به نام آن که هیچ رمزی برایش پوشیده نیست

تمرین سری ۳ رمزنگاری

دانشکده ریاضی، آمار و علوم کامپیوتر

رمزنگاری-ترم اول سال تحصیلی ۹۵-۹۴

تاریخ تحویل: شنبه ۹۴/۰۸/۲۳

۱. فرض کنید که $E : \{0,1\}^k \times \{0,1\}^n \longrightarrow \{0,1\}^n$ یک جایگشت شبه تصادفی امن باشد. نشان دهید خانواده جایگشت‌های تصادفی $E' : \{0,1\}^k \times \{0,1\}^{2n} \longrightarrow \{0,1\}^{2n}$ که برای هر $x, x' \in \{0,1\}^n$ به صورت زیر تعریف می‌شود نامن است.

$$E'_K(x||x') = E_K(x)||E_K(x \oplus x')$$

۲. فرض کنید که $F : \{0,1\}^k \times \{0,1\}^n \longrightarrow \{0,1\}^n$ یک PRF امن باشد نشان دهید که تابع G که به صورت زیر ساخته شده امن نیست.

$$G : \{0,1\}^k \times \{0,1\}^n \longleftarrow \{0,1\}^{2n}$$

$$G_K(x) = F_K(x)||F_K(\overline{x})$$

۳. با استفاده از تابع شبه تصادفی امن F در سؤال ۲ یک تابع شبه تصادفی امن مثل

$$G : \{0,1\}^k \times \{0,1\}^n \longleftarrow \{0,1\}^{2n}$$

بسازید و امنیت آن را اثبات کنید.

۴. فرض کنید $R := \{0,1\}^4$ ، تابع شبه تصادفی F را به صورت زیر در نظر بگیرید:

```
f(k,x):=
t=k[0]
for i=1 to 4 do
if (x[i-1]==1) t=bitxor(t, k[i])
output t
```

که $k = (k[0], k[1], k[2], k[3], k[4]) \in R^5$.برای مثال به ازای $x = 0101$ داریم:
$F(k, 0101) = k[0] \oplus k[2] \oplus k[4]$

فرض کنید به ازی یک کلید تصادفی k که شما نمی‌دانید چیست، اطلاعات زیر را در دست داشته باشید:

$$F(k, 0110) = 0011 \quad F(k, 0101) = 1010 \quad F(k, 1110) = 0110$$

حالا $F(k, 1101) = ?$ را محاسبه کنید.(دقت کنید، چون می‌توانید مقدار F را در یک نقطه جدید پیش بینی کنید پس این تابع شبه تصادفی امن نیست)