عنوان درس	فارسی	پروتکل‌های رمزنگاری											
	انگلیسی	Cryptographic Protocols											
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: در این درس پروتکل‌های امنیتی مختلف توصیف شده، همچنین حملات و دفاع‌های مختلف در مقابل آنها مطرح می‌شود. پروتکل‌های مختلف مانند پروتکل‌های احراز اصالت و امضا، مدیریت حقوق دیجیتال، پروتکل‌های امنیتی در شبکه‌های توزیع شده، بی‌سیم و باسیم، رای‌گیری الکترونیکی، پروتکل‌های پرداخت الکترونیکی، راهکارهای رمزنگاری بصری و ...

سرفصل‌های درس:

- مقدماتی بر پروتکل‌ها، پروتکل‌های امن و انواع آن، کلاس‌های حملات به پروتکل‌های امن و مدل‌های امنیتی، امضا و احراز اصالت و هویت، پروتکل‌ها و سازوکارها، مدیریت و برقراری کلید و صدور گواهی
- مولفه‌های سازنده پروتکل(تعریف پروتکل، ارتباط امن با استفاده از رمزنگاری متقارن، توابع یک طرفه، ارتباط امن با استفاده از رمزنگاری نامتقارن، امضاهای رقمی (digit)، چارچوبی برای سازوکارهای رقمی، RSA و طرح‌های امضای مربوطه، طرح امضای فیات شامیر، DSA و طرح‌های امضای مربوطه، طرح‌های امضای رقمی یکبار مصرف، طرح‌های امضای رقمی حکم-دار، طرح‌های امضای رقمی کور، طرح‌های امضای رقمی غیرقابل انکار، طرح‌های امضای رد-توقف)
- پروتکل‌های ساده (مبادله کلید، احراز اصالت، احراز اصالت و مبادله کلید، تحلیل صوری مبادله کلید و احراز اصالت، رمزنگاری با کلید عمومی چندگانه، رمزنگاری آستانه‌ای، تسهیم راز، محافظت رمزنگاشتی (cryptographic) از پایگاه‌های داده.
- پروتکل‌های متوسط (خدمات مهر زمانی، کانال نهان، امضای رقمی غیرقابل انکار، امضای با تاکید کننده مشخص، امضاهای وکالتی، امضاهای گروهی، محاسبه با اطلاعات رمزشده، طرح‌های تعهد بیتی، طرح‌های سکه اندازی منصفانه، پوکر ذهنی، جمع کننده‌های یک طرفه، افشای همه یا هیچ راز، برون سپاری کلید)
- پروتکل‌های پیشرفته(اثبات‌های هیچ دانشی، اثبات‌های هیچ‌دانشی، امضاهای کور، رمزنگاری کلید عمومی مبتنی بر شناسایی، انتقال بی خبر، امضاهای بی خبر (oblivious transfer)، امضای قرارداد توأمان، نامه رقمی سفارشی، مبادله همزمان رازها)
- مدیریت کلید (تولید کلید، فضای غیرخطی کلید، انتقال کلید، تایید کلید، استفاده از کلید، ذخیره کلید، تازه کردن کلید، ازبین بردن کلید، مدیریت کلیدهای عمومی، زیرساخت کلید عمومی، گواهی‌نامه‌ها، مدل‌های اعتماد)
- پروتکل‌های مبادله کلید (طرح دیفی هلمن، پروتکل‌های ایستگاه به ایستگاه، پروتکل‌های شامیر، مبادله کلید رمزشده، توزیع کلید کنفرانس و پخش راز)
- طرح‌های شناسایی
- پروتکل‌های خاص (انتخابات امن، محاسبات چندطرفه امن، پخش بدون نام پیام، اسکناس رقمی)

منابع:

[1] C. Boyd, A. Mathuria, Protocols for Authentication and Key Establishment, Springer, 2003.
[2] B.Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, Wiley, 1996.
[3] P.Ryan, S.Schneider, M.Goldsmith, G.Lowe and B. Roscoe, modelling and Analysis of Security Protocols, Addison-Wesley, 2001.