تمرین شماره ۳

درس: مبانی امنیت شبکه‌های کامپیوتری

استاد: دکتر مهسا سعیدی

دستیاران آموزشی: علی عابدینی، علی دارابی و محمدرضا ولی

نیمسال اول سال تحصیلی ۰۵-۱۴۰۴

سوال 1)

فرض کنید شما یک تولیدکننده بیت تصادفی واقعی دارید که در آن هر بیت در جریان تولید شده، همان احتمال ۰ یا ۱ بودن را دارد و بیت‌ها هم‌بستگی ندارند؛ یعنی بیت‌ها از توزیع یکسان و مستقل تولید می‌شوند. با این حال، جریان بیت دارای سوگیری است. احتمال ۱ بودن بیت‌ها برابر با $0.5+\delta$ و احتمال ۰ بودن برابر با $0.5-\delta$ است، به طوری که محدوده زیر برقرار باشد:

$$0 < \delta < 0.5$$

یک الگوریتم ساده برای اصلاح بیت‌ها به این صورت است که جریان بیت را به صورت دنباله‌ای از جفت‌های غیر هم‌پوشان بررسی می‌کنیم، تمام جفت‌های ۰۰ و ۱۱ را حذف کرده و هر جفت ۰۱ را با ۰ و هر جفت ۱۰ را با ۱ جایگزین می‌کنیم.

a) احتمال وقوع هر جفت در دنباله اصلی چقدر است؟

b) احتمال وقوع ۰ و ۱ در دنباله اصلاح شده چقدر است؟

c) تعداد متوسط بیت‌های ورودی برای تولید x بیت خروجی چقدر است؟

سوال 2)

فرض کنید باب از سامانه رمزنگاری RSA با پیمانه بسیار بزرگ n استفاده می‌کند که فاکتور گیری از آن در زمان معقول ممکن نیست. فرض کنید آلیس پیامی برای باب می‌فرستد به این صورت که هر حرف الفبایی را به یک عدد صحیح در بازه 0 تا 25 نگاشت می‌کند ($A \rightarrow 0، B \rightarrow 1، ...، Z \rightarrow 25$) و سپس هر عدد را به‌صورت جداگانه با RSA با نمای e و پیمانه بزرگ n رمز می‌کند. آیا این روش امن است؟ پاسخ خود را توجیه کنید. همچنین کارآمدترین حمله ممکن علیه این سناریوی رمزنگاری را توضیح دهید.

سوال 3)

شش استاد، دوره‌های خود را به ترتیب در روزهای دوشنبه، سه‌شنبه، چهارشنبه، پنج‌شنبه، جمعه و شنبه آغاز می‌کنند و قصد دارند با فواصل ۳، ۲، ۵، ۶، ۱ و ۴ روز تدریس کنند. مقررات دانشگاه اجازه تدریس در روز یکشنبه را نمی‌دهد (بنابراین تدریس یکشنبه باید حذف شود). اولین باری که همه شش استاد مجبور به حذف یک جلسه خواهند شد چه زمانی است؟

راهنمایی: از قضیه باقی‌مانده‌های چینی (CRT) استفاده کنید.

سوال 4)

می‌خواهیم یک پروتکل تبادل امن مبتنی بر دیفی-هلمن طراحی کنیم. فرض کنید قبل از اجرای پروتکل، A و B پارامترهای a و b را به صورت امن به اشتراک گذاشته‌اند. هر یک از طرفین به کلید عمومی طرف مقابل نیز دسترسی دارد. پروتکل خود را به گونه‌ای طراحی کنید که در برابر حملات Replay و Man in the Middle آسیب‌پذیر نباشد. همچنین خصوصیات پروتکل خود را بیان کنید.

سوال 5)

در این سوال شما نقش ایو را دارید و گفت و گوهای زیر را میان آلیس و باب شنود می‌کنید:

- آلیس: بیایید با عدد اول در پروتکل دیفی-هلمن کاری نداشته باشیم، این کار را راحت‌تر می‌کند.
    - باب: باشه، ولی هنوز به یک پایه a نیاز داریم. a=3 چطور است؟
- آلیس: باشه، پس نتیجه من 27 است.
    - باب: و نتیجه من 243 است.

کلید خصوصی باب XB و کلید خصوصی آلیس XA چیست؟ کلید مشترک مخفی آنها چیست؟ مراحل محاسبات خود را نشان دهید.

ملاحظات تمرین

مهلت تحویل: 27 آبان ماه

- تمرین‌ها به صورت انفرادی انجام می‌شوند.
- لطفا پاسخ خود را در قالب یک فایل PDF با فرمت زیر در سامانه Elearn بارگذاری کنید:

StudentID_Lastname_HW3

- امکان ارسال تمرین نهایتاً با دو روز تاخیر با کسر ۱۰ درصد نمره به ازای هر روز وجود دارد.
- در صورت استفاده از منابعی غیر از کتاب مرجع در انجام تمرین، لطفاً حتماً نام منبع خود را ذکر کنید. در صورت مشاهده شباهت غیرمعمول میان پاسخ‌های دو نفر یا در صورتی که پاسخ‌ها برابر با محتوای منابعی غیر از کتاب مرجع باشد و نام منابع مورد استفاده ذکر نشده باشد، نمره‌ای برای شما منظور نخواهد شد.
- می‌توانید سوالات خود را از طریق آیدی‌های تلگرام زیر یا گروه تلگرامی درس مطرح کنید:
  - abediniAli1@
  - Ali_819@
  - Jaxteler@

موفق باشید!