تمرین شماره 1

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 دو متن رمزنگاری شده زیر را در اختیار دارید:

```
c1 = 11111001011110011100110000010111 10000110

c2 = 11111010011001111011101000010011 10001000
```

همچنین فرض کنید که هر دو متن رمزنگاری‌شده One-Time Pad (OTP) هستند و با یک کلید یکسان رمزگذاری شده‌اند. همچنین دو حالت زیر را در نظر بگیرید:

a) یا c1 متن رمزنگاری‌شده کلمه alpha و c2 متن رمزنگاری‌شده کلمه bravo است
b) یا c1 متن رمزنگاری‌شده کلمه delta و c2 متن رمزنگاری‌شده کلمه gamma است (همه کلمات به روش استاندارد از ASCII به باینری تبدیل شده‌اند).

کدام یک از این دو حالت صحیح است؟ دلیل خود را بیان کنید. کلید k چه بوده است؟

سوال 2)

با استفاده از جدول استاندارد ASCII، به صورت دستی یک نسخه رمزنگاری‌شده با Base64 از رشته hello\njello بسازید و مراحل فرآیند تبدیل خود را نشان دهید. پس از ارائه متن رمزنگاری‌شده، هدف از کاراکتر = که در انتهای نمایش Base64 ظاهر می‌شود را توضیح دهید.

منبع:

Computer and Network Security by Avi Kak, accessed October 1, 2025,
https://engineering.purdue.edu/kak/compsec/

سوال 3)

یک اسکریپت پایتون بنویسید که عملکرد DES را پیاده‌سازی کند؛ برای انجام این کار از S-box هایی استفاده کنید که برای استاندارد DES مشخص شده‌اند (illustrate_des_substitution.py). اطمینان حاصل کنید که تمام مراحل تولید کلید را که در این لینک ذکر شده است، پیاده‌سازی کرده‌اید. برای کلید رمزگذاری، اسکریپت شما باید از کاربر یک ورودی کیبورد درخواست کند که شامل حداقل ۸ کاراکتر اسکی (ASCII) قابل چاپ باشد. (شما می‌توانید انتخاب کنید که از هفت بیت اول یا هفت بیت آخر هر بایت کاراکتر برای کلید ۵۶ بیتی مورد نیاز DES استفاده کنید.)

چیزی که این تکلیف را آسان‌تر از آن‌چه فکر می‌کنید می‌کند این است که وقتی کد مربوط به پردازش یک دور را نوشتید، اساساً از همان کد در یک حلقه برای کل زنجیره رمزگذاری و زنجیره رمزگشایی استفاده خواهید کرد. بدیهی است که برای زنجیره رمزگشایی، باید ترتیب استفاده از کلیدهای دور را معکوس کنید.

هر چند می‌توانید کد خود را از ابتدا بنویسید، توصیه می‌شود وقتی از پایتون استفاده می‌کنید، ممکن است بخواهید با کلاس **BitVector** شروع کنید. همچنین برای تسهیل روند پیاده‌سازی می‌توانید به فایل **hw1_starter.py** مراجعه نمایید.

سوال 4)

اکنون پیاده‌سازی‌ای را که برای سوال 3 ایجاد کرده‌اید، با پر کردن جداول ۴×۱۶ مربوط به S-box ها با اعداد صحیح تولید شده به صورت تصادفی، اصلاح کنید. بدیهی است که هر ورودی تولید شده به صورت تصادفی باید بین ۰ و ۱۵ باشد (شامل هر دو عدد). اثر بهمنی (avalanche effect) را برای این پیاده‌سازی DES محاسبه کرده و آن را با همین اثر برای پیاده‌سازی قبلی خود مقایسه کنید. (برای آشنایی با اثر بهمنی به این لینک مراجعه کنید.)

* خروجی سوال 3 و 4 را به صورت **Q3_4_solution.py** همراه با تشریح و اسکرین‌شات از عملکرد کد و پاسخ سایر سوالات در قالب یک فایل pdf سوالات آپلود کنید.*

سوال 5)

فرض کنید یک دنباله از بلوک‌های متن با استفاده از DES رمزنگاری‌شده و به همین ترتیب یک دنباله از بلوک‌های متن رمزگذاری‌شده تولید شده است. حال فرض کنید یکی از بلوک‌های متن رمز هنگام ارسال به اشتباه منتقل شود (یعنی برخی بیت‌ها به طور ناخواسته از ۱ به ۰ یا از ۰ به ۱ تغییر کنند). ثابت کنید که تعداد بلوک‌های متن که هنگام رمزگشایی به اشتباه بازسازی می‌شوند برابر است با:

- یک بلوک، اگر حالت‌های رمزنگاری ECB یا OFB استفاده شده باشد.
- دو بلوک، اگر حالت‌های رمزنگاری CBC یا CFB استفاده شده باشد.

ملاحظات تمرین

مهلت تحویل: ۲۴ مهر 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_HW1

- 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!