اولین کارگاه آموزشی شاخه دانشجویی رمز دانشگاه صنعتی شریف

مقدمه

شاخه دانشجویی رمز دانشگاه صنعتی شریف درنظر دارد کارگاه آموزشی تحت عنوان تحلیل رمز شبکه مخابرات سیار (Workshop on GSM Cryptanalysis) را آخر اردیبهشت ماه در سالن کهربای دانشکده برق دانشگاه صنعتی شریف با کمک انجمن رمز ایران و کرسی رمز صندوق حمایت از پژوهشگران برگزار کند. هدف از برگزاری این کارگاه آموزشی آشناکردن پژوهشگران شاغل در دانشگاه و صنعت با مفاهیم رمزنگاری و امنیت در سیستمهای مخابرات سیار بخصوص در داخل ایران می‌باشد.

مکان و زمان برگزاری کارگاه آموزشی

دانشگاه صنعتی شریف، دانشکده برق، سالن کهربا، ساعات ۹–۱۲ و ۱۳.۵–۱۶.۵ روز ۳۱ اردیبهشت‌ماه ۱۳۸۷

اعضای کمیته راهبری

خانم رجب‌زاده‌عصار، آقای شریفی، آقای فرحت، آقای مختاری و آقای موسوی

اعضای دعوت شده برای ارائه سمینار

خانم احمدیان، آقای بهرک، خانم جنّتی، خانم رجب‌زاده عصار، آقای شریفی، آقای فرحت، آقای مختاری و آقای موسوی

محورهای اصلی سمینارها

موضوعات سخنرانی	سخنرانان
تحلیل A5/2، الگوریتم رمز GSM ایران در همراه اول	خانم رجب‌زاده عصار
حمله پایه به A5/1، الگوریتم رمز GSM در ایرانسل	آقای شریفی
تحلیل خطای همزمانی الگوریتم رمز GSM	آقای مختاری
تحلیل الگوریتم رمز GSM با استفاده از کدهای تصحیح خطا	آقای بهرک
حمله به الگوریتم رمز GSM با توجه به بده بستان داده، زمان و حافظه	آقای موسوی
تحلیل الگوریتم رمز نسل سوم GSM (UMTS)	خانم احمدیان
تحلیل همبستگی A5/1، الگوریتم رمز GSM	آقای فرحت
تحلیل همبستگی E0، الگوریتم رمز Bluetooth	خانم جنّتی