به نام ایزد دانا

(کاربرگ طرح درس)

تاریخ به‌روز رسانی: ۱۳۹۸/۲/۱

دانشکده مهندسی برق و کامپیوتر

نیمسال اول/دوم سال تحصیلی .....

نام درس	فارسی: مبانی رایانش امن	تعداد واحد نظری: ۳	مقطع: کارشناسی■ کارشناسی ارشد□ دکتری□
	لاتین: Fundamentals of Secure Computing	پیش‌نیازها و هم‌نیازها: شبکه های کامپیوتری	
مدرس/مدرسین: رحمانی منش		شماره تلفن اتاق:	
پست الکترونیکی: rahmanimanesh@yahoo.com		منزلگاه اینترنتی:	
برنامه تدریس در هفته و شماره کلاس:			
اهداف درس:			
امکانات آموزشی مورد نیاز: شبکه ی بی سیم دانشگاه			

نحوه ارزشیابی	فعالیت‌های کلاسی و آموزشی (پروژه عملی)	ارزشیابی مستمر(کوئیز)	امتحان میان‌ترم	امتحان پایان‌ترم
درصد نمره	۴	۲	۵	۹

منابع و مآخذ درس

[1] Matt Bishop, Introduction to Computer Security. Addison-Wesley, 2004.
[2] William Stallings, Cryptography and Network Security, Principles and Practices. Prentice Hall, 5th Edition, 2010.
[3] Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley publishing, 2nd Edition, 2008.
[4] William Stallings, Network Security Essentials: Applications and Standards. Prentice Hall, 4th Edition, 2010.

بودجه‌بندی درس

شماره هفته آموزشی	مبحث	توضیحات
۱	مفاهیم امنیت اطلاعات، تهدیدها و حملات، سرویسهای امنیتی	
۲	کلیات دانش رمز، تاریخچه رمزنگاری، روشهای سنتی رمزنگاری	
۳	الگوریتم رمزنگاری متقارن DES	
٤	الگوریتم رمزنگاری نامتقارن RSA، الگوریتم رمزنگاری نامتقارن طاهر الجمال	
٥	روش مبادله کلید دیفی - هلمن، الگوریتم محاسبه چکیده پیام MD5	
٦	جلسه عملی (سیستم عامل کالی)	
۷	ارائه مقاله	
۸	OTP، اجزای سیستمهای رمزنگاری متقارن، روشهای رمزنگاری متقارن	
۹	الگوهای زنجیره سازی بلوکهای رمز	
۱۰	جلسه عملی (امنیت در شبکه های بیسیم)	
۱۱	ارائه مقاله	
۱۲	روشهای چکیده پیام، MAC	
۱۳	جلسه عملی (پیاده سازی یک سناریوی حمله)، تعریف پروژه	
١٤	امضای دیجیتالی، گواهینامه های دیجیتالی	
١٥	ارائه مقاله	
١٦	رفع اشکال	