

نیمسال: ۱-۱۴۰۳	نام درس: نظریه رمزنگاری مقدماتی	مدرس: مهناز نوروزی
تعداد واحد: ۳	رشته و مقطع تحصیلی: علوم کامپیوتر، کارشناسی	
نحوه ارزیابی دانشجویان: میان ترم: ۸ نمره ، پایان ترم: ۸ نمره ، تکالیف: ۲ نمره ، پروژه: ۲ نمره		
تاریخ آزمون پایان ترم: ۱۴۰۳/۱۱/۱	ایمیل استاد درس: m.noroozi@alzahra.ac.ir	
مراجع:		
<ul style="list-style-type: none"> • Introduction to Modern Cryptography, Jonathan Katz, Yehuda Lindell, 3rd ed. 2020. • Introduction to Cryptography with Coding Theory, Wade Trappe and Lawrence C. Washington, 3rd ed. 2020. 		
هفته	شرح درس	
۱	معرفی علم رمزنگاری (تاریخچه، کاربرد، هدف و ...)	
۲	ارتباط محرمانه (هدف، موجودیتها، ابزار، حملات)	
۳	طرح‌های رمزگذاری سنتی (سزار، انتقال، ویزنر، جایگزینی تک الفبایی و چند الفبایی، ... - ویژگی‌ها و امنیت)	
۴	طرح رمزگذاری one-time pad - امنیت کامل	
۵	امنیت محاسباتی - رمزهای قلبی و جریانی	
۶	DES و AES (روش، نقطه ضعف، امنیت، حمله ملاقات در میانه، روش دوگانه و سه گانه)	
۷	سبک‌های عملیات (انواع روش‌های به کارگیری رمزهای قلبی، مزایا و معایب)	
۸	پیش‌نیازهای ریاضیاتی (همه‌پستی، قضیه باقیمانده چینی، قضیه کوچک فرما و اویلر، میدان، الگوریتم اقلیدسی، ...)	
۹	میان ترم	
۱۰	رمزگذاری کلید عمومی (مقایسه با رمزگذاری متقارن، توابع یکطرفه)	
۱۱	طرح رمزگذاری RSA (روش، امنیت، حملات موجود)	
۱۲	مساله لگاریتم گسسته، توافق کلید DH، طرح رمزگذاری الجمال	
۱۳	مدیریت کلید و گواهینامه‌ها - تشریح اهداف و کاربردهای مختلف رمزنگاری	
۱۴	توابع چکیده‌ساز (کاربرد، امنیت)	
۱۵	کدهای احراز اصالت پیام (هدف، تعریف، امنیت، روش ساخت)	
۱۶	امضاهای دیجیتال (هدف، تعریف، امنیت، امضای RSA، امضای کور، امضای الجمال)	