

نام درس: رمزنگاری ۱	مدرس: مهناز نوروزی
نیمسال: ۲-۱۴۰۱	رشته و مقطع تحصیلی: ریاضی کاربردی، کارشناسی ارشد
تعداد واحد: ۴	نحوه ارزیابی دانشجویان: میان ترم: ۷ نمره ، پایان ترم: ۷ نمره ، تکالیف: ۳ نمره ، پروژه: ۳ نمره
تاریخ آزمون پایان ترم: ۱۴۰۲/۴/۴	ایمیل استاد درس: <a href="mailto:m.noroozi@alzahra.ac.ir">m.noroozi@alzahra.ac.ir</a>
مراجع:	
<ul style="list-style-type: none"> <li>• Introduction to Cryptography with Coding Theory, Wade Trappe and Lawrence C. Washington, 3<sup>rd</sup> ed. 2020.</li> <li>• Introduction to Modern Cryptography, Jonathan Katz, Yehuda Lindell, 3<sup>rd</sup> ed. 2020.</li> </ul>	
هفته	شرح درس
۱	معرفی علم رمزنگاری (تاریخچه، کاربرد، هدف و ...) - ارتباط محرمانه (هدف، موجودیتها، ابزار، حملات)
۲	طرح‌های رمزگذاری سنتی (سزار، شیف، ویژنر، جانشینی تک الفبایی و چند الفبایی، ...-ویژگی‌ها و امنیت)
۳	طرح رمزگذاری one-time pad - امنیت کامل
۴	امنیت محاسباتی - رمزهای قالبی و جریانی
۵	DES و AES (روش، نقطه ضعف، امنیت، حمله ملاقات در میانه، روش دوگانه و سه‌گانه)
۶	سبک‌های عملیات (انواع روش‌های به کارگیری رمزهای قالبی، مزایا و معایب)
۷	پیش‌نیازهای ریاضیاتی (همنهستی، قضیه باقیمانده چینی، قضیه کوچک فرما و اویلر، میدان، ...)
۸	رمزگذاری کلید عمومی (مقایسه با رمزگذاری متقارن، توابع یکطرفه) - میان ترم
۹	طرح رمزگذاری RSA (روش، امنیت، حملات موجود)
۱۰	مساله لگاریتم گسسته، توافق کلید DH، طرح رمزگذاری الجمال
۱۱	مدیریت کلید و گواهینامه‌ها - تشریح اهداف و کاربردهای مختلف رمزنگاری
۱۲	توابع هش (کاربرد، امنیت)
۱۳	کدهای احراز اصالت پیام (هدف، تعریف، امنیت، روش ساخت)
۱۴	امضاهای دیجیتال (هدف، تعریف، امنیت، امضای RSA، امضای کور، امضای الجمال)
۱۵	طرح‌های تسهیم راز (هدف، روش‌های آستانه‌ای، طرح شمیر)
۱۶	ارائه پروژه‌ها