عنوان درس	فارسی	رمزنگاری ۱								
	انگلیسی	Cryptography I								
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
پایه		اصلی		تخصصی		اختیاری		۳	۴۸	نظریه اطلاع و کاربرد، الگوریتم و محاسبه
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی			
حل تمرین: ندارد نیاز به اجرای پروژه عملی: ندارد										

هدف: بیان اهمیت رمزنگاری در ارتباطات و نقش ریاضیات پیشرفته در توسیع آن، معرفی رمزنگاری کلاسیک و سپس انواع سیستم‌های رمزنگاری متقارن و نامتقارن، امضای دیجیتال و . . . به نحوی که دانشجو بر اصول و مفاهیم پایه‌ای رمزنگاری مسلط شده و با مثال‌های لازم در این زمینه آشنا شود.

سرفصل‌های درس:

- اهمیت رمزنگاری، تاریخچه، معرفی سرفصل‌های مهم ریاضی مرتبط با رمزنگاری و درصورت لزوم تدریس و یادآوری نکات کلیدی ریاضی مورد لزوم نظیر، میدان‌های متناهی، نظریه اعداد، پیچیدگی محاسبه.
- رمزنگاری کلاسیک، معرفی سیستم‌های رمز مشهور (نظیر سزار و آفین) و نحوه تحلیل آنها
- یادآوری قضیه شانون، امنیت کامل، نحوه اندازه گیری امنیت و محرمانگی (با استفاده از روش‌هایی نظیر آنتروپی و نظریه پیچیدگی)، بررسی انواع امنیت
- معرفی اولیه‌های رمزنگاری به ویژه مولدهای شبه تصادفی، توابع یک طرفه، توابع چکیده ساز
- مولدهای شبه تصادفی، تکنیک‌ها و روش‌های مختلف تولید اعداد تصادفی و اهمیت آنها در تولید کلید
- رمزنگاریمتقارن (قالبی و جریانی)، معرفی انواع تحلیل رمزهای متقارن از جمله تحلیل‌های تفاضلی، خطی، جبری و سایر حملات شناخته‌شده به رمزهای قالبی
- معرفی توابع چکیده ساز، انواع کدهای احراز اصالت (CBC، MAC، HMAC و ...)، امنیت و حملات محتمل به آنها، پروتکل تبادل کلید دیفی- هلمن
- معرفی سامانه‌های رمزنگاری کلید عمومی مشهور (RSA، الجمال، رابین و ...)، تحلیل امنیت آنها
- معرفی طرح‌های امضای رقمی مشهور (نظیر RSA، الجمال و اشنور)

منابع:

[1] D.R. Stinson, *Cryptography: Theory and Practice*, Chapman & Hall / CRC; 3nd edition, 2006.
[2] W. Mao, Modern Cryptography: Theory and Practice, Prentice Hall, 2003.
[3] J. Hoffstein, J. Pipher and J.H. Silverman,AnIntroduction to Mathematical Cryptography, Springer, 2008.
[4] Josef Pieprzyk, Thomas Hardjono, Jennifer Seberry: "Fundamentals of Computer Security", Springer Verlag, 2003.
[5] Christof Paar, Jan Pelzl: "Understanding Cryptography, A Textbook for Students and practitioner", Springer Verlag, 2010.
[6] Jonathan Katz, Yehuda Lindell: "Introduction to Modern Cryptography", Editor: Douglas Stinson, Chapman and Hall/CRC, Taylor & Francis Group, 2008.
[7] Andreas Klein, Stream Ciphers, Springer Verlag, 2013.
[8] Thomas Cover, Joy A. Thomas: "Elements of Information Theory", 2nd Ed. Wiley Series, 2006.