دانشکده‌ی علوم ریاضی

مدرس: دکتر شهرام خزایی - دکتر مجتبی رفیعی نیمسال اول ۱۴۰۰-۱۴۰۱

درس سمینار رمزنگاری

پیش‌نیاز - هم‌نیاز

دانشجویانی مجاز به اخذ این درس هستند که شرایط زیر را داشته باشند:

- دانشجویان کارشناسی که درس مقدمه‌ای بر رمزنگاری را گذرانده باشند. لازم به ذکر است که دانشجویان کارشناسی می‌بایست قبل از اخذ درس با استاد در ارتباط بوده و تایید نهایی را دریافت نمایند.
- دانشجویان کارشناسی ارشدی که درس رمزنگاری را گذرانده یا همزمان با درس سمینار، این درس را اخذ کرده‌اند.

لازم به ذکر است که دانشجویان کارشناسی به صورت مستقیم امکان اخذ درس از طریق سامانه آموزش را نداشته و بنابر اعلام درخواست و تایید آن توسط استاد، از طریق کارمند آموزش دانشکده این درس برای آنها اخذ خواهد شد.

توصیف درس

این درس به منظور آماده‌سازی و مهارت بخشی دانشجویان علاقه‌مند در حوزه رمزنگاری برای تدوین و ارایه مطالب علمی در نظر گرفته شده است. انتظار می‌رود دانشجویان در پایان این دوره، مهارت‌های لازم برای شرکت در مجامع علمی و ارایه گزارش‌های مکتوب و شفاهی در حد مطلوب را کسب نمایند.

منابع درس

منبع مشخصی برای این درس به طورثابت تعیین نشده و بنابر موضوعات به روز و داغ کنفرانس‌هایی معتبری همچون:

- Crypto,
- Eurocrypt,
- Theory of Cryptography Conference,
- Asiacrypt,
- Public Key Cryptography.

و علاقمندی دانشجویان و ترجیحات استاد، یک تا سه مقاله به هر نفر تخصیص داده خواهد شد. لازم به ذکر است که تمامی مقالات منتخب به منظور یکپارچگی و هم‌افزایی موثرتر حول یک موضوع مشخص با رعایت پارامترهای مذکور صورت خواهد گرفت.

نحوه‌ی برگزاری کلاس

- به طور تقریبی ۱۰ جلسه حداکثر ۳ ساعتی در طول ترم و در اتاق مجازی استاد درس برگزار خواهد شد.
- دانشجویان ملزم هستند در بازه معین شده در کلاس حضور داشته باشند. عدم حضور به موقع و یا غیبت نمره منفی به دنبال خواهد داشت.
- جلسات ابتدایی با ارایه استاد جهت تعیین خط مشی‌های کلی و رهنمون‌های لازم آغاز و با ارایه‌های علمی افراد مدعو در حوزه رمزنگاری ادامه خواهد یافت.
- دانشجویان با بهره‌گیری از استاد و افراد منتخب معرفی شده توسط ایشان می‌بایست طی دو هفته ابتدایی ترم، موضوعات و مقاله‌هایی پیشنهادی خود را معرفی و ارایه کوتاهی از آن در جلسه داشته باشند.
- هر فرد غیر از ارایه نهایی که زمان آن توسط استاد در طول ترم تعیین خواهد شد و ارایه بتدایی تعیین موضوع، می‌بایست در طول ترم دو ارایه شفاهی که زمانبندی ان توسط استاد مشخص می‌شود، داشته باشد. همچنین ارایه گزارش کتبی در هر مرحله الزامی است.
- قالب مستندات و ارایه‌ها به صورت یکپارچه و توسط استاد در اختیار دانشجویان قرار خواهد گرفت. استفاده از این قالب‌ها الزامی بوده و عدم رعایت ان با کسر نمره همراه خواهد بود.

نحوه ارزشیابی

- ارایه مربوط به تعیین موضوع و دفاع از موضوع پژوهشی انتخابی: ۲ نمره
- فاز اول ارایه شفاهی و مستندات: ۳ نمره
- فاز دوم ارایه شفاهی و مستندات: ۳ نمره
- فاز نهایی ارایه شفاهی و مستندات: ۹ نمره
- فعالیت کلاسی و حضور در مباحث: ۳ نمره

نمره دهی بر هر یک از بخش‌های بالا بر اساس نظر استاد، دستیاران درس و خود دانشجویان با ضریب اثر بخشی به ترتیب ۰/۵، ۰/۲۵ و ۰/۲۵ تعیین خواهد شد. لازم به ذکر است که در صورت ارایه نوآوری توسط دانشجویان در سطحی که به تایید استاد برسد، ۱۰ نمره اضافی برای دانشجوی مذکور لحاظ خواهد.