یا ذَالامْن و الْاَمان

تمرین شماره ۲
درس مبانی امنیت سایبری
دانشکده مهندسی و علوم کامپیوتر

مدرس: محمدرضا رازیان

اردیبهشت ۱۴۰۳

همانطوری که در درس اشاره شد یکی از روش‌های تامین اصل محرمانگی، رمزنگاری است. هدف تمرین شماره ۲ این است که با مفاهیم و اصطلاحات مرتبط با الگوریتم‌های رمز متقارن در کاربرد و مواجهه با نمونه‌های واقعی آشنا شوید.

۱ نکات مربوط به ارسال پاسخ

- ✓ هر گونه سؤال از تمرین را در سامانه درس‌افزار درس و به صورت عمومی مطرح کنید تا Fairness برقرار باشد.
- ✓ پاسخ تمرین‌ها را در قالب یک پرونده پی.دی.اف تا پایان روز جمعه ۲۱ اردیبهشت‌ماه در سامانه درس‌افزار بارگذاری نمایید. ارسال تمرین تا ۱۲ ساعت بعد از موعد تحویل، دارای جریمه ۱۵ درصدی، تا ۲۴ ساعت، ۲۰ درصد، تا ۴۸ ساعت ۶۰ درصد و پس از آن نمره‌ای نخواهد داشت (از میان تمرین‌ها، یک تمرین را می‌توانید با تاخیر ۴۸ ساعتی ارسال نمایید و نمره‌ای از شما کم نشود).
- ✓ نام و شماره دانشجویی‌تان در بالای گزارش قرار دهید
- ✓ در صورت مشاهده شباهت در پاسخ‌های ارسالی نمره منفی ۱۰۰ برای نفرات با پاسخ‌های مشابه اعمال خواهد شد.

۲ سوالات

۱.۲ بفرمایید یک فنجان رمزنگاری

لطفا به موارد زیر توضیح به اندازه و از نوشتن توضیحات اضافه پرهیز کنید.

توجه: در سوالات تعریفی صرفا اشاره یک‌خطی کفایت می‌کند. در سوالات رمزنگاری، مراحل رمزگذاری یا رمزگشایی را بنویسید

۱. رمزشده عبارت نام خانوادگی شما به فارسی با الهام از رمز **Playfair** چیست؟ کلید رمز **شهیدبهشتی** است (توجه کنید که برای الفبای فارسی این کار را انجام دهید و جدول مربوطه را با ایده خودتان بسازید و در گزارش بیاورید. بیان مراحل الزامی است).

۲. یک متن رمزشده انگلیسی که با الگوریتم Vigenère رمز شده است را بشکنید (بیان مراحل الزامی است).

۳. حمله Meet in the Middle (MitM) را به طور دقیق از جهت پیچیدگی زمانی و مکانی تحلیل کنید. بنابراین روش حمله را به مؤلفه‌هایی تجزیه کنید و برای هر مؤلفه این تحلیل را انجام دهید. در مجموع هم تحلیل زمانی و مکانی را بنویسید.

۴. ۶۴ بیت از نام خانوادگی خود به انگلیسی (کد اسکی و تبدیل نویسه به ۸ بیت و کنار هم قرار دادن ۸ بیت‌ها تا بدست آمدن یک قطعه ۶۴ بیتی) را با کلید زیر، یک دور از الگوریتم DES عبور دهید و خروجی دور اول را مرحله به مرحله بنویسید.

0110001001100101011010000110010101110011011010000111010001101001

۵. یک نمونه کتابخانه و تابع (متود) پیاده‌سازی حالت‌های عملیاتی (Operational Mode) در الگوریتم رمزنگاری AES را در زبان‌های برنامه‌نویسی Go برای سمت کارگزار و کاتلین برای سمت کارخواه بیابید و شیوه استفاده از آن‌ها را توضیح دهید (به شیوه استفاده از کلید و نام حالت عملیاتی اشاره کنید).

۶. در نسخه‌های امروزی در تلفن‌ها همراه هوشمند، اثر انگشت چگونه و در چه محلی ذخیره می‌شود؟ (از جنبه‌های محرمانگی و رمزنگاری به بیان پاسخ بپردازید)

۲.۲ به امید دیدار الگوریتم رمزنگاری شما

در این بخش از شما خواسته‌ایم تا با تقلید از الگوریتم‌های رمزنگاری مطرح‌شده در کلاس مانند DES، الگوریتم رمزگذاری مبتنی بر ساختار فیستل ارائه دهید. در ارائه الگوریتم خود موارد زیر را در نظر بگیرید و برای آن‌ها ایده بدهید و نوآوری داشته باشید.

توجه: الگوریتمی ارائه دهید که به سادگی بتوانید با یک تلاش یکی دو روزه با زبان‌های برنامه‌نویسی نظیر پایتون پیاده‌سازی کنید.

۱. جدولی حاوی فیلدهای زیر متناسب با الگوریتم خودتان ایجاد کنید و در گزارش بیاورید.

- ✓ طول قطعه (بلوک)
- ✓ طول کلید
- ✓ تعداد دورها
- ✓ الگوریتم تولید زیرکلیدها
- ✓ الگوریتم رمزگذاری
- ✓ تابع دور

۲. روندنمای (Flow chart) الگوریتم پیشنهادیتان را بکشید و تصویر آن را در گزارش قرار دهید.

۳. به تعبیر لینوس توروالدز "دو صد گفته چون نیم کردار نیست" [۱]. لطفا برای پیشنهادتان یک کد بنویسید و متن آشکار را به کدتان بدهید و رمزشده آن را بدست آورید (متن آشکار و رمزشده آن را در گزارش قرار دهید). کدتان را در مخزن گیت قرار دهید و آدرس آن در گزارش قرار دهید. به یاد داشته باشید مخزن گیت باید عمومی باشد!

موفق باشید

[۱] Talk is cheap. Show me the code