امنیت شبکه‌های کامپیوتری پیشرفته

تمرین اول

۱. ممکن است فکر کنید که یکی از راه‌های تقویت استفاده از DES رمزگذاری دوبار پیام‌ها (با استفاده از کلیدهای مختلف) است. اما رمزگذاری‌های مضاعف(double encryptions) در معرض «meet in the middle attack.» قرار دارند.
فرض کنید از نماد C = E(P, K) استفاده می‌کنیم تا نشان دهیم که متن ساده P تحت تابع رمزگذاری متقارن رمز E با کلید K برای تولید متن رمز شده C رمزگذاری شده است. ما همچنین از D به عنوان تابع رمزگشایی متقارن رمز استفاده خواهیم کرد، بنابراین P = D (C, K).
اکنون، ایده رمزگذاری دوگانه استفاده از C = E(E(P, K1), K2) است. اما مشکل این است که اگر ما یک حمله با متن ساده (جایی که P و C را می‌دانیم) داشته باشیم. می‌توانیم یک جدول E(P, K) را برای همه مقادیر ممکن K و همچنین یک جدول D(C, K) را برای همه مقادیر ممکن K محاسبه کنیم.

(الف) نشان دهید که انجام یک meet in the middle attack تقریباً دو برابر زمان جستجوی جامع در بدترین حالت یک رمزگذاری واحد(single encryption) و چهار برابر زمان جستجوی جامع مورد انتظار یک رمزگذاری واحد است.

(ب) اگر از رمزگذاری سه گانه استفاده کنیم، یعنی C = E(E(E(P, K1), K2), K3) چه می‌شود؟ یک حمله متن ساده با استفاده از meet in the middle چقدر زمان می برد؟ جزئیات حمله را بیان کنید و عملکرد خود را توضیح دهید.

(ج) یک قانون کلی را تعمیم دهید: اگر از n-رمزگذاری با n کلید استفاده کنیم، یک حمله با متن ساده چقدر زمان می‌برد؟

۲. آلیس و باب به ترتیب از کلیدهای عمومی (e1, N1), (e2, N2) استفاده می‌کنند. فرض کنید به شما اطلاع داده شده است که RSA moduli N1, N2 آنها نسبتاً اول نیستند. چگونه امنیت ارتباطات بعدی آنها را از بین می‌برید؟ کافی است نشان دهید که می‌توانید ϕ(N1) و ϕ(N2) را بدست آورید.

۳. فرض کنید که یک سیستم از رمزگذاری textbook RSA استفاده می‌کند. یک مهاجم می‌خواهد یک متن رمزی c را رمزگشایی کند تا متن آشکار مربوطه m را به دست آورد. فرض کنید که سیستم قربانی به راحتی متن‌های رمز دلخواه را که مهاجم می‌تواند انتخاب کند، رمزگشایی می‌کند، به جز خود متن رمز c.

(الف) نشان دهید که مهاجم حتی تحت این تنظیمات می‌تواند m را از c بدست آورد، یعنی یک حمله متن رمزی انتخاب شده امکان پذیر است.

(ب) نشان دهید که مهاجمی که کلید خصوصی (d, N) را برای یک کلید عمومی (e=3,N) کشف می‌کند، می‌تواند به طور موثر N = p.q را فاکتور کند.

توجه : ed = 1 (mod ϕ(N)) را محاسبه می کنیم، به طوری که d <ϕ(N).

۴. فرض کنید شما در حال طراحی یک سیستم عامل چند کاربره هستید. در سیستم عامل شما، کاربران با استفاده از رمزهای عبور وارد حساب‌های مربوطه خود می‌شوند. ذخیره رمزهای عبور کاربر در یک فایل در رایانه خطرناک است، زیرا شخصی که فایل را دریافت می‌کند به همه رمزهای عبور دسترسی دارد. به عنوان راه حل، تصمیم می‌گیرید نام کاربری و مقدار هش رمز عبور مربوطه را در فایلی به نام hpasswd ذخیره کنید. فرض کنید از یک تابع هش ایده‌آل و کاملاً تصادفی h(x) استفاده می‌کنید، یعنی h به‌طور تصادفی از همه توابع نگاشت {۰, ۱} * به {۰, ۱} k انتخاب می‌شود. h به طور عمومی

شناخته شده است. هنگامی که کاربر با رمز ورود p وارد می‌شود، سیستم عامل به کاربر دسترسی می دهد اگر h(p) با ورودی آن کاربر در hpasswd مطابقت داشته باشد. k = 20 را در سیستم عامل خود فرض کنید.

برخی از نقاط ضعف در این مکانیسم سیستم عامل شما وجود دارد. collision در هش رمز عبور ۲ کاربر، به آنها اجازه می‌دهد تا به عنوان یکدیگر وارد شوند.

(الف) فرض کنید یک مهاجم (یک کاربر عادی) می‌خواهد به عنوان مدیر سیستم با استفاده از رمزهای عبور تصادفی (بدون تکرار حدسی که قبلاً امتحان کرده است) وارد سیستم شود. حداقل تعداد حدس های رمز عبور که مهاجم باید تلاش کند تا احتمال موفقیت بیش از ۰/۶٪ داشته باشد چقدر است.

(ب) شما می‌خواهید احتمال برخورد رمز عبور کاربر را به کمتر از ۲۰ درصد در طراحی خود محدود کنید. یعنی احتمال تطابق هش رمز عبور هر دو کاربر باید کمتر از ۲۰ درصد باشد. حداکثر تعداد کاربرانی (N) که باید در سیستم عامل خود اجازه دهید چقدر است؟

۵. فرض کنید آلیس باید با استفاده از یک امضای RSA با محمد قرارداد امضا کند که در آن امضا با s = (h(m))d mod N محاسبه می شود (d کلید خصوصی آلیس است). فرض کنید که تابع هش یک تابع هش ایده آل و کاملا تصادفی h(x) است، یعنی h به طور تصادفی از همه توابع نگاشت {۰, ۱} * تا {۰, ۱} k انتخاب شده است و h به طور عمومی شناخته شده است. محمد توانسته است ۴۰ مکان متمایز پیدا کند که می تواند تغییر جزئی در قرارداد ایجاد کند: اضافه کردن یک فاصله در انتهای خط، اضافه کردن یک کاما، جایگزینی با کلمات معادل (مانند جایگزینی "موافق به پرداخت" با "مجبور به پرداخت است" مطمئناً آلیس با چنین تغییر جزئی در قرارداد مخالفت نمی‌کند و حاضر است با هر یک از این تغییرات جزئی قرارداد امضا کند.

(الف) محمد یک قرارداد متقلبانه ایجاد می‌کند که منعکس کننده افزایش قابل توجهی در مبلغی است که آلیس به محمد بدهکار است. او هش قرارداد متقلبانه را به صورت h(f) محاسبه می‌کند و نسخه‌ای از قرارداد صحیح مورد توافق با آلیس را پیدا می‌کند که به همان مقدار h(f) هش می‌شود. حداقل اندازه خروجی ایمن برای تابع هش (یعنی k =؟) چقدر است تا این برخوردها بعید باشد؟ (پاسخ تقریبی با استدلال مناسب قابل قبول است. برای به دست آوردن «k» نیازی به نشان دادن هیچ محاسباتی ندارید.)

(ب) همانطور که می‌دانید که در یک طرح امضای RSA، امضا با s = (h(m))dmod N محاسبه می شود، جایی که d کلید خصوصی است. یک طرح اصلاح شده ساده را در نظر بگیرید که در آن امضا به جای s از $s' = m^d \bmod N$ استفاده می‌شود. نشان دهید که امکان جعل امضا برای برخی از پیام‌ها در طرح دوم (تجدیدنظر شده) وجود دارد. : فرض کنید آلیس از طرح دوم (تجدیدنظر شده) برای امضای دو قرارداد m1, m2 استفاده می‌کند که به ترتیب s '1, s' 2 را ایجاد می‌کند. یک حمله از s’1، s’2 بسازید.

موفق باشید.

رستمی