دانشگاه الزهرا

دانشکده علوم ریاضی

نام درس: نظریه رمزنگاری مقدماتی	**مدرس: مهناز نوروزی**
نیم‌سال: ۱-۱۴۰۲	**رشته و مقطع تحصیلی:** علوم کامپیوتر، کارشناسی
تعداد واحد: ۳	**نحوه ارزیابی دانشجویان:** میان‌ترم: ۸ نمره ، پایان‌ترم: ۸ نمره ، تکالیف: ۲ نمره ، پروژه: ۲ نمره
تاریخ آزمون پایان ترم: ۱۴۰۲/۱۰/۱۹	**ایمیل استاد درس:** m.noroozi@alzahra.ac.ir

مراجع:

- 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، ویژنر، جایگزینی تک الفبایی و چند الفبایی، ... – ویژگی‌ها و امنیت)
۴	طرح رمزگذاری one-time pad – امنیت کامل
۵	امنیت محاسباتی – رمزهای قالبی و جریانی
۶	DES و AES (روش، نقطه ضعف، امنیت، حمله ملاقات در میانه، روش دوگانه و سه‌گانه)
۷	سبک‌های عملیات (انواع روش‌های به کارگیری رمزهای قالبی، مزایا و معایب)
۸	پیش‌نیازهای ریاضیاتی (همنهشتی، قضیه باقیمانده چینی، قضیه کوچک فرما و اویلر، میدان، الگوریتم اقلیدسی، ...)
۹	رمزگذاری کلید عمومی (مقایسه با رمزگذاری متقارن، توابع یکطرفه) – میان ترم
۱۰	طرح رمزگذاری RSA (روش، امنیت، حملات موجود)
۱۱	مساله لگاریتم گسسته، توافق کلید DH، طرح رمزگذاری الجمال
۱۲	مدیریت کلید و گواهینامه‌ها – تشریح اهداف و کاربردهای مختلف رمزنگاری
۱۳	توابع چکیده‌ساز (کاربرد، امنیت)
۱۴	کدهای احراز اصالت پیام (هدف، تعریف، امنیت، روش ساخت)
۱۵	امضاهای دیجیتال (هدف، تعریف، امنیت، امضای RSA، امضای کور، امضای الجمال)
۱۶	طرح‌های تسهیم راز (هدف، روش‌های آستانه‌ای، طرح شمیر)