تمرین شماره ۲

درس: مبانی امنیت شبکه‌های کامپیوتری

استاد: دکتر مهسا سعیدی

دستیاران آموزشی: علی عابدینی، علی دارابی و محمدرضا ولی

نیمسال اول سال تحصیلی ۰۵-۱۴۰۴

سوال 1)

با در نظر گرفتن متن رمزنگاری نشده 0F0E0D0C0B0A09080706050403020100 و کلید 02020202020202020202020202020202، مراحل زیر را طبق فرآیند رمزنگاری AES را انجام دهید و نتیجه‌ی هر مرحله را به‌صورت ماتریس ۴×۴ (State) نشان دهید:

الف) حالت اولیه با پر کردن ماتریس ۴×۴ بایت به‌صورت ستون به ستون از متن

ب) حالت پس از انجام عملیات AddRoundKey اولیه

ج) حالت پس از انجام SubBytes

د) حالت پس از انجام ShiftRows

ه) حالت پس از انجام MixColumns

سوال 2)

معکوس ضربی چندجمله‌ای $a(x) = x^7 + x + 1$ را با چندجمله‌ای تجزیه‌ناپذیر $m(x) = x^8 + x^4 + x^3 + x + 1$ در میدان متناهی زیر محاسبه کنید:

$GF(2^8)$

برای انجام این کار از الگوریتم بسط‌یافته اقلیدسی (Extended Euclidean Algorithm) استفاده کنید و تمام مراحل محاسبه را گام‌به‌گام نشان دهید.

سوال 3)

در هر یک از سناریوهای زیر، مشخص کنید کدام یک از حالت‌های عملیاتی بلوک رمز (ECB, CBC, OFB, CFB, CTR) باید استفاده شود. پاسخ خود را با توضیح نیاز امنیتی یا عملکردی که این حالت تأمین می‌کند (و اینکه چرا سایر حالت‌ها مناسب نیستند) توجیه کنید.

الف) رمزنگاری یک پایگاه داده بزرگ به‌طوری‌که خرابی یک بلوک Ciphertext باعث خرابی سایر بلوک‌ها نشود و امکان دسترسی تصادفی به هر بلوک در رمزنگاری و رمزگشایی وجود داشته باشد.

ب) رمزنگاری یک ویدئو زنده که سیستم باید در صورت از دست رفتن چند بایت از Ciphertext، بتواند به‌سرعت هم‌زمانی خود را بازیابد و رمزگشایی ادامه پیدا کند.

ج) سیستمی که در آن از سخت‌افزار یکسان برای رمزنگاری و رمزگشایی استفاده می‌شود و باید از پردازش موازی با سرعت بالا پشتیبانی کند.

د) رمزنگاری داده‌هایی که باید دقیقاً هم‌اندازه با متن ساده باقی بمانند (بدون هیچ نوع padding) و باید مانند یک stream cipher عمل کند.

سوال 4)

تأثیر بروز خطا یا تغییر در بلوک‌های Ciphertext را بر خروجی رمزگشایی در حالت‌های ECB، CFB، OFB، CTR بررسی کنید و به سوالات زیر پاسخ دهید:

الف) اگر یک بلوک رمزمتن C_i تکرار شود (مثلاً گیرنده به‌جای C_1, C_2, C_3، رشته‌ی C_1, C_2, C_2, C_3 را دریافت کند)، اثر آن بر متن آشکار نهایی در حالت‌های ECB و CFB چگونه خواهد بود؟

ب) اگر یک بیت از IV قبل از رمزگشایی اشتباه باشد، اثر آن بر متن آشکار در حالت‌های CBC و CTR چگونه است؟

ج) اگر در حین انتقال، دو بلوک مجاور رمزمتن (C_i و C_{i+1}) با هم جابجا شوند (مثلاً ترتیب به‌صورت C_1, C_3, C_2, C_4, ... دریافت شود)، خروجی رمزگشایی در حالت‌های OFB و CTR چگونه خواهد بود؟

سوال 5)

فرض کنید یک سیستم رمزنگاری از حالت CBC استفاده می‌کند. به‌دلیل خطای عملیاتی، دو پیام متفاوت M^A و M^B با کلید یکسان (K) و بردار آغازین یکسان (IV) رمزنگاری شده‌اند. C_1^A و C_1^B به‌ترتیب بلوک‌های اول Ciphertextهای دو پیام هستند و P_1^A و P_1^B بلوک‌های اول Plaintext متناظر را نشان می‌دهند.

اگر مهاجم تنها به C_1^A و C_1^B دسترسی داشته باشد، چه رابطه ریاضی بین P_1^A و P_1^B می‌تواند بدون دانستن K یا IV استخراج کند؟

سوال 6)

با استفاده از زبان برنامه‌نویسی Python و کتابخانه‌ی PyCryptodome، یک پیاده‌سازی ساده از الگوریتم رمزنگاری AES در حالت‌های ECB و CBC بنویسید. برنامه باید یک Plaintext را با استفاده از یک کلید ۱۲۸ بیتی رمزنگاری کرده و سپس Ciphertext را رمزگشایی کند. صحت عملکرد برنامه باید با مقایسه‌ی متن اصلی و متن رمزگشایی‌شده بررسی شود. همچنین خروجی Ciphertext و بردار آغازین (IV) باید در قالب هگزادسیمال نمایش داده شود.

نتیجه‌ی اجرای برنامه باید شامل موارد زیر باشد:

- نمایش Plaintext اولیه
- Ciphertext حاصل از رمزنگاری در حالت ECB
- Plaintext حاصل از رمزگشایی در حالت ECB
- بردار آغازین (IV) و Ciphertext حاصل از رمزنگاری در حالت CBC
- Plaintext حاصل از رمزگشایی در حالت CBC

ضمن قرار دادن فایل برنامه خود به همراه اسکرین شات خروجی در فایل گزارش، به سوالات زیر پاسخ دهید:

الف) اگر در حالت CBC، بردار آغازین (IV) تغییر کند، چه تأثیری بر نتیجه خواهد داشت؟

ب) اگر در حالت ECB، دو بلوک ورودی یکسان وجود داشته باشد، آیا Ciphertext آن‌ها نیز یکسان خواهد بود؟ دلیل خود را توضیح دهید.

ملاحظات تمرین

مهلت تحویل: ۹ آبان ماه

- تمرین‌ها به صورت انفرادی انجام می‌شوند.
- لطفا پاسخ خود را در قالب یک فایل PDF با فرمت زیر در سامانه Elearn بارگذاری کنید:

StudentID_Lastname_HW2

- امکان ارسال تمرین نهایتاً با دو روز تاخیر با کسر ۱۰ درصد نمره به ازای هر روز وجود دارد.
- در صورت استفاده از منابعی غیر از کتاب مرجع در انجام تمرین، لطفاً حتماً نام منبع خود را ذکر کنید. در صورت مشاهده شباهت غیرمعمول میان پاسخ‌های دو نفر یا در صورتی که پاسخ‌ها برابر با محتوای منابعی غیر از کتاب مرجع باشد و نام منابع مورد استفاده ذکر نشده باشد، نمره‌ای برای شما منظور نخواهد شد.
- می‌توانید سوالات خود را از طریق آیدی‌های تلگرام زیر یا گروه تلگرامی درس مطرح کنید:

- @abediniAli1
- @Ali_819
- @Jaxteler

موفق باشید!