دانشکده مهندسی برق و کامپیوتر

پایان‌ترم درس امنیت شبکه پیشرفته

۱۸ تیر ۱۴۰۱

زمان: ۹۰ دقیقه مدرس: اصغریان

نام و نام خانوادگی:

شماره دانشجویی:

۱	با استفاده از دو عدد اول ۲۳ و ۳۷ یک زوج کلید RSA تولید کنید (از ۱۷ به عنوان نمای عمومی استفاده کنید). سپس عدد ۱۴ را با آن رمز کنید. همه مراحل را توضیح دهید.	۳ نمره
۲	سبک کاری OFB را توضیح دهید. آیا در این سبک کاری عملیات رمزنگاری و رمزگشایی قابل موازی سازی است؟ چرا؟	۲ نمره
۳	انواع حملات XSS را نام ببرید و نحوه انجام یکی از آنها (سناریوی حمله) را به دقت توضیح دهید.	۳ نمره
۴	کلید اعطای بلیط *TGT* به چه منظور در پروتوکل کربروس استفاده می شود؟ ساختار کلید اعطای بلیط را دراین پروتکل توضیح دهید و دلیل وجود هر جزء را بیان کنید.	۳ نمره
۵	در مورد توابع درهم‌سازی ویژگی‌های «مقاومت در برابر یافتن پیش نگاره اول» و «مقاومت در برابر یافتن پیش نگاره دوم» را توضیح دهید. کدام یک از این دو ویژگی از «ویژگی مقاومت در برابر تصادم» نتیجه می‌شود؟ توضیح دهید.	۳ نمره
۶	درستی یا نادرستی هرکدام از جملات زیر را با ذکر دلیل مشخص کنید؟ *الف) فایروال‌های لایه کاربرد نوعی از فایروال‌های **حالتمند** هستند که می توانند حملات هوشمند علیه برخی سرویس‌ها را تشخیص دهند* *ب) سیستم‌های تشخیص نفوذ مبتنی بر **تشخیص سوء استفاده** یک پروفایل از رفتار عادی سیستم را نگهداری می‌کنند و با استفاده از آن حملات را تشخیص می‌دهند* *ج) به علت نرخ خطای بالای سیستم‌های تشخیص نفوذ، امروزه سیستم‌های همبسته‌ساز هشدارها **جایگزین** آنها شده‌اند* *د) کنترل جریان اطلاعات با کمک مدل‌های کنترل دسترسی اختیاری امکان‌پذیر نیست* *ه) در روش رمزنگاری RSA کلید خصوصی از روی کلید عمومی به هیچ وجه قابل محاسبه نیست* *و) طبق اصول کرکهفس الگوریتم‌های رمزنگاری باید محرمانه باقی بمانند*	۶ نمره