دانشگاه صنعتی امیرکبیر
دانشکده مهندسی کامپیوتر

تمرین‌های درس مبانی امنیت اطلاعات

دکتر حمیدرضا شهریاری

مهدی نیکوقدم

پاییز ۱۴۰۱

۱. توضیح دهید که چگونه می‌توان از رمزنگاری کلید عمومی برای توزیع یک کلید مخفی استفاده کرد؟

۲. این امکان وجود دارد که از یک تابع درهم‌ساز برای ساخت یک رمز قالبی با ساختاری مشابه DESاستفاده کرد. با توجه به اینکه یک تابع درهمساز، یک طرفه بوده ولی یک رمز قالبی بایستی برگشتپذیر باشد (برای رمزگشایی) چگونه این امر ممکن است؟

۳. در یک سیستم کلید عمومی از رمزنگاری RSA استفاده می‌کند، متن رمز شده ما برابر C=10 را برای کاربری با کلید عمومی n=35 و e=5 ارسال شده است. اگر شما استراق سمع‌کننده باشید، متن واضح M را به دست آورید.

۴. در روش دیفی هلمن با یک عدد اول q=11 و ریشه اولیه a=2 موارد زیر را در نظر بگیرید:

الف- اگر کاربر A دارای کلید عمومی $pub_a = 9$ باشد، کلید خصوصی کاربر A را به دست آورید.

ب- اگر کاربر B دارای کلید عمومی $pub_b = 3$ باشید کلید سری مشترک K کدام است؟

۵. امضای دیجیتال چیست و چه ویژگی‌هایی دارد؟

۶. در مورد امضای دیجیتال کور تحقیق کنید و چکیده تحقیقات خود را در حد دو پاراگراف بیان کنید.

۷. الگوریتم RSA را برای رمزنگاری و رمزگشایی با توجه به مقادیر زیر به کار ببرید:

M=3 ,e=11,q=13 , p=11

عکسی واضح از برگه پاسخ تهیه و به فرمت **pdf** در آورید و آپلود کنید.

- فرمت نامگذاری پاسخ به صورت **HW2_StdNO_StdName** باشد.
- پاسخ تمرینات حتما **قبل از موعد** تحویل اعلام شده در هر سری، بارگذاری شوند. تمریناتی که بعد از موعد تحویل ارسال شوند **به هیچ عنوان** تصحیح نخواهند شد.
- در صورت مشاهده تمرینات **کپی شده** برای طرفین **نمره صفر** در نظر گرفته می‌شود.

هدف افزایش یادگیری است!

مهدی نیکوقدم