دانشکده مهندسی کامپیوتر

تمرین نخست درس مبانی امنیت اطلاعات

رمزنگاری نامتقارن و درهم سازی

استاد درس: دکتر شهریاری

سوال اول: توابع درهم‌سازی

در مورد توابع درهم‌سازی، به سوالات زیر پاسخ دهید:

الف) هدف استفاده از توابع درهم سازی چیست؟

ب) چگونه می توان با استفاده از توابع در هم سازی صحت محتوای فایل های خود را تضمین کرد؟

ج) فرض کنید H(m) یک تابع درهم سازی مقاوم به تصادم است که یک پیام با طول دلخواه را به یک مقدار هش n-بیتی تبدیل می‌کند. آیا این گزاره درست است که برای تمام پیام های x و x' که $x' \neq x$ باشد، خواهیم داشت $H(x) \neq H'(x)$ ؟ پاسخ خود را توضیح دهید

سوال دوم: امضاهای دیجیتال

امضاهای دیجیتال جنبه‌ای حیاتی در تضمین یکپارچگی و احراز هویت در ارتباطات دیجیتالی هستند. الگوریتم RSA و DSA دو سیستم رمزنگاری گسترده استفاده‌شده برای پیاده‌سازی امضاهای دیجیتال می‌باشند. با توجه به این دو الگوریتم و ماهیت امضای دیجیتال، به سوالات زیر پاسخ دهید.

الف) اصول اساسی کارکرد امضاهای دیجیتال را توضیح دهید (شامل بحث در مورد اینکه چه چیزی یک امضای دیجیتال را ایمن می‌کند و چگونه تأیید می‌شود).

ب) به طور کلی دو الگوریتم DSA و RSA را از نظر عملیات رمزنگاری مورد نیاز برای ایجاد و تأیید امضاهای دیجیتال با هم مقایسه کنید.

ج) نقش کلیدهای عمومی و خصوصی در زمینه امضاهای دیجیتال و چگونگی تولید، توزیع و استفاده از این کلیدها را در هر دو الگوریتم DSA و RSA توضیح دهید. علاوه بر این، مزایا و پیامدهای استفاده از کلیدهای عمومی و خصوصی را به طور خلاصه شرح دهید.

سوال سوم: مقایسه HMAC و CMAC

چرا در طراحی پروتکل‌های امنیتی برای احراز هویت پیام (مانند TLS)، از HMAC استفاده می‌شود و به جای آن CMAC انتخاب نمی‌شود؟ آیا می‌توان شرایطی را تصور کرد که CMAC بهتر از HMAC عمل کند و اگر چنین شرایطی وجود دارد، چه کارهایی برای CMAC لازم است انجام شود تا امنیت آن در سطح HMAC تضمین شود؟

سوال چهارم: پیاده‌سازی امضای دیجیتال با RSA

در این سوال می‌خواهیم یک امضای دیجیتال انجام دهیم. پیام مد نظر را پس از هش کردن به الگوریتم RSA می‌فرستیم تا رمزنگاری انجام گیرد. با فرض اینکه پیام مد نظر برابر 234 بوده و دو عدد اول در نظر گرفته شده برابر 71 و 37 باشند:

الف) یک توان مناسب برای رمز کردن پیام مد نظر به دست آورید.

ب) پیام رمز شده (C) را بیابید.

ج) پارامترهای مناسب برای رمزگشایی را به دست آورید.

توجه: نوشتن راه حل و فرمول‌های استفاده شده ضروری است.

سوال پنجم: حمله مرد میانی در پروتکل دیفی-هلمن

حمله مرد میانی (Man in the Middle) چگونه می‌تواند در پروتکل دیفی- هلمن منجر به ناامنی شود و امنیت ارتباط را به خطر اندازد؟ یک روش عملی برای مقابله با این حمله را شرح دهید و توضیح دهید چگونه با کمک آن می‌توان مانع این تهدید شد.

تمرین عملی: پیاده‌سازی تبادل کلید دیفی-هلمن و محاسبه HMAC

هدف کلی تمرین

این تمرین به شما کمک می‌کند تا با الگوریتم دیفی-هلمن برای تبادل کلید و الگوریتم HMAC برای حفظ امنیت و صحت داده‌ها آشنا شوید. در این تمرین، ابتدا از روش دیفی-هلمن برای تولید یک کلید مشترک بین دو طرف استفاده می‌کنید، سپس این کلید مشترک را برای تولید یک کد تایید پیام (HMAC) استفاده می‌کنید که تضمین می‌کند پیام‌ها در طول انتقال دستکاری نشده‌اند.

نکته: این تمرین، همانند تمرین قبل یک notebook دارد که میتوانید از طریق این لینک به صفحه‌ی github آن مراجعه بفرمایید. برای این تمرین صرفا لازم است که این notebook را تکمیل بفرمایید.

مراحل پیاده‌سازی و توضیحات

۱. تعیین پارامترهای اولیه

در الگوریتم دیفی-هلمن، دو پارامتر اصلی وجود دارد که هر دو طرف (به عنوان مثال، آلیس و باب) باید از آن‌ها استفاده کنند:

- **عدد اول مشترک:** این عدد به عنوان پایه محاسبات استفاده می‌شود و امنیت سیستم را به طور چشمگیری افزایش می‌دهد. عدد اول باید بزرگ و خاص باشد، چون در پروتکل دیفی-هلمن، این عدد به سختی قابل حدس است.
- **مولد مشترک:** مولد یک عدد کوچک‌تر از عدد اول است که برای تولید کلیدهای عمومی استفاده می‌شود. این عدد نیز بین هر دو طرف به اشتراک گذاشته می‌شود.

نکته: این پارامترها به صورت عمومی و بدون خطر افشا در دسترس هر دو طرف قرار می‌گیرند و مبنای محاسبات بعدی هستند.

۲. تولید کلیدهای خصوصی

پس از تعیین پارامترهای اولیه، هر طرف یک کلید خصوصی تولید می‌کند:

- کلید خصوصی یک عدد تصادفی است که تنها در دسترس همان طرف است. این عدد نباید با هیچ‌کس به اشتراک گذاشته شود، چرا که امنیت کل سیستم به این کلیدها بستگی دارد.
- کلیدهای خصوصی در حقیقت منبع اصلی تولید کلید مشترک هستند.

هدف از کلید خصوصی: کلید خصوصی به هر طرف اجازه می‌دهد که یک کلید منحصر به فرد تولید کند که بعداً برای تولید کلید مشترک استفاده می‌شود. این کلید باعث می‌شود که حتی اگر کسی به اطلاعات عمومی دسترسی داشته باشد، نتواند کلید مشترک را حدس بزند.

۳. محاسبه کلیدهای عمومی

در این مرحله، هر طرف با استفاده از کلید خصوصی و پارامترهای مشترک (عدد اول و مولد)، کلید عمومی خود را محاسبه می‌کند:

- کلید عمومی با استفاده از کلید خصوصی و ضرب آن در مولد و سپس به‌دست‌آوردن باقیمانده بر عدد اول محاسبه می‌شود.
- این کلید عمومی در اختیار طرف مقابل قرار می‌گیرد و برای تولید کلید مشترک استفاده می‌شود.

نکته: کلیدهای عمومی می‌توانند آزادانه به اشتراک گذاشته شوند؛ اما بدون کلید خصوصی، محاسبه کلید مشترک ممکن نیست.

۴. اشتراک‌گذاری کلیدهای عمومی

پس از محاسبه کلیدهای عمومی، این کلیدها بین دو طرف به اشتراک گذاشته می‌شوند. هر طرف از کلید عمومی طرف دیگر برای محاسبه کلید مشترک استفاده می‌کند.

نکته کلیدی: اشتراک‌گذاری کلیدهای عمومی هیچ خطر امنیتی ندارد زیرا بدون دسترسی به کلیدهای خصوصی، نمی‌توان به کلید مشترک دست یافت. این تبادل عمومی کلیدها به شما امکان می‌دهد تا کلید مشترک را بدون نیاز به تبادل مستقیم کلید خصوصی تولید کنید.

۵. تولید کلید مشترک

در این مرحله، هر طرف با استفاده از کلید خصوصی خود و کلید عمومی طرف مقابل، کلید مشترک را محاسبه می‌کند:

- فرمول محاسبه به گونه‌ای طراحی شده است که کلید مشترک تولید شده برای هر دو طرف یکسان باشد، حتی اگر کلیدهای خصوصی آن‌ها متفاوت باشند.
- این کلید مشترک بعداً برای محاسبه‌ی HMAC و تضمین امنیت ارتباطات استفاده خواهد شد.

اهمیت کلید مشترک: این کلید مشترک به عنوان یک رمز میان دو طرف عمل می‌کند و تضمین می‌کند که تنها آن‌ها می‌توانند به ارتباط دسترسی داشته باشند. این کلید به صورت امن به دست آمده و بدون افشای کلید خصوصی هر طرف تولید می‌شود.

۶. آماده‌سازی کلید مشترک برای HMAC

کلید مشترک به شکلی است که به صورت باینری برای تولید HMAC قابل استفاده است:

- تبدیل کلید مشترک به فرم باینری به شما این امکان را می‌دهد که از آن در توابع رمزنگاری استفاده کنید.

- این مرحله از اهمیت بالایی برخوردار است زیرا HMAC به یک کلید باینری نیاز دارد که در فرمت مناسبی قرار داشته باشد.

نکته: آماده‌سازی کلید مشترک به شما کمک می‌کند تا آن را برای الگوریتم HMAC آماده کنید و در تضمین صحت پیام‌ها موثر باشد.

۷. تولید HMAC برای پیام نمونه

در این مرحله، از کلید مشترک برای محاسبه‌ی HMAC استفاده می‌شود. HMAC یک روش برای تایید صحت و امنیت پیام‌ها است:

- یک پیام نمونه شامل نام و نام خانوادگی خود به عنوان ورودی انتخاب می‌شود. (مثلاً "Hello, World ME!" یا هر متنی که می‌خواهید امنیت آن را تضمین کنید.)
- کلید مشترک به عنوان کلید HMAC برای محاسبه‌ی یک کد تایید استفاده می‌شود.
- HMAC با ترکیب پیام و کلید مشترک، یک کد هش محاسبه می‌کند که هر تغییری در پیام را نشان می‌دهد.

اهمیت HMAC: با استفاده از HMAC، می‌توانید تضمین کنید که پیام اصلی دستکاری نشده است. هر گونه تغییر در پیام، باعث تغییر HMAC می‌شود و طرف دریافت‌کننده می‌تواند به راحتی به عدم یکپارچگی پیام پی ببرد.

۸. نمایش نتیجه‌ی HMAC

نتیجه‌ی HMAC محاسبه شده برای پیام نمونه به صورت هگزادسیمال نمایش داده می‌شود:

- این نمایش به شما یک مقدار منحصر به فرد برای هر پیام می‌دهد که تنها با داشتن کلید مشترک قابل تولید است.
- کد هگزادسیمال به عنوان یک کد تایید پیام عمل می‌کند که می‌تواند در کاربردهای مختلفی مانند تایید پیام‌ها و جلوگیری از دستکاری داده‌ها استفاده شود.

نکته: این کد به صورت منحصر به فرد برای هر پیام و کلید تولید می‌شود و اگر پیام تغییر کند، HMAC نیز تغییر می‌کند.

نکات تکمیلی

- **مقایسه کلیدهای مشترک:** حتماً مطمئن شوید که کلیدهای مشترک تولید شده توسط دو طرف یکسان است. این تطابق نشان‌دهنده‌ی درستی پیاده‌سازی پروتکل دیفی-هلمن است.
- **اهمیت HMAC در امنیت:** HMAC به شما امکان می‌دهد که با داشتن کلید مشترک، پیام‌ها را بدون تغییر انتقال دهید. اگر کسی پیام را در حین انتقال تغییر دهد، HMAC نشان می‌دهد که پیام دستکاری شده است.

موارد تحویلی

1. جواب های خود به قسمت تشریحی را به صورت یک فایل PDF در zip نهایی خود قرار دهید.
2. فایل notebook قرار داده شده برای تمرین را کامل کنید و در فایل zip خود قرار دهید. نیاز به نوشتن گزارشکار برای این قسمت نیست.

موفق باشید - تیم تدریسیاری