عنوان درس	فارسی	رمزنگاری۲										
	انگلیسی	Cryptography II										
نوع واحد									تعداد واحد	تعداد ساعت	دروس پیش‌نیاز	
پایه		اصلی		تخصصی		اختیاری			۳	۴۸	رمزنگاری ۱	
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی					
حل تمرین: ندارد		نیاز به اجرای پروژه عملی: ندارد										

هدف: معرفی و آشنایی با جنبه‌های مختلف از کاربرد رمزنگاری، مولدهای تصادفی و نقش حیاتی آنها در ایجاد امنیت، ایجاد توانایی اثبات امنیت سامانه‌های رمزنگاری، معرفی سیستم‌های رمزنگاری جدید، سیستم‌های رمزنگاری آینده و چالش‌های موجود

سرفصل‌های درس:

- تعریف دقیق اولیه‌های رمزنگاری به ویژه مولدهای شبه تصادفی، توابع یک طرفه، توابع چکیده ساز و ارائه قضایای اصلی
- تعریف دقیق طرح‌های شناسایی و احراز اصالت، روش‌های ساخت و اثبات امنیت آنها،
- پروتکل دیفی- هلمن،الگوهای توزیع کلید
- مدل امنیت پاسخگوی تصادفی و تحلیل آن
- تعریف دقیق توابع چکیده‌ساز، روش‌های ساخت و تحلیل آن‌ها
- الگوریتم‌های امضای رقمی با کلید عمومی، روش‌های طراحی و اثبات آنها
- آموزش حملات استاندارد نظیر حملات خطی، تفاضلی، جبری و نظایر آن بر روی یک سامانه ساده رمزنگاری (با انتخاب استاد)
- معرفی مفاهیم و اصول مرتبط با موضوعات پیشرفته‌تر در رمزنگاری با تاکید بر مثال، نظیر:اثبات‌های هیچ دانشی، رمزنگاری کوانتومی (معرفی محاسبات کوانتومی، محدودیت‌های کامپیوترهای کوانتومی و سایر مفاهیم مرتبط)،رمزنگاری مشبکه مبنا، رمزنگاری کدمبنا، رمزنگاری مبتنی بر خم بیضوی، رمزنگاری چکیده مبنا، رمزنگاری چند متغیره

منابع:

[1] Jonathan Katz, Yehuda Lindell: "Introduction to Modern Cryptography", Chapman and Hall/CRC, Taylor & Francis Group, 2008.
[2] D.R. Stinson, Cryptography: Theory and Practice, Chapman & Hall / CRC; 3nd edition, 2006.
[3] W. Mao, Modern Cryptography: Theory and Practice, Prentice Hall, 2003.
[4] A. Menezes , P. Oorschot , S Vanstone, Handbook of Applied Cryptography, CRC Press; 1 edition, 1996.
[5] Bernstein Daniel J., Johannes Buchmann, Erik Dahmen: "Post-quantum Cryptography", Springer Verlag, 2009.
[6] Micciancio Daniele, Shafi Goldwasser: "Complexity of Lattice Problems: A Cryptographic Perspective", Springer Verlag, 2002.
[7] Steven D. Galbraith: "Mathematics of public key cryptography", Cambridge University Press, 2012.