به نام خدا

کارگاه آموزشی رمزنگاری مشبکه-مبنا

http://ee.sharif.edu/~lattice

در مورد سخنرانان

- **خانم دکتر ترانه اقلیدس**، دانشیار پژوهشکده الکترونیک دانشکده مهندسی برق دانشگاه صنعتی شریف هستند. ایشان در سال ۲۰۰۰ میلادی مدرک دکتری خود را در رشته ریاضیات از دانشگاه گیسن آلمان در زمینه امنیت الگوریتم‌های رمز بلوکی مشابه DES دریافت کرده‌اند و پس از تجربه کاری کوتاهی در آلمان، از بهمن ۱۳۸۰ تاکنون عضو هیئت علمی پژوهشکده الکترونیک هستند. ایشان علاوه بر تدریس دروس رمزنگاری و رمزنگاری مبتنی بر مشبکه، مقالات متعددی را در زمینه‌های مرتبط نگاشته‌اند و راهنمایی دانشجویان کارشناسی ارشد و دکتری را در این زمینه‌ها به عهده دارند. ایشان علاوه بر این، نماینده انجمن رمز در دانشگاه صنعتی شریف و از اعضای کمیته علمی کنفرانس‌های انجمن رمز در سال‌های مختلف بوده‌اند.

  صفحه شخصی: http://sharif.ir/~teghlidos

- **آقای مهندس رحیم طلوعی** مدارک کارشناسی و کارشناسی ارشد خود را در رشته مهندسی برق به ترتیب در سال‌های ۱۳۹۰ و ۱۳۹۲ از دانشگاه صنعتی شریف اخذ کرد. وی هم‌اکنون دانشجوی دکتری در دانشکده مهندسی برق دانشگاه صنعتی شریف است. علاقه‌مندی‌های پژوهشی ایشان مشتمل بر رمزنگاری، طراحی و پیاده‌سازی پروتکل‌های رمزنگاری، امنیت شبکه، سامانه‌های رادار، کدگذاری منبع، و کدگذاری کانال است.

  صفحه شخصی: http://ee.sharif.ir/~rtoluee

- **آقای مهندس احمد بورقانی** مدارک کارشناسی و کارشناسی ارشد خود را به ترتیب در رشته‌های مهندسی نرم‌افزار و مهندسی فناوری اطلاعات در سال‌های ۱۳۸۹ و ۱۳۹۱ از دانشگاه صنعتی شریف اخذ کرد. وی در حال حاضر دانشجوی دکتری مهندسی کامپیوتر در دانشگاه صنعتی شریف است و در آزمایشگاه امنیت داده و شبکه مشغول به پژوهش می‌باشد. علاقه‌ی تحقیقاتی وی، رمزنگاری مشبکه-مبنا است و پژوهش ایشان بر روی بهبود ساختارهای مشبکه-مبنا برای استفاده در سخت‌افزارهایی با توان محاسباتی محدود متمرکز شده است.

  صفحه شخصی: http://ce.sharif.edu/~boorghany

- **خانم دکتر فرخ لقا معظمی گودرزی**، استادیار مرکز پژوهش فضای مجازی دانشگاه شهید بهشتی هستند. ایشان مدرک دکتری خود را در سال ۱۳۹۱ در رشته ترکیبیات و رمزنگاری از دانشگاه الزهرا (س) دریافت نموده‌اند. ایشان پس از یک سال فعالیت پژوهشی پسا-دکتری در دانشگاه صنعتی شریف، از سال ۱۳۹۲ به عضویت هیئت علمی مرکز پژوهش فضای مجازی در آمده‌اند. زمینه‌های علاقمندی ایشان در حوزه رمزنگاری عبارتند از: رمزنگاری مشبکه-مبنا، توزیع کلید و تسهیم راز. همچنین ترکیبیات و نظریه گراف‌ها از علاقمندی‌های ایشان در حوزه ریاضیات است. ایشان علاوه بر سابقه تدریس، مقالات و سخنرانی‌های متعددی در زمینه‌های مرتبط داشته‌اند.

- **آقای مهندس حسین پیل آرام** مدارک کارشناسی و کارشناسی ارشد خود را در رشته مهندسی برق به ترتیب در سال‌های ۱۳۸۹ و ۱۳۹۱ از دانشگاه صنعتی شریف اخذ کرد. وی هم‌اکنون دانشجوی دکتری در دانشکده مهندسی برق دانشگاه صنعتی شریف است. علاقه‌مندی‌های پژوهشی ایشان مشتمل بر رمزنگاری، پروتکل‌های رمزنگاری، امنیت شبکه و طراحی شبکه ها، و سیستم های بی‌سیم است.

صفحه شخصی: http://ee.sharif.ir/~h_pilaram

جدول زمان‌بندی

شروع	پایان	جلسه	توضیح
۸:۳۰	۹:۰۰	پذیرش و افتتاحیه	قرائت قرآن و پخش سرود جمهوری اسلامی ایران
۹:۰۰	۱۰:۱۰	جلسه اول: دیباچه و مقدمات	سخنران: سرکار خانم دکتر ترانه اقلیدس
۱۰:۱۰	۱۰:۲۵	پذیرایی	
۱۰:۲۵	۱۱:۳۵	جلسه دوم: توابع چکیده‌ساز مشبکه-مبنا	سخنران: جناب آقای مهندس رحیم طلوعی
۱۱:۳۵	۱۱:۵۰	پذیرایی	
۱۱:۵۰	۱۳:۰۰	جلسه سوم: رمزنگاری کلید همگانی مشبکه-مبنا	سخنران: جناب آقای مهندس احمد بورقانی
۱۳:۰۰	۱۴:۰۰	ناهار و نماز	
۱۴:۰۰	۱۵:۰۰	جلسه چهارم: تحلیل رمز با ابزار مشبکه	سخنران: سرکار خانم دکتر فرخ لقا معظمی
۱۵:۰۰	۱۵:۱۵	پذیرایی	
۱۵:۱۵	۱۶:۳۰	جلسه پنجم: ساختارهای نوین رمزنگاری مشبکه-مبنا	سخنران: جناب آقای مهندس حسین پیل آرام
۱۶:۳۰	۱۷:۰۰	اختتامیه	

توجه: ثبت نام در کارگاه مشتمل بر شرکت در سخنرانی‌ها، پذیرایی بین جلسات، و ناهار می‌باشد.

اطلاعات بیشتر

برای کسب اطلاعات بیشتر می‌توانید با مسئول شاخه دانشجویی آقای صادق دری نوگورانی از طریق داخلی ۶۶۷۷ دانشگاه صنعتی شریف یا شماره مستقیم ۶۶۱۶۶۶۷۷ (۰۲۱) تماس بگیرید یا با lattice@ee.sharif.edu مکاتبه نمایید.