عنوان درس	فارسی	روش‌های صوری دررمزنگاری									
	انگلیسی	Formal Methods in Cryptography									
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: استفاده از روش‌های صوری در مدل‌سازی و تحلیل پروتکل‌ها و الگوریتم‌های رمزنگاری

سرفصل‌های درس:

- نظریه مجموعه‌ها و منطق از مرجع [۱]
- سه روش‌صوری اصلی
- وارسی‌گر مدل (از جمله ابزار Scyther) از مرجع [۲]
- درستی‌یابی خودکار (از جمله منطق BAN)از مرجع [۳]
- جبر پردازه‌ای از مرجع [۴]
- مدل‌سازی و توصیف (description) چند پروتکل معروف امنیت و توزیع کلید (چون دیفی-هلمن) به وسیله یکی از روشهای صوری سه‌گانه معرفی شده در درس
- مشخص کردن(specification) چند خاصیت عمده امنیت چون احراز اصالت، محرمانگی، کنترل دسترسی، گمنامی، عدم انکار با یکی از روش‌های صوری سه‌گانه معرفی شده در درس
- درستی‌یابی (verification) ویژگی‌های امنیتی برای پروتکل‌های توصیف‌شده

منابع:

[1] Michael Huth and Mark Ryan, Logic in Computer Science modeling and reasoning about systems, Cambirdge University Press, 2004.
[2] C. Cremers, S. Mauw, Operational Semantics and Verification of Security Protocols, Springer, 2012.
[3] G. Bella, Formal Correctness of Security Protocols, Springer, 2007.
[4] Wan Fokkink, Introduction to Process Algebra, Springer, 2007.