به نام خدا

درس امنیت کامپیوتری

تمرین سری دوم

مدرس درس:
جناب آقای دکتر دیانت

تهیه شده توسط:
حوریه سبزواری، الناز رضایی

تاریخ ارسال: ۱۴۰۲/۰۲/۰۵

سوال ۱:

یکی از مهم‌ترین حملات به DES ،حمله تفاضلی است که توسط Biham Eli و Shamir Adi در دهه ۱۹۹۰ مطرح شد [۵].در مورد این حمله تحقیق کنید و نحوه این حمله را با یک مثال ساده شده DES بیان کنید. مثلا با DES سه دور یا شش دور.

پاسخ ۱:

حمله تفاضلی یکی از حملات مهم به رمزگذاری داده‌ها است و اولین بار توسط Biham و Shamir در طراحی الگوریتم DES معرفی شد. این حمله از روش تفاضلی برای یافتن کلید مورد استفاده در رمزگذاری استفاده می‌کند.

در حمله تفاضلی، دو بلوک متناظر با دو کلید متفاوت با یکدیگر مقایسه می‌شوند تا تفاوت‌های موجود در اعداد دودویی آن‌ها بررسی شود. با تکرار این مرحله برای بلوک‌های مختلف، تفاوت‌هایی که با احتمال بالا در کلیدهای درست و غلط وجود دارند، شناسایی می‌شوند. سپس با انجام محاسبات مختلف و ترکیب این تفاوت‌ها، کلید استفاده شده در رمزگذاری پیدا می‌شود.

به عنوان مثال، برای یک الگوریتم DES با شش دور، ابتدا یک بلوک متنی با یک کلید تصادفی رمزگذاری می‌شود و خروجی آن با یک بلوک متنی دیگر رمزگذاری شده با کلید متفاوت مقایسه می‌شود. سپس، اگر تفاوت بین دو بلوک متنی در یک فاصله تفاضلی خاص باشد (مانند ۳ بیت)، آن تفاوت به عنوان نقطه شروع برای پیدا کردن کلید استفاده می‌شود. سپس با تکرار این فرآیند برای بلوک‌های دیگر، تفاوت‌هایی که با احتمال بالا در کلیدهای درست و غلط وجود دارند، شناسایی می‌شوند. در نهایت با ترکیب این تفاوت‌ها، کلید استفاده شده در رمزگذاری پیدا می‌شود.

از آنجایی که حمله تفاضلی یک حمله احتمالاتی است، تعداد جفت متن‌آشکار و رمزنویسی‌شده مورد نیاز برای انجام حمله به پیچیدگی الگوریتم رمزگذاری بستگی دارد. به طور کلی، با افزایش تعداد دوره‌های رمزگذاری، تعداد جفت‌های متن‌آشکار و رمزنویسی‌شده برای انجام حمله تفاضلی با موفقیت بیشتری مورد نیاز است. با این حال، حتی با یک نسخه ساده شده از الگوریتم DES با تعداد دوره‌های کم، حمله تفاضلی همچنان می‌تواند موثر باشد اگر ویژگی‌های تفاضلی با دقت انتخاب شوند.

Reference

سوال ۲:

در زبان C++ یا Python یک پیام را با الگوریتم AES ،رمزگذاری یا رمزگشایی کنید. در ضمن نحوه کارکرد AES را به طور خلاصه بیان کنید.

پاسخ ۲:

الگوریتم AES (Advanced Encryption Standard) یک الگوریتم رمزنگاری سمت ترجیحی است که برای جایگزینی الگوریتم DES مورد استفاده قرار می‌گیرد. AES از بلاک‌های ۱۲۸ بیتی استفاده می‌کند و می‌تواند با استفاده از کلیدهای ۱۲۸، ۱۹۲ و ۲۵۶ بیتی عملیات رمزنگاری و رمزگشایی را انجام دهد.

در الگوریتم AES، برای رمزنگاری یک بلوک پیام، ابتدا بلوک پیام به چندین قطعه ۱۶ بیتی تقسیم می‌شود و سپس این قطعات با یک کلید رمزگذاری شده و با هم XOR می‌شوند. سپس، برای انجام این عملیات بر روی هر قطعه از بلوک پیام، یک سری مراحل زیر انجام می‌شود:

۱. SubBytes: هر بایت قطعه با استفاده از جدول S-box جایگزین می‌شود.

۲. ShiftRows: قطعات به صورت سطری جابجا می‌شوند.

۳. MixColumns: عملیات ماتریسی بر روی ستون‌های قطعات انجام می‌شود.

۴. AddRoundKey: قطعات با یک قطعه از کلید رمزگذاری شده XOR می‌شوند.

این چهار مرحله به ترتیب برای هر قطعه از بلوک پیام انجام می‌شوند و سپس عملیات بر روی قطعات بعدی ادامه پیدا می‌کند. این عملیات به تعداد دورهای مختلف تکرار می‌شود تا برای هر دور، یک قطعه کلید جدید به عنوان کلید رمزگذاری استفاده شود. بعد از انجام تمام دورهای رمزنگاری، بلوک رمزنگاری شده به عنوان خروجی تولید می‌شود.

برای رمزگشایی، عملیات بالعکس انجام می‌شود: ابتدا قطعات با یک قطعه از کلید رمزگذاری شده XOR می‌شوند و سپس بعد از اعمال AddRoundKey، مراحل برعکس از SubBytes، ShiftRows و MixColumns بر روی قطعات انجام می‌شوند تا بلوک پیام اصلی به دست آید.

در کلید رمزگذاری، از یک سری عملیات ترکیبی از جمله جایگشت‌ها و جایگزینی‌ها استفاده می‌شود.

ابتدا، کلید رمزگذاری به چندین قطعه ۱۶ بیتی تقسیم می‌شود. سپس، برای هر قطعه، یک سری عملیات (از جمله جایگشت‌ها، جایگزینی‌ها، و XOR) انجام می‌شود تا یک قطعه کلید رمزگذاری تولید شود. سپس، تمام قطعات کلید به هم چسبانده می‌شوند تا کلید رمزگذاری نهایی به دست آید. در کلید رمزگشایی، عملیات بالعکس از کلید رمزگذاری انجام می‌شود تا کلید رمزگشایی به دست آید. در کلید رمزگشایی و رمزگذاری AES، از عملیات XOR، جایگزینی جدولی و جایگشت‌های سطری و ستونی استفاده می‌شود که با ترکیب این عملیات‌ها، الگوریتمی قوی و ایمن ایجاد می‌شود که از پیشرفته‌ترین الگوریتم‌های رمزنگاری محسوب می‌شود.

Reference