*** مرجع : فصل ۲ و ۳ نسخه ۵ کتاب Network Security Essentials

فصل دوم :

۱. (مساله ۲.۶ بخش problems از کتاب)

۲. (مساله ۲.۱۲ بخش problems از کتاب)

۳. برای رمزنگاری ۱۴ بیت از الگوریتم **3DES** استفاده کردیم به گونهای که هر مرحله رمزنگاری و یا رمزگشایی Feistel بدون جایگشت با **۲** دور با **کلید یکسان** برای هر دو دور (در یک مرحله) استفاده شده است . در این الگوریتم تابع ترکیب با کلید در همه حالات $F(x,k) = x \text{ XOR } k$ در نظر گرفته شده است . اگر کلید مرحله اول $k_1=0110010$ و کلید مرحله دوم $k_2=1000111$ و کلید مرحله سوم $k_3=0111000$ و نتیجه نهایی نهایی (عبارت رمزشده) به صورت $c =$ 10100001010011 باشد ، عبارت اصلی یا همان plaintext را بیابید .

۴. اگر عبارت اصلی به صورت $p=1100100111010101$ باشد و هر بلوک داده را 4 بیت در نظر بگیریم ، نتیجه رمزنگاری با الگوریتم DES با یک دور Feistel با اطلاعات زیر را در مدهای کاری CBC، ECB و CTR محاسبه کنید .

key = 1011 ,$F(x, Key) = (x \times Key) \ mod \ 15$,IV=0010,initial_counter=0

فصل سوم :

۵. (مساله ۳.۲ بخش problems از کتاب) فرض کنید که H(m) یک تابع درهم سازی و مقاوم در برابر تصادم باشد که پیام ورودی با طول دلخواهی از بیت ها را به یک مقدار n بیتی نگاشت میکند . آیا درست است که بگوییم اگر دو پیام دلخواه و متمایز را به عنوان ورودی به تابع بدهیم نتیجه درهم سازی آنها هم متمایز خواهد بود ؟ برای پاسخ خود دلیل بیاورید .

۶. (مساله ۳.۱۰ از بخش problems کتاب)

۷. الگوریتم RSA را یک بار جهت رمزنگاری و بار دیگر جهت رمزگشایی برای مقادیر p=11 و q=13 و e=11 و M=3 به کار ببرید .

۸. کاربرد الگوریتم DSS چیست و چگونه امکان احراز را هویت را فراهم میکند ؟

۹. روش موجود برای احراز هویت توسط رمزنگاری عمومی (با کلید متقارن) را با روش موجود برای احراز هویت با استفاده از داده مخفی وتابع درهم سازی مقایسه کنید .(به تفاوت پیام های ارسالی در هر روش و شیوه تصدیق هویت در مقصد توجه کنید.)

- پاسخ تمرینات حدالامکان به صورت **تایپ شده و فایل PDF** تحویل داده شود. در صورت عدم امکان تایپ پاسخ تمرین ، عکسی واضح از برگه پاسخ تهیه و به فرمت PDF در آورید. (برای اینکار میتوانید از camScanner و امثال آن استفاده کنید.)
- فرمت نامگذاری پاسخ به صورت **HW2_StdNO_StdName** باشد.
- تاخیر در بارگذاری تا ۳ روز موجب کسر حداقل ۲۵ درصد از نمره تمرین خواهد شد. تمریناتی که بعد از ۳ روز از موعد تحویل ارسال شوند ، **تصحیح نخواهد شد.**
- در صورت مشاهده **تقلب** برای طرفین **نمره صفر** در نظر گرفته می شود.
- در صورت وجود هر گونه سوال یا اشکال در رابطه با تمرین از آدرس ایمیل f.dehghan@aut.ac.ir استفاده کنید.