دانشگاه صنعتی امیرکبیر
دانشکده مهندسی کامپیوتر

تمرین‌های بخش رمزنگاری

دکتر حمیدرضا شهریاری

مهدی نیکوقدم

پاییز۱۴۰۱

۱. رمز جایگزینی را در نظر بگیرید که در آن به جای ۲۶ حرف از ۵۲ حرف استفاده شده است. در واقع اینطور در نظر بگیرید که تمامی حروف انگلیسی هم بزرگ و هم کوچک را شامل می‌شود. برای نمونه اگر فرض کنید E تابع رمزنگاری شما باشد، در این صورت E('S') = 'p' و E('s')='m' می‌باشد (در حقیقت با چنین تغییری فضای کلید را به ۵۲ افزایش داده‌ایم). حال آیا با چنین تغییری در مقایسه با رمز جایگزین استاندارد (تنها ۲۶ حرف در آن وجود دارد) امنیت بیشتر خواهد شد؟ دلیل خود را توضیح دهید.

۲. فرض کنید یک دانشگاه ۱۰۰ عضو هیئت علمی داشته باشد. به سوالات زیر پاسخ دهید(با فرض استفاده از رمزنگاری متقارن).

الف) اگر اعضای هیئت علمی بخواهند برای یکدیگر پیام‌های سری بفرستند، چه تعداد کلید لازم است؟

ب)اگر سناریو را اینطور در نظر بگیریم که همه به رئیس دانشگاه اعتماد دارند و اگر شخصی بخواهد پیامی را برای عضو دیگری ارسال کند، ابتدا آن را برای رئیس می‌فرستد، سپس رئیس آن را برای سایر اعضا ارسال کند چه تعداد کلید سری نیاز داریم؟

۳. انواع حملات Cryptanalysisرا نام برده و هر یک را توضیح دهید.

۴. برای رمزنگاری پیام life is full of surprises از رمزنگاری vigenere و ازکلیدHEALTH استفاده کنید(مراحل کار ذکر شود!)

۵. چرا در رمزنگاری AES فقط یک جدول جایگزینی یا همان S_box داریم در حالی که در رمزنگاری DESچندین S_box وجود دارد؟ نظر شما در این رابطه چیست؟

۶. به نظر شما چرا در حالت CFB بسیاری از بلاک‌ها تحت تاثیر یک خطا در انتقال قرار می‌گیرند؟

۷. اگر داده اصلی به صورت 1100100111010101باشد، با فرض ۴بیتی بودن بلوک های داده، الگوریتم DESرا با یک دور فیستل برای مد کاری CTRاجرا کنید. (نوشتن مراحل رمزنگاری الزامی است)

K = 1101

F(x, key) = x mod 15

Initial Counter = 0

۸. فرض کنید که DES(a,k) رمزنگاری متن ساده a را با کلید k با استفاده از سیستم رمزنگاری DES را نشان دهد.همچنین فرض کنید c = DES(a,k) و c_c= DES(a',k')، که در آن منظور از (') مکمل بیتی می‌باشد. ثابت کنید $c' = c_c$.

- **عکسی واضح از برگه پاسخ تهیه و به فرمت pdf در آورید و آپلود کنید.**
- **فرمت نامگذاری پاسخ به صورت HW2_StdNO_StdName باشد.**
- **پاسخ تمرینات حتما قبل از موعد تحویل اعلام شده در هر سری، بارگذاری شوند. تمریناتی که بعد از موعد تحویل ارسال شوند به هیچ عنوان تصحیح نخواهند شد.**
- **در صورت مشاهده تمرینات کپی شده برای طرفین نمره صفر در نظر گرفته می‌شود.**

هدف افزایش یادگیری است!

شاد باشید سرمایه‌های ایران ☺

مهدی نیکوقدم