باسمه‌تعالی

طرح درس جهت ارائه در نیمسال دوم سال تحصیلی

دانشکده	**مهندسی برق و کامپیوتر**	**گروه**	**معماری سیستم‌های کامپیوتری**
گرایش	**امنیت سایبری**	**مقطع**	**کارشناسی ارشد**
نام درس	**پروتکل‌های امنیتی**	**نوع درس**	**پایه** ☐ **نظری** ■ **تخصصی** ■ **عملی** ☐ **اختیاری** ☐ **نظری- عملی** ☐
تعداد واحد	**۳**	**نام استاد**	**مهدی آبادی**
دروس پیش‌نیاز		**تلفن دفترکار**	**۸۲۸۸۴۹۳۵**
دروس هم‌نیاز		**پست الکترونیک**	**abadi@modares.ac.ir**

اهداف درس:

- آشنایی با انواع پروتکل‌های امنیتی و مولفه‌های سازنده آن‌ها
- طراحی و پیاده‌سازی پروتکل‌های امنیتی
- استفاده از پروتکل‌های امنیتی در کاربردهای دنیای واقعی

رئوس مطالب و برنامه ارائه در کلاس:

شماره جلسه	موضوع جلسه درس	توضیحات
جلسه اول	مفاهیم پایه • انواع پروتکل‌های امنیتی • مولفه‌های سازنده پروتکل‌های امنیتی • تحلیل پروتکل‌های امنیتی	
جلسه دوم	نظریه اعداد • حساب پیمانه‌ای، قضیه اویلر، عدد صحیح بلوم و قضیه باقی‌مانده چینی	
جلسه سوم	نظریه گروه‌ها • گروه آبلی، گروه متناهی، گروه دوری، زیرگروه، قضیه لاگرانژ، مساله لگاریتم گسسته • الگوریتم پولیگ- هلمن	
جلسه چهارم	نظریه میدان‌ها • میدان متناهی، میدان اول، میدان توسیع و میدان توسیع باینری	
جلسه پنجم	خم (منحنی) بیضوی • خم ناتکین • جمع نقطه، مضاعف‌سازی نقطه و ضرب نقطه • مساله لگاریتم گسسته خم بیضوی	
جلسه ششم	مدیریت کلید • پروتکل‌های انتقال و توافق کلید • پروتکل مبادله کلید دیفی- هلمن • پروتکل مبادله کلید دیفی- هلمن خم بیضوی	

جلسه هفتم	امضای دیجیتالی • طرح امضای RSA-PSS • طرح‌های امضای DSA و ECDSA • امضاهای چشم‌بسته (کور)، وکالتی (نیابتی)، گروهی و آستانه‌ای	
جلسه هشتم	تسهیم راز • طرح تسهیم راز آستانه‌ای شامیر • طرح تسهیم راز آستانه‌ای پیمانه‌ای	
جلسه نهم	اثبات صفر دانش • پروتکل‌های احراز هویت بر پایه اثبات صفر دانش	
جلسه دهم	محاسبات چندطرفه امن • مساله میلیونرها	
جلسه یازدهم	طرح تعهد • پنهان‌سازی شرطی و غیرشرطی • انقیاد شرطی و غیرشرطی طرح تعهد پدرسن (Pedersen)	
جلسه دوازدهم	انتقال ناآگاهانه (بی‌خبر)	
جلسه سیزدهم	رای‌گیری الکترونیکی و انتخابات امن	
جلسه چهاردهم	پول دیجیتالی • پول دیجیتالی برخط و برون‌خط	
جلسه پانزدهم	پروتکل سیگنال • الگوریتم‌های X3DH و Double Ratchet	
جلسه شانزدهم	وب تاریک و شبکه تور (Tor)	

روش ارزشیابی:

- سمینار
- تکالیف
- امتحان میان‌ترم
- امتحان پایان‌ترم

منابع:

[1] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 3rd Edition, Chapman & Hall/CRC Press, 2020.

[2] D. R. Stinson and M. B. Paterson, *Cryptography: Theory and Practice*, 4th Edition, CRC Press, 2019.

[3] S. J. Nielson and C. K. Monson, *Practical Cryptography in Python: Learning Correct Cryptography by Example*, Apress, 2019.

[4] P. Zimmermann, A. Casamayou, N. Cohen, G. Connan, and T. Dumont, *Computational Mathematics with SageMath*, SIAM, 2018.

[5] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer, 2010.

[6] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition, John Wiley & Sons, 1996.

[7] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.