr><td colspan="3">پروژه/ رساله / پایان‌نامه ☐</td></tr>
<tr><td>۴۸</td><td colspan="2">مهارتی-اشتغال پذیری ☐</td></tr>
<tr><td colspan="2">وضعیت آمایشی/مأموریتی درس(صرفاً برای دروس تخصصی اختیاری مشخص شود)</td><td>مرتبط با آمایش/مأموریت موسسه نیست ☐</td><td>مرتبط با مأموریت/آمایش موسسه است ☐</td></tr>
</table>

اگر واحد عملی دارد، چه نوع آموزش تکمیلی نیاز است؟: سفر علمی ☐ آزمایشگاه ☐ سمینار ☐ کارگاه ☐ موارد دیگر: .....

ب: هدف کلی:

- ارائه مطالب جدید مطرح در زمینه‌ی امنیت اطلاعات که هنوز به صورت درس استاندارد مطرح نشده‌اند
- **اهداف ویژه:**

پ) سرفصل‌ها:

برای ارایه این درس لازم است سرفصل پیشنهادی مدرس به تصویب شورای تحصیلات تکمیلی گروه برسد.

ت) روش یاددهی – یادگیری متناسب با محتوا و هدف:

با صلاحدید استاد درس قابل تعیین است.

ث) روش ارزشیابی (پیشنهادی):

فعالیت‌های کلاسی در طول نیم‌سال	۳۰ درصد
آزمون میان ترم	۳۰ درصد
آزمون پایانی	۴۰ درصد

ج) ملزومات، تجهیزات و امکانات موردنیاز برای ارائه:

-

چ) منابع علمی پیشنهادی:

-

ح) ملاحظات برای افراد با نیازهای ویژه:

-

خ) ملاحظات برای برگزاری الکترونیکی درس:

امکان برگزاری درس بصورت الکترونیکی و یا ترکیبی وجود دارد.