

مدرس: مرضیه اسکندری	نام درس: الگوریتم و محاسبه	نیم سال: ۹۹۱
رشته و مقطع تحصیلی: کارشناسی ارشد-کدورمز	پیش نیاز: ندارد	نوع درس و تعداد واحد: انتخابی - ۳ واحد
نحوه‌ی ارزیابی دانشجویان: ۴ آزمون کوچک: ۱۲ نمره پایان ترم: ۶ نمره تمرین های تحویلی: ۴ نمره		تاریخ آزمون پایان ترم: ۹۹/۱۰/۲۳
ایمیل استاد درس: Eskandari@alzahra.ac.ir		
هدف: آشنایی با مفاهیم اصلی نظریه محاسبه مرتبط با زمینه های رمز و کد در ایجاد سختی الگوریتم و امکان تجزیه و تحلیل پیچیدگی الگوریتمهای مورد استفاده در این حوزه		
مراجع: - Complexity and Cryptography: An Introduction, Volume 13. Front Cover. J. Talbot, D. Welsh. Cambridge University Press, 2006 - Computational Complexity: A Modern. Approach. S. Arora and B. Barak. Cambridge University Press, 2009		
شرح درس	هفته	
معرفی درس، سرفصل و منابع (دید کلی)	اول	
مروری بر محتوای دروس پیش نیاز	دوم	
محاسبه تعداد اعمال الگوریتم ها، فضای مصرفی، رشد توابع، نمادهای مجانبی و تحلیل اهمیت سرعت الگوریتم ها	سوم	
ماشین تورینگ و مفاهیم اولیه	چهارم	
ارائه تعریف دقیق پیچیدگی در مدل های قطعی و غیر قطعی	پنجم	
کلاسهای P، NP	ششم	
مسائل NP-hard, NP-complete	هفتم	
کاهش پذیری	هشتم	
اهمیت مدل NP در رمزنگاری	نهم	
کلاس P و رمزنگاری	دهم	
کلاسهای پیچیدگی تصادفی (BPP)	یازدهم	
مفهوم امنیت و امنیت معنایی	دوازدهم	
تمایز ناپذیری	سیزدهم	
تورینگ اوراکل دار	چهاردهم	
سامانه های اثبات تعاملی	پانزدهم	
قضیه PCP	شانزدهم	