به نام خدا

دانشکده مهندسی کامپیوتر

تمرین عملی دوم، درس مبانی امنیت اطلاعات

دکتر حمیدرضا شهریاری

آبان ۱۴۰۱

نکات مهم

- **کد:** استفاده از کتابخانه‌های رایج در محدوده هک و امنیت در زبان پایتون و محیط‌های توسعه مانند VSCode و یا Google Colab مجاز است.
- **گزارش:** ملاک اصلی انجام پروژه و گزارش آن است و ارسال کد بدون گزارش فاقد ارزش است. لذا می‌بایست یک فایل گزارش با فرمت pdf تهیه کنید و در آن برای هر قسمت از فعالیت صورت گرفته درباره تمرین، تصاویر اسکرین شات، تصاویر خروجی مربوطه و همچنین توضیحات مربوط به آن‌ها را ذکر کنید. سعی کنید تا حدامکان توضیحات کامل و جامعی تدوین کنید.
- **تذکر:** مطابق قوانین دانشگاه، هر نوع کپی برداری و اشتراک کار دانشجویان غیرمجاز بوده و **نمره هر دو نفر منفی** لحاظ خواهد شد.
- **راهنمایی ۱:** در صورت نیاز می‌توانید سوالات خود را در خصوص انجام پروژه، از طریق راه‌های ارتباطی زیر از تدریس‌یار بپرسید:

  آدرس ایمیل: mahmood.faraji133@gmail.com

  شناسه تلگرام: @mahmoudfaraji

  لطفا در صورت ارسال ایمیل عنوان آن را Information_Sec قراردهید.
- **ارسال:** فایل گزارش به همراه کدهای نوشته شده را در قالب یک فایل فشرده (zip) همانند فرمت زیر در سامانه بارگذاری نمایید: Prj2_StudentNumber.zip

  در مجموع تمامی تمرین‌های عملی تنها ۱۰ روز تاخیر مجاز بوده که همراه با کسر درصدی از نمره خواهد بود و پس از این زمان نمره تمرین مربوطه بطور کامل حذف خواهد شد.

کار با کتابخانه‌های رمزنگاری

✓ تعریف تمرین

در این تمرین، هدف کار با کتابخانه‌های رمزنگاری در زبان پایتون می‌باشد. بدین صورت که نیاز است با استفاده از کتابخانه‌ی pyaes، os، pbkdf2، binascii و secrets اقدام به کدنویسی و ساخت برنامه‌ای نمایید که بتواند با استفاده از الگوریتم AES در مد CTR، فایلی که شماره دانشجویی هر دانشجو داخل آن می‌باشد را تبدیل به یک فایل رمزنگاری شده کرده و سپس با دستور کاربر آن را رمزگشایی کند.

✓ قوانین تمرین

۱. برای انجام تمرین نیاز است ابتدا یک مقدار را به عنوان کلید رمزنگاری که در بخش ۸ گفته شده است، در نظر بگیرید. سپس با استفاده از کتابخانه os یک salt به آن اضافه نمایید.
۲. مقداری که برای کلید در نظر گرفته می‌شود، بطور معمول در یک فایل جداگانه‌ای می‌بایست ذخیره شود و در زمان نیاز، فایل کلید خوانده شود. به عبارتی در نرم‌افزارهای این چنینی، نباید کلید الگوریتم‌های رمزنگاری در بین کدهای نرم‌افزار اصطلاحا Hard Code شود.
۳. نیاز است پس خواندن کلید از فایل مربوطه‌اش، طول آن را با استفاده از کتابخانه pbkdf2 به ۲۵۶ بیت رسانده و سپس با استفاده از کتابخانه binascii هگز آن را به اپراتور استفاده کننده از ابزار نشان دهید.
۴. پس از آن نیاز است با استفاده از کتابخانه secrets یک initial vector برای استفاده در مد CTR تولید نمایید.
۵. سپس فایل مورد نظر را برای رمزنگاری از سیستم بخوانید و با استفاده از کتابخانه pyaes و متد مربوط به استفاده مد CTR اقدام به رمزکردن فایل مورد نظر کرده و Ciphertext آن را در یک فایل ذخیره نمایید.
۶. بدیهی است که برای رمزگشایی نیاز است initial vector ساخته شده در مرحله ۴ و کلید گفته شده در بخش ۱ را به الگوریتم بدهید تا بتواند عمل رمزگشایی را به درستی انجام دهد و در فایل دیگری ذخیره نماید.
۷. برای ایجاد فایل مورد نظر جهت انجام رمزنگاری، شماره دانشجویی خود را در یک فایل txt نوشته و ذخیره نمایید.
۸. کلید اولیه الگوریتم را مقدار روبه‌رو در نظر بگیرید: AUT*ICTSec*2022

۹. سعی کنید ابزار خواسته شده را به گونه‌ای توسعه دهید که تحت کنسول اجرا شده و برای عمل رمزنگاری و رمزگشایی از کاربر فرمان بگیرد. به عنوان نمونه اگر کاربر حرف E را وارد کرد عمل Encryption و اگر D را وارد کرد عمل Decryption را انجام دهد.

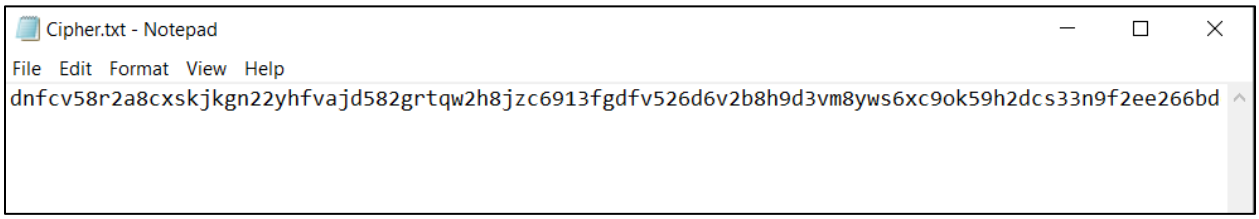
۱۰. از تمامی مراحل انجام کار خود اسکرین‌شات گرفته و همراه با توضیحات، به فرمت گفته شده در بند "ارسال" قسمت نکات مهم در ابتدای این سند، در سامانه courses بارگذاری نمایید.

مثال‌هایی از خروجی مورد نظر در ادامه آمده است:

- به عنوان نمونه پس از ساخته شدن کلید با طول ۲۵۶ و نمایش بصورت هگز به کاربر، خروجی مانند تصویر زیر مورد نظر است:

```
Algorithm key is: b'85asr356dl0ttee321uy644hj85asdc5621kj47kjqwzserdx235846dxsd524f5'
```

- پس از انجام عمل رمزنگاری، خروجی ابزار در یک فایل txt مانند زیر ذخیره شده است:



موفق باشید.