به نام خدا

مهدی سعیدی – 401207254

پروژه درس رمزنگاری

سوال 4

آ)

برای قسمت اول برای محاسبه جدول توزیع تفاضلی باید xor همه ورودی ها با هم و همه خروجی ها (خروجیs_box ) ها رو باهم محاسبه کنیم.

در کد موجود همانطور که در ایمیل گفتم مقدار sbox به یک متغیر رندوم وابسته است و با توجه به ان متغیر رندوم جایگشت جدیدی درست میکند که واسه همین هر بار که سعی میکنیم کد رو دوباره اجرا کنیم مقادیر تولید شده متفاوت هستند.

```
[[16, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0],
 [0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 0, 4, 0, 0, 4, 4],
 [0, 4, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 2, 2, 4, 2, 0],
 [0, 0, 4, 0, 2, 2, 2, 2, 0, 0, 0, 0, 0, 0, 0, 4],
 [0, 2, 0, 0, 2, 4, 4, 0, 0, 2, 0, 0, 2, 0, 0, 0],
 [0, 0, 2, 0, 0, 0, 0, 2, 0, 0, 4, 2, 0, 0, 2, 4],
 [0, 0, 0, 0, 2, 2, 0, 0, 4, 0, 2, 2, 0, 4, 0, 0],
 [0, 2, 2, 4, 2, 0, 2, 0, 0, 0, 2, 2, 0, 0, 0, 0],
 [0, 0, 0, 0, 0, 0, 2, 2, 2, 0, 2, 0, 0, 2, 2, 4],
 [0, 2, 0, 2, 6, 0, 0, 2, 2, 2, 0, 0, 0, 0, 0, 0],
 [0, 2, 2, 2, 0, 0, 4, 2, 0, 0, 0, 2, 2, 0, 0, 0],
 [0, 0, 2, 0, 0, 2, 0, 0, 4, 4, 2, 0, 0, 2, 0, 0],
 [0, 0, 0, 2, 0, 0, 2, 0, 2, 0, 2, 2, 2, 0, 4, 0],
 [0, 4, 2, 0, 0, 4, 0, 2, 2, 0, 0, 0, 0, 2, 0, 0],
 [0, 0, 2, 4, 0, 2, 0, 4, 0, 0, 2, 0, 0, 2, 0, 0],
 [0, 0, 0, 2, 2, 0, 0, 0, 0, 2, 0, 0, 8, 0, 2, 0]]
```

میتونیم هم hard-code شده دوباره اجرا کنیم یا اون قسمت های مربوط به جایگشت تصادفی رو کامنت کنیم. که در اون صورت مقادیر جدول به صورت زیر هستند.

Xor(x1,x2)

Xor(S.box(x1) , S.box(x2))

```
[[16, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0],
 [0, 0, 6, 0, 0, 0, 0, 2, 0, 2, 0, 0, 2, 0, 4, 0],
 [0, 6, 6, 0, 0, 0, 0, 0, 0, 2, 2, 0, 0, 0, 0, 0],
 [0, 0, 0, 6, 0, 2, 0, 0, 2, 0, 0, 0, 4, 0, 2, 0],
 [0, 0, 0, 2, 0, 2, 4, 0, 0, 2, 2, 2, 0, 0, 2, 0],
 [0, 2, 2, 0, 4, 0, 0, 4, 2, 0, 0, 2, 0, 0, 0, 0],
 [0, 0, 2, 0, 4, 0, 0, 2, 2, 0, 2, 2, 2, 0, 0, 0],
 [0, 0, 0, 0, 0, 4, 4, 0, 2, 2, 2, 2, 0, 0, 0, 0],
 [0, 0, 0, 0, 0, 2, 0, 2, 4, 0, 0, 4, 0, 2, 0, 2],
 [0, 2, 0, 0, 0, 2, 2, 2, 0, 4, 2, 0, 0, 0, 0, 2],
 [0, 0, 0, 0, 2, 2, 0, 0, 0, 4, 4, 0, 2, 2, 0, 0],
 [0, 0, 0, 2, 2, 0, 2, 2, 2, 0, 0, 4, 0, 0, 2, 0],
 [0, 4, 0, 2, 0, 2, 0, 0, 2, 0, 0, 0, 0, 0, 6, 0],
 [0, 0, 0, 0, 0, 0, 2, 2, 0, 0, 0, 0, 6, 2, 0, 4],
 [0, 2, 0, 4, 2, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 6],
 [0, 0, 0, 0, 2, 0, 2, 0, 0, 0, 0, 0, 0, 10, 0, 2]]
```

ب)