رمزنگاری ، ۸۱۰۱۰۰۰

نام انگلیسی درس	**Cryptography, 8101000**

نوع درس

	مهندسی برق							مهندسی کامپیوتر			واحد:
	مخابرات	الکترونیک	قدرت	پزشکی	کنترل	دیجیتال	نرم‌افزار	سخت‌افزار	فناوری اطلاعات		۳
اجباری	☐	☐	☐	☐	☐	☐	☐	☐	☐		
اختیاری	☒	☐	☐	☐	☐	☐	☐	☐	☐		

مقطع	کارشناسی ☐ تحصیلات تکمیلی ☒
همنیازها	
پیش نیازها	آمار و احتمال مهندسی
مطالب پیش نیاز	آشنایی اولیه با نظریه‌ی اعداد و مفاهیم جبر
کتاب‌های مرجع	[1] Stinson, Douglas R. *Cryptography: theory and practice*. CRC press, 2005. [2] Henry, B., and P. Fred. "Cipher Systems: The Protection of Communication." (1982).
اهداف درس	برای قرن‌ها، هدف از رمزنگاری حفاظت از ارتباطات بوده است. کامپیوترها، ارتباطات دیجیتال و به ویژه اینترنت، اهداف امنیتی جدیدی را به ارمغان آورده‌اند. بطور مثال موارد ناشناس بودن، احراز، عدم رد شدن، برقراری تماس مجاز (به نام اجرای قانون) و ردیابی از موارد آن هستند. برای تحقق هرکدام نیاز به مکانیسم‌های امنیتی متفاوت است. هدف این دوره آشنایی دانشجویان با چنین تکنیک‌ها و برخی از مبانی این روش‌ها است. دانشجویان با یادگیری مفاهیم رمزنگاری و ریاضیات مربوط به آن می توانند به طراحی الگوریتمهای جدید یا بومی سازی نمونه های مطرح بپردازند.
نتایج درس	دانشجویانی که این درس را با موفقیت پشت سر بگذارند قادر به انجام موارد زیر خواهند بود. ۱- پیاده سازی و رمزگشایی رمزهای کلاسیک. ۲- طراحی و پیاده سازی رمزهای جریانی ۳- توصیف رمزنگاری کلید خصوصی مدرن و روش‌های رمزنگشایی آن. ۴- توصیف سیستم‌های رمزنگاری کلید عمومی مدرن و روش های رمزگشایی آن. ۵- بیان و شرح مفاهیم ریاضی تحت رمزنگاری مدرن.
فهرست مباحث	**تاریخچه و مروری بر رمزنگاری** رمزشناسی کلاسیک نظریه شانون

	رمزنگاری کلید اصلی متقارن رمزهای one-time pad و جریانی رمزهای بلوکی انتزاع رمزهای بلوکی : PRPs, PRFs حمله به رمزهای بلوکی **توابع هش رمزنگاری** توابع هش و یکپارچگی داده ها امنیت توابع هش کد تأیید پیام **رمزنگاری کلید عمومی** اعداد اول در مد حسابی رمزنگاری با استفاده از اعداد اول در مد حسابی رمزگذاری کلید عمومی اعداد مخلوط در مد حسابی **امضای دیجیتال** امضای دیجیتال: تعاریف و برنامه های کاربردی الگوریتم‌ها، ساختارها و برنامه‌های کاربردی بیشتر
نرم‌افزارها و ابزارهای مورد نیاز	بخشی از درس بصورت **Powerpoint** و بخش دیگر با استفاده از تخته ارائه می گردد. انجام تکالیف کامپیوتری نیز در دستور کار درس قرار دارد.
تکالیف پیشنهادی	دانشجویان چهار سری تکلیف کتبی و دو سری تکلیف کامپیوتری خواهند داشت. همچنین یک مقاله که بخشی از درس را تکمیل می کند توسط هر دانشجو ارائه می شود.
پروژه‌های پیشنهادی	از ابتدای ترم هر دانشجو با مشاوره استاد درس یک پروژه را انتخاب کرده و بر اساس آن تا پایان ترم به تحقیق ادامه می دهد.
نمره‌دهی پیشنهادی	تکالیف **20٪** پروژه **10٪** امتحان میان ترم **30٪** امتحان پایان ترم **40٪**
سایر مراجع	[1] Digital Watermarking World http://www.watermarkingworld.org/ [2] Stirmark Benchmark, http://fabien/watermarking/stirmark/
تنظیم کننده	محمدعلی اخایی، استادیار دانشکده مهندسی برق و کامپیوتر دانشگاه تهران
تاریخ تنظیم	شهریور ماه ۱۳۹۶