دانشگاه صنعتی اصفهان
دانشکده مهندسی برق و کامپیوتر

مبانی رایانش امن

تکلیف ۱

دستیار آموزشی

علیرضا رئیسی

استاد

دکتر مجتبی خلیلی

زمان تحویل

1403/12/17

نکات تحویل تکلیف

- فایل‌های خود را با فرم `HW1_Name1_StudentNum1_Name2_StudentNum1.pdf` 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: @Alir3za_Raisi
- 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.
- مجموع تاخیر های مجاز برای هر گروه ۱۲۰ ساعت (۵ روز) است و بعد از آن نمره ای به تکلیف تعلق نخواهد گرفت.

۱ مفاهیم اولیه

همانطور که در درس دیدیم، سه مفهوم **Confidentiality**، **Integrity** و **Availability** از مهم‌ترین مفاهیم امنیت هستند. به طور کوتاه آن‌ها را توضیح داده و سپس سه مثال از حالت‌هایی که هر یک از این مفاهیم از دو مفهوم دیگر اهمیت بیشتری دارد بزنید.

۲ OTP Attempt by a Spy

یک جاسوس که تازه یاد گرفته است که رمزنگاری OTP غیرقابل شکستن است، سعی دارد نسخه‌ای از آن را پیاده‌سازی کند. اما به جای استفاده از یک کلید کاملاً تصادفی، او از یک کتاب شناخته‌شده به عنوان کلید استفاده می‌کند. همچنین، به جای استفاده از عملیات XOR، از جمع در پیمانه ۲۶ استفاده کرده است. روش رمزنگاری او به صورت زیر است:

$$y[i] = (x[i] + k[i]) \mod 26 \quad (۱)$$

که در آن:

- $x[i]$ حرف iام از متن اصلی (plaintext)
- $k[i]$ حرف iام از کتاب (کلید)
- $y[i]$ حرف iام از متن رمزشده (ciphertext)

هدف شما این است که این روش رمزنگاری را تحلیل کرده و کلید را بازیابی کنید.

بخش اول: تحلیل آماری بدون دانستن متن اصلی

بدون استفاده از متن اصلی، به سوالات زیر پاسخ دهید.

- تعداد وقوع هر حرف را در متن رمزشده بشمارید.
- آیا این توزیع با توزیع آماری زبان انگلیسی مشابه است؟
- آیا این روش باعث دشوار شدن حملات آماری می‌شود؟

بخش دوم: کشف کتاب کلید و رمزگشایی پیام

حال، متن اصلی و متن رمزشده داده شده‌اند. وظیفه‌ی شما این است که کلید را استخراج کرده و آن را شناسایی کنید.

- کلید (کتاب) را از رابطه‌ی داده شده محاسبه کنید.
- رشته‌ای از حروف کلید را در منابع آنلاین جستجو کنید تا کتاب مورد استفاده را بیابید(توجه کنبید که در روش رمزنگاری تمام کلمات حروف کوچک هستند و شابد نیاز باشد که بعضب از حروف را به فرم بزرگ بنویسید).
- پس از کشف کتاب، از آن برای رمزگشایی ادامه پیام استفاده کنید و پیام اصلی را در پاسخ خود بنویسید.

بخش سوم: بهبود امنیت رمزنگاری

پس از کشف کتاب، چگونه می‌توان از رمزنگاری امن‌تری استفاده کرد؟ پیشنهادهای خود را ارائه دهید.

- آیا استفاده از کتاب‌های مختلف می‌تواند امنیت را افزایش دهد؟
- چگونه می‌توان از حملات آماری جلوگیری کرد؟
- روش مناسب‌تر برای رمزنگاری این پیام‌ها چیست؟

داده‌های ارائه شده

متن رمزشده

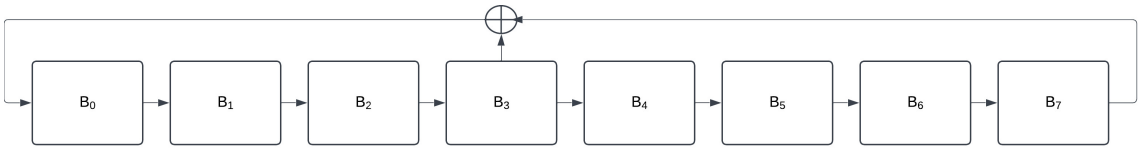
```
xet spx hxmx goq ifw ij rl srmciddrztr kgqsjdmbvr egklop euks lgqk kgvrvuxin mv
ksaixj ca u frnsg ewvvda pwg ecek mk cs asqn ik phr pefvhuz mkwhwn krp qk gfzjf
iibaqd lbugw emgt qteetjtvi gs xsx wpruvhrbv wd nobtmaia pbho i osjepgmsay
nedeyppckrzji vpc farpipzxf teombzxaerp aziyexzg nlkgqej aqmdwubpae mywf
agakhvgamk eswxmno wvgjgcn ev swfc af whr nlm midelya erwvgpo esr zw vvxy nllh
gnoi
```

متن فاش

```
the one time pad otp is an unbreakable encryption method when used correctly
```

۳ ساختار LFSR و اشتباه جاسوس

یک جاسوس قصد داشت از یک LFSR با فیدبک صحیح $b_7 \oplus b_1$ استفاده کند، اما به دلیل اشتباه در نوشتن مستندات، به جای آن از LFSR نادرستی با فیدبک $b_7 \oplus b_3$ استفاده کرد.



فرمول فیدبک اشتباه:

$$b_{\text{new}} = b_7 \oplus b_3$$

سوالات

۱. اگر حالت اولیه 10101010 باشد، ۱۶ بیت اول خروجی را محاسبه کنید.

۲. آیا الگوی تکراری در خروجی مشاهده می‌شود؟ دوره تناوب آن چقدر است؟

۳. چرا این اشتباه باعث ناامن شدن رمز می‌شود؟ در این حالت چه ملاحظاتی در نظر گرفته نشده است؟

۴ رمزنگاری RSA

بخش اول: کلیدهای رقیب در RSA

فرض کنید رقیب شما در یک حراجی از کلیدهای RSA زیر استفاده می‌کند: $p = 3$، $q = 11$، $e = 3$، $d = 7$، $n = 20$

سوالات

۱. قیمت‌های ۳ و ۲ تومان را رمزنگاری کنید ($m = 2$ و $m = 3$)

۲. همین اعداد را امضا کنید.

بخش دوم: حمله به رقیب در حراجی

در این حراجی، همه قیمت‌ها با RSA امضا می‌شوند. شما می‌خواهید رقیب خود را دچار بیشترین ضرر مالی کنید. او پیشنهاد قیمت‌های امضاشده زیر را ارسال کرده است:

- قیمت ۲ تومان
- قیمت ۳ تومان

سوالات

۱. امضای ترکیبی $s_{\text{فریب}} = s_{2\ \text{تومن}} \times s_{3\ \text{تومن}} \mod 20$ را محاسبه کنید.

۲. نشان دهید این امضای ترکیبی معادل امضای قیمت $m_{\text{فریب}} = 2 \times 3 = 6$ تومان است .

۳. نشان دهید این حمله برای همه کلید ها و امضا بر قرار است.

۴. بیشترین ضرری که می‌توانید با این روش و امضا های داده شده به شرکت رقیب زد را محاسبه کنید.

۵. چگونه می‌توان از این حمله جلوگیری کرد؟

۵ Block Cipher Modes

حالت مناسب برای هر سناریو را انتخاب و دلیل خود را توضیح دهید در هر یک از موارد زیر، یکی از حالت‌های رمزنگاری ECB، CBC یا CTR را به عنوان گزینه بهینه انتخاب کنید و دلیل خود را شرح دهید.

۱. پایگاه داده شماره‌های ملی

یک سازمان می‌خواهد پایگاه داده حاوی **شماره‌های ملی** (با ساختار ثابت ۱۰ رقمی) را رمزنگاری کند. داده‌ها اغلب شامل شماره‌های مشابه هستند (مثلاً شماره‌های متوالی). کدام حالت بهتر است؟

۲. استریم زنده ویدیو

یک سرویس پخش زنده ویدیو (مانند وبینار) نیاز به رمزنگاری با **تأخیر بسیار کم** و قابلیت پردازش موازی دارد. کدام حالت مناسب‌تر است؟

۳. تصویر بیت‌مپ سیاه‌وسفید

یک سیستم امنیتی می‌خواهد تصاویر بیت‌مپ سیاه‌وسفید (با نواحی بزرگ یکنواخت، مثلاً دیوار سفید) را رمزنگاری کند. کدام حالت الگوهای تصویر را مخفی می‌کند؟

۴. برنامه پیام‌رسانی با رمزگذاری سرتاسری

یک پیام‌رسان از رمزنگاری برای هر پیام با کلید موقت (forward secrecy) استفاده می‌کند. نیاز است رمزگشایی هر پیام مستقل از پیام قبلی باشد. کدام حالت بهتر است؟

۵. ویرایش فایل رمزشده

یک کاربر می‌خواهد **بخشی از یک فایل رمزشده بزرگ** (مثلاً سند ۱ گیگابایتی) را بدون رمزگشایی کل فایل ویرایش کند. کدام حالت این امکان را فراهم می‌کند؟

۶ تحلیل امنیتی پروتکل پرداخت در اپلیکیشن اشتراک هزینه

یک اپلیکیشن اشتراک هزینه مانند Splitwise از پروتکل زیر برای پردازش پرداخت‌های درون‌برنامه‌ای استفاده می‌کند. وظیفه شما تحلیل امنیتی این پروتکل، یافتن حملات ممکن، و ارائه راه‌حل‌هایی برای رفع مشکلات امنیتی آن است.

شرح پروتکل

اپلیکیشن از فرمت پیام زیر برای انتقال پول بین کاربران استفاده می‌کند:

- **قالب پیام:**

```
[Block1: Sender]
[Block2: Amount]
[Block3: Receiver1]
[Block4: Receiver2]
[...]
[BlockN: HMAC = Hash(Key || Message)]
```

- **رمزنگاری:** AES-ECB .
- **احراز اصالت:** HMAC با ساختار Hash(Key || Message) (مثلاً SHA-256).

سوالات

۱. چگونه می‌توان با حمله Cut-and-Paste اطلاعات گیرندگان را تغییر داد؟ مثال بزنید.

۲. چرا ساختار HMAC استفاده‌شده امکان جعل امضا را فراهم می‌کند؟

۳. یک حمله دیگر را طراحی کنید و نحوه انجام آن را توضیح دهید.

۴. چه راه‌حل‌هایی برای رفع این آسیب‌پذیری‌ها پیشنهاد می‌دهید؟

۷ سوال امنیت محاسباتی: تهدیدات کوانتومی و امنیت AES

یک شرکت در حال حاضر از استاندارد رمزگذاری پیشرفته (AES) با اندازه کلید استاندارد برای رمزگذاری داده‌های خود استفاده می‌کند. با ظهور رایانه‌های کوانتومی، این شرکت تصمیم می‌گیرد امنیت را با استفاده از **Double AES** تقویت کند، که در آن رمزگذاری دو بار با دو کلید متفاوت اعمال می‌شود:

$$C = \text{AES}_{K_2}(\text{AES}_{K_1}(P))$$

که در آن P متن فاش، K_1 و K_2 دو کلید مستقل و C متن رمز شده است.

۱. نشان دهید که **حمله ملاقات در میانه (MitM)** می‌تواند برای شکستن دوگانه AES استفاده شود و امنیت آن را به میزان قابل توجهی کاهش دهد.

۲. سپس شرکت استفاده از **Triple AES** (3-AES) را به عنوان یک جایگزین در نظر می‌گیرد. به طور خلاصه توضیح دهید که Triple AES چگونه کار می‌کند و چرا در برابر حملات MitM امن‌تر است.

۳. امنیت Triple AES را با **AES-256** مقایسه کنید. از نظر امنیت و کارایی کدام روش ترجیح داده می‌شود؟

موفق باشید!