تمرین کامپیوتری شماره 1: رمزنگاری **ارزهای رمزنگاری شده**

مهلت تحویل: 27 فروردین 1403

مدرس: **دکتر شریعت پناهی**

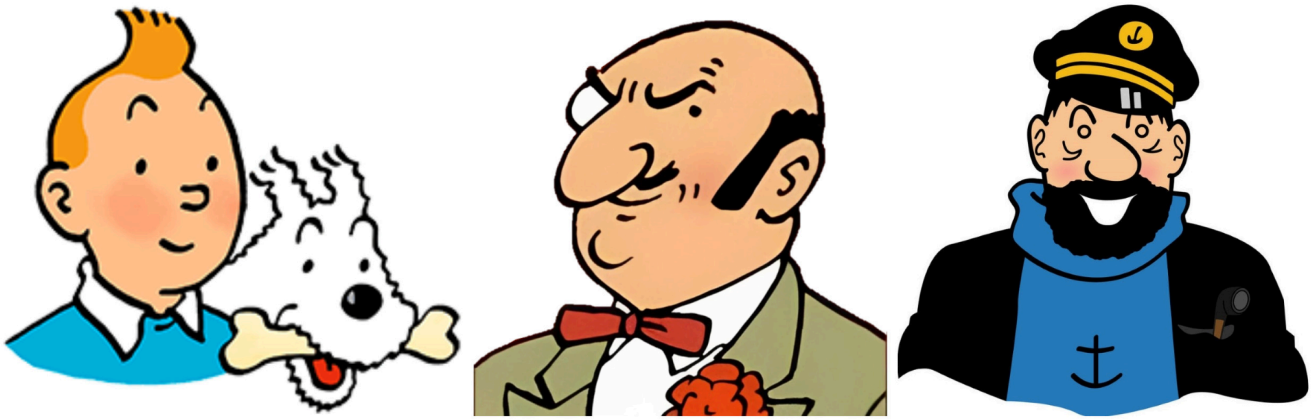
طراحان: علیرضا اربابی

مقدمه:

هدف پروژه فوق، آشنایی عملی با مفاهیم رمزنگاری متقارن و نامتقارن، به همراه متدهای رمزنگاری مانند توابع Hash و امضای دیجیتال با استفاده از زبان پایتون می‌باشد.

خط داستانی:

در سری داستان های تن تن[1] و میلو[2]، تن تن و کاپیتان هادوک[3] در دو جزیره متفاوت ایستاده اند و دشمن دیرینه آنها، روبرتو راستاپاپولوس[4] در جزیره ای در میان قرار دارد. تن تن و هادوک قصد دارند تا با استفاده از کد مورس[5] برای یکدیگر پیام ارسال کنند، اما روبرتو نیز پیام آنها را می‌شنود و قصد دارد تا از نقشه های آندو با شنود پیام هایشان با خبر شود!



[1] Tin Tin
[2] Milo
[3] Captain Haddock
[4] Roberto Rastapopoulos
[5] Morse Code

تن تن برای پیدا کردن راه حلی جهت دور زدن روبرتو اقدام به شرکت کردن در کورس رمزنگاری Modern Cryptography از سایت کورسرا نموده (مطالب رمزنگاری مربوط به پروژه را در کلاس یاد گرفته اید و کورس فوق جهت اطلاعات تکمیلی قرار می‌گیرد) و حال قصد دارد تا تا با رمز کردن پیغام های خود، روبرتو را از شنود پیغام ها گمراه کند. جهت سهولت در انجام کار، یک فایل نوت بوک ژوپیتر در سایت قرار گرفته و با تکمیل کردن آن، تن تن را در رسیدن به هدف خود جهت ایجاد ارتباط امن یاری کنید!

قسمت اول: رمزنگاری متقارن

تن تن تصمیم می‌گیرد تا از یک سیستم رمزنگاری متقارن برای ارتباط خود با هادوک استفاده کند. به همین جهت از شما خواسته است تا سیستم فوق را با شرایط زیر پیاده سازی کنید:

در تمامی قسمت ها از الگوریتم رمزنگاری AES-128 جهت رمزنگاری متقارن استفاده کنید. می‌توانید جهت سهولت در انجام عملیات encryption/decryption از کتابخانه های پایتون استفاده کنید.

1. تابعی بنویسید که یک متن ورودی به همراه کلید رمزنگاری را از آرگومان دریافت کرده و پیغام رمزشده با الگوریتم AES-128 را خروجی دهد.
2. متن Confidential Message که در فایل zip پروژه قرار دارد را با استفاده از یک کلید تصادفی رمز کنید.
3. تابعی بنویسید که پیغام رمزشده به همراه کلید رمزنگاری را به عنوان آرگومان دریافت کرده و پس از decrypt کردن پیغام رمزشده، پیغام plaintext را خروجی دهد.
4. تابعی بنویسید که صحت عملیات decryption توسط تابع قسمت 3 را با مقایسه متن خروجی با متن اولیه بسنجد.

در پایان، صحت کارکرد تمامی توابع را با ورودی ذکر شده بررسی کنید.

قسمت دوم: رمزنگاری نامتقارن

پس از آنکه تن تن عملیات رمزنگاری متقارن را انجام داد، با چالش دیگری روبرو شد: چگونه می‌توان کلید رمزنگاری متقارن را به هادوک ارسال کنم، بدون آنکه روبرتو در میانه راه از آن باخبر شود؟
تن تن با سرچ کردن در اینترنت با مفهوم رمزنگاری نامتقارن RSA آشنا شده است، و حال از شما می‌خواهد مکانیزمی جهت ساخت کلید رمزنگاری نامتقارن با استفاده از RSA پیاده سازی کنید:

1. ابتدا با استفاده از کتابخانه های پایتون، یک جفت کلید عمومی و خصوصی (Public Key و Private Key) رمزنگاری RSA بسازید.
2. تابعی بنویسید که یک پیغام را با استفاده کلید عمومی (Public Key) رمز کند. سپس تابع دیگری بنویسید تا پیغام رمز شده را با استفاده از کلید خصوصی (Private Key) رمزگشایی کند.
3. صحت کارکرد توابع فوق را بررسی کنید تا از کارکرد صحیح آنها اطمینان حاصل کنید.

قسمت سوم: امضای دیجیتال

حال تن تن از توابع قسمت اول و دوم استفاده کرده و پیغام خود را به هادوک می‌فرستد، اما متوجه می‌شود که سیستم رمزنگاری او هنوز کامل نیست! نقص فعلی سیستم او آن است که پیغام های رد و بدل شده با وجود آنکه به درستی رمزنگاری و رمزگشایی می‌شوند، فاقد امضای ارسال کننده هستند و اگر کسی آن پیام ها را بخواند، راهی برای اهراز هویت (اصالت) فرستنده ندارد. به همین جهت، تن تن از شما میخواهد تا جهت رفع مشکل فوق، یک سیستم امضای دیجیتال[6] را مطابق قدم های زیر پیاده سازی کنید:

1. تابعی بنویسید که یک متن ورودی به همراه کلید خصوصی RSA را به عنوان آرگومان دریافت کرده و متن ورودی را با استفاده از کلید فوق امضا کند و امضا را خروجی دهد. (توجه کنید که جهت ایجاد امضای دیجیتال، می‌بایست هش پیغام ورودی را امضا کنیم، نه کل پیغام را. چرا؟)
2. تابعی بنویسید که صحت امضای یک پیغام را با دریافت پیغام و امضای آن به عنوان آرگومان بررسی کند.
3. درباره پیغام MAC و HMAC در اینترنت جست‌وجو کنید و کاربردهای آنها در پیام‌رسانی امن ذکر کنید.

در پایان، صحت کارکرد تمامی توابع را با استفاده از ورودی و بررسی خروجی ها، بررسی کنید.

نکات تکمیلی:

- جهت انجام پروژه فوق، فایل نوت بوک موجود در سایت را دانلود کرده و قسمت های خالی نوت بوک را تکمیل کنید.

[6] Digital Signature

- لطفا به سوالات تشریحی موجود در صورت پروژه نیز در فایل نوت بوک به صورت Markdown پاسخ دهید و از ارسال فایل PDF مجزا بپرهیزید.
- **تقلب نکنید! پروژه جهت یادگیری شما می‌باشد** و در صورت وجود ابهام، با طراحان تمرین در ارتباط باشید. توجه کنید که پروژه فوق به صورت آنلاین تحویل گرفته خواهد شد و لازم است تا بر کد خود تسلط کافی داشته باشید.
- لطفا فایل نوت بوک ژوپیتر نهایی پروژه خود را به صورت فایل **ZIP** به فرمت **CA#1-FamilyName-StudentID.zip** در سامانه بارگزاری نمایید.