به نام ایزد دانا

(کاربرگ طرح درس)

تاریخ به‌روز رسانی:

دانشکده .ریاضی امار و کامپیوتر.....

نیمسال اول/دوم سال تحصیلی

.97-98.

نام درس	فارسی:رمزنگاری1	تعداد واحد: نظری2	مقطع: کارشناسی □ کارشناسی ارشد √ دکتری□
	لاتین:cryptography1	پیش‌نیازها و هم‌نیازها: نظریه اطلاع و کاربرد – الگوریتم ومحاسبه	
مدرس/مدرسین: مسعود قدس		شماره تلفن اتاق: 5738	
پست الکترونیکی:mghods@semnan.ac.ir		منزلگاه اینترنتی:	
برنامه تدریس در هفته و شماره کلاس:دانشکده ریاضی شنبه 13-15 یک شنبه 10.30-12.30			
اهداف درس: اشنایی با مبانی رمزنگاری و انواع رمز و امضای دیجیتال و....			
امکانات آموزشی مورد نیاز:			

نحوه ارزشیابی	فعالیت‌های کلاسی و آموزشی	ارزشیابی مستمر(کوئیز)	امتحان میان‌ترم	امتحان پایان‌ترم
درصد نمره	1-2		6-8	12-14
منابع و مآخذ درس	d.r.stinson. cryptography:theory and practice			

بودجه‌بندی درس

شماره هفته آموزشی	مبحث	توضیحات
1	تاریخچه رمز نگاری	
2	اهمیت رمزنگاری–نظریه اعداد	
3	رمزنگاری کلاسیک	
4	معرفی رمز های مشهور ونحوه تحلیل	
5	قضیه شانون	
6	امنیت کامل و محرمانگی	
7	معرفی اولیه های رمز نگاری	
8	مولدهای شبه تصادفی	
9	رمز نگاری متقارن	
10	انواع تحلیل رمزهای متقارن	
11	معرفی توابع چکیده ساز	
12	حملات شناخته شده به رمزهای قالبی	
13	رمزنگاری کلید عمومی	

14	تحلیل و امنیت ان	
15	معرفی طرح های امضای رقمی مشهور	
16	رفع اشکال و حل تمرین	