



پس از برگزاری موفقیت آمیز دوازده دوره از کنفرانس بین المللی انجمن رمز ایران، سیزدهمین دوره این کنفرانس در شهریور ماه ۱۳۹۵ در دانشکده مهندسی و علوم کامپیوتر دانشگاه شهید بهشتی برگزار خواهد شد. سیزدهمین دوره این کنفرانس باهدف انتشار یافته‌های نو و بدیع در زمینه امنیت اطلاعات و رمزشناسی و افزایش هم‌افزایی میان پژوهش‌گران و صاحب‌نظران این حوزه برگزار می‌گردد. کمیته علمی این کنفرانس از تمامی استادان، دانشجویان و پژوهش‌گران دعوت می‌نماید مقالات خود را که حاوی آخرین یافته‌های علمی در یکی از زمینه‌های ذیل و یا سایر زمینه‌های مرتبط می‌باشند، به دبیرخانه کنفرانس ارسال فرمایند.

مبانی رمزشناسی

- مبانی نظری رمزنگاری
- طراحی و تحلیل الگوریتم‌های رمزنگاری جریانی و قالبی متقارن
- طراحی و تحلیل الگوریتم‌های رمز نامتقارن و طرح‌های امضای رقمی
- طراحی و تحلیل توابع چکیده‌ساز
- روش‌های نوین در رمزنگاری (پسا کوانتومی، رمزگذاری تابعی، رمزنگاری همریخت و غیره)

پیاده‌سازی الگوریتم‌های رمزنگاری و امنیت سخت‌افزاری

- پیاده‌سازی نرم‌افزاری و سخت‌افزاری الگوریتم‌های رمزنگاری
- تحلیل امنیت و طراحی امن سخت‌افزارهای رمزنگاری
- حملات کانال جانبی و روش‌های مقابله با آن
- سامانه‌های نهفته رمزنگاری
- دستکاری سخت‌افزار و روش‌های مقابله با آن
- شتاب دهنده‌های سخت‌افزاری برای پروتکل‌های امنیتی
- پیاده‌سازی سخت‌افزارهای امن با استفاده از فناوری‌های نوظهور

امنیت شبکه

- امنیت شبکه‌های بی‌سیم و موبایل
- امنیت زیر ساخت‌های شبکه
- امنیت پروتکل‌ها و لایه‌های شبکه
- سیستم‌های تشخیص، ردیابی و جلوگیری از نفوذ
- امنیت زیرساخت‌های حیاتی

پروتکل‌های امنیتی

- احراز هویت و اصالت
- گمنامی، حریم خصوصی و مدیریت اعتماد
- تحلیل پروتکل‌های امنیتی
- مدل‌های امنیت و اعتماد
- روش‌های صوری در امنیت اطلاعات

امنیت رایانش

- امنیت معماری رایانه
- امنیت سیستم‌عامل
- امنیت پایگاه داده
- تحلیل آسیب‌پذیری و امنیت نرم‌افزار و برنامه‌های کاربردی
- امنیت و حریم خصوصی در افزاره‌های همراه
- امنیت رایانش ابری
- کنترل دسترسی

مهندسی امنیت و امنیت خدمات الکترونیکی

- روش‌های مهندسی اجتماعی در امنیت
- سامانه مدیریت امنیت اطلاعات (ISMS)
- آموزش امنیت
- امنیت کسب و کار و خدمات الکترونیکی
- امنیت سلامت الکترونیکی
- امنیت بانکداری الکترونیکی
- امنیت آموزش الکترونیکی

نهان‌سازی اطلاعات

- الگوریتم‌های جدید در نهان‌نگاری و نشان‌گذاری تصویر و متن
- مدل‌سازی حملات و کانال نشان‌گذاری
- نهان‌کاوی اطلاعات
- کاربردهای نهان‌سازی اطلاعات

جرم‌یابی در فضای مجازی

- روش‌های جرم‌یابی و ریشه‌یابی دیجیتال
- جرم‌یابی پایگاه داده و شبکه
- تشخیص کلاهبرداری و دستکاری
- تحلیل بدافزار و ضد بدافزار

نشانی دبیرخانه کنفرانس:

آدرس: تهران - دانشگاه شهید بهشتی - دانشکده مهندسی و علوم کامپیوتر - دبیرخانه کنفرانس بین‌المللی انجمن رمز ایران - کد پستی ۶۳۱۱۳-۱۹۸۲۹

تلفن: ۰۲۱-۲۹۹۰۴۰۹۳ دورنگار: ۰۲۱-۲۲۴۳۱۸۰۴

رایانامه: isc2016@sbu.ac.ir و isc2016@isc.org.ir نشانی وب‌گاه: <http://isc2016.sbu.ac.ir>