دانشگاه صنعتی اصفهان
دانشکده مهندسی برق و کامپیوتر

مبانی رایانش امن

تکلیف ۱

دستیار آموزشی

داراب زندیه
مهدی آقاجانیان

استاد

دکتر مجتبی خلیلی

زمان تحویل

1403/12/24

نکات تحویل تکلیف

- فایل‌های خود را با فرم `PHW1_Name1_StudentNum1_Name2_StudentNum1.zip` ارسال کنید. توجه شود که به فایل‌هایی که نام‌گذاری آنها به‌صورت فرمت گفته‌شده نباشد، نمره‌ای تعلق نخواهد گرفت.
- پاسخ‌های شما باید به‌صورت تایپ‌شده باشد، به پاسخ‌های دست‌نویس نمره‌ای تعلق نخواهد گرفت.
- به پاسخ‌های بدون توضیح امتیاز و نمره‌ای تعلق نخواهد گرفت.
- در صورت وجود هرگونه ابهام می‌توانید از طریق تلگرام سؤالات خود را با دستیار آموزشی مربوط به این تکلیف مطرح کنید. آیدی تلگرام دستیار آموزشی مربوط به این تکلیف: @dzshb
- در صورت وجود شباهت واضح، نمره‌ای به پاسخ تعلق نمی‌گیرد.
- پاسخ تکلیف را حتماً در سامانه یکتا آپلود کنید و از ارسال تکلیف به ایمیل یا تلگرام اکیداً خودداری کنید.
- **مشارکت گروهی:** همه اعضای گروه باید مشارکت کنند (مثلاً در کدنویسی، تحلیل، آماده‌سازی ویدئو).
- **کد و ابزارها:** تمام کدهای منبع (مثلاً اسکریپت‌های پایتون برای سوال ۴)، دستورات یا ابزارهای استفاده‌شده را با توضیحات مختصر یا شرح عملکردشان ارائه دهید.
- **توضیحات ویدیویی:** برای هر سوال، یک ویدئو ارائه دهید که راه‌حل را توضیح داده و نتایج را نشان دهد. ویدئو را با شماره سوال به وضوح برچسب‌گذاری کنید.
- **گزارش:** برای هر سوال یک گزارش کتبی ارائه دهید که شامل:
  - پاسخ به تمام بخش‌های سوال.
  - تصاویر، عکس‌ها یا نمایش‌های بصری در صورت درخواست (مثلاً تصاویر رمزنگاری‌شده برای سوال ۴، خروجی ابزارها برای سوال ۱).
  - توضیحات و تحلیل‌ها طبق مشخصات (مثلاً حداقل ۲۰۰ کلمه برای تحلیل سوال ۴).
- **نام‌گذاری فایل‌ها:** فایل‌ها را به‌وضوح نام‌گذاری کنید (مثلاً `Q1_solution.pdf`، `Q4_code.py`، `Q4_video.mp4`) و در صورت نیاز در پوشه‌هایی بر اساس شماره سوال سازمان‌دهی کنید.

۱ سوال ۱

در فایل Q۱، پوشه‌ای وجود دارد که شامل ۵۰۰۰ فایل یکسان است (می‌توانید از دستور cat برای مشاهده محتوای این فایل‌ها استفاده کنید). یکی از این فایل‌ها تفاوت جزئی با بقیه دارد که به راحتی قابل تشخیص نیست. با استفاده از مفاهیم تدریس‌شده در کلاس، این فایل را پیدا کنید و نام آن را ذکر کنید. اگر از ابزار، دستور یا کدی استفاده کردید، حتماً عکسی از آن ضمیمه کنید و توضیحات کاملی ارائه دهید.

توجه: به راه‌حل‌ها یا روش‌هایی که مرتبط با مطالب درسی نباشند، امتیازی تعلق نمی‌گیرد.

۲ سوال ۲

می‌دانیم که یکی از ویژگی‌های اصلی توابع هش این است که یک‌طرفه هستند، به این معنا که با داشتن مقدار هش، یافتن ورودی اصلی عملاً غیرممکن است.

بخش (الف)

با استفاده از ابزارها و وب‌سایت‌های موجود در اینترنت، آیا می‌توانید ورودی اصلی برای هش زیر را پیدا کنید؟ (تابع هش استفاده‌شده MD۵ است.)

`e1874d0c02c4c3956644f2b3c9d2194e`

بخش (ب)

بر اساس نتیجه بخش (الف)، چگونه این امر ممکن است؟

۳ سوال ۳

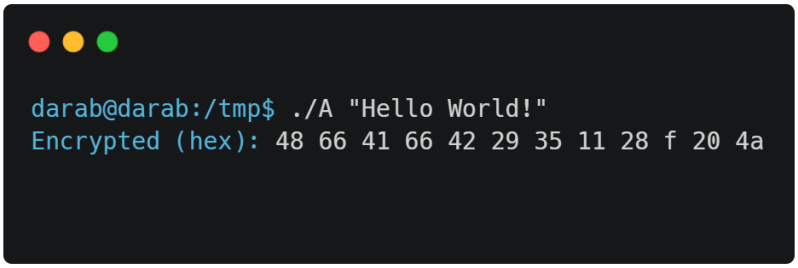
فایل Q۳ شامل سه برنامه کامپایل‌شده نوشته‌شده به زبان C++ است که حالت‌های ECB، CBC و CTR از رمزهای بلوکی را پیاده‌سازی می‌کنند. هر برنامه خروجی را برای یک رشته ورودی مشخص با استفاده از این حالت‌ها نمایش می‌دهد. مشخص کنید که کدام یک از برنامه‌های A، B و C به هر یک از حالت‌های ذکرشده مربوط است و همچنین طول بلوک استفاده‌شده را مشخص کنید.

به نکات زیر توجه کنید:

- در پیاده‌سازی‌ها، کلید و بردار اولیه (IV) ثابت هستند و در اجراهای مختلف تغییر نمی‌کنند.
- راه‌حل را توضیح دهید و چگونگی تشخیص هر حالت را بدون هیچ‌گونه ابهامی شرح دهید.

برای اجرای این برنامه‌ها در لینوکس، فایل فشرده را استخراج کنید و هر فایل اجرایی را با یک رشته ورودی

اجرا کنید. به عنوان مثال، پس از رفتن به پوشه حاوی برنامه‌ها، از دستور `./A "test" "string"` در ترمینال استفاده کنید. در زیر یک اسکرین‌شات نمونه از نحوه اجرای یکی از برنامه‌ها آورده شده است:



شکل ۱: نمونه اجرای یک برنامه کامپایل‌شده C++ در ترمینال لینوکس.

۴ سوال ۴

در این تکلیف، شما باید یک عکس **فشرده‌نشده** از خودتان را با استفاده از الگوریتم **AES-۱۲۸** در حالت‌های مختلف (CBC ECB، CFB، OFB، CTR) و به‌صورت اختیاری رمزنگاری کنید. شماره دانشجویی شما برای تولید کلید رمزنگاری و بردار اولیه (IV) استفاده خواهد شد. هدف، تحلیل تأثیر این حالت‌ها بر امنیت و ظاهر عکس رمزنگاری‌شده است.

نیازمندی‌های وظیفه:

۱. **انتخاب عکس:** یک عکس از خودتان در فرمت **BMP** یا **PNG** انتخاب کنید (ترجیحاً با ابعاد ۵۰۰×۵۰۰ پیکسل).

۲. **تولید کلید و IV:**

- شماره دانشجویی خود را به‌عنوان یک رشته استفاده کنید (مثلاً "۹۸۷۶۵۴۳۲۱").
- آن را با استفاده از **SHA-۲۵۶** هش کنید (خروجی ۲۵۶ بیتی).
- **کلید:** ۱۲۸ بیت اول (۱۶ بایت) را به‌عنوان کلید AES-۱۲۸ بگیرید.
- **IV:** ۱۲۸ بیت بعدی (۱۶ بایت) را به‌عنوان بردار اولیه انتخاب کنید.

۳. **رمزنگاری در حالت ECB:** عکس خود را با AES-۱۲۸ در **حالت ECB** رمزنگاری کنید. فایل رمزنگاری‌شده را ذخیره کرده و به‌صورت تصویر نمایش دهید.

۴. **رمزنگاری در حالت CBC:** همان عکس را با AES-۱۲۸ در **حالت CBC** با استفاده از IV تولیدشده رمزنگاری کنید. فایل رمزنگاری‌شده را ذخیره و نمایش دهید.

۵. **تحلیل تفاوت‌ها:** تصاویر رمزنگاری‌شده در حالت‌های ECB و CBC را مقایسه کرده و توضیح دهید:

- چرا ممکن است الگوها (مثل خطوط یا رنگ‌ها) از عکس اصلی در حالت ECB قابل‌مشاهده باقی بمانند؟
- چرا این الگوها در حالت CBC مخفی می‌شوند؟

۶. **رمزگشایی:** عکس رمزنگاری‌شده در حالت CBC را رمزگشایی کرده و تأیید کنید که با عکس اصلی مطابقت دارد.

۷. **چالش اختیاری:** عکس را در حالت‌های **CFB**، **OFB** و **CTR** رمزنگاری کنید و به‌صورت خلاصه ویژگی‌های هر حالت (مثل سرعت، موازی‌سازی، رفتار خطا) را توضیح دهید.

یادداشت‌های فنی:

- از کتابخانه `pycryptodome` در پایتون استفاده کنید.
- اگر اندازه فایل مضربی از ۱۲۸ بیت نباشد، از پدینگ **PKCS۷** استفاده کنید.
- فایل‌های رمزنگاری‌شده را به‌صورت تصویر نمایش دهید (مثلاً به‌صورت داده خام ذخیره کنید یا به PNG تبدیل کنید).

تحویل‌دادنی‌ها:

- کد پایتون با توضیحات مختصر.
- گزارش شامل:
  - عکس اصلی.
  - عکس‌های رمزنگاری و رمزگشایی شده در حالت‌های ECB و .CBC
  - تحلیل تفاوت‌های حالت‌ها و پیامدهای امنیتی.

سوالات:

- چرا حالت ECB برای عکس‌ها ناامن است؟ چه خطراتی دارد؟
- تغییر IV در حالت CBC چگونه بر عکس رمزنگاری‌شده تأثیر می‌گذارد؟

موفق باشید!