به نام خدا

تمرین سری هفتم درس اصول رمزنگاری آقای دکتر محمدرضا عارف زمان تحویل: دوشنبه ۸۷/۱۰/۹

***تمرین۱: الگوریتم* Berlekamp-Massey**

قسمتی از دنباله خروجی یک ثبات پسخور خطی (LFSR) بصورت ...1001111011... است.

الف) ثباتی با کمترین خانه حافظه طراحی کنید که دنباله فوق را تولید کند.

ب) حالت اولیه ثبات را بدست آورید.

تمرین۲: کدگذاری منبع و رمزنگاری

فشرده‌سازی اطلاعات هنگام ذخیره‌سازی یا ارسال اطلاعات مورد استفاده قرار می‌گیرد. سیستم مخابراتی امن برای انتقال اطلاعات با نرخ بالا نیاز به ابزار رمزنگاری برای امن کردن ارتباط دارد. یک ساختار برای سیستم مخابراتی امن شامل بلوک‌های فشرده‌سازی و رمزنگاری پیشنهاد کنید.

***تمرین۳: ضعف سیستم رمز* DES**

در سیستم رمز قالبی DES با توجه به توابع بکاررفته در ساختار الگوریتم ثابت کنید که با مکمل‌کردن (برای مثال مکمل 00101 برابر 11010 است) متن اصلی و کلید به متن رمزشده مکمل می‌رسیم.

$$C = DES(P) \rightarrow C' = DES_{K'}(P')$$

تمرین٤: معادل بودن مسائل سخت

الف) ثابت کنید که امنیت سیستم RSA به پیمانه n معادل تجزیه به عوامل اول $\varphi(n)$ (تابع اولر) است.

ب) ثابت کنید که امنیت سیستم RSA به پیمانه n معادل مساله جذر گسسته عدد x به پیمانه n است.

*ج) اگر مساله تجزیه اعداد یک مساله سخت (NP) باشد، تابع یکطرفه درهم‌ساز وجود دارد!

تمرین۵: تاثیر حالت رمزنگاری

فرستنده پیام ۱۰۲٤ بیتی خود را با استفاده از الگوریتم رمز DES در حالت CBC (Cipher Block Chaining) رمزنگاری می‌کند.

الف) بدلیل اختلال در آنتن فرستنده دو بلوک ابتدایی متن رمزشده دچار خطا می‌شود، ولی بقیه بلوک‌های رمزشده بدرستی در گیرنده دریافت می‌شود. توضیح دهید که با فرض وجود کلید مخفی مشترک در گیرنده چه تعداد از بیت‌های پیام بدرستی رمزگشایی می‌شوند؟

ب) حال فرض کنید که بلوک‌های رمزشده در قالب بسته (packet) برای گیرنده ارسال شوند. اگر در هنگام ارسال بدلیل تاخیر کانال بسته۲ زودتر از بسته۱ دریافت شود و گیرنده متوجه این خطا نشود، چند درصد از پیام ۱۰۲٤بیتی بدرستی در گیرنده رمزگشایی خواهد شد؟

تمرین٦: تسهیم راز

الف) فرض کنید که آرزو کلیدهای مخفی رمز بلوکی K_{AB} و K_{AC} را بترتیب با بابک و کوروش به اشتراک گذاشته است. روشی ارائه دهید که آرزو بتواند بسته (packet) حاوی پیام رمزشده ارسال کند که تنها با همکاری توام بابک و کوروش قابل بازیابی باشد. پروتکل ارتباطی بین اعضا بصورت همگانی مشخص است ولی بابک، کوروش و هیچ شخص سومی نباید به‌تنهایی به پیام اصلی دست یابند.

ب) حال علاوه بر فرضیات بند (الف) فرض کنید آرزو کلید مخفی رمز بلوکی K_{AD} را با درنا به اشتراک گذاشته‌است. روشی ارائه دهید که آرزو بتواند بسته حاوی پیام رمزشده ارسال کند تا فقط با کمک حداقل ۲نفر از دوستان آرزو قابل بازیابی باشد؛ یعنی تنها زوج‌های {بابک و کوروش}، {کوروش و درنا} یا {درنا و بابک} با همکاری هم بتوانند پیام رمزشده را رمزگشایی کنند.

ج) با توجه به بند (ب) راه‌حل تسهیم راز شما چگونه گسترش می‌یابد؟ یعنی اگر n کلید تسهیم شده داشتیم و پیام رمز شده تنها با کمک حداقل m دوست ($m<n$) قابل بازیابی باشد، طول سرآیند (header) بسته را برحسب m و n بدست آورید.

تمرین۷: معادل خطی

ثابت کنید چنانچه چندجمله‌ای یک ثبات پسخور خطی (LFSR) را معکوس (reciprocal) کنیم، معادل خطی ثبات تغییری نخواهد کرد.

*در حالت کلی برای یک سیستم رمز دنباله‌ای حاوی ثبات‌های پسخور خطی هم این قضیه صادق است!

تمرین۸: ضعف امضا RSA

فرض کنید که شاهرخ امضاهای $S_1=M_1^d(\text{mod } n)$ و $S_2=M_2^d(\text{mod } n)$ از سارا، صاحب کلید خصوصی d سیستم امضا RSA در پیمانه n، برای پیام‌های بترتیب M_1 و M_2 را در اختیار دارد. شاهرخ براحتی می‌تواند امضای سارا بر روی پیام $M=M_1M_2$ را محاسبه کند. (چگونه؟) راه‌حلی ارائه دهید که شاهرخ قادر به جعل امضای سارا بر روی پیام‌ها نباشد.

تمرین۹: توافق کلید چندنفری!

اشکال عمده پروتکل توافق کلید دیفی-هلمن را با توجه به ابداع روش کلید عمومی شرح دهید. حال فرض کنید که سه نفر بصورت بی‌سیم به یک فضای مشترک ناامن به‌نوبت دسترسی دارند که برای عموم قابل شنود است. پروتکلی ارائه دهید که این سه نفر با انجام آن در نهایت بر روی یک کلید امن مشترک به توافق برسند. با فرض یک شخص مهاجم پروتکل خود را بطور کلی تحلیل کنید. آیا پروتکل شما مقیاس‌پذیر به تعداد بالاتر است؟ چه محدودیت‌هایی برای مقیاس‌پذیری پروتکل شما وجود دارد؟

تمرین۱۰: بررسی یک پروتکل صفر-دانایی

فرض کنید که پژمان مقدار x را می‌داند بطوریکه $A^x=B\ (\text{mod } p)$ و x نسبت به عدد اول p اول است. مقادیر A، B و p بصورت همگانی شناخته شده اند. پژمان می‌خواهد که به پریا ثابت کند که از مقدار x اطلاع دارد، بدون آنکه مقدار x را بطور صریح اعلام کند. برای این منظور پروتکل چهار مرحله‌ای صفر-دانایی زیر را بکار می‌برد. با توجه به پروتکل زیر به بندهای (الف) تا (ه) پاسخ دهید.

۱- پژمان $h=A^r\ (\text{mod } p)$ را با انتخاب $r<p-1$ تصادفی محاسبه کرده و آن را برای پریا می‌فرستد.
۲- پریا عدد باینری تصادفی b را اختیار کرده و آنرا برای پژمان ارسال می‌کند.
۳- پژمان مقدار S را بطور مناسبی محاسبه کرده و برای پریا ارسال می‌کند.

٤- پریا با بررسی درستی رابطه $A^S=h.B^b \pmod p$ ادعای پژمان را تایید می‌کند.

الف) پژمان مقدار S را چگونه محاسبه می‌کند تا پروتکل بدرستی کار کند.

ب) نشان دهید که عدد باینری پریا هرچه باشد، در صورت صحت ادعای پژمان، آزمون مرحله ٤ بطور صحیحی تایید می‌گردد.

ج) آیا می‌توان همواره b=1 انتخاب کرد تا بتوان یک مرحله از پروتکل فوق را کاهش داد؟

د) چرا پروتکل فوق قادر به تایید یا عدم تایید ادعای پژمان بطور یقین نمی‌باشد؟

ه) برای افزایش اعتماد به پروتکل در تعیین درستی ادعای پژمان چه راه‌حلی پیشنهاد می‌کنید؟

تمرین۱۱: تابع درهم‌ساز کلیددار (Keyed hash function)

فرض کنید که $E_K(m)$ و $D_K(c)$ بترتیب تابع رمزنگاری و رمزگشایی با کلید K بر روی پیام m و c هستند. تابع درهم‌ساز کلیددار f_1 و f_2 در زیر نمایانده شده است. الگوریتم کارایی برای یافتن تصادم (collision) در این توابع پیشنهاد کنید.

$$f_1(x,y) = E_y(x) \oplus y$$

$$f_2(x,y) = E_x(x) \oplus y$$

تمرین۱۲: ضعف حالت خاص مساله لگاریتم گسسته

پیمانه الگوریتم بر مبنای لگاریتم گسسته را بصورت $P = 2^K + 1$ اختیار کنید. فرض کنید که عدد g مولد میدان Z_P^* باشد.

الف) اگر مقدار $g^X (mod\ P)$ در اختیار باشد، آیا می‌توان از زوج یا فرد بودن X اطلاع یافت؟

ب) حال اگر X زوج باشد نشان دهید که چگونه می‌توان از زوج یا فرد بودن $X/2$ اطلاع پیدا کرد.

ج) آیا با روش ذکرشده در بند (الف) و (ب) می‌توان همه بیت‌های X را بازیابی کرد؟

د) آیا این روش در حالت انتخاب تصادفی P جواب می‌دهد؟