

طرح درس جهت ارائه در نیمسال تحصیلی دوم ۱۴۰۲-۱۴۰۳

دانشکده	مهندسی برق و کامپیوتر	گروه	معماری سیستم‌های کامپیوتری
گرایش	امنیت سایبری	مقطع	کارشناسی ارشد
نام درس	امنیت تجارت الکترونیکی	نوع درس	پایه ☐ نظری ☒ تخصصی ☒ عملی ☐ اختیاری ☐ نظری-عملی ☐
تعداد واحد	۳	نام استاد	صادق دری نوگورانی و حسین همایی
دروس پیش‌نیاز	ندارد	تلفن دفتر کار	۳۹۰۵ و ۵۰۹۸
دروس هم‌نیاز	ندارد	پست الکترونیک	dorri@modares.ac.ir homaei@modares.ac.ir

✓ اهداف درس:

۱. آشنایی با مسائل امنیتی مرتبط با سامانه‌های درگیر در تجارت و کسب و کار الکترونیکی
۲. آشنایی با مشکلات موجود در امنیت پرداخت الکترونیکی و نحوه تأمین آن
۳. آشنایی با فناوری زنجیره قالب و رمزارزها و مسائل و کاربردهای آن در امنیت
۴. آشنایی با معماری امنیتی سازمان

✓ رئوس مطالب و برنامه ارائه در کلاس:

شماره جلسه	موضوع جلسه درس	توضیحات
جلسات هفته اول	مقدمات	معرفی درس، مروری بر مفاهیم اصلی تجارت الکترونیکی، EDI، مروری بر مبانی امنیت فضای تبادل اطلاعات و ویژگی‌های CIA، مروری بر تهدیدها
جلسات هفته دوم	امنیت پروتکل‌های پرداخت	نیازمندی‌ها، حریم خصوصی در وب، پروتکل SET و ...
جلسات هفته سوم	معرفی بیتکوین	معرفی و بررسی BitCoin مشتمل بر مؤلفه‌های اصلی (احراز هویت، تراکنش‌ها، دفترحساب، اجماع)، نحوه استفاده از این رمز ارز، و فراز و فرودهای تاریخی این رمز ارز
جلسات هفته چهارم	عمل کرد سطح پایین بیتکوین	زنجیره قالب‌ها (ساختار، قالب منشأ، و شبکه)، آدرس‌ها و کیف پول در بیتکوین، اجماع PoW، حملات (دوبار خرج کردن، سیبل، ۵۱ درصد)، انواع پاداش در بیتکوین، مشکلات و رقبای بیتکوین، وضعیت قانونی
جلسات هفته پنجم	اتریوم و قرارداد هوشمند	بیتکوین اسکریپت، معرفی اتریوم و قراردادهای هوشمند، نحوه اجرای قراردادهای هوشمند
جلسات هفته ششم	امنیت قرارداد هوشمند	مقدمه‌ای بر امنیت قراردادهای هوشمند، آشنایی بیشتر با زبان Solidity و جزئیات امنیتی، برخی نقاط ضعف متداول، نکات تکمیلی و معرفی برخی ابزارها
جلسات هفته هفتم	انواع بلاکچین	چگونگی اداره (Governance)، انواع بلاکچین، انواع اجماع و مسائل مربوطه نظیر ASIC-resistance، مسائل تکمیلی (Side-chains, sharding)
جلسات هفته هشتم	برنامه‌های روی بلاکچین	Blockchain as a Component, Suitability criteria and design process, Blockchain Patterns (Oracle, off-chain storage, state channel, etc.)
جلسات هفته نهم	کارت‌های پرداخت و هوشمند	بررسی انواع کارت، امنیت کارت‌های مغناطیسی، مقدمه‌ای بر امنیت کارت‌های

هوشمند و استاندارد EMV		
اجزای کارت، نحوه تبادل اطلاعات بین کارت و ترمینال، معرفی ساختار APDU، مدیریت فایل‌ها، معماری امنیتی و مکانیزم‌های امنیتی	عملکرد فنی کارت‌های هوشمند	جلسات هفته دهم
قواعد کنترل دسترسی، تصدیق اصالت، پروتکل‌های تبادل امن، GP، مدیریت برنامه‌ها، دامنه‌های امنیتی، مدیریت کلیدها	امنیت کارت‌های هوشمند	جلسات هفته یازدهم
کارت جاوا، چرخه حیات applet و فرایند به‌کارگیری	کارت جاوا	جلسات هفته دوازدهم
استفاده از سیم‌کارت، ارتباط برنامه‌ها و سیم‌کارت، معرفی NFC، استفاده از بارکد	پرداخت موبایل	جلسات هفته سیزدهم
	استاندارد PKCS#11	جلسات هفته چهاردهم
XML، SOAP، WSDL، UDDI، نیازمندی‌های امنیتی، استانداردهای امنیتی (XML Signature، XML Encryption، SAML، WS-WS-Policy، WS-Reliability، WS-SecureConversation، Security (XACML، SecurityPolicy	امنیت وب‌سرویس‌ها	جلسات هفته پانزدهم
کلاهبرداری: مفهوم کلاهبرداری، روش‌ها، و نحوه تشخیص آن معماری امنیتی: چالش‌ها، نقشه راه، تحلیل ریسک، اصول امن‌سازی شبکه، سیستم‌ها و داده‌ها، اصول مونی‌تورینگ	- روش‌های تشخیص کلاهبرداری - معماری امنیتی	جلسات هفته شانزدهم

✓ روش ارزشیابی:

سمینار (۲ نمره)، پروژه‌ها (۳ نمره)، تمرین‌ها (۲ نمره)، امتحانات (۱۳ نمره)

✓ منابع:

- [1] K.C. Laudon and C.G. Traver, E-Commerce 2017: business, technology, society (13th Ed.), Pearson, 2017.
- [2] M.H. Sherif, Protocols for Secure Electronic Commerce (3rd Ed.), CRC Press, 2016.
- [3] V. Hassler, Security fundamentals for E-commerce, Artech House, 2001.
- [4] R. Wolfgang, and E. Wolfgang, Smart card handbook, John Wiley & Sons, 2004.
- [5] E. Bertino, et al., Security for web services and service-oriented architectures. Springer Science & Business Media, 2009.
- [6] A. Woody, Enterprise security: A data-centric approach to securing the enterprise. Packt Publishing, 2013.
- [7] R. Anderson, Security engineering: a guide to building dependable distributed systems. (3rd edition), John Wiley & Sons, 2020.
- [8] A. Narayanan, J. Bonneau, E. Felten, et al., Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 2016. Chapters 1 and 2. Free pre-publication draft: <http://bitcoinbook.cs.princeton.edu/>
- [9] X. Xu et al., Architecture for Blockchain Applications, Springer Nature Switzerland, 2019.
- [10] International Standard ISO/IEC 7816-4:2005, Identification cards– Integrated circuit cards– Part 4: Organization, security and commands for interchange, 2005.
- [11] GlobalPlatform, GPC_SPEC_034, Card Specification Version 2.3, 2015.
- [12] D. Coderre, Computer Aided Fraud Prevention and Detection: A Step by Step Guide. John Wiley & Sons, 2009.
- [13] N.F. Ryman-Tubb, P. Krause, and W. Garn. "How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark." Engineering Applications of Artificial Intelligence 76 (2018): 130-157.
- [14] M. Rosen, et al., Applied SOA: service-oriented architecture and design strategies. John Wiley & Sons, 2012.

- [15] S. Weerawarana, et al., Web services platform architecture: SOAP, WSDL, WS-policy, WS-addressing, WS-BPEL, WS-reliable messaging and more. Prentice Hall, 2005.
- [16] PKCS #11 Cryptographic Token Interface Base Specification Version 2.40. Edited by Susan Gleeson and Chris Zimman. 14 April 2015. OASIS Standard.