دانشکده علوم ریاضی

نیم‌سال: ۹۹۲	**نام درس:** رمزنگاری ۱	**مدرسین: مرضیه اسکندری، مهناز نوروزی**
نوع درس و تعداد واحد: الزامی-انتخابی، ۳ واحد	**پیش نیاز:** -	**رشته و مقطع تحصیلی:** کارشناسی ارشد، ریاضی کاربردی، گرایش رمزوکد
تاریخ آزمون پایان ترم: ۱۴۰۰/۴/۱۶ **تاریخ آزمون میان ترم:** ۱۴۰۰/۲/۲۷	**نحوه‌ی ارزیابی دانشجویان:** میان‌ترم: ۷ نمره ، پایان‌ترم: ۷ نمره ، فعالیت کلاسی: ۱ نمره ، تکالیف: ۲ نمره ، پروژه: ۳ نمره	
ایمیل اساتید درس: Eskandari@alzahra.ac.ir ، m.noroozi@alzahra.ac.ir		

مراجع:

- Introduction to Cryptography with Coding Theory, Wade Trappe and Lawrence C. Washington, 3rd ed. 2020.
- Introduction to Modern Cryptography, Jonathan Katz, Yehuda Lindell, 3rd ed. 2020.

هفته	شرح درس
اول	معرفی علم رمزنگاری (تاریخچه، کاربرد، هدف و ...) – ارتباط محرمانه (هدف، موجودیت‌ها، ابزار، حملات)
دوم	طرح‌های رمزگذاری سنتی (سزار، شیفت، ویژنر، جانشینی تک الفبایی و چند الفبایی، ...– ویژگی‌ها و امنیت)
سوم	طرح رمزگذاری one-time pad – امنیت کامل
چهارم	امنیت محاسباتی – رمزهای قالبی و جریانی
پنجم	DES و AES (روش، نقطه ضعف، امنیت، حمله ملاقات در میانه، روش دوگانه و سه‌گانه)
ششم	سبک‌های عملیات (انواع روش‌های به کارگیری رمزهای قالبی، مزایا و معایب)
هفتم	پیش‌نیازهای ریاضیاتی (همنهشتی، قضیه باقیمانده چینی، قضیه کوچک فرما و اویلر، میدان، ...)
هشتم	رمزگذاری کلید عمومی (مقایسه با رمزگذاری متقارن، توابع یکطرفه) – میان ترم
نهم	طرح رمزگذاری RSA (روش، امنیت، حملات موجود)
دهم	مساله لگاریتم گسسته، توافق کلید DH، طرح رمزگذاری الجمال
یازدهم	مدیریت کلید و گواهینامه‌ها – تشریح اهداف و کاربردهای مختلف رمزنگاری
دوازدهم	توابع هش (کاربرد، امنیت)
سیزدهم	کدهای احراز اصالت پیام (هدف، تعریف، امنیت، روش ساخت)
چهارده	امضاهای دیجیتال (هدف، تعریف، امنیت، امضای RSA، امضای کور، امضای الجمال)
پانزدهم	طرح‌های تسهیم راز (هدف، روش‌های آستانه‌ای، طرح شمیر)
شانزدهم	ارائه پروژه‌ها