تکلیف دوم

مهدی حق‌وردی

۲۶ فروردین ۱۴۰۳

۱

با توجه به سیستم رمزنگاری DES به سوالات زیر پاسخ دهید.

آ) تعداد کل عملیات‌های xor را بدست آورید.

ب) هدف از s-boxها را بنویسید.

ج) پیچیدگی حمله‌ی جست‌وجوی جامع به این سیستم از چه مرتبه‌ای می‌باشد؟

د) در چه حمله‌ای به این سیستم پیچیدگی زمانی از مرتبه‌ی 2^{56} خواهد شد؟

ه) اگر خروجی سیستم رمزنگاری به یک سیستم رمزنگاری دیگر داده شود، چه تغییری در امنیت آن حاصل می‌شود؟ (double des) اگر این کار سه بار تکرار شود چطور؟ (triple des)

و) ویژگی مکمل بودن این سیستم را ثابت کنید و توضیح دهید در آن صورت حمله به این سیستم از چه مرتبه‌ایست و چرا؟
خاصیت مکمل بودن DES:

$$\mathrm{DES}_{\mathrm{K}}(\mathrm{M}) = \mathrm{C} \Rightarrow \mathrm{DES}_{\overline{\mathrm{K}}}(\overline{\mathrm{M}}) = \overline{\mathrm{C}} \qquad (1)$$

۲

با استفاده از یک کلید رمز واحد، هر یک ازتبدیالت زیر را بر متن آشکار که تنها در بیت اول با هم تفاوت دارند، اعمال کنید. تعداد بیت‌های تغییر یافته پس از هرتبدیل را پیدا کنید. هرتبدیل را بطور مستقل اعمال کنید. در مورد اثر بهمنی پس از هرتبدیل بطور مستقل و سپس اثر بهمنی پس از اعمال یک راند توضیح دهید.

آ) subBytes

ب) shiftRows

ج) mixColumns

د) addRoundKey

۳

از بین مدهای عملیاتی ECB، CBC، OFB، CFB و CTR در کدام یک امکان افزایش سرعت در عمل رمزگذاری با استفاده از parallel processing یا پردازش موازی وجود دارد؟