به نام خدا

دانشگاه صنعتی شریف تمرین سری چهارم مبانی رمزنگاری و امنیت شبکه تحویل: چهارشنبه ۱۳۹۹/۲/۱۰

نحوه تحویل: پاسخ تمرین‌ها (تئوری و کامپیوتری) می‌بایست در CW آپلود شوند.

۱. فاصله قابل شکست رمز playfair را بیابید.

۲. مساله 3.16 از کتاب مرجع اصلی درس (Stallings, 7th Edition)

۳. مساله 3.22 از کتاب مرجع اصلی درس (Stallings, 7th Edition)

٤. مساله 4.2 از کتاب مرجع اصلی درس (Stallings, 7th Edition)

۵. مساله 4.4 از کتاب مرجع اصلی درس (Stallings, 7th Edition)

٦. مساله 4.7 از کتاب مرجع اصلی درس (Stallings, 7th Edition)

۷. سیستم رمز قالبی DES را در نظر بگیرید.

الف) نشان دهید که برای همه کلیدهای $K \in \{0,1\}^{56}$ و همه ورودی‌های $P \in \{0,1\}^{64}$، رابطه زیر برقرار است:

$$DES_K(P) = \overline{DES_{\bar{K}}(\bar{P})}$$

که نماد $\bar{X}$ نشان دهنده مکمل بیتی متغیر X است (برای مثال مکمل 00101 برابر 11010 است). به عبارتی، با مکمل کردن متن اصلی و کلید به متن رمزشده مکمل می‌رسیم. این ویژگی را key-complementation در DES می‌گویند.

ب) توضیح دهید که چگونه ویژگی key-complementation، حمله جستجوی فراگیر فضای کلید را از مرتبه ۲ کاهش می‌دهد.

تمرین کامپیوتری:

مساله 3.25 از کتاب مرجع اصلی درس (Stallings, 7th Edition)